

**United States Army Signal Center and Fort Gordon
Fort Gordon, Georgia 30905-5144**



**School of Information Technology
Information Assurance Division**

**System Administrator Security Course
Week One**

10 September 2004



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Table of Contents

Introduction slides	3
STAT Scanner slides.....	6
Practical Exercise SAS 2A (STAT scanner).....	11
W2K Security intro slides.....	16
W2K Physical Security slides.....	19
Reading Assignment 1.....	33
W2K System Security.....	38
NTFS ADS Practical Exercise SAS 2C.....	48
W2K Group Policy slides.....	52
Practical Exercise SAS 2D (Group Policy).....	56
Practical Exercise SAS-2F (File Permissions).....	61
W2K Network Security slides.....	66
Practical Exercise SAS 2B (Network Monitor).....	68
Practical Exercise SAS-2G (IPSEC).....	77
W2K Authentication slides.....	83
Practical Exercise SAS-2E (Access).....	89
Practical Exercise SAS-3A (Shared Folders/Anonymous Login).....	95
W2K Account Security slides.....	106
Practical Exercise SAS-4A (Security Configuration and Analysis console).....	113
Practical Exercise SAS-4B (Security Database and Template Snap-in).....	116
W2K Auditing and Logging slides.....	122
Practical Exercise SAS-5A (Logging).....	129
Unix Security Quiz.....	132
UNIX Command Reference List.....	133
Machine and Site Preparation.....	138

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS-6A (Unix Security Intro).....	141
Best Security Practices.....	156
Reading Assignment 2.....	168
Practical Exercise SAS-7A (Hidden File Names).....	170
Practical Exercise SAS-7B (Unix System Security).....	176
Practical Exercise SAS-7C (FACL).....	189
Practical Exercise SAS-7D (Banners,etc.).....	196
Practical Exercise SAS 7E (Patches and Packages).....	199
Reading Assignment 4.....	201
UNIX Network Security.....	203
Practical Exercise SAS 8A (Remote Connections).....	211
Practical Exercise SAS 8B (Secure Shell).....	218
Practical Exercise SAS-8C (Cron).....	221
Practical Exercise SAS-8D (X Windows).....	223
Practical Exercise SAS-8E (Network Services).....	228
Practical Exercise SAS-8F (NFS, Sendmail).....	235
Practical Exercise SAS-8G (NFS).....	240
Practical Exercise SAS-9A (Account Security).....	243
Reading Assignment 5.....	249
Practical Exercise SAS 10A (Unix Auditing and Logging).....	254
Practical Exercise SAS 10B (Bad Login Log).....	259
Encryption Algorithms.....	261
Discovering a Break-in.....	263

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

 <p style="text-align: center;"><i>Introduction and Orientation</i></p> <p style="text-align: center;">Module 1</p> <p>September 10, 2004 1-1</p>	 <p style="text-align: center;">Lesson Objectives</p> <ul style="list-style-type: none">■ Course Information■ Meet the Instructor■ Course Objectives■ Course Ground Rules■ Student Introductions■ Course Outline <p>September 10, 2004 1-1</p>
 <p style="text-align: center;">Course Information</p> <ul style="list-style-type: none">■ Title<ul style="list-style-type: none">◆ System Administrator / Network Manager Security Course, course number 7E-F66/531-F21 (CT)■ Location<ul style="list-style-type: none">◆ Office: Information Assurance, Room 205, Cobb Hall, Building 25801, Fort Gordon, GA 30905◆ Phone: (706) 791-5137/5179, DSN 780, Fax 791-6161◆ Email Address: ia@gordon.army.mil◆ Web site: http://ia.gordon.army.mil■ Telephone<ul style="list-style-type: none">◆ Military phones: To dial out from the military phones, dial "9" for local and 800 numbers. To dial DSN, dial "8". No phones can dial long distance.◆ Other numbers: TSACS 791-4291, 1-800-632-0196 <p>September 10, 2004 1-1</p>	 <p style="text-align: center;">Your Staff</p> <p>Mr. Randy McNeil – Chief, IA Training</p> <p style="text-align: center;"><u>Instructors</u></p> <p>Mr. Larry McLean (NMS) Mr. Paul Gozaloff (NMS) Mr. Kelly Larsen (SAS) Ms. Sue Clark (NMS) Ms. Cynthia Jones (SAS) SFC LaBranche (SAS/NMS) SFC Jedrusiejko (SAS)</p> <p style="text-align: center;"><u>Webmaster</u></p> <p>Mr. Rodney Driggers</p>  <p>September 10, 2004 1-1</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY



Course Objective

- Week 1
 - ◆ To train DOD personnel to recognize vulnerabilities and defeat potential threats within the computer system; identify and repair common Windows 2K and UNIX operating system weaknesses and identify approved free security-based software
- Week 2
 - ◆ To train DOD personnel to recognize vulnerabilities and defeat potential threats within the network; operate and maintain firewalls using routers and bastion hosts and a simple web server Microsoft Internet Information Server (IIS)

September 10, 2004 1-1



Ground Rules

- Course materials are yours
- Ask questions any time
- Respect opinions of others
- Products mentioned or demonstrated, not endorsed
- Logistics and break schedule (smoking area, class hours, restrooms, phones & messages)
- Do not hack your fellow students!!!
- Cell phones are prohibited in class
- IASO Level 1 Security Course is a prerequisite to this course



September 10, 2004 1-1



Student Introductions

- Name
- Where you work; unit & location
- What you do; not just the job title
- What you expect to learn
- What is your computer background



September 10, 2004 1-1



Course Outline

- Day 1
 - ◆ Introduction
 - ◆ STAT Scanner and IAVA discussion
 - ◆ Security Introduction
 - ◆ Physical Security



September 10, 2004 1-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY



Course Outline

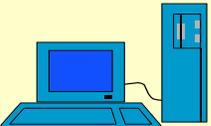
- Day 2
 - ◆ System Security
 - ◆ Network Security
- Day 3
 - ◆ Account Security
 - ◆ Auditing and Logging
 - ◆ Begin Unix Security Check List and Lab Work
- Day 4
 - ◆ Continue with Unix Security Check List and Lab Work

September 10, 2004 1-1



Course Outline

- Day 5
 - ◆ Finish Unix Security Check List and Lab Work
 - ◆ Exam (50 multiple choice questions, 1 hour, closed book/notes, 80% to certify)

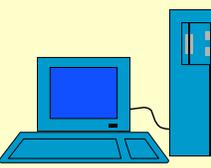


September 10, 2004 1-1



Course Outline

- Day 6
 - ◆ ACERT Brief /Network Vulnerabilities
 - ◆ Military Intelligence Brief
- Day 7
 - ◆ Encryption
 - ◆ Web Server Vulnerabilities



September 10, 2004 1-1



Course Outline

- Day 8
 - ◆ Router Security
- Day 9
 - ◆ Firewall Security
- Day 10
 - ◆ Intrusion Detection Systems
 - ◆ Exam (50 multiple choice questions, 1 hour, closed book/notes, 80% to certify)

September 10, 2004 1-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p style="text-align: right;"></p> <p style="text-align: center;">Security Threat Avoidance Technology And IAVA Process</p> <p style="text-align: right;"> 2-1</p>	<p style="text-align: right;"></p> <p style="text-align: center;">Harris STAT Scanner</p> <ul style="list-style-type: none">• A software product that performs a complete security vulnerability and analysis of your Windows NT 4.0, Windows 2000, and UNIX networks<ul style="list-style-type: none">– Uses a unique database of over 2,913 Windows NT®/Windows 2000®, Cisco Routers, HP Printers, Linux, Red Hat and UNIX® vulnerabilities (similar to a virus scanner in operation)– Vulnerabilities detected can be fixed using the AutoFix™ feature <p style="text-align: right;">2-1</p>
<p style="text-align: right;"></p> <p style="text-align: center;">Minimum Software Requirements</p> <ul style="list-style-type: none">• Windows 2000/NT 4.0 with SP 3 (or higher)• Microsoft TCP/IP, NetBEUI, or IPX/SPX protocols• Microsoft Data Access Component 2.5 or later• Internet Explorer 4 (or higher)• SSH protocol 1.5, 1.99, or 2.0 is required on UNIX systems <p style="text-align: right;">2-1</p>	<p style="text-align: right;"></p> <p style="text-align: center;">Minimum Hardware Requirements</p> <ul style="list-style-type: none">• PC or compatible:<ul style="list-style-type: none">– Pentium 133 MHz (or higher) processor– 64 MB of RAM (128 recommended)– 800 x 600 monitor resolution– Hard drive with 40 MB of free space– CD-ROM drive or Internet connection <p style="text-align: right;">2-1</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Administrative Requirements



- For a full local vulnerability analysis, the user must be logged on with an account that has local administrator privileges
- To perform an analysis of other machines on the network, the user must be logged on with an account that has domain administrator privileges
- To analyze Windows 2000/NT workgroups, the user must have administrator privileges on every machine to be scanned.

2-1

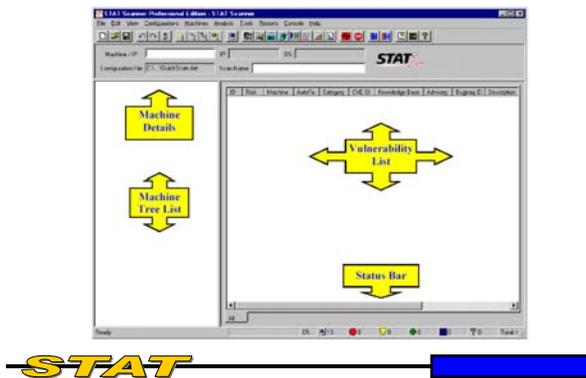
Administrative Requirements



- You need CSLA authorization to use this tool.
- POC is Julia Conyers-Lucero @ FT Huachuca
DSN 879-8259, COMM (520) 538-8259
E-Mail julia.conyers.lucero@csla.army.mil
- Need to pass training/testing 1st. Test site is online at <https://iatraining.us.army.mil>
- Once authorized, you must update STAT's vulnerabilities database often. (usually every 1-2 wks)

2-1

Getting Around in STAT Scanner



Header



The **Name** field displays the name of the computer or domain that is selected in the **Machine List**.

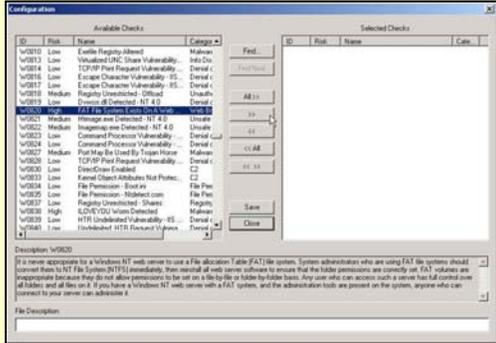
The **IP** field displays the IP address of the computer that is selected in the **Machine List**.

The **OS (Operating System)** field displays the operating system of the computer that is selected in the **Machine List**.

The **Configuration File** area of the **STAT Scanner Main screen** displays the current configuration (*.dat) file being used by the program. The default configuration file is **vcid.dat**.

2-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

2-1

Load Configuration From File

Under the **Configurations** menu, select **Load Configuration From File**. The Open display appears.



Select the Configuration (*.dat) file to be used. Click **Open**.

The file that is loaded is now the Current Configuration. **STAT Scanner** will assess the selected machines for only the vulnerabilities contained within the selected file.

2-1

Risk Levels

Vulnerabilities are classified in five different levels of risks:

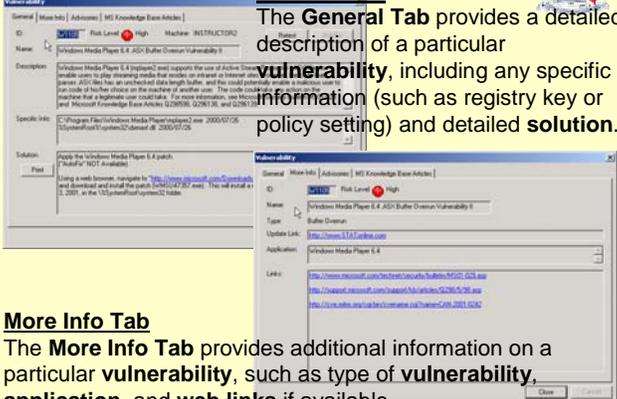
- 🔴 **High** - Grants unauthorized administrative access or privilege elevation to System or Administrator level.
- 🟡 **Medium** - Grants unauthorized access or serious denial of service.
- 🟢 **Low** - Potential to grant unauthorized access or denial of service.
- 🟠 **Warning** - Recommended for good security practices.
- 🔍 **Unable To Assess** - STAT Scanner cannot assess the vulnerability.

2-1

Vulnerabilities

General Tab

The **General Tab** provides a detailed description of a particular **vulnerability**, including any specific **information** (such as registry key or policy setting) and detailed **solution**.

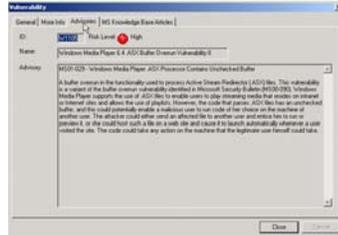


More Info Tab

The **More Info Tab** provides additional information on a particular **vulnerability**, such as type of **vulnerability**, **application**, and **web links** if available.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Vulnerabilities Cont...



Advisories Tab

The **Advisories Tab** provides a **security advisory**, if available, for a particular **vulnerability**. Advisories include **Microsoft Security Bulletins**, **CERT Advisories**, **CIAC Bulletins**, as well as other security advisories.

Knowledge Base Tab

The **Knowledge Base Tab** provides the **Microsoft Knowledge Base article's**, if any, associated with a particular **vulnerability** such as type of **vulnerability**, **application**, and **web links** if available



Lesson Review



- Introduction to STAT Scanner
- Getting Around in STAT Scanner
- Selecting machines to scan
- Configuration of Vulnerabilities for scan
- Scanning
- Results of the scan

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

W2K System Security

Practical Exercise SAS 2A

EXERCISE A

This practical exercise will provide hands-on experimentation with the STAT scanner. On the W2K server please logon local as the Administrator and perform the following:

Check for vulnerability on your local machine.

1. Start the STAT application. Double click on the STAT icon on your desktop.
2. Close the read me screen if it is displayed.
3. Close tip of the day screen if it is displayed.
4. Change the configuration, from the STAT scanner main screen select:
Configuration > Load configuration from file
This open display allows you to select various types of categories to examine or autofix.
Select IE.dat >click on open
On your STAT main screen, the configuration File should now read IE.dat (Upper left corner.)
5. Perform an Analysis, from the console menu select:
Analysis > Perform an Analysis or select the red sign wave icon on your toolbar. You may see the "Scan Ports & Services Screen. Leave defaults and hit scan. Click ok on warning banner. Note: If IE6 is installed with all hotfixes no vulnerabilities should be found. Faults will be found in the right window. For classroom purposes, **DO NOT FIX THE ID# W0064 "FAT FILE SYSTEMS EXISTS."** It is needed for our Ghost version.
6. Change the configuration file setting to C2.dat and perform an analysis. The Replace/Append dialog box will appear if there is at least one scan already completed. Click Replace; note all the high and low risk vulnerabilities.
7. Change the configuration file setting to all.dat and perform an analysis. Click Replace. Note: Your machine should display numerous vulnerabilities. Scan down the list and locate ID # W0149. (if not there, pick a couple others)
8. What type of vulnerability does it display?

9. Could this vulnerability be auto fixed?

10. Scan other machines in your subnet.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

11. From the STAT scanner main screen select:
Machines > Select Machines... Also ensure the block “Automatically Test for Admin Rights” is selected.
12. The Machine list menu will be displayed. Find Machines to scan will open the Machine selection Wizard. Select:
IP Range Selection...
(Select a range of two computers that will include your machine and that of the neighbor within your domain.)
Starting IP Address 147.51.217.xxx (Instructors will inform of IP Addressing scheme for each site)
Ending IP Address 147.51.217.xxx
Click on Next
(Standby while your computer does a search)
Click on OK
13. Select the two computers that are now present on the Machine Selection Wizard and add them to the computers currently selected. Close the wizard by hitting Finish. Save and close.
14. From the STAT scanner main screen: Highlight one computer hold down the shift key and select the other computer. Perform an analysis using the steps you learned above. Use the all.dat file.
15. You should see all of the vulnerabilities that the scanner performed on the machines on the right pane, or you could select each machine from its tab on the bottom and examine each machine's vulnerability.
16. Take ten minutes to view some of the vulnerabilities that were found by the STAT scanner.
17. Wait for instructor review.

Exercise B

ation of custom IAVA configuration files

A. In version 5.222+ of STAT Scanner, the IAVA numbers are available in the configuration editor. This allows you to more easily create a custom IAVA scan file.
Perform the following steps:

1. open STAT Scanner
2. select [configuration] [new configuration]
3. On the left hand side of the editor, scroll to the right and find the ACERT IAVA ID.
4. click on the top of the column to sort on the ACERT IAVA ID
5. select desired IAVAs and click the [>>] button
6. click [save] and give it file name (IAW LSOP), click [save]
7. click [close]
8. select [load configuration from file....] select [newly created file]
Note.
 - a. in the Configuration File window verify that the correct file name is loaded
9. Perform an analysis
10. Review the vulnerability results, Scan Summary, and Port and Services Report.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

B. Lets look at the procedures to run a single scan that will verify if your Anti-Virus DAT files are out of date and then create a custom configuration DAT file:

1. Open STAT Scanner
2. select [configuration] [new configuration] the configuration display appears
3. From the [available checks] window of the configuration display, select the following vulnerabilities by clicking on it with the mouse. (hint: hold the ctrl key to select multiple vulnerabilities at once and look in the Category Column for Anti-Virus)

W1142 McAfee (Network Associates) Medium
W1986 Norton (Symantec) Medium
W1999 Trend (PC-cillian)

Also add to the new custom configuration file:

W1983 Spyware Detection
W1985 Warning Network/Monitor Sniffer
W1798 LastLogon username

4. The vulnerabilities selected will be moved to the selected check column. If you accidentally added a check by mistake remove by selecting << option.
5. click [save] and give it file name (IAW LSOP)
6. click [close]
7. select [load configuration from file....]
8. select the newly created file
9. scan your network

Additional Information:

The Department of the Army CIO/G-6 IAVA training site is in development. The first training modules available from this site are Harris Stat Training Modules. There are 3 modules for the Harris Stat training. You must register a User ID and Password for this site before being allowed access to the training modules. (<http://iatraining.us.army.mil>)

STAT Scanner has published a STAT-IAVA cross-reference file. This file does not need to be requested and is available to any Army user with a licensed copy of STAT Scanner. The file may be downloaded from RCERT CONUS or from the STAT Premier Web Site, which is the same location for downloading program updates.

To download the IAVA mapping file from the Premier Web Site:

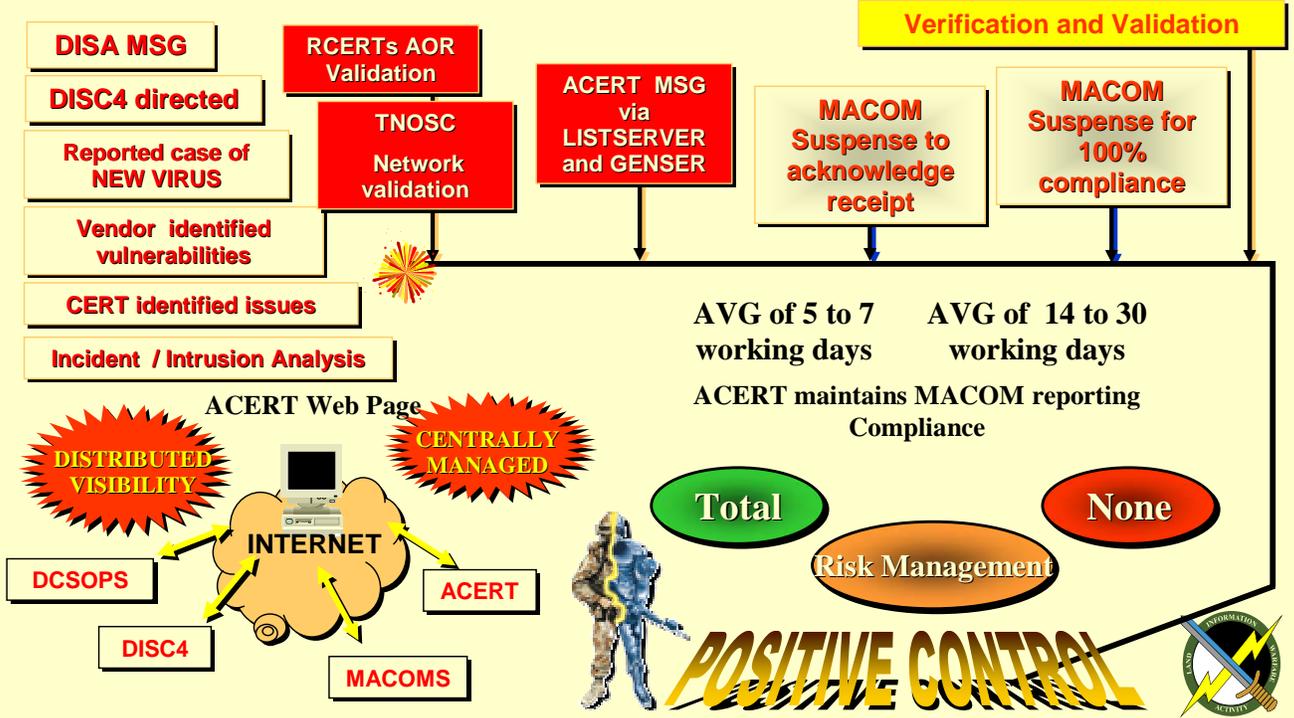
PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

1. Go to RCERT CONUS at www.rcert-c.army.mil/stat_index.html (you must be at a .mil site) or <https://premier.harris.com/stat/>
2. Login (depends on download site)
3. Locate and Select "STAT Scanner - Army IAVA Configuration File" This is the configuration file with the list of vulnerabilities the STAT program will use.
4. Locate and Select "army_iava_stat_scanner_vuln_mapping_1-27-03.pdf" (The name of the file will change slightly each time it is released to reflect the date of most current release). This is for your reading enjoyment.
5. Done.

Army Information Assurance Vulnerability Alert Process



**T
R
I
G
G
E
R
S**



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p style="text-align: right;"></p> <p style="text-align: center;">System Administrator/Network Manager Security Course</p> <p style="text-align: center;">W2K Security Introduction Module 3</p>	<p style="text-align: right;"></p> <p style="text-align: center;">Win2K Security Features</p> <p><i>Group</i></p> <ul style="list-style-type: none">• ^Policy Editor is still your friend<ul style="list-style-type: none">– System Polices are replaced with Group Policies– Changes are easily reversed• IntelliMirror<ul style="list-style-type: none">– Control to W2K Pro systems– Defines policies based on respective user's business roles, group memberships and locations• Active Directory <p style="text-align: right;">3-1</p>
<p style="text-align: right;"></p> <p style="text-align: center;">Win2K Security Features (cont)</p> <ul style="list-style-type: none">• Multiple Authentication Protocols• Certificate Services• IP Security Extensions (IPSec)• Transport Layer Security (TLS) & Secure Socket Layer (SSL)• Disk Quota Support• Encrypting File System (EFS)• Kerberos• Layer 2 Tunneling Protocol (L2TP) <p style="text-align: right;">3-1</p>	<p style="text-align: right;"></p> <p style="text-align: center;">Win2K Security Issues</p> <ul style="list-style-type: none">• More complex then other versions of Windows• 3rd party software incorporated into OS<ul style="list-style-type: none">– IPSec, Kerberos• Trust is transitive<ul style="list-style-type: none">– Implicit– Explicit <p style="text-align: right;">3-1</p>

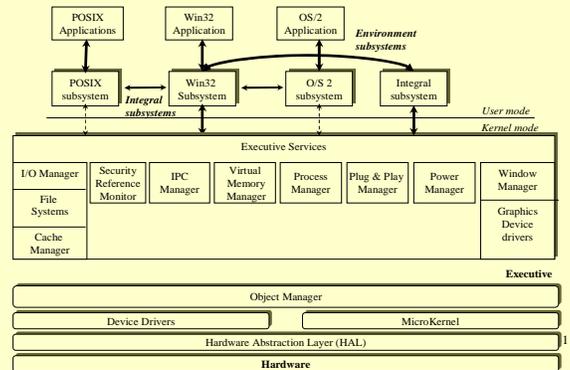
PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Win2K Features or Issues ?

- Automatic Log-on Support
- Indexing Service
- Single Sign-on
 - Directory information can be accessed by various operating systems
 - Allows users the ability to access files, printers, web services with one sign-on
- Kerberos Support
 - MS version of Kerberos
 - Win2K networks only

3-1

W2K Architecture Overview

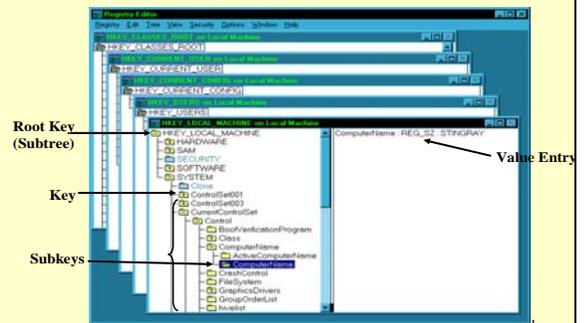


W2K Security Architecture Components

- Security Reference Monitor (SRM)
- Local Security Authority (LSA)
- Logon Process
- Graphical Identification and Authentication (GINA)
- Network Logon Service
- Security Packages
- Security Support Provider Interface (SSPI)
- Security Account Manager (SAM)
- Active Directory (AD)

3-1

The Registry Structure

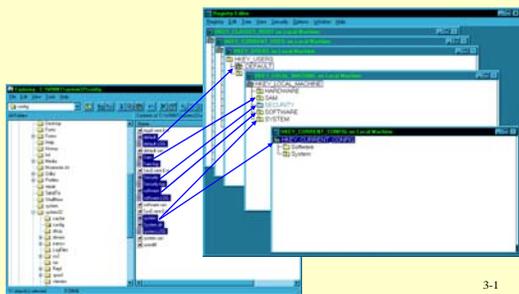


PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Regedit.exe	
Vulnerability	Countermeasures
<p>Regedit.exe may be found associated with registry files. An attacker can mail or place a .reg registry file on the system, causing it to modify the registry when the file is run.</p>	<p><input type="checkbox"/> 1. Associate the .reg file name extension with a text editor.</p> <ul style="list-style-type: none"> • Go to control panel and double click on “Folder Options”. • Click on “File Types” tab. Drill down till you find “REG Registration Entries”. • Highlight and click on change. Drill down till you find Notepad. • Highlight Notepad and click on OK. • . reg will now be associated with Notepad. <p><input type="checkbox"/> 2. Modify the registry with the following entry.</p> <ul style="list-style-type: none"> • Run regedt32.exe • Go to the HKEY_LOCAL_MACHINE/Software/Classes/regfile/shell/open/ command key. • Double-click the value that is similar to : REG_SZ : regedit.exe %1 to display the String Editor. • Change the regedit.exe entry to notepad.exe. DO NOT ALTER any portion of the string. • Click OK. <p>Note: After completing the association, if a .reg file appears in your text editor, then an attack may be in progress to compromise your system.</p> <p>References: Microsoft Knowledge Base Article Q132664</p>

Registry Hives 

■ The Registry Hives map directly to operating system files



3-1

Registry Editors 

WARNING!

Incorrect use of the Registry Editor can cause serious, system wide problems that may require the reinstallation of Windows 2000.

3-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

 <p>System Administrator/ Network Manager Security Course</p> <p>W2K Checklist Physical Security</p> <p style="text-align: right; font-size: small;">3-2</p>	 <p>Control Server Access</p> <ul style="list-style-type: none"> • Access by unauthorized personnel could result in <ul style="list-style-type: none"> – theft of peripherals, – denial of service, – security overrides via removable media, – miscellaneous tampering. • Remember that there is NO security without Physical Security. Control the keys and control the access <p style="text-align: right; font-size: small;">3-2</p>
--	--

Server Access	
Vulnerability	Countermeasure
<p>Physical access by unauthorized personnel could result in theft of peripherals, denial of service, security overrides via removable media, or miscellaneous tampering. Remember that there is NO security without Physical Security. Access to the interior of the CPU case exposes the computer to theft, sabotage, and reconfiguration.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> 1. Place the server in a locked room accessible only by the System Administrator. <ul style="list-style-type: none"> • Maintain a list of personnel authorized entry • Establish key/access control. <input type="checkbox"/> 2. PHYSICALLY lock the CPU case

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<div style="text-align: center;">  <h3 style="margin: 0;">Input/Output devices</h3> </div> <ul style="list-style-type: none"> Connected peripheral devices provide easy access for the would be hacker. Removal of unneeded input devices prevents any one from causing the system to execute programs or loading software. <p style="text-align: right; font-size: small;">3-1</p>	<div style="text-align: center;">  <h3 style="margin: 0;">Manage your CMOS</h3> </div> <ul style="list-style-type: none"> Alter your boot-up sequence so that removable media can not be used for boot up. Establish a CMOS password to protect your settings Lock the computer case to prohibit removal of the CMOS battery and resetting of the CMOS password. <p style="text-align: right; font-size: small;">3-1</p>
--	--

<i>Input/Output Devices</i>	
Vulnerability	Countermeasure
If your system has peripheral devices connected, then it will not take an attacker long to gain access. Removal of input devices prevents any one from causing the system to execute programs or load software.	<input type="checkbox"/> 1. Remove the Keyboard, mouse, and monitor, if possible.

<i>Check equipment for unauthorized attached devices</i>	
Vulnerability	Countermeasure
Devices can be attached to equipment which can record network transmission, keystrokes, or other information	<input type="checkbox"/> 1. IT equipment should not have any attached equipment or connections that are unknown to the system administrator. Check network transmission lines for additional devices. Check USB, serial, and parallel ports for attached equipment.

<i>Smart Card Readers</i>	
Vulnerability	Countermeasure
Equipment must be in place before advanced authentication methods can be utilized.	<input type="checkbox"/> 1. Install Smart Card readers to enable advanced authentication techniques.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

--	--

Boot Sequence	
Vulnerability	Countermeasures
<p>An operating system can be rebooted using removable media. Once rebooted, the operating system can be modified or reinstalled, overriding password controls.</p>	<ul style="list-style-type: none"> <li style="margin-bottom: 10px;"><input type="checkbox"/> 1. CHANGE the Boot sequence (in the CMOS). <li style="margin-bottom: 10px;">• Change boot sequence to Hard drive, CDROM, then Floppy. For complete safety, change it so only the hard drive is available for boot. <p>Note:</p> <ul style="list-style-type: none"> <li style="margin-bottom: 10px;">• Most personal computers today can start a number of different operating systems. For example, if normally Windows 2000 is started from the C: drive, another version of Windows could be selected from another drive, including a floppy drive or CD-ROM drive. If this happens, security precautions taken within the default version of Windows 2000 might be circumvented. <li style="margin-bottom: 10px;">• In general, install only those operating systems required. For a highly secure system, this will probably mean installing one version of Windows 2000 and ensuring that all partitions are NTFS volumes.

CMOS Passwords	
Vulnerability	Countermeasures
<p>Access to the CMOS enables changing of the boot sequence order. Changing the boot sequence can enable reboot via removable media.</p>	<ul style="list-style-type: none"> <li style="margin-bottom: 10px;"><input type="checkbox"/> 1. INSTALL a CMOS password.

Hard drives	
Vulnerability	Countermeasure
<p>It is trivial to take the hard drive from one system and read it on another. Hard drives are the goal of any attacker who has physical access to your system.</p>	<ul style="list-style-type: none"> <li style="margin-bottom: 10px;"><input type="checkbox"/> 1. Physically lock the CPU case.

Removable Media	
Vulnerability	Countermeasure

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

AutoPlay begins reading from a CD-ROM drive as soon as media is inserted in the drive. As a result, the setup file of programs and the sound on audio media starts immediately. This could lead to introduction of viruses and malicious code.

Note:

For more info go to Microsoft Knowledge Base and lookup Q155217.

□ 1. Disable Automatically Running CD-ROMs. By default, AutoPlay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.

- Click Start, click Run, type regedit in the Open box, and then press ENTER.
- Locate and click the following registry key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDRom

- To disable automatically running CD-ROMs, change the Autorun value to 0 (zero). To enable automatically running CD-ROMs, change the Autorun value to 1.
- Restart your computer.

Additional Information

There are two other registry keys that can affect this functionality:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ExplorerNoDriveTypeAutoRun = 0x00000095

-and-

HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\ExplorerNoDriveTypeAutoRun = 0x00000095

Alternate method using the MMC.

- Disable Automatically Running CD-ROMs by snapping in the Group Policy utilizing the MMC.
- Expand the Local Computer Policy, Computer Configuration, and Administrative Templates folders, till you can click on the System folder.
- Double click on Disable AutoPlay, then click on enable. Choose Disable AutoPlay on CD-ROM drives or in the dropdown box choose All Drives.
- Click on Apply

Note:

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<ul style="list-style-type: none"> • By default, AutoPlay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives. If you enable this policy, you can also disable AutoPlay on CD-ROM drives, or disable AutoPlay on all drives. This policy disables AutoPlay on additional types of drives. You cannot use this policy to enable AutoPlay on drives on which it is disabled by default. This policy appears in both the Computer Configuration and User Configuration folders. If the settings conflict, the setting in Computer Configuration takes precedence over the setting in User Configuration. A Media Change Notification (MCN) message from the CD-ROM drive triggers AutoPlay. If the Windows interface does not receive this message, AutoPlay does not operate, regardless of the value of this entry. Entries that suppress the MCN message, such as <u>Autorun</u> and <u>AutoRunAlwaysDisable</u> also disable AutoPlay.
--	---



Protect Unattended Workstations

- Utilize passwords with your screen savers
- Lock your workstation or log out when leaving your workstation for any period of time.

3-1

Lock Workstations	
Vulnerability	Countermeasures
<p>If workstation consoles are left unattended and not secured, unauthorized personnel could access the</p>	<p><input type="checkbox"/> 1. LOCK your workstation/console whenever a workstation/console is left unattended.</p> <ul style="list-style-type: none"> • Press <Ctl>, <alt> simultaneously. The default is “Lock Workstation”, then hit Enter

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>workstation and the associated network system.</p>	<ul style="list-style-type: none"> • <input type="checkbox"/> 2. Here is how you create a shortcut to lock a computer without using the "Ctrl, Alt, Del" keys. <ul style="list-style-type: none"> • Start Windows Explorer. • Navigate to %userprofile%\application data\microsoft\internet explorer\quick launch (e.g., C:\documents and settings\john\application data\microsoft\internet explorer\quick launch). • Right-click in the right-hand pane and select New, Shortcut. • Enter "rundll32.exe user32.dll,LockWorkStation" without the quotes and click Next. • Name the shortcut "Lock Workstation" and click Finish. • To change the icon highlight the following text and select the appropriate icon. • Select the icon shortcut you just created. • Right click and select properties. • Select "Change Icon" in the lower right corner. • Select the following text: %SystemRoot%\system32\SHELL32.dll and paste the text in the "File Name" box. Select "OK" and "OK". • If you want to place the icon in the System Tray drop and drag the icon to the position desired. Delete the icon on the desktop.
---	--

Screen Saver Passwords	
Vulnerability	Countermeasure
<p>If a workstation is left unattended and the screen saver is not password protected, unauthorized personnel could access the workstation and the associated network.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> 1. IMPLEMENT a Screen Saver Password <ul style="list-style-type: none"> • Right click on the desktop background • Select properties • Select the "Screen Saver" tab. • Choose a screen saver from the screen saver drop down menu. Make sure you choose one that enables the "password protected" • Check the password protected box. Your Windows 2000 password will now grant you access should the screen saver engage. • Set the wait time so that the screen will engage in 10 minutes or less. A specified period of 3-5 minutes of no activity is recommended. • Click on the apply button and close the display properties window

Develop a Backup Strategy



- Identify personnel for members of Backup Operators group
- Identify Systems and data
- Determine the type of backup
- Store backed up data off site
- Test the backup plan and backup data
- Provide training for those performing backups
- Document all backup requirements and procedures

3-1

Backups	
Vulnerability	Countermeasures
<p>Since backup tapes contain sensitive information from your system, to include user data, and passwords, they become a target for anyone who has physical access to your system.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> 1. Ensure the following are addressed in you local IA SOP <ul style="list-style-type: none"> • MAKE regular backups. • UPDATE your backups whenever you update or change your system. • ENSURE that EVERYTHING on your system is addressed in your backup plan. • DO NOT reuse a backup tape too many times because it will eventually fail. • RESTORE a few files from your backup tapes on a regular basis. This ensures that you have good backup tapes. • REBUILD your system from a set of backup tapes to be certain that your backup procedures are complete. • KEEP your backup tapes under lock and key. • Keep written records of key backup and system configuration information. • Store back-up tapes off-site whenever possible. • Encrypt back-up tapes whenever possible. <input type="checkbox"/> 2. Create an Emergency Repair Disk <ul style="list-style-type: none"> • Click the Start button, Select Programs, Select Accessories, Select System Tools, click Backup • On the General Tab, click the <i>Create an Emergency Repair Disk</i> button. • When prompted, insert a blank, formatted 1.44 MB

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p>disk in the floppy drive and click OK</p> <ul style="list-style-type: none"> • When the process is complete, remove the disk, label it “Emergency Repair disk” and then store it in a safe location. <p>Note: Make sure to create an ERD when your computer is functioning well so that you are prepared if you need to repair system files</p>
--	--

Uninterruptible Power Supplies (UPS)	
Vulnerability	Countermeasure
Unexpected power loss can compromise security and data integrity	<input type="checkbox"/> 1. Install Uninterruptible power supplies on all critical IT systems.



Emergency Repair Disks

- Make sure that you maintain an updated Emergency Repair Disk for all of your critical systems.
- The Emergency Repair Disk (ERD) can help you to repair or recover a system that can't load Windows 2000. The ERD helps you repair problems with system files and the partition boot sector.

3-1

Emergency Repair Disks (ERD)	
Vulnerability	Countermeasure
The Emergency Repair Disk (ERD) provides the capability to repair or recover a system that can't load Windows 2000. The ERD provides the capability to repair problems with system files and the	<input type="checkbox"/> 1. Repair damaged system with ERD. If a system failure occurs, you can start the system using the Windows 2000 Setup CD or the Windows 2000 Setup floppy disks which can be created by running Makeboot.exe from the Boot disk folder on the Windows 2000 Setup CD. Then use the Emergency Repair Process to restore core system files. <input type="checkbox"/> 2. Re-apply the checklist after a repair to ensure the integrity of the security of the system.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

partition boot sector. This situation occurs when the hard disk fails or when some of the system files are corrupted or accidentally deleted. *System files* are the files Windows 2000 uses to load, configure, and run the operating system. If some system files are missing or corrupted, you can use the ERD to repair those files.

Note:

Try using safe mode or the Recovery console before using an ERD.

Important

- The ERD allows you to make only basic system repairs, such as to the system files, boot sector, and startup environment. The ERD does not back up data, programs, or the registry and is not a replacement for regular system backups.
- The Windows 2000 ERD, unlike the ERD used with Windows NT, does not contain a copy of the registry files. The backup registry files are in the folder %SystemRoot%\Repair. However, these files are from the original installation of Windows 2000. In the event of a problem, they can be used to return your computer to a usable state.
- When you back up system state data, a copy of your registry files is placed in the folder %SystemRoot%\Repair\Regback. If your registry files become corrupted or are accidentally erased, use the files in this folder to repair your registry without performing a full restore of the system state data. This method is recommended for advanced users only and can also be accomplished by using the Recovery Console commands.
- Because missing or corrupted files are replaced with files from the Windows 2000 CD, any changes you made to the system after the original installation are lost.
- The ERD must include current configuration information. Make sure that you have an ERD for each installation of Windows 2000 on your computer, and never use an ERD from another computer.
 - To restore your settings from the ERD, the Windows 2000 CD, the Windows 2000 Setup disks, and the ERD are required. During the restoration process, you can press F1 for more information about your options.



Configuration Management

- Maintain an up-to-date listing of
 - systems,
 - software versions and patches loaded,
 - peripheral devices, and required drivers.

3-1

Configuration Management	
Vulnerability	Countermeasures
Rebuilding a system from scratch can be complicated by a lack of documentation. Backup tapes/disks are not always enough.	<input type="checkbox"/> 1. Document all hardware and software configurations in a Configuration Management database. Including but not limited to: <ul style="list-style-type: none">• System architecture• Key nodes and connections identified.• Software Inventory• Patches and OS versions information• BIOS and partitioning information.• Additional device drivers per requirements.• Document and mark all cables and connections.



Facilities

- Ensure that your facilities meet your security requirements
- Conduct risk assessments which address your physical environment
- Maintain a proper security environment per requirements (ie. tempest, temperature control, black/red separation)

3-1

Facilities	
Vulnerability	Countermeasures
Improperly maintained facilities can be a source of service disruption.	<input type="checkbox"/> 1. Ensure the following are addressed in you local IA SOP <ul style="list-style-type: none"> • Separate black-red communication lines. • If TEMPEST requirements apply to the system, has TEMPEST testing been accomplished. • Are TEMPEST test results acceptable or is the physical control zone sufficient. • Conduct a physical risk assessment. • Is there adequate power or UPS support available. • Make sure hardware and software configurations support the security policy. • Maintain proper temperatures per manufacturer specifications.
syskey	
Vulnerability	Countermeasures
To provide greater level of protection for master keys and various other secrets use the system key. The system key protects the following sensitive information:	<input type="checkbox"/> 1. For all computers in a domain, the secret key is enabled by default and all master keys and protection keys stored on a computer are encrypted with the unique 128-bit symmetric random system key. The system key must be in volatile memory on the operating system during system startup to unlock the password protection key. There are three ways to configure the system key for computers: <ul style="list-style-type: none"> • Use a computer-generated random key as the system

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<ul style="list-style-type: none">• Master keys that are used to protect private keys• Protection keys for user account passwords stored in Active Directory• Protection keys for passwords stored in the registry in the local Security Accounts Manager (SAM) registry key• Protection keys for LSA secrets• The protection key for the administrator account password that is used for system recovery startup in safe mode	<p>key and store it on the local system by using a complex obfuscation algorithm that scatters the system key throughout the registry. This option allows you to restart the computer without having to enter the system key. This is the default configuration for the system key.</p> <ul style="list-style-type: none">• Use a computer-generated random key, but store it on a floppy disk. The system key is not stored anywhere on the local computer, and the floppy disk must be inserted for the system to start. It is inserted when prompted after Windows 2000 begins the startup sequence, but before it is available for users to log on to the system.• Use a password chosen by the administrator to derive the system key. The password is not stored anywhere on the computer. Windows 2000 prompts the administrator for the password when the system is in the initial startup sequence, but before the system is available for users to log on. <p>The system key configuration options are available from the system key dialog boxes that appear when you run syskey. For computers in a domain, you must be a member of the Domain Admin group to run syskey. For stand-alone computers, you must be logged on as the local Administrator to run syskey. You can configure the system key differently for each computer in the domain.</p> <p>System key protection is enabled by default in each domain, but you might want to change the default system key option for various computers in a domain. You also might need to enable system key protection for stand-alone computers.</p> <p>To configure system key protection</p> <ol style="list-style-type: none">1. Type syskey at the command prompt. This brings up the dialog box. After system key protection is enabled, it cannot be disabled.2. If it is not already selected, click Encryption Enabled, and then click OK. After a reminder that you should create an updated emergency repair disk, you are presented with options for the Account Database Key. The default option is a system-generated password that is stored locally.3. Select the system key option that you want, and then click OK.
--	---

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

4. Restart the computer.

When the system restarts, you might be prompted to enter the system key, depending on the key option you chose.

Windows 2000 detects the first use of the system key and generates a new random password encryption key. The password encryption key is protected with the system key, and then all account password information is strongly encrypted.

At subsequent startups:

1. Windows 2000 obtains the system key, either from the locally stored key, the password entry, or insertion of a floppy disk, depending on the option you chose.
2. Windows 2000 uses the system key to decrypt the master protection key.
3. Windows 2000 uses the master protection key to derive the per-user account password encryption key that is then used to decrypt the password information in Active Directory or the local SAM registry key.

The syskey command can be used again later to change the system key storage option or to change the password.

To change the system key option or password

1. Type syskey at a command prompt to bring up the initial system key dialog box.
2. Click Update.
3. In the Account Database Key dialog box, select a key option or change the password, and then click OK.
4. Restart the computer.

Changing the system key requires knowledge of, or possession of, the current system key. If the password-derived system key option is used, syskey does not enforce a minimum password length; however, passwords longer than 12 characters are recommended. The maximum length is 128 characters.

Warning

If the system key password is forgotten or the floppy disk that contains the system key is lost, it might not be possible to start the system. Protect and store the system key safely. If it is on a floppy disk, make backup copies and store them in a different location. The only way to recover the system if the system key is lost is by using a repair disk to restore the registry to a state prior to enabling system key protection. This means that you would lose any information or changes which have accrued since then.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p>System key options can be configured independently on all computers in a domain. When configured for the system key, each computer has a unique password encryption key and a unique system key. For example, the first domain controller might be configured to use a computer-generated system key stored on a disk, and secondary domain controllers might each use a different computer-generated system key stored on the local system. A computer-generated system key stored locally on a primary domain controller is not replicated.</p> <p> Before enabling the system key when you have a single domain controller, you might want to ensure that a second, complete, updated domain controller is available as a backup system until changes to the first domain controller are complete and verified. Before you change the system key options on a computer, it is recommended that you make a fresh  copy of the emergency repair disk for that computer.</p>
--	---



Reading Assignment 1

Day 1

All W2K related reading assignments come from the "Microsoft Windows Security Resource Kit"

Subjects covered in this reading assignment are: Securing accounts, SIDs, Authentication, Group policies, Permissions, and the Encrypting File System,

Pages to read are: 33 - 43, 67 - 113, 135 - 171

1. What are the components of a SID?

2. The contents of an access token include?

3. What does the RunAs service do?

4. Why is Lan Manager (LM) authentication especially vulnerable?

5. What is the default authentication protocol in Windows 2000?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

6. Which authentication protocol protects you from replay attacks? How?



7. What are LSA secrets?

8.  What does a GPO applied to an OU affect?



9. What does block inheritance mean?



10. Who does a Group Policy Object pertain to when it is applied to a container?

11. What do the acronyms DACL and SACL stand for?



12. What permissions can be assigned to an NTFS folder? Which one can not be applied to a file?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY



13. What does the acronym FEK stand for and when is it created?



14. True or False, EFS uses an asymmetric encryption algorithm along with the FEK to encrypt files?



15. Does decryption take place when EFS encrypted files are moved to a non-NTFS partition or to a remote server?





16. A registry key has which two basic permissions?

17. True/False: Can administrators take ownership of files and folders on the local computer.



Topics covered: TCP/IP Security, Security Templates and Auditing.

Pages to read: 205 -241, 269 - 302, 305 – 334, 519-527



17. What is TCP/IP and list some common threats to TCP/IP?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

18. What does TCP filtering allow you to do?

19. What are the two protocols that comprise IPSEC?

20. What are IPSEC's two modes?

21. IPsec in W2K, WXP has what 3 pre-created policies?

22. Local policies are separated into what three sub-categories?

23. What is included in the Security-Configuration Toolset?

24. True or False, the secedit.exe command has all the functionality of the Security Configuration and Analysis MMC snap-in?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

25. What is the default, maximum size that an event log can reach before the overwrite behavior is initiated?

26. What is another name for the "stop error" generated when events can not be written to the security event log?

27. By tracking failed logon events, your organization might be able to prevent?

28. True or False, Windows 95 and 98 clients do not generate computer logon event entries for network logon events?

29. MBSA is used for _____

30. The two core protocols of the transport layer are?



System Administrator/Network Manager Security Course

W2K Checklist System Security

Service Packs/Hot Fixes/Patches	
Vulnerability	Countermeasure
<p><i>IAW MSG DTG 042100Z Mar99 Fm ACERT Ft Belvoir VA.</i></p> <p><i>A. Ensure all Hotfixes (HF) and Service Packs (SP) approved by ACERT are installed on your computer.</i></p> <p>Note: Review the service pack read me file for hardware/software compatibility. HF/SP may, in some cases decrease the level of security on your system. Re-implement this checklist again after installing any new HF/SP. Failure to comply with these directives could leave</p>	<p><input type="checkbox"/> 1. Verify the most-current service pack for Windows 2000 is installed.</p> <ul style="list-style-type: none"> • From the menu bar click “Start” and then “<u>R</u>un”. • Type “winver.exe” in the dialog box and click OK. (You should see a dialog box that displays the following info. “Version 5.0 (Build 2195: Service Pack 1 or greater).”) <p><input type="checkbox"/> 2. Verify 128 bit version of the Service Pack 1 is installed:</p> <ul style="list-style-type: none"> • Select the NDISWAN.SYS member in the %systemroot%\System32\Drivers directory. • Right-click on the member to bring up the context menu. • Select “Properties” from the context menu. • Select the “Version” tab. <p>(If the Description does not specify “US/Canada,” then this is not the 128-bit version.)</p> <p>Note: Run SPI-2000 after installing HF/ SP. This will help you to detect changes within your system.</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

your system susceptible to a variety of vulnerabilities and attacks.	
--	--

Remove POSIX & OS/2 Support	
Vulnerability	Countermeasures
<p>Ensure that support for POSIX and OS/2 is removed from the 2000 Server. Vulnerabilities exist that could be exploited if not removed. OS/2 and POSIX subsystems are actually mapped to calls in the Win32 subsystem where the actual functionality is implemented. This can allow programs written for these subsystems to run at root.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> 1. OS/2 Subsystem File Components <ul style="list-style-type: none"> • Select the “Search” button from the Tools bar. • Enter the following name in the “Search for files and folders named” field: OS2 • Click on the “Search Now” button. • If the search indicates that the files “OS2SS.EXE,” “OS2.EXE” or “OS2SRV.EXE” exist, or the directory “OS2” exists, then the option is considered to be on. • Remove the above listed items. • OS2 files should also be removed from the \dllcache directory, otherwise Windows 2000 will restore them. In rare instances some mail servers require the OS/2 modules to function properly. If these exceptions are not documented, you should remove all of the above files. <input type="checkbox"/> 2. POSIX Subsystem File Components <ul style="list-style-type: none"> • Select the “Search” button from the Tools bar. • Enter the following name in the “Search for files and folders named” field: POSIX PSX. • Click on the “Search Now” button. <ul style="list-style-type: none"> • If the search indicates that the files “POSIX.EXE,” “PSXSS.EXE” or “PSXDLL.DLL” are present then the option is considered to be on. • Remove the above listed items.



File System Formats Recommendations

- Use NTFS 5.0 partitions.
- Avoid the use of FAT16 FAT32
- Use Convert Utility to convert FAT partitions to NTFS
 - Sets ACLs of the converted partition to Everyone: Full Control
 - Use the Security Configuration templates that contain the default settings for NTFS permissions, registry permissions, and default user rights to reset the ACLs to more secure values

3-1

<i>File System Formats</i>	
Vulnerability	Countermeasures
<p>IAW MSG DTG 042100Z Mar 99 Fm ACERT Ft Belvoir VA. I. Ensure that the type of file system you are using is the NTFS file system versus the FAT file system.. Although supported by W2K, FAT16 (FAT) and FAT32 do not provide file/folder security support, encryption and disk quotas.</p>	<p><input type="checkbox"/> 1. Make sure that all partitions on your server are formatted using NTFS. If necessary, use the <i>convert</i> utility to non-destructively convert your FAT partitions to NTFS.</p> <p>Warning If you use the convert utility, it will set the ACLs for the converted drive to Everyone: Full Control.</p>



File System Formats Recommendations (cont)

- Use Dynamic Disks
 - Not recognized by other OS
 - Defeats the NTFS DOS threat.
 - Disk configuration data is stored in last 1 MB of space of HD
 - Changes are not recorded in partition table

3-1

DOS file systems	
Vulnerability	Countermeasures
DOS Volumes only allow share file/directory security. DOS partition could provide a door way to the rest of the system. A user who has physical access to the machine could boot into DOS and use ntfsdos.exe to gain access to critical areas of the OS.	<ul style="list-style-type: none"> <input type="checkbox"/> 1. Avoid if possible, minimize at a minimum, the use of FAT16 and FAT32 file systems. <input type="checkbox"/> 2. Use Dynamic Disks <ul style="list-style-type: none"> Partitions associated with dynamic disks are not currently recognized by any other OS (defeats NTFS-DOS threat) <input type="checkbox"/> 3. Verify no DOS bootable partitions exist. <input type="checkbox"/> 4. Utilize Computer Management/Disk Management to verify file system partitions.

Verify that all disk partitions are formatted with NTFS	
Vulnerability	Countermeasures
NTFS 5.0 partitions offer access controls and protections such as file/folder security support, on the fly encryption (EFS) and disk quotas that aren't available with the FAT16, FAT32, or FAT32x file systems. These file systems are open and vulnerable.	<ul style="list-style-type: none"> • Make sure that all partitions on your server are formatted using NTFS. If necessary, use the <i>convert</i> utility to non-destructively convert your FAT partitions to NTFS. <p>Warning If you use the convert utility, it will set the ACLs for the converted drive to Everyone: Full Control. Use the Security Configuration templates that contain the default settings for NTFS permissions, registry permissions, and default user rights to reset the ACLs to more secure values</p>



Encrypting File System (EFS)

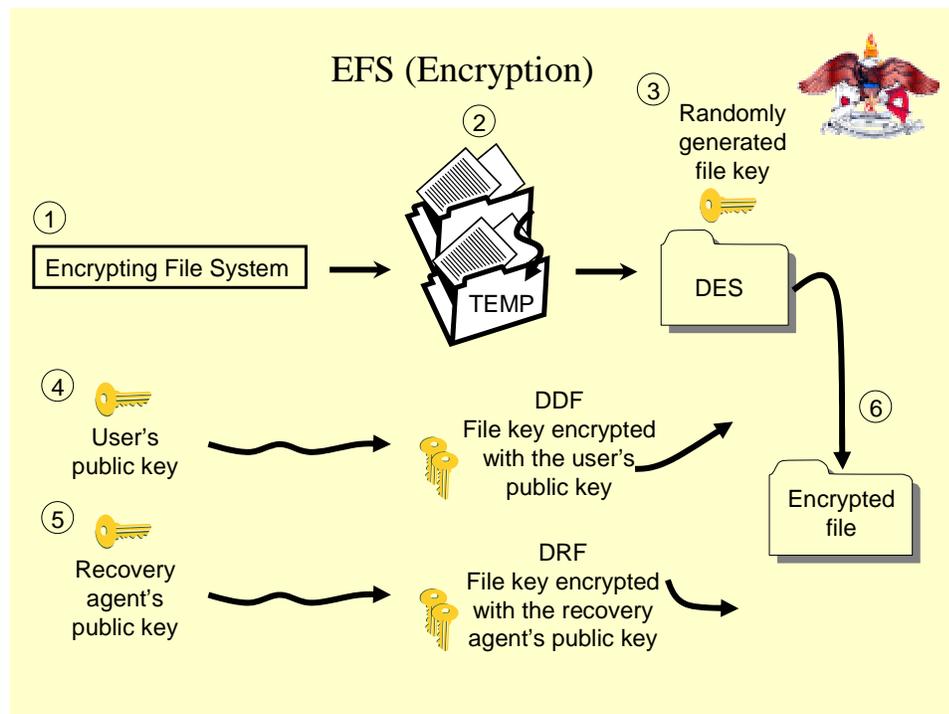
- NTFS is required.
- Transparent to users.
- Introduces “Wipe” function.
- Compression cannot be used in conjunction with (EFS)
- System Files not affected.
- Pagefile not affected by EFS

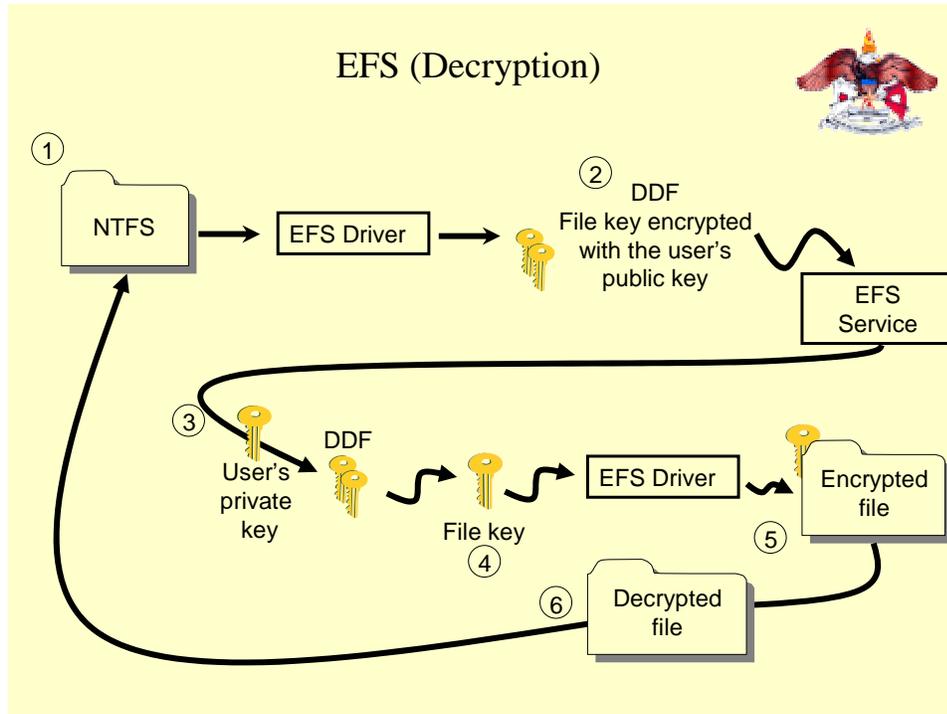
3-1

Encrypting File System (EFS)	
Vulnerability	Countermeasures
<p>Once an attacker has physical access to the system the data on the system is vulnerable. Another possibility is the use of another OS (such as Linux) to bypass the OS and mount the NTFS volume.</p> <p>Note: Encrypt folder vice files. The encryption of files very quickly becomes manually intensive.</p>	<p>The Encrypting File System (EFS) is a feature introduced in Windows 2000 that provides automatic encryption and decryption of data on NTFS disk drives. The important characteristics of EFS are:</p> <ul style="list-style-type: none"> • It’s transparent to applications. Encryption and decryption occurs automatically as part of normal file write and read operations, respectively. • It applies to folders as well as files. If the "encrypt" attribute is selected for a folder, all files within it, and all files subsequently added to it, are encrypted. <p>It’s easy to use. Users can select files or folders to be encrypted via a checkbox on the Properties page of the item. The new tool introduces a "Wipe" function that overwrites all of the deallocated data on an NTFS drive permanently. This improves security by ensuring that even an attacker who gained complete physical control of a Windows 2000 machine would be unable to recover previously deleted data.</p> <p>Countermeasure A</p> <p><input type="checkbox"/> Use EFS to encrypt file systems</p> <ul style="list-style-type: none"> • Right-click desired file/folder; select properties • Within general sheet, click advanced button • Within advanced attributes sheet, select encrypt

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p style="text-align: center;">contents to secure data checkbox</p> <p>Note: Gotchas of EFS</p> <ul style="list-style-type: none">• NTFS is required. If data is moved from an NTFS to non-NTFS data is decrypted.• Can share encrypted files but accessing or copying them over the network will decrypt the files.• Compression is mutually exclusive from encryption• Only user who encrypts or recovery agent can decrypt• System files can not be encrypted• Encrypted files can still be deleted.• Pagefile is not affected by EFS
--	--





Security Templates

- Used with the MMC as a snap in.
- Text files
- Regulate and monitor access
- Security Configuration and Analysis tool
- Fully customizable can create your own based on any specific circumstances or mission.

3-1

Security Templates	
Vulnerability	Countermeasures
Security Templates essentially are text files. Anyone gaining access to root could create his or her own templates that would	<input type="checkbox"/> 1. Implement Security Templates <ul style="list-style-type: none"> • From MMC console, select the Security Templates snap-in • Double-click the Security Templates icon to open it.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>affect system security on a forest wide basis depending on the affected servers' placement. The use of secedit.exe tool should be restricted to only administrators.</p>	<ul style="list-style-type: none"> • Double-click the folder icon to open it and see the included templates • Double-click the <i>appropriate policy template</i> to open it. • Make <i>appropriate policy selections</i> • In the left pane of the MMC window, right-click on the <i>appropriate policy template</i> icon. Select Save as. Save the policy with an <i>appropriate name</i>. • Open the Event Log Settings for <i>appropriate name</i> to make sure you changes were saved. • Close the Security Templates namespace. • Right-Click the Security configuration and Analysis icon and select Open Database • Enter a filename of <i>appropriate name</i> and click Open • When prompted for a template to import, select the appropriate name and click Open • Right-click the Security configuration and Analysis icon and select configure Computer Now. <p>When adding additional templates to an open security database, the effect is cumulative.</p> <p>Basicws, Basicsrv, basicdc Resets or reverses the application of other security policies Ensures continued compatibility with currently installed applications Doesn't modify User Rights policy settings</p> <p>Securews, securesrv, securedc Recommended settings for all security areas Except files, folders and Registry Key which are configured by the compatible template</p> <p>Highsecurityws, highsecuritysrv, highsecuredc Settings for network communications No network communication capabilities with downlevel systems</p> <p>Compatiblews Provides compatibility with existing NT4.0-based applications Regular users are placed in the Power Users group in W2KPro Removes users from Power Users while maintaining legacy application compatibility ???</p>
---	--



NTFS Streams

Unnamed Streams, Named Streams, Multiple Streams

- History
- Misunderstood
- NT 4.0 Workstation, NT 4.0 Server, and all W2K platforms
- Uses
 - Authentication mechanism to show ownership of files.
 - To send malicious code undetected throughout a network.

3-1

NTFS Streams	
Vulnerability	Countermeasures
<p>Due to the manner in which the command line is parsed streams are not displayed in file management utilities. Some of the security considerations with respect to streams are</p> <ul style="list-style-type: none"> • data will be added to user's quota • most virus scanners do not attempt to discover and scan streams • fragmentation could hinder performance • used as a covert channel • survive copy operations between computers 	<p>□ 1. Scan the harddrive looking for suspicious streams LADS</p> <p>Note: Several freeware and shareware utilities are available (unfortunately most have poor performance), see http://europe.iss.net/streams and www.lancanyon.com</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

supporting NTFS and backup operations	
--	--

<p style="text-align: center;">What is being hidden </p> <ul style="list-style-type: none">• Data<ul style="list-style-type: none">– Text (samdump)– Output of command• Executables<ul style="list-style-type: none">– Programs– Games– Rootkits <p style="text-align: right; font-size: small;">3-1</p>	<p style="text-align: center;">NTFS Streams (cont) </p> <ul style="list-style-type: none">• Available formats<ul style="list-style-type: none">– Compressed– Encrypted• Undetectable by on board GUI based viewing tools• Solutions<ul style="list-style-type: none">– Anti-Virus products (i.e. Norton Anti-Virus) <p style="text-align: right; font-size: small;">3-1</p>
---	---

NTFS ADS Practical Exercise

W2K System Security

Practical Exercise SAS 2C: The Dangers of NTFS ADS.

REQUIREMENTS:

1. Windows NT/2000/XP with NTFS partition
2. streams.exe from SysInternals (<http://www.sysinternals.com/ntw2k/source/misc.shtml>)
or
lads.exe from Frank Hayne Software (http://www.heysoft.de/Frames/f_sw_la_en.htm)

If you have Windows NT 3.1, 4.0, 2000, and XP and use NTFS, test your system

NTFS Alternate Data Streams (ADS)

- Developed by Microsoft for compatibility with Apples' Macintosh Hierarchical File System (HFS).
- Why would Microsoft do that? They developed a version of Microsoft Office for Macintosh and needed the ability to share information between HFS and NTFS.
- Malicious users take advantage of this by storing a virus or Trojan on your system. Users can abuse this by hiding graphics or data behind text files, etc.
- How to create an Alternate Data Stream: The syntax used to create the Stream is straightforward. An ADS associated with the file normal.txt, simply separate the default stream name from the ADS name with a colon. (normal.txt:hidden)

Key issues about NTFS Data Streams

Streams are only visible to specialized software.

Public awareness of streams is very low.

Streams can attach themselves to directories as well as files.

Disk space used by Streams are not reported by programs such as Windows Explorer or commands such as 'DIR'

Streams can be executed.

Executed streams do not have their filenames displayed correctly in Windows Task Manager.

Examples

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

1. Open Command Prompt and type in the following commands:

```
cd \streams
echo This is a normal text file > normal.txt
type normal.txt
dir normal.txt
```

From the output, you should notice the text "This is a normal text file" appear from the type command. You should also have a directory listing for the file normal.txt.

What is the size of the file? _____

2. At Command Prompt and type in the following command:

```
notepad normal.txt:hidden.txt
```

Click **Yes** to create file, and type the following text

This is a hidden text file

Click **File > Save**, then **File > Exit**.

3. Back at the Command Prompt and type in the following command:

```
Dir
```

Was there a file hidden.txt? **YES / NO**

What is the file size of normal.txt? _____

Did the file size change from step 1? **YES / NO**
(will not detect the presence of these newly created ADS)

4. At Command Prompt and type in the following command:

```
more < normal.txt:hidden.txt
```

Did you see the text "This is a hidden text file"? **YES / NO**

5. We will need the program streams.exe from SysInternals. Check to make sure streams.exe is located in your streams directory. (should be e:\streams)

6. At Command Prompt and type in the following command:

```
type \winnt\notepad.exe > normal.txt:np.exe
type \winnt\system32\sol.exe > normal.txt:s.exe
```

7. At Command Prompt and type in the following command:

```
notepad normal.txt:test.vbs
```

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Click **Yes** to create file, and **type** the following text (*remember to click your enter key after typing your script.*)

MsgBox "Hello World!!! This could be a malicious script"

Click **File > Save**, then **File > Exit**.

8. At Command Prompt and type in the following command:

```
streams normal.txt
dir normal.txt
```

What ADS files are attached to the file normal.txt?

Was there a change in the file size of normal.txt? **YES / NO**

In the next couple of steps we are going to execute a couple of ADS programs in normal.txt

9. At Command Prompt and type in the following command:

```
start .\normal.txt:s.exe
```

Are we able to execute the solitaire program? **YES / NO**

10. At Command Prompt and type in the following command:

```
start .\normal.txt:test.vbs
```

Did you get a message box with "Hello World!!! This could be a malicious script"? **YES / NO**

Currently there are no antivirus products capable of detecting NTFS ADS.

Are NTFS ADS a security risk? **YES / NO**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Why?

What sort risk rating would you give NTFS ADS? **HIGH / MEDIUM / LOW**

Why?

Should we replace NTFS with FAT/FAT32 to avoid NTFS ADS? **YES / NO**

Why?

Should we be scanning our system(s) for NTFS ADS usage? **YES / NO**

If so, how often? _____

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<div style="text-align: right; margin-bottom: 10px;"></div> <h3 style="text-align: center;">Managing Security with Group Policy</h3> <ul style="list-style-type: none"> Configuration settings use to control behaviors of objects. Apply policies to large numbers of computers in a uniform way. Group Policy settings applied to computers at boot time and to users when they log on. <p style="text-align: right; font-size: small;">3-1</p>	<div style="text-align: right; margin-bottom: 10px;"></div> <h3 style="text-align: center;">Group Policy (cont)</h3> <ul style="list-style-type: none"> Types of Configurable options <ul style="list-style-type: none"> – Security options – Manage applications – Manage desktop appearance – Assign scripts – Redirect folders from local computers to network locations. <p style="text-align: right; font-size: small;">3-1</p>
---	--

Display Last User's Name	
Vulnerability	Countermeasures
<p>Current access procedures into systems using user ID and password are vulnerable when one or both pieces to the puzzle are known.</p>	<p><input type="checkbox"/> 1. Use regedit32 to create or assign the following registry key</p> <pre style="font-family: monospace; font-size: small;"> Registry Hive: HKEY_LOCAL_MACHINE SubKey: \SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\System Value Name: DontDisplayLastUserName Data Type: REG_SZ Value Data: "1" Registry Hive: HKEY_LOCAL_MACHINE SubKey: \SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon Value Name: DontDisplayLastUserName Data Type: REG_SZ Value Data: "1" </pre> <ul style="list-style-type: none"> Default value for both registry entries is 0 The SubKey: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System takes precedence. The value data on these edits must be set to 1.

Display Legal Notice	
Vulnerability	Countermeasures
<p>This check verifies that Windows 2000 is configured to display a legal notice prior to logging on.</p> <p>*see AR 380-53 and AR 380-5 for guidance.</p>	<p><input type="checkbox"/> 1. Use regedit32 to create or assign the following registry key</p> <pre style="font-family: monospace; font-size: small;"> Registry Hive: HKEY_LOCAL_MACHINE SubKey: \SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon Value Name: LegalNoticeCaption Data Type: REG_SZ Value Data: "US DEPARTMENT OF DEFENSE WARNING STATEMENT" </pre>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

```
Registry Hive: HKEY_LOCAL_MACHINE
SubKey: \SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Policies\System
Value Name: LegalNoticeCaption
Data Type: REG_SZ
Value Data: "US DEPARTMENT OF DEFENSE WARNING STATEMENT"
```

```
Registry Hive: HKEY_LOCAL_MACHINE
SubKey: \SOFTWARE\Microsoft\System
Value Name: LegalNoticeCaption
Data Type: REG_SZ
Value Data: "US DEPARTMENT OF DEFENSE WARNING"
```

- At a minimum, at least one of these values must exist.
- In the Registry Editor, navigate to each of the following registry values:

```
Registry Hive: HKEY_LOCAL_MACHINE
SubKey: \SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
Value Name: LegalNoticeText
Data Type: REG_SZ
Value Data: "THIS IS A DEPARTMENT OF DEFENSE ..."
```

```
Registry Hive: HKEY_LOCAL_MACHINE
SubKey: \SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
Value Name: LegalNoticeText
Data Type: REG_SZ
Value Data: "THIS IS A DEPARTMENT OF DEFENSE ..."
```

```
Registry Hive: HKEY_LOCAL_MACHINE
SubKey: \SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Policies\System
Value Name: LegalNoticeText
Data Type: REG_SZ
Value Data: "THIS IS A DEPARTMENT OF DEFENSE ..."
```

```
Registry Hive: HKEY_LOCAL_MACHINE
SubKey: \SOFTWARE\Policies\Microsoft\System
Value Name: LegalNoticeText
Data Type: REG_SZ
Value Data: "THIS IS A DEPARTMENT OF DEFENSE ..."
```

- At least one of the registry values must exist.
- A meaningful message equivalent to the below DOD Banner should be inputted in the value data field.

This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U. S. Government use. DOD computer systems may be monitored for all lawful purposes to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring of this system.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

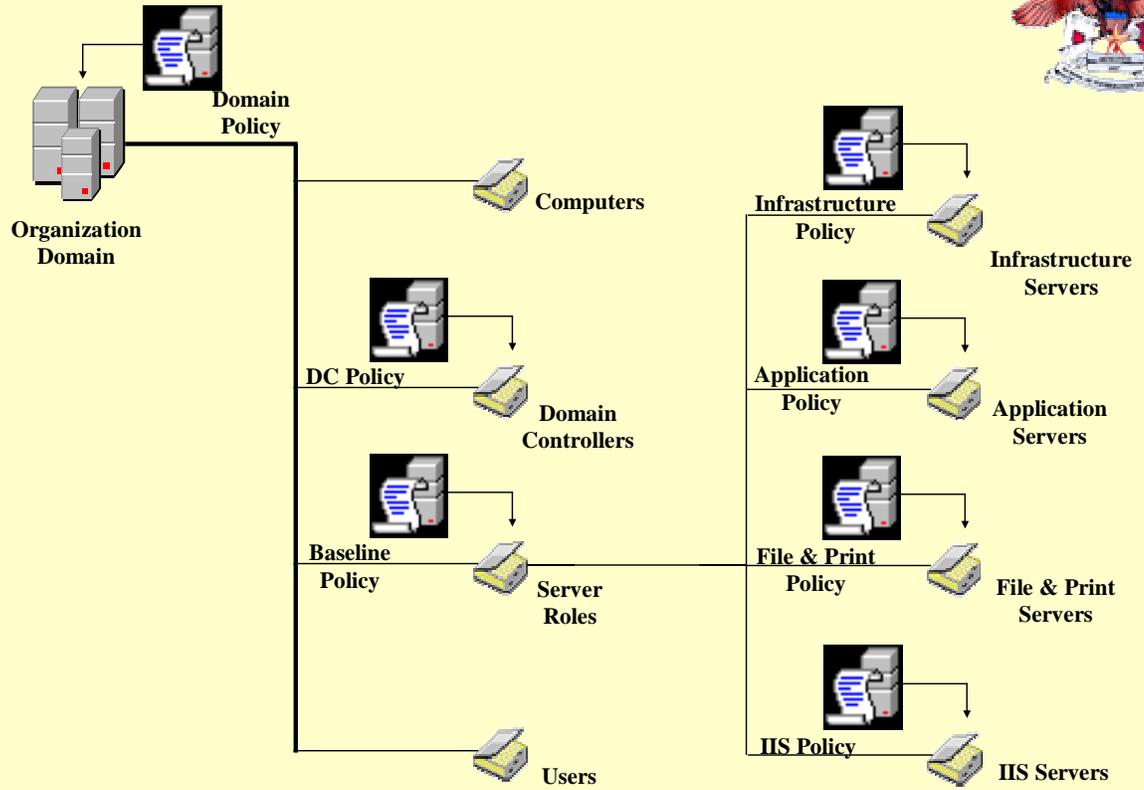
	Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or adverse action. Use of this system constitutes consent to monitoring for these purposes.
--	--

<i>Logon Prompt</i>	
Vulnerability	Countermeasures
CONSIDER customizing the Logon Prompt.	<input type="checkbox"/> 1. Use regedt32 to create or assign the following registry key value: Registry Hive: HKEY_LOCAL_MACHINE SubKey: \SOFTWARE\ Microsoft\WindowsNT\CurrentVersion\Winlogon Value Name: LogonPrompt Data Type: REG_SZ Value Data: <variable text> Note: On a default system this key needs to be added.

<i>Welcome Message</i>	
Vulnerability	Countermeasures
CONSIDER customizing the Welcome Message.	<input type="checkbox"/> 1. Use regedt32 to create or assign the following registry key value: RegistryKey:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \WindowsNT\CurrentVersion\Winlogon Value Name: Welcome Data Type: REG_SZ Value Data: <variable text> Note: On a default system this key needs to be added.

<i>Quotas</i>	
Vulnerability	Countermeasures
Quotas can be utilized to limit the damage of a malicious user by denying the success of denial of service attacks.	<input type="checkbox"/> 1. To enable disk quota on a particular drive: <ul style="list-style-type: none"> • Right-click the drive and selected Properties-> Quotas • Select Enable Quota management • Also select Deny Disk Space to Users Exceeding Quota Limits

Global Policy Implementation Infrastructure



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS 2D

Exercise C

This practical exercise presents an overview of Group Policy and shows how to use the Group Policy snap-in to specify policy settings for groups of users and computers. Boot the system into Windows 2000 Professional and obtain from the instructor the appropriate user account and Organizational Unit (OU) with which to complete this exercise. Domain Controllers stay Administrator, in W2K Server.

Scoping a Group Policy for a Domain or OU

- 1. Log on to the Domain using the LabuserXXa user account (password = LUXXa-pass).
- 2. Click Start, point to Programs, click Administrative Tools, and click Active Directory Users and Computers to open the Active Directory Users and Computers snap-in.
- 3. Click the + next to the Domain icon to expand the tree (this may take a few seconds).
- 4. Right-click the OU associated with your machine, and click properties.
- 5. Click the Group Policy tab.

Creating a Group Policy Object (GPO)

- 6. Starting at step five, click New and in the available text box type "OUXX Screen Saver Policy". Once you've entered the policy name press <enter>.

Editing a Group Policy Object (GPO)

- 7. To edit the Screen Saver Policy GPO, highlight the GPO and click the Edit button, or just double-click the GPO.
- 8. Click the + next to Computer Configuration to expand the tree (if it is not already expanded).
- 9. Click the + next to the Windows Settings.
- 10. Click the + next to the Security Settings extension.
- 11. Click the + next to the Local Policies.
- 12. Click the Security Options.
- 13. Double-click the Message text for users attempting to log on policy.
- 14. Check the Define this policy setting; and in the available box, enter Welcome to the School of Information Technology's Systems Administration/Network Managers Security Course.
- 15. Click OK to close the Security Policy Setting window.
- 16. Double-click the Message title for users attempting to log on policy.
- 17. Check the Define this policy setting; and in the available box, enter Information Assurance.
- 18. Click OK to close the Security Policy Setting window.
- 19. Click the + next to User Configuration to expand the tree (if it is not already expanded).
- 20. Click the + next to Administrative Templates to expand the tree.
- 21. Click the + next to Control Panel to expand the tree.
- 22. Click the Display folder.
- 23. Double-click Hide Screen Saver tab to open.
- 24. Click the Enabled radio button.
- 25. Click OK.
- 26. Double-click Activate screen saver.
- 27. Click the Enabled radio button.
- 28. Click OK.

- 29. Double-click Screen saver executable name.
- 30. Click the Enabled radio button and in the "Screen saver executable name" entry space, enter "Logon.scr".
- 31. Click OK.
- 32. Double-click Password protect the screen saver.
- 33. Click the Enabled radio button.
- 34. Click OK.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- 35. Double-click Screen Saver time out.
 - 36. Click the Enabled radio button and in the “Number of seconds to wait to enable the Screen Saver” space, enter “30”.
 - 37. Click OK.
 - 38. Close the Group Policy window.
 - 39. Close the OU properties window.
 - 40. Close the Active Directory Users and Computers snap-in.
 - 41. Reboot the system into Windows 2000 Professional. (A second reboot may be necessary to apply the Screen Saver policy).
 - 42. Log on to the Domain using the LabuserXX user account (password = LXXX-pass).
 - 43. Did the screen saver display after 30 seconds?
-

- 44. Did you have to re-authenticate to gain access to the desktop?
-

- 45. What screen saver was activated?
-

- 46. Once you re-authenticate, right-click the desktop and click properties. What tabs are displayed?
-

Managing Group Policy

- 47. Logoff and logon to the Domain using the LabuserXXa user account (password = LXXXa-pass).
 - 48. Click Start, point to Programs, click Administrative Tools, and click Active Directory Users and Computers to open the Active Directory Users and Computers snap-in.
 - 49. Click the + next to the Domain icon to expand the tree.
 - 50. Right-click the OU associated with your machine, and click properties.
 - 51. Click the Group Policy tab (this page displays any GPOs associated with the currently selected OU).
 - 52. To associate (link) a new GPO, click the Add button.
 - 53. Select the All tab from the “Add a Group Policy Object Link” window.
 - 54. Double-click the Logon Policy GPO.
 - 55. Give the Logon Policy GPO the highest precedence by moving it up in the list of GPOs (highlight the Logon Policy GPO and click the Up button).
 - 56. Disable the computer configuration settings of the Screen Saver Policy GPO (highlight the OUXX Screen Saver Policy GPO, click the Properties button, check the Disable Computer Configuration settings check box, and answer Yes to the Confirm Disable window).
 - 57. Click OK to close the Screen Saver Policy properties window.
 - 58. Click OK to close the OU properties window.
 - 59. Close the Active Directory Users and Computers snap-in.
 - 60. Reboot the system into Windows 2000 Professional.
 - 61. What appears in the User Name entry of the Graphical Identification and Authentication screen?
-

- 62. How did the order of the GPOs effect the application of policies?
-
-

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- ❑ 63. Logon to the domain with the LabuserXX user account (password = LUXX-pass). Are the policies from the SECXX Screen Saver Policy still in effect?



- ❑ 64. What are the results from loading multiple group policies?

Security Group Filtering

In this part of the exercise, you will modify which security group's are affected by a GPO.

- ❑ 65. Logoff and logon to the Domain using the LabuserXXa user account (password = LUXXa-pass).
- ❑ 66. Does the screen saver display after 30 seconds?

-
- ❑ 67. Click Start, point to Programs, click Administrative Tools, and click Active Directory Users and Computers to open the Active Directory Users and Computers snap-in.
 - ❑ 68. Click the + next to the Domain icon to expand the tree.
 - ❑ 69. Right-click the OU associated with your machine, and click properties.
 - ❑ 70. Click the Group Policy tab.
 - ❑ 71. Right-click the OUXX Screen Saver Policy GPO and select Properties.
 - ❑ 72. Click the Security tab.
 - ❑ 73. From the "OUXX Screen Saver Policy Properties" window, highlight the LabuserXXa user account.
 - ❑ 74. Check the Deny "Apply Group Policy" Permissions.
 - ❑ 75. Click OK and click Yes to affirm the Security window.
 - ❑ 76. Click OK to close the OU properties window.
 - ❑ 77. Close the Active Directory Users and Computers snap-in.
 - ❑ 78. Reboot the system into Windows 2000 Professional.
 - ❑ 79. Log on to the Domain using the LabuserXXa user account (password = LUXXa-pass).
 - ❑ 80. Does the screen saver display after 30 seconds?

No Override

- ❑ 81. Click Start, point to Programs, click Administrative Tools, and click Active Directory Users and Computers to open the Active Directory Users and Computers snap-in.
- ❑ 82. Click the + next to the Domain icon to expand the tree.
- ❑ 83. Right-click the OU associated with your machine, and click properties.
- ❑ 84. Click the Group Policy tab.
- ❑ 85. Enable the computer configuration settings of the Screen Saver Policy GPO (highlight the OUXX Screen Saver Policy GPO, click the Properties button, uncheck the Disable Computer Configuration settings check box, and click OK to close the OUXX Screen Saver Policy Properties window.
- ❑ 86. Set No Override on the OUXX Screen Saver Policy GPO (highlight the OUXX Screen Saver Policy GPO, click the Options button, select the "No Override: prevents other Group Policy Objects from overriding policy set in this one" check box, and click OK.
- ❑ 87. Click OK to close the OU properties window.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- ❑ 88. Close the Active Directory Users and Computers window.
- ❑ 89. Reboot the system into Windows 2000 Professional.
- ❑ 90. What does the Message text for users attempting to log on policy display?

- ❑ 91. What does the Message title for users attempting to log on policy display?

- ❑ 92. How does implementing the no override setting on the OUXS Screen Saver Policy effect the application of policies?

- ❑ Wait for instructor review



Access Control

- Control access to a specific object attribute.
- Security descriptors include an access control list (ACL)
- ACLs defines which users have permission to perform particular actions with objects
- After account authentication, either the users rights or object permissions determine the type of access granted
- Administrators can assign security descriptors to objects

3-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS-2F

EXERCISE E

This practical exercise will provide hands-on experimentation with file permissions including inheritance. Please retain from the instructor the appropriate drive letter or partition to use in place of *W2K Server*.

1. Log on locally to the W2KServer, using the administrator account (pwd = student).
2. Select Start->Programs->Accessories->Windows Explorer
3. Open the root of the W2K Server (MyComputer\W2KServer).
4. Create a new folder name stage1. On the right-hand side panel, right-click and select New->Folder or use the File Menu dropdown.
5. Right-click the folder, stage1.
6. Select Properties. On the Properties Window select the Security tab.
7. On the Properties window, clear the Allow inheritable permissions from parent to propagate to this object checkbox.
8. On the Security window, select Remove to discard all inherited ACEs.
9. On the Properties window, select the Add button (near the top of the right side of the Window).
10. If the Network Password Window appears, select cancel. On the Users, computers or Groups Window, at the Look in drop-down box, select the current workstation name.
11. Select the Administrators group and click ADD. Select the Everyone group and click ADD. Click OK to close the Permissions Window.
12. On the properties windows, configure two ACEs: Administrators: Full Control, Everyone: Read & Execute, List folder Contents and Read.
13. Click OK to save the new ACL.
14. Open the stage1 folder (double-click folder to open)
15. Create a subfolder inside folder stage1, named stage2. On the right-hand side panel, right-click and select New->Folder or use the File Menu dropdown.
16. Right click on the stage2 folder. Select Properties. Select the Security Tab. Verify the default ACL on the stage2 folder. How is the ACL defined?

17. On the properties window, unselect "allow inheritable permissions from parent to propagate to this object". Click on copy when the security box appears. Click OK in the stage2 properties box
18. Open the stage2 folder (double-click folder to open).
19. Create a new text file named file1.txt. On the right-hand side panel, right-click and select New->Text Document or use the File Menu dropdown.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

20. Right-click file1.txt. Select Properties. On the Properties Window, select the Security tab and verify the permissions.

How is the ACL defined?

21. Close the Permissions window for file1.txt by pressing the OK button.

22. Click on the back button, right click stage2, select Properties, and select the Security Tab to open the Permissions window for stage2.

23. Click Add, if the Network Password Window appears, select cancel. At the Look in drop-down box, select the current workstation name.

24. Select labuserXa, click Add, click OK, click box for Deny Write. This will add an ACE to explicitly deny write access to user labuserXa.

25. Click OK.

26. Select YES to the Security Caution window.

27. Open stage2 (double-click) and right-click on file1.txt, select Properties, select the Security Tab and verify the permissions.

How is the ACL defined?

28. Close the Properties Box, by selecting the OK button.

29. Click on the back-button, right-click stage2, select Properties, select the Security Tab to open the Permissions window for stage2.

30. Click Add, if the Network Password Window appears, select cancel. At the drop-down box, select the current workstation name.

31. Add an ACE to explicitly granting write access to authenticated users. Select authenticated users group, click Add, click OK, and click Allow Write.

32. Click OK.

33. Log off of the administrator account.

34. Log in as the labuserXa account (password = LUXa-pass).

35. Select Start->Programs->Accessories->Windows Explorer

36. Drill down to the stage2 folder (double-click MyComputer\W2Kserver\stage1\stage2).

37. Attempt to create a new text file named file2.txt. Right-click and select New->Folder or use the File Menu dropdown. Was the new file successfully created?

38. Open the file1.txt file. Attempt to make changes to the file and save it. Was the file modification successful?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

39. Close all windows.

40. Log out.

41. Wait for instructor review.



Protect Files and Directories

- Clean-installed Windows 2000 systems have secure default ACLs on the file system.
- Upgrades from previous versions (e.g., Windows NT 4) do not modify the previous security settings.
- The default Windows 2000 settings should be re-applied.

3-1

File, Directory, and Registry Permissions															
Vulnerability	Countermeasures														
<p>Clean-installed Windows 2000 systems have secure default ACLs on the file system. However, upgrades from previous versions (e.g., Windows NT 4) do not modify the previous security settings and should have the default Windows 2000 settings applied.</p>	<ul style="list-style-type: none"> • Users are the opposite of administrators. Provided that the Windows 2000 operating system is clean-installed onto an NTFS partition, the default security settings are designed to prohibit Users from compromising the integrity of the operating system and installed applications. Users cannot modify computer-wide registry settings, operating system files, or program files. Users cannot install applications that can be run by other members of the Users group (preventing Trojan horses). Users cannot access other users' private data. • Below are the minimum recommended settings for users providing that you upgraded from a 4.0 system. <p>Users Write Access Locations</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;"><u>Object</u></th> <th style="text-align: left;"><u>Permission</u></th> <th style="text-align: left;"><u>Comment</u></th> </tr> </thead> <tbody> <tr> <td>HKEY_Current_User</td> <td>Full Control</td> <td>User's portion of the registry</td> </tr> <tr> <td>%UserProfile%</td> <td>Full Control</td> <td>User's Profile directory</td> </tr> <tr> <td>All Users\Documents</td> <td>Read, Create File</td> <td>Shared Documents Location.</td> </tr> </tbody> </table>			<u>Object</u>	<u>Permission</u>	<u>Comment</u>	HKEY_Current_User	Full Control	User's portion of the registry	%UserProfile%	Full Control	User's Profile directory	All Users\Documents	Read, Create File	Shared Documents Location.
<u>Object</u>	<u>Permission</u>	<u>Comment</u>													
HKEY_Current_User	Full Control	User's portion of the registry													
%UserProfile%	Full Control	User's Profile directory													
All Users\Documents	Read, Create File	Shared Documents Location.													

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

			Allows Users to create files that can subsequently be read (but not modified) by other Users.
	% Windir%\Temp	Synchronize, Traverse, Add File, Add Subdir	Per-Machine temp directory. This is a concession made for service-based applications so that Profiles do not need to be loaded in order to get the per-User temp directory of an impersonated user.
	\ (Root Directory)	Not Configured during setup	Not configured during setup because the Windows 2000 ACL Inheritance model would impact all child objects including those outside the scope of setup

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

 System Administrator/Network Manager Security Course W2K Checklist Network Security <small>3-1</small>	 Services <ul style="list-style-type: none"> • Default services in Windows 2000 • Vulnerabilities with unneeded services • Turning off unneeded services <ul style="list-style-type: none"> - Using Snap-in - Using Command Line <small>3-1</small>
---	--

Services	
Vulnerability	Countermeasure
<p>By default, services are started under the LocalSystem account in Windows 2000. The LocalSystem account has unlimited access not only to the service, but also to the server itself. If compromised, an intruder can insert malicious code that will be executed during or upon completion of the service. The code can be anything from installing a Trojan on the server to altering/deleting system files.</p>	<p><u>COUNTERMEASURE A:</u></p> <p><input type="checkbox"/> 1. Utilize the Services Snap-in within the Microsoft Management Console (MMC) to start and stop services within W2K. This tool can be used both locally and remotely:</p> <ul style="list-style-type: none"> • Click the Start button and choose Run. • Type in MMC. • Once the MMC console box comes up left-click on Console from the tool bar. • Choose Add/Remove Snap-in. • Left-click Add, choose Services, left-click Add, Close, OK. • Expand the Services policy. • Choose the Services to stop. • Save the policy to the default directory and reboot the server. • From here you can double-click on the services that you wish to modify. <p><u>Note:</u> The Services snap-in is the preferred method to manage your services within W2K. It provides a central point of management. If the service is not needed, stop it.</p> <p><u>COUNTERMEASURE B:</u></p> <p><input type="checkbox"/> 1. Utilize the command line tool net.exe. It exposes basic start/stop/pause and query functionality.</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<ul style="list-style-type: none">• From the command line, type net.exe to view the available syntax• To stop a service, type net stop service. (service being the name of the service you wish to stop)• To start a service, type net start service. Without a parameter, this command will provide a list of started services.• To pause a service, type net pause service.
--	--

W2K System Security

Practical Exercise SAS 2B

EXERCISE B

Network Monitor

Network Monitor

Network Monitor is a Microsoft diagnostic tool that allows you to examine network traffic to and from the server at the packet level. It also allows capturing network traffic for later analysis, giving you a more technical method of performing a specific security check.

I. Getting Started:

We need to add the Network Monitor program if not in Administrative Tools:
(if there, skip to section II of this PE)

1. Begin by selecting **Start–Settings–Control Panel–Add/Remove Programs**
2. Select **Add/Remove Windows Components**
3. Scroll down to **Management and Monitoring Tools** and Double click
4. Select **Network Monitor Tools** – make sure the box is checked
5. Click **OK**
6. Click **Next**
7. Accept Remote installation mode - Click **Next**
8. A prompt will ask for the Win2K CD Click **OK**
9. Enter Copy files from: **C:\i386**
10. Click **OK**
11. Click **Next**
12. Click **Finish**
13. Click **Close**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

II. The Network Monitor is now installed on your system.

1. Execute the monitor by clicking on **Start --> Programs --> Administrative Tools --> Network Monitor**
2. Click **OK**
3. At the “**Select a network**” box, expand the “**Local Computer**”
4. Select the **bottom** Ethernet card and Select **OK**
5. Maximize your network monitor screen
6. In the tool bar at the top of the screen, click the funnel (filter) shaped one
This will allow us to edit the capture filter
7. An information box pops up. Read it and briefly explain what this means. Click **OK**
8. In the Capture Filter window select [**Address Pairs**] (**by double clicking**)
9. In the **Address Expression** set the filter to include **ANYGROUP <--> ANY**
*This allows us to include and exclude entries for detection from station to station.
It also allows us to control the directional flow of data we detect.*
10. Can we set the filter to only capture outgoing broadcast traffic from the local host? If so how could we do this?
11. Click **OK**
12. You can click **OK** to exit out of the Capture Filter window.

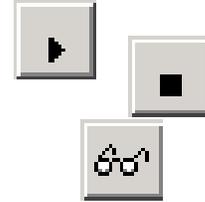


**We will now capture all traffic going to or coming from this machine to include general broadcasts*

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

III. Capturing Network Traffic

1. In the tool bar at the top of the Network Monitor screen, click on the ICON shaped like the play button on a VCR.
This will start the network capture
2. After allowing the Network Monitor to run for a minute or two stop it.
3. Click on the eyeglass ICON in the toolbar to view captured data.



IV. Analysis:

1. Which protocol was the most common?
2. What was the most common Source MAC Address?
3. What was the most common Destination MAC Address?
4. By clicking on **Display** ---> **Colors** set the most common protocol to be a different color than the rest, click **OK**. How can changing the color scheme on certain protocols be beneficial to the administrator?
5. Take a closer look at the Ethernet Frame. Double Click on one of the Frames in the list. If a password were sent across the network in clear text, would it be viewable by the Network Monitor?
Yes / No

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

V. Clear Text Vulnerability

Utilizing our partner PC we will examine clear text vulnerability and how to utilize IPSecurity to counteract this vulnerability. We will change the filter to only capture traffic between our partner PC's. We will then Ping, FTP, and Telnet to our partner PC.

**** Please stay in sync with your lab partner**

1. **Both Users**
2. From menu at the top of the screen - Select **Window** then the – **Ethernet ... Capture Window** – session
3. Click on the **Funnel** icon
4. Double Click **INCLUDE *ANY GROUP <--> *ANY**
5. Now we will add in our partner PC
6. Click **Edit Addresses**.
7. In the Address Database select **Add**.
8. Enter Partner PC name – **wsxxx** (xxx is the last octet of IP)
9. Change **Type** to **IP**
10. Enter your Partner PC IP address – **147.51.217.xxx** (xxx is the last octet of IP)
11. Select **OK**
12. Click **Close**
13. Set the filter to **WSXXX** (your machine name) <--> **sanmxxx** (your partner pc)
14. Select **OK**

Now we will only capture packets between our two machines

*The filter should look like **Your machine name(IP) <--> Your partner PC(IP)***

15. Select **OK** to close the Capture Filter window

****Once both you and your lab partner have completed this step**

PING session

1. **Both Users**
2. Click the **record** button to start the recording session 
3. **One of the users** - Open a command prompt – **start** – **run** – type **cmd**
4. Ping your partner PC – type **PING 147.51.217.xxx**
5. Once the Ping has finished – stop the capture 

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

6. View what has been captured
7. What did we capture?



FTP session - We will now FTP from one box to the other

1. **Both Users**
2. From menu at the top of the screen - Select **Window** then the – **Ethernet ... Capture Window** – session
3. Click the **record** button to start the recording session
4. **One of the users** - start – run
5. Enter **ftp 147.51.217.xxx** (partner PC)
6. Enter **administrator** as user and **student** as password
7. At the ftp> enter **bye**



8. **Both Users**

9. Stop the capture



10. View what has been captured



11. What did we capture? Can you locate the User name and password?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Telnet session - We will now Telnet from one box to the other

1. **One of the users** – Needs to start telnet
2. Select **Start–Run**–enter–**tlntadm.exe** – this will open the telnet administrator
3. Type an option number – enter **3** – Display / Change Registry Settings
4. Type an option number – enter **7** – NTLM – enter **y** we want to change this value
5. Enter **0** for **NTLM** value
6. Confirm change with **y**

We have just changed the NTLM setting so that Telnet will prompt you for a password. Telnet will now prompt you for a user Id and password. If this setting was not changed Telnet would authenticate using NTLM and the password would be encrypted. However, all other communication would not be encrypted.

7. Select **0** to exit this menu
8. Select **4** to start telnet [*Telnet is now up and running*]
9. **Both Users**
10. From menu at the top of the screen - Select **Window** then the – **Ethernet ... Capture Window** – session

11. Click the **record** button to start the recording session



12. **The user that did not setup Telnet** - Click – **start – run**

13. Enter **telnet 147.51.217.xxx** (partner PC)

14. Enter **administrator** as user and **student** as password

15. Type **dir**

16. Type **cd** (find a directory to change to)

17. Type **dir**

18. Type **Exit**

19. **Both Users**

20. Stop the capture



21. View what has been captured



22. What did we capture? Can you locate the User name and password? How about the commands that were issued? Telnet is different from FTP, look very closely.

23. What are some things we can we do to protect our selves from clear text vulnerability?



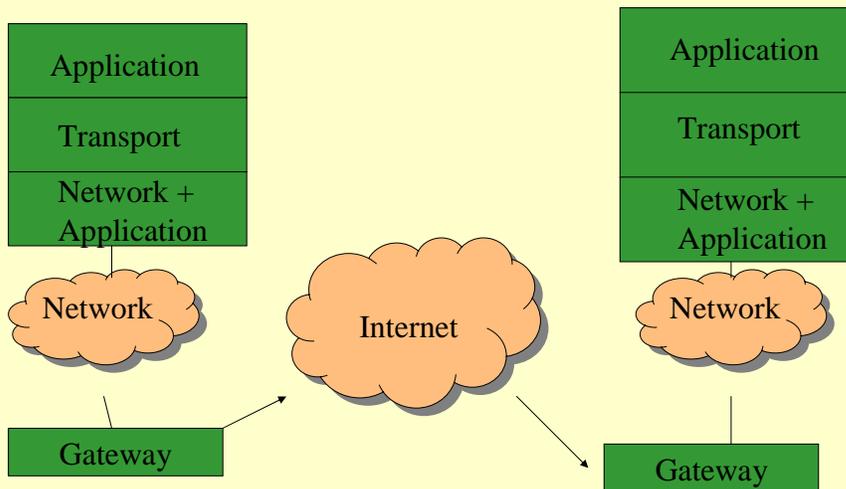
IP Security

- How IPSec works
 - Cryptographic based security for IPv4/6
 - Internet Layer Protocol
 - 2 security modes
 - Uses shared public key
 - Local Policy of GPO driven
- Provides
 - Authentication
 - Integrity Protection
 - Data Confidentiality

3-1



IPSec (End to End Security)



IP Security	
Vulnerability	Countermeasure
One of the biggest security issues on a network is network	Countermeasure A <ul style="list-style-type: none"> <input type="checkbox"/> 1. Select an IPSec policy <ul style="list-style-type: none"> • Open Network and Dial-up Connections

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

traffic passed along the wire as unencrypted, or clear-text, data. When your information is traveling as clear-text (as most SMTP, Telnet, HTTP, and FTP traffic does), an attacker who has gained access to your physical network can listen in and read any unencrypted traffic. By allowing unencrypted traffic on your network, you are vulnerable to many different attacks such as, network sniffing, Man-in-the-Middle, and spoofing just to name a few.

- Click **Local Area Connection**, and on the **File** menu, click **Properties**.
- In the **Local Area Connection Properties** dialog box, under **Components checked are used by this connection**, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
- Click **Advanced**, and then click the **Options** tab.
- Under **Optional settings**, click **IP security**, and then click **Properties**.
- Click **Use this IP security policy**, and then select the IPsec policy you want from the drop-down list.

IP Security Policies:

Client (Respond Only): Communicate normally (unsecured). Use the default response rule to negotiate with servers that request security. Only the requested protocol and port traffic with that server is secured.

Secure Server (Require Security): For all IP traffic, always require security using Kerberos trust. Do NOT allow unsecured communication with untrusted clients.

Server (Request Security): For all IP traffic, always request security using Kerberos trust. Allow unsecured communication with clients that do not respond to request.

Note:

You must be a member of the Administrators group to set Internet Protocol security (IPsec) policies. If the computer participates in a Windows 2000 domain, the computer may receive the IPsec policy from Active Directory, overriding the local IPsec policy. In this case, the options are disabled and you cannot change them from the local computer.

Countermeasure B

□ 1. An alternative method of selecting IPSEC Policy is through the MMC.

- Click the **Start** button and choose **Run**.
- Type in **MMC**.
- Once the MMC console box comes up left-click on **Console** from the tool bar.
- Choose **Add/Remove Snap-in**.
- From the Snap-in window choose **Add**.
- Choose **IP Security Policies on Active Directory**.
- Choose **Close**.
- Choose **OK**.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<ul style="list-style-type: none">• Expand the policy and choose which policy best meets your requirements.• Save the new settings under the default directory and reboot the server.
--	--

IP Security Tunneling Mode	
Vulnerability	Countermeasures
IPSec Tunneling modes specifies endpoints and uses computer certificates vice user certificates for validation. Any user with access to the endpoint computer has access to the tunnel.	<input type="checkbox"/> 1. When using IPSec in tunneling mode, use PPTP or L2TP over IPSec. Note: L2TP over IPSec is the W2K default.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

IPSEC

Practical Exercise SAS-2G

This practical exercise will provide hands-on training using Internet Protocol Security (IPSec) to encrypt network traffic. IPSec provides the ability to authenticate and encrypt network connections between two computers. You will need to synchronize your steps with your PARTNER on another machine. This practical exercise will be performed in Windows Server.

- I. a. activate an IPSec Policy on Work Station #1
 1. Log on locally to W2Kserver, using the **administrator** account
 2. Using ADMIN Tools, run the Local Security Policy MMC plug-in. If not available, create custom snap-in for Local Security Policy and save it.
 3. In the Local Security Policy setting box, **click** on IPSec Policies on Local Machine
Note the three entries in right pane: Client, Secure Server, and Server
 4. Right-click **Secure Server (require security)**, and then choose **Assign**. The status in the Policy Assigned Column should change from **No** to **Yes**.
- b. activate an IPSec Policy on Work Station #2
 5. To Active an IPSec Policy on **Work Station 2**, execute steps 1-3 above.
 6. Three entries should be in right pane: Client, Secure Server, and Server
 7. Right click **Client**, and then choose **Assign**.
 8. The status in the Policy Assigned column should change from No to Yes.

Both Computers:

9. **Note:** Now one computer (wk station #1) is acting as a **secure server**, and your partners computer (wk station #2) is acting as the **client**. The client will initially send unprotected ICMP Echo packets (ping) to the server, but the server will request security from the client, after the rest of the communication will be secure.

Why ? If the server was to initiate the ping, the ping would have to be secured to the client before the server would send unprotected pings or any other traffic because it would request IPSec protection before any application data was sent. If both computers had client policies, no data would be protected, because neither side requests security.
10. Execute the network monitor by clicking on **Start --> Programs --> Administrative Tools --> Network Monitor**
11. Execute IPSec monitor by clicking on **Start --> RUN --> ipsecmon -->**
The IP Security Monitor dialog box will open and confirm if your Active connections are successful and will be displayed and contain information relating to the IPSec Policy, Active Filter Action and IP Filter List.
12. **Click** the Options button to change refresh rate to **1** --- > select **ok** --- > minimize.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

13. Wk Station # 2, open a command window and **ping** Wk station # 1. The command window will show IPSEC being negotiated. If negotiation is not viewed continue on the P.E.
14. **Restore** the IP Security Monitor, and review Security Association between the two machines
15. Repeat the *ping* command until you see successful ping replies.
16. Stop the Net Monitor and review captured packets.
17. Note: You should see IPSEC Security Association. Review the description of the event.
18. Un-assign **Wk Station #1** and **Wk Station #2**. In right pane, **right click policy**, (IP Security Policies on Local Machine in Left Pane), and then click **Unassign**.

II. Creating a Custom Management console for local IPSec Policy

1. Create IP Security Policy snap-in and save it as Ipsec.msc
2. In *left* pane of IP Security Policy
3. **Right click** on IP Security Policy s select **Create IP Security Policy**
4. When the IPSec Policy wizard appears, click the **Next** Button
5. Type the policy name **IPSEC Custom1**, in text box add **Information Assurance** click **NEXT** button
note: The Requests For Secure Connection page appears
6. Verify that the Active The Default Response Rule check box is **selected**, click **NEXT**
7. Accept default response, (Kerboes Rule Authentication Method Box) click **next**
8. Leave the Edit Properties check box selected, click **Finish** Button
9. **Clear** the Use Add Wizard in the newly created IPSec Custom1 properties Box.
10. In **Rules** tab of properties dialog box, click **ADD** button.
 1. Note: You will be configuring filters between your computer and your partners computer.
 2. Click the **ADD** button in the IP Filter List tab.
 - a. Workstation #1
 - i. In IP Filter List pane, highlight and rename the filter to **CustomFilter1 Host A to B**.
 - b. Workstation #2
 - i. In IP Filter List pane, highlight and rename the filter to **CustomFilter1 Host B to A**.
 3. **Both Computers**
 4. **Clear** the Use Add Wizard check box.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

5. In Ip Filter list tab, click **ADD** button.(filter properties box appears)
6. In *Source Address* list, select Specific IP address.
7. Input your ip address.
8. In the *Destination Address* list, select A specific IP Address
9. Input your partners IP address, click OK, click close
10. In IP Filter List tab, select CustomFilter1 option
11. Open Filter Action tab, clear the Use Add Wizard check box, and then click add
12. Security Methods tab, click ADD
13. In New Security Method dialog box, select Medium (AH) option, click OK

III. Next task is to configure input and output Filter Action:

Note: Filter Action specifies what security action will take place upon starting a filter. The action specifies whether to permit the traffic, block the traffic, or negotiate the security for the given connection. In addition, additional settings are available to react if non-IPSec protected data is received.

14. Highlight or click New Filter Action Properties dialog box, open General tab.
15. In the Name box, type MediumFilter, enter description then click ok
16. Close dialog box
17. select the option button next to MediumFilter.
18. Open Authentication Methods tab.
19. Click add button.
20. The new Authentication Method dialog box appears
21. Select the *Use This String to Protect The Key Exchange (preshared key)*
22. In the *New Authentication Method* properties, Type informationassurance in the text box, click ok
23. Select Preshared Key in the list, click the **Move Up Button**.
24. Click Close to return to the Policy Properties dialog box and to complete the creation of this rule.
25. Click Close in the Policy Properties dialog box.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Testing a Custom Policy

Note: Ensure you and your partner are working together.

26. Assign the policy just made (IPSec Custom1)
27. In right pane of custom console, r-click the IPSec Custom1 policy, click assign
28. The policy Assigned column value is set to yes.
29. Bring up IPsecmon and review security association and IPSec statistics
30. *PING* your partners computer
 - a. The first ping will usually fail due to time it takes to negotiate policy.
 - i. with matching policies on both computers, future **pings** will work.
 - ii. Alternatively, enable and disable the policy to see the effects of non-matching policy settings.

Note: In IPSec Monitor, you will see in the Security Association Box, the policy name, security, filename, src address, dest address, protocol, src port, dst port and tunnel equipment. IP Stat

31. Stop !!! and review information.

To view IPSEC integrity packets (AH format)

32. 1. Start *Network Monitor* and if not set from previous Practical Exercise set the *capture network* to the appropriate media access control address network card.
33. In MMC interface, assign IPSec Custom1 policy.
34. Start capturing packets w/ NETMON
35. Start **ipsecmon**
36. *Ping* second computers IP address.
Note: may have to repeat because PING has a short time-out, and the delay establishing IPSEC association between two computers. Notice IPSec Negotiations is command window.

37. Stop and view the capture on NETMON.



38. Double-click the first Internet Control Message Protocol (ICMP) packet

Note: you should see headers for *frame, Ethernet, IP, AH* and ICMP in detailed pane.

39. Expand **IP entry** and record IP Protocol number. _____.
40. Record Number of Data Bytes remaining _____

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

41. Notice IP payload is in clear text.
42. The data for a PING is _____.

Now we will initiate FTP and Telnet connections utilizing IPsec.

43. Open a command prompt – **start** – **run**
44. Enter **ftp xxx.x.xxx.xx** (partner PC)
45. Enter **administrator** as user and **student** as password
46. Type **bye**
47. **The user that did not setup Telnet** - Click – **start** – **run**
48. Enter **telnet xxx.x.xxx.xx** (partner PC)
49. Enter **administrator** as user and **student** as password
50. Type **exit**

Now let's see if we can still see our user and password information

51. **Both Users**

52. Stop the capture



53. View what has been captured



54. What did we capture for FTP and Telnet ? Can you locate the User name and password?

55. What protocols did we pick up?
Note: refer to reading assignment

EXERCISE 1. **To set higher encryption:** By configuring AH security method, we ensured authentication but did not encrypt the data in the packet. AH just makes sure that the packet data, as well as most parts of the IP header, source and destination IP addresses, are not modified. We will now look at traffic using the ESP security method that will encrypt the data part of the IP packet.

56. Right-click IP Security Policy on Local Machine
57. Click manage IP Filter Lists and Filter Action
58. Click Manage Filter Action tab
59. Select Medium Filter
60. Click edit
61. Click edit, In Medium Filter Properties to change security method

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

62. Change Medium to High (ESP)

63. Close all Dialogue Boxes

64. Assign the IPSec Custom1 Policy

View IPSec encrypted (ESP) Packets.

65. Begin capturing packets with Network Monitor

66. Run IPSECMON utility

67. *Ping* your second computers IP address. Note: may have to repeat because PING has a short time-out, and the delay establishing IPSEC association between two computers

68.  *View the results of the negotiation (ipsecurity negotiation)*

69. View IPsec Mon

70. Stop and view the NETMON

71. Double-click the first ESP frame

72. The four entries in the details pane are: Frame, Ethernet, IP, and ESP:SPI
IPSEC has created a hash of the ICMP and Data fields of the frame

73. Expand the IP section and record the IP Protocol

74. Scroll to the bottom of the IP details and double-click the IP:

Data: Number of Data Bytes Remaining will vary but you will see **the data has been encrypted** verses results in step = 42 (0x004c) line. Look at the Hex pane; you will see the data has been  instead of results of when the IP Payload was in clear text.

75. By configuring the ESP Security Method the data part of the IP packet was encrypted where as by just configuring AH security we all ensured authentication of the packet was ensured.

FINISHED !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Bonus: Repeat steps 65-76, instead of ping use telnet and ftp and view the results .



Authentication



- Authentication in Widows 2000
- NTLM vs. NTLMv2
 - Vulnerabilities
 - Countermeasures
- Support for legacy systems

3-1

Authentication							
Vulnerability	Countermeasure						
<p>Authentication is the process whereby the computer takes the typed username and password and compares it to the Security ID assigned to it, after the comparison matches the user is authorized to use the items that the security token is assigned to. If an insecure method is utilized to authenticate a user, persons may gain unauthorized access to your system.</p> <p>Note: For</p>	<p><u>COUNTERMEASURE A:</u></p> <p><input type="checkbox"/> 1. Define a particular level of authentication</p> <ul style="list-style-type: none"> • Start Registry Editor regedit32 • Find the following Key HKLM\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel <table style="margin-left: 20px; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;"><u>Data Type</u></th> <th style="text-align: left;"><u>Range</u></th> <th style="text-align: left;"><u>Default Value</u></th> </tr> </thead> <tbody> <tr> <td>REG_DWORD</td> <td>0x0-0x05</td> <td>0xYY</td> </tr> </tbody> </table> <p>Where YY equals</p> <p>0 = Send LM & NTLM responses</p> <p style="padding-left: 40px;">1 = Send LM & NTLM - use NTLMv2 session security if negotiated:</p> <p>2 = Send NTLM responses only:</p> <p>3 = Send NTLMv2 responses only:</p> <p style="padding-left: 40px;">4 = Send NTLMv2 responses only\refuse LM</p> <p style="padding-left: 40px;">5 = Send NTLMv2 responses only\refuse LM and NTLM:</p> <p style="text-align: center;">Note: Default value for the above registry entry is 0.</p> <p style="color: red;">Warning: Setting this value higher than 2 on a Windows 2000 system could prevent some connectivity to systems that support only LM authentication (Windows 95/98 and Widows for</p>	<u>Data Type</u>	<u>Range</u>	<u>Default Value</u>	REG_DWORD	0x0-0x05	0xYY
<u>Data Type</u>	<u>Range</u>	<u>Default Value</u>					
REG_DWORD	0x0-0x05	0xYY					

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>compatibility with down-level clients and servers, W2K supports NTLM. NTLM has four versions. These versions are : LAN Manager (LM), Windows NT LanManager Version 1 (NTLM), Windows NT LanManager Version 2 (NTLMv2), and Secure Socket Layer/Transport layer Security. The LanManager authentication (LM) is the most insecure method, allowing encrypted passwords to be easily sniffed off the network and cracked. NT LanManager (NTLM) is somewhat more secure. By default, W2K will try NTLMV2, first when communicating to a down-level client.</p>	<p>Workgroups) or only NTLM (Windows 4.0 prior to Service Pack 4)</p> <p>Warning: If adding a Windows 2000 machine to a Windows NT 4.0 domain, this value may need to be set to 4 on the Windows NT 4.0 domain controller.</p> <p>Note: To configure legacy systems see Countermeasure C below.</p> <p><u>COUNTERMEASURE B:</u></p> <ul style="list-style-type: none"><input type="checkbox"/> 1. Migrate to a total Windows 2000 network. <p><u>COUNTERMEASURE C:</u></p> <ul style="list-style-type: none"><input type="checkbox"/> 1. To configure legacy system install AD Client Extension (MSClient) from the W2K installation CD. See Q239869.• WIN 2000 should be configured to always send NTLM V2 response_only\refuse LM+NTLM
--	---

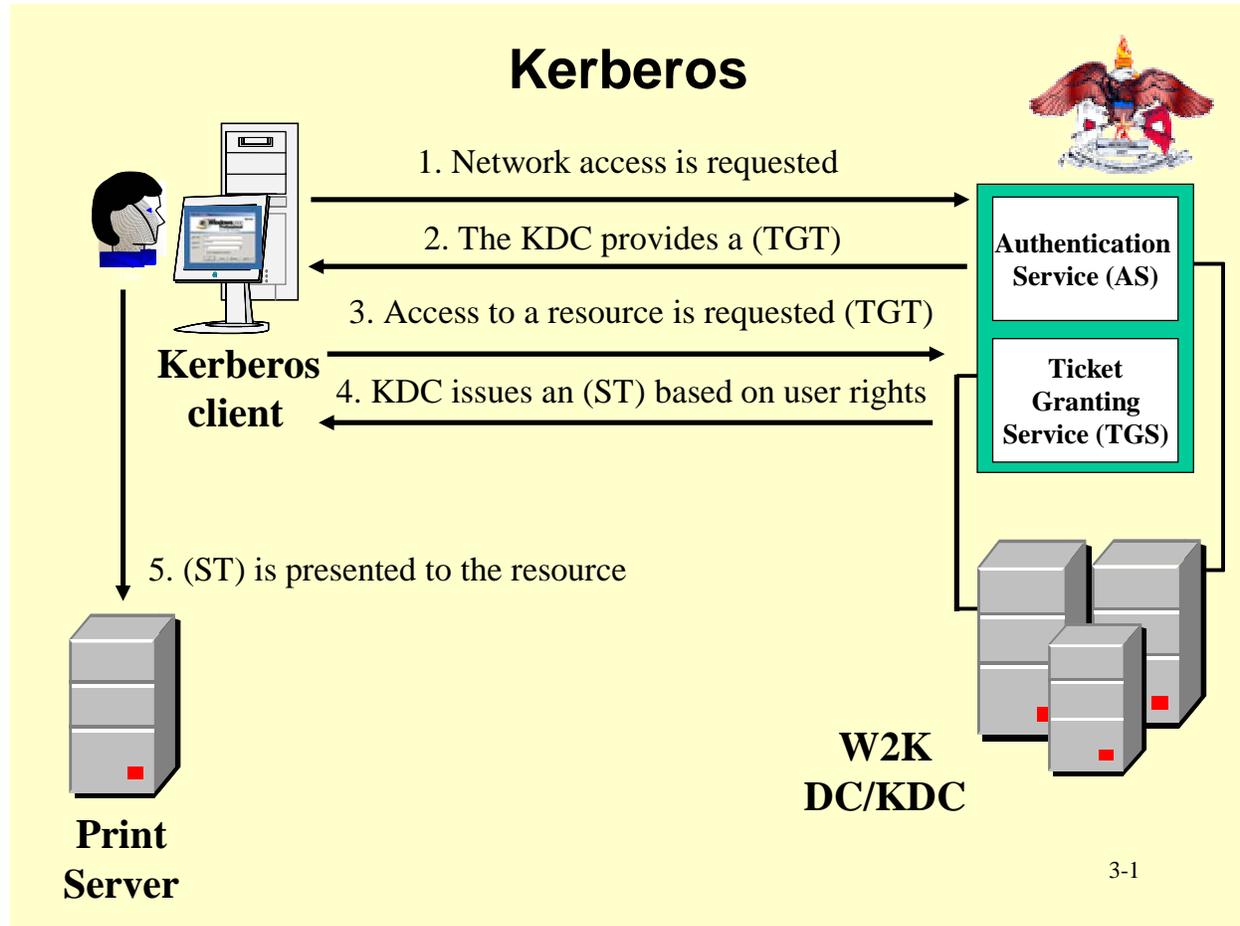
Kerberos



- What is Kerberos
- How does Kerberos work
 - Client/application
 - Network resource
 - Key Distribution Center (KDC)



Kerberos	
Vulnerability	Countermeasure
<p>Kerberos is the core Windows 2000 security protocol typically used by IKE for IPSec authentication. This traffic uses a UDP/TCP protocol source and destination port 88. Kerberos is itself a security protocol that does not need to be secured by IPSec. The Kerberos exemption is basically this: If a packet is TCP or UDP and has a source or destination port = 88, permit.</p> <p>If a port scan using source port 88 is ran, it will get results no matter what W2K IPSec filters are in place.</p>	<p><input type="checkbox"/> 1. Use regedt32 to create or assign the following registry key value:</p> <p style="margin-left: 40px;">Registry Hive: HKEY_LOCAL_MACHINE SubKey: \System\CurrentControlSet\Services\IPSEC ValueName: NoDefaultExempt Data Type: REG_DWORD Value Data: 1</p> <ul style="list-style-type: none"> • Save and Reboot the system. <p>Note:</p> <ul style="list-style-type: none"> • On a default system this key needs to be added. • Lock the Key Distribution Center (KDC) server in a secure room and do not attach a keyboard or display. Administer this server from a client workstation with appropriate administration software installed. Audit every access and attempted access to the server. If you KDC is not secure, nothing is.



Kerberos Configuration

- Credential Time
 - Service Ticket (session ticket) = 10 hrs
 - User Ticket (TGT) = 10 hrs
 - Maximum renewal time = 7 days

3-1

Kerberos

- Vulnerability within Kerberos
 - IPSec
 - Known port numbers
 - System clocks need to be synchronized

3-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<div style="text-align: center;">  <p>Network Access</p> <ul style="list-style-type: none"> • Who needs Access • Access to the server • Remote Access • Revoking Access <p style="text-align: right; font-size: small;">3-1</p> </div>	
--	--

Network Access	
Vulnerability	Countermeasure
<p>Consider revoking network access to the server. By doing this, you are requiring all server administration to be done from the server console.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> 1. Click the Start button and choose Run. <input type="checkbox"/> 2. Type in MMC. <input type="checkbox"/> 3. Once the MMC console box comes up left-click on Console from the tool bar. <input type="checkbox"/> 4. Choose Add/Remove Snap-in. <input type="checkbox"/> 5. Left-click Add, choose Security Configuration and Analysis, left-click Add, Close, OK. <input type="checkbox"/> 6. Right-click on Security Configuration and Analysis, choose Open Database. <input type="checkbox"/> 7. Type in a new database name, and then click Open. <input type="checkbox"/> 8. Select a Security Template to import, and then click Open. <input type="checkbox"/> 9. Right-click the Security Configuration and Analysis scope item and choose Configure Computer Now. <p>Note: After the configuration is complete, you must perform an analysis to view the information in your database.</p> <ul style="list-style-type: none"> <input type="checkbox"/> 10. Right-click the Security Configuration and Analysis scope item and choose Analyze Computer Now. <input type="checkbox"/> 11. In the dialogue box, type the path of the log file, and click OK. You may choose the default path if you do not have log files set up. <input type="checkbox"/> 12. Expand the Security Configuration and Analysis scope item. <input type="checkbox"/> 13. Expand the Local Policies. <input type="checkbox"/> 14. Double-click User Rights Assignment. <input type="checkbox"/> 15. Double-click Access this computer from the network.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p><input type="checkbox"/> 16. Place a check mark in the box “define this policy in the database”.</p> <p style="padding-left: 40px;"><input type="checkbox"/> 17. Place a check in the box for the group/groups you wish to have network access to the computer.</p> <p><input type="checkbox"/> 18. Click O.K.</p> <p><input type="checkbox"/> 19. Save the policy under the default directory and reboot the server.</p>
--	--



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS-2E

EXERCISE D

This practical exercise will provide hands-on experimentation with process tokens.

Please retain from the instructor the appropriate drive letter to use in place of *W2KServer*.

1. Log on locally to the *W2KServer*, using the *backupXXX* account (pwd = student). The *backupXXX* account has the *SEBACKUP* and *SERESTORE* privileges.

2. Select Start->Run.



3. Enter the command *PVIEW* and Press enter key or click the OK Button.

4. From the drop-down menu in the middle-left select *pview.exe*.

5. Click the Token Process button in the lower-left corner of the *PVIEW* window. Which groups are enabled to use *pview.exe*?

Note the disable privileges. Why are some privileges disabled?

6. Close *PVIEW* window by pressing the OK button to close the Security context and the Exit button to close the *PVIEW* Window.

7. Select Start->Programs->Accessories->Windows Explorer.

8. Attempt to open the secret folder on the *W2KServer* Partition (*MyComputer\W2KServer*). Only administrators have full control on the secret folder. No other group has been granted access. What were your results?

9. Close the Error Dialog Box.

10. Select Start->Run

11. Enter the command *PVIEW* and Press enter key or click the OK Button.

12. From the drop-down menu in the middle-left select *explorer.exe*.

13. Click the Token Process button in the lower-left corner of the *PIEW* window.

14. Enable the *SEBACKUP* and *SERESTORE* privileges for *explorer.exe* by selecting *SEBACKUP* and *SERESTORE* from the Disable Listing and pressing the << button.

15. Click OK to close the Process Access Token window.

16. Using the Explorer window already open, double-click on the secret folder again.

What are your results?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

17. What Security issues are associated with the SEBACKUP and SERESTORE privileges?

18. Log out.

19. Wait for instructor review.

Server Message Block (SMB)



- What is SMB
- Anonymous connections
- Session hijacking
- Sniffing SMB Packets

3-1

Vulnerability	Countermeasure
<p>SMB is implemented as the Server and Workstation service on W2K computers. However, SMB is generally considered a security problem if you are connected to an untrusted network. Some of the potential risks associated with the SMB are:</p> <ol style="list-style-type: none"> 1. Using anonymous connections to access SMB “shares” that do not have appropriate ACL’s. 2. Having a session “hijacked” by someone who then masquerades as the real client. 3. Sniffing the data out of the SMB packets. 	<p><u>Countermeasure A:</u></p> <p><input type="checkbox"/> 1. Enable SMB signing, also known as Common Internet File System (CIFS). Take the following steps to enable SMB signing utilizing Security Snap-ins within MMC.</p> <ul style="list-style-type: none"> • Click the Start button and choose Run. • Type in MMC. • Once the MMC console box comes up left-click on Console from the tool bar. • Choose Add/Remove Snap-in. • Left-click Add, choose Security Templates, left-click Add, Close, OK. • Expand the Security Templates scope item. • Expand Local Policies. • Left-click Security Options. • At this point, you can enable four separate options to tailor the SMB signing options to meet your organizations security requirements. <p>Note: To use SMB digital signing, this option must be enabled on both the SMB client and server.</p> <ul style="list-style-type: none"> • Digitally sign Client Communications (Always) Forces an SMB client to always digitally sign SMB communications. Digital signatures provide mutual authentication during SMB exchanges, preventing “man-in-the-middle” and active message attacks.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<ul style="list-style-type: none"> • Digitally sign Client Communications (When Possible) Enables an SMB client to perform digital packet signing when communicating with an SMB server that also supports packet signing. • Digitally Sign Server Communications (Always) Forces an SMB server to always digitally sign SMB communications. • Digitally Sign Server Communications (When Possible) Enables an SMB server to perform digital packet signing when communicating with an SMB client that also supports packet signing.
--	--



NULL Session

- What is a Null Session
 - A connection with a blank (null) username and password
 - The anonymous user is placed in the Everyone Group

3-1

<i>Null Access</i>	
Vulnerability	Countermeasure
<p>Null session (a.k.a. Anonymous access) is defined as a connection with a blank username and a blank password. When someone makes an anonymous connection, the anonymous user is Granted privileges and permissions of the Everyone Group. Once this anonymous authentication is made, the user may issue MSRPC calls to obtain information or attempt to access any files that are shared by the Everyone group.</p>	<p><u>Countermeasure A:</u></p> <p><input type="checkbox"/> 1. Disable ports 139 and 445.</p> <ul style="list-style-type: none"> • Go to Network and Dial-up Connections in Control Panel. • Highlight Local Area Connection. • From the toolbar, choose Advanced, Advanced Settings. • Remove the check from the File and Printer Sharing box. • Click O.K. <p>Note: TCP 139 will still appear during a port scan even after this is set. However, the port will no longer provide NetBIOS-related information.</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Countermeasure B:

1. If you choose to leave NetBIOS/SMB enabled, you must set RestrictAnonymous. Use regedt32 to **create** or **assign** the following registry key value:

Registry Hive: HKEY_LOCAL_MACHINE
SubKey: \System\CurrentControlSet\Control\Lsa
ValueName: RestrictAnonymous
Data Type: REG_DWORD
Value Data: 1

Note: The default value is 0

Countermeasure C:

1. Alternative method of setting RestrictAnonymous is through the MMC.

- Click the **Start** button and choose **Run**.
- Type in **MMC**.
- Once the MMC console box comes up left-click on **Console** from the tool bar.
- Choose **Add/Remove Snap-in**.
- From the Snap-in window choose **Add**.
- Choose **Group Policy** and choose **Add**.
- Browse until you find the domain you wish to implement the policy on, choose **OK**.
- Highlight **Default Domain Controller Policy**, choose **OK**.
- Select **Finish**.
- Select **Close**.
- . Select **OK**.
- Expand the policy to **Windows Settings, Security Settings, Local Policies, Security Options**.
- Double-click **Additional restrictions for anonymous connections**.
- Place a check in **Define this policy setting** box.
- From the pull-down menu, choose **Do not allow enumeration of SAM accounts and shares**.
- Choose **OK**.
- Save policy to default directory and reboot server.

Note:

The following method can be used to verify that anonymous log-ins are not allowed.

1. In the “Command Prompt” window, enter the following

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p>command, and attempt to logon as the user “anonymous:”</p> <pre>c:\>ftp 127.0.0.1 Connected to ftru014538 Microsoft FTP Service (Version 2.0). User (ftru014538.ncr.disa.mil: (none)): anonymous 331 Anonymous access allowed, send identity (email name) as password. Password: <i>password</i> 230 Anonymous user logged in. ftp></pre> <ul style="list-style-type: none">• If the command response indicates that an anonymous FTP login was permitted, you should immediately check to see that no blank passwords are permitted. That the guest account is truly disabled, and that ftp services are turned off unless needed.
--	---



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

W2K Network Security

Practical Exercise SAS-3A

Exercise A

This practical exercise will provide hands-on experimentation with shared folders and anonymous logons. Please retain from the instructor the appropriate drive letter to use in place of *W2K Server*.

1. Log on locally to the W2KServer, using the administrator account.
 2. Select Start->Programs-> Accessories ->Windows Explorer
 3. Drill down to the stage1 folder (MyComputer\W2Kserver\). Right-click the folder, stage1.
 4. Select Sharing.
 5. Click the Share This Folder button.
 6. Accept the default share name for stage1.
 7. Click the Permissions button.
 8. On the Permissions window, modify the default permissions to Everyone: Read, by deselecting allow Full Control & Change. Press apply.
 9. Click OK to close the Permissions window.
 10. Click OK to close the stage1 Properties window.
 11. Click Start->Run.
 12. Enter the UNC name of the share you created: \\your machine name\stage1.
 13. Attempt to create a folder in the stage1 share. What are your results?
-
14. Close the share window.
 15. Drill down through the file system to the stage2 folder.
 16. Right-Click the stage2 folder.
 17. Select the Sharing Tab. Click the Share This Folder button.
 18. Click the Permissions button. On the Permissions window, click add, if the Network Password Window appears, select cancel. At the drop-down box, select the current workstation name. (ex. WS217xxx)
 19. Add an ACE for Administrators: Read & Change. Select the Administrators group, click Add, click OK. On the Permissions window, select Administrators, select Change, press apply. Delete the default ACE for Everyone by selecting the Everyone group and press the Remove button.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

20. Click OK to close the Permissions window.
 21. Click OK to close the stage2 Properties window.
 22. Click Start->Run
 23. Enter the UNC name of the share you created: \\your machine name. Select the stage2 share.
 24. Attempt to create a folder, named stage3, in the stage2 share. What are your results?
-
25. Right-Click the stage3 folder.
 26. Select Properties.
 27. Select the Security Tab button.
 28. Add an ACE for Anonymous Logon: Modify. On the Permissions window, click Add, if the Network Password Window appears, select cancel. At the drop-down box, select the current workstation name.
 29. Select the Anonymous Logon group. Click Add. Click OK. Select Modify. Click OK to close the Permissions window.
 30. Verify the permission setting on the stage3 folder. What ACE's are defined?
-

Investigating hidden shares

Note: In this part of the exercise, you will need to synchronize your activities with your partner on another machine. The instructor will pair the students. One system shall be booted into Server. One system shall be booted into Professional.

On the system booted into Server

31. Log on locally to the W2KServer, using the administrator account.
32. Click Start->Run.
33. Type mmc in the command window.
34. From the Console drop-down menu, select Add/Remove Snap In.
35. Click the Add button.
36. Select the Shared Folders Snap In.
37. Click the Add button.
38. Click Finish to accept the default values.
39. Click Close to close the Snap In List window.
40. Click OK to close the Add/Remove window.
41. Double-click Shared Folders (Local).

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

42. On the Tree pane, click Shares. What information is displayed?

43. On the Tree pane, click Sessions. What information is displayed?

44. Click Start->Run

45. Type cmd in the command window.

46. In the command window, type net use to view a list of the active sessions. If any active sessions exist, type **net use ^*/delete**. Enter Y when prompted.

On the system booted into Professional

47. Log on locally to the W2Kprofessional, using the administrator account.

48. Click Start->Run

49. Type cmd in the command window.

50. Map to W2K Server by typing: **net use ^ z: ^ \\machine_name\administrative share** (where machine_name is your partner's computer and administrative share is the administrative share provided by the instructor). **DO NOT DELETE ANY FOLDERS OR FILES FOUND ON THE MAPPED DRIVE !!!!**

51. Click Start->Run

52. Type **\\\\machine_name\administrative share** or open the share with Windows Explorer.

On the system booted into Server

53. On the Tree pane, click Shares. What information is displayed?

54. On the Tree pane, click Sessions. What information is displayed?

On the system booted into Professional

55. In the command window type: **net use ^*/delete** to clear the drive mappings. Enter Y when prompted.

On the system booted into Server

56. On the Tree pane, click Shares. What information is displayed?

57. On the Tree pane, click Sessions. What information is displayed?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Anonymous logon exploits

Note: To demonstrate the capabilities of resource enumeration using anonymous logon, we must create a unique local user account. This account will be “unauthenticated” at the other member servers and domain controllers in our enterprise.

Execute this following on the W2K Professional (non-firewall machine)

On the system booted into Professional

58. Right-click on My Computer.

59. Select Manage.

60. Open the Local User and Groups folder.

61. Open the user folder, right-click in the right pane and select New User

62. Name the user LocalX, where X is the last octet of your computer’s IP. Leave the password blank and clear the User must change password at next logon checkbox. Click the create button. Close the new user box.

63. Close the Computer Management Console.

64. Log out of the administrator account.

65. Log in using the LocalX account .

66. Click Start->Run

67. Attempt to browse your neighbor’s computer by typing `\\machine_name`, where machine_name is the name of your neighbor’s machine, in the command window.

Why does the Connect As window appear? Note: If the Connect As window does not appear, this may be an indication that the LocalX account created is being authenticated by the network and not a local account to the system.

68. Cancel the Connect As window.

69. Select Start->Programs->Administrative Assistant->Red Button. The Red Button program establishes a null-user session to exploit the anonymous logon.

70. On the Red Button Window, select the Select Server button. Provide the IP address of the victim computer and click OK and clicking the big GO button.

What information does Red Button reveal?

71. Close Red Button by pressing OK to close the Access Granted Window and Close to close Red Button.

72. Select Start->Programs-> Accessories ->Windows Explorer

73. Open the root of the W2KPro (MyComputer\W2KPro).

74. Select Start->Programs->System Tools->DumpSec. Explorer (Have the students do a search on Dumpsec).

75. On the DumpACL Window, select Report->Select Computer.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

76. Type the name or IP address of the intended victim. What error message did you receive?

DumpACL does not automatically establish a null-user session as Red Button did.

77. In a command window type `net use \\intended_victim_IP\ipc$ /user:"" ^ ""`. (The quotes are 2 sets of double quotes).

78. Repeat steps 75 - 76.

79. On the DumpACL Window, select the Report drop-down menu, select the DumpUsers as Table option. Add fields from the available fields to the Selected fields. Press OK.
How can the information displayed be utilized by an intruder ?

80. Close DumpACL

81. Logout.

82. Wait for instructor review.



Denial of Service

- What is Denial of Service
- Vulnerabilities in Windows 2000
- Exploits to TCP/IP Stack within Windows 2000
 - IP Fragment Flooding
 - SYN Flooding
- Countermeasures

3-1

Denial of Service Against TCP/IP Stack	
Vulnerability	Countermeasure
<p>DoS attacks attempt to remove a system or resources from the network. Networking protocols such as TCP/IP were designed to be used in an open and trusted community, and current version-4 incarnations of the protocol have inherent flaws. In addition, many operating systems and network devices have flaws in their network stacks that weaken their ability to withstand DoS attacks. These may include bandwidth consumption, resource starvation, or routing and DNS attacks.</p> <p>Note: DoS attacks against NT were patched in service pack 6a, W2K is comparatively quite</p>	<p>Countermeasure A: Security Considerations for Network Attacks Take the following steps to lower the vulnerability of a website to these and other network attacks:</p> <ul style="list-style-type: none"> <input type="checkbox"/> 1. Monitor networks boundaries for attacks. Many third party companies offer tools that can detect these types of attacks. (an intrusion detection tool that Is widely used can be found at:www.iss.net) <input type="checkbox"/> 2. Ensure that routers are not converting layer 3 broadcasts into layer 2 broadcasts. The Cisco command to disable this is: no ip directed-broadcast. This is the default setting for routers that use IOS version 12.0 or greater. <input type="checkbox"/> 3. Restrict routers to allow only the use of ports that are necessary for the site to function. <input type="checkbox"/> 4. Disable unnecessary or optional services (i.e.: Client for Microsoft Networks on a IIS server) <input type="checkbox"/> 5. Enable TCP/IP filtering and restrict access to only the ports that are necessary for the server to function. (see Q150543 for a list of ports that Windows services use) <input type="checkbox"/> 6. Unbind NetBIOS over TCP/IP where it is not needed. <input type="checkbox"/> 7. Configure static IP addresses and parameters for public adapters. <input type="checkbox"/> 8. Configure registry settings for maximum protection <p>Countermeasure B: Use regedit32 to create or assign the following registry key value:</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

robust in this regard. However, nothing is invulnerable to DoS, therefore, certain steps should be taken to harden the system.

Registry Hive: HKEY_LOCAL_MACHINE
SubKey:
\\System\\CurrentControlSet\\Services\\Tcpip\\Parameters
ValueName: SynAttackProtect
Data Type: REG_DWORD
Value Data: *x*

Where *x*:

- 0 – no synattack protection
- 1 – reduced retransmission retries and delayed RCE (route cache entry) creation if the TcpMaxHalfOpen and TcpMaxHalfOpenRetried settings are satisfied
- 2 – in addition to 1 a delayed indication to Winsock is made.

Default: 0 (False)

Recommendation: 2

Description: Synattack protection involves reducing the amount of retransmissions for the SYN-ACKS, which will reduce the time for which resources have to remain allocated. The allocation of route cache entry resources is delayed until a connection is made. If synattackprotect = 2, then the connection indication to AFD is delayed until the three-way handshake is completed. The actions taken by the protection mechanism only occur if TcpMaxHalfOpen and TcpMaxHalfOpenRetried settings are exceeded.

Note:

- On a default system this key needs to be added.
- The Registry changes for configuring Windows 2000 and IIS are described in the [IIS security checklist](#)
- Consult Microsoft security web site regularly for [security bulletins](#)

Registry Key:

Registry Hive: HKEY_LOCAL_MACHINE
SubKey:
\\System\\CurrentControlSet\\Services\\Tcpip\\Parameters
ValueName: TcpMaxHalfOpen
Data Type: REG_DWORD
Value Data: *x*

Where *x* is

- 100 – Professional Server
- 500 – Advanced Server

Recommendation: default

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Note: On a default system this key needs to be added.
Description: This parameter controls the number of connections in the SYN-RCVD state allowed before SYN-ATTACK protection begins to operate. If SynAttackProtect is set to 1, ensure that this value is lower than the AFD listen backlog on the port you want to protect (see Backlog Parameters for more information). See the SynAttackProtect parameter for more details.

Registry Key:

Registry Hive: HKEY_LOCAL_MACHINE
SubKey:
\\System\\CurrentControlSet\\Services\\Tcpip\\Parameters
ValueName: TcpMaxHalfOpenRetried
Data Type: REG_DWORD
Value Data: *x*

Where *x* is

80 – Professional Server
400 – Advanced Server

Recommendation: default

Note: On a default system this key needs to be added.
Description: This parameter controls the number of connections in the SYN-RCVD state for which there has been at least one retransmission of the SYN sent, before SYN-ATTACK attack protection begins to operate. See the SynAttackProtect parameter for more details.

Registry Key:

Registry Hive: HKEY_LOCAL_MACHINE
SubKey:
\\System\\CurrentControlSet\\Services\\Tcpip\\Parameters
ValueName: EnablePMTUDiscovery
Data Type: REG_DWORD
Value Data: *x*

Where *x* is

0 – False
1 - True

Default: 1 (True)

Recommendation: 0

Note: On a default system this key needs to be added.
Description: When this parameter is set to 1 (True) TCP attempts to discover the Maximum Transmission Unit (MTU or largest packet size) over the path to a remote host. By discovering the Path MTU and limiting TCP segments to this

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

size, TCP can eliminate fragmentation at routers along the path that connect networks with different MTUs. Fragmentation adversely affects TCP throughput and network congestion. Setting this parameter to 0 causes an MTU of 576 bytes to be used for all connections that are not to hosts on the local subnet.

Registry Key:

Registry Hive: HKEY_LOCAL_MACHINE
SubKey:
\\SYSTEM\\CurrentControlSet\\Services\\NetBt\\Parameters
ValueName: NoNameReleaseOnDemand
Data Type: REG_DWORD
Value Data: X

Where *x* is

0 – False
1 - True

Default: 0 (False)

Recommendation: 1

Note: On a default system this key needs to be added.

Description: This parameter determines whether the computer releases its NetBIOS name when it receives a name-release request from the network. It was added to allow the administrator to protect the machine against malicious name-release attacks.

Registry Key:

Registry Hive: HKEY_LOCAL_MACHINE
SubKey:
\\SYSTEM\\CurrentControlSet\\Services\\Tcpip\\parameters
ValueName: EnableDeadGWDetect
Data Type: REG_DWORD
Value Data: *x*

Where *x* is

0 – False
1 - True

Default: 1 (True)

Recommendation: 0

Description: When this parameter is 1, TCP is allowed to perform dead-gateway detection. With this feature enabled, TCP may ask IP to change to a backup gateway if a number of connections are experiencing difficulty. Backup gateways

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

may be defined in the Advanced section of the TCP/IP configuration dialog in the Network Control Panel.

Registry Key:

Registry Hive: HKEY_LOCAL_MACHINE
SubKey:
 \System\CurrentControlSet\Services\Tcpip\Parameters
ValueName: KeepAliveTime
Data Type: REG_DWORD
Value Data: x

Where x is:

Time in milliseconds – 1 – 0xFFFFFFFF

Default: 7,200,000 (two hours)

Recommendation: 300,000

Note: On a default system this key needs to be added.

Description: The parameter controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote system is still reachable and functioning, it acknowledges the keep-alive transmission. Keep-alive packets are not sent by default. This feature may be enabled on a connection by an application.

Registry Key:

Registry Hive: HKEY_LOCAL_MACHINE
SubKey:
 \System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
ValueName: PerformRouterDiscovery
Data Type: REG_DWORD
Value Data: x

Where x is:

0 - disabled

1 - enabled

2 - enable only if DHCP sends the router discover option

Default: 2, DHCP-controlled but off by default.

Recommendation: 0

Note: On a default system this key needs to be added.

Description: This parameter controls whether Windows 2000 attempts to perform router discovery per RFC 1256 on a per-interface basis.

Registry Key:

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p>Registry Hive: HKEY_LOCAL_MACHINE SubKey: \\System\\CurrentControlSet\\Services\\Tcpip\\Parameters ValueName: EnableICMPRedirect Data Type: REG_DWORD Value Data: <i>x</i></p> <p>Where <i>x</i> is: 0 – False 1 - True</p> <p>Default: 1 (True) Recommendation: 0 (False)</p> <p>Note: On a default system this key needs to be added. Description: This parameter controls whether Windows 2000 will alter its route table in response to ICMP redirect messages that are sent to it by network devices such as a routers.</p>
--	---



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

  System Administrator/Network Manager Security Course W2K Checklist Account Security 	 Strong Password Policies <ul style="list-style-type: none"> • In accordance with AR 25-2 passwords will match the following criteria. <ul style="list-style-type: none"> – Min (10) characters long – Contain two (2) characters from all of the following four (4) classes: <ul style="list-style-type: none"> • .English upper case letters A, B, C, ... Z • .English lower case letters a, b, c, ... z • .Westernized Arabic numerals 0, 1, 2, ... 9 • .Non-alphanumeric ("special characters") such as punctuation symbols – May not contain references stated in AR 25-2 Section IV, para 4-12e4.
---	---

3-1

Password Policies & Configuration	
Vulnerability	Countermeasure
<p>IAW MSG DTG 042100Z Mar 99 Fm ACERT Ft Belvoir VA. G. Army policy dictates that passwords in unclassified systems be changed every six months; however, increased security is achieved by changing the password even more frequently</p> <p>Reference: AR 25-2</p> <p>Note: Microsoft has documented conflicting information; reference the maximum password length for Windows 2000 (127 v 128 characters). This discrepancy is being further researched.</p>	<p><input type="checkbox"/> 1. Verify that Windows 2000 is implementing strong password filtering. Passfilt.dll implements the following password policy:</p> <ul style="list-style-type: none"> • Passwords must be at min ten (10) characters long. • Passwords must contain characters from all of the following four (4) classes: <ol style="list-style-type: none"> a. English upper case letters A, B, C, ... Z b. English lower case letters a, b, c, ... z c. Westernized Arabic numerals 0, 1, 2, ... 9 d. Non-alphanumeric ("special characters") such as punctuation symbols <p>Passwords may not contain your user name or any part of your full name.</p> <p><input type="checkbox"/> 2. Use MMC to configure password attributes</p> <ul style="list-style-type: none"> • Select "Start" and "Run" from the desktop. • Type "mmc.exe" in the Run dialog. • Select "Console" from the MMC menu bar. • Select "Add/Remove snap-in" from the drop-down menu. • Click the "Add" button on the Standalone tab. • Select the "Group Policy" snap-in and click the "Add" button. • Insure that "Local Policy" is in the Group Policy Object line and click the "Finish" button.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<ul style="list-style-type: none"> • Click “Close”. • Click “OK”. • Expand the "Computer Configuration" object in the tree window. (<i>Professional & Server</i>) • Expand the "Windows Settings" object. • Expand the "Security Settings" object. • Expand the "Account Policies" object and select "Password Policy". • Maximum Password Age - should be set to 150 days! • Minimum Password Age - should be set to 90 day! • Minimum Password Length - should be set to 10 characters! • Password Uniqueness - "Enforce password history" – should be set to 10 passwords remembered! • Enable Strong Password Filtering - "Passwords must meet complexity requirements" - should be set to enable
--	--

Default Password Protected Screen Saver	
Vulnerability	Countermeasure
<p>If a workstation is left unattended and the screen saver is not password protected, unauthorized personnel could access the workstation and the associated network.</p>	<p><input type="checkbox"/> 1. Use regedt32 to create or assign the following registry key value:</p> <p style="margin-left: 40px;">Registry Hive: HKEY_USERS SubKey: \.DEFAULT\Control Panel\Desktop Value Name: ScreenSaveActive Date Type: REG_SZ Value Data "1"</p> <ul style="list-style-type: none"> • The above registry entry is the default setting • This setting will ensure by default that the user accounts screen savers are activated. <p><input type="checkbox"/> 2. Use regedt32 to create or assign the following registry key value:</p> <p style="margin-left: 40px;">Registry Hive: HKEY_USERS SubKey: \.DEFAULT\Control Panel\Desktop Value Name: ScreenSaveIsSecure Date Type: REG_SZ Value Data "1"</p> <ul style="list-style-type: none"> • The default setting is 0 • This setting will ensure that the screen saver is password protected.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p><input type="checkbox"/> 3. Use regedt32 to create or assign the following registry key value:</p> <p style="margin-left: 40px;">Registry Hive: HKEY_USERS SubKey: \.DEFAULT\Control Panel\Desktop Value Name: ScreenSaveIsTimeOut Date Type: REG_SZ Value Data "900"</p> <ul style="list-style-type: none"> • The above registry setting is the default setting. • This setting will ensure that the screen saver will engage in 15 minutes or less. <p><input type="checkbox"/> 4. Use regedt32 to create or assign the following registry key value:</p> <p style="margin-left: 40px;">Registry Hive: HKEY_USERS SubKey: \.DEFAULT\Control Panel\Desktop Value Name: SCRNSAVE.EXE Date Type: REG_SZ Value Data "logon.scr"</p> <ul style="list-style-type: none"> • The above setting is the default setting. After the value has been set, the complete path may be displayed. • This setting makes sure that there is a valid executable .scr file defined.
---	---

Unnecessary Accounts 

- Remove inactive accounts that exceed 45 days
- Disable any non-active accounts
- Delete user accounts before departure.
- Use "usrstat" to display the last login for each user in a given domain

3-1



Dormant Accounts	
Vulnerability	Countermeasure
Dormant Accounts	<input type="checkbox"/> 1. Disable accounts that have not been logged into within

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>may provide doorways into a system.</p>	<p>the past 45 days.</p> <ul style="list-style-type: none"> • Although there is currently no mechanism for deactivating user accounts, especially if the user has not logged in after a specified amount of time. You can however age an account and specify a time frame for the user account to be disabled. • I. E. In the MMC snap in Active Directory Users and Computers. • Right click on a user account. Click on properties then click on account tab. • Under account expires click on “End of:” Use drop down box and choose a date 45 days from the current date. Once account has reached the date you specified it will be disabled. <p>Note: Use usrstat.exe to display the last login for each user in a given domain.</p> <ul style="list-style-type: none"> • Must have NT 4.0 resource kit loaded. <p>Note: The following accounts are exempt from this check.</p> <ul style="list-style-type: none"> • The built-in administrator account • The built-in guest account • The “IUSR” guest account (used with IIS or Peer Web Services) • Accounts that are less than 45 days-old • Application Accounts • Disabled Accounts
--	--

Administrator & Guest Accounts 

- Rename the administrator and guest account
- Establish decoy accounts named “Administrator” and “Guest” with no privileges.
- Review the event log regularly for attempted access to these accounts

3-1

Rename Administrator Account	
Vulnerability	Countermeasure

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>IAW MSG DTG 042100Z Mar 99 Fm ACERT Ft Belvoir VA. D. Rename the administrator account.</p> <p>Hackers will try to compromise the administrator account by a variety of methods. If they could use a LDAP client such as ldp.exe to enumerate the Active Directory. All of the existing users and groups could be enumerated with a simple LDAP query.</p>	<p><input type="checkbox"/> 1. Rename the administrator account to a non-obvious name (e.g., not "admin," "root," etc.)</p> <p><input type="checkbox"/> 2. Enable account lockout on the real Administrator accounts by using the passprop utility.</p> <p><input type="checkbox"/> 3. Disable the local computer's Administrator account.</p> <p>Note: None of these countermeasures avoid a SID search for the Administrator's account.</p>
---	--

Administrator's Group	
Vulnerability	Countermeasure
<p>The more accounts that are members of the administrator's the more chances for administrative access can fall into the wrong hands.</p>	<p><input type="checkbox"/> 1 LIMIT the membership of the Administrator group.</p>

Everyone Group	
Vulnerability	Countermeasure
<p>The everyone group is a global or universal group and is very dangerous because every account is a member of the Everyone Group. When the Everyone group is granted full control to an object, then ANY account (including the guest</p>	<p><input type="checkbox"/> 1. REPLACE the "Everyone" group with "Authenticated Users"</p> <p>Note: By doing a <u>fresh install</u> of W2K the "Everyone group" for the most part has been replaced with "Authenticated Users". If you do an upgrade then you will</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>account) has full access to the object.</p> <p>Note: The authenticated users group is controlled by the SRM and the systems account.</p>	<p>have to go through and manually remove and replace those items.</p> <p style="text-align: center;">IAW HQ DA SAIS-IAS message DTG 060048Z MAR 99 all guest accounts shall be disabled.</p>
--	---

Set Account Lockout Policy

- Account lockout feature
 - disables account after an administrator-specified number of logon failures.
- Password Protected Screensavers will be automatically activated after 10 minutes when a terminal is left unattended
- Enable lockout after 3 failed attempts

3-1 

Account Lockout Configuration	
Vulnerability	Countermeasure
<p>Intruder will attack systems by a variety of methods. One such method is to bombard the computer with usernames and guessed passwords via a program.</p> <p>Note: Conforms to DISA standards.</p>	<p><input type="checkbox"/> 1. Minimize the number of attempts a User can make when logging in. Use MMC to configure account attributes</p> <ul style="list-style-type: none"> • Select “Start” and “Run” from the desktop. • Type “mmc.exe” in the Run dialog. • Select “Console” from the MMC menu bar. • Select “Add/Remove snap-in” from the drop-down menu. • Click the “Add” button on the Standalone tab. • Select the “Group Policy” snap-in and click the “Add” button. • Insure that “Local Policy” is in the Group Policy Object line and click the “Finish” button. • Click “Close”. • Click “OK”. • Expand the “Computer Configuration” object in the tree window. (<i>Professional & Server</i>) • Expand the “Windows Settings” object. • Expand the “Security Settings” object. • Expand the “Account Policies” object and select “Account Lockout Policy.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- | | |
|--|---|
| | <ul style="list-style-type: none">• Set Account lockout threshold three attempts or less. |
|--|---|



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS-4A

Exercise A

In this lab you will access the Security Configuration and Analysis console, set a working security database, analyze system security, and then view the results. The Security Configuration and Analysis tool offers the ability to configure security, analyze security, view results, and resolve any discrepancies revealed by analysis. This tool is located on the Security Configuration and Analysis console. This lab shows you how to use the Security Configuration and Analysis console. For more clarification, see the Additional Info section, which follows the PE. Please perform the following steps on **W2K Server**.

Accessing the Security Configuration and Analysis Console

In this exercise you access the Security Configuration and Analysis console, the main tool for using the Security Configuration and Analysis tool.

To access the Security Configuration and Analysis console

- ❑ 1. Click Run, type mmc, and then click OK.
 - ❑ 2. On the Console menu, click Add/Remove Snap-In, and then click Add.
 - ❑ 3. In the Add Standalone Snap-In dialog box, select Security Configuration and Analysis, and then click Add.
 - ❑ 4. Click Close, then click OK.
 - ❑ 5. On the Console menu, click Save.
 - ❑ 6. In the File Name box, type security config & analysis to name this console and click Save.
 - ❑ 7. On the console menu, click exit.
 - ❑ 8. To verify that the console appears on the Administrative Tools menu, click start->programs->admintools.
 - ❑ 9. Does the security config & analysis snap-in appear as a menu item?
-
-
-

Setting a Working Security Database

In this exercise you determine the working security database to use. To set a working security database

- ❑ 1. Click Start->Programs->Admintools->Security Config & Analysis.
- ❑ 2. In the Security Configuration and Analysis console, right-click Security Configuration and Analysis.
- ❑ 3. Click Open Database.
- ❑ 4. In the Open Database dialog box, in the File Name box, type **new** for the new personal database file name, then click Open.
- ❑ 5. In the Import Template dialog box, select the "securedc" security template to load into the security database, then click Open.

The "new" database is now the working security database, and it contains the "securedc" security template.

Analyzing System Security

In this exercise you analyze system security, comparing the settings in the security template securedc with the security settings currently running on your system. To analyze system security

- ❑ 1. Right-click Security Configuration and Analysis, then click Analyze Computer Now.
- ❑ 2. In the Perform Analysis dialog box, verify the path for the log file location, then click OK. (accept the default location)
- ❑ 3. The different security areas are displayed as they are analyzed.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Viewing Security Analysis Results

In this exercise you view the security analysis results. To view security analysis results

- 1. In the Security Configuration and Analysis console (left panel), expand Security Configuration and Analysis.
- 2. Expand the Account Policies node, then click the Password Policy security area.
- 3. In the details pane, what is indicated in the Policy column? In the Database Setting column? In the Computer Setting column?

- 4. In the Policy column, what does the red X indicate? What does the green check mark indicate? What would the absence of an icon indicate?

- 5. Wait for instructor review.

Additional Info:

How the Security Configuration and Analysis Console Works

The Security Configuration and Analysis console uses a database to perform configuration and analysis functions. The Security Configuration and Analysis database is a computer-specific data store. The database architecture allows the use of personal databases, security template import and export, and the combination of multiple security templates into one composite security template that can be used for analysis or configuration. New security templates can be incrementally added to the database to create a composite security template; overwriting a template is also an option. You can also create personal databases for storing your own customized security templates.

Security Configuration

The Security Configuration and Analysis console can be used to configure local system security. Through its use of personal databases, you can import security templates created with the Security Templates console and apply these templates to the GPO for the local computer. This immediately configures the system security with the levels specified in the template.

Security Analysis

The state of the operating system and applications on a computer is dynamic. For example, to enable immediate resolution of an administration or network issue, security levels may occasionally be required to change temporarily. After this security requirement is finished, the temporary change may not be reversed. This means that a computer may no longer meet the requirements for enterprise security.

The Security Configuration and Analysis console allows administrators to perform a quick security analysis. In the analysis, recommendations are presented alongside current system settings, and icons or remarks are used to highlight any areas where the current settings do not match the proposed level of security. Security Configuration and Analysis also offers the ability to resolve any discrepancies revealed by analysis.

Regular analysis enables an administrator to track and ensure an adequate level of security on each computer as part of an enterprise risk management program. Analysis is highly specified and information about all system aspects related to

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

security is provided in the results. This enables an administrator to tune the security levels, and most important, to detect any security flaws that may occur in the system over time.

Using Security Configuration and Analysis

- A. The tasks for using Security Configuration and Analysis are
- B. Accessing the Security Configuration and Analysis console
- C. Setting a working security database
- D. Importing a security template into a security database
- E. Analyzing system security
- F. Viewing security analysis results
- G. Configuring system security
- H. Exporting security database settings to a security template

Viewing Security Analysis Results

The Security Configuration and Analysis console displays the analysis results organized by security area with visual flags to indicate problems. For each security policy in the security area, the current database and computer configuration settings are displayed.

In the details pane, the Policy column indicates the policy name for the analysis results, the Database Setting column indicates the security value in your template, and the Computer Setting column indicates the current security level in the system.

- A red X indicates a difference from the database configuration.
- A green check mark indicates consistency with the database configuration.
- A “?” means that the item defined is not on that system.
- No icon indicates that the security policy was not included in your template and therefore not analyzed.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS-4B

Exercise B

This PE provides the student with familiarity with the security database and templates snap-in. The student will learn the relationship between the security database settings and the current computer settings and how you can modify settings in the current security database directly, by modifying templates, and by importing templates.

- 1. Click Start->Programs->Administrative Tools->Security Config & Analysis.
- 2. In the Security Configuration and Analysis console, right-click Security Configuration and Analysis.
- 3. Click Open Database.
- 4. In the Open Database dialog box, select the "new" personal database file, then click Open. The "new" database is now the working security database, and it contains the "securedc" security template.
- 5. Right-click Security Configuration and Analysis, then click Analyze Computer Now.
- 6. In the Perform Analysis dialog box, verify the path for the log file location, then click OK. (accept the default location)
- 7. Expand Security and Configuration Analysis and Account Policies, then click the Password Policy security area.
- 8. Are there places where the Database Setting column differs from the Computer Setting column?

- 9. Expand local policies and click on audit policy. Are there differences between the database setting and the computer setting?

- 10. Click on user rights. Are the computer settings more stringent than the database setting?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- ❑ 11. Expand event log. Click on settings for event log. What is the value for the database security log size? What is the value for the computer security log size?

- ❑ 12. Right click security configuration and analysis
- ❑ 13. Select "configure computer now".
- ❑ 14. Accept the default error log location by clicking "ok".
- ❑ 15. Right click on "security configuration and analysis" and select "analyze computer now".
- ❑ 16. Accept default location and select "ok".
- ❑ 17. Expand account policies and click on password policy.
- ❑ 18. Do the database settings and the computer settings differ now?. _____
- ❑ 19. Expand local policies and click on audit policy.
- ❑ 20. Do database settings and the computer settings differ now?

- ❑ 21. Click on user rights. Have the settings changed at all? Does the computer update the policy on the computer if the database does not define it?

- ❑ 22. Expand event log and click on settings for event log. What is the computer setting value for the size of the security log? How does it compare to the database setting?

- ❑ 23. Go to account policies and click on password policy
- ❑ 24. Double click on "minimum password age"
- ❑ 25. Click the Define This Policy In The Database check box to allow editing, if not selected
- ❑ 26. Enter a new value of 20 for the minimum password age value. then click OK. This will change the value in the database.
- ❑ 27. Click on account lockout policy
- ❑ 28. Double click on account lockout threshold.
- ❑ 29. Click the Define This Policy In The Database check box to allow editing.
- ❑ 30. Set invalid login attempts to 3 and click OK.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- 31. Click OK on the Suggested Value Change Window.
- 32. Take a couple of minutes and double click on some other policies and see how easy it is to modify their value.
- 33. Right click on security configuration & analysis
- 34. Select configure computer now
- 35. Accept the default error log location by clicking OK
- 39. Expand account policies and click on password policy. Has the minimum password age changed on the computer settings? Click on account lockout policy. Has the account lockout threshold changed to match the database value?

- 40. Right click on security configuration & analysis
- 41. Select "export template"
- 42. In the export template to box, type **new** for the file name and click on save.
- 43. Close the Security Configuration & Analysis window
- 44. Select Start->Run , type mmc and hit enter
- 45. In the console menu, select add snap-in
- 46. Select add
- 47. Select "security templates" and click add
- 48. Click close and then OK
- 49. In the console menu choose "save as"
- 50. In the file name block, type **security templates** and click save
- 51. Close console window, if asked to save, choose no.
- 52. Select Start->Programs->Administrative Tools->security templates
- 53. Expand security templates
- 54. Expand \WINNT\Security\Templates
- 55. Expand new. If you expand and look at the policy values, you will see they match the ones you just configured in the database.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- 56. Expand account policies
- 57. Select password policy
- 58. Double click "maximum password age"
- 59. Click the Define This Policy In The Database check box to allow editing.
- 60. Set the password to expire in 150 days and click OK
- 61. Right click on "new" and choose save.
- 62. Close the security templates window but do not save settings
- 63. Select Start->Programs->Administrative Tools->security configuration & analysis
- 64. Right click on security configuration and analysis and select "open database".
- 65. Select "new" and hit enter.
- 66. Expand account policies and select password policy.
- 67. Did the maximum password age value change? What is the value for both the database and the computer ?

- 68. What does this tell you about editing an exported template?

- 69. Right click on security configuration & analysis
- 70. Select "export template"
- 71. Enter **new1** as the file name and click save
- 72. Select Start->Programs->Administrative Tools->security templates
- 73. Expand security templates
- 74. Expand /WINNT/Security/Templates
- 75. Expand new1
- 76. Expand account policies and click on password policy
- 77. Double click maximum password age
- 78. Click the Define This Policy In The Database check box to allow editing.
- 79. Set the password to expire in 90 days and click OK
- 80. Right click on new1 and select save.
- 81. Close the security templates window and if asked to, do not save

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- 82. Select the security configuration & analysis window and right click on security configuration & analysis
- 83. Select import template.
- 84. Select "new1" and click open
- 85. Expand account policies and select password policy
- 86. Has the maximum password age changed for both the database and computer value? what is the current value? What does this tell you about importing templates?

- 87. Close all windows.
- 88. Wait for instructor review

Additional Info:

Configuring System Security

Security Configuration and Analysis offers the ability to resolve any discrepancies revealed by analysis, including the following:

- Accepting or changing some or all of the values flagged or not included in the configuration if you determine the local system security levels are valid due to the context (role) of that computer
- Configuring the system to the original database configuration values if you determine the system is not in compliance with valid security levels
- Importing a more appropriate template, for the role of that computer, into the database as the new database configuration and applying it to the system
- You can repeat the import process and load multiple templates. The database will merge the various templates to create one composite template, resolving conflicts in order of import; the last one imported takes precedence when there is contention. Once the templates are imported to the database, you can choose Configure System Now to apply the stored template (database configuration) to the system.

IMPORTANT

These changes are made to the stored template in the database, not to the security template file. The security template file will only be modified if you either return to Security Templates and edit that template or export the stored configuration to the same template file.

Security Templates Snap-In

A security template is a physical representation of a security configuration; it is a file where a group of security settings may be stored. Windows 2000 includes a set of security templates, each based on the role of a computer. The templates range from security settings for low security domain clients to highly secure domain controllers. They can be used as provided, modified, or serve as a basis for creating custom security templates.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Using the security Templates Snap-In

A security template is a physical file representation of a security configuration, and can be applied to a local computer or imported to a Group Policy Object (GPO) in the Active Directory service. When you import a security template to a GPO, Group Policy processes the template and makes the corresponding changes to the members of that GPO, which may be users or computers.

The security Templates snap-in allows you to perform a variety of tasks:

- Customize a predefined security template
-  Define a security template
-  Delete a security template
- Refresh the security template list
- Set a description for a security template



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

 <p align="center">System Administrator/Network Manager Security Course</p> <p align="center">W2K Checklist Auditing/Logging</p>	<p align="center">W2K different than NT4 </p> <ul style="list-style-type: none"> • Capabilities are comparable • Basic events that can be reported are similar • The mechanisms that enable auditing are slightly different with W2K directory services bringing new auditing capabilities <p align="right">3-1</p>
 <p align="center">Why is Auditing Important?</p> <ul style="list-style-type: none"> • It is the LAW. • Helps you maintain a watchful eye, potentially alerting you to security issues before they become a problem. <p align="right">3-1</p>	

DISC4 Policy																									
Vulnerability	Countermeasure																								
<p>IAW MSG DTG 042100Z Mar 99 Fm ACERT Ft Belvoir VA. K. Enable auditing for the following events: ENSURE that the minimum required auditing is enabled per DISC4 policy.</p> <p>Enabling system auditing can inform</p>	<p><input type="checkbox"/> 1. Configure the following events:</p> <table border="0"> <thead> <tr> <th>EVENT</th> <th>SUCCESS</th> <th>FAILURE</th> </tr> </thead> <tbody> <tr> <td>Audit logon events</td> <td align="center">X</td> <td align="center">X</td> </tr> <tr> <td>Audit object access</td> <td align="center">-----</td> <td align="center">X</td> </tr> <tr> <td>Audit privilege use</td> <td align="center">X</td> <td align="center">X</td> </tr> <tr> <td>Audit account management</td> <td align="center">X</td> <td align="center">X</td> </tr> <tr> <td>Audit policy changes</td> <td align="center">X</td> <td align="center">X</td> </tr> <tr> <td>Audit system events</td> <td align="center">X</td> <td align="center">X</td> </tr> <tr> <td>Audit process tracking</td> <td align="center">-----</td> <td align="center">X</td> </tr> </tbody> </table>	EVENT	SUCCESS	FAILURE	Audit logon events	X	X	Audit object access	-----	X	Audit privilege use	X	X	Audit account management	X	X	Audit policy changes	X	X	Audit system events	X	X	Audit process tracking	-----	X
EVENT	SUCCESS	FAILURE																							
Audit logon events	X	X																							
Audit object access	-----	X																							
Audit privilege use	X	X																							
Audit account management	X	X																							
Audit policy changes	X	X																							
Audit system events	X	X																							
Audit process tracking	-----	X																							

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>you of actions that pose security risks and possibly detect security breaches.</p> <p>Note: that auditing is a "detection" capability rather than "prevention" capability. It will help you discover security breaches after they occur and therefore should always be considered in addition to various preventive measures.</p>	<p>Note: Setting up auditing is a two-part process:</p> <ol style="list-style-type: none"> 1. Set the audit policy. Enables the auditing of objects but does not activate auditing of specific objects 2. Enable auditing of specific resources.
<p>Hacker-type break-in using random passwords</p>	<p>Enable failure auditing for log on and log off events.</p>
<p>Break-in using stolen password</p>	<p>Enable success auditing for log on and log off events. The log entries will not distinguish between the real users and the phony ones. What you are looking for here is unusual activity on user accounts, such as logons at odd hours or on days when you would not expect any activity.</p>
<p>Misuse of administrative privileges by authorized users</p>	<p>Enable success auditing for use of user rights; for user and group management, for security policy changes; and for restart, shutdown, and system events. (Note: Because of the high volume of events that would be recorded, Windows 2000 does not normally audit the use of the Backup Files And Directories and the Restore Files And Directories rights. Appendix B, "Security In a SOFTWARE Development Environment," explains how to enable auditing of the use of these rights.)</p>
<p>Virus outbreak</p>	<p>Enable success and failure write access auditing for program files such as files with .exe and .dll extensions. Enable success and failure process tracking auditing. Run suspect programs and examine the security log for unexpected attempts to modify program files or creation of unexpected processes. Note: that these auditing settings generate a large number of event records during routine system use. You should use them only when you are actively monitoring the system log.</p>
<p>Improper access to sensitive files</p>	<p>Enable success and failure auditing for file- and object-access events, and then use File Manager to enable success and failure auditing of read and write access by suspect users or groups for sensitive files.</p>
<p>Improper access to</p>	<p>Enable success and failure auditing for file- and object-access</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

printers	events, and then use Print Manager to enable success and failure auditing of print access by suspect users or groups for the printers.
----------	--

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p style="text-align: center;">Don't Over Audit </p> <ul style="list-style-type: none"> • By default, none of Windows 2000 auditing features are turned on. • By enabling every possible aspect of auditing, you would end up with a server that does little else except auditing. <p style="text-align: right; font-size: small;">3-1</p>	<p style="text-align: center;">Three broad categories can be monitored </p> <ul style="list-style-type: none"> • Logon/logoff • Object Access <ul style="list-style-type: none"> – Files and Folders – Printers – Registry – Directory Access • Process Tracking • Investigate all failed login attempts or failed account lockouts <p style="text-align: right; font-size: small;">3-1</p>
--	--

<p style="text-align: center;">Set Up an Auditing Policy </p> <ul style="list-style-type: none"> • Events to Audit: <ul style="list-style-type: none"> – Account Login(logging in/out) – Account Management – Directory Service Access – Logon Events – Object Access – Policy Change – Privilege Use – Process Tracking – System Events <p style="text-align: right; font-size: small;">3-1</p>	Empty space for content
--	-------------------------

Setting up an Auditing Policy	
Vulnerability	Countermeasure
<p>Without proper auditing techniques, you'll never know if your security plan is working effectively.</p>	<p><input type="checkbox"/> 1. General Categories to consider when setting up a secure server auditing policy</p> <ul style="list-style-type: none"> • Account Logon Events • Account Management • Directory Service Access • Logon Events • Object Access • Audit Policy Changes • Use of Privileges • Process Tracking

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<ul style="list-style-type: none"> • System Events <p>Note: Guide for setting up an audit policy. http://networking.earthweb.com/netos/print/0,,12083_624921,00.htm</p>
--	---

Enabling Auditing	
Vulnerability	Countermeasure
Failure to enable success/failure auditing can cause hacking activities to go undetected.	<input type="checkbox"/> 1 To activate auditing on a standalone machine, follow these steps: <ul style="list-style-type: none"> • Log on as the administrator of the local workstation. • Click the Start button, point to Programs, point to Administrative Tools, and then click Local Security Policy. • In the Local Security Settings window's console tree, double-click Local Policies and then click Audit Policy. • Select the type of event to audit, and then, on the Action menu, click Security. • Select the Success check box, the Failure check box, or both. • Click OK. • Restart your computer. <p>Note: This setting only affects the standalone system. To set auditing on a domain controller use the countermeasure in 5.4</p>

Enabling Group Policy	
Vulnerability	Countermeasure
Failure to enable success/failure auditing can cause hacking activities to go undetected. Group policies may be set at the local, site, domain and organizational unit levels.	<input type="checkbox"/> 1. To enable which categories of events can be audited, you use the Group Policy Snap-in with the MMC. <ul style="list-style-type: none"> • Click Start, Run, and enter mmc. • Select Add/Remove Snap-in from the Console menu. • Click the add button. • Find the Group Policy Snap-in from the "add Standalone Snap-in dialog box" then click add • Accept the default (local computer) for where the Group Policy Object will be stored and click the finish button.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<h3 style="text-align: center;">Troubleshooting </h3> <ul style="list-style-type: none"> • Event Viewer displays detailed information about system events • Information includes the event type, date and time the event occurred, source, category, Event ID, user logged on, and computer involved. <p style="text-align: right;">3-1</p>	<h3 style="text-align: center;">Windows 2000 Event Logs </h3> <ul style="list-style-type: none"> • All W2K servers have at least three log files: <ul style="list-style-type: none"> – System Log – Application Log – Security Log • W2K may have an additional three log files: <ul style="list-style-type: none"> – Directory Service – DNS Server – File Replication Service <p style="text-align: right;">3-1</p>
--	--

Event Log Configuration	
Vulnerability	Countermeasure
<p>Improper configuration of the Event viewer/log files can degrade monitoring capabilities.</p>	<p><input type="checkbox"/> 1. Open the Computer Management Console</p> <ul style="list-style-type: none"> • Right-click the "my computer" icon on the desktop • Select manage from the drop down menu. • Expand System Tools • Expand event Viewer • Right-click the event log. Perform the following procedure for each event log. • Select properties from the pop up menu • Review the fields identifying the maximum log size and the event log overwriting. • If the server or workstation shares resources, click the radio button marked "do not overwrite events". If the workstation does not share resources, click the radio button marked "overwrite events older than 30 days". <p>For servers and workstations that share resources, enter "4194240 KB" for the maximum log size value. Workstations that do not share resources can be set to "10240 KB".</p>



Safeguard Your Log Files

- Review Audit trails at a min weekly. (not enough)
- Create an “**Audit Account**”
- Log all access and access attempts
- Store log files on a - machine separate from where the event took place
- Retain classified and sensitive IS audit files for 1 year and 5 years for SCI systems

3-1

W2K Auditing & Logging

Practical Exercise SAS-5A

Exercise A

Various steps are involved when you set up a secure server. One of the most important is arriving at an auditing policy that does not degrade performance and meets your security needs. By default, Windows 2000 has auditing turned off. In order to capture any auditing information, you must individually enable those items you wish to capture data about. Your auditing policy will guide you as you select those events to audit.

- 1. Login to the Windows 2000 Server as the **administrator**
 - 2. Click Start->Programs->Admintools->Security Config & Analysis.
 - 3. In the Security Configuration and Analysis console, right-click Security Configuration and Analysis.
 - 4. Click Open Database. In the Open Database dialog box, in the File Name box, type **new2** for the new personal database file name, then click Open.
 - 5. In the Import Template dialog box, select the "basicsv" security template to load into the security database, then click Open. The "new2" database is now the working security database, and it contains the "basicsv" security template.
 - 6. Right click security configuration and analysis
 - 7. Select "configure computer now".
 - 8. Accept the default error log location by clicking "ok". Close configuration and security analysis console.
 - 9. Select Start->Programs->Administrative Tools->Local Security Policy
 - 10. Expand Local Policies
 - 11. Select Audit Policy. Which policies are enabled by default?
-
-

You should see a column labeled local settings. In the case of inherited policies, you may see two columns, one for local settings and one for effective settings. The local settings pertain to settings established on the computer itself. The effective settings are the settings it inherits as a member of the domain. If the computer is not a member of a domain, the local settings will be the effective settings. If the computer is a member of a domain and the effective settings say no auditing and the local settings say success/failure, no auditing will occur.

- 12. Right click on **Audit Logon Events** and select **security**
- 13. Click on both **success** and **failure** and then click **ok**
- 14. Right Click on **Audit Object Access** and select **security**
- 15. Click on both **Success** and **failure** and then click **ok**
- 16. Right click on **Audit Privilege Use** and select **security**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- 17. Click on **failure** and then click **ok**
- 18. Right click on **Audit System Events** and select **security**
- 19. Click on **failure** and then click **ok**
- 20. Close Local Security Settings window and then reopen Local Security Policy. Have your changes become effective?

- 21. Select Start->Programs->Administrative Tools->Event Viewer
- 22. Right Click on the Security Log choice in the left panel
- 23. Choose properties
- 24. If you click on the filter tab you will see the various events the log looks for. You can keep the size of your log down by choosing to not filter for certain events. What events can you filter on?

- 25. Click on the General tab.
- 26. What is the default size setting? _____
- 27. Change the log file size setting to 100KB and click **Apply**. Were you successful? _____
- 28. What is the restriction when setting the log file size? When you attempted to set the log size to 100KB, what did the system choose as a setting?

- 29. Select OK and close all windows
- 30. Logoff as the administrator
- 31. Log on as labuserXX but do not provide a password (just hit enter)
- 32. Repeat the previous step, four more times
- 33. Logon as labuserXXa with the proper password
- 34. Click on Start and select programs
- 35. Select administrative tools

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- 36. Select Event Viewer
 - 37. View the Security Log. Were you successful? _____
 - 38. Close the Event viewer Window.
 - 39. Double click on the time display in the lower right portion of the screen. Will it allow you to change the time?

 - 40. Logout as labuserXXa
 - 41. Login as the administrator but do not provide a password (just hit enter)
 - 42 Repeat the previous step, four more times.
 - 43. Login as the administrator with the proper password
 - 44. Click Select Start->Programs->Administrative Tools->Event Viewer
 - 45. View the Security Log.
 - 46. Can you identify the entries that were generated as a result of the bad login attempts, successful login attempts, and failure of privilege use?
-
- 47. Right Click on a few of the failure and success audit event numbers event and view the properties. You should see a fairly understandable explanation of the event.
 - 48. Close the event viewer.
 - 49. Wait for the instructor to review the exercise.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Welcome to Unix Security.....

(Circle the correct answer)

1. **T** **F** By changing the name of the root account you stop hacker brute force attacks.
2. **T** **F** System accounts are logged into like normal accounts but are used as Administrator accounts.
3. **T** **F** Unix has no logging enabled by default.
4. **T** **F** Both the root administrator and regular users can establish trusts with other computers and users.
5. **T** **F** Unix by default, requires the use of uppercase, lowercase, symbols, and numbers in password construction.
6. **T** **F** Viruses cause a lot of problems for Unix administrators.
7. **T** **F** If a user ran the chown command, a user could assign someone else ownership of a file.
8. **T** **F** By enabling process accounting, you will log all the commands that are ran and whom they were ran by.
9. **T** **F** Unnecessary services are turned off in the /etc/services file.
10. **T** **F** The /etc/ftpusers file contains the list of accounts that can utilize ftp.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

UNIX Command Reference List

In this section . . .

Command words and arguments are shown exactly as you type them. Note that most are in lowercase. They must be typed that way: UNIX treats uppercase letters as different from their lowercase counterparts. Type the punctuation shown, such as a hyphen or vertical bar. Control characters, typed by holding down the CTRL key while typing the character, are shown by the notation ^x, where x is the character. You must finish all UNIX commands by pressing the RETURN key, which is not shown here. Most commands have an assortment of flags/options that are not shown. Use the man page to learn about program flags/options

Connecting

Connecting from Another Computer

If you are using another computer on the network or on the Internet, and if that computer has a telnet command, you can use it to connect to a UNIX host. If the other computer is also running UNIX, you can connect using rlogin. If your computer offers ssh, the Secure SHell, you can also connect using ssh or slogin.

Special Characters

^C

Interrupts and aborts execution of the current process, which cannot be restarted.

^Z

Suspends a process (temporarily stops it by putting it in the "background") so that you can give other UNIX commands. To resume the process, use fg (foreground) or %n, where n is the background job number. To disable ^z (make it undefined), give the command:

^D

Ends a telnet session

^]

Used to escape out of some commands or processes. Similar to ^C.

>

Writes to the file named to the right of this symbol instead of to standard output. Thus:

```
cat myfile
```

displays contents of "myfile" at your terminal (standard output), but:

```
cat myfile > listout
```

copies it to file "listout" instead, overwriting and destroying any previous contents of the file "listout".

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

>>

Appends output to the file named to the right of this symbol. Thus:

```
cat nextfile >> listout
```

appends a copy of "nextfile" to file "listout" instead of overwriting what is already in "listout".

|

Creates a "pipe" so that output from one program (on left) becomes input to the next one (on right). Thus:

```
ls | lpr
```

sends output from the ls (listing) program to the lpr (printing) program.

*

Matches zero or more characters in a filename. For example, A* matches A, AbC, ARGUE, African, etc.

?

Matches any single character in a filename. For example, A?C matches AAC, ABC, ACC, etc.

\

Prevents the following character from being interpreted as special. For example, \`*` makes `*` an ordinary character.

Getting Online Help

Online UNIX documentation consists of "man" (manual), pages that you can display or print by using the man program. For example, to display the man page for the rm (remove) program, type:

```
man rm
```

```
apropos keyword
```

to get a list of man pages that contain keyword in their title lines.

Files and Directories

A UNIX filename or directory name can contain up to 255 letters, digits, and punctuation characters (best limited to period and underscore). To list names of files in your own directory, type:

```
ls
```

This will not list filenames that begin with a period, unless you include the -a (all) option, like this:

```
ls -a
```

Other ls options include:

```
-l
```

long form, gives file protections, size in bytes.

```
-F
```

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

marks directory names with a slash, executable files with an asterisk.

-b Forces the printing of nonprintable characters to an octal format.

Deleting a File

Use rm (remove) to delete files from your directory. For example:

```
rm trashfile
```

The -i (interactive) option to rm causes the system to request confirmation of each file deletion. This option may prevent accidental deletions and is useful if you are removing several files, as in:

```
rm -i *file
```

Summary of Useful Commands

The following commands are grouped alphabetically by function. Unless noted otherwise, each has a man page describing it in full. Commands marked "C shell only" are described in the csh man.

Access Control

admintool - create, assign, modify groups, users, printers, etc.
exit - terminate a shell (see "man sh" or "man csh")
getfacl - read file access control lists
id - identify the UID, GID, EUID, EGID
logout - sign off; end session (C shell and bash shell only; no man page)
passwd - change login password
rlogin - log in remotely to another UNIX system
setfacl - set file access control list
slogin - secure version of rlogin
su - switch user/super user
usermod - modify user account information

Communications

Mail - send and receive mail
wall - send message to all users
talk - talk to another logged-in user (full screen)
write - write to another logged-in user

Programming Tools

awk - pattern scanning and processing language
cc - C compiler (xlc on ADS)
crontab - maintain periodic tasks
csh - C shell command interpreter
kill - kill a process
make - manage multipart program projects
nice - run a command at low priority (see "man nice" or "man csh")
nohup - run a command immune to hangups
sh - Bourne shell command interpreter

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Documentation

apropos - locate commands by keyword lookup
man - find manual information about commands
whatis - describe what a command is
whereis - locate source, binary, or man page for a program

Editors

emacs - screen-oriented text editor
ex - line-oriented text editor
sed - stream-oriented text editor
vi - full-screen text editor
dtpad - text editor within CDE
textedit -text editor within open windows

File and Directory Management

cd - change working directory
chgrp - change group owner
chmod -change the protection of a file or directory
chown - change owner
cmp - compare two files
compress - compress a file
cp - copy files
crypt - encrypt/decrypt files (not on ADS)
cut - display specific file information
diff - compare the contents of two ASCII files (sdiff for side by side)
find - look for files by name
grep - search a file for a pattern
ln - make a link to a file
ls - list the contents of a directory
mkdir - create a directory
mv - move or rename files and directories
pwd - show the full pathname of your working directory
rm - delete (remove) files
rmdir - delete (remove) directories
sort - sort or merge files
touch - create file
umask - change default file protections
uncompress - restore compressed file
wc - count lines, words, and characters in a file

File Display and Printing

cat - show the contents of a file; catenate files
lpr - print a file
lprm - remove jobs from the printer spooling queue
more - display a file, one screen at a time
page - like "more", but prints screens top to bottom
tail - show the last part of a file
zcat - display a compressed file

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

File Transfer

ftp - transfer files between network hosts
rcp - transfer files between networked UNIX hosts
scp - secure version of rcp

Miscellaneous

alias - define synonym commands
chsh - change default login shell
clear - clear terminal screen
echo - echo arguments
setenv - set an environment variable (C shell only)
stty - set terminal options

Networks

netstat - show network status (on UTS, /usr/sbin/netstat)
rlogin - login remotely on another UNIX system
slogin - secure version of rlogin
rsh - run shell or command on another UNIX system
ssh - secure-shell version of rsh
telnet - run Telnet to log in to remote host

Process Control

(The following commands function under the C shell, bash, and ksh. They do not have separate man pages.)

bg - put suspended process into background
fg - bring process into foreground
jobs - list processes
^y - suspend process at next input request
^z - suspend current process

Status Information

acctcom - read processing accounting data
date - show date and time
df - summarize free disk space
dmesg - read message log
du - summarize disk space used
env - display current environment or run programs under modified environment
finger - look up user information
history - list previously issued commands (C shell, bash, and ksh only)
last - indicate last login of users
lastcomm - read processing accounting data
lpq - examine spool queue
ps - show process status
pwd - display full pathname of working directory
set - set shell variables (C shell, bash, and ksh only)
stty - set terminal options
w - show who is on system, what command each job is executing
who - show who is logged onto the system
whois - Internet user name directory service

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Machine and Site Preparation

Written Security Policy	
Vulnerability	Countermeasure
Only by doing proper analysis and security planning, can you hope to provide a secure environment for your data. Security without a security policy is synonymous with a long journey without a road map	<input type="checkbox"/> 1. Asset identification and evaluation <input type="checkbox"/> 2. Threat identification and assessment <input type="checkbox"/> 3. Vulnerability and exposures identification and assessment <input type="checkbox"/> 4. Determine access and control requirements <input type="checkbox"/> 5. Qualitative and quantitative risk assessment <input type="checkbox"/> 6. Develop your plan and policies to maintain number 1 while defending against numbers 2,3, 4 and 5.

Server Access	
Vulnerability	Countermeasure
Physical access by unauthorized personnel could result in theft of peripherals, denial of service, security overrides via removable media, or miscellaneous tampering. Remember that there is NO security without Physical Security. Access to the interior of the CPU case exposes the computer to theft, sabotage, and reconfiguration.	<input type="checkbox"/> 1. Place the server in a locked room accessible only by the System Administrator. <ul style="list-style-type: none"> • Maintain a list of personnel authorized entry • Establish key/access control. <input type="checkbox"/> 2. PHYSICALLY lock the CPU case

Access Control	
Vulnerability	Countermeasure
Access control has several primary objectives. They are: Identification, Authentication, Authorization, Confidentiality, Integrity, Availability, and Accountability	<input type="checkbox"/> 1. Before a user gains access to an access control object, the user must go through three levels of access control. <ul style="list-style-type: none"> • The user must be identified • The user must be authenticated based on the identification supplied • Once identified and authenticated, the user must be authorized for access to the object under control.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Authentication Methods	
Vulnerability	Countermeasure
Authentication is the transfer of some information that proves you are who you say you are. Failure to properly identify users results in a breakdown of authorization and access control	<input type="checkbox"/> 1. There are 3 types of authentication <ul style="list-style-type: none"> • Something you know (password) • Something you have (token, smart cards, Id badges) • Something you are (biometrics)

Contingency Planning	
Vulnerability	Countermeasure
If Information Technology operations are disrupted, mission critical functions could be lost.	<input type="checkbox"/> 1. Minimize the impact of fire, flood, civil disorder, natural disaster, or bomb threat. <input type="checkbox"/> 2. Identify an alternate site containing compatible equipment. <input type="checkbox"/> 3. Identify backup procedures if the primary IT operation site is disrupted. <input type="checkbox"/> 4. Destruction or safe guarding plan in case of site evacuation. (classified sites) <input type="checkbox"/> 5. Plan the test - test the plan.

Installation and Configuration

Securing a Unix server starts with the installation.	
Vulnerability	Countermeasure
Security should be involved in every phase of installation and system use.	<input type="checkbox"/> 1. Some things that should be part of a secure installation process <ul style="list-style-type: none"> • Do not be connected to the network. • Install the OS w/Patches • Secure the inetd • Secure the startup scripts • Enable logging • Protect against <ul style="list-style-type: none"> –buffer overflows, root network access, system account access, sendmail, motd misuse, permissions, trusts • Install ssh (secure remote communication method) <p>NOTE: A minimum install will increase security by not loading various applications.</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Into to UNIX System Security

Practical Exercise SAS-6A

EXERCISE A

This Practical exercise is designed to get you familiar with Unix, Unix files and the system in general. In the following steps, you will learn about, view and examine files for structure and key security entries. The commands you type will be printed in bold text. Do not type those that are bold and underlined. Type the commands as you see them. The "^" symbol shows you when to hit the space bar.

1. It is time to login into your computer. You should see a box with a warning banner greeting you. This is where you will type your Log On ID. Your Log On ID is: **root**
2. Upon submitting you Log On ID, you will need to supply a password. Your Log On Password is: **student**
3. The system should boot up in the common desk top environment (CDE). It has a background that is purple in color and has the word Solaris tiled all over it. There may be boxes popping up in the desktop window. Go ahead and close them by right clicking in the title bar and selecting close.
4. After you have closed all the boxes, right click anywhere in the background, a popup menu will appear. Select **Tools**. A new popup menu will appear, select **Terminal**. A shell window will popup. This is where we will be doing the majority of our work.
5. You may have to shut down the system either at the end of the day or for some other reason. To shut down you must be root on the system.
 - DO NOT** Press the reset button
 - DO NOT** Press the power button
 - DO NOT** pull the power cord**Improper shutdown will result in the loss of data or the requirement to run a file system check (fsck -y)**
 - shut down by entering the proper command at a shell prompt
init 0, shutdown, (sync, sync, halt), halt
 - reboot the system by entering the command at the shell prompt
init 6(soft boot), reboot

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

6. So what constitutes a Unix system. This simple definition will suffice:

A set of enabling technologies first developed at AT&T that have been incorporated into several legally distinct but closely related operating systems, each of which can be considered to be a Unix system. If it looks like Unix, operates like Unix, runs common Unix utilities and programs, and is developed with Unix as a model, its Unix.

7. On any Unix system, there are 3 types of Users:

Root

- Has complete control over the complete system.
- Can access all files
- The only one that can execute certain commands
- Has the **UID of 0**

Normal users

- Any user that can login
- Have a home directory that they can create and manipulate files in.
- Can not perform many system level functions
- Usually a human being

System users

- System users don't login
- Accounts that are used for specific system purposes.
- The nobody account is an example (nobody handles http requests).
- System accounts are created during install and without passwords

8. Unix has various run levels that you can choose between. Each run level (0 through 6 to include S/s) is tied to a directory filled with scripts. The run levels 2 through 5 may vary between Unix and Linux distributions.

- 0** - Used to terminate the operating system.
Safe to power down the system.
- 1** - Single user, admin/maintenance level.
- 2** - Multi-user, no NFS services
- 3** - Multi-user including NFS (default)
- 4** - Not used by most flavors.
- 5** - Safe for automatic power down if supported.
- 6** - Used to shut the system down and reboot to
the default level (soft boot).
- S or s** - Single user mode with all file systems mounted.

- The command “**who -r**” will show you the run level
- To invoke the run level, type “**init #**”

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

9. Check your default run level.

a. run the "who -r" command to find your default run level. # **who_r**

When you boot into a run level, you are actually running the scripts in that run level. Let's go look at an example:

b. Change to the directory for run level two. # **cd _etc/rc2.d**

c. Run the "ls" command to see the directory contents. # **ls_al**

d. Notice the contents of the directory. Some scripts start with a capital "K" and others start with a capital "S". Those scripts starting with a "K" run first and will kill processes. Those with an "S" are starting up a service or process. These are known as your "start up" scripts. To stop a script from running, rename the script. Example: S72inetsvc could be renamed to _S72inetsvc. This would effectively turn off this script.

e. Run the "cd" command to go back to your home directory. # **cd**

Startup (S) and Shutdown (K) scripts	
Vulnerability	Countermeasure
<p>Attackers, if they gain access to your system, will more than likely add scripts or modify existing scripts. Understanding what scripts should be in the /etc/rc* directories is crucial.</p>	<p><input type="checkbox"/>1. ALL startup/shutdown scripts should be readable and executable only by root (500).</p> <p><input type="checkbox"/>2. ENSURE that the line "rm -f /tmp/t1" (or similar) exists in a startup script to clean up the temporary file used to create /etc/motd. This should occur BEFORE the code to startup the local daemons.</p> <p><input type="checkbox"/>3. EXAMINE all "S" files in /etc/rc2.d and /etc/rc3.d (or similar directories). Any files that start unneeded facilities should be renamed (be sure the new names DO NOT start with a capital "S").</p> <p><input type="checkbox"/>4. TEST all boot files changes by rebooting, examining /var/adm/messages, and checking for extraneous processes.</p> <pre style="margin-left: 40px;">#mv /etc/rc2.d/Sfilename /etc/rc2.d/.NOSfilename #cat /var/adm/messages #ps -elf</pre>

10. Let's find out where our default run level is set up.

a. View the /etc/inittab file. # **cat_etc/inittab**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- b. Find the line that reads "is:3:initdefault". The 3 refers to the default run level. It should match what you saw when you ran the "who -r" command. Changing this setting would change the default run level.
11. Let's look at the file that contains our user information.
- a. View the /etc/passwd file. # **cat /etc/passwd**
 - b. The structure is "login-id; password; user-id#; group-id; user info; home directory; shell"
 - c. The "x" in the password column reflects that each password is stored in the shadow file.
 - d. The "0" user-id reflects the root user. Any account with the user-id of zero will be treated as root. There should only be one root account.
 - e. The last thing on the line is the shell. If one is not listed, a default shell will be assigned. The bourne shell (/bin/sh) is assigned in Solaris in such instances. Accounts may be disabled by assigning a false shell to them. **Every account must have an authorized valid shell assigned to them in order to operate on the system.**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Examples of some shells:

<u>VALID SHELLS</u>	(file name)	(prompt)
Bourne Shell (1)	/bin/sh	\$
Korn Shell (4)	/bin/ksh	\$
Bourne Again Shell (5)	/bin/bash	\$
C Shell (2)	/bin/csh	%
Tenet C Shell (3)	/bin/tcsh	>
	any shell	# (you are ROOT)

FALSE SHELLS (disable login)

/bin/false /dev/null

RESTRICTED SHELLS

restricted Bourne shell /usr/bin/rsh
restricted Korn shell /usr/lib/rksh

f. There are also shells designed for remote connections. and secure connections. These type of shells are not assigned to a user but act as utilities to gain network access. Examples are remote shell or secure shell.

g. Shells can be valid and still not authorized for login. Root can create a /etc/shells file and can list in it, the shells authorized for login. If a /etc/shells file exists, all shells not listed in it, will function similar to a false shell in regards to login.

Shells	
Vulnerability	Countermeasure
<p>Shells are almost always in a binary directory. Ensure that you list <u>only</u> the absolute pathnames to the shells. Shells may be in /bin, /usr/bin, /sbin, etc. Because the entire /etc/shells file is read by Unix, DO NOT use pathnames to non-shell scripts, nor should you use any extraneous characters as these will be interpreted as 'non-shells' by Unix and your users will not be able to log in.</p>	<p><input type="checkbox"/>1. ENSURE that ALL authorized shells are listed in the /etc/shells file, i.e. /bin/sh, /bin/ksh, /bin/csh, /bin/bash, /sbin/sh, /bin/tcsh, /bin/zsh, etc.</p> <p style="text-align: center;">#cat /etc/shells</p> <p><input type="checkbox"/>2. ENSURE that each username entry in the /etc/passwd file invokes an authorized shell listed in the /etc/shells file.</p> <p>NOTE: /dev/null, /bin/false, or /bin/true will be used to replace shells, but WILL NOT be listed in the /etc/shells file because they are used to <u>disable</u> account login. If you place them in the /etc/shells file, ftp access is enabled for the accounts with a false shell.</p> <p><input type="checkbox"/>3. EACH authorized shell listed in the /etc/shells file WILL NOT have the SUID and/or SGID bits set, WILL be owned by root, and WILL have access permissions of 555.</p> <p style="text-align: center;">#chmod u-s shell (i.e. /bin/sh) #chmod g-s shell (i.e. /bin/csh) #chmod 555 shell (i.e. /bin/ksh) #chown root shell (i.e. /bin/bash)</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Accounts listed in the /etc/passwd file which do not have an assigned shell, receive one by default from the system, normally the bourne shell (/bin/sh).	
---	--

12. Let's look at the file that contains our password information.

- a. View the /etc/shadow file. # **cat /etc/shadow**
- b. The format is "login-id; password; lastchange; minimum time before changing; maximum time its good; warning; inactive date; expire date; optional flags"
- c. Your login-id's should match your /etc/passwd file entries. These two files contain a list of all your accounts by login-id.
- d. The system accounts have passwords of "NP" (no password) or "*LK*" (locked).
- e. Let's lock an account. # **passwd -l nobody**
- f. View the /etc/shadow again. # **cat /etc/shadow**
- g. See where the "nobody" account now says that it is locked.
- h. To unlock an account, run the command in the same format without the "-l" switch. **Do not unlock** the nobody account. When you unlock an account, you will have to provide a password for the account unlocked.

13. Lets look at the file that lists your groups and group membership. Only members of multiple groups are listed in this file. If you belong to only one group, the /etc/passwd file will show that group. Never add members to the wheel group natively (don't make that their primary group in /etc/passwd). Staff members should be in staff group. Only add to the wheel group in the /etc/group file.

- a. View the /etc/group file. # **cat /etc/group**
- b. The format is "group name; password; group id; user list separated by commas"
- c. The /etc/passwd, /etc/shadow, and /etc/group files represent your authentication files.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

14. Now let us view the file that establishes some of our more important security settings.

a. View the `/etc/default/login`. # **cat `/etc/default/login`**

b. Find the line that says `CONSOLE=/dev/console`. This entry controls root logon. This setting will allow root login at the server but not over the network. It is called "securing the terminal". Always assume that the root password is compromised. That is why we restrict access to only local. In Linux, make sure all the ptys in the `/etc/ttys` file are set to unsecure. This stops the rlogin/telnet connections.

c. Find the line that says `PASSREQ=yes`. This entry ensures that your users will be authenticated via passwords.

d. Find the line that says `SYSLOG=yes`. This entry ensures that root logons are recorded.

e. Find the entry `#UMASK 022`. This entry is one of the places that your system umask may be assigned. The pound sign in the front indicates that it is commented out and that the computer will ignore any code on this line. Normally this indicates that the system umask is set in the `/etc/profile`.

f. Find the entry that says `#RETRIES=5`. This entry is commented out so that you know it does not get read by the computer. Army policy is you get 3 bad tries to logon before your account gets locked. This would need to be changed to 3 and the comment (#) mark removed. This would then reset the telnet session after every 3rd bad login.

g. Find the entry for `SYSLOG_FAILED_LOGINS`. This variable determines how many failed login attempts are recorded before a failed login message is logged. The default is 5. A setting of "0" would log all failed attempts.

15. Let's view the `/etc/profile` file. # **cat `/etc/profile`**

a. If you check towards the bottom of the file, you should see that there is an entry for umask. Solaris 8 has it set to 022. This value will be shared by all who log on the system unless they set their own unique umask in their `~/.profile`, `~/.login`, or `~/.cshrc` file.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

16. Let's look at the file that allows us to set up a password policy within Unix.

a. View the `/etc/default/passwd` file. # **cat /etc/default/passwd**

b. Notice that it only has three options, two of which are not even assigned. The `PASSLENGTH` refers to the character length of the password. The Army standard calls for 10. You would have to adjust this with a text editor. The `MAXWEEKS` refers how long the password is good before it expires; 150 days/21 weeks for systems. The `MINWEEKS` establishes the earliest time when you would be able to change your password, 90 days/13 weeks for systems.

c. This file does not control password content nor address security measures found in Windows systems. You must turn to 3rd party tools for those needs.

17. At the heart of the operating system lies the kernel. It is the compiled code that controls how the system manages system memory, the file system, disk operations, and processes. The kernel stays resident in memory at all times. Many of the things that the kernel controls, are directly targeted in denial of service attacks. As the kernel is compiled, changing how the kernel operates can only be accomplished by recompiling the kernel with new instructions or by placing entries in the `/etc/system` file. The `/etc/system` file is the one file that directly communicates to the kernel and allows you to alter settings that were precompiled. It operates similar to the Windows registry.

a. View the `/etc/system` file. # **cat /etc/system**

b. You will notice that there are some commented out instructions in the file. A default installation will normally not contain entries. Examples of items you could alter: maximum number of user processes; maximum number of users; number of groups per user; file descriptor limits; maximum number of queued commands, buffer overflows, and many others.

c. Example entries are:

1. `set nfssrv:nfs_portmon 1` (this would allow only nfs requests via ports 1 - 1024)

2. `Set rstchown=0` (this would allow all users to change ownership on files)

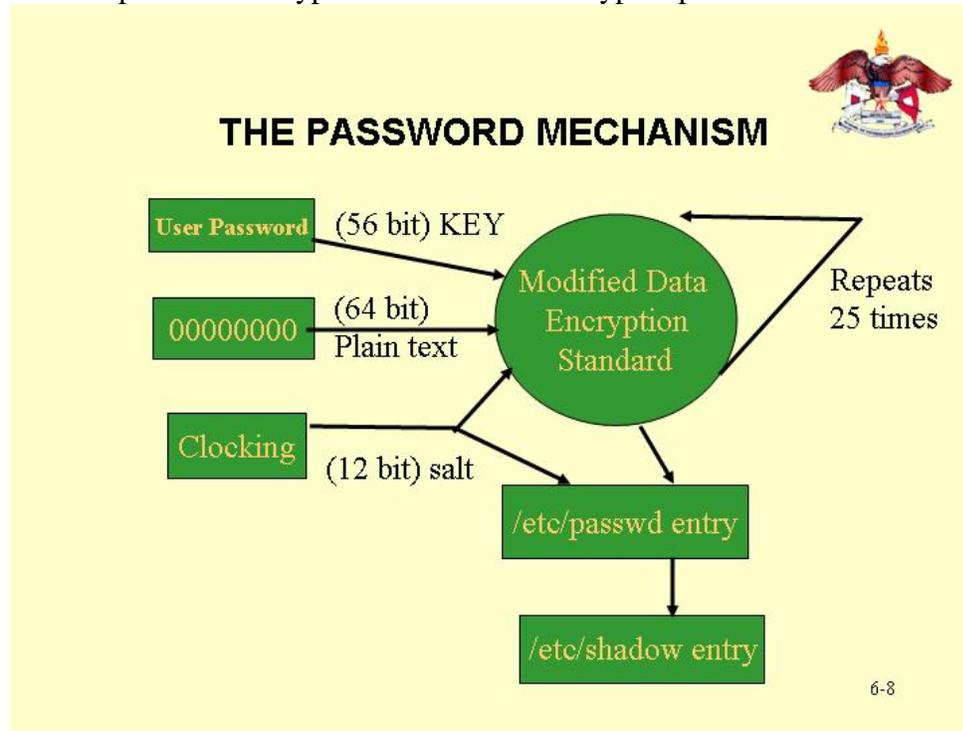
18. You sit down at your computer. You enter in your user name, and then you enter your password. Magically, you are taken into your account. What is actually happening behind the scenes? How does your computer store passwords, and how does it keep them secure?

To begin with, a basic understanding of cryptography is necessary. There are three fundamental techniques of encryption: symmetric key- based algorithms, such as block ciphers and stream ciphers; asymmetric key-based algorithms, such as public key encryption; and hash ciphers, such as SHA and MD5. These are the primary methods of cryptography systems, and most encryption schemes are based around one or a combination of these.

Unix passwords are stored using hash ciphers, one-way hash systems. The encryption is fairly simple, a fact that has its merits and its disadvantages. On the one hand, the relative simplicity

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

means the encryption is performed quickly, so logging in happens immediately. On the other, the simplicity means passwords are easy to crack. One advantage is that your password is not stored on your computer anywhere. A hash, an encrypted string of characters is stored in the password file (/etc/passwd, by default). That hash was formed the first time you typed in your password; when you originally set the password, the system encrypted it using a set mathematical formula, the hash function. The system knows how it hashed the sequence of characters that is your password, so every time you log on, the system encrypts what you have just typed using the same hash function, and compares the encrypted results to the encrypted password.



But the password file is easy to crack...that's a pretty big downside. Surely there's got to be a way to protect our passwords. Well, in the classic configuration of Unix systems, there isn't. The password file, /etc/passwd, is world readable. It has to be, because of the other crucial information that's stored in /etc/passwd. Since it's world readable, anyone who's got read access to your computer can view your password file and run cracking programs against it. Obviously, this is a problem. To enhance security, the shadow password system was developed. When using shadow passwords, the computer stores non-sensitive information in /etc/passwd, which is world readable, and stores the hashed passwords in /etc/shadow, which is -not- world readable. This way, not everyone can read the file; only those with root access can read the shadow file, and if you've already got root, then there's often little need for the password file. FreeBSD uses encrypted passwords. Check the /etc/master.passwd file and see that the longer passwords are encrypted with MD5 and the shorter, DES. MD5 passwords start with \$1\$. DES is encrypted in a 64 character alphabet which does not include the \$ character.

NIS, NIS+ and /etc/passwd entries (Distributed Authentication)	
Vulnerability	Countermeasure
Improper setup of NIS and/or NIS+ have been the cause of several	<input type="checkbox"/> 1. DO NOT run NIS or NIS+ if you don't really need it. <ul style="list-style-type: none"> • If NIS functionality is required, DO use NIS+ if possible. Ensure that NIS+ cannot talk to NIS by setting NIS+ to 2.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>exploits against Unix systems. Users could have access to the /etc/passwd and the /etc/shadow files. If you do not need to have a distributed database of all objects in your network, then do not use NIS/NIS+.</p>	<p style="text-align: center;">#grep passwd /etc/nsswitch.conf</p> <p>If response is passwd: files, you do not use NIS or NIS+.</p> <ul style="list-style-type: none"> • ENSURE that the only machines that have a '+' entry in the /etc/passwd files are NIS (YP) clients; i.e., NOT the NIS master server! There appears to be conflicting documentation and implementations regarding the '+' entry format and so a generic solution is not available here. It would be best to consult your vendor's documentation. Some of the available documentation suggests placing a '*' in the password field, which is NOT consistent across all implementations of NIS. We recommend testing your systems on a case-by-case basis to see if they correctly implement the '*' in the password field. <p>Ensure that * in the password field is correctly implemented</p> <ol style="list-style-type: none"> 1. Try using NIS with the '*' in the password field for example: +:*:0:0::: If NIS users cannot log in to that machine, remove the '*' and try the next test. 2. With the '*' removed, try logging in again. If NIS users can log in AND you can also log in unauthenticated as the user '+', then your implementation is vulnerable. Contact the vendor for more information. If NIS users can log in AND you cannot log in as the user '+', your implementation should not be vulnerable to this problem. <ul style="list-style-type: none"> • ENSURE that /etc/rc.local or the equivalent startup procedure is set up to start ybind with the -s option. This may not be applicable on all systems. Check your documentation. • /etc/rc.local is only used by NIS/NIS+ • CONSIDER using Secure RPC (used by default with NIS+) <p>NOTE: Secure RPCs are discussed on pages 570-578</p> <ul style="list-style-type: none"> • If you are using NIS (YP) or NIS+, DEFINE each netgroup (Pgs 581-586, 750) to contain only usernames or only hostnames. All utilities parse /etc/netgroup for either hosts or usernames, but never both. Using separate netgroups makes it easier to remember the function of each netgroup. The added time required to administer these extra netgroups is a small cost in ensuring that strange permission combinations have not left your machine in an insecure state. <p>Refer to the manual pages for more information</p>
---	--

Guest Accounts	
Vulnerability	Countermeasure
Guest accounts allow	□1. IAW HQ DA SAIS-IAS message DTG R 050951Z

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>an unauthorized user to access the system. This user will not have been verified against login criteria. The identity of this user will be unknown.</p>	<p>MAR 99, all guest accounts shall be disabled.</p> <ul style="list-style-type: none">• VERIFY that NO guest accounts exist in /etc/passwd or /etc/shadow. NOTE: Most systems come preconfigured with guest accounts• If you cannot remove the account, disable login to the account by assigning /bin/false or /dev/null as the shell.• USE special groups (such as the wheel group under SunOS) to restrict which users can use su to become root. Some versions of Unix use the group /etc/su.people which contains a list of users that may su. On Solaris, you must know the su password or utilize the sudo utility.• DISABLE login to accounts that have no password which execute a command, for example sync. SET the account's shell to /bin/false or /dev/null <p>DELETE or change ownership of any files owned by system accounts, i.e. bin, sys, sync, daemon, etc.</p> <p>ENSURE that these accounts do not have any cron or at jobs. It is best to remove these accounts entirely.</p> <ul style="list-style-type: none">• ALWAYS assign non-functional shells (such as /bin/false or /dev/null) to system accounts such as bin, daemon, lib, uucp, news, sys, sync, etc. if they are not needed. This will disable login to them. #more /etc/passwd Most system accounts have no shell associated with them. For example: #usermod -s /bin/false bin
--	--

19. Let's examine permissions and other key file information. The best way to do that is with the "ls" command and various flags. (-a) all files; (-l) long listing; (-b) nonprinting characters; (-R) recursive; (-u) access time

a. View the contents of the "/" directory. # **ls -alb**

b. The format is: file type (-,d,c,b,l,s,p), owner's permission (r,w,x/s/S), Group's permission (r,w,x/s/S/l), other's permission (r,w,x/t/T), access control list if any (+), links to the file, owner, group owner, file size in bytes, date saved or modified, file name, and file linked to with file type "l" Example: "file type" "owner permission" "group permission" "other permission" "ACL"

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- c. The file types are: (-) regular files/type f; (d) directories; (c) character devices; (b) block devices; (l) links; (s) sockets; (p) buffers.
- d. The permissions are: (r) read; (w) write; (x) execute; (s) set UID/set GID; (t) sticky bit
- e. Read permission on a file gives you permission to copy or view. Read permission on a directory allows you to view directory contents. `r--r--r--` . Read has a binary value of 4.
- f. Write permission on a file lets you edit the file contents and write permission on a directory allows you to delete files. **Write permission for the other's category is the most dangerous permission to allow.** Write permission for others is most often targeted by umask settings.
`-w--w--w-` . Write has a binary value of 2
- g. Execute permission allows you to execute a program or access files within a directory.
`--x--x--x` . Execute has a binary value of 1
- h. Set UID permission allows the executer of a program to run it as if they owned it by assigning them an effective UID of the owner. `--s-----` (uppercase "S" in case of no underlying "x"). The SUID bit has a binary value of 4.
- i. Set GID permission allows the executer of a program to run it as if they belonged to the group that owns it by assigning them an effective GID of the owning group. `-----s---` (uppercase "S" (or an "l") in case of no underlying "x"). If the system supports mandatory file locking, an l (lowercase L) may appear if the SGID is set and the group executable is removed. This will lock the file and prevent execution by both the group and others categories. The SGID bit has a binary value of 2.
- j. Sticky bit permission, set on directories, allows deletion of files if your UID matches the file owner UID, directory owner UID, or root UID. `-----t` (uppercase "T" in case of no underlying "x"). The sticky bit has a binary value of 1.

20. Permissions are changed via the command "chmod". Permissions are known as the file's mode and chmod stands for "change mode". Only a file's owner may change file permissions. Either numbers or alpha/character entries are acceptable when assigning permissions. Examples of each:

alpha/character syntax:	numeric syntax:
<code>chmod [-Rfh] [agou] [+ =] [rwxXstugol] file list</code> separate multiple permission settings by a comma: ● <code>chmod u+rw,go+r "file"</code> a = all r = read g = group w = write u = owner x = execute o = other - = remove + = add = = replace s = suid/sgid	(example) <code>chmod 0644</code> or <code>chmod 644</code> 1000 = sticky bit 2000 = SGID 3000 = SGID/sticky bit 4000 = SUID 5000 = SUID/stickybit 6000 = SUID/SGID 7000 = SUID/SGID/sticky bit 0777 = rwxrwxrwx

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

t = sticky bit	0666 = rw-rw-rw- 4555 = r-sr-xr-x 1777 = rwxrwxrwt 6745 = rwsr-Sr-x or rwsr-lr-x
----------------	---

Consolidated Octal values	7	7	7	7
Individual Octal values	4 2 1	4 2 1	4 2 1	4 2 1
Symbol values	s s t	r w x	r w x	r w x
Some of the values share space on the screen		s	s	t
		r w x	r w x	r w x
If all values are set, you would see		r w s	r w s	r w t

21. Lets examine a file that is both a Set UID and a Set GID file.

a. View permissions for the /etc/passwd file. # **ls -l /etc/passwd**

b. Notice that the owner of the file is root and the group is sys. Neither owner, group, or other has anything but read authority. This means that only root may edit this file as root has explicit write capability on files. This also means in order to change your password, you must involve root.

c. View the permissions of the program you run to change your password. # **ls -l /bin/passwd**

d. You will notice that permissions are -r-sr-sr-x. Both the Set UID and Set GID are turned on. It is owned by root and sys. This means everyone can run this program (other executable) and they will be assigned the effective GID of sys and the effective UID of root. While the /bin/passwd program is running, the system will see the person that ran it has having both root and sys authority. This is what allows you to change your password even though you lack the access.

22. Umask stands for "user file-creation mode mask". More simply put, you create a file and it gets a default permission that can be masked out. The default permission for a file is 666 (rw-rw-rw-) and a directory 777 (rwxrwxrwx). These permissions do not meet our "least access" requirements. The others and group categories may be receiving permissions that are above normal requirements. An umask setting would address this problem.

Examples of how umask works:

<u>Permission</u>	<u>Mode Setting</u>	<u>Umask</u>	System default for text file(Solaris)
•No Access	Setting 0		666 r w - r w - r
	7		w -
•Execute Access	1		umask

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">•Write Access</td> <td style="width: 10%; text-align: center;">6</td> <td style="width: 10%; text-align: center;">2</td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> </tr> <tr> <td></td> <td style="text-align: center;">5</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>•Read Access</td> <td style="text-align: center;">4</td> <td style="text-align: center;">3</td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;">3</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>•Full Control</td> <td style="text-align: center;">7</td> <td style="text-align: center;">0</td> <td></td> <td></td> <td></td> </tr> </table>	•Write Access	6	2					5					•Read Access	4	3					3					•Full Control	7	0				<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">022</td> <td style="width: 10%; text-align: center;">-</td> </tr> <tr> <td>w -</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>End result</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>644</td> <td style="text-align: center;">r</td> <td style="text-align: center;">w</td> <td style="text-align: center;">-</td> <td style="text-align: center;">r</td> <td style="text-align: center;">-</td> </tr> <tr> <td></td> <td style="text-align: center;">-</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	022	-	-	-	-	-	w -						End result						644	r	w	-	r	-		-				
•Write Access	6	2																																																											
	5																																																												
•Read Access	4	3																																																											
	3																																																												
•Full Control	7	0																																																											
022	-	-	-	-	-																																																								
w -																																																													
End result																																																													
644	r	w	-	r	-																																																								
	-																																																												
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Permissions</td> <td style="width: 10%; text-align: center;">7</td> <td style="width: 10%; text-align: center;">7</td> <td style="width: 10%; text-align: center;">7</td> <td style="width: 10%;">Permissions</td> <td style="width: 10%; text-align: center;">7</td> <td style="width: 10%; text-align: center;">7</td> <td style="width: 10%; text-align: center;">7</td> </tr> <tr> <td>(-)Umask</td> <td style="text-align: center;">0</td> <td style="text-align: center;">3</td> <td style="text-align: center;">3</td> <td>(-)End Permissions</td> <td style="text-align: center;">7</td> <td style="text-align: center;">5</td> <td style="text-align: center;">5</td> </tr> <tr> <td>End permissions</td> <td style="text-align: center;">7</td> <td style="text-align: center;">4</td> <td style="text-align: center;">4</td> <td>Umask</td> <td style="text-align: center;">0</td> <td style="text-align: center;">2</td> <td style="text-align: center;">2</td> </tr> </table>	Permissions	7	7	7	Permissions	7	7	7	(-)Umask	0	3	3	(-)End Permissions	7	5	5	End permissions	7	4	4	Umask	0	2	2																																					
Permissions	7	7	7	Permissions	7	7	7																																																						
(-)Umask	0	3	3	(-)End Permissions	7	5	5																																																						
End permissions	7	4	4	Umask	0	2	2																																																						

23. Below are some file permissions. Remember that the first character from the left identifies the file type, the next 3 the owner's privileges, the next three the group's privileges, and the last three the other's privileges. (r = 4, w = 2, x = 1) (--s----- = 4***) (-----s--- = 2***) (-----t = 1***) Place the correct "octal" number next to each permission listed. Output can be 3 or 4 digits. Ignore the file type. (Example: -rw-rw-rw- = 666)

- | | |
|--|--|
| a. dr--r--r-- <u>444</u> | b. br--r--r-- _____ |
| c. -rwxr-xr-x _____ | d. lrwxrwxrwx _____ |
| e. -r-xr-xr-x _____ | f. cr----- _____ |
| g. -r-sr-x--x <u>4551</u> | h. drwx---r-x _____ |
| i. brwxrwxrwx _____ | j. srwxrwxrwx _____ |
| k. ---S--l--x _____ | l. dr---S--T _____ |
| m. crw-rw-rw- _____ | n. -r-sr-sr-x _____ |

24. Solve for the umask results. (Example: 666 (text file) 027 (umask) = 640)

<u>File default</u>	<u>umask value</u>	<u>results (octal)</u>
a. 666	002	<u>664</u>
b. 666	046	_____
c. 777	046	_____

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- | | | |
|--------|-----|-------|
| d. 777 | 011 | _____ |
| e. 666 | 011 | _____ |
| f. 666 | 033 | _____ |
| g. 777 | 077 | _____ |
| h. 666 | 055 | _____ |
| i. 777 | 055 | _____ |
| j. 666 | 013 | _____ |

25. Write out the following permission values. (Example: `chmod 555 = r-xr-xr-x`)

- | | |
|---|------------------------------------|
| a. <code>chmod 1555 =</code> <u> r-xr-xr-t </u> | b. <code>chmod 6775 =</code> _____ |
| c. <code>chmod 2744 =</code> _____ | d. <code>chmod 4501 =</code> _____ |
| e. <code>chmod 0444 =</code> _____ | f. <code>chmod 611 =</code> _____ |
| g. <code>chmod 4040 =</code> _____ | h. <code>chmod 1111 =</code> _____ |
| i. <code>chmod 7000 =</code> _____ | j. <code>chmod 3111 =</code> _____ |

26. If you finish early, spend some time getting acquainted with the Unix system. Examine the directory structure or desktop until everyone is ready to discuss the PE.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Best Security Practices

Least Privilege	
Vulnerability	Countermeasure
A user should only have the access they require to perform their mission.	<input type="checkbox"/> 1. Users do not need elevated access to perform normal job functions <input type="checkbox"/> 2. Applications should not run with more access than they require <input type="checkbox"/> 3. Developers do not need administrator access <input type="checkbox"/> 4. Keep the number of root level accounts to a minimum <input type="checkbox"/> 5. Users should be assigned to groups that are in keeping with their level of access.

Patches	
Vulnerability	Countermeasure
Failure to stay current with available vendor patches may leave your system vulnerable to attack. Always check with ACERT for the latest approved patches for your version of Unix.	<input type="checkbox"/> 1. Use the command <code>#showrev -p</code> to list patches installed on your system <ul style="list-style-type: none"> ▪ {PRIVATE}RETRIEVE the latest patch list from your vendor (NOTE: Check ACERT advisories to be sure you have the latest "approved" patch). ▪ INSTALL patches that are recommended for your system. Some patches may re-enable default configurations. For this reason, it is important to go through this checklist AFTER installing <u>ANY</u> new patches or packages. ▪ ALWAYS review the Readme files. <p>NOTE: Ensure that current vulnerability patches are loaded as provided by the vendor and listed in ACERT/CC advisories.</p>

Secure terminals	
Vulnerability	Countermeasure
By default, on most Unix systems, root may log on from any terminal. This allows the root account to be accessed from anywhere in the network. A malicious attacker can target the root account to compromise your	<input type="checkbox"/> 1. DISABLE network login for root. All unencrypted root account access must take place on the physical console. The files to check may be called <code>/etc/ttys</code> , <code>/etc/default/login</code> , <code>/etc/securetty</code> , or <code>/etc/security</code> <p style="text-align: center;">For the <code>/etc/ttys</code> file, ADD: <i>Console "etc/getty std_9600" vt100 on local secure</i> For the <code>/etc/default/login</code> file, ADD: <i>CONSOLE=/dev/console</i></p> See the manual pages for file format and usage information

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

system.	<p>for your version of UNIX.</p> <p><input type="checkbox"/>2. ENSURE that the secure option is removed from all entries that don't need root login capabilities. The secure option should be removed from console if you do not want users to be able to reboot in single user mode.</p> <p>NOTE: This does not affect usability of the SU command.</p> <p><input type="checkbox"/>3. ENSURE that the permissions on this file are 640.</p> <p><input type="checkbox"/>4. ENSURE that the file is owned by root.</p> <pre>#ls -l /etc/default/login #chmod 640 /etc/default/login #chown root /etc/default/login</pre> <p><input type="checkbox"/>5. For Linux systems, edit the /etc/securetty file to contain: tty1, tty2, etc. Do not put in any pseudo terminals such as tty1. A tty* entry restricts root to only local logon. (The "*" symbol represents a number)</p>
---------	---

Lock Workstations	
Vulnerability	Countermeasures
If a user leaves their workstation unattended and does not lock the workstation, unauthorized personnel could access the workstation and the associated network system.	<p><input type="checkbox"/> 1. LOCK your workstation whenever you walk away</p> <ul style="list-style-type: none"> • Right-click the display background and select "Lock Display" from the menu pop-up box. • Some Unix GUI's will display an icon of a "lock" on the menu bar. Clicking on this icon will automatically lock the workstation. The password to unlock the workstation is equal to that of the login.

Screen Saver Passwords	
Vulnerability	Countermeasure
If a user leaves their workstation unattended and the screen saver is not password protected, unauthorized personnel could access the workstation and the associated network.	<p><input type="checkbox"/> 1. IMPLEMENT a Screen Saver Password</p> <ul style="list-style-type: none"> • Open up your desktop controls properties section of the GUI and set the desired time for the Screen to initiate the lock. There is normally a check box that you would also check to turn on the feature. • Set screen saver to execute no later than 10 minutes after last activity.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Backups	
Vulnerability	Countermeasures
<p>Since backup tapes contain all of your sensitive information from your system, to include user data, and passwords, they become a target for anyone who has physical access to your system.</p>	<p>☐ 1. MAKE regular backups.</p> <ul style="list-style-type: none"> • UPDATE your backups whenever you update or change your system. • ENSURE that EVERYTHING on your system is addressed in on your backup plan. • DO NOT reuse a backup tape too many times because it will eventually fail. • RESTORE a few files from your backup tapes on a regular basis. This ensures that you have good backup tapes. • REBUILD your system from a set of backup tapes to be certain that your backup procedures are complete. • KEEP your backup tapes under lock and key. • Keep written records of key backup and system configuration information. • Store back-up tapes off-site whenever possible. • Encrypt back-up tapes whenever possible.

Root account	
Vulnerability	Countermeasure
<p>Gaining root access is the primary goal of every hacker trying to get into your system. Root has absolute control over your box. If an attacker gains root access, it's no longer your system. This account should be protected at all costs.</p>	<p>☐1. IAW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, ALL unencrypted root account access must take place on the physical console. Programs such as secure shell (ssh) should be used for remote login, ensuring the passwords are not transmitted in the clear.</p> <ul style="list-style-type: none"> • DO NOT log in as root over the network. • ENSURE that direct logon for root is limited to the system console. <p>NOTE: This is enabled by default on Solaris 2.6, Sol 7 and Sol 8. #grep CONSOLE /etc/default/login Line should be CONSOLE=/dev/console</p> <p>If the file contains the entry, make sure it is uncommented. Remove the # at the beginning of the line that contains the entry CONSOLE=/dev/console</p> <ul style="list-style-type: none"> • RESTRICT the number of people who know the root password. These should be the same users registered with groupid 0. Typically this is limited to at most 3 or 4 people. <p>CONSIDER the use of sudo</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

     	<p>DO NOT use the root account for routine activities that can be done under a regular user ID.</p> <ul style="list-style-type: none"> • su from user accounts rather than logging in as root. This provides greater accountability. • ENSURE that root does not have a <code>~/.rhosts</code> file. <pre style="margin-left: 40px;">#ls -la / #rm /.rhosts</pre> <ul style="list-style-type: none"> • ENSURE that "." is <u>NOT</u> in root's search path. Use <code>set</code> to display the value of the <code>PATH</code> variable. • ENSURE that root's home directory is something other than "/" (i.e. <code>/roothome</code>), and has permissions of 700. <pre style="margin-left: 40px;">#mkdir /roothome #chmod 700 /roothome #grep root /etc/passwd</pre> <p>Edit the <code>/etc/passwd</code> file to reflect the new home directory</p> <ul style="list-style-type: none"> • ENSURE that root's login files do not source any other files not owned by root or which are group or world-writable. <p>Note: Root, by default, is usually assigned the Bourne shell</p> <pre style="margin-left: 40px;">#more .profile</pre> <ul style="list-style-type: none"> • ENSURE that root cron job files do not source any other files not owned by root or which are group or world-writable. <pre style="margin-left: 40px;">#cat /usr/spool/cron/crontabs/*</pre> <p>USE absolute path names when logged in as root, e.g., <code>/bin/su</code>, <code>/bin/find</code>, <code>/bin/passwd</code>. This is to stop the possibility of root accidentally executing a trojan horse. To execute commands in the current directory, root should prefix the command with <code>./</code>, e.g., <code>./command</code>.</p>
--	---



Files run by root	
Vulnerability	Countermeasure
 s not owned by root, if ran by root, may compromise root access or perform	<input type="checkbox"/> 1. CHECK the contents of the files listed below. Any programs or scripts referenced in these files should meet the following <u>requirements</u> : 1. ANYTHING run by root SHOULD be owned by root.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>Directories that are unwanted.</p>	<ol style="list-style-type: none"> 2. SHOULD NOT be group or world-writeable. 3. SHOULD be located in a directory where every directory in the path is owned by root. 4. IS NOT group or world-writeable. <p>CHECK the contents of these files:</p> <ul style="list-style-type: none"> - /.login, /.profile, /.cshrc and similar login initialization files. - /.exrc and similar program initialization files - /.logout and similar session cleanup files - crontab and at entries - files on NFS partitions - /etc/rc* and similar system startup and shutdown files - If any programs or scripts referenced in these files source/call additional programs or scripts they also need to be verified and meet the requirements of 1-4. <pre>#chmod 555 file #chown root file</pre>
---------------------------------------	---

Administration	
Vulnerability	Countermeasure
<p>A password/security policy is only as good as its enforcement.</p>	<ol style="list-style-type: none"> <input type="checkbox"/> 1. -IAW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, all system administrators will review date stamp for each user account password for compliance with current Army policy. <input type="checkbox"/> 2. - IAW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, all systems will be configured to limit logon attempts to three tries by timing out or disabling them. <p>ALL user files should be routinely backed up utilizing ufsdump.</p> <ul style="list-style-type: none"> • CONSIDER imposing quotas on users. Consult the manual pages on <code>quotaon</code> and <code>edquota</code> for specifics. <code>quotaon</code> turns on disk quotas for one or more ufs file systems. Before a file system may have quotas enabled, a file named <code>quotas</code>, owned by root, must exist in the root directory of the file system. The file system specified must already be mounted. <code>edquota</code> allows you to specify one or more users and limit how many files they may create. • REQUIRE users to physically identify themselves before granting any requests regarding accounts (e.g., before creating a user account). <p>It is recommended that users sign a UserID Receipt Form at the time that they are assigned a userid/password.</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<ul style="list-style-type: none"> • ENSURE that each user account has a unique name, and UNIQUE user id (UID) [usually greater than 100]. <pre style="margin-left: 40px;">#cat /etc/passwd #cat /etc/shadow</pre> <p>ENSURE that every user account is assigned to at least one group.</p> <p>ENSURE that normal users are NOT assigned to privileged groups.</p> <p>ENSURE that the /etc/group file does not contain duplicate GIDs.</p> <p>ENSURE that every group referenced in the /etc/passwd file is defined in the /etc/group file.</p>
--	---

Password Policy

Vulnerability	Countermeasure
<p>Weak, easily guessed passwords allow access to accounts by unauthorized personnel. Passwords of insufficient length increase password cracking tool's efficiency.</p>	<p><input type="checkbox"/> 1. Passwords on all systems MUST comply with AR25-2, Password Control.</p> <p>This regulation applies to the Active Army, the Army National Guard of the U.S. (ARNGUS), and the United States Army Reserve (USAR). It applies to contractors who operate Government-owned or contractor-owned, AIS (Army Automated Information Systems) that process or store Army information. Contractors who process Sensitive But Unclassified (SBU) information on contractor-owned AIS are governed by this regulation if specified in the contractual requirements or if they connect to an installation AIS/network system. All of the above must comply with sections 1 through 8, Act of 8 January 1988, PL 100-235, 101 Stat 1,724-1,730. During mobilization, deployment, or national emergency, this regulation remains in effect without change.</p> <p>NOTE: In Unix, if using DES, only the first 8 characters of a password are significant. Unix will truncate any password to 8 characters or less. This is a default behavior and cannot be modified.</p> <ul style="list-style-type: none"> • Passwords must be at least 10 characters in length • Passwords will also contain UPPERCASE, lowercase, numbers, or special characters (8 of each) • Passwords will not contain personal information, or any part of the user login name or full name • Minimum time before a password can be changed will be set to 90 days • Maximum time before a password has to be changed is 150 days. • The maximum and minimum time for passwords and password length are set in the /etc/default/passwd file.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

--	--

Proactive Checking	
Vulnerability	Countermeasure
<p>Dormant accounts, backdoor system passwords, and accounts without passwords allow unauthorized access to the system.</p> <p style="text-align: center;"></p>	<p style="text-align: center;"></p> <p><input type="checkbox"/>1. CHANGE default system passwords which were created when software was installed</p> <p><input type="checkbox"/>2. MAKE sure that all accounts have a password. The second field of <code>/etc/shadow</code> should contain an encrypted password. Ensure that users listed in <code>/etc/passwd</code> are listed in <code>/etc/shadow</code></p> <p><input type="checkbox"/>3. MAKE sure that users that should no longer have access are removed from all the systems to which they had access. Inactive accounts inactive for 45 days should be disabled. You must do this on every system on which the user had a valid account. <pre>#grep username /etc/passwd</pre></p> <p><input type="checkbox"/>4. MAKE sure the system is configured to limit logon attempts to three tries by timing out or disabling them.</p> <ul style="list-style-type: none"> • MAKE sure that the home directories and files of users removed from the system are also deleted or moved to the ownership of someone else.

Password Shadowing	
Vulnerability	Countermeasure
<p>Most current versions of Unix/Linux/BSD have implemented password shadowing. The permissions on this file are more restrictive than those on the <code>/etc/passwd</code> file. This prevents anyone other than <code>root</code> from reading the file or attempting to make a copy of the file and then attempt to crack user passwords.</p>	<p><input type="checkbox"/>1. ENABLE vendor supplied password shadowing or a third party product. With password shadowing, the encrypted password hashes are kept in <code>/etc/shadow</code> which has a 1 to 1 relationship with the <code>/etc/passwd</code> file. The <code>pwconv</code> command is normally used to implement shadow passwords. Check your vendor documentation.</p> <p><input type="checkbox"/>2. PERIODICALLY audit your password and shadow password files for unauthorized additions or inconsistencies.</p> <p style="text-align: center;"><pre>#cat /etc/passwd #cat /etc/shadow</pre></p> <p>Suggest backing it up regularly via a cron job and checking what changes have been introduced.</p> <p><input type="checkbox"/>3. ENSURE that the <code>/etc/shadow</code> file is accessible only by</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p>root.</p> <p>NOTE: root ownership is enabled by default on the /etc/shadow file.</p> <pre>#ls -l /etc/shadow #chmod 400 /etc/shadow</pre>
--	---

Restricted Shell	
Vulnerability	Countermeasure
<p>Many systems must provide “open accounts”, guest accounts or ftp “drop-box” account, an intruder can use an open account to gain initial access to your machine and then use that access to probe further for greater security lapses.</p> <p>Restricted shells can limit some of the vulnerabilities that having access to a open account will create. The main advantages are:</p> <ul style="list-style-type: none"> • The user can't change the current directory • The user can't change the value of the PATH environmental variable (even though they own their .profile) • The user can't use 	<p>□1. IAW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, ENABLE restricted shells to limit access for application specific accounts.</p> <p>Solaris: /usr/bin/rsh (restricted Bourne shell) /usr/bin/rksh (restricted Korn shell)</p> <p>NOTE: There is no such thing as a restricted C-shell.</p> <ul style="list-style-type: none"> • ENSURE that the account's default PATH statement does not include “.” or “:.” Check the manual pages for your version of UNIX. Files that contained the PATH variable are diverse. /etc/profile or /usr/profile <p>Also check in the following directories: /etc/skel/ /usr/skel/ /etc/security/ /usr/lib/mkuser/shell_name /etc/d.profile or stdprofile /etc/d.login or stdlogin /etc/d.cshrc or stdcshrc</p> <ul style="list-style-type: none"> • DISCONNECT users after a period of inactivity In implementation of the C shell, set autologout=?? Within the .cshrc file <p>NOTE : this option is not available with all versions of c-shell</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>command names containing slashes (means they can't start commands at root)</p> <ul style="list-style-type: none"> • The user can't redirect output with > or >> <p>If the user attempts to interrupt the restricted shell while it is processing the \$HOME/.profile, restricted shell will immediately exit.</p>	
--	--

Special accounts	
Vulnerability	Countermeasure
<p>Special and optional accounts have caused numerous problems for system administrators. Access to these accounts gives attackers elevated privileges, which will ultimately be used to gain root access. These accounts should be disabled wherever possible.</p>	<p>□1. ENSURE that there are no shared accounts other than root in accordance with site security policy, i.e. more than one person should not know the password to an account.</p> <p>NOTE: Some systems utilize Roll Based Access Control (RBAC) to break down administrator functions to specific tasks. Accounts are then created with only the necessary privileges required for completion of the particular task.</p>

Tripwire (ACERT APPROVED)

Tripwire is a utility that scans a set of designated files and directories, computes a digital signature, then compares the digital signature/fingerprint to a signature previously generated and stored in a database. Differences are flagged and logged including additions and deletions. When used regularly it enables a system administrator to spot any changes to files and directories rapidly.

Tripwire has 9 levels of security descriptors for each file or directory it monitors. It can monitor files that can not be changed, binaries with the SUID/SGID bit set, read only binaries, configuration files, logs, directory permissions/ownership, members of the trusted computing base, Kernel processes, and dynamic Kernel processes. Tripwire watches file sizes and computes checksums of files to produce signatures that shouldn't change.

Tripwire is a good tool for keeping Trojan horses off of your system. It protects you from unauthorized persons toying with your critical data files. You establish a policy in the `twpol.txt` file that consists of variable and rule definitions. The Tripwire policy tells tripwire what files to examine, what types of information to look for, and when to alert you to changes. Tripwire utilizes a site and local pass-phrase to encrypt tripwire policies, databases, and configuration files to keep them from being tampered with.

It can be found at: <https://www.acert.belvoir.army.mil/ACERTmain.htm>

NOTE: It does not currently function with the Solaris 8 x86 platform.

Sudo

Sudo is a program designed to allow a sysadmin to give limited root privileges to users and log root activity. The basic philosophy is to give as few privileges as possible but still allow people to get their work done. Sudo is configured in the sudoer file. The commands or directories from which commands can be run are identified by the individual user allowed to run them. The sudolog records activity.

It is available at: <http://www.courtesan.com/sudo> or
<ftp://coast.cs.purdue.edu/pub/tools/unix/sysutils/sudo>

tcp_wrapper (ACERT APPROVED)

tcp_wrapper: This software gives logging and access control to most network services.

- IAW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, tcp wrappers are recommended for all UNIX systems. Ensure the program is downloaded from a verifiable source-ACERT web site has tcp wrappers and portmap available at

<https://www.acert.belvoir.army.mil/ACERTmain.htm>.

Contact your supporting ACERT/CC or RCERT for assistance.

- TCP Wrappers will provide additional logging, a banner, reverse DNS lookup, and access control.
- **CUSTOMIZE** and install it for your system.

It is available from the ACERT site: <https://www.acert.belvoir.army.mil/ACERTmain.htm>

- **ENABLE** PARANOID mode.

Note: This is usually enabled by default.

- **CONSIDER** running with the RFC 931 option.

This is a connection-based application on TCP. A server listens for TCP connections on TCP port 113 (decimal). Once a connection is established, the server reads one line of data which specifies the connection of interest. If it exists, the system dependent user identifier of the connection of interest is sent out the connection. The service closes the connection after sending the user identifier.

- **DENY** all hosts by putting “all:all” in /etc/hosts.deny and explicitly list trusted hosts who are allowed access to your machine in /etc/hosts.allow.

```
#more /etc/hosts.deny
#more /etc/hosts.allow
```

- **WRAP** all TCP services that you have enabled in /etc/inet/inetd.conf or /etc/inetd.conf, or other appropriate file.

Modify the /etc/inetd.conf. For example, to modify telnet:

Original entry:

```
telnet stream tcp nowait root /usr/sbin/in.telnetd in.telnetd
```

Modified entry:

```
telnet stream tcp nowait root /usr/sbin/in.tcpsd /usr/sbin/in.telnetd
```

- **CONSIDER** wrapping any udp services you have enabled. If you wrap them, then you will have to use the nowait option in the /etc/inet/inetd.conf file.
- TCP Wrappers is high speed, low drag protection that does not require additional communications between the client and server. It serves as a stateless firewall, applying rules prior to allowing connections. New releases of some OS's already come with TCP Wrappers incorporated into a xinetd.conf file for use by the xinetd program.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>IPSEC</p> <ul style="list-style-type: none"> • IPSEC is a security architecture for the IP protocol. It is a layer 3 (network layer) security solution that is an Internet standard and is not dependent on any particular encryption or authentication algorithm or operating system. IPSEC is transparent to upper-level protocols and applications. IPSEC provides authentication, encryption, integrity, and replay protection. • IPSEC uses two protocols to provide security at the IP level: Authentication Header (AH) and Encapsulating Security Payload (ESP). • IPSEC has two modes: Transport and tunnel modes • IPSEC may be used to configure a VPN (virtual Private Network)

<p>Npasswd (ACERT APPROVED)</p> <p><input type="checkbox"/>1. USE npasswd as a replacement for the default Unix passwd command.</p> <p>Npasswd (new password) is a replacement for the system passwd command that incorporates a password checking system (word lists) that refuses poor password selections. It also incorporates the crack utility to eliminate easily guessed passwords from being used. This program reduces the chance of users choosing poor passwords.</p> <p>It is available from: https://www.acert.belvoir.army.mil/ACERTmain.htm</p>
--

Penetration Testing	
Vulnerability	Countermeasure
<p>One of the best tests of your security is to break into your system. Hacking your own system can identify backdoors that may exist for the hacker.</p>	<ul style="list-style-type: none"> <input type="checkbox"/>1. Start your penetration testing with the simplest methods first. Use common tools readily available on the Internet. <input type="checkbox"/>2. Analyze the access control infrastructure for vulnerabilities and single points of failure. <input type="checkbox"/>3. Any weaknesses identified by the penetration testing should be fixed immediately <p>NOTE: Make sure that the testing is authorized and conducted with management's knowledge. Create a step by step plan and document findings as you encounter them.</p>

Reading Assignment 2

Day 2 – Subject: UNIX Security
Practical UNIX & Internet Security

Pages 82 – 121, 131 – 154

1. Explain what a SUID program is and why it is used?

2. How can you tell if a file has the SUID set?

3. What security problems can occur with the SUID set? 

4. How can you turn off the SUID and SGID on mounted file systems? 

5. What is the purpose of the sticky bit being set on directories? 

6. What is an access control list?

7. What is an umask value used for in UNIX?

8. What are the default file permissions before an umask  is applied?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

9. What are the default programs and directory permissions before an umask is applied?

10. Name two (2) files that may be used to set the system umask value.

11. What information is found in both the /etc/passwd and /etc/shadow file?

12. Describe how Unix encrypts the password

13. What is the PAM and what is its purpose?

14. What are the things the superuser can not do?

15. What is sudo?



UNIX System Security

Practical Exercise SAS-7A

EXERCISE A

The purpose of this PE is to get you familiar with hidden file names and how to detect them.

Commands to type are written in bold. Only type what is in bold. The **^** symbol indicates where you put in a space. To type **^E**, hit the control key and letter e at the same time.

1. Check your directory and make sure you are in the root directory (/). Type: # **pwd**
 - a. If you are in a directory other than "/", type: # **cd**
2. Make a directory with a non-printing character (control-E). Type: # **mkdir^E**
3. Change to that directory. Type: # **cd^E**
4. Make a new directory. Type: # **mkdir^E**
5. Change to that directory. Type: # **cd^E**
6. Make a new directory. Type: # **mkdir^E**
7. Change to that directory. Type: # **cd^E**
8. Create a file. Type: # **touch^E hacktool**
9. Create another file. Type: # **touch^E B**
10. Go back to the root directory. Type: # **cd**
11. Use the **ls** command to see your **^E** directory. Can you see it? _____
12. Use the **ls^E-a** command to see your **^E** directory. Do you see it? _____
13. Use the **ls^E-al** command to see your **^E** directory. Do you see it? _____
14. Does the **ls^E-alb** command show you the **^E** directory? _____
15. What does the name of the **^E** directory print out as? _____

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

16. Try and find the file you created. Type: # **find** / **-name** **hacktool**

17. What is the location for the hacktool file? _____

18 Write the proper syntax to delete the file using the rm command (rm /directory/filename).

19. Now try and find the ^B file using syntax similar to step 16. What is its location?

20. Using your answer in step 19, write the proper syntax that will delete (rm) the ^B file. What is the syntax?

_____ 

21. Lets check the computer for any and all hidden nonprinting characters that have been used in the creation of file or directory names. At the command prompt#, type: **ls** **-laR** | **grep** **'\'**

Note: The first non-character symbol in the command is the vertical bar (pipe). The symbols in ‘ ‘ are back slashes.

21A. What files or directories were found? No files found are an acceptable answer.

_____ 

At the command prompt#, type: **ls** **-labR** | **grep** **'\'**

21B. What files or directories were found? What is strange about these files? Why were the files not displayed in the previous command? Notice that only the -b flag for ls will display nonprinting characters. Grep couldn't find the “\” until -b forced it to print.

_____ 



Using the table below, identify the character that is defined by the octal characters in the file name. Omit the ones that you created earlier.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<u>Decimal</u>	<u>Octal</u>	<u>Hex</u>	<u>Character</u>	<u>Remark</u>
0	000	00	CTRL-@	NUL (Null prompt)
1	001	01	CTRL-A	SOH (Start of heading)
2	002	02	CTRL-B	STX (Start of text)
3	003	03	CTRL-C	ETX (End of text)
4	004	04	CTRL-D	EOT (End of transmission)
5	005	05	CTRL-E	ENQ (Enquiry)
6	006	06	CTRL-F	ACK (Acknowledge)
7	007	07	CTRL-G	BEL (Bell)
8	010	08	CTRL-H	BS (Backspace)
9	011	09	CTRL-I	HT (Horizontal tab)
10	012	0A	CTRL-J	LF (Linefeed)



Now lets find the absolute pathname to the file.

22. Lets search for .\007 . At the command prompt#, type: **find ^/^ -name ^.^G**
Note: To create the ^G, press the CTRL key and the G key simultaneously.

22A. Where is the file?



Now let's delete the file so that this anomaly is no longer present on your system.

23. At the command prompt#, type: **rm ^/^var/preserve/.^G**



24. Is the use of hidden non-printing characters an effective way of hiding files and directories from most administrators.

End of PE.

Hidden files	
Vulnerability	Countermeasure
Unix doesn't typically create files with Non-printing characters unless there happens to be a catastrophic system crash. If you	<input type="checkbox"/> 1. USE the ls -alb command to show hidden files and files with nonprintable characters #ls -abl NOTE: ls with the -b option will display the nonprintable characters. An example of non-printable

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>discover hidden files, you can bet that someone is attempting to hide files on your system. The operative question would be ‘Why?’</p>	<p>characters would be the sequence backspace control-H (\^H). In SYSV systems, <code>ls -b</code> shows file names with non-printing characters represented by their octal value, i.e. \010 is octal for \^H. To determine the octal value of a character type:</p> <p style="text-align: center;">#man ascii</p> <p>BSD systems generally automatically show non-printable characters as "?" in the output of <code>ls</code></p>
---	---



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

UNIX PRACTICAL EXERCISES Special Notes

(Fort Gordon students do not do this)

Before beginning the following exercises, create 2 new user accounts. (This has been done  you at the Fort Gordon site)

Log in as root (password student). Ensure the session is Common Desktop Environment (CDE). Place focus on the terminal window by moving your cursor into the window and pressing the left mouse button. At the command prompt #, type: admintool &. On the Admintool Window, select **Edit>Add**. Use the following information to create the new user account.

NAME: labuser1

UserID: 1001

Group ID: Accept the default (you would normally change this)

Do not change the Shell (default is Bourne)

In the password field, select **Normal Password** (left mouse click on button)

Place focus on the Enter Password textbox (left mouse click)

Enter the password **student1** for both the password and verification of the password.

Press **OK** to close Set User Password window.

Verify the **Create Home Directory** box is checked. If it is not checked, check the box.

Enter the home directory as **/export/home/labuser1** in the Path textbox.

Click **APPLY** (**NOTE**: Do not click Apply and OK. This is not Windows.)

Now create another user account, labuser2.

NAME: labuser2

UserID: 1002

Group ID: Accept the default (you would normally change this)

Do not change the Shell (default is Bourne)

In the password field, select **Normal Password** (left mouse click on button)

Place focus on the Enter Password textbox (left mouse click)

Enter the password **student2** for both the password and verification of the password.

Press **OK** to close Set User Password window.

Verify the create home directory box is checked. If it is not checked, check the box.

Enter the home directory as **/export/home/labuser2** in the Path textbox.

Click **OK** (**NOTE**: Do not click Apply and OK. This is not Windows.)

Select **FILE>Exit** to close Admintool

General information about UNIX syntax and representations.

UNIX command syntax must be **precise**. You must use spaces between commands, options, and (most) arguments, e.g. `ls -l /usr`. Also UNIX is **case-sensitive**.

For the purposes of this exercise, UNIX commands and options are represented in Tahoma font, e.g. `chmod`. Files and directories are also represented in Tahoma font; however, they are italicized. e.g. */export/home/labuser1*.

The Practical Exercise identifies the UNIX command line interface commands for each step. Students who understand how to use the File Manager in CDE may use those interfaces vice the

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

command line steps identified (e.g. the result of the command **cat /etc/default/login** can also be obtained by placing focus on the  File Manager Window and double clicking on the **etc** folder, the **default** folder and finally the **login** file). The " ^ " has been placed in most of the syntax examples. The " ^ " represents a space.



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

 **Practical Exercise SRS-7B**
EXERCISE B

PURPOSE: To give students familiarity with the UNIX file & directory structure, and to reinforce good security practices as specified in Section 2.0 of the UNIX checklist

1. Log in as root (password is 'student').  Click on the options button (hold the mouse button in), move to session, move to common desktop environment, release the button, log in as normal.

Let's investigate if root login is restricted.

2. Access "terminal" window. (right mouse click on the desktop background, select tools, select terminal)

3. At the # prompt type: `cat /etc/default/login`

3A. Do you have the entry 'CONSOLE=/dev/console'? What restriction does this put on the root account ? 

Let's verify the system is only using authorized shells. If not, modify the system to do so

Determine if an /etc/shells file exists.

4. At the command prompt #, type: `ls -l /etc/shells`

4A. Is the system requiring the use of authorized shells (does the /etc/shells file exist)?



Find the valid shells.

5. At the command prompt #, type `ls -l /bin/*sh` (or `ls -l /usr/bin/*sh`)

The UNIX shells you are looking for are *sh*, *csh*, *ksh*, and *rksh* (possibly *remsh*, *bash*, *jsh*, depending on vendor).

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Create the */etc/shells* file.

6. We'll use dtpad, it's a text editor. If you want, you can use the vi editor. At the command prompt #, type: **dtpad /etc/shells**

(you may have to type the absolute path to get the dtpad command to work. If so, type: **/usr/bin/dtpad /etc/shells.**)

Confirm the creation of the new file if prompted.

Add the following entries on separate lines: ***/bin/csh, /bin/ksh, /bin/rksh, /sbin/sh.***

(example)

/bin/csh

/bin/ksh

etc.

Select **File>Save** to save the file.

Right mouse click in the title bar and select **Close** to close the Text Editor.

6A. */bin/false* and */dev/null* are examples of false shells. False shells disable login. Should you add the lines: */bin/false* and/or */dev/null* to the */etc/shells* file? Why or why not?



7. Lets look at the account names and the shells that are assigned to them. At the command prompt #, type: **cut -d: -f1,7 /etc/passwd**

(this shows the first and seventh column of the */etc/passwd* file)

7A. Which accounts have an authorized shell now that you have created an */etc/shells* file?

What should you do to the accounts which do not have an authorized valid shell identified?

Let's test to see if the */etc/shells* file works.

8. Log out of CDE. CDE is the graphical desktop program we are using. (select the **Exit** button in the Frontpanel toolbar)

9. Log in as **labuser1** (password is **student1**). During be careful to verify CDE is the selected Desktop. Solaris has two. CDE is the one we've been using. Open Windows is the other.

9A. Were you able to login as labuser1? Why ?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

10. Log in as root. 

Add the Bourne (/bin/sh) shell to /etc/shells list so that the labuser1 account can be utilized later.

11. At the command prompt #, type: **dtpad**  **/etc/shells**

Add the following entry on a separate line: **/bin/sh**

Select **File>Save** to save the file.

Right mouse click in the title bar and select **Close** to close the Text Editor.

Let's determine if the system has any files that may imply the system as been compromised.

Orphaned files	
Vulnerability	Countermeasure
Unix doesn't normally create files without an identifiable owner or group. The discovery of such files either indicates that there is a major problem with your operating system, administrators are not removing user files when they delete user accounts, or someone is attempting to hide files.	<input type="checkbox"/> 1. ENSURE that all directories and files (both data and executable) have an identifiable owner and group. <pre style="margin-left: 40px;">#find / -nouser -o -nogroup (-print as required)</pre> <p style="margin-left: 40px;"><u>NFS:</u></p> <pre style="margin-left: 40px;">#find / \ (-local -o -prune \) -nouser -o -nogroup (-print as required)</pre>

12. Find all files and directories that do not have an identifiable owner or group (orphaned files).

At the command prompt #, type: **find**  **/**  **-nouser**  **-o**  **-nogroup**

(the script matches all file UID and GIDs to existing accounts)

12A. What files or directories do not have an identifiable owner or group ? If none were found, state so.

Writable Files and Directories	
Vulnerability	Countermeasure
World-writeable files and directories are normally set as a matter	<input type="checkbox"/> 1. ENSURE that there are no <u>unnecessary</u> or <u>unexpected</u> world-writeable files or directories on your system. NOTE: it is necessary for some (maybe most) /dev files

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>of convenience; however, attackers will not overlook the obvious. Reconfiguration of system files, such as those located in /etc/rc*.d, could give attackers root access. Especially important are system initialization files, system configuration files, or user startup files.</p>	<p>to be world-writeable.</p> <pre>#find / -type f -perm -g+w (-print as required) #find / -type f -perm -o+w (-print as required) #find / -type d -perm -g+w (-print as required) #find / -type d -perm -o+w (-print as required)</pre> <p>Could be added to a cronjob to routinely check. See manual page on crontab</p> <p>To remove Group and Other write permissions from all files in a particular directory, use the following command: #chmod -R go-w /directoryname (for instance /etc, /bin, etc.)</p> <p><input type="checkbox"/>2. ENSURE that you don't have ANY system writeable directories, i.e. /etc, /bin, /usr, /dev, /export, /sbin</p> <p><input type="checkbox"/>3. ENSURE that writeable directories are not also readable. Directories that are both writeable and readable may be used in an unauthorized manner.</p> <p>Note: There are also implications in having writeable directories in user's home directories</p> <pre>#ls -l #chmod -R g-w directoryname</pre> <p><input type="checkbox"/>4. ENSURE that any writeable directories are owned by root and have permissions 1733.</p> <p>The sticky bit should be set. If the directory has the sticky bit set, a file can be deleted only by the owner of the file, the owner of the directory or by root.</p>
---	--

As an administrator, you should be concerned about the unrestrictive permissions that are set by default in a typical UNIX system. The permission that will cause the greatest security problem is the Write permission. You need to know which files and directories have the Write permission set for Group, but in particular for Other. Let's determine the files that have write permissions set for group, other or both.

13. We'll search all the type -,b,c,p files for other's write permission and then stick the results into a file called wfiles. At the command prompt #, type:

```
find / \(-type f -o -type b -o -type c -o -type p\) -perm -o+w > wfiles
```

*note: when you direct output to a file, it no longer displays on the screen.

14. This script searches the same file list for group write permission and appends the file. At the command prompt #, type:

```
find / \(-type f -o -type b -o -type c -o -type p\) -perm -g+w >> wfiles
```

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

15. This script checks all directories for group write permission and sends the results to a file called *wdirs*. At the command prompt #, type: `find / -type d -perm -g+w > wdirs`

16. This script appends the previous list with all the directory names that have others write permission. At the command prompt #, type: `find / -type d -perm -o+w >> wdirs`

Now let's look and see what our command did for us. The 1st 2 commands created a file (*wfiles*) that contains a list of all the files that have either Write permissions for group or Write permissions for other. The 2nd 2 commands created a file (*wdirs*) that contain a list of all the directories that had either Write permissions for group or Write permissions for other.

17. At the command prompt #, type: `cat wfiles`

17A. What is the contents of the file *wfiles*? Are the file names listed one per line ?

Let's count the number of lines in the *wfiles* file.

18. At the command prompt #, type: `wc -l wfiles` (the result of this command provides the number of lines)

18A. How many files have the 'Write' permission set for Group or Other ? Do the default file permissions leave potential holes in the system ?

19. At the command prompt #, type: `cat wdirs`

19A. What is the contents of the file *wdirs*?



Let's count the number of lines in the *wdirs* file.

20. At the command prompt #, type: `wc -l wdirs`

20A. How many directories have the 'Write' permission set for Group or Other? Do the default directory permissions leave potential holes in the system ?



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

In your reading assignment, you learned about the “Set User Id – SUID” and “Set Group Id – SGID”. Let’s see if your system has ber of these set on files. We’ll search the computer by searching for the permission octal values

21. At the command prompt #, type: `find / -type f -perm -004000 > suidfiles`

22. At the command prompt #, type: `find / -type f -perm -002000 > sgidfiles`

22A. Write the proper syntax that will find  of the directories with the "sticky bit" set

22B. Write the proper syntax that will find all of the files that have both the SUID and SGID bits set.

Let’s count the number of lines in the *suidfiles* file

23. At the command prompt #, type: `wc -l suidfiles`

23A. How many files have the SUID? What security implication does the SUID bit indicate? _____

23B. Check the output of step 21. Does the file "/usr/bin/admintool" exist on the list? Write the proper syntax using the "chmod" command that will turn off the SUID bit in /usr/bin/admintool.

Let’s count the number of lines in the *sgidfiles* file.

24. At the command prompt #, type: `wc -l sgidfiles`

24A. How many files have the SGID? Is this a concern? Which should cause you the most concern, SUID or SGID?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Let's investigate the vulnerability associated with SUID.

25. At the command prompt #, type: **cp /usr/bin/ksh /export/home/labuser1**
This makes a copy of the Korn shell and puts it into the /export/home/labuser1 directory.

26. At the command prompt #, type: **ls -l /export/home/labuser1/ksh**

26A. What are the current permissions?

27. At the command prompt #, type: **chmod 4555 /export/home/labuser1/ksh**

28. At the command prompt #, type: **ls -l /export/home/labuser1/ksh**

28A. Now what are the current permissions? How did the chmod command change the program?

29. At the command prompt #, type: **telnet localhost**

30. Log in as labuser1.

31. At the command prompt \$, type: **/export/home/labuser1/ksh**

31A. What happened? What does this mean?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

32. At the command prompt #, type: **id**

32A. What is your user id? What is your effective user id? Could this be a security issue?

33. At the command prompt #, type: **exit** to quit the korn shell session.

34. At the command prompt \$, type: **exit** to quit the telnet session.

SUID/SGID	
Vulnerability	Countermeasure
<p>Processes that have a SUID or SGID will execute as either the owner of the file or the group that is assigned to the file. Files that are executed as root are particularly dangerous.</p> <p>NOTE: Buffer overflows, race conditions, and symlink attacks (mentioned in other parts of this checklist) would be virtually useless unless the program were SUID root.</p>	<p><input type="checkbox"/>1. REMOVE the set-user-id (SUID) or set-group-id (SGID) bit from processes that do not need it. Most systems ship with more preset suid files than are required. Many of these programs are only accessed by root.</p> <p><input type="checkbox"/>2. Disable XHOST and CHROOT applications and any other application or process that uses a SETUID to Root upon execution, on all servers.</p> <p>NOTE 1: This is the point of failure on all standard UNIX machines. Virtually every attack is based around the concept of gaining root access on a machine. Once this is achieved an intruder can literally do anything with your system.</p> <p style="margin-left: 40px;"><u>SUID</u> #find / -type f -perm -4000 -ls (-print as required)</p> <p style="margin-left: 40px;"><u>SGID</u> #find / -type f -perm -2000 -ls (-print as required)</p> <p>Could be added to a cronjob to routinely check. See manual page on crontab.</p>

As a System Administrator, you are concerned about security and want to make permissions more restrictive. In your reading assignment, you learned about the “UMASK”. Let’s see how the UMASK affects the creation of files and directories.

35. At the command prompt #, type: **umask**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

35A. What is your current umask setting? How does this setting affect the permissions of newly created files?

Let's set a system default umask..

36. At the command prompt #, type: **dtpad** [^] */etc/profile*

Change the umask entry to **077**.

Select **File>Save** to save the file.

Close the Text Editor Window by placing the cursor on the title bar; pressing the right mouse button and selecting **Close**

37. At the command prompt #, type: **touch** [^] *foobar*

38. At the command prompt #, type: **ls** [^] **-l** [^] *foobar*

38A. What are the permissions? Do they match the umask in the */etc/profile*? Why ?

39. Log out of CDE. Log back in as root.

40. At the command prompt #, type: **touch** [^] *foobar2*

41. At the command prompt #, type: **ls** [^] **-l** [^] *foobar2*

41A. What are the permissions? Was the umask setting in the */etc/profile* used to create these permissions?

42. Log out of CDE, then log back in as labuser1. **NOTE:** Be careful to verify CDE is the selected Desktop.

43. At the command prompt \$, type: **umask**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

43A. What is your current umask setting? What does it indicate about the umask setting in the /etc/profile file?

44. At the command prompt \$, type: **pwd**

44A. Are you in labuser1's home directory?

Create a file called *file1*.

45. At the command prompt \$, type: **touch *file1***

46. At the command prompt \$, type: **ls -l *file1***

46A. What permissions does the file have? Was the umask setting in the /etc/profile file utilized to set the file permissions?

Change labuser1 umask so that all files you create have the following permissions:

owner = read, write
group = read, write
other = read

47. At the command prompt \$, type: **umask *002***

48. At the command prompt \$, type: **touch *file2***

48A. What are the permissions? Are they different from *file1*?

Let's set the labuser1 umask so that labuser1 always get the permissions labuser1 wants on login vice the system defaults (e.g. labuser1 won't have to type the umask command every time labuser1 logs in). labuser1 wants everyone to be able to read and write the files labuser1 creates.

49. At the command prompt \$, type: **dtpad *.profile***

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Editing the *.profile* allows you to change your operating environment. Create a new line and add:

umask ^ **000**

Select **File>Save** to save the file.

Close the dtpad Window by placing the cursor on the title bar; pressing the right mouse button and selecting **Close**

50. Log out of CDE, log back in as labuser1.

Let's verify the labuser1 umask has changed

51. At the command prompt \$, type: **touch** ^ **file3**

52. At the command prompt \$, type: **ls** ^ **-l** ^ **file3**

52A. What are the permissions? Are they different from *file1*? *file2*? Which umask (*/etc/profile*, *.profile*) is being utilized? Is this good security?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

52B. What could you do to stop a user from creating a .profile umask setting?

53C. What would the umask setting in the ~/.profile need to be to create a resulting directory permission of:
owner = read, write, execute
group = read
other = read

NOTE: When changing the default umask for root, be careful of the final result.

54. End of PE.

Umask for Users	
Vulnerability	Countermeasure
<p>Users can set their own Umask. This will override system defaults for the user. Hackers can take advantage of files that have weak permission settings.</p> 	<p><input type="checkbox"/> 1. ENSURE that the umask value for each user is set to 037 (consider a more restrictive value, such as 077). Check .profile (for sh, ksh) or .login (for csh) for setting umask value. Don't universally grant other permissions.</p> <p>The first way to set the system Umask is to Edit the file /etc/default/login by modifying the umask line to read umask 037 or 077.</p> <p>The second and more popular option is to edit the file /etc/profile by modifying the umask line to read umask 037 or 077.</p> <p>NOTE: The /etc/default/login and /etc/profile files are used for every user. Which file is used depends on the version of UNIX. Also, umask settings will be superseded/overridden by a user's .profile/.login/.cshrc.</p>

UMASKS for Root	
Vulnerability	Countermeasure
<p>Default Umask values may not be set appropriately to protect files created by root.</p> 	<p><input type="checkbox"/> 1. ENSURE that the umask value for root is set to 077 Check .profile (for sh, ksh) or .login (for csh) for setting umask value. Don't universally grant other permissions.</p> <ul style="list-style-type: none"> • To set a umask value for root which is different than the umask value for all users, you must create a .profile, .cshrc, or .login for root and place it in root's home directory. • If the system Umask is set to 077 in the /etc/default/login or /etc/profile, root will not need a

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	separate entry in a .profile/.login/.cshrc.
--	---

Race conditions	
Vulnerability	Countermeasure
Attackers will take advantage of a program or process while it is performing a privileged operation. This usually involves timing the attack to abuse the program after it enters a privileged mode but before it gives up its privileges. A vulnerability that allows attackers to abuse this window of opportunity is called a “race condition.”	<input type="checkbox"/> 1. REMOVE the SUID bit from as many files as possible and apply all relevant vendor-related security patches. NOTE 1: As with symlinks, there is no sure-fire cure to this vulnerability. The best defense is for programmers to ensure that the programs they create run trap signals in a secure manner. NOTE 2: A good practice for reducing this vulnerability is to reduce the number of SUID/SGID binaries on the system.



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS-7C

EXERCISE C



The purpose of this PE is to get you acquainted with file access control lists. Commands to type are written in bold. Only type what is in bold. The $_$ symbol indicates where you put in a space.

Vulnerability	Countermeasure
ACLs allow the administrator to set finer controls than are allowed by the default Unix permissions. Failure to set ACLs on critical files and directories may potentially leave those files and directories exploitable by malicious attackers.	<input type="checkbox"/> 1. USE FACLs (access control lists) if your version of UNIX supports it. NOTE: Using chmod on a file that has an FACL set, both the file group and owner permissions, and the FACL mask are changed to the new permissions. The new FACL mask permissions may change the effective permissions for additional users and groups who have FACL entries on the file. <ul style="list-style-type: none">• If a file or directory has an FACL set, a '+' will appear as the last character (far right) following the permissions.• FACL are only supported by the UFS and are best used to control access to binaries which have the suid or sgid bit set.

1. Locate your current directory. Make sure it is the root directory (/). Type: # **pwd**
2. Create a file to assign an access control list to. Type: # **touch $_$ myfile**
3. Check the file for assigned permissions. Type: # **ls $_$ -l $_$ myfile**
 - a. What are the permissions? _____
4. Remove all permissions to the file. Type: # **chmod $_$ 000 $_$ myfile**
5. Verify the new permissions. Type: # **ls $_$ -l $_$ myfile**
6. Are the new permissions set to no access for owner, group, and other? _____
7. Set up your access control list so that labuser2 has read/write privilege on the file.
 - a. Type: # **setfacl $_$ -m $_$ user:labuser2:rw- $_$ myfile**
8. Verify the new access control list. Type: # **getfacl $_$ myfile**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- a. Who has access to this file? _____
9. Verify that the file is reporting the access control list by checking permissions.
 - a. Type: # **ls -l myfile**
 - b. Have the permissions changed from step 3? _____
 - c. Has a plus sign appeared at the end of the permissions to indicate an access control list?

10. End of PE....

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Banners	
Vulnerability	Countermeasure
<p>Security warning banners notify users that they may be monitored. Lack of a banner may potentially give the impression that this system may be hacked without repercussion. A banner should be provided for both the <u>desktop (GUI) login</u> and the <u>command line/network login</u>. Individual banners may also be set up for individual network services.</p> <p>A banner should tell the visitor who the system belongs to, that the system is being monitored, that their use of the system is agreement to their being monitored, and the regulations governing the monitoring or use of the system.</p> <p>* See AR 380-53 and AR 380-5</p>	<p>□1. vi /etc/issue (create a <u>command line login banner</u> for connections which bypass the GUI)</p> <ul style="list-style-type: none"> • The /etc/default/telnetd and /etc/default/ftpd may also be used for the corresponding network service. <p>□2. For systems using the Dtlogin login screen, modify the /usr/dt/config/Xresources file. Set the Dtlogin*greeting.labelString to the Attention Banner.</p> <p>“ATTENTION! THIS IS A DOD COMPUTER SYSTEM. BEFORE PROCESSING CLASSIFIED INFORMATION, CHECK THE SECURITY ACCREDITATION LEVEL OF THIS SYSTEM. DO NOT PROCESS, STORE, OR TRANSMIT INFORMATION CLASSIFIED ABOVE THE ACCREDITATION LEVEL OF THIS SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (INCLUDES INTERNET ACCESS) ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL</p>

       	<p>PURPOSES, INCLUDING TO ENSURE THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY, MONITORING INCLUDES, BUT IS NOT LIMITED TO, ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR</p>
--	---

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

    	<p>UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING. UNAUTHORIZED USE OF THIS DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES”</p>
--	--

Message of the Day, & Mount Tab	
Vulnerability	Countermeasure
 The information can be released to system users. The Message of the Day (MOTD) goes to all users on the system. Do not use the motd file for login banners.	<input type="checkbox"/> 1. ENSURE that the permissions of /etc/motd and /etc/mtab are set to 644 or more restrictive. <pre style="margin-left: 40px;">#ls -l /etc/motd #ls -l /etc/mtab #chmod 644 /etc/motd #chmod 644 /etc/mtab</pre>

Core dump files	
Vulnerability	Countermeasure
Core files are generally world-readable and their memory often	<input type="checkbox"/> 1. CONSIDER disabling the creation of core dump files. Core images are created when a process abnormally terminates. The ulimit command can be used to place limits

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>contains sensitive information, including password hashes derived from the <code>/etc/shadow</code> file.</p> <p>The operating system writes out a core image of a process when it is ungracefully terminated. The core image is called <code>core</code> and is written in the process's working directory (Note: this is critical. Each terminated process, such as telnet or ftp, can create separate core images). <code>coreadm</code> is the command used to specify the name and location of core files produced by abnormally-terminated processes.</p>	<p>on the user. You can limit the user's core file size, data segment size, maximum amount of CPU time, maximum number of open files, and more.</p> <p>To prevent the creation of core files by users, add the entry ulimit -c 0 to their <code>.login</code>, <code>.cshrc</code>, or <code>.profile</code>.</p> <p>To prevent system daemons from creating core files, add the entry ulimit -c 0 to the appropriate boot script (usually in <code>/etc/rc*.d</code>)</p> <p>To prevent <u>ANY</u> process from creating a core dump, add the entry set sys:coredumpsize = 0 to the <code>/etc/system</code> file. This may not work on i386 versions of Unix.</p>
--	--

Buffer Overflow	
Vulnerability	Countermeasure
<p>A buffer overflow condition occurs when a user or process attempts to place more data into a buffer than was originally allocated. This would normally cause a segmentation violation to occur, however, this type of behavior can be exploited to gain access, often root, to the target system.</p>	<p>□1. PREVENT the execution of arbitrary code in the data buffer.</p> <p>For Solaris, to prevent the execution of instructions in the data stack, add the following entries to the <code>/etc/system</code> file.</p> <pre>set noexec_user_stack=1 set noexec_user_stacklog=1</pre> <p>Restart the system by typing: <code>init 6</code></p> <p>NOTE 1: Check your vendor documentation for your version of Unix.</p> <p>NOTE 2: Software patches are your best defense against buffer overflows and poor programming.</p> <p>NOTE 3: Stack settings currently fail to work on the X86 architecture (PC's running Unix).</p> <p>For more information, see "Smashing the Stack for Fun and</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p>Profit” at: http://www.2600.com/phrack/p49-14.html</p> <p>*** Linux systems****</p> <p>Buffer overflow events can be prevented by compiling programs with the <u>StackGuard compiler</u> available at: http://www.immunix.org. This compiler places other values called "canaries" on the stack area that are overwritten by buffer overflow attacks. An overwritten canary results in immediate program termination.</p>
--	--

Kernel	
Vulnerability	Countermeasure
<p>The kernel, or heart of the UNIX system, is the operating system. It should not be modified or recompiled unless by root. Modifications could affect computer input/output systems and filesystem security.</p>	<p><input type="checkbox"/>1. ENSURE that the kernel (may be called /vmunix, /unix, or /kernel) is owned by root, has group set to 0 and permissions set to 644 or more restrictive.</p>

External file systems/devices	
Vulnerability	Countermeasure
<p>By default, most file systems are mounted with Read/Write permissions for everyone, as well as allowing the ability to create SUID files. To protect your system, file systems should be mounted as Read-Only, and no SUID.</p>	<p><input type="checkbox"/>1. MOUNT file systems non-setuid and read-only where practical.</p> <p>NOTE: DO be VERY careful when using the mountall or umountall commands.</p> <ul style="list-style-type: none"> • Newer versions of Unix utilize volume managers and automatic removable media mounting scenarios. Check volume manager or rmmount configuration files for nosuid entries. Normally the /etc/vold.conf and /etc/rmmount.conf. <p><input type="checkbox"/>2. Check the /etc/fstab; /etc/export; or /etc/dfstab for entries without the nosuid flag.</p> <ul style="list-style-type: none"> • Example: /dev/hdc /mnt/cdrom iso9660 ro,user,noauto,nosuid

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS-7D

EXERCISE D

The purpose of this PE is to learn some of the basic configuration settings and default settings of the Unix operating system as they relate to security. Commands to type are written in bold. Only type what is in bold. The `^` symbol indicates where you put in a space.

1. Be logged in as the root administrator. Make sure you are in the Bourne shell and using a terminal window. Your desktop should be CDE.
2. Login banners are a requirement for DoD systems. A good banner will convey the identity of the computer system, the fact that monitoring is taking place, use of the system is permission to be monitored, and any regulation governing the system use or the security of the system. We are going to create a couple of banners that a user will see when telneting into a system. These are sometimes referred to as "command line" banners.
3. Create a login banner for command line logins **`dtpad ^ /etc/issue`**
4. Enter the following text: **`is ^ this ^ my ^ banner?`**
Save and close the editor
5. Enter at the prompt: **`telnet ^ localhost`**
6. Do you see your banner? _____
To get out of telnet type: **`^D`**
7. Now we'll create a specialized banner for telnet sessions only. **`dtpad ^ /etc/default/telnetd`**
8. Enter the following text: **`BANNER="Hey ^ Einstein, ^"`**
9. Hit enter, save and close the editor
10. At the prompt type: **`telnet ^ localhost`**
11. Do you see both banners? _____
12. To get out of telnet type: **`^D`**
- 13.
13. Next, we'll look at the problems concerning core dumps. Core files can fill up a file system. Core dumps can have clear text passwords and keys in them. Hackers look for core dump files (files with "core" in the name). Password hashes and IP's are gained through doing this. Solaris

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

has a utility called (coreadm). It will allow you to manage coredumps selectively. There is also a /etc/coreadm.conf file.

14. coreadm - shows dump process settings (new systems create dumps with mode 600. They will either make them global coredumps or by process. Let's check our system settings. To see dump process settings, type: **coreadm**

15. dumpadm - shows your dump configuration. To see your dump configuration, type: **dumpadm**

16. A big part of the core dump problem stems around content. By eliminating content, we can eliminate that part of the problem. To prevent any process from creating a core dump, modify the /etc/system file. The /etc/system file allows us to modify kernel activity without recompiling the kernel. Type: **dtpad ^ /etc/system**

17. Go to the bottom of the file and enter on the last line: **set ^ sys:coredumpsiz=0**
Hit enter, save and close the editor.

18. Now lets deal with the issue of buffer overflows. Buffer overflows are the most common attacks you'll see these days. They take advantage of bad programming. Once again, we'll use the /etc/system file to modify our systems behavior. Type at the prompt: **dtpad ^ /etc/system**

19. Go to the bottom of the file, below the coredumpsiz entry and add the following entries on two new lines of the /etc/system file.

set ^ noexec_user_stack=1

set ^ noexec_user_stacklog=1

NOTE: If you are using a PC version of Unix, close the file without saving. The PC version of Unix does not have the program variable required to perform this function. If you are using hardware specifically designed for Unix, save and exit the editor.

20. The stack =1 entry disables the execution of code directly on the stack by forcing a core dump on any buffer overflow attempt. The second command causes any attempt to run code from the stack to be logged. This fix could possibly stop some legitimate programs from running properly. Some programs need to be able to execute code in the stack. The stack is a reserved area of memory used to keep track of a program's internal operations, including functions' return addresses, passed parameters, and so on. A stack is usually a LIFO (last in/last out) data structure. The last item added is the first item used.

21. Now we'll check to see if our mounted drives are being mounted with the "nosuid" option. It is normally easy to figure out if automounting is occurring. If you insert a CD into the CDROM drive and the file manager creates a file window for you, automounting is happening. Check the Volume Manager daemon to see which file is responsible for handling the loading of the various mounted volumes. Type at the prompt: **cat ^ /etc/vold.conf**

Do you see where the removable media mount program (rmmount) is called on to handle mounted media? _____

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

22. Check the rmmount.conf file: **cat ^/etc/rmmount.conf**
23. Can you locate the “nosuid” setting? _____ What file systems are supported? _____ (file systems usually end in fs)
24. END OF PE

Practical Exercise SAS 7E

Installing Packages and Patches Practical Exercise

This PE will help you identify the software packages that have been loaded to your system and how to install new ones. This PE also will help you identify the patches that have been placed on your system and how to update your system with additional patches. Commands to run are identified in bold print.

1. Log in as root and open a terminal window in CDE (common desktop environment)
2. Use the package information command: **pkginfo**
3. You should see a long scrolling list of packages that are loaded to your system.
4. Pick one and look at its individual information: **pkginfo -l SUNWdtdst**
5. This command should display the information about the desktop application package. Each individual package has its own pkginfo file that can be queried for information.
6. Take a look at the patches loaded on your system by using both the showrev and patchadd commands
7. **showrev -p**
8. **patchadd -p**
9. both commands show that no patches have been loaded to this Solaris 9 base system
10. Insert the cdrom the instructor gives you. It will automount to your system. Open up the file manager if cdrom content does not display on the desktop. (**right click on the desktop, select files, and then file manager**)
11. The cdrom will mount as either CDROM0 or New
12. Access the cdrom: **cd /cdrom/cdrom0**
13. List the contents: **ls**
14. Do you see the file contents. Some are patches and some are software packages. All are compressed with some sort of encryption.
15. The 114134_0.zip and 114137_0.zip are patches for mail and sendmail
16. Make the default patching directory: **mkdir /var/spool/patch**
17. Copy the patches over to the default directory:
cp /cdrom/cdrom0/114* /var/spool/patch
18. Change over to the patch directory: **cd /var/spool/patch**
19. Unzip the patches
20. **unzip 114134_0.zip**
21. **unzip 114137_0.zip**
22. Install the patches
23. **patchadd 114134-01**
24. **patchadd 114137-04**
25. You should see the patches load after each patchadd command.
26. run either **patchadd -p** or **showrev -p** to see the current list of installed patches. You should see the two patches you just loaded.
27. Go back to the root home directory: **cd**
28. Double check that you are in the / directory: **pwd**
29. List out the cdrom components : **ls /cdrom/cdrom0**
30. Now install some packages to enable the Solaris Jump Start imaging program. First we need to copy the package to the default package directory.
31. **cp /cdrom/cdrom0/jetpkg.bz2 /var/spool/pkg**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

32. Change to the /var/spool/pkg directory and uncompress the file
33. **cd /var/spool/pkg**
34. **bunzip2 /var/spool/pkg/jetpkg.bz2**
35. Do a listing to see if the unzip was successful: **ls**
36. Add the package: **pkgadd -d /var/spool/pkg/jetpkg**
37. A list of packages will display, hit enter to accept all.
38. Answer yes to all questions.
39. run the package info command: **pkginfo**
40. Check for the packages you just added. You should see packages like JetEXPLO, JetFLASH, JetSAN, JetSDS, and JetVTS
41. Congratulations you have installed software
42. Now lets upgrade our overall encryption package
43. **cp /cdrom/cdrom0/sol_9_x8.zip /var/spool/pkg**
44. Now unzip the package.
45. **unzip /var/spool/pkg/sol_9_x8.zip**
46. This creates a directory of sol-9-x86-crypto
47. Lets view the packages available:
48. **ls /var/spool/pkg/sol-9-x86-crypto/Encryption_9/i386/Packages**
49. You'll see a list of 3 packages that deal with encryption.
50. Install the packages
51. **pkgadd -d /var/spool/pkg/sol-9-x86-crypto/Encryption_9/i386/Packages**
52. You see a choice of 3, hit enter to select all 3.
53. Answer yes to each prompt as you install all 3
54. When you've installed all 3, hit the "q" key to stop the install loop
55. Type pkginfo to find out what we installed: **pkginfo**
56. You should see SUNWcrman(Solaris Crypto Man Pages), SUNWcry(Crypt utilities), and SUNWcryr(Solaris Root Crypto) have been added to the package list.
57. You have just installed software updates to improve current encryption levels and to enable stronger encryption in programs such as IPSEC.
58. Use the cd command to get back to the / directory: **cd**
59. End of PE

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Pages 331 - 337

9. As ftp has some security and management problems, what are some of the replacements for ftp?

10. Once a user has established an ftp connection, how many commands are available within ftp?

11. Explain the difference between passive ftp and active ftp?

12. What is a ftp bounce attack?

Pages 576 - 578

13. What four main restrictions go into effect when a user is placed in a restricted shell?

Pages 591 - 593

14. List 2 additional method of protecting the root account?

15. How can you restrict the ability of users to login to the root account from any terminal other than the console?

16. Does the above restriction prevent a user from su to the root account?

UNIX Network Security

Turn off unnecessary services	
Vulnerability	Countermeasure
<p>Unnecessary services leave a system open to outside attack in a variety of ways. A system should only offer services that are necessary for mission performance.</p>	<p><input type="checkbox"/>1. Services often running by default</p> <p>7/tcp - echo 11/tcp - systat 13/tcp - daytime 19/tcp - chargen 21/tcp - ftp 23/tcp - telnet 25/tcp - smtp 37/tcp - time 42/tcp - nameserver 43/tcp - whois 53/tcp/udp - DNS lookup/zone 69/udp - tftp 79/tcp - finger 80/tcp - http 111/tcp - portmapper/rcpbind 139/tcp - netbios 512/tcp - rexec 513/tcp - rlogin 514/tcp - rsh</p> <p>(1)Only root can bind to a port below 1024 (2)Binding is when a service connects to and begins listening at a port. (3)Machines trust that a connection coming from a port less than 1024 on the remote machine is from a program that is run by root. (4)Port numbers are used by some protocols as a means of authentication. (5)Attempts to connect to another machine at a low numbered port are taken to be from the official daemon that is possibly requesting a username and password and not some rogue server created by a clever user on that machine. This also applies to authentication services like ident/auth port, which is used to provide the username associated with an existing connection. (6)rsh and ssh can be configured to allow certain users to log in without a password from specified systems. Since the connection is coming from a privileged port, the server can trust that the client username supplied is accurate.</p> <p><input type="checkbox"/>2 Protect TCP Sequence attacks by modifying the <code>/etc/default/inetinit</code> to read <code>TCP_STRONG_ISS=2</code></p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p><input type="checkbox"/>3 To <u>stop IP forwarding</u>, creat the file called /etc/notrouter (no content)</p> <p></p> <p><input type="checkbox"/>4 Solaris can <u>detect promiscuous mode</u> with the public domain software “ifstatus”. It will return a machines promiscuous status.</p> <p><input type="checkbox"/>5 DA procedural guidance for Unix systems, DA msg 050951Z MAR 99, requires all high numbered ports with known vulnerabilities to be disabled. ACERT maintains a list of these ports.</p>
--	--

/etc/inetd.conf	
Vulnerability	Countermeasure
<p>It is best to avoid telnet, ftp, tftp, http, smtp, snmp, udp, and any “r” commands, as they have been major sources of insecurities.</p>	<p>Network services – IAW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, and as stated in a number of previous alerts, unused or unnecessary ports and services should not be active. Disable and/or disable at the network layer if possible all unused and unnecessary ports and services, e.g., rpc, tftp, gopher, smtp, http, finger, netstat, etc. Conduct risk assessments to determine if that port must remain open.</p> <p>NOTE 1: Some system services, specified in system startup files, WILL NOT be disabled simply by commenting them out in the /etc/inetd.conf file.</p> <p>NOTE 2: The location of the inetd.conf file will vary between Unix/Linux flavors. It is oftened linked to the /etc directory and it will be referred to as "/etc/inetd.conf" in this document.</p> <p><input type="checkbox"/>1. DISABLE any services that you do not need to operate. To do this, comment out ALL services by placing a “#” at the beginning of each line. Then enable the ones you NEED by removing the “#” from the beginning of the line. For changes to take effect, you need to restart the inetd process.</p> <p style="padding-left: 40px;">Restart inetd</p> <p style="padding-left: 40px;"><u>BSD commands</u></p> <p style="padding-left: 40px;">#ps -aux grep inetd </p> <p style="padding-left: 40px;">#kill -HUP <inetd-PID></p> <p style="padding-left: 40px;"><u>SVR4 commands</u></p> <p style="padding-left: 40px;">#ps -ef grep inetd</p> <p style="padding-left: 40px;">#kill -HUP <inetd-PID></p> <p>For some systems (including AIX), these commands are not sufficient. Refer to vendor documentation for more information.</p> <p>If the above commands do not work, then do this:</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>This file identifies what service is listening on what port. If you have disabled services in /etc/inetd.conf, then you should disable the same service in the /etc/services file.</p>	<p>□1. COMMENT out any ports of services that you want disabled. This should match the services commented out in the /etc/inetd.conf.</p> <ul style="list-style-type: none"> • IAW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, and as stated in a number of previous alerts, unused or unnecessary ports and services should not be active. Disable and/or disable at the network layer if possible all unused and unnecessary ports and services, e.g., rpc, tftp, gopher, smtp, http, finger, netstat, etc. Conduct risk assessments to determine if that port must remain open. <p>#cat /etc/inetd.conf #vi /etc/services</p> <ul style="list-style-type: none"> • Place a # symbol at the start of each line, for the port you wish to disable. • Save the /etc/services. No process restarting or rebooting is required. This file acts as a database which is referred to as network service requests are received. <p>□2. ENSURE that the permissions on this file are set to 440. □3. ENSURE that the owner is root.</p> <p style="text-align: center;">#ls -l /etc/services #chmod 440 /etc/services #chown root /etc/services</p>
---	--

Remote Commands ("R" services)	
Vulnerability	Countermeasure
<p>The "R" services were developed by Berkeley to provide seamless authentication between trusted hosts and users. The remote commands can allow users/attackers to circumvent password authentication via trusts. Authentication is based on IP address, TCP port, and client username. Remote shell (in.rshd) port 514 and remote login (in.rlogind) port 513</p>	<p>□1. USE the Secure Shell (ssh) program to replace rlogin (remote login) and rsh (remote shell). Secure shell is a suite of utilities which utilize port 22 to set up public key encrypted remote access packages with a secure shell daemon (sshd) which handles all the connections, a secure shell program (ssh), a secure copy program (scp), a secure login program (slogin), and a secure program (sftp).</p> <p>NOTE 1: Secure Shell is an ACERT recommended commercial product and can be obtained at: http://www.ssh.org</p> <p>There is also a free version of SSH. It can be obtained at: http://www.openssh.com/</p> <p>NOTE 2: Use more secure versions (like Wietse Venema's)</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>are the more dangerous remote services.</p>	<p>of the “r” commands for cases where there is a specific need. These versions can be configured to consult only /etc/hosts.equiv and not \$HOME/.rhosts. There is an option to disable the use of wildcards (+’).</p> <p>NOTE 3: To stop the threat of remote services, comment them out in the inetd.conf, comment out the port in /etc/services (rlogin uses port 513 and rsh uses port 514), or rename the associated daemon file.</p> <p>NOTE 4: REXEC is oftentimes confused with other “r” services. It runs on TCP port 512. Many Unix distributions do not ship with REXEC. REXEC uses standard username and password authentication. All data is sent in clear text.</p>
--	---

REXEC (remote execute)	
Vulnerability	Countermeasure
<p>REXEC runs on port 512 and uses standard username and password authentication. Brute force attempts may go unnoticed as the rexecd performs poor logging.</p> <p>All communications are unencrypted.</p> <p>There is no access control built in to rexec.</p>	<p>❑1. Disable REXEC. If client applications rely upon it, figure out a migration path away and then disable it.</p> <ul style="list-style-type: none"> • If you can not disable REXEC, consider using Secure Shell (ssh) to tunnel the program. SSH provides remote terminal access • <p>NOTE 1: Secure Shell is an ACERT recommended commercial product and can be obtained at: http://www.ssh.org</p> <p>There is also a free version of SSH. It can be obtained at: http://www.openssh.com/</p>

/etc/hosts.equiv	
Vulnerability	Countermeasure
<p>The /etc/hosts.equiv file explicitly or implicitly trusts other hosts. Since trust is transitive, you may be trusting hosts not under your control. Be very careful when establishing trust. Remote users can gain unauthorized root access to the system.</p>	<p>❑1. – IAW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, eliminate all .rhosts+, .rhosts ++, or <u>host.equiv</u> to external hosts (external to the network)</p> <ul style="list-style-type: none"> • DETERMINE if the file /etc/hosts.equiv is required. <u>If you are running certain “r” commands, such as rlogin, rsh, and rcp</u>, this file allows other hosts to be trusted by your system. Programs such as rlogin can then be used to log on to the same account name on your machine from a trusted machine without supplying a password. <p style="text-align: center;">#ls -l /etc/hosts.equiv</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>Under normal circumstances, you should have no use for this file and it should be removed.</p>	<pre>#rm /etc/hosts.equiv</pre> <ul style="list-style-type: none">• DO NOT specify a username with a specific host. This allows that user listed in the <code>/etc/hosts.equiv</code> to log into the local system as <i>any user on the local machine!!</i>• ENSURE that you list only a small number of TRUSTED hosts. Remember that trust is <u>transitive</u>.• ONLY trust hosts within your network or under your management. <pre>#more /etc/hosts.equiv</pre> <ul style="list-style-type: none">• ENSURE that you use fully qualified hostnames i.e., <code>hostname.domainname</code>.• ENSURE that you DO NOT have a '+' entry by itself anywhere in the file as this will possibly allow users on any host to access your system. <pre>#more /etc/hosts.equiv</pre> <ul style="list-style-type: none">• ENSURE that you do not use '!' or '#' in this file. <p>NOTE: There are no comment characters for this file.</p> <pre>#more /etc/hosts.equiv</pre> <ul style="list-style-type: none">• ENSURE that the first character of the file is not '-'. NOTE: The presence of a '-' as the first character in <code>/etc/hosts.equiv</code>, <code>/etc/hosts.lpd</code> and <code>.rhosts</code> files may allow unauthorized access to the system. <pre>#more /etc/hosts.equiv</pre> <p>Refer to the CERT advisory CA-91.12. http://www.cert.org/advisories/CA-91.12.Trusted.Hosts.Configuration.VULNERABILITY.html</p> <ul style="list-style-type: none">• ENSURE that the permissions are set to 600.• ENSURE that the owner is set to root. <pre>#ls -l /etc/hosts.equiv</pre> <p>If the file exists:</p> <pre>#chmod 600 /etc/hosts.equiv</pre> <pre>#chown root /etc/hosts.equiv</pre> <p>CHECK it again after each patch or operating system</p>
---	---

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	installation.
--	---------------

\$HOME/.rhosts	
Vulnerability	Countermeasure
<p>The .rhosts file is potentially a greater security risk than the /etc/hosts.equiv, as one can be created by each user.</p>	<p>□1. IAW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, eliminate all <u>rhost+</u>, <u>rhost ++</u>, or host.equiv to external hosts (external to the network).</p> <ul style="list-style-type: none"> • ENSURE that no user has a .rhosts file in their home directory. To check: <pre>#find / -name .rhosts -print</pre> <pre>#rm -r \$HOME/.rhosts</pre> • Use CRON to periodically check for, report the contents of, and delete \$HOME/.rhosts files. Users should be made aware that you regularly perform this type of audit, as directed by policy. To see if check is being made for .rhosts <pre>#more /usr/spool/cron/crontabs/*</pre> <p>Add or modify an existing cron job. See crontab manual page.</p> <p>Refer to the CERT advisory CA-91.12. http://www.cert.org/advisories/CA-91.12.Trusted.Hosts.Configuration.VULNERABILITY.html</p> <p>□2. Edit the /etc/pam.conf file by commenting out the lines for rsh and rlogin that contain reference to pam_rhosts_auth.so.1. This will allow the login function to skip its check for .rhosts files.</p> <p>NOTE Unlike /etc/hosts.equiv, .rhosts allow for root login.</p>

Remote Procedure Call (RPC)	
Vulnerability	Countermeasure
<p>RPC was originally developed by Sun Microsystems, but it has been widely ported to other versions of Unix. It is a mechanism commonly</p>	<p>□1. DISABLE any RPC services that you do not need, such as rexd, rwall, rwho, rusers, rstat, rpc.ttdbserverd, rpc.statd, rpc.cmsd, rpcgen, kcms_server, sprayd, sadmin, etc. To do this, comment out ALL services by placing a “#” at the beginning of each corresponding line of the /etc/inetd.conf file.</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>used to simplify development of networked applications, in particular NFS and NIS. However, RPC uses very weak authentication. Under the standard RPC authentication mechanism, a given RPC service will only respond to requests from a certain set of user IDs. However, the remote server relies on the client to authenticate the user IDs being sent in the request.</p>	<pre>#more /etc/inetd.conf #vi /etc/inetd.conf Restart inetd</pre>
--	--

Samba (SMB)

Vulnerability	Countermeasure
<p>SMB is the Microsoft file and print sharing protocol. Samba makes a Unix server look like an NT server by enabling it to run SMB. Vulnerabilities have been discovered in all versions of Samba, especially for Linux running Intel platforms. Exploits may allow unauthorized remote users to obtain root access.</p>	<p><input type="checkbox"/>1. ENSURE that Samba has been removed from your server (if installed and unnecessary). #find / -name samba (-print as required) NOTE. Samba loads NetBios to your Unix computer.</p> <p><input type="checkbox"/>2. A serious security hole has been discovered that effects all versions of Samba. Edit the smb.conf configuration file and replace all occurrences of the macro "%m" . Replace %m with %I .</p>

Domain Name Service

Vulnerability	Countermeasure
<p>DNS is one of the few services that is almost always required and running on an organization's Internet perimeter network. Thus, a flaw in BIND will almost surely</p>	<p><input type="checkbox"/>1. DISABLE and REMOVE BIND on any system that is not being used as a DNS server.</p> <p style="padding-left: 40px;">In Solaris, comment entry to start in.named in the file: /etc/rc2.d/S72inetsvc kill in.named process and remove any named.xfer processes</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>result in a remote compromise. In a typical example of a BIND attack, intruders erased the system logs, and installed tools to gain administrative access.</p> <p>SANS rates unpatched BIND servers as the number one security problem on the Internet.</p>	<pre>#ps -ef grep in.named; ps -ef grep xfer #kill -9 (in.named PID) #kill -9 (xfer PID)</pre> <p><input type="checkbox"/>2. ENSURE that the version of BIND you are using is current and patched for security-related flaws. Bind has had 12 security advisories in the last 4 years.</p> <p><input type="checkbox"/>3. Don't run BIND as root. Create a new user and group.</p> <p><input type="checkbox"/>4. Configure BIND to disallow zone transfers except to authorized servers.</p> <p><input type="checkbox"/>5. Do you check your DNS logs regularly. A working DNS is often a forgotten DNS</p> <p>It is available at: https://www.acert.belvoir.army.mil/ACERTmain.htm</p> <p>References: http://www.cert.org/advisories/CA-99-14-bind.html http://www.cert.org/advisories/CA-98.05.bind_problems.html http://www.cert.org/summaries/CS-98.04.html</p>
--	---

Practical Exercise SAS 8A

EXERCISE A

This PE will familiarize you with identifying remote connections, disconnecting remote sessions, identifying ports and services that are open and some of the dangers of leaving unnecessary ports open and unnecessary services running. Commands to type are written in **bold**. Only type what is in bold. The \wedge symbol indicates where you put in a space. The # symbol represents the command prompt. Not all commands in this PE will be typed on a command prompt. Some commands will be typed within a TCP session.

1. This PE will have you "telnet" to various ports and observe some of the disadvantages of leaving them open when certain services are running on them.
2. Login to your Solaris workstation as root. Make sure that the desktop you are using is the Common Desktop Environment (CDE).
3. Break down into groups of two.
4. Each partner should telnet to their partner's workstation: # **telnet \wedge (partner ip)**
(example: #telnet 147.51.217.151) Were you greeted by your partner's banner?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

5. Login as labuser2 with a password of student2.

6. Change to root with su and root's password. # **su root**

netstat	
Vulnerability	Countermeasure
The netstat daemon will report network connections, routing information, and statistics.	netstat displays the contents of certain network-related data structures in various formats, depending on the options selected. <input type="checkbox"/> 1. ENSURE that permissions for netstat are set to 500 <input type="checkbox"/> 2. ENSURE that the netstat daemon (netstatd) has been disabled in the /etc/inetd.conf file. #chmod 500 /usr/bin/netstat

7. Use the netstat command to determine the connections on your partners computer. Remember, you are viewing your partner's computer connections. This will show all of the tcp protocol activity.

#**netstat -a -P tcp**

8. You should see a lot of ports listening or in use. Find the line where telnet and your IP or machine name are listed. One is the connection from you. The other is your partner connecting to you.

9. Find the process that is your connection to your partner. The in.telnetd daemon makes the inbound connection possible. Search for processes that involve it.

ps -ef | grep in.telnetd

10. The first number listed, from the left, is the process id of the telnet connection you are using to connect to your partner. Kill this process. #**kill -9 (PID)** (example: # kill -9 488)

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

11. Did you just get notification that your connection was disconnected by the foreign host?

_____ You just disconnected yourself.

12. Check to see if the process  exists. It should be gone from both machines.

ps_ -ef_|_grep_in.telnetd

13. Use netstat to see if the connection is still there. The connection you will be viewing is that of your own workstation. You are no longer connected to your partner. **#netstat_-a_-P_tcp**

14. The connections should be gone or in a TIME_WAIT status. A TIME_WAIT status would indicate that your tcp connection ended unnaturally. Your computer is still waiting for the command to close the connection. It will time out naturally. When you used kill -9, you forced the connection to close on your partners machine. No command was ever sent back to your machine. The connection was left open on your machine.

15. Check to see what ports and services are open. The following set of syntax will show you services and ports that are open on your computer. Do the following steps in order.

#netstat_-a_>_file1

#netstat_-an_>_file2

#sdiff_file1_file2

16. Look for your connection to your partner. It should no longer be listed as being in a TIME_WAIT status. It should be gone.

17. Look at the IPv6 TCP section and notice the services on the left with the corresponding port number near the center of the line. There are services open expecting a connection from the outside. Notice the listening status. If you browse the entire list you'll see the UDP: IPv4, UDP: IPv6, TCP: IPv4, and TCP: IPv6 ports and services.

18. Go look at what can be learned from the FTP port of 21. Type: **# telnet_localhost_21**

Solaris 9 users will also type: **USER_ labuser1** (hit enter) **PASS_ student1** (hit enter)

a. What information does the system give you once you connect to port 21?

b. Type: **help**

1. You should see a bunch of commands that are not meant for public consumption. Manipulation of these commands enables hackers to take over systems.

c. Type: **quit**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

19. Go look at what can be gained by going to port 13. Type: # **telnet localhost 13**
- a. It won't really let you connect but it will give you some information. What did you learn?
-

20. Go look at what can be gained by going to port 79. This is port for finger.

- a. Type: # **telnet localhost 79**
- b. Hit enter twice. What did you learn?



21. Go look at what port 25 has to offer. This is the port for SMTP. Port 587 is the submission port for sendmail and works similar. Type: # **telnet localhost 25**

- a. What did you learn?



-
- b. Type: **help**

Do you see some commands that you could use to manipulate email.

- c. Type: **vrfy labuser1**



- d. Type: **vrfy labuser2**

- e. Type: **vrfy labuser3**

f. You'll notice that in steps c and d, you found out about labuser 1 and 2's email accounts. Step e indicated that there wasn't a labuser3 the system. This is one of the ways hackers verify or identify valid users on a system.

- g. Type: **quit**

22. Take a look at another unnecessary port. Type: # **telnet localhost 7**

- a. Type: **enter**

- b. Type: **quit**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

c. See how the port repeats what it gets. This is the echo service. It doesn't serve much purpose and is liable to utilize large amounts of process time when given large amounts of data to repeat.

d. Type: ^]

1. The above command is the control-right bracket combination

e. To get out of the telnet prompt ">", type: ^D

23. Another seemingly harmless port is 19. Type: # telnet localhost 19

a. Seems like you've tapped into a treasure trove of useless data. This is the character generator service. You should notice that the CPU meter on the bottom right is starting to show red. What do you think would happen if you redirected this output to your port 7?

24. To stop the data flow, type: ^C

25. Type: ^]

26. To get out of the telnet prompt ">", type: ^D

27. If you are not back to the # prompt, you can try various combinations of the above control characters or close and reopen your window.

28. Let's summarize what we've learned from these unnecessary ports by matching the correct fact with the port that we visited.

Choices: Port 7, 13, 19, 21, 25, 79

a. The port that told us what time zone the computer was in was? _____

b. The port that told us who was logged onto the system was? _____

c. The port that took data and repeated it was? _____

d. The port that tied up our processor was? _____

e. The port that helped us determine if the computer was a mirror site was? _____

f. The port that told us the version number of a often hacked program was? _____

g. The port that told us the machine name was? _____

h. The port that told us our operating system was? _____

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- i. The port that helped us id all the users was? _____
- j. With  two ports could be used to tie up resources and create a denial of service attack?

29. Lets take a look at the traffic on the wire utilizing the "snoop" utility that is provided with Solaris 8/9. Snoop is a tool that really has no basis for existence as System Administrator's should not be analyzing traffic in this manner. Utilize your partnership from earlier in the PE to complete these steps.
30. Both partners need to capture some network traffic. Type: # **snoop**
31. After a slight delay you should see quite a bit of packet information. This is being generated by your classmate's computers. Your network card is capturing all broadcast traffic on the network. Type: # ^c to stop the flow of data. Take a couple of seconds to familiarize yourself with the format.
32. Partner B now should ping another computer in the room. Type: # **ping_s(some IP)**
(some IP represents an IP number, ping -s sends that IP a ping each second, do not type "((" or ")")
33. Partner A will now capture the traffic between the two computers in a file called cap.
34. Type: # **snoop_o_cap(partner B IP)_SOME IP**
Example: snoop -o cap 147.51.217.151 147.51.217.166
(this captures the traffic between your partner and the IP they pinged in a file called cap)
35. Partner A should see a little counter on the command line increase numerically. When Partner A has received a comfortable amount of packets (over 40), both partners need to type : # ^C
36. Partner A can now examine the packets. Type: # **snoop_i_cap_p0,40**
(this allows you to view the first 40 packets of the file cap)
37. You should see the ping (ICMP) packets between the two machines. You may see a few packets of another type. Do you see the echo requests and echo replies?
38. Partner A can now examine the details on any packet. This script looks at the 16th packet. You may substitute the number 16 for any of your packet numbers. Type: # **snoop_i_cap_v_p16**
(Notice the nice breakdown of the packet information)
39. If you like, reverse your roles so both partner can capture traffic.
40. Let's see if a regular user can use snoop to spy on fellow users. Both partners type: # **exec_login**
41. Enter **labuser1** for login and hit enter
42. Enter **student1** for the password and hit enter

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

43. Type : \$ **snoop**
44. Did it work or were you denied permission? _____
45. Check out your permissions, type: \$ **ls_ -l_ /dev/iprb0**
46. What was the outcome? Is this a link? _____
47. Check the target of the link, type: \$ **ls_ -l_**
/devices/pci@0,0/pci8086,244e@1e/pci8086,50@2:iprb0
Link targets will vary from system to system
48. What are the permissions on the actual network
adapter?_____
49. Snoop needs to be deleted or disabled. Is it disabled for user use? _____
50. Return to the root account, type: \$ **exec_ ^ login**
51. Type **root** at the login prompt and hit enter
52. Type **student** at the password prompt and hit enter
53. The terminal window will close and you will be back at root
54. End of PE.

Practical Exercise SAS 8B

EXERCISE B

Secure Shell Practical Exercise

The following steps will take you through a demonstration on how Secure Shell (SSH) protects your communications from prying eyes (snooping). The PE is designed around working in groups of 3, 2 is acceptable. Two (partner A and C) will be setting up telnet sessions and SSH sessions. The third team member (partner B) will be the man in the middle, snooping the traffic between the other two. Partners need to perform their respective tasks in order to avoid incorrect results. Bold print identifies what needs to be typed. The `_` symbol identifies where a space needs to be. The entry `<enter>` means enter key and the `<ctrl-d>` and `<ctrl-c>` stand for control key sequences.

Here are some of the scripts you will be using:

<code>snoop_ -o _cap_ (partner A IP) _ (partner C IP)</code>	-Snoop will scan for traffic between the two ips and put the captured packets in a file called cap.
<code>snoop_ -i_ cap</code>	-this will read the contents of cap
<code>snoop_ -i_ cap_ -v _-p _ (packet#)</code>	-this will analyze a selected packet

1. Partner B will set up the traffic intercept.

At the # prompt, type: **snoop_ -o _cap_ A-IP_ C-IP**

Example: `snoop -o cap 147.51.217.151 147.51.217.153`

2. Partner A will connect to partner C

At the # prompt, type: **telnet_ C-IP**

3. Partner A will then log in to partner C's computer utilizing the **labuser2** account and password of **student2**

4. Partner A will type at the \$ prompt: **who**

5. Identify the root login at either pts/4 or pts/5. We are going to type a message to partner C.

6. At the \$ prompt, type: **write_ root_ (pts/4 or pts/5)**

Example: `write root pts/4`

The prompt will be a line without a prompt. On this line type: **Unix is a wonderful operating system**

Partner A hit the `<enter>` key and then hit `<ctrl-d>`

7. Partner A should see the message print on partner C's computer. Partner B should be seeing a packet counter on partner B's screen continue to climb numerically. Partner B hit `<ctrl-c>` and stop the capturing of packets.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

8. Partner B can view the packet history by reading the file called cap.

At the # prompt, type: **snoop_A -i_A cap**

9. Partner B should see a printout of all the packets that A and C exchanged. Notice that to the right you see the ASCII values of some of the packets. Do you see the message partner A typed? _____ . Do you see the attempts for the typing to be echoed back to partner A from partner C? _____. Can you see the password "student2" laid out vertically in packet sequence? _____

10. Partner B can pick a packet at random and plug its number into the following script. At the # prompt, type: **snoop_A -i_A cap_A -v_A -p_A (packet #)**

11. Do you see the breakdown of the packet? _____

12. Partner A can disconnect from partner C now. At the \$ prompt, type, **exit**

13. Partner B can now set up capturing again, this time between partner C and partner A. The roles will be reversed. 

14. Partner B at the # prompt, type: **snoop_A -o_A cap2_A C-IP_A A-IP**

15. Partner C will now set up a secure shell connection to partner A

Partner C at the # prompt, type: **su_A labuser2**

Partner C at the \$ prompt type: **ssh_A (partner A IP)**

If prompted about the RSA key, ignore it by typing **yes** and hitting **<enter>**

16. When prompted for the password, partner C will type: **student2**

17. Partner C will type at the \$ prompt: **who**

18. Partner C identify the root login at either pts/4 or pts/5. We are going to type a message to partner A.

19. At the \$ prompt, type: **write_A root_A (pts/4 or pts/5)**

The prompt will be a  without a prompt. On this line type: **Unix is a lot better than the windows operating system** 

Hit the **<enter>** key and then hit **<ctrl-d>**

20. You should see the message print on partner A's screen. Partner B should be seeing a packet counter on partner B's screen continue to climb numerically. Partner B hit **<ctrl-c>** and stop the capturing of packets.

21. View the packet history by reading the file called cap2.

Partner B at the # prompt, type: **snoop_A -i_A cap2**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

22. Partner B should see a little bit different output than before. The packet capture doesn't show any of the ASCII value text and there is additional sequence and coding numbers. Do you see any of the previous ASCII values? _____

23. Partner B can pick a packet at random and plug its number into the following script. At the # prompt, type: **snoop -i -cap2 -v -p (packet #)**

24. Do you see the breakdown of the packet? _____
Notice that the previous telnet capture showed plaintext telnet lines that are now gone.

25. Partner C can disconnect from partner A now. At the \$ prompt, type, **exit**

26. What conclusion do you come to when confronted with the question, "what is the benefit of running secure shell over telnet?"

27. END OF PE

Secure Shell (ACERT APPROVED)

Secure Shell (ssh) is a program used to log into another computer over a network, to execute commands in the remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a suggested replacement for telnet, rlogin, rsh, ftp, and rcp.

Secure Shell can be used to tunnel remote X sessions, do secure network backups, and remote administration.

USE the **Secure Shell (ssh)** program to replace telnet, rlogin (remote login) and rsh (remote shell). Secure shell is a suite of utilities which utilize port 22 to set up public key encrypted remote access. It packages with a secure shell daemon (sshd) which handles all the connections, a secure shell program (ssh), a secure copy program (scp), a secure login program (slogin), and a secure ftp program (sftp).

NOTE: IAW DA Msg 050951ZMar99, all unencrypted root account access must take place on the physical console. Secure Shell is an ACERT recommended commercial product and can be obtained at:

<http://www.ssh.org>

There is also a free version of SSH. It can be obtained at:

<http://www.openssh.com/>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS-8C

EXERCISE C

The purpose of this PE is to familiarize you with  Unix's main scheduling utility. "cron" is a chronological scheduler that allows you to run programs or scripts unattended. Commands to type are written in bold. Only type what is in bold. The `_` symbol indicates where you put in a space.

Cron is the scheduling utility of choice on unix systems. If you use it you have "cron jobs" pending or in the works. To use cron, you edit the cron Table. Type `crontab` with one of the following flags:

- e (edit)
- l (list)
- r (remove)
- d (kills all cronjobs)

1. Make sure your system date is correct. Type: `# date` 

2. If the date and time is incorrect, you can reset it by typing: `# date_nnddhhmm`

- a. nn = month
- b. dd = day
- c. hh = hour
- d. mm = minutes

3. Check date again by typing: `# date`

4. Open up the cron Table for editing by typing: `# crontab_ e`

- a. The format for a cronjob is minute, hour, date, month, day, file or script. Separate entries  a space.

5. Go down to the last line of the cron jobs and create a new line to run a script that hunts for user created `~/rhosts` files. Make the script so that it runs every day at 10:55am and saves to a file in the root directory called "trusts".

- a. Type: `55_10*_***_find_/_-name_.rhosts_>_/trusts`

6. Click on "file" and select "save (needed)".

7. Close the editor. Your script should now be set to run at 10:55am everyday.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

8. Use of the cron utility is controlled through cron.deny and cron.allow files. Take a look at the cron.deny file.

a. Type: # **cat** */etc/cron.d/cron.deny*

9. Are any of the normal users listed? _____

10. Lets add labuser1 and labuser2 to the cron.deny file.



a. Type: # **dtpad** */etc/cron.d/cron.deny*

11. The users listed cannot use cron. On a line by themselves, add both labuser1 and labuser2 to the bottom of the list.

a. Click on "file" and select "save (needed)" to save the list with changes.

12. Double-check your changes. Type: # **cat** */etc/cron.d/cron.deny*

13. A cron.allow file is not normally created. Check for its existence.

a. Type: # **cat** */etc/cron.d/cron.allow*

b. A cron.allow file is usually used when all users are included in the cron.deny file. The cron.allow would allow only the users listed to use cron. The system reads the cron.allow file prior to the cron.deny file. Do not be surprised if you do not have one by default.

14. End of PE.



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS-8D

EXERCISE D

Purpose: Show the dangers of X-Windows. Hackers can exploit your X-Windows sessions in various ways.



1. Pair up the students so that they are in groups of two. Select one to be partner A and one to be partner B.
 2. Have the students log in as root and open a terminal window (Bourne shell is fine).
 3. Have each student type: # **xhost** \wedge +
 4. Notice what the computer tells you about access control lists. What does it indicate to you?
-
-

5. Have each student type: # **xhost** \wedge -
 6. Notice what the computer tells you about access control lists. What does it indicate to you?
-
-



7. Have each student type: # **xhost** \wedge +(*IP of partner computer*)
"example: #xhost \wedge +147.51.217.157"
 8. Have each student type: # **xhost**
 9. Who is listed in your access control list for the Xserver?
-
-

10. Have each student type: # **xhost** \wedge -(*IP of partner computer*)
"example: #xhost \wedge -147.51.217.157"
 11. Have each student type: # **xhost**
 12. Who is listed in your access control list for the Xserver?
-
-



13. Have each student type: # **xhost** \wedge +
14. Have partner B start a program on his computer. Type # **xclock** \wedge &
15. Partner A will type # **xlsclients** \wedge -a \wedge -l \wedge -display \wedge (*partner-B-IP*):0
"example: #xlsclients -a -l -display 147.51.217.155:0"

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

16. Record the names of the clients (open windows) open on your partners machine.



17. You will see that the all the windows that are open on partner B's computer have an ID (0x?????????). What is the window ID for the window named xclock?

18. Partner A type # **xkill_A-id_A(xclock ID from question 17)_A-display_A(partner-B-IP):0**
"example: #xkill -id 0x40000040 -display 147.51.217.155:0"

19. What happened on your partner B's display?

20. Have partner A type: # **xterm_A-display_A(partnerIP):0**
"example: #xterm -display 147.51.217.155:0"

21. What happened to the partner B's screen?

22. Have partner B click on the xterm window and type # **cat_A/etc/hosts** and hit enter . Did the IP
e hosts file match the IP of partner A or partner B?

23. Have partner B type # **reboot** and hit the enter key.

24. What happened?



25. What does this tell you about the potential danger of xhost files?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

26. When communicating with your partner's screen were you ever prompted for a password? Did you have to utilize a .rhosts or hosts.equiv file? Who does the "xhost" _^+ command allow Xserver access to?

Security and the X Window System	
Vulnerability	Countermeasure
<p>The major problem with X is that its security model is an all or nothing approach. Once a client is granted access to an X server, pandemonium is allowed. X clients can capture the keystrokes of the console user, kill windows, capture commands for display elsewhere, and remap keyboard to use nefarious commands not matter what the user types. Most problems stem from a weak access control paradigm.</p>	<p>Access to your X server may be controlled through either a host-based or user-based method. The former is left to the discretion of the Systems Administrator at your site and is useful as long as all hosts registered in the /etc/Xn.hosts file have users that can be trusted, where "n" represents your X server's number.</p> <p>This may not be possible at every site, so a better method is to educate each and every user about the security implications of the references below. Better still, when setting up a user, give them a set of X security related template files, such as .xserverrc and .xinitrc. These are located in the users home directory.</p> <p>You are strongly advised to read the section on X window system security referred to in the X Window System Administrators Guide (C.4).</p> <ul style="list-style-type: none"> <input type="checkbox"/> 1. IAW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, disable xhost and chroot applications and any other application or process that uses a setuid to root upon execution on all servers <input type="checkbox"/> 2. Xwindows uses TCP ports 6000-6063. Blocking these ports will stop outside access.

Problems with xdm.	
Vulnerability	Countermeasure

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

xdm bypasses the normal getty and login functions, which means that quotas for the user, ownership of /dev/console and possibly other preventive measures put in place by you may be ignored.

Refer to CERT Vendor-Initiated Bulletin VB-95:08

NOTE: Release 6 of X11 is now available and solves many problems associated with X security which were present in previous releases. If possible, obtain the source for R6 and compile and install it on your system.

X11R6

It is available from:

<ftp://archie.au/X11/R6>/*<ftp://archie.au/X11/contrib>/* or
<ftp://ftp.x.org/pub/R6>/*

□1. **Secure XWindows**

- **DO NOT** permit access from arbitrary hosts.
- **Remove** all instances of the 'xhost +' command from the system-wide Xsession file, from user .xsession files, and from any application programs or shell scripts that use the X window system.
- If you must allow access to your X server, specify each server by IP address. Keep in mind that any user on that server can connect to your X server and snoop away.
- **DO** use xauth to replace xhost. If you use ssh, the xauth is automatic.
- **READ** the manual pages for xauth and Xsecurity. Use this information to set up the security level you require.

- **USE** the X magic cookie mechanism MIT-MAGIC-COOKIE-1 or better. With logins under the control of xdm, you can turn on authentication by editing the xdm-config file and setting the DisplayManager*authorize attribute to true. When granting access to the screen from another machine, use the xauth command in preference to the xhost command.

MIT-MAGIC-COOKIE-1: Shared plain-text "cookies"

XDM-AUTHORIZATION-1: Secure DES based private-keys

SUN-DES-1: Based on Sun's Secure RPC system

MIT-KERBEROS-5: Kerberos version 5 user-to-user

- **ENSURE** that the permissions on /tmp are set to 1777 (or drwxrwxrwt), i.e., the sticky bit should be set. The owner **MUST** always be root. If the sticky bit is set, no one other than the owner can delete the file /tmp/.X11-unix/X0, which is a socket for your X server. Once this file is deleted, your X server will no longer be accessible.

Set ownership and permissions for /tmp correctly

```
# chown root /tmp
```

```
# chmod 1777 /tmp
```

NOTE: This will NOT recursively set the sticky bit on sub-

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p>directories below /tmp, such as /tmp/.X11-unix and /tmp/.NewUnix; you may have to set these manually.</p> <p>Linux Note: Start the xinit program with the -auth argument. This forces the system to use magic cookies for authentication. Another solution is to use ipchains. # ipchains -A input -p tcp -j DENY 0.0.0.0/0 -d 0.0.0.0/0 6000:6063</p>
--	--



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS-8E

 EXERCISE E

PURPOSE: To give students familiarity with the UNIX default network services & to understand the security implications in Section 3.0 of the UNIX checklist

1. If you are not logged in as root, log in as root.

Where are the remote daemons that allow the use of "r-commands"?

2. At the command prompt #, type: `find /usr/sbin -name "in.r*" > rcmds`

3. At the command prompt #, type: `cat rcmds`

3A. Which r-command daemons do you want to delete or disable? How could you do this?

The greatest vulnerabilities in your system are network services. You need to know which services are currently running on your system.

4. At the command prompt #, type: `dtpad /etc/inetd.conf`

4A. Any line not preceded by a # symbol is a service that is running on this computer. The first word on each line is the name of the service. The second column tells you the type of socket. The third column tells you protocol. The fourth column tells you the wait status. The fifth column tells you the UID that it runs as. The sixth column tells you the full path to the actual daemon program. The last column allows you to specify arguments. What are some of the services that are currently running by default?. By what name do in.rshd, in.rexecd, and in.rlogind go by?

Most of these services are unnecessary.

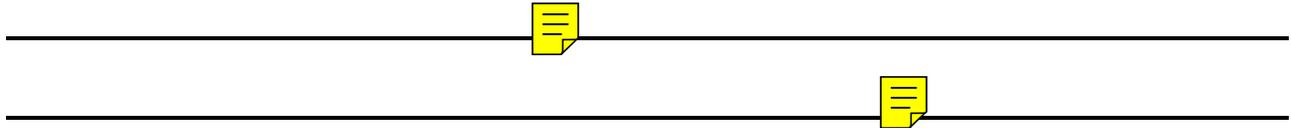
PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

5. **Disable the telnet service only.** To disable this service, comment it out by placing the # symbol at the beginning of the line that contains the service you wish to disable. When done, save the file (**File>Save**) and exit the dtpad program (exit the Text Editor Window by placing the cursor on the title bar; pressing the right mouse button and selecting  **lose**).

NOTE: Commenting out services in the inetd.conf DOES NOT automatically terminate these services. You must stop the inetd daemon, and then restart it, so the new configuration file is initialized. 

In the next step terminate the inetd daemon and then restart it.

6. At the command prompt #, type: **ps [^]-ef [^]| [^]grep [^]inetd**
Write down the [PID of inetd]. The PID is found in the second column of the line with the /usr/sbin/inetd filename at the end. Of the two columns of numbers, it will be the left one.



7. At the command prompt #, type: **kill [^]-HUP [^][PID of inetd in step 6 above]**
(HUP is a hang-up argument which stops and restarts a service) 

8. Let's try to telnet.
At the command prompt #, type: **telnet [^]localhost** 

8A. Write down message received.

(**Note:** If you did not receive an error message when the telnet command was executed then the kill command executed in step 7 did not work correctly. To ensure the inetd has read the updated /etc/inetd.conf type: **kill -9 [PID of inetd]**, then at the command prompt, type **inetd -s**. This will restart the inetd daemon using the modified configuration file. Try step 8 again. A word of caution—using kill -9 is **NOT** the recommended way to restart processes, however, it may be necessary.)

In addition to the /etc/inetd.conf, you can edit the file that specifies which service runs on a specific port. The /etc/services file lists the available ports by service name., port number/protocol.

9. At the command prompt #, type: **dtpad [^]/etc/services**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Comment out the same service that you specified in STEP 5 (telnet). Add the # symbol to the beginning of the line that contains the service you wish to disable. When done, save the file and exit the dtpad program.

10. Let's try to telnet.

At the command prompt #, type: **telnet localhost**

10A. Write down the message received. Is the message different from the message received when the services had simply not been started ?

Just as in NT, UNIX also has the ability to establish trust relationships. However, it is more dangerous in UNIX because every user can establish a trust. First let's determine if the administrator has set up a trust.

11. At the command prompt #, type: **ls -l /etc/hosts.equiv**

11A. Does a hosts.equiv file exist on the system? When is a hosts.equiv file allowed?

In STEP 11, we addressed the fact that the system administrator may establish a trust. UNIX will also allow ANY user to establish a trust with any other user, either internal or external. This is done through the creation of a .rhosts file.

Do you have any .rhosts files in your system?

12. At the command prompt #, type: **find / -name .rhosts**

12A. Do any .rhosts files exist on the system? What would it mean if a .rhosts file did exist? Name 2 methods to increase security from the vulnerability associated with .rhosts files?

13. **Switch user to the labuser1 account.** At the command prompt #, type: **su labuser1**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Now let's try to compromise a default system account.

14. At the command prompt \$, type: **rlogin ^ -l ^ lp ^ localhost**
(NOTE: The lp account does not have a password. When asked for a password, abort the rlogin attempt by typing a Ctrl-D.)

14A. Are you able to log in as lp? Why ?

15. At the command prompt \$, type: **exit**
This should put you back as 'root.' (NOTE : the # prompt)

Create a .rhosts file in the lp home directory.

16. At the command prompt #, type: **dtpad ^ /usr/spool/lp/.rhosts**
Enter the following line as the first line:

+ ^ + (The line should be a plus sign followed by a space, followed by a plus sign., followed by pressing the enter key)

Save the file (**File>Save**).

Close the text editor window by placing the cursor on the title bar; pressing the right mouse button and selecting **Close**

Now change the owner of the file to lp. For a .rhosts file to work, the directory owner must have at least read permission on the file.

17. At the command prompt #, type: **chown ^ lp ^ /usr/spool/lp/.rhosts**

17A. Why did lp not have read permission on the file prior to changing ownership?

Let's try to compromise the lp account

18. At the command prompt #, type: **su ^ labuser1**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Now try to rlogin to the lp account.

19. At the command prompt \$, type: **rlogin -l lp localhost**

19A. Were you able to log in? (use the id command). Why is use of a *.rhosts* file a security risk? What does the ++ mean?

20. At the command prompt \$, type: **exit** to quit the rlogin session.

21. At the command prompt \$, type: **exit** to quit the su labuser1 session.

Remain logged in as root (**NOTE** : the # prompt)

Let's disable the lp account login by giving it a false shell.

22. At the command prompt #, type: **cat /etc/passwd**

22A. Does the lp account have an authorized shell? Should you be able to login as lp?

23. At the command prompt #, type: **usermod -s /bin/false lp**

23A. What did you just do?

24. At the command prompt #, type: **cat /etc/passwd**

24A. What's different about the lp account?

25. At the command prompt #, type: **su labuser1**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Now try to login as lp.

26. At the command prompt \$, type: **rlogin** **-l** **lp** **localhost**

26A. Are you able to login now? (use the id command) Why or why not? (**NOTE** : Look carefully at the messages from the rlogin)

27. At the \$ prompt type: **exit** (this will put you back at root)

28. Remove the false shell from the lp account (hint: # **usermod** **-s** **/bin/sh** **lp**)

29. Edit your pam.conf file: # **dtpad** **/etc/pam.conf**

30. Locate the lines for rlogin and rsh. Place a # symbol in front of each line that has the rhosts reference. They should look like this when you are done if using Solaris 9 (Solaris 8 is slightly different):

```
#rlogin      auth    sufficient    pam_rhosts_auth.so.1
#rsh         auth    sufficient    pam_rhosts_auth.so.1
```

31. Save the /etc/pam.conf file and close your editor.

32. At the # prompt, type: **su** **labuser1**

33. Try and rlogin again as you did in step 26. (hint: **rlogin** **-l** **lp** **localhost**)

34. What was different this time as compared to step 26? Why do you think you were prompted for a password?

32. How can system accounts be secured from *.rhosts* logins?

33. At the command prompt \$, type: **exit** to quit the su labuser1 session.

Pluggable Authentication Module (PAM)

PAM enables the authentication mechanism to be extended beyond UNIX passwords and to be both "stackable" and "tailorable" on a host- or application-basis using other authentication mechanisms like s/key, kerberos, and smart cards. Rules can be written such that a user must pass multiple authentication schemes to access high-security servers. In addition to authentication, PAM enables administrative customization of account management and session management. PAM allows you to change on the fly your authentication methods, requirements, and encapsulate all local authentication methods without re-compiling any of your binaries.

Just a few of the things you can do with PAM:

- Use a non-DES encryption for your passwords. (Making them harder to brute force decode)
- Set resource limits on all your users so they can't perform denial of service attacks (number of processes, amount of memory, etc)
- Enable shadow passwords (see below) on the fly
- allow specific users to login only at specific times from specific places
- Create a password history file
- Write your own PAM to lockout accounts after 3 failed login attempts.
- Disable.rhosts lookup
- Port over Linux modules to Solaris and other Unix platforms.

PAM is supported in Solaris 2.5 - Solaris 9 (see vendor documentation), and many distributions of Linux, such as Caldera, Debian, FreeBSD, Red Hat, SuSE.

For Solaris, PAM is a separate software package.

For Linux, it is available at: <http://www.kernel.org/pub/linux/libs/pam/index.html>



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS-8F

EXERCISE F

PURPOSE: To gain some familiarity with default network settings and the necessary security adjustments.

1. If you are not logged in as root, log in as root. 
2. NFS is the Network File System. With NFS, a Unix/Linux user can share files between other users. The security involved is often weak. Check the default settings on your system. Type:
cat `/etc/nfssec.conf`
3. What is the default security setting? _____
4. The present setting only requires a request to have generated from the proper system and user. These can easily be spoofed. Stronger settings are available. Some additional options are: none; dh (Diffie Hellman); Kerberos. Selecting dh would greatly increase security by requiring DES encryption. Kerberos is normally supplied only in the client form.
5. Files are shared out by placing them in the distributed file system (`/etc/dfs/dfstab`). Files we connect to are identified in the virtual file system (`/etc/vfstab`). Take a look at the default distributed file system. Nothing should be shared by default. Type: **# cat `/etc/dfs/dfstab`**
6. You may have noticed in an earlier PE that port 25 (sendmail) has a habit of broadcasting its version number. This is something best left for the hacker to guess. Sendmail is an often hacked program and it does no good to share version information with the world. Let's remove the version info from public access.
7. Edit the sendmail configuration file. **# dtpad `/etc/mail/sendmail.cf`**
8. **Click on edit and select find. Search for Smtpl. This will send you to the line for the SmtplGreetingMessage. Delete everything to the right of the \$j entry.** This is what causes the version to be broadcast. The next time the system boots up, the sendmail version will not be so easily obtained.
9. File transfers are a way of life for most IT personnel. The FTP protocol is one of our most well known and widely used. Unix provides a way of controlling who is using FTP. Check the FTP access list by viewing the ftpusers file.
(Solaris 8 users) **# cat `/etc/ftpusers`** (Solaris 9 users) **# cat `/etc/ftpd/ftpusers`**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

10. What users on this system can use FTP?

11. At a minimum, make sure that the root Administrator and the system accounts are listed. This is a list of those accounts that can not connect to the system to use FTP.

12. Let's test access to ftp. At the # prompt, type: **ftp localhost**

13. When prompted for Name(localhost:root), enter: **labuser1**

14. Enter the appropriate password: **student1**

15. At the ftp> prompt, type: **help**
(you should see the wide range of commands that ftp allows)

16. Exit your ftp session by typing: **quit**

17. Assign a false shell to the labuser1 account: # **usermod -s /bin/false labuser1**

18. At the # prompt, type: **ftp localhost**

19. When prompted for a name, enter: **labuser1**

20. Enter the appropriate password: **student1**

21. What happened?

22. Type: **quit**

23. Now add the /bin/false shell to the /etc/shells file. # **dtpad /etc/shells**

24. Add **/bin/false** on a new line, save the file, and exit the editor.

25. At the # prompt, type: **ftp localhost**

26. When prompted for a name, enter: **labuser1**

27. Enter the appropriate password: **student1**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

28. Did the results from step 21 repeat? What happens when you put a false shell in the /etc/shells file?



29. Exit the ftp session, type: **quit**

30. Remove the /bin/false entry from the /etc/shells file and reassign /bin/sh as labuser1's shell.
(hint: **dtpad** `^` `/etc/shells`) (hint: **usermod** `^` `-s` `/bin/sh` `^` `labuser1`)

31. Finger is a service that gives us the ability to find out information on other users on other systems. Its very nature is intrusive. It is an unnecessary service that can be turned off. Lets use the usermod command to alter some information about labuser2.

32. # **usermod** `^` `-c` `"(your name) loves Unix"` `^` `labuser2`

33. Lets use finger to retrieve labuser2's account information. # **finger** `^` `labuser2@localhost`

fingerd	
Vulnerability	Countermeasure
<p>The Finger daemon can leak sensitive system information like usernames, home directories, and login patterns.</p> <p>The Finger daemon has a built in denial of service (DOS) vulnerability.</p> 	<p>❑1. IAW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, as stated in a number of previous alerts, unused or unnecessary ports and services should not be active. Disable and/or disable at the network layer if possible all unused and necessary ports and services, e.g., rpc, tftp, gopher, smtp, http, finger, netstat, etc. Conduct risk assessments to determine if that port must remain open.</p> <p>Finger can provide a would-be intruder with a lot of information about your host.</p> <ul style="list-style-type: none"> • CONSIDER the finger information you provide and think about reducing the content by disabling finger or by replacing it with a version that only offers restricted information. <p>NOTE: Other services such as rusers and netstat may give out similar information.</p> <pre>#grep finger /etc/inetd.conf</pre> <p>To disable fingerd, put # in front of the line that starts with fingerd in /etc/inet/inetd.conf or /usr/sbin/inetd.conf</p> <ul style="list-style-type: none"> • CONSIDER restricting access to finger (client service) by changing the permissions to 500. <pre>#chmod 500 /usr/bin/finger</pre>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<ul style="list-style-type: none"> • DO NOT use GNU finger v1.37 as it may allow intruders to read any file.
--	--

34. Did you see that the name column says  love Unix? _____
35. Lets see where the source info comes from for a finger search. # **cat**  /etc/passwd
36. Do you see your entries from step 32 recorded in labuser2's information? _____
37. Now shut down the finger service. On your own, edit the /etc/inetd.conf file to turn off finger, stop and restart the inetd. If you are having trouble doing this, refer to PE SAS-8D steps 4 through 9.
38. Test the finger service by repeating step 33.
39. Did you successfully stop the finger service? _____
40. Could you stop other unnecessary network services in a similar manner? _____
41. Does the finger service still exist for internal users? _____
42. Test it: #**finger labuser2**
43. How would you disable the command for use by internal users?


44. END OF PE

Sendmail	
Vulnerability	Countermeasure
<p>Many vulnerabilities relate to buffer overflow and input validation attacks. In addition, Sendmail allowed attackers to pipe commands directly to sendmail for execution. It is also possible to gain privileged access.</p>	<p><input type="checkbox"/> 1. If you do not need Sendmail running, turn it off.</p> <ul style="list-style-type: none"> • Remove or rename the sendmail startup script located in /etc/rc2.d/S88sendmail. Then restart Unix. This will stop sendmail from listening to the network for incoming mail. • If you must run sendmail, do not run it as root. Build a chroot environment and  n it as a non-privileged user. • Sendmail is not required to listen to the network to send outgoing mail. You can set up cron so that sendmail will service the queue of outgoing messages

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

<p>Sendmail is a daemon that runs at root level.</p> <p>Older versions of sendmail allow spammers to relay mail through your system. In addition to abusing your resources, systems that participate in spamming can be listed on the RBL (Realtime Blackhole List). Many mail servers will disallow servers who try to connect from a mail server on the RBL.</p> <p>http://mail-abuse.org/rbl/</p>	<p>on a schedule.</p> <ul style="list-style-type: none"> • Stop sendmail from reporting the version during scans by editing the /etc/mail/sendmail.cf file. (change to SmtgreetingMeesage=\$j) • Stop the use of EXPN and VRFY. Edit /etc/mail/sendmail.cf to show: PrivacyOptions=authwarnings,noexpn,novrfy,goaway,restrictgrun,restrictmailq <p>See section 7 of this document for additional information.</p>
---	---

File Transfer Protocol (ftp)	
Vulnerability	Countermeasure
<p>Another widely exploited service is FTP. It transmits passwords in the clear, and could give attackers root access to your system. If you do not have a need to run ftp on your server, then it should be disabled.</p>	<p>❑1. DISABLE ftp if you are not an ftp server. FTP can be disabled by commenting out the ftp line in the /etc/inetd.conf file. Additional steps can be taken by commenting out port 21 in the /etc/services file.</p> <p>NOTE: If you run ftp, make sure the /etc/ftpusers file has the root and system account names listed. Also place any user account that you <u>do not</u> want to use ftp in this file.</p> <p>For additional information see section 7</p>

Practical Exercise SAS-8G

EXERCISE G



Network File System (NFS) Vulnerability PE

The purpose of this PE is to expose the student to the fundamental weakness of NFS. NFS allows for the accessing or sharing of files over the network. This PE has the student setting up a simple share, modifying the file, and checking the output for security issues.

This is a two partner PE and both partners will need to be logged in as root on their respective machines. When ever you see the reference to three x's (xxx), it refers to the last octet of the IP address. The \wedge symbol identifies where the space goes.

1. Both partner A and B will need to create a directory.



Type at the # prompt: **mkdir \wedge /testnfs**

3. Partner A needs to create a file in the /testnfs directory.

Type at the # prompt: **dtpad \wedge /testnfs/nfsfile**



3. Partner A needs to put some text in the open file and then save it. Once you've done that, go ahead and close dtpad.



4. Partner A needs to create a host table entry.

At the # prompt type: **dtpad \wedge /etc/hosts**

5. On a new line, create an entry for your partner's machine.



(example) **147.51.217.171 ws217171**

6. Partner A now needs to share the file out by making an entry in the distributed file system table. At the # prompt type: **dtpad \wedge /etc/dfs/dfstab**



7. Partner A needs to create a share entry which gives partner B access. Place the cursor on the beginning of the first free line and type the following entry.

share \wedge -F \wedge nfs \wedge -o \wedge rw=ws217xxx,root=ws217xxx \wedge -d \wedge "nfs test" \wedge /testnfs



8. Save your changes and close the text editor

9. Partner A needs to enable the share.

At the # prompt, type: **/etc/init.d/nfs.server \wedge start**

10. Partner A needs to set up the capturing of packets to analyze the network activity. The first IP to use is Partner B and the second is Partner A.

At the # prompt, type: **snoop \wedge -o \wedge nfscap \wedge 147.51.217.xxx \wedge 147.51.217.xxx**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

11. Partner B can now check to see if the share is available. You will use the dfshares command to check Partner A's machine for the share.
At the # prompt, type: **dfshares 147.51.217.xxx**
12. Partner B should see the share that Partner A made available. Now it is time to mount it to a directory for access. The IP is the IP of Partner A.
At the # prompt type: **mount -F nfs -o rw 147.51.217.xxx:/testnfs /testnfs**
13. Let's see if it allows for editing. Partner B will now edit the file on Partner A's machine.
At the # prompt, type: **dtpad /testnfs/nfsfile**
14. Partner B should see the file open up in the desktop editor (dtpad). Make some sort of modification to the message that Partner A originally created. Once you've done that, save the file and close the editor.
15. While this transaction was taking place, a counter on Partner A's machine should have been recording packets captured. Partner A needs to hit the control key and "c" key combination: **ctrl-C**. This will stop the capture of packets. Partner A should be able to open the file and see the new changes. At the # prompt, type: **dtpad /testnfs/nfsfile**
16. After viewing the file and making the appropriate comments to your partner, close the editor.
17. Partner A may now view the captured packet information. At the # prompt, type:
snoop -i nfscap
18. This will give you a read out of the captured packets. Remember the number of the very last packet captured as we will now look at the packets and their hexadecimal and ascii data. Lastnumber -20 refers to your last packet number and subtract 20 from that. Your screen buffer will not hold all of the packet data so we have to be selective. You may have to play with the packet numbers to view the packet data.
At the # prompt, type: **snoop -i nfscap -v -x 0 -p(lastnumber-20),(lastnumber-10)**
Example: **snoop -i nfscap -v -x 0 -p82,92**
19. scroll up through the packets until you arrive at the packet that corresponds to the modification that Partner B did to Partner A's text file when Partner B saved the file. You'll be looking at the lines starting with NFS.
20. The Ether header has the packet number, packet size, and time stamp. The IP header has the source and destination IP numbers. The TCP header has the source and destination port numbers. The RPC header has the user credentials like UID. The NFS header has the file handle number and the packet data payload.
21. The packets mention a file handle value. This is the number that is used to keep track of files within NFS. You will also notice that the port 2049 is used either as the source or destination port in each packet. The big thing to notice is that information that is shared in

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

this manner is totally visible to anyone with the ability to capture the packet. This is a clear text file sharing capability.

22. NFS should be avoided if possible. Use sftp or scp to transfer or share files. There are a few security options that can be set with NFS that we didn't set. The default mode in Solaris 9 is read only. We had to specifically give root write access for this PE. Normally we would also want to specify the `-nosuid` option when we mount the directory on the receiving end. Both the share and mount commands allow for specifying authentication mechanisms like Kerberos or DES.

23. End of PE.

Network File System (NFS)	
Vulnerability	Countermeasure
<p>NFS allows transparent access to files and directories of remote systems as if they were stored locally. The impact varies depending on which vulnerabilities are present. In the worst case, intruders gain unauthorized root access from a remote host.</p> <p>Sharing system related filesystems can occur when NFS is Misconfigured.</p> <p>Weak authentication is used. Requests can be spoofed or sometimes proxied through the local portmapper.</p>	<p>❑1. DO NOT use NFS if you do not need to export file systems.</p> <ul style="list-style-type: none"> • DISABLE NFS and related services, i.e. mountd, statd, and lockd. • Firewall protect your NFS server and block port 2049 on the firewall • Keep up on NFS security patches • Share information as "read only" whenever possible. • BE AWARE that you <u>implicitly</u> trust the security of the NFS server to maintain the integrity of the mounted files. NOTE: A "web of trust" is created between hosts connected to each other via NFS. That is, you are trusting the security of any NFS server you use. • Use strong authentication in the <code>/etc/nfssec.conf</code> file <p>Refer to the CERT Advisory 94:15. http://www.cert.org/advisories/CA-94.15.NFS.Vulnerabilities.html</p> <p>See section 7 of this document for additional information.</p>

UNIX Account Security

Practical Exercise SAS-9A

EXERCISE A

PURPOSE: To give students familiarity with the default UNIX user and system accounts & to understand the security implications in Section 4.0 of the UNIX checklist.

1. If you are not logged in as root, log in as root.

Determine which user accounts are currently active. Let's take a look.

2. At the command prompt #, type: **cat _^ /etc/passwd**

2A. Which accounts utilize password authentication? Can you determine if an account has a password with the /etc/passwd file? Why? ?

3. At the command prompt #, type: **ls _^ -l _^ /etc/passwd**

3A. What are the permissions on this file?

4. At the command prompt #, type: **cat _^ /etc/shadow**

4A. What is the difference between the /etc/passwd and /etc/shadow files? Is shadowing?

5. At the command prompt #, type : **ls _^ -l _^ /etc/shadow**

5A. What are the differences in permissions? What implication does this have for security? Is shadowing important?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

We've mentioned certain files that determine a user's operating environment, e.g. `.profile`, `.login`, and `.cshrc`. Let's see how these files can affect the execution of programs in a user's environment.

6. At the command prompt #, type: `ls -la /`
6A. Does the 'root' account have a `.profile`, `.login`, or `.cshrc` file in its home directory? Why? Should the root account have these types of files?
-

7. Logout of CDE.

8. Login as labuser1

Typically, `.profile`, `.login` or `.cshrc` files have a modification to the `PATH` statement. Let's see how the `PATH` environment variable can be a security vulnerability.

To exploit this vulnerability we need to create a script file. This script file will execute the `ls` utility with the appropriate argument(s), make a copy of the `ksh` shell and print two messages on the terminal window.

9. At the command prompt \$, type: `cd /tmp`
10. At the command prompt \$, type: `dtpad ls`

Add the following lines to the file :

```
#!/bin/sh
```

```
cp /usr/bin/ksh /tmp/.secret_ksh 2>/dev/null &  
chmod 4755 /tmp/.secret_ksh 2>/dev/null &  
echo "Hello world"  
echo "This could be a bad program"  
/usr/bin/ls $*
```

Select **File>Save** to save the file.

Right mouse click in the title bar and select **Close** to close the Text Editor.

To make the script file executable, use the following command to change permissions on the file.

11. At the command prompt \$, type: `chmod 755 ls`

Verify our script works by executing it.

12. At the command prompt \$, type: `/tmp/ls`

Verify the script is working correctly. On the terminal the following should be displayed:

1. the statement "Hello World" (without "")
2. the statement "This could be a bad program" (without "")

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

3. the files in the /tmp directory shall be displayed

Minimize the footprints you have left on the system.

13. At the command prompt \$, type: `rm ^ .secret_ksh`

14. Logout of CDE.

15. Login as root

You have just took over as System Administrator of an existing system. You would like to configure your environment on log in. Since the bourne shell is your startup shell you will create a .profile file.

16. At the command prompt #, type: `cp ^ /etc/skel/local.profile ^ /.profile`

17. At the command prompt #, type: `cat ^ .profile`

17A. Does the *.profile* have a 'path' statement? If so, is there anything in that path that could be considered vulnerability?



Let's modify the *.profile* to look first at the current directory for executables.

At the command prompt #, type `dtpad ^ .profile`

Move the `.` to the front of the PATH statement.

Originally the line looks like: `PATH=/usr/bin:/usr/ucb:/etc/.`

Change to `PATH=./usr/bin:/usr/ucb:/etc`

Select **File>Save** to save the file.

Right mouse click in the title bar and select **Close** to close the Text Editor.

It is standard practice as an administrator to periodically review the contents of the /tmp directory.

18. Logout of CDE.

19. Login as root

20. At the command prompt #, type: `cd ^ tmp`

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

21. At the command prompt #, type:

ls 

21A. What were the results of the running the script? Look carefully at the files that exist on the /tmp directory. Were any new files recently created ? If so, which ones?

21B. What would be the result if labuser1 were to login and execute the command /tmp/.secret_? (HINT- PE #1 Step 34)



Let's try to fix the vulnerability.

22. At the command prompt #, type: **dtpad  /.profile**

Modify the file so that the path statement does not have the .: .

Select **File>Save** to save the file.

Right mouse click in the title bar and select **Close** to close the Text Editor.

23. Logout of CDE.

24. Login as root

25. At the command prompt #, type: **cd  /tmp**

26. At the command prompt #, type: **ls  -a**

26A. Which ls did you execute this time (the one in /tmp or the standard system file) ?

Does the .secret_ksh file exist ? What security vulnerability does the .secret_ksh file present?

As you have seen in previous exerci, the su command (switch user), allows root to change into any user account without a password. UNIX will also allow ANY user to execute the su command. From a security point on view, this is NOT a good idea. So, let's restrict access to the 'su' command.

27. At the command prompt #, type: **ls  -l  /usr/bin/su**

27A. Who is the current owner? What is the current group? What are the file permissions? Who can execute this file? Who does it execute as (effective user id)? Is this a security vulnerability?



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

28. At the command prompt #, type: **su** _^ *labuser1*
29. At the command prompt \$, type: **/usr/bin/su**
When requested, enter the root account password.

28A. Was the switching user to root successful?

30. At the command prompt #, type: **exit** to quit the su session.
31. At the command prompt \$, type : **exit** to quit the su labuser1 session

Change the permissions on the su command such that only the owner and group can execute the file

32. At the command prompt #, type: **ls** _^ **-l** _^ */usr/bin/su*
33. At the command prompt #, type: **chmod** _^ **4550** _^ */usr/bin/su*
34. At the  command prompt #, type: **su** _^ *labuser1*

35. At the command prompt \$, type: **/usr/bin/su**
35A. Was the switching user to root successful? Why or why not?
-
-

36. At the command prompt \$ type: **exit**

Create a special group that will be utilized to identified users that can use the su command.

37. At the command prompt #, type: **admintool** _^ **&**

Create a new group called 'susers.' Click on 'Browse,' select 'Groups', then click on 'Edit,' then 'Add.' Accept the default group ID, make labuser1 a member of this group. Exit Admintool. 

38. At the command prompt #, type: **chgrp** _^ *susers* _^ */usr/bin/su*
39. At the command prompt #, type: **ls** _^ **-l** _^ */usr/bin/su*
39A. Did your changes take effect? (Is the group name different ?)
-

Let's test the new group.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

40. At the command prompt #, type: **su** *labuser2*

41. At the command prompt \$, type: **/usr/bin/su**

41A. Can you execute the 'su' command? Why?

42. At the command prompt \$, type: **exit**

43. At the command prompt #, type: **su** *labuser1*

44. At the command prompt \$, type: **/usr/bin/su**

When prompted, enter the root user password.

44A. Can you execute the 'su' command? Why?

45. Exit out of the root account (type **exit**).

46. Exit out of the labuser1 account (type **exit**)



Reading Assignment 5

Practical UNIX and Internet Security

Day 4

Pages 641 - 677



1. Which log file records if the *su* command was successful or ?

2. Which file records  the last time each user logged in?

3. Which file records who is currently logged in on a *tty* line?

4. What does the *last* command do?

5. How do you turn on accounting?

6. What information s the *aculog* file store?

7. Which option allows for logging incoming network services?

8. What is the *syslog* facility?



9. What is the SWATCH program?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Log files	
Vulnerability	Countermeasure
<p>Logs often harbor trace evidence of a crime. Logs are a good starting point to piece together what occurred on a computer system or network. Unfortunately, log files have an inherent vulnerability in that they may be forged and/or give misleading information. Securing the various log files on a UNIX system can mitigate this vulnerability.</p>	<p><input type="checkbox"/>1. I AW HQ DA SAIS-IAS message DTG R 050951Z MAR 99, all systems servers, as a minimum, shall have auditing turned on and reviewed for the following activities:</p> <ul style="list-style-type: none"> • all logins and attempts • all service connection requests • all ftp connections • all super user (root) connections, and requests.. <p>Logs often harbor trace evidence of a crime.</p> <ul style="list-style-type: none"> • DO determine where your log files are located. They are normally in the /var/log, /usr/adm, or /var/adm directories. <p style="text-align: center;">#find / -name *log -print</p> <p>Note – there is both a syslog file which is a text file and an executable file named syslog which is used to update the syslogd from third party and home grown software.</p> <p>Important log files:</p> <p><i>lastlog</i> – logs each user’s most recent successful login time, and possibly the last unsuccessful login too</p> <p><i>sulog</i> – logs use of the su command</p> <p><i>utmp</i> – records each user currently logged in</p> <p><i>utmpx</i> – extended <i>utmp</i></p> <p><i>wtmp</i> – provides a permanent record of each time a user logged in and logged out. also records system shutdowns and startups</p> <p><i>wtmpx</i> – extended <i>wtmp</i></p> <p><i>syslog</i> – a host-configurable, uniform system logging facility</p> <p><i>loginlog</i> – records bad logins attempts (after 5 tries)</p> <p><i>vold.log</i> – logs errors encountered with the use of external media, such as floppy disks/cdroms</p> <p><i>xferlog</i> – logs ftp access</p> <p><i>messages</i> – records output to the system console and other messages generated from the syslog</p> <p><i>acct</i> or <i>pacct</i> – records command run by every user (accounting)</p> <p><i>.history</i> - keeps a record of recent commands used by the user</p> <p><input type="checkbox"/>2. CONSIDER installing a PC or other machine as a</p>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	<p>network log server.</p> <p>☐3. REGULARLY monitor logs for successful and unsuccessful SU attempts. All su attempts are, by default, logged in /var/adm/sulog. This location is controlled in the /etc/default/su file. The entry: SULONG=/var/adm/sulog may be changed. #more /var/adm/sulog #more /var/adm/messages grep su</p> <p>☐4. ENSURE that you turn logging and debugging on for ftp Edit /etc/inetd.conf Modify the ftp entry as follows: ftp stream tcp nowait root /usr/sbin/in.ftpd in.ftpd -dl</p> <p>☐5. CAPTURE repeated login failures. Create file /var/adm/loginlog. This file does not exist by default. After 5 unsuccessful attempts on Solaris an entry is made in the log. This can be varied in the /etc/default/login file. #ls -l /var/adm/loginlog. If it does not exist as root, create /var/adm/loginlog #touch /var/adm/loginlog #chmod 600 /var/adm/loginlog #chgrp sys /var/adm/loginlog</p> <p>☐6. REGULARLY check for LOGIN REFUSED messages. #cat /var/adm/messages grep <i>keyword</i> more where <i>keyword</i> = FAILED, failed, FAILURES, su: or login:</p> <p>☐7. ENSURE that the permissions of all audit logs are set to 640 or more restrictive. #ls -al /var/log #chmod 640 /var/log/*</p> <p>Note : remember to update <u>all</u> logs; not all log files are found in /var/log</p> <p>RUN last periodically to see who has been using the system.</p> <ul style="list-style-type: none">• TURN on accounting for all users. This will log every command run by every user. <p>NOTE: This file will become quite large and should be either backed up or pruned daily.</p> <p><u>Syslog consists of 4 files</u> syslog() - an application program interface (API) logger - a Unix command used to add single line entries to a system log /etc/syslog.conf - configuration file used to control the</p>
--	---

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

	logging and routing of system log events. Syslogd - system daemon used to receive and route system log events from the syslog () and logger program.
--	---

Syslog priorities and sources	
Vulnerability	Countermeasure
<p>The daily/weekly requirement to review log files is complicated by the sheer volume of information available. Care should be taken to view log information that is relevant and important on a daily basis while lesser log entries can be viewed on a weekly basis.</p>	<p>□1. Log information is affixed a priority.</p> <ul style="list-style-type: none"> • Emerg - most immediate messages like system shutdown • Alert - system conditions require immediate attention • Crit - critical system conditions exist • Err - other system errors • Warning - warning messages • Notice - notices requiring attention at a later time • Info - informational messages • Debug - messages for debugging purposes <p>□2. Log information has an originating facility</p> <ul style="list-style-type: none"> • User (default) - generated by user processes • kern - generated by kernel processes • mail - generated by e-mail processes • daemon - generated by system daemons • auth - generated by authorization programs • lpr - generated by printing system • news - generated by usenet news system • uucp - generated by uucp system • cron - generated by cron and at • local 0 thru 7 - generated by up to eight locally defined categories • mark - generated by syslog itself for time stamping logs

Simple Watcher (SWATCH) (ACERT APPROVED)

- **CONSIDER** running an automatic log monitor such as Swatch. The Perl Compiler is required for installation.

SWATCH is a program that is designed to monitor system activity and filter log files. This package monitors and scans log files for pattern matches specified by the system administrator and takes action as specified by the system administrator. SWATCH's configuration file identifies what the program looks for and what it does when it locates a pattern match. SWATCH can react in three different ways to triggers: email; page; execute scripts.

CVE-MAP-NOMATCH /Bugtraq 4746: Under some circumstances, a message may not be reported by swatch. When an event occurs on a system numerous times, and swatch has placed a throttle on the event to prevent multiple alerts, swatch does not sufficiently handle events of the same type afterwards. When an event has occurred and alerts for the event are throttled, a bug in the swatch throttle code prevents swatch from reporting the event if it occurs a month later.

It is available from: <https://www.acert.belvoir.army.mil/ACERTmain.htm>

UNIX Auditing/Logging

Practical Exercise SAS 10A

EXERCISE A

This PE will familiarize you with some of the more important Unix log files and how to read or manipulate them. To do this PE, log into CDE as root and be at the root home directory of "/".

Commands to type are written in **bold**. Only type what is in bold. The **_** symbol indicates where you put in a space.

1. One of the logs in Unix tells you who is actually logged in the system and on what terminal. This log is a binary log called the utmpx file (utmp in older systems). It can be read by the "who" or "w" command. Other commands can access it but knowing these is fine for now. Type: # **who**

a. Who was listed as being actively logged on the system? _____

2. Another of the Unix logs tells us who is historically logging on the system. This log is referred to as the "lastlog" but normally is known as the wtmpx file (wtmp in older systems). The wtmpx file is a binary file that requires a special tool to read it. The command to use is the "last" command. Type: # **last**

a. Did you see a long list of logins? _____

b. Were any of the logins from IP addresses other than your own? _____

c. Were any of the logins for accounts you haven't used? _____

d. If you answered yes to b or c, you may have experienced some unauthorized visits during the class.

3. You can target individual users to verify their login habits or history.

a. Type: # **last_ labuser1**

b. Do you see the login history for labuser1? _____

4. Since the wtmpx file is binary and does not clean itself up, you have to take special steps to keep its size in check.

a. To archive the file, type: # **last_>_ /lastlog1**

b. Type: # **cat_ lastlog1**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

c. Do you see the wtmpx file in ascii format now, safely archived? _____

d. To zero out the file, pass a null value to it.

1. Type: # **cat /dev/null > /etc/wtmpx**

e. Test your efforts. Type: # **last**

f. Is the log empty? _____

g. Do you see a new log start date? _____

5. Process accounting is when the system keeps track of all commands that were ran and by whom they were ran. It is not a DA requirement to do process accounting as it takes a toll on system resources. It does, however, give you a complete picture of the goings on with respect to commands. Start up process accounting

a. Type: # **/usr/lib/acct/accton /var/adm/pacct**

b. Process accounting is now started. To read it you need to use special commands. The "acctcom" and "lastcomm" commands will do this for you.

c. Type: # **clear**

d. Type: # **ls**

e. Type: # **acctcom**

f. Type: # **lastcomm**

g. When you used acctcom and lastcomm, did you see the previous commands you ran? _____
Did you see that both commands read the /var/adm/pacct file but deliver a slightly different output? _____

6. Set up some of the reporting features within process accounting.

a. Type: # **/usr/lib/acct/runacct**

1. This will set up process report info. You may see mention of it failing or setting up of holidays. Ignore these for classroom purposes.

b. Type: # **acctcom**

c. Did you see the process accounting structured format? _____

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

- d. Type: `# /usr/lib/acct/prdaily|more`
1. This will print out a daily process report that can be viewed a page at a time. You will also notice that one page gives a record of the last time users logged in which is good for auditing account activities.
7. The general purpose logging facility known as "syslog" keeps track of errors and messages from numerous sources. Look at how it is configured.
- a. Type: `# cat/etc/syslog.conf`
1. Notice where different information is directed.
- b. Type: `# cat/var/adm/messages`
- c. Type: `# cat/var/log/syslog`
- d. Did you see some of the various errors or messages that have been generated during the class? _____
- f. Normally we only want to view the most current info.
1. Type: `tail-10/var/log/syslog`
 2. This views the last 10 entries in the /var/log/syslog file
- g. Type: `# dmesg|tail-10`
1. This will read the last 10 entries in the /var/adm/messages file
8. It is important to track super-user activity. The "sulog" tracks this information.
- a. Type: `# more/var/adm/sulog`
- b. Do you see the various times you became a different user during previous PE's?

- c. Check the sulog configuration: Type: `# cat/etc/default/su`

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

9. Set up logging of network services. Type: # **dtpad** **/etc/init.d/inetsvc**
- a. Go to the bottom of the file where the line containing "inetd -s " is. Edit it to look like "inetd -s **-t** " (do not put in quotation marks). Solaris 8 may also have a & symbol. Save the file.
 - b. Close the editor and check to see if /etc/rc2.d/S72inetsvc is also changed. S72inetsvc is a link of inetsvc. Type: # **cat** **/etc/rc2.d/S72inetsvc**
 - c. Do both files look identical? _____ A change to one is a change to both. /etc/rc2.d/S72inetsvc is a link of /etc/init.d/inetsvc.
 - d. Now edit the default inetd file. Type: # **dtpad** **/etc/default/inetd**
 - e. Un-comment (remove the # symbol) the line for enable_connection_logging=NO
 - f. Change the enable_connection_logging=NO to **YES**
 - g. Save the file and exit the dtpad program.
 - h. Next find the ID for the inetd process. In the terminal window, type: # **ps** **-ef** | **grep** **inetd**
 - i. Kill and restart the process, type: # **kill** **-HUP** **(PID#)**
 - j. Test the logging features, type: # **telnet** **localhost** **21**
Solaris 9 users will also type: **USER labuser1** (hit enter) **PASS student1** (hit enter)
 1. Type: **quit**
 - k. Type: # **telnet** **localhost** **79**
 1. Hit the enter key twice (2 times)
 - l. Type: # **dmesg** | **tail** **-10**
 1. Do the logs indicate some ftp or finger activity? _____
10. A big problem with logs are that they grow big and need to be kept in manageable sizes. Take a look at the current log sizes.
- a. Type: # **du** **-s** **-k** **/var/log/*** | **sort** **-rn**
 - b. Type: # **du** **-s** **-k** **/var/adm/*** | **sort** **-rn**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

c. Were you able to see some familiar log names and the size of the files? _____

1. The log sizes are shown in kilobytes.

d. Check the overall health of your file systems.

1. Type: `# df -k | awk '{print $6 "\t" $4}'`

2. Do you see the names of the directories and how many kilobytes of free space they have? _____

11. From time to time you will need to store files in an encrypted state. Encrypting sensitive data can be very useful.

a. Type: `# dtpad testfile`

b. Enter the text: **I am a test file with very little ambition in life.**

1. Save the file and close the editor

c. Type: `# cat testfile | crypt > testfile.cpt`

1. Enter: **password** when prompted for a key

d. Type: `# cat testfile.cpt`

e. Is the file encrypted? _____

f. Un-encrypt it. Type: `# cat testfile.cpt | crypt > testfile.new`

1. Enter: **password** when prompted for the key

g. Type: `# cat testfile.new`

1. Is the file unencrypted? _____

12. End of PE

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise SAS 10B

EXERCISE B

PURPOSE: To give students familiarity with setting up specialized Unix log files and observing the output.

1. Login as root

Create a log to collect failed login attempts. The /var/adm/loginlog file will collect failed login attempts. Bad login attempts will not be logged unless the /var/adm/loginlog file exists, is owned by root, the group is sys, and has read and write permissions only for root.

2. Open a Terminal Window.

3. At the command prompt #, type **touch** \wedge */var/adm/loginlog*

Change the group to sys.

4. At the command prompt #, type **chgrp** \wedge *sys* \wedge */var/adm/loginlog*

Change the permissions so that only root has read and write permissions.

5. At the command prompt #, type **chmod** \wedge *600* \wedge */var/adm/loginlog*

Verify your changes.

6. At the command prompt #, type **ls** \wedge *-l* \wedge */var/adm/loginlog*

7. Right click the background, left click Hosts and select Terminal Console.

8. Minimize the Console Window opened in step 7. **Do not close the window.**

9. In the Terminal Window, at the password prompt, type:

rlogin \wedge *localhost* \wedge *-l* \wedge *labuser1*

When a password is requested, enter a password of **duh**

10. At the login prompt type: **labuser1** with a password of **duh**

11. Repeat steps 10 four (4) more times.

12. Open the Console window by double clicking on the Console icon.

13. What message is displayed ?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

14. Close the Console window.

Check to see if the bad login attempts have been captured by the /var/adm/loginlog file.

15. On the Terminal Window, at the command prompt #, type **cat** _^ **/var/adm/loginlog**

16. You should see that the bad login attempts have been logged. Have they? _____

17. The log file will tell you the account that had the bad login attempts, the port used, and the date and time of the attempts. Which port was used during the attempted logins?

18. On the Terminal Window, at the command prompt #, type: **grep** _^ **FAILURES** _^ **/var/adm/messages** _^ | _^ **more**

19. What information is displayed?

End exercise.....

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Data Encryption System (DES) (ACERT APPROVED)

- **If possible, ALWAYS** super-encrypt with Triple-DES.
- **DO NOT** use the 40-bit DES algorithm for encryption (it has been broken).

DES is a kit that builds a DES encryption library. It supports numerous encryption modes including: Electronic Code Book (ecb), Cipher Block Chaining (cbc), Output Feedback (ofb), Cipher Feedback (cfb), Triple cbc, MIT's pcbc and has a fast implementation of crypt. It contains support routines to read keys from a terminal, generate a key from an arbitrary length string, read/write encrypted data from a file descriptor.

It can be found at: <https://www.acert.belvoir.army.mil/ACERTmain.htm>

- **NEVER** use a login password as an encryption key.
- **PROTECT** your encryption key as you would your password
- **PROTECT** your encryption programs against tampering.

Triple DES Algorithm

- Based on the DES algorithm. The encryption is performed three times with three different keys. The multiple encryptions result in a ciphertext that has an effective key size as large as the sum of the sizes of the three keys.
- If all three 64bit keys have the same value, the algorithm is no stronger than DES.

Advanced Encryption Standard (AES)

- A new algorithm to use in place of DES. It utilizes the Rijndael algorithm.
- AES has a private key symmetric block cipher similar to DES
- AES is stronger and faster than DES. Encrypts at 70.2 Mbps versus DES at 28 Mbps.
- AES has a life expectancy of 20 to 30 years
- AES supports key sizes of 128 bit, 192 bit, and 256 bit.

Pretty Good Privacy (PGP)

- **USE** PGP (where authorized, if practical) to encrypt files and sensitive email, and to create and check digital signatures on important files.
- **VERIFY** the digital signature of any signed files. Tools like PGP may be used to sign files and to verify those signatures.

PGP implements encryption and authentication.

It can be found at: <ftp://ftp.ox.ac.uk/pub/pgp/unix/>

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Message Digest 5 (MD5) (ACERT APPROVED)

- **USE** a message digest program, such as MD5 or SHA-1. **MD5** is a message digest algorithm. If no digital signature is supplied but an md5 checksum is supplied, then verify the checksum information to confirm that you have retrieved a valid copy.
- **Creates** a 128 bit message digest

It can be found at: <ftp://coast.cs.purdue.edu/pub/tools/unix/md5/>

SHA-1

- **USE** a message digest program, such as MD5 or SHA-1. **SHA-1** is a message digest algorithm. If no digital signature is supplied but an SHA-1 checksum is supplied, then verify the checksum information to confirm that you have retrieved a valid copy.
- **Creates** a 160 bit message digest.
- **Stronger but slower than MD5**

It can be found at: <ftp://coast.cs.purdue.edu/pub/tools/unix/md5/>

SunScreen Secure Net (ACERT APPROVED)

Type of Firewall: Proxy and stateful-inspection

Operating System: Solaris and Solaris X68

Latest Version: 3.1

Features:

- Stealth and routing design, hardened OS
- Dynamic and proxy filtering (SMTP, HTTP, FTP, Telnet)
- Remote administration and central management
- High availability and scalability
- SPARC and INTEL hardware, ATM (CIP or LANE), FDDI, token ring, or Ethernet (10, 100, and Gigabit)

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

DISCOVERING A BREAK-IN

(Note: The following information was taken in its entirety from the Software Engineering Institute, Carnegie Mellon University)

U.S. Government only

Software Engineering Institute authored documents are sponsored by the U.S. Department of Defense under Contract F19628-95-C-0003. Carnegie Mellon University retains copyrights in all material produced under this contract. The U.S. Government retains a non-exclusive, royalty-free license to publish or reproduce these documents, or allow others to do so, for U.S. Government purposes only pursuant to the copyright license under the contract clause at 52.227-7013.

References:

ftp://info.cert.org/pub/tech_tips/intruder_detection_checklist
ftp://info.cert.org/pub/tech_tips/UNIX_configuration_guidelines
ftp://info.cert.org/pub/tech_tips/security_tools
ftp://info.cert.org/pub/tech_tips/root_compromise
<http://www.porcupine.org/satan/admin-guide-to-cracking.html>

Log files

□1. **EXAMINE** log files for connections from unusual locations or other unusual activity. For example, look at your **last** log, process accounting, all logs created by **syslog**, and other security logs.

If your firewall or router writes logs to a different location than the compromised system, remember to check these logs also. Note that this is not foolproof unless you log to append-only media; many intruders edit log files in an attempt to hide their activity.

SetUID & SetGID files

□1. **LOOK** for setuid and setgid files (especially setuid root files) everywhere on your system. Intruders often leave setuid copies of `/bin/sh` or `/bin/time` around to allow them root access at a later time. The UNIX `find(1)` program can be used to hunt for setuid and/or setgid files. For example, you can use the following commands to find setuid root files and setgid `kmem` files on the entire file system:

```
# find / -user root -perm -4000 (-print as required)
#find / -group kmem -perm -2000 (-print as required)
```

- Note that the above examples search the entire directory tree, including NFS/AFS mounted file systems. Some `find(1)` commands support an `"-xdev"` option to avoid searching those hierarchies.

For example:

```
#find / -user root -perm -4000 -print -xdev
```

- Another way to search for setuid files is to use the `ncheck(8)` command on each disk partition. For example, use the following command to search for setuid files and special devices on the disk partition `/dev/rsd0g`:

```
#ncheck -s /dev/rsd0g
```

System binaries

□1. **CHECK** your system binaries to make sure that they haven't been altered. We've seen intruders change programs on UNIX systems such as `login`, `su`, `telnet`, `netstat`, `ifconfig`, `ls`, `find`, `du`, `df`, `libc`, `sync`, any binaries referenced in `/etc/inetd.conf`, and other critical network and system programs and shared object libraries. Compare the versions on your systems with known good copies, such as those from your initial installation media. Be careful of trusting backups; your backups could also contain Trojan horses.

Trojan horse programs may produce the same standard checksum and timestamp as the legitimate version. Because of this, the standard UNIX `sum(1)` command and the timestamps associated with the programs are not sufficient to determine whether the programs have been replaced. The use of `cpm`, `MD5`, `Tripwire`, and other cryptographic checksum tools is sufficient to detect these Trojan horse programs, provided the checksum tools themselves are kept secure and are not available for modification by the intruder. Additionally, you may want to consider using a tool (PGP, for example) to "sign" the output generated by `MD5` or `Tripwire`, for future reference

Monitoring programs

□1. **CHECK** your systems for unauthorized use of a network monitoring program, commonly called a sniffer or packet sniffer. Intruders may use a sniffer to capture user account and password information.

- For related information, see CERT advisory CA-94:01 available in http://info.cert.org/pub/cert_advisories/CA-94:01.network.monitoring.attacks

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Cron & at jobs

- 1. **EXAMINE** all the files that are run by **cron** and **at**. We've seen intruders leave back doors in files run from **CRON** or submitted to **at**. These techniques can let an intruder back on the system (even after you believe you had addressed the original compromise). Also, verify that all files/programs referenced (directly or indirectly) by the **cron** and **at** jobs, and that the job files are not world-writable.

Unauthorized services

- 1. **CHECK** for unauthorized services. Inspect `/etc/inetd.conf` for unauthorized additions or changes. In particular, search for entries that execute a shell program (for example, `/bin/sh` or `/bin/csh`) and check all programs that are specified in `/etc/inetd.conf` to verify that they are correct and haven't been replaced by Trojan horse programs.
 - Also **CHECK** for legitimate services that you have commented out in your `/etc/inetd.conf`. Intruders may turn on a service that you previously thought you had turned off, or replace the `inetd` program with a Trojan horse program.

Password file

- 1. **EXAMINE** the `/etc/passwd` file on the system and check for modifications to that file. In particular, look for the unauthorized creation of new accounts, accounts with no passwords, or UID changes (especially UID 0) to existing accounts.

Configuration files

- 1. **CHECK** your system and network configuration files for unauthorized entries. In particular, look for '+' (plus sign) entries and inappropriate non-local host names in `/etc/hosts.equiv`, `/etc/hosts.lpd`, and in all `.rhosts` files (especially `root`, `uucp`, `ftp`, and other system accounts) on the system. These files should not be world-writable. Furthermore, confirm that these files existed prior to any intrusion and were not created by the intruder.

Hidden or unusual files

- 1. **LOOK** everywhere on the system for unusual or hidden files (files that start with a period and are normally not shown by `ls`), as these can be used to hide tools and information (password cracking programs, password files from other systems, etc.). A common technique on UNIX systems is to put a hidden directory in a user's account with an unusual name, something like `'...'` or `'.. '` (dot dot space) or `'..^G'` (dot dot control-G). Again, the `find(1)` program can be used to look for hidden files, for example:

```
#find / -name ".. " -xdev (-print as required)
```

```
#find / -name ".*" -xdev | cat -v (-print as required)
```

Also, files with names such as `'xx'` and `'mail'` have been used (that is, files that might appear to be normal).

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Local machines

1. **EXAMINE all machines on the local network when searching for signs of intrusion. Most of the time, if one host has been compromised, others on the network have been, too. This is especially true for networks where NIS is running or where hosts trust each other through the use of .rhosts files and/or /etc/hosts.equiv files. Also, check hosts for which your users share .rhosts access.**

Create a Unix Response Toolkit

1. **When investigating an incident, it is vital to have trusted commands on hand. Create a CD or floppy disk with the following tools:**

- **ls, dd, des, file, pkginfo, find, icat, lsof, md5sum, netcat, netstat, pcat, perl, ps, strace, strings, truss, df, vi, cat, more, gzip, last, w, rm, script, hash, modinfo, lsmod, ifconfig**

Protect the Evidence

1. **When an incident is suspected, preserve the evidence by making a duplicate of the evidence media. Perform the investigative steps on the restored image. Freezing the scene is key to preserving evidence. Evidence has differing levels of volatility. It can be in places such as the processor registers, kernel data structures in memory, swap space, network data structures and counters, user process memory and stacks, file system buffer cache, the file system itself, etc.**

Conducting a Unix investigation

- 1. Review **all pertinent logs**
- 2. Perform **key word searches**
- 3. Review **relevant files**
- 4. Identify **unauthorized user accounts or groups**
- 5. Identify **rogue processes**
- 6. Check for **unauthorized access points**
- 7. Analyze **trust relationships**
- 8. Maintain a chain of custody on any evidence collected.