

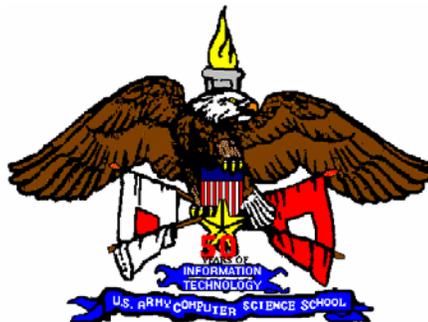
**United States Army Signal Center and Fort Gordon
Fort Gordon, Georgia 30905-5144**



**School of Information Technology
Information Assurance Division**

**Network Manager Security Course
Week Two**

10 September 2004



PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Table of Contents

Introduction and Orientation.....	2
Incident and Vulnerability Reporting.....	8
Network Threats.....	24
Reading assignment 1.....	40
Fundamentals of Cryptography.....	42
Encryption.....	55
PKI Practical exercise.....	20
Fault Tolerance.....	75
Microsoft Internet Information Server Security.....	81
Reading assignment 2.....	93
IIS Practical exercise.....	95
Cisco Routers.....	109
Router Practical exercises.....	129
Reading Assignment 3.....	141
Firewalls.....	142
Symantec Enterprise Firewall.....	151
Firewall Practical exercise.....	167
Reading Assignment 4.....	184
Real Secure.....	185
IDS Practical exercises.....	199



Introduction and Orientation

Module 1

September 20, 2004

1-1



Lesson Objectives

- Course Information
- Meet the Instructor
- Course Objectives
- Course Ground Rules
- Student Introductions
- Course Outline

September 20, 2004

1-1

Course Information



- Title
 - ◆ System Administrator / Network Manager Security Course, course number 7E-F66/531-F21 (CT)
- Location
 - ◆ 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
 - ◆ 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

September 20, 2004

1-1

Your Staff



Mr. Randy McNeil – Chief, IA Training

Instructors

Mr. Larry McLean (NMS) Mr. Paul Gozaloff (NMS)

Mr. Kelly Larsen (SAS) Ms. Sue Clark (NMS)

Ms. Cynthia Jones (SAS) SFC LaBranche (NMS)

SFC Jedrusiejko (SAS)

Webmaster

Mr. Rodney Driggers



September 20, 2004

1-1

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 20, 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



September 20, 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 20, 2004

1-1

Course Outline



- Day 1
 - ◆ Introduction
 - ◆ STAT Scanner and IAVA discussion
 - ◆ Begin W2K Security Check List



September 20, 2004

1-1

Course Outline



- Day 2
 - ◆ Continue with W2K Security Check List and Lab Work
- Day 3
 - ◆ Continue with W2K Security Check List and Lab Work
 - ◆ Begin Unix Security Check List and Lab Work
- Day 4
 - ◆ Continue with Unix Security Check List and Lab Work

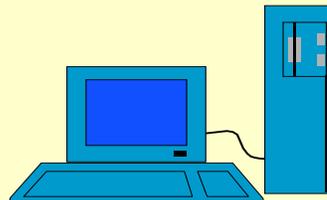
September 20, 2004

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 20, 2004

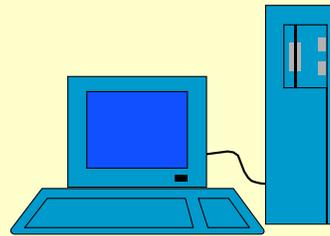
1-1

Course Outline



- Day 6
 - ◆ ACERT Brief /Network Vulnerabilities
 - ◆ Military Intelligence Brief

- Day 7
 - ◆ Encryption
 - ◆ Web Server Vulnerabilities



September 20, 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 20, 2004

1-1

Incident and Vulnerability Reporting

Module 04

Lesson Objectives

- Identify information system related incidents and vulnerabilities
- Describe how to detect and report incidents and vulnerabilities



Incidents and Violations

- Incident - Unexpected behavior by an information system that yields abnormal results or indicates unauthorized use or access, unexplained outages, denial of service, loss of accountability, or the presence of a virus

September 20, 2004

4-1



Incidents and Violations

- Technical Vulnerability - A hardware, firmware, communication, or software weakness which leaves a computer processing system open for potential exploitation or damage, either externally or internally.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Windows #1

- Internet Information Service:
 1. Failure to handle unexpected requests.
 2. Buffer Overflows
 3. Sample Applications

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Windows #2

- Microsoft SQL Server (MSSQL):
 1. Recently exposed for it's plethora of security issues in May 2002 by the MSSQL Worm.
 2. Remote leaking of information.
 3. Remote compromise.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Windows #3

- General Windows Authentication:
 1. Weak, or nonexistent passwords.
 2. Failure to protect passwords.
 3. LM, NTLM v1/2 authentication has exceptionally weak password protection.
 4. Password hashes are available to anyone.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Windows #4

- Internet Explorer:
 1. ALL existing versions of IE have critical vulnerabilities.
 2. Default web browser installed with all versions of Windows.
 3. web page spoofing, ActiveX control vulnerabilities, Active scripting vulnerabilities, buffer overflows.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Windows #5

- Remote Access Service:
 1. Netbios, SMB and Common Internet File System (CIFS) protocols can expose critical files.
 2. Remote Registry access
 3. RPC/ Anonymous logons

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Windows #6

- Microsoft Data Access Components (MDAC):
 1. Remote Data Services (RDS) of MDAC have a flaw which allow execution of local commands with administrative privilege.
 2. Combined with MS Access, can provide anonymous external access to internal databases.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Windows #7

- Windows Scripting Host:
 1. This is how the “Love Bug” propagated.
 2. Visual Basic Script (VBS) is the most commonly used method.
 3. Windows Scripting Host (WSH) permits any text file with certain extensions to be executable.
 4. Either viewing, or even PREVIEWING these files can cause execution.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Windows #8

- Outlook and Outlook Express --
 1. Patches and updates
 2. Automated preview pane
 3. Executes any code embedded in html or links

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Windows #9

- Peer to Peer (P2P) file sharing:
 1. Improper security settings can permit remote access to the system registry.
 2. Hackers can use this to adjust system settings, and file associations in order to enable execution of malicious code.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Windows #10

- Simple Network Management Protocol:
 1. Blank or default SNMP community names. (Public, Private)
 2. Guessable SNMP community names.
 3. Hidden SNMP community strings. .

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Unix #1

- The Berkeley Internet Name Domain (BIND) Domain Name System (DNS):
 1. Most widely used DNS system on the internet.
 2. Vendor is quick to supply security fixes.
 3. Outdated and misconfigured servers still exist everywhere.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Unix #2

- Remote Procedure Calls (RPC):
 1. RPC is a widely used method of distributed networking.
 2. Multiple flaws commonly exploited.
 3. Often run as root

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Unix #3

- Apache Web Server:
 1. Apache Mod_SSL Worm
 2. Apache chunk handling exploit
 3. No web server can be considered secure until considered in the context of it's interaction with web applications.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Unix #4

- General Unix Authentication:
 1. Same issues as General Windows Authentication.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Unix #5

- Clear text services:
 1. Authentication data is transferred in clear text.
 2. R-Services (rsh, rcp, rlogin, etc)
 3. FTP servers can result in full system compromise.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Unix #6

- Sendmail:
 1. Widespread use across internet makes it a prime target for attackers resulting in multiple exploits over the years.
 2. Most exploits are only against older versions. Sendmail has not had a “high” severity vulnerability in over 2 years.
 3. Outdated/misconfigured servers.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Unix #7

- Simple Network Management Protocol (SNMP):
 1. Authentication protocols implemented have serious exploitable vulnerabilities.
 2. Older, unpatched versions of SNMP (ver. 1 and 2) use unencrypted “community strings” for authentication.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Unix #8

- Secure Shell (SSH):
 1. Improperly maintained SSH servers may be vulnerable.
 2. Possible remote root compromise.
 3. Mostly small bugs, but some major security issues if not updated.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Unix #9

- Misconfiguration of NIS/NFS
 1. Allow access to the NIS and NFS servers only from authorized clients .
 2. buffer overflows, DoS and weak authentication .
 3. Poor host-authentication.

September 20, 2004

4-1

■ TOP 20 Security Vulnerabilities Unix #10

- Open Secure Sockets Layer (SSL):
 1. Attacking applications using SSL.
 2. Several versions of SSL contain buffer overflows that can lead to arbitrary code ran on system.

September 20, 2004

4-1



Incidents and Violations

- Violation - Failure to comply with the policies and procedures established which could reasonably result in the loss or compromise of classified information

September 20, 2004

4-1



Examples of Security Violations

- Removal of classified information
- Wrongful disclosure of classified information
- Introduction of high risk software
- Introduction of malicious code
- Sharing passwords

September 20, 2004

4-1



Indicators of a Reportable Incident

- Suspected intrusions
- Unauthorized access attempts
 - System or system resources
- Unexplained file modifications
- Unexplained output

September 20, 2004

4-1



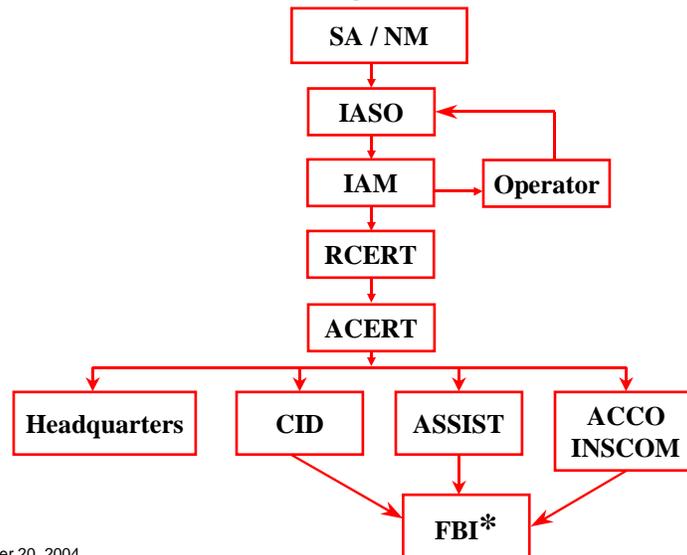
Indicators of a Reportable Incident

- Security system failures
- Abnormal system responses
- Malicious software
- Network intrusion alerts
- Anything “alarming”

September 20, 2004

4-1

Army Reporting Structure



September 20, 2004

4-1

The Security Incident Report

- Report incident to IASO
 - Information system name and/or number
 - Location
 - Date and time
 - Description
 - Impact
 - Any pertinent information
- IASO investigates and advises IAM

September 20, 2004

4-1



The Security Incident Report

- IAM advises community
- ACERT advises IAM and IASO
 - Further guidance
 - Further reporting requirements
- Vulnerability assistance

September 20, 2004

4-1



Summary

- The Army has a clear incident reporting chain of command
- Roles and responsibilities are established for your support
 - IASOs, IAMs, LIWA
- Incidents are to be reported
 - Contact Your IASO Immediately

September 20, 2004

4-1

Network Security Threats and the Hacker

Threats

- Threat Definition
 - A circumstance or event that could exploit or cause harm by violating security
- Threat Assessment
 - Consider the likelihood and possible impact of the threat
- Threat Objectives
 - Information Leakage – Viruses
 - Integrity Violation – Illegitimate Use
 - Denial of Service

5-1



Threat Methods

- Masquerading, forging, or spoofing
- Playback or replay
- Bypassing security controls
- Authorization violations or misuse of authority
- Network Attacks:
 - Smurf - Teardrop
 - Zombie - Land
 - OOB - Fuzz
- Traffic analysis network scanning
- War dialing
- Malicious code
- Back doors
- Media scavenging
- Dumpster diving
- Social engineering

5-1



Internal vs. External Threats

- Internal (Insider) Threats
 - Systems administrator, network manager, system operator, programmer, or user
 - Potential reasons
 - Fired or disgruntled
 - Coerced, greedy or financially strapped
 - Lazy or untrained
 - For the thrill or challenge
- External (Outsider) Threats
 - Foreign intelligence agent, terrorist, criminal, intruder.....HACKER!!!

5-1



Pre-Hacking

- Footprinting
- Scanning
- Enumeration

5-1



Footprinting

The act of creating a profile of your target.

This profile includes the technologies used by your target.

5-1



Technologies sought out in Footprinting

- Internet
- Intranet
- Remote Access
- Extranet

(A Hacker Needs A Way In)

5-1



Internet

- Domain Names
- Static IP's
- TCP & UDP Services Running
- System Architecture (SPARC/X86)
- Firewall and Router ACLs
- Intrusion Detection Systems
- User and Group Names

5-1



Intranet

- Networking Protocols in Use
- Internal Domain Names
- Internal Static IP's
- TCP & UDP Services Running
- System Architecture (SPARC/X86)
- Firewall and Router ACLs
- Intrusion Detection Systems (IDS)
- User and Group Names

5-1



Remote Access

- Analog/Digital Telephone Numbers
- Type of Remote System
- Authentication Mechanisms

5-1



Extranet

- Connection Origination and Destination
- Type of Connection
- Access control Mechanism

5-1



Footprint Summary

The ultimate goal when a hacker footprints is to gain the following type of information:

1. Employee Names & Phone Numbers
2. IP Address Ranges
3. DNS Servers
4. Mail Servers
5. Outline of the Software and Hardware used by the company

5-1



Scanning

After Footprinting it's time to take a look at the systems we gathered information about and see what is alive on them.

Tools Used

- Ping Sweeps (ICMP Queries)
- Port Scans
- Automated Discovery Tools

5-1



ICMP ECHO Scan Prevention

- There are 13 types of ICMP traffic
- At Minimal the Following Can Be Let In
 1. ICMP ECHO-REPLY
 2. HOST UNREACHABLE
 3. TIME EXCEEDED

5-1



Why is ICMP a vulnerability?

- If you compromise a system you can back-door the operating system and tunnel data within an ICMP ECHO packet. A program most commonly used to do this is Loki.

5-1



ICMP Query Countermeasure

- Block ICMP type 17 = ADDRESS MASK
Block ICMP type 13 = TIMESTAMP
- This will keep an intruder from gaining knowledge of the subnets being used.

Example:

```
Access-list 101 deny ICMP any any eq 13
```

```
Access-list 101 deny ICMP any any eq 17
```

5-1



Port Scanning

- The process of connecting to TCP and UDP ports on a target system to determine which services are running.
- A running service may be a potential access point on the target.

5-1



Port Scanning Objectives

- Identifying both the TCP and UDP services running on the target system
- Identifying the type of operating system of the target system
- Identifying specific applications or versions of a particular service.

5-1



Port Scan Types

- TCP connect scan
- TCP SYN scan
- TCP FIN scan
- TCP Xmas Tree scan
- TCP Null scan
- UDP scan

5-1



Port Scan Types

- TCP connect scan - Completes a full three-way handshake (SYN, SYN/ACK, and ACK) Easily detected.
- TCP SYN scan - Also called “half-open scanning” because a full TCP connection is not made. (SYN, SYN/ACK, RST/ACK)

5-1



Port Scan Types

- TCP FIN scan - Sends a FIN packet, this will get the target to send back a RST for all ports that are closed. Usually only works on UNIX machines.
- TCP Xmas Tree scan - This sends a FIN, URG, and PUSH packet to the target. This usually gets an NT system to speak. The system will send an RST for all closed ports

5-1



Port Scan Types

- TCP Null scan - This is supposed to turn off all flags, and get the system to send back an RST for all closed ports.
- UDP scan - These are usually unreliable. It sends a UDP packet to the target, if the target responds with an "ICMP port unreachable" this lets us know that the port is closed.

5-1



Port Scan Results

- A successful port scan will yield the following results:
 1. Port# 21, 23, 80 etc...
 2. State open/closed
 3. Protocol TCP/UDP
 4. Service Ftp, SMTP, Http, Finger etc...

5-1



Port Scan Countermeasures

- Intrusion Detection Systems
- Shut down all services that are not necessary.

5-1



Automated Discovery Tools

- Due to the many differences in IP stack implementations between different Vendors operating systems. It is virtually impossible to prevent detection of the operating system running in a Intranet environment. In a Internet environment the best protection is a good bodyguard (Firewall/Proxy).

5-1



Enumeration

- Enumeration involves active connections to systems.
- Is very risky from a Hacker Standpoint
- Enumerated information can be grouped into the following areas:

- 1. Network resources and shares**
- 2. Users and groups**
- 3. Applications and banners**

5-1



Enumerating NT Domains

- Standard Net View Commands (Domains and Computer List)
- NT Resource (Hacking) Kit
 - Nltest (List PDC/BDC)
 - Rmtshare (Like Net View)
 - Srvcheck (Shares & Authorized Users)
 - Srvinfo (Lists Shares)

5-1



NT Domain Countermeasure

- Tough to countermeasure
- Service packs, security rollups, and hotfixes
- Apply your System Security Checklist.
- Audit your systems regularly
- Host Intrusion Detection. (Tripwire, Tiger, SARA, etc.)

5-1



Miscellaneous NT Enumeration

- Edump, Getmac, Netdom, Netviewx
(Shows services bound to IP #s and Ports)
(Shows MAC #'s)
(Probe for RAS Service)

5-1



Countermeasure

- Filter TCP and UDP ports 135-139 at perimeter network access devices.

5-1



Username Enumeration

- Almost half of the puzzle!!!
- NBTSTAT
- sid2user - Good for getting Admin acct.
- user2sid
- Once SID is gained, can determine which is administrator account.
- These will work even if RestrictAnonymous is enabled

5-1



Username Countermeasures

- Block port 139 from all perimeter networks.
- Difficult to block internally.

5-1

Reading assignment 1

Subject: **Encryption, Signatures, Hashes, and Certificate Authorities**

Pages: 89-95, 115-161, 177-201 (Cryptography Decrypted)

(Complete before day 2)

1.  What services do digital signatures provide?

2.  Define Non-Repudiation:

3.  Define some of the differences between RSA and DSA.

4.  What other names are used for a hash?

5.  What is the purpose of using a hash?

6.  What assurances are provided by message digests?

7. Define them:

8.  Define 3 non-keyed digests and their sizes:

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

9.  What are the 2 major PKI frameworks?

10.  Briefly describe them:

11.  What is a Certificate Authority?

Fundamentals of Cryptography and Public Keys

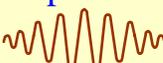
Module 6

Lesson Objective

- Introduce basic concepts of cryptography
- Understand how conventional encryption works.
- Understand public key encryption.
- Understand how hashing works.
- Understand how key length determines security.



Cryptography (Secret Writing)

- Encryption: Transform plaintext into ciphertext
Plaintext →  → **HK\$**
- Decryption: Transform ciphertext into plaintext
HK\$ →  → **Plaintext**
- Algorithms: Control specific encryption and decryption process

September 20, 2004

6-1

Ciphers

- Substitution Cipher: Replace bits or bytes
Example - Caesarian Cipher which is shift up 3
The enemy is nigh = Wkh hqhpv lv qljk
- Transposition Cipher:
Example - Transposition rotate three characters right
The enemy is nigh = ene myisn ig hthe
- Substitution and Transposition (modern algorithm)
The enemy is nigh = hqh pblvq lj kwkh

September 20, 2004

6-1

Security Services Supported by Cryptography

- Confidentiality
- Integrity
- Basic-authentication (Assumption)
- Non-repudiation



September 20, 2004

6-1

Algorithms

- A math formula that determines how data is encrypted or decrypted with a key.
- Three primary algorithm types:
 - Symmetric or conventional encryption or secret key
 - Asymmetric or public key encryption
 - Hashing
- Two ways to attack an encrypted message.
 - Systematic trial of each key used in the algorithm
 - Figure out a way to solve the algorithm without going through every calculation
- Randomness is important.



September 20, 2004

6-1

Cryptographic Components

- Three components of cryptography

- Data to be encrypted
- Algorithm to encrypt with

An Algorithm is the “method” used to encrypt.

- Key to use with the Algorithm

The Key is used to change the resulting ciphertext normally received from use of the Algorithm.

September 20, 2004

6-1

Conventional Encryption (Symmetric Key)

- Encryption and decryption processes use the same key.
- This key must be protected against compromise.
- Secret key encryption provides confidentiality and a basic authentication service.
- Standard secret key encryption does not provide a non-repudiation service (or good authentication).
- Normally uses a proven algorithm to encrypt or decrypt.



September 20, 2004

6-1

Point-to-Point Encryption Using Conventional Encryption



September 20, 2004

6-1

Hashing

- Sender and recipient use identical key to compute a hash value sometimes called an ICV or a message digest (SHA-1 or MD-5).
- Key is known only to the sender and recipient.
- The hash value or ICV is computed on the message to be sent (by the sender) and attached to the message.
- If the message is change by 1 bit then the hash value is altered.
- If the ICV computed by recipient matches ICV received, then message is accepted.

September 20, 2004

6-1

Conventional Encryption (Secret Key)

- Advantages
 - Faster – smaller key lengths.
 - Math algorithm is straight forward usually cannot be broken (it is not theoretical).
- Disadvantages
 - No true means of authenticating sender and of course this means no capability of a digital signature.
 - Breaking one key can compromise multiple parties.
 - Does not scale well (if you use unique keys between all parties).

September 20, 2004

6-1

Public Key Cryptography (Asymmetric Encryption)

- Digital Certificate – normally a set of keys, 1 private, 1 public (with other information, like ID).
- Public key encryption is asymmetric
 - The sender and receiver do not use the same key to encrypt/decrypt.
 - The math algorithm ensures this (it uses prime numbers).
 - If something is encrypted with a public key it cannot be decrypted with the same public key.
 - Public keys can be shared because of this.
 - The public key of the destination is used to encrypt

September 20, 2004

6-1

Public Key Encryption with Authentication

- Public Keys can be used to authenticate messages because the opposite is also true.
 - What is signed with a private key (of the sender) can only be verified with a public key (of the sender).
 - Private keys of the sender are not used to encrypt but are used to digitally sign.
 - Everyone can verify a private key.
- With Public Key Encryption
 - Encryption uses the public key of the recipient.
 - Decryption uses the private key of the recipient.
 - Signing uses the private key of the sender.
 - Authentication uses the public key of the sender.

September 20, 2004

6-1

Point-to-Point Encryption Using Public Key



September 20, 2004

6-1

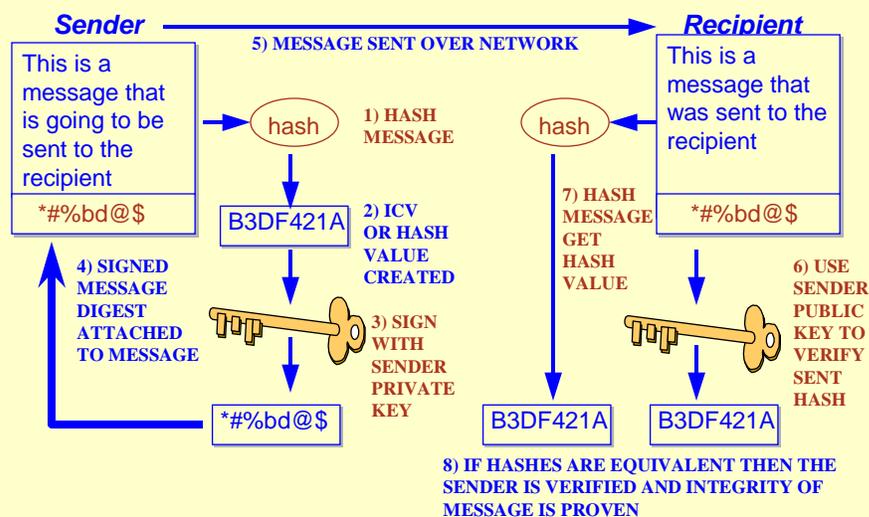
Digital Signatures

- Digital signatures are used to verify the sender of a message.
- An ICV or hash value is attached to a message.
- This hash value is signed with a sender's private key (not the message it's appended to).
- The receiver takes the message digest and first verifies the sender by using the public key of the sender.
- If the message digest matches then the message has not been altered and the sender is authenticated.
- This provides the foundation of non-repudiation.

September 20, 2004

6-1

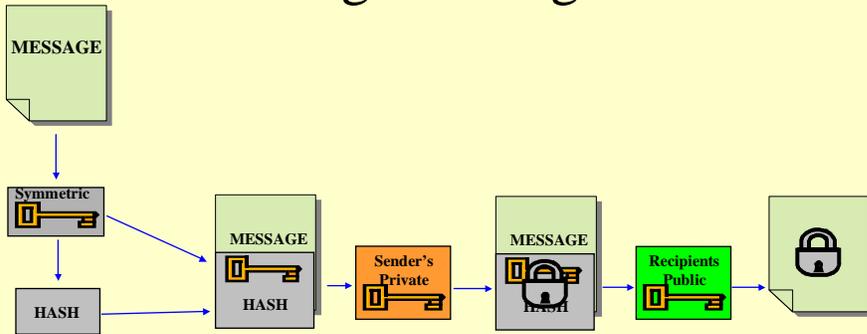
Digital Signatures and Integrity



September 20, 2004

6-1

Putting it all together

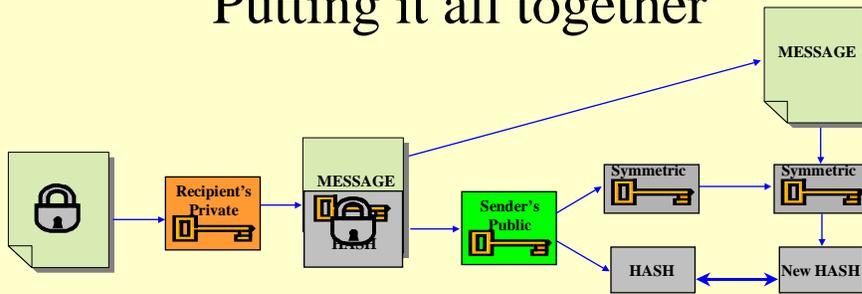


1. **Generate a hash.**
 A 1-time, symmetric key is used to create a hash of the message.
2. **Attach key/hash**
 The symmetric key and the hash are attached to the message.
3. **Sign**
 The private key of the sender is used on the attached key and hash to produce a digital signature.
4. **Encrypt message**
 All data (including the signature) is encrypted with the Recipient's public key.

September 20, 2004

6-1

Putting it all together



1. **Decrypt data**
 The Recipient's private key is used to decrypt all the data received.
2. **Authenticate**
 The Digital signature is processed with the Sender's public key.
3. **Generate new hash**
 The symmetric key retrieved from the signature is then used to generate a new hash of the received plaintext data.
4. **Verify data**
 The new hash is then compared to the hash retrieved from the signature. If they match, the data is good.

September 20, 2004

6-1

Key Length

- Difference in key lengths is significant
 - 40 bits = $2^{40} = 1,099,511,627,776$
 - 128 bits = $2^{128} = 34,028,200,000,000,000,000,000,000,000,000,000$
- 128 bit keys are therefore
 - 309,000,000,000,000,000,000,000,000 times harder to crack than a 40 bit key.
- Comparison if a key can be broken in an algorithm.
 - Using 40 bits in 5 seconds
 - Then 128 bits will take 49,068,526,417,640,960,921 years
- Difference between weak and strong is **BIG**

September 20, 2004

6-1

Key Lengths (continued)

- Not all algorithms can use every number in the key length so it does vary by encryption algorithm and method of encryption
- Equivalent strength between public and conventional keys.

Conventional Key	Public Key	Person	Military
40	274	days	microseconds
56	384	years	seconds
64	512	millennia	minutes
80	1024	infeasible	centuries
112	2048	infeasible	infeasible
128	3072	infeasible	infeasible

September 20, 2004

6-1

Public Key Algorithms – Trade Off

- Public key algorithms are slower (100+ times slower) than conventional encryption algorithms due to bit lengths.
- Public key algorithms however provide the following services:
 - Confidentiality
 - Authentication
 - Non-repudiation.
 - Ease of use with revocation lists.

September 20, 2004

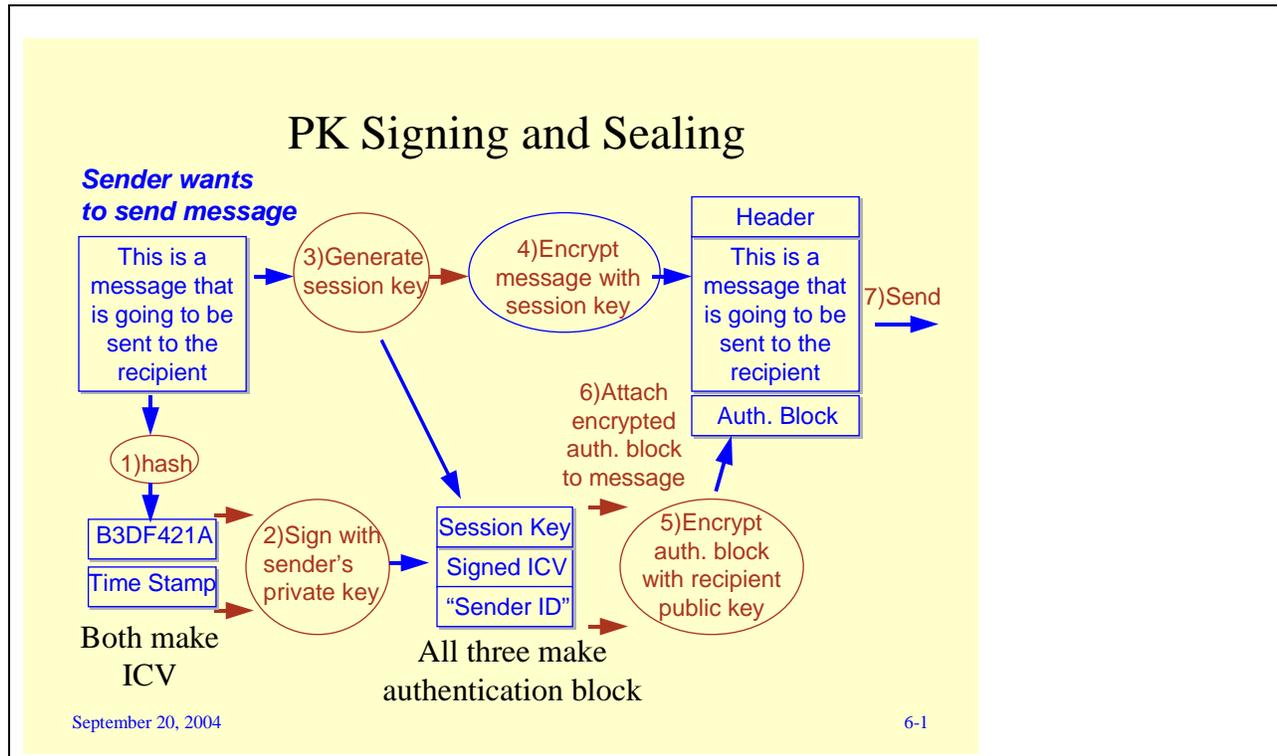
6-1

Authentication Block Technique

- Due to speed most messages using PK are encrypted with a conventional encryption key (its faster).
- An authentication block is attached to the message, this authentication block includes:
 - The conventional encryption key (secret key).
 - The hashed value of the message already signed with the sender's private key.
 - A way to identify the sender (name).
- The authentication block is encrypted with the receiver's public key.

September 20, 2004

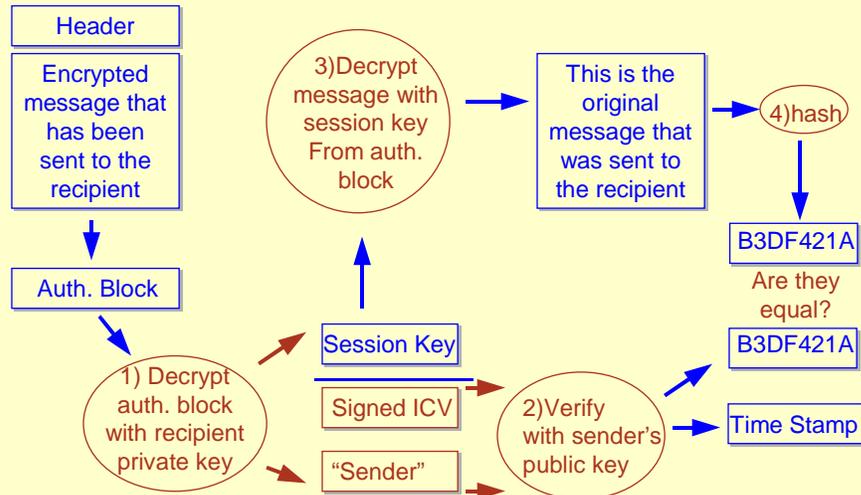
6-1



Authentication Block Technique

- The authentication block is detached and decrypted with recipient's private key. The recipient now has:
 - A signed hash value.
 - The name of the sender.
 - The conventional (session) key used to encrypt the message.
- The conventional key is then used to decrypt main message.
- The recipient then uses public key of sender to authenticate sender and verify integrity of message.
- Two examples - PGP uses IDEA for conventional encryption and RSA normally uses DES.

PK Unsealing and Verifying



September 20, 2004

6-1

Security Services Supported by Cryptography

- Confidentiality – Encryption whether with a public or conventional algorithm.
 - Integrity – Hash or message digest or ICV.
 - Authentication – Verifying the sender by an assumption or by a signature.
- AND....
- Non-repudiation – Validating a digital signature where no one can disclaim it.

September 20, 2004

6-1

Encryption

Module 7

Lesson Objectives

- Understand how encryption works.
- Identify how keys are distributed securely over networks.
- Understand certificate authorities.
- Understand standard encryption techniques used by Army systems.

7-1

Attacks on Network Traffic

- **Passive Methods (Packet Sniffing)**
 - Reading (Content Analysis)
 - Tracking (Traffic Analysis)
 - Counter by Encryption

- **Active Methods**
 - “Jamming” or Packet Substitution Counter by Checking Integrity
 - Spoofing Counter by Authentication



7-1

Basic Strategies for Encrypting Network Traffic

- **Link encryption**
 - Node to node
 - Based on network scheme
- **End-to-end encryption**
 - Host to host
 - VPN (e.g. firewall to firewall)
 - IPSEC

7-1

Link Encryption

- Encrypts traffic as it enters each link or node.
- Decrypts traffic as it arrives from each link.
- Uses multiple keys and slow.
- Plain-text traffic potentially vulnerable at communications nodes.
- Example is any TED.

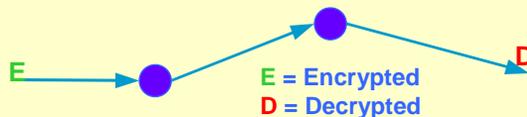
E = Encrypted
D = Decrypted



7-1

End-to-End Encryption

- Encrypts traffic at source.
 - Can be host to host
 - Can be firewall to firewall
- Decrypts traffic at final destination.
- Plain-text traffic not available at communications nodes (irrelevant for routing).
- More information exposed (header), key more exposed.
- Example most VPN and routed traffic.



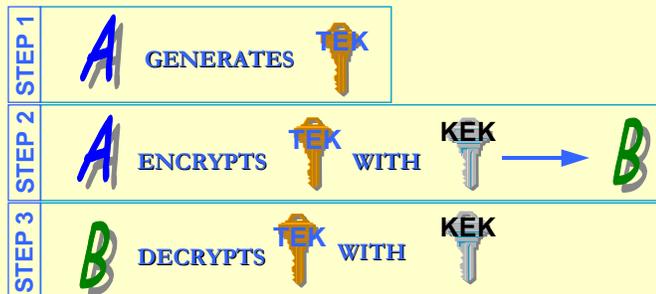
7-1

Key Distribution

- Manual key distribution
 - Common in symmetric (conventional) encryption.
 - KYK-13 or ANCD.
- Automatic key distribution
 - Encrypt with another key.
 - Authentication of source is a bonus of public key.
 - Regular updates?
 - Distribution normally from a key server or key distribution center (KDC).

7-1

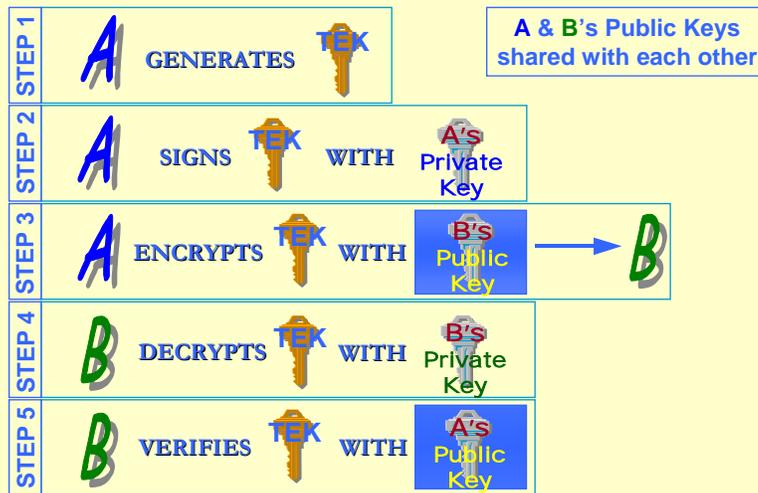
Point-to-Point Key Distribution Using Secret Key



A & B already share a common key encryption key (KEK)

7-1

Point-to-Point Key Distribution Using Public Key



7-1

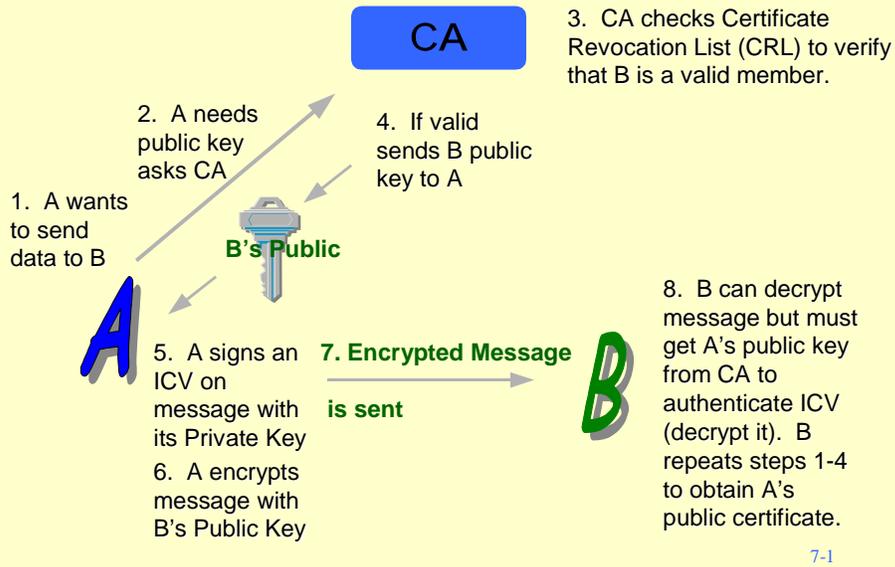
Certificate Authorities



- Public keys need to be manageable:
 - protected by authentication and integrity services.
 - allow for recovery agents
 - identify public keys that are no longer valid
- A certification authority (CA) assigns combination of identifier and public key for each entity in its domain.
- Several ways to use CA but the private key must be protected
- Before issuing a public key a CA will check the certificate revocation list (CRL).

7-1

Certificate Authorities



Common Encryption Algorithms

- Trunk Encryption Devices (TEDs)
- EFS
- DES
- PGP
- DMS and the Fortezza Card
- SSL
- NTLM Authentication
- Kerberos Authentication
- UNIX passwords

7-1

Trunk Encryption Devices (TEDS)

- Use 128 bit conventional encryption.
- Utilize limited transposition.
- Very secure, but limited authentication.
- TEDS operate at the trunk level.

7-1

Data Encryption Standard (DES)

- Conventional Encryption.
- Uses a 56 bit key on 64 bit blocks (outdated).
 - Key lengths don't affect the amount of bits they encrypt.
- Used by several O/S to encrypt password files.
- An old business standard.
- In Jan 1999 a \$250,000 computer broke DES in 22 hours...hmmm.
 - 2002 equivalent number of current processors probably 6-9 hours

7-1

Triple Data Encryption Standard (3DES)

- Conventional Encryption.
- Uses 3 DES keys to encrypt data..
- It uses a method called EDE (encrypt-decrypt-encrypt).
- Provides encryption key lengths of 112 or 168 depending on whether 2 or 3 keys are used.
- Brute force attacks on 3DES are considered unfeasible.

7-1

Advanced Encryption Standard (AES)

- Conventional Encryption.
- Developed by Vincent Rijmen and Joan Daemen..
- Replacement for DES.
- Uses key and block lengths of 128,192,and 256 to encrypt data.
- AES is faster and more efficient than DES .

7-1

Encryption File System (EFS)

- Windows 2000 contains a system to encrypt local files.
- EFS uses the DESX algorithm for file encryption.
 - Encryption key is 128 bits long
 - Called a FEK (file encryption key).
- When a file (or folder) is encrypted:
 - FEK is generated
 - FEK encrypts file or folder contents
 - FEK is stored encrypted as an attribute (attached) to the file
 - Uses a public key in both a DDF (data decryption field) and DRF (data recovery field).

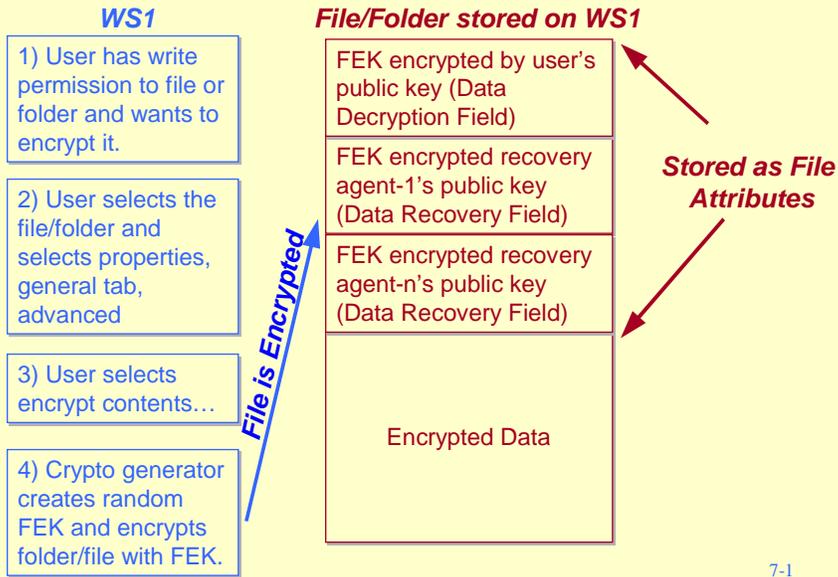
7-1

Encryption File System (EFS)

- Requires the use of certificates (public keys for both DRF and DDF).
- EFS must have:
 - a recovery agent (user account) available:
 - default for domain is domain administrator (also person who can change recovery agent)
 - default for stand-alone is local Admin.
 - file system must be NTFSv5
- Preferred method is to encrypt by folder:
 - less tedious
 - allows for automatic encryption

7-1

Encryption a File/Folder with EFS



EFS – Things to Know

- Note: any user (by default) with write permission can encrypt a file and it uses their private key.
- If you send an encrypted file over the network it is decrypted by the crypto API and sent as plain text.
- The local administrator (stand alone) or the domain administrator account are the default recovery agents.
- Do not encrypt files when you are logged in as the local administrator (uses your key for DDF).
- You can not encrypt files under the system root.
- Applications sometimes store files in Temp folder.
- Recommended that you encrypt My Documents.

7-1

Pretty Good Privacy (PGP)

- PGP uses Peer Trust instead of a certificate authority. (No Certificate Revocation Lists).
- PGP uses Rivest, Shamir, Adleman (RSA) as its public key (2048 bits) algorithm.
- PGP is secure and is a de facto standard in Europe.
- PGP uses IDEA (128 bit) for its conventional encryption algorithm.
- Digital signatures are available as are integrity checks using MD5 (for hashing).
- Major disadvantage no 3rd party checks.

7-1

Defense Messaging System (DMS) and the CAC

- Both utilize a certificate authority scheme.
- DMS uses the Fortezza Card to provide encryption mechanisms.
 - DMS Encryption
 - Public key uses the Key Encryption Algorithm to distribute conventional keys for sessions between two parties.
 - Conventional encryption uses the Skipjack Algorithm (80 bits).
 - Digital signatures and hashing are used.
 - CAC Encryption
 - Public key uses the RSA Algorithm to distribute conventional keys
 - Public certificate lengths are no greater than 1024
 - Conventional encryption is DES (56) or 3DES (112)
 - Digital signatures on encrypted MAC

7-1

Fortezza Smart Cards (CAC similar)

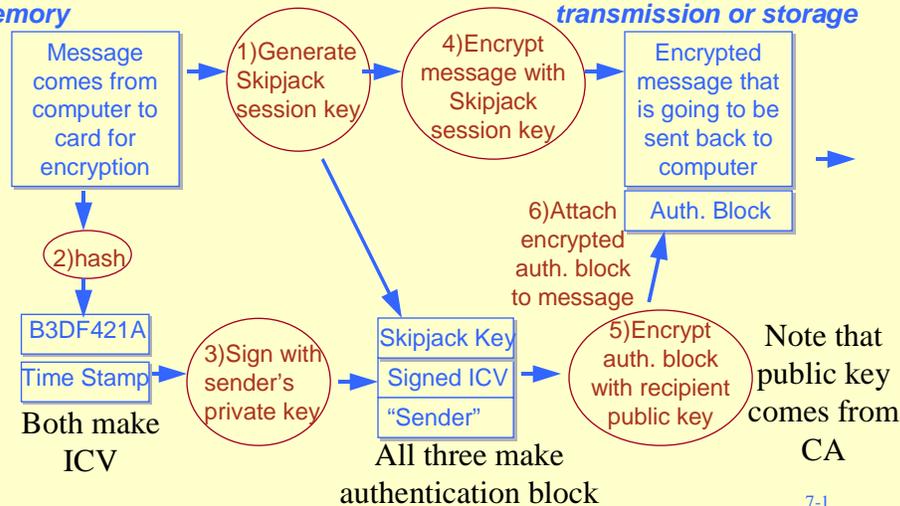
- A Fortezza card is a cryptographic module packaged on PCMCIA smart card.
- Fortezza cards have:
 - A capstone chip which is the cryptographic processor.
 - A clock for timestamps.
 - Permanent memory for certificates (public key storage).
 - Temporary registers for conventional key storage.
 - RAM for decryption and encryption of data.
- Fortezza cards are zeroed if:
 - Someone tampers with the card.
 - You login to the card incorrectly ten times in a row.

7-1

Fortezza Card Encryption and Signing

Message comes from computer and goes to Fortezza card main memory

Encrypted message goes back to computer for transmission or storage

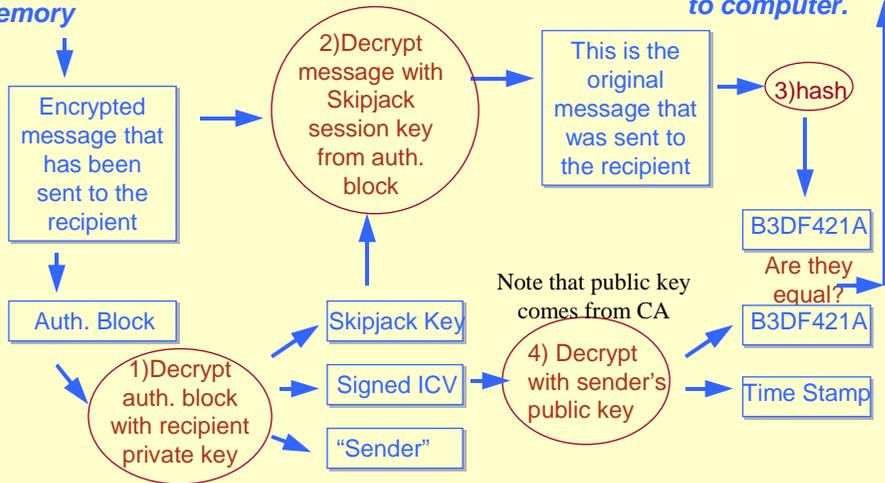


7-1

Fortezza Decrypt and Verification

Message comes from computer and goes to Fortezza card main memory

If valid decrypted message goes to computer.

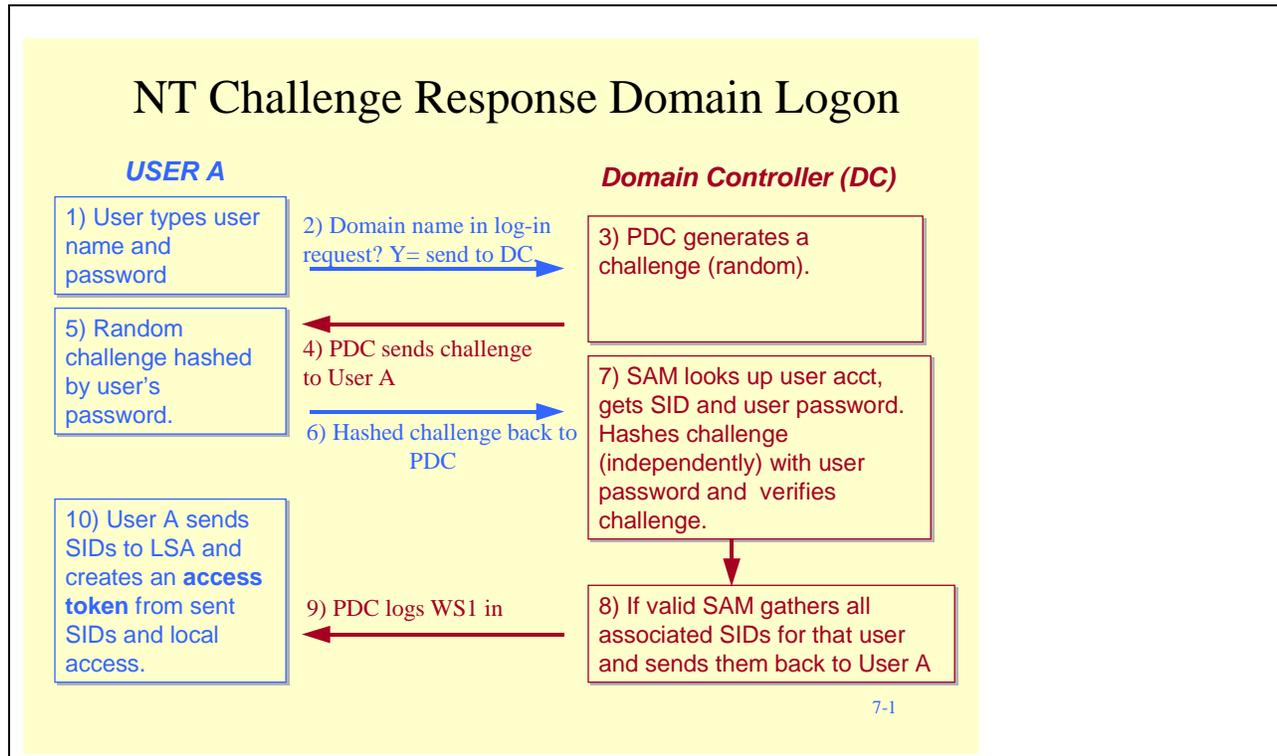


7-1

Challenge-Response NT

- User requests logon for a domain to PDC.
- PDC sends a random challenge to user's WS.
- The WS encrypts (hashes) challenge using the user password to as the hash key value.
- Encrypted challenge sent back to PDC.
- PDC verifies challenge independently.
- If hashes match PDC send user SID and all associated SIDs back to WS.
- Local LSA takes SIDs checks local account data and then creates an access token.
- Winlogon launches user's shell.

7-1



- ## NTLM – Things to Know
- Challenge and response can be captured by packet sniffer.
 - Three hashes used, LanMan (LM), NTLM, NTLMv2.
 - Default is that both the NTLM and LM hash are sent.
 - LM splits all passwords into 7 character hashes, while NTLM or v2 use all 14 characters.
 - LM is much easier to crack.
 - Physical security of servers is critical (protect SAM).
 - To set-up NTLMv2 all DCs must be NT 4.0 SP4+
 - NTLMv2 can be 56 or 128 bits
- 7-1

Kerberos - Windows 2000

- An authentication service
 - Uses conventional encryption (only) default is DES
 - Based on users (not machines) identifying themselves on an untrusted network to access services in a distributed environment.

- Three parts to the exchange
 - Logon on to the domain (realm) through a KDC
 - Request a type of service
 - Use a service

7-1

Kerberos Step 1, Logon to Network

1. Joe User provides his Principal (username) and Password to the Kerberos Client



Credentials Cache:
PSK
TGT^{LTK}
LSK

2. The Kerberos Client sends a login request to the Domain Controller (KDC) for the requested username. This request is totally unauthenticated.

Username

(TGT^{LTK} + LSK)^{PSK}

3. The KDC looks up the username, and if it exists, creates a Principal-Session-Key (PSK) from the password associated with it.



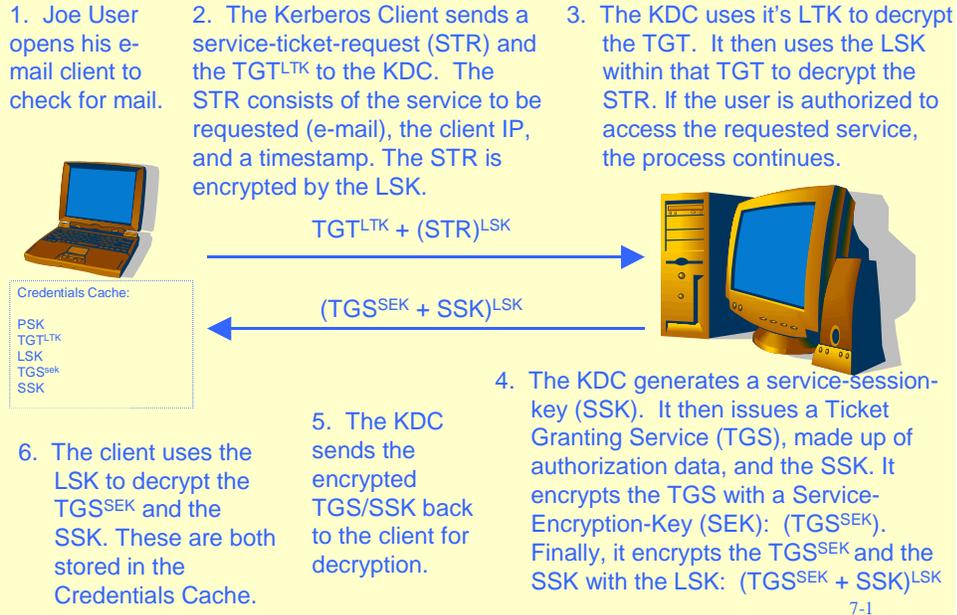
6. The client creates its own PSK from the password entered, then decrypts the package from the KDC and stores it in the Credentials Cache.

5. The KDC encrypts the package with the PSK:
(TGT^{LTK} + LSK)^{PSK}

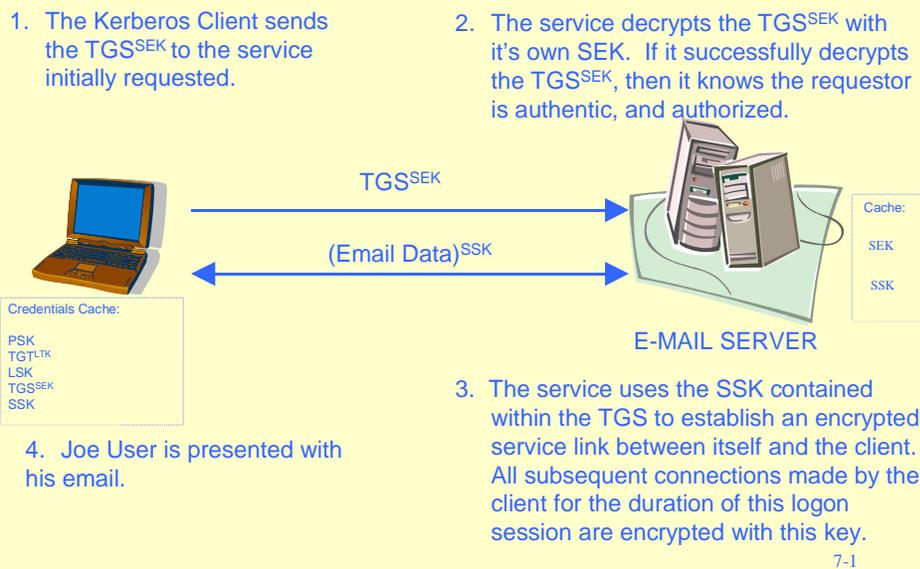
4. The KDC then creates a Logon Session-Key (LSK) for this session. Then a Ticket-Granting-Ticket (TGT). The TGT contains the LSK, the users SIDs, rights, and privileges. This TGT is then encrypted with the KDC's Long-Term-Key (LTK): (TGT^{LTK})

7-1

Kerberos Step 2, Access Service



Kerberos Step 3, Use Service



Kerberos – Things to Know in Windows 2000

- Since timestamps are used in the authenticators - computer clocks must be within tolerance (default is five minutes).
- By default NTLM and Kerberos are loaded by the LSA on a Windows 2000 computer.
- The credentials cache is not paged and is erased upon logoff or system shut-down
- Smart Cards can be used to replace the password logon.
- Kerberos is authentication NOT authorization.

7-1

Summary

- You need to know what forms of encryption your operating system uses and HOW IT WORKS and HOW STRONG IT IS – it defines your problems.
- Both Windows 2000 and Solaris 8.0 have multiple forms of encryption and can integrate COTS encryption mechanisms.
- Logon processes affect the placement of domain controllers, certificate authorities and the distribution of certificates.
- Physical security of servers is very critical.

7-1

PKI Practical Exercise

Lesson 1

This practical exercise is intended as a supplement to material learned during the Cryptography and Encryption lectures. Students will become familiar with concepts and implementation necessary to configure and send encrypted emails.

You will need a partner for this exercise.

1. Open My Computer and double-click on the server drive.
 - a. Open the PGP folder.
 - b. Double-click on Setup.exe
 - c. Click Next at the Welcome.
 - d. Read the Agreement and click Yes.
 - e. Read Product Information, and click Next.
 - f. Accept the name and company information by clicking Next.
 - g. Click Next at Choose Destination.
 - h. At Select Components, ensure that PGP Microsoft Exchange/Outlook Plugin, PGP Outlook Express Plugin, and PGP Command-line are checked.
 - i. Click Next.
 - j. Click Next to copy files.
 - k. When asked if you have an existing keyring, click No.
 - l. Ensure "Launch PGPkeys" is checked, and click Finish.

2. The Key Generation Wizard will open. Click Next.
 - a. Enter your fullname.
 - b. Enter your **classroom email address** for your email address.
(ask the instructor if you don't know what it is)
 - c. Accept the pre-selected Diffie-Hellman/DSS and click Next.
 - d. Accept the pre-selected 2048 bit key strength, and click Next.
 - e. Accept the pre-selected "Key pair never expires" and click Next.
 - f. Type in a  phrase that **YOU CAN REMEMBER** and confirm it by entering it again in the confirmation box. Click Next.
(**IF** you are warned that your passphrase is a potential security hazard, click Next.
IF asked to move the mouse to create some random data, do so, then click Next.)
Once your key is generated, click Next.
 - h. Your Digital Certificate will be generated. What 3 pieces of information does your digital certificate consist  (Hint, it was in the lecture and the slides earlier.)

 - i. **DO NOT** check "send my key to the root server now." Click Next, and Finish.
 - j. Now, manually start PGPtray. (Start -> Programs -> PGP ->  Ptray) (Nothing will open.)

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

You will see a small lock icon in your taskbar tray afterwards.)

- k. Close the “My Computer” window that is currently displaying the PGP folder.
3. PGPkeys should still be open. PGPkeys is a user interface to allow you to manage your “keyring”, and access a certificate server for the purpose of sending, finding, and retrieving public keys.
- a. Select all keys that are not yours, and delete them. (You can right click them, or you can use the trash-can icon on the toolbar.)
 - b. Click Edit, and then Options.
 - c. Select the Servers tab.
 - d. Click New. Leave the protocol at LDAP, set the server name to the classroom's server IP (The instructor will tell you it's IP), and set the port to 3890. Click OK.
 - e. Select the server you just added, and click the "Set as root" button.
 - f. Delete the other servers in the list by selecting them and clicking Remove.
 - g. Check every box in the “Synchronize with server upon” section of this window.
 - g. Click OK.
 - h. Select your key pair in PGPkeys.
 - i. Right-click it, and select "Send to". Select the server you just added to your list to have your key sent to it.
 - j. You will get a message "Key(s) successfully uploaded to server." At this point, the classroom server will now make your keys available to anyone who asks for them. Click OK.
4. Once your partner has reached this step, add their key to your keyring:
- a. Click the magnifying glass on the toolbar. A search window will open. Do not type in anything, just click on search. This will return a list of all the keys that have been uploaded to the classroom server. Find your partner's key in the list, and add it to your keyring by right-clicking on it, and selecting "Import to local keyring".
 - b. Close the search window.
5. Open Outlook Express.
- a. Click "Create Mail", and enter your partner's **FULL** ail address in the "To:" field.
 - b. For the subject, enter ENCRYPTION TEST MESSAGE 1.
 - c. Write out a test message in the body of the email.
 - d. ck on the ">>" symbol on the toolbar if there is one, or stretch the message window out, you will see "Encrypt (PGP)" and "Sign (PGP)". Notice that there are **two** sets of buttons or menu entries labeled "Encrypt Message" and "Sign Message". The first set is for use with Microsoft and Commercial Certificates such as Verisign. The second set is there because you ran PGPTray earlier. (Step “j” at the top of this page. You *DID* take that step, didn't you?) Make sure you use the PGP buttons for this exercise. The others **will not work.**
Click each of them once.
 - e. Click Send.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

6. If the Recipient Selection dialogue box opens, ensure the right key for your partner is in the Recipients area of the window. If it is not, you can click-and-drag it down. Click OK. Are you prompted for your passphrase  so, why 

7. When your partner reaches this point in the PE,  ck your email. (Click "Send/Recv" in Outlook Express.)
8. Go to your Inbox, and select the email with the subject: ENCRYPTION TEST MESSAGE 1. Are you able to read it from the preview pane  _____
9. Double-click the message in the message list, this will open the message in it's own window. Click the >> button if there is one, and then click the button labeled "Decrypt PGP message". Are you prompted for your passphrase  so, why 

10. Once the passphrase was entered, what was done with the encrypted/signed message  Which keys were used for which parts 

11. What is the signature's status  _____
12. What does it say next to the signer's name and address  _____
13. The (Invalid) indicates that the key used to verify the signature is not yet a trusted key. Let's assign this key some trust.
14. Open PGPkeys, select your partner's key, right-click on it, and select "Sign..."
15. Look at the statement at the top of the Sign Key window. What is the term for the kind of trust those two sentences are talking about 

16. Click "Allow signature to be exported", and click OK.
17. Enter your passphrase if asked. Right-click on your partner's key again, and select Properties. Slide the Trust Model slide bar over to Trusted and click Close. You have just assigned trust to your partner's key.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

18. Go back to Outlook Express. Open your Inbox, and double-click on your partner's message. Decrypt it as you did before. Is the (Invalid) still by the signer's name and address 

19. Now, send your partner an email that is signed, but not encrypted. Which key did you just use 

20. When your partner reaches this point in the Practical Exercise, click on Send/Recv and open the new message. You can read it, but there is a signature attached. In order to verify that signature, you can use the decrypt button again. Did the signature authenticate  Were you asked for a passphrase  Which key did you use to authenticate this message 

21. Now, send your partner an email that is encrypted, but not signed. Which key did you use to encrypt the message  Were you asked for a passphrase this time  Why 

22. When your partner reaches this point in the Practical Exercise, click on Send/Recv and open the new message. Decrypt it as before. Is there a signature status  What key did you just use 

23. Try some more encryption tests between yourself and your partner, or with other people in the classroom. Don't forget which keys you need, and how to get them.

System Availability

- **Backup**
- **RAID**
- **UPS**

Backup Strategies

- **Why Backup ?**
- **What are some good software choices?**
- **What is your backup policy?**
- **Remember... Its Your Last Line of Data Protection**

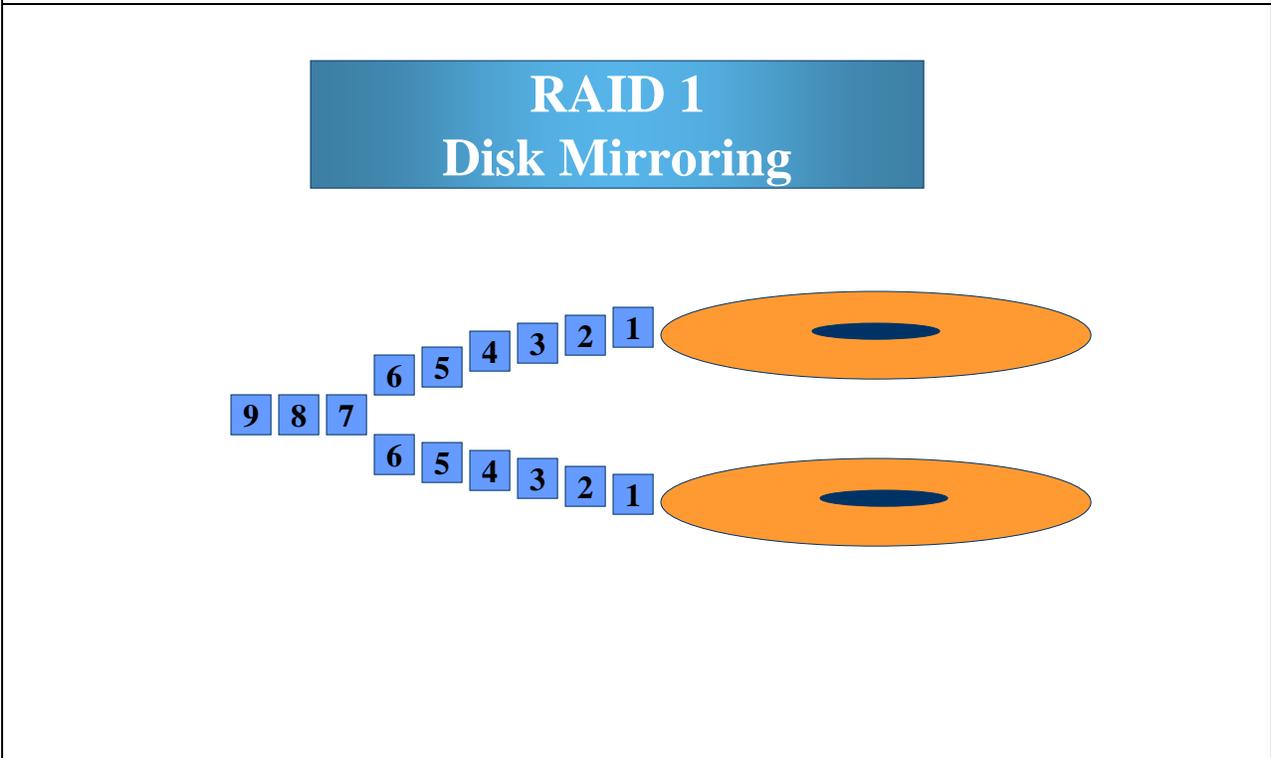
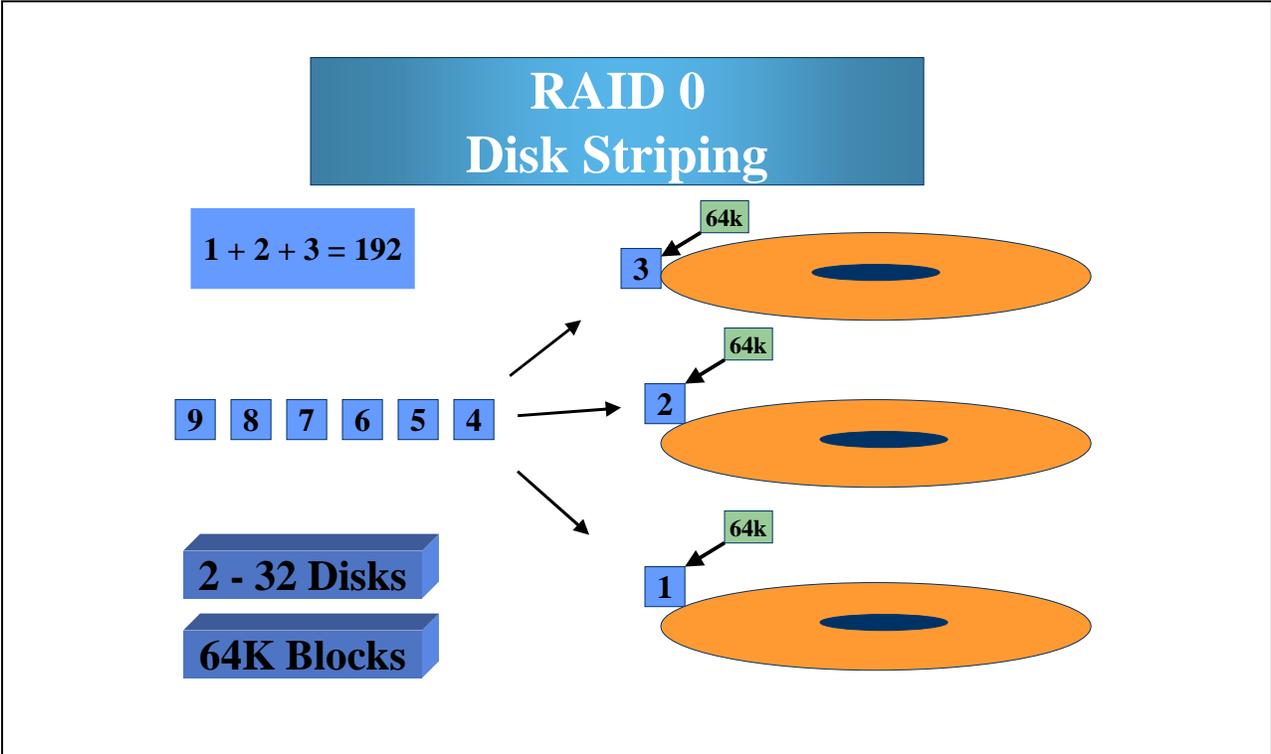
Backup Policy

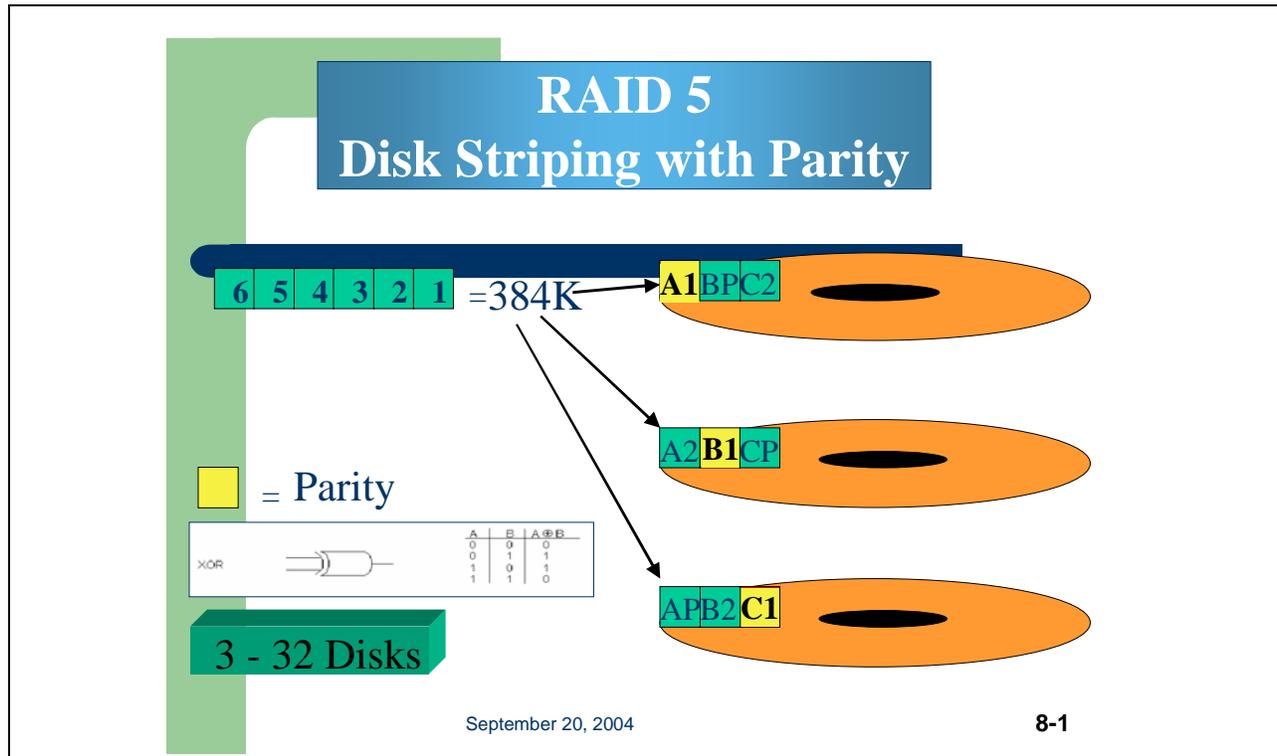
Backup regime:

- **Media rotation / retention schedule**
- **Encryption, compression, and error-checking and correcting**
- **Automate backup**
- **Train operators**
- **Off-site storage**
- **Document policy and procedures**
- **Distribute policy to interested parties**
- **Incremental, Selective, Selective incremental, System**

A rectangular graphic with a red-to-teal gradient background. The word "RAID" is written in the center in a white, serif, all-caps font.

RAID





Power Protection

- Power conditioning
 - Surges, Spikes, Brownouts, Sags
- Capacity planning
 - VA , Uptime

System Recovery Basics

- **Develop recovery plans and procedures**
- **Test initial system recovery measures**
- **Maintain system configuration information**

The Bigger Picture...

Purpose of Contingency Planning

- **Road map to recovery**
- **Minimize recovery period**
- **Minimize errors in decision making**
- **Minimize errors in implementation**
- **Identifies critical assets / processes**
- **Establish responsibilities**
- **Establish priorities and resources**

Contingency Planning Update

- **Obtain Commitment from Management**
- **Establish Planning Committee**
- **Conduct Capability Assessment**
- **Conduct Risk Analysis**
- **Establish Priorities**
- **Define Requirements for Plan**
- **Develop Plan**
- **Train for Plan**
- **Test Plan**
- **Update Plan**



Secure Web Services

Using IIS

Module 9

20-Sep-04

9-1



[Lesson Objectives]

- Explore Microsoft Internet Information Server 5.0 features.
- Discuss web server vulnerabilities and methods of securing web servers.

20-Sep-04

9-1

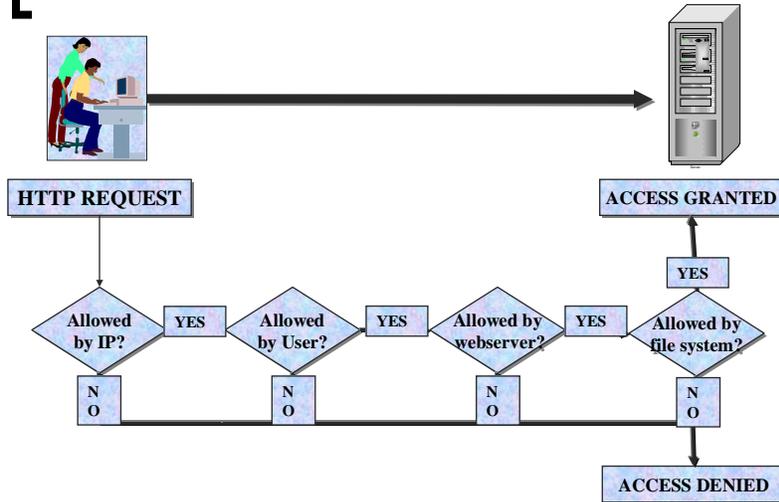
[Web Security Model]

- Platform Security
- Web Server Security
- Communications Security
- Application Security

[Access Controls]

- Logon and Username
- IP Address
- Availability of Directories and Files
(Virtual Directories & Browsing)

WWW Authentication Process



Anonymous Access and Authentication Control

Anonymous Access has user-applied restrictions



Authentication Control denies access and then queries the user for authentication

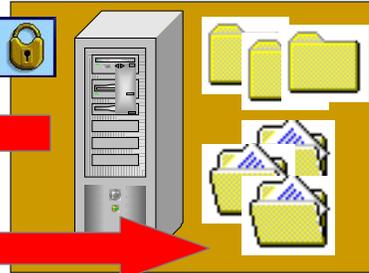


Name

Password

Name

Password



Resource Access Control

NTFS File and Directory Permissions

- **Create WebAdmin group and put all web administrators in the group**
- **Remove**
 - **EVERYONE GROUP** from the ACL for virtual directories or Web Pages
 - **Administrators**
- **Add**
 - **WebAdmin group with full controls**
 - **IUSER_Computer** with appropriate permissions
 - **Authenticated Users** with appropriate permissions

Resource Access Control

Combining NTFS and ISS Permissions

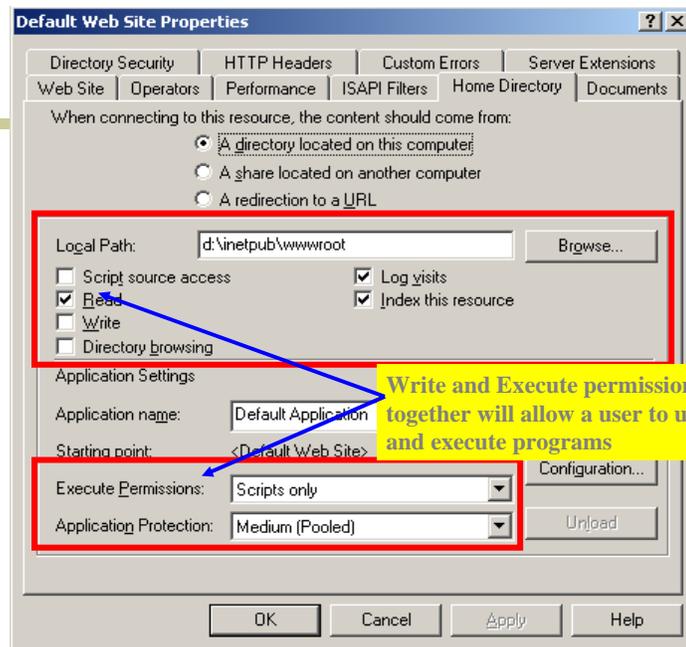
Assign permissions in IIS

- **Read permission to the directory to allow browsing.**
- **Script permission for directories containing Active Server Pages, CGI or other scripts.**

Assign permissions in NTFS

- **Read permissions to the Users local groups.**
- **Change permissions to group responsible for creating content in the directory.**
- **Full control permission to the Web Administrators local group responsible for administrating the Web server.**
- **No access permission to any group or user who should not be allowed to browse the contents of the directory.**

Resource Access Control



Communications Security

- Is TCP/IP Secure?
- Minimize available protocols
- Routers
- Firewalls... In front of? Or Behind?

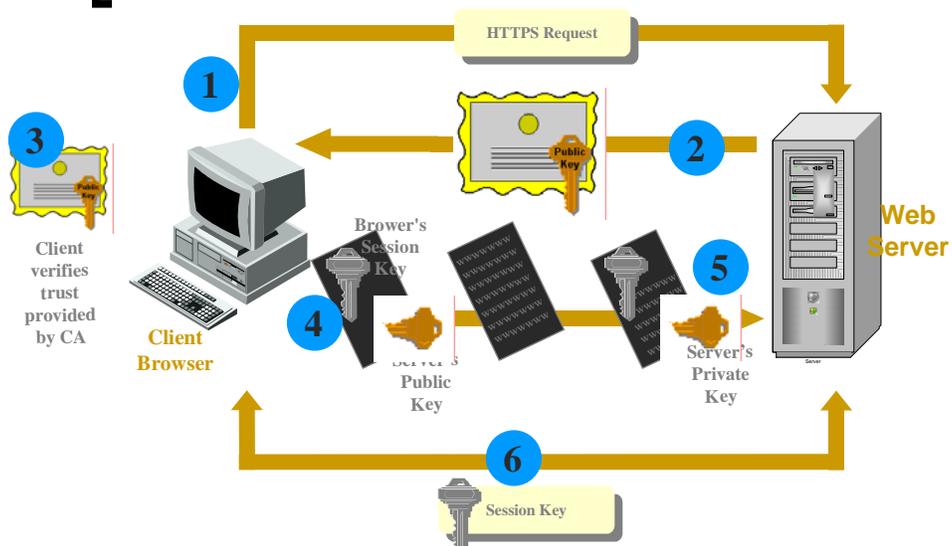
[Application Security]

- One of the most serious risks
- Use Secure Protocols
 - Secure HTTP (S-HTTP)
 - SSL (Secure Sockets Layer)
 - PCT (Private Communication Technology)
 - SET (Secure Electronic Transactions)

[Secure Sockets Layer (SSL)]

- Supports web browsers and servers
- Uses a one way public key algorithm (by default).
- Server issues its public key.
- Client generates a session key using browser.
- Client sends session key to Server encrypted with Server public key.
- Client and Server exchange information using session key generated by client.
- Can you be sure that the Server is who he says he is?
- The standard case does not authenticate client.

Secure Sockets Layer (SSL)



Application Security

- CGIs (Common Gateway Interfaces)
- ISAPIs (Internet Server Application Programming Interfaces)
- Run in restricted environment
- Verify design of interface and test
- Java & Active X

[Web Server Vulnerabilities]

- CGI Scripts
- Active Server Pages (*ASP*)
- Server Side Includes
- Superfluous Decoding Operation
- Buffer Overflows
- Security Policies
- Administrators
- Denial of Service attacks

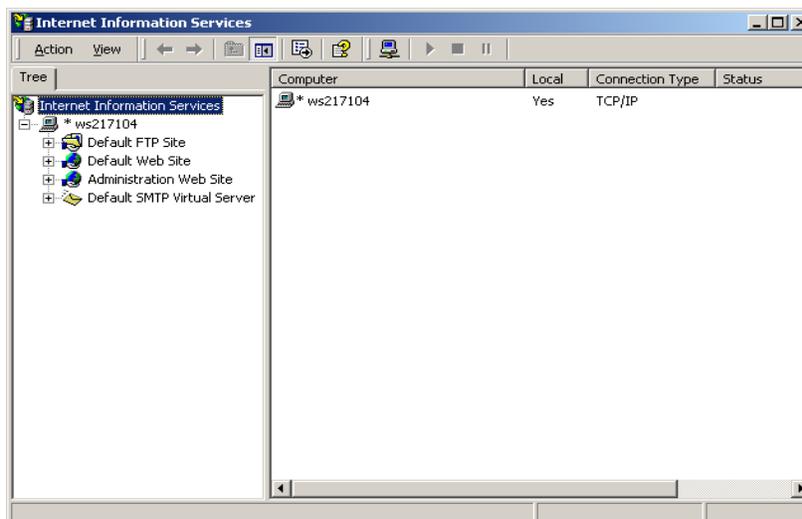
[Denial of Service Attacks]

- Bandwidth Consumption
- Resource Starvation
- DNS Attacks
- Malformed URL
- Malformed WebDAV Request

Internet Information Server

- Components
 - WWW, FTP, SMTP, & NNTP
 - Microsoft Index Server 2.0
 - Microsoft Transaction Server 2.0
 - Microsoft Site Server Express 2.0
 - Microsoft Certificate Server 1.0
- Integrates Windows NTFS security

Microsoft Management Console

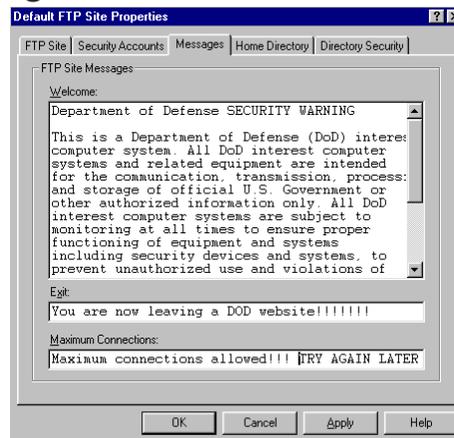


IIS FTP Service

- FTP Service
 - Allows FTP access to server
 - Disable if not needed
 - Restrict access as appropriate

FTP Legal Considerations

- Welcome Message
- Warning Banners

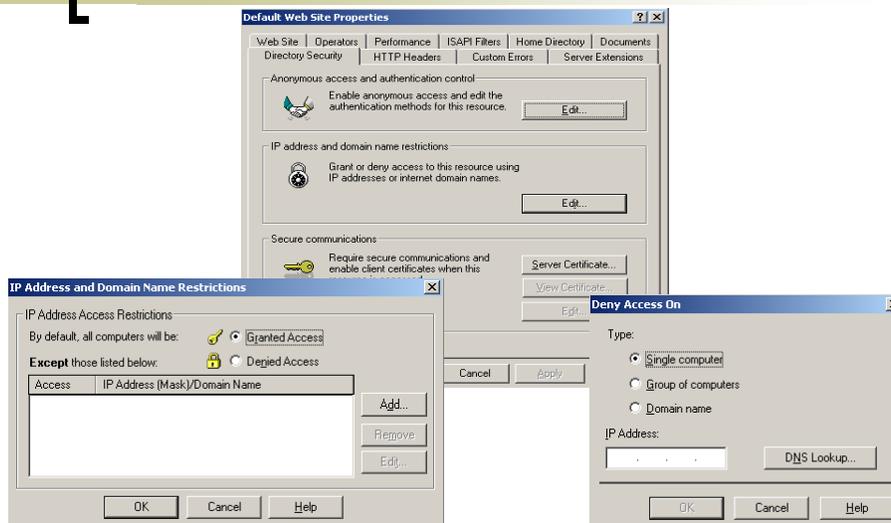


IUSR_computername Account

- Installed with IIS
- Default IIS anonymous user
- Member of Guests
- Restrict via NTFS permissions



Restricted Access for Intranet



SUMMARY

- Hackers have shut down or changed numerous Web-sites just to prove a point.
- Your Web site is a reflection of your good intention to service your users.
- Keep the world out of your network while permitting them see your web-site .

[Any Questions?]



Reading assignment 2

Subject: **Defense in Depth, and Router Intro**

Pages: 3-21, 26-37, 42-43

(Complete before day 3)

1. Briefly define the following in your own words:

der Router:

wall:

:

N:

Z:

eened Subnet:

xy:

figuration Management:

2.  the range of numbers used to define a standard vs. extended access list, and explain the primary differences of each.
3. ine “Implicit Deny.” And describe where it occurs in an access list.
4. y use an ACL on a router when you have a high-tech firewall right behind it?

PRACTICAL EXERCISES

C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

5.  When you create a group of IP addresses to always be denied by your ACLs, what is this group sometimes called?

6.  What does an ingress filter protect, and what does it protect it from?

7.  What does an egress filter protect, and what does it protect it from?

Microsoft Internet Information Server Security

Lesson 2

This practical exercise allows hands-on interaction with Microsoft Internet Information Server 5.0 in order to allow students to gain experience with web server configuration and security policies.

Objectives

1. Configure various IIS options.
2. Apply security controls through user, group and directory management and IP restriction.
3. Protect content through application of IIS and NTFS permissions.
4. Demonstrate remote virtual directory vulnerabilities.
5. Understand IIS logging capabilities and features.

Internet Information Server (IIS) 5.0

Practical Exercise 1

NOTE: During this practical exercise, do NOT open multiple copies of the Internet Service Manager.

FTP Site Security Settings

1. Open the **Internet Service Manager (Start->Programs->Administrative Tools)**
2. Select the **Default FTP Site** right click and select **Properties**
3. In the **FTP Site** Tab. Verify that **Enable Logging** is checked, select the **W3C Extended Log File Format** and click on **Properties**
4. Where is the default Log file directory  _____
5. Is this something you might want to change?  **S/NO**
6. Why  _____
7. Select the **Extended Properties** Tab
8. Verify that **Date, Time, Client IP Address, User Name, Method, URI Stem,** and **Protocol Status** are checked. You can check other options if you would like, but do **NOT** uncheck any. Click **OK**.
9. Next select the **Security Accounts** Tab
10. Notice the IUSR_computername account, what is this for  _____
11. Verify that **Allow only anonymous connections** and **Allow IIS to control password** ARE Checked. Depending on how your FTP site is setup, this is the recommended method. Why would you want to force your users to log into FTP using the anonymous account 

12. Next select the **Messages** Tab. In the **Welcome** window we will be adding the DOD Warning Banner.
13. Copy the warning banner text and paste it into the FTP **Welcome** window (It can be found on your CD.)
14. Next select the Home Directory Tab. Verify that **Read** is checked, **Write** is NOT checked, and **Log visits** is checked. Are these webserver or filesystem permissions  _____
15. Next select the **Directory Security** Tab.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

16. Now we will modify the **TCP/IP Access Restrictions** so that only your partner is **Granted Access** to your FTP sight.
17. Click on the **Denied Access** radio button. Click on **Add**. Select the **Single Computer** radio button and type in your partner's IP address. Click **OK**.
18. Click **OK** to close the FTP Properties Sheet.

Connecting to the FTP Server to verify TCP/IP Access Restrictions

1. Any files you place into the **(Server Drive)\inetpub\ftproot** directory will be downloadable when someone FTP's to your site, if they are given read access.
2. Begin by creating a file called **Army.txt** in the **(Server Drive)\inetpub\ftproot** directory. (you can add some text to the file if you wish)
3. Log onto your partners FTP site. You can use **either** of the following methods:

Command Line Method:

- a) Open up a command prompt
- b) Type **ftp** (Partners IP Address)
- c) Enter **anonymous** as the login (watch spelling)
- d) You do not have to enter a password, just hit **enter**.
- e) Did the DOD Login banner appear  **S/NO** (If no, make sure your partner made one.)
- f) Type **dir** to get a directory listing. Does **Army.txt** appear in the listing  **S/NO** (If no, make sure your partner put one in their ftproot directory.)
- g) Type **get Army.txt** to copy the Army.txt file to your hard drive. (Note: the file will be copied to whatever directory you started the FTP command from.)
- h) Next try to FTP into any system that has not permitted you. Are you allowed access **YES**  (If yes, make sure the person at that system is at least this far in the PE.)

Browser Method (If you used the above method, this is not necessary)

- a) Open up **Internet Explorer**
- b) In the Address Field type **ftp://(Your Partners IP Address)**
- c) The Browser will automatically enter the anonymous username & null password
- d) Did the DOD Login banner appear  **S/NO** (If no, make sure they made one.)
- e) On the screen you should see the **Army.txt** file. (If not, make sure they put one in their ftproot.)
- f) Right click on **Army.txt** and select **Copy to folder...** Keep the defaults and save the file as Army.txt in the base directory of the Server drive.
- g) Next try to FTP into any system that has not permitted you. Are you allowed access **YES**  (If yes, make sure they are at least this far in the PE.)
- h) Now continue to the **FTP Logging Exercise**.

FTP Logging Exercise

(Note: There will be no log file if no-one has logged into your FTP server)

1. Open up the directory located at
(Server Drive)\Winnt\system32\LogFiles\MSFTPSVC1
2. Notice the date in the filename, it should be today's date.
3. Open the file and look at the time indicated by the entries in it. Why does it seem so off?  Hint: remember, your time zone is not the primary one used by the rest of the world).

4. Did the logfile successfully capture the IP addresses accessing your FTP site?
 **S/NO**
5. Does the logfile tell you whether or not the user was granted access?  **S/NO** (Hint: look at the three digit code)

530 = Wrong Password
230 = Correct Password



6. Does the logfile indicate filenames, if any that were sent to a user?  **S/NO**
7. You probably see **USER**, **PASS**, **sent**, and **QUIT** under the uri-stem. What would it mean if you saw **created** in your log file? 

8. Close the logfile, the logfile folder, and the command prompt.

Practical Exercise 2

Web Site Security Settings

Log onto your favorite web site, select file, select save as and save the website to (Server Drive)\inetpub\wwwroot. Save the file name as **default**. This is now the website hosted on your computer. (Select a basic page that does not contain java script and ASP scripts, because it may not display properly)

1. Open the **Internet Service Manager**
2. Select the **Default Web Site** right click and select **Properties**
3. What is the default TCP Port used for the Web site  _____
4. Could a user setup a renegade web server in your office on a different port?
 **S/NO**
5. In the **Web Site** Tab Verify that **Enable Logging** is checked, select the **W3C Extended Log File Format** and click on **Properties**
6. Select the **Extended Properties** Tab
7. Verify that **Date, Time, Client IP Address, Method, URI Stem, Protocol Status,** and **User Agent** are checked. Uncheck **URI Query**. You can check other options if you would like. Click **OK**.
8. Next select the **Home Directory** Tab.
9. Verify that **Write**, and **Directory browsing allowed** are NOT checked.

10. Recall what Directory Browsing allows. In what type of setup would you allow Directory browsing 

11. Next select the **Directory Security** Tab
12. Under Anonymous Access and Authentication Control click on **Edit**
13. What are the four types of Authentication Methods 

1. _____
2. _____
3. _____
4. _____

14. Why would you use Basic Authentication instead of Integrated Windows Authentication 

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

15. Basic Authentication is sent in Clear Text, is there a way to keep Basic Authentication from being read off the wire?  **YES/NO**
16. How  _____
17. Cancel out of Authentication Methods.
18. Under IP Address and Domain Name Restrictions click on **Edit**
19. As you did in the FTP Lab, set access restrictions on your web site so that only your partner can gain access.
20. Click **Apply**, then **OK** to close the Default Website Properties Sheet. (If asked about Inheritance Overrides, just click **OK**.)

Connecting to the Web Server to verify TCP/IP Access Restrictions

1. Start by having your partner open up **Internet Explorer** and typing in your IP address in the address bar.
2. Next have someone you did not permit attempt to access your web page. If your IP Address Restrictions are set up correctly, they should not be able to access your web site.
3. If your access-list is working correctly proceed to the WWW Logging exercise.

WWW Logging

(Note: There will be no logfile if no-one has logged into your WWW server)

1. Open up your service log at **(Server Drive)\winnt\system32\LogFiles\W3svc#**
Find the most current log file. **[ex Year Month Day]**
2. After opening up the log file, answer the following questions: (The columns do not line up with the field names, you can count them over at the top to find out which column is which.)

- a)  at time was the web page accessed? _____
- b) What was the IP of the client accessing the web page? _____
- c) What HTTP method was used  s-method column.) _____
- d) Did each object on the web page require it's own GET?  **S/NO**

Close the log file and folder.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Create Virtual Directories using the following procedures:

1. Highlight and right click on **Default Web Site** and select **New > Virtual** directory. Give it an alias of **Virt1**.
 - Open “My Computer”, and create a temp directory on your server drive.
 - Back in the Virtual Directory Wizard, use the browse button to point to the temp directory you just created
 - Allow read access
 - Allow browse
 - Click **Next** and **Finish**
2. Highlight default Web Site and right click Properties.
 - Limit connections to 10
3. On the Web-Site tab (Advanced button), what port would be used if SSL was installed 
4. Open Internet Explorer and in the address box type [http://\(your IP address\)/Virt1](http://(your IP address)/Virt1) – the virtual directory should appear. **Note:** If the directory does not appear, read the error message and look for the error code in it. It will usually give you a clear reason why you aren’t allowed to view the page. Don’t forget about the troubleshooting flowchart in your student handouts. Fix this problem.
5. Now that you can see the Virtual Directory, add some files to it by going back to “My Computer” and placing some files in the temp directory you made earlier. When you refresh your browser, they should appear in a list.
6. Go back to the temp directory folder and create a new text file. Type a few lines of text in the file, and save it. Then rename the file to **default.htm**.
7. From the Internet Explorer, hit the refresh button. What happened?

8. Go back to the Internet Services Manager. Right-click on your Virt1 Virtual Directory. Select **Properties**. Click on the **Documents** tab. Notice the section labeled “**Enable Default Documents**.” This section controls the documents that will be automatically displayed to viewers if they are present. The documents listed are processed in order from top to bottom. The first one it finds in the directory will be the one displayed. This can be used as a type of safety feature to keep users from viewing directories. Even if directory browsing is enabled, as long as one of these files exists in a directory, the contents of that directory will not be displayed by IIS. At the same time, the existence of one of these files can inadvertently affect directory browsing. If you wish to show the contents of a directory that does contain one of the listed document files, you have to either uncheck the **Enable Default Documents** box, or remove the necessary filenames from the list.
9. Close the folder, Internet Explorer, and any editors you may still have open.

Practical Exercise 3

Secure Socket Layer Lab

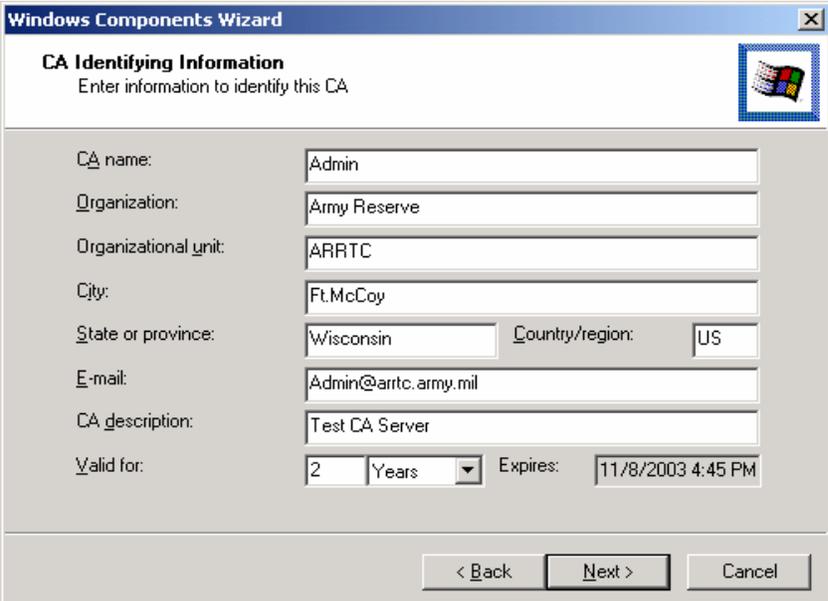
Objectives:

- I. Setup a Certificate Authority
- II. Request and Process a Server Certificate
- III. Verify functionality of SSL

I. Setting up a Certificate Authority

Our Certificate Authority issues the keys needed to run our Public Key Infrastructure

1. Click **Start, Settings, Control Panel**.
2. Double click **Add/Remove Programs**. (Close the Control Panel)
3. Click **Add/Remove Windows Components**. This will start the **Windows Components Wizard**.
4. Check the **Certificate Services** box, select **Yes** in the dialog box to continue and then click **Next**. Once installed, the computers name, or domain can no longer be changed.
5. The Wizard now prompts you to select the type of Certification Authority. Keep the default selection of **Stand-alone root CA.**, click **Next**. (The **Advanced Option** is used to change cryptographic settings)
6. Next you must enter identifying information. See Figure 1. (You may enter anything you wish in any of the areas, but leave CA Name set to Admin.) Then click **Next**.



The screenshot shows the 'Windows Components Wizard' dialog box, specifically the 'CA Identifying Information' step. The title bar reads 'Windows Components Wizard' and the subtitle is 'CA Identifying Information'. Below the subtitle, it says 'Enter information to identify this CA'. The dialog contains several text input fields and a dropdown menu. The fields are: 'CA name' (Admin), 'Organization' (Army Reserve), 'Organizational unit' (ARRTC), 'City' (Ft. McCoy), 'State or province' (Wisconsin), 'Country/region' (US), 'E-mail' (Admin@arrtc.army.mil), 'CA description' (Test CA Server), and 'Valid for' (2 Years). The 'Expires' field shows '11/8/2003 4:45 PM'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

CA name:	Admin			
Organization:	Army Reserve			
Organizational unit:	ARRTC			
City:	Ft. McCoy			
State or province:	Wisconsin	Country/region:	US	
E-mail:	Admin@arrtc.army.mil			
CA description:	Test CA Server			
Valid for:	2	Years	Expires:	11/8/2003 4:45 PM

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Figure 1

- Next we need to define a location for the certificate database, configuration information, and Certificate Revocation List (CRL). Leave the default entries. See Figure 2. Then click **Next**..

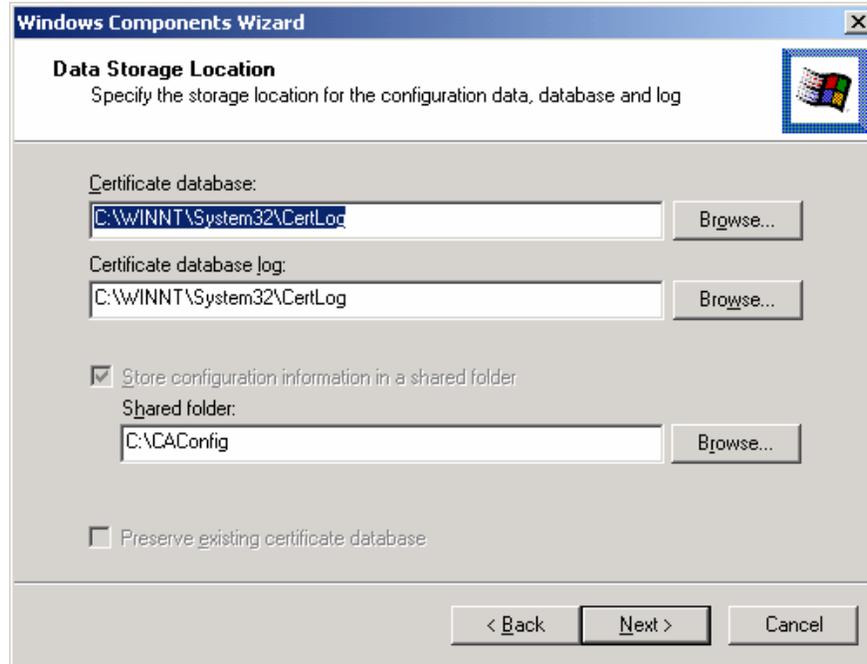


Figure 2

- If IIS is running, a message will prompt you to stop IIS. Hit **OK** to Stop IIS. This must be done in order to install the Web components.
- If windows prompts you for some needed files, Browse or point the Wizard to the (CDROM):\i386 folder. You may have to insert the Windows 2000 CD. Then click **OK**.
- Click **Finish** and **Close** the **Add/Remove** window.
- Now lets verify that the Certificate Authority is installed and running:

At a Command Prompt type **net start** and scroll up to find **Certificate Services**.

If Certificate Services is not listed, contact the instructor. If it is, close the command prompt.

II. Request and Process a Server Certificate

We need to set up IIS with a Web Server Certificate

- Go back to the **Internet Services Manager**.
- Right click on **Default Web Site**, then **Properties**.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

3. Select **Directory Security** tab.
4. Under **Secure communications**, select **Server Certificate**.
5. In the Wizard click **Next**
6. Select **Create a new certificate**, Click **Next**
7. Then select **Prepare the request now, but send it later**. Click **Next**.
8. Type **Test Server** in the **Name** field and leave **Bit Length** at **512**. Click **Next**
9. In the **IIS Certificate Wizard** enter the following info:

Organization:	US ARMY	
Organizational unit:	SIT	click Next
Leave Common name at default		click Next
Country/Region:	Us (United States)	
State/province:	Georgia	
City/locality:	Ft. Gordon	click Next
File name:	(Server Drive)\certreq.txt	click Next
10. Verify information is correct, click **Next**, then **Finish**
11. In the **Default Web Site Properties** window, click **OK**
12. Open IE (Internet Explorer), type [http://\(Your IP address\)/certsrv](http://(Your IP address)/certsrv) , Select **Request a certificate**, click **Next**
13. Select **Advanced request**, click **Next**
14. Select **Submit a certificate request using a base64 encoded PKCS #10 file...**, click **Next**
15. Find the **certreq.txt** file that you created in step 10. Open it in Notepad (You will have to go to "My Computer" to do this), then select (highlight) **ALL** of the text, including:

-----BEGIN NEW CERTIFICATE REQUEST-----

{ lots and lots of stuff }

-----END NEW CERTIFICATE REQUEST-----

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

16. Once **ALL** of the text is highlighted, **Copy** and **Paste** it into the **Saved Request** field. Close notepad when done. See figure 3

QUESTION:

What does the *Block of the Garbage* look like  (hint: Peek at Appendix A)

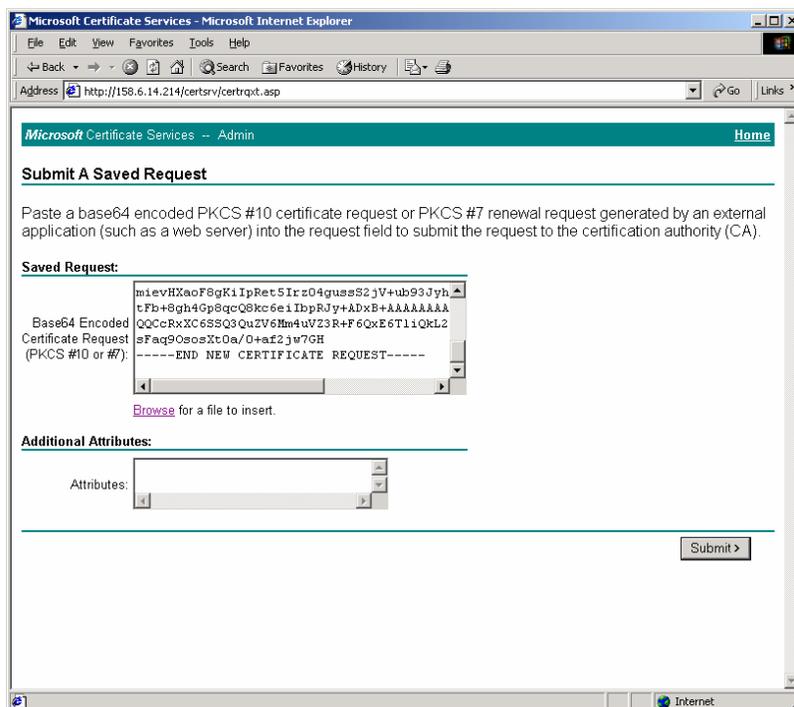


Figure 3

17. Click **Submit**

18. Notice the Certificate Pending status

Process the Certificate we just requested.

1. **Start, Programs, Administrative Tools, Certification Authority**
2. Select **Pending Requests** folder
3. You should have one certificate pending. Right click on the pending request, select **All Tasks, Issue**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

4. The pending request should now be in the **Issued Certificates** folder.
5. Certificate Service must be restarted at this point. Right-click on **Admin**, Select **All Tasks**, then click on **Stop Service**. When it completes stopping the service, take the same steps, but click on **Start Service**.
6. In your browser (IE), type [http://\(Your IP address\)/certsrv](http://(Your IP address)/certsrv)
7. Select **Check on pending certificate**, click **Next**.
8. Select the **Save-Request Certificate**, click **Next**.
9. Select **Base 64 encoded**, click on **Download CA certificate**.
10. In the **File Download** dialog box, select **Save**.
11. Save it on your (**Server Drive**), leave File name: **certnew**, click **Save**.
12. In the IIS (Internet Information Services) window, right click on **Default Web Site**, select **Properties**, select **Directory Security** tab, select **Server Certificate** in the **Secure communications** section.
13. Click **Next** in the **Web Server Certificate Wizard**.
14. Select **Process the pending request and install the certificate**, click **Next**.
15. Make sure the Path and file name is (**Server Drive**)\certnew.cer, click **Next**.
16. View the certificate information, click **Next**.
17. After you see the **You have successfully completed the Web Server Certificate Wizard** message, click **Finish**.

III. Let's setup and verify the functionality of SSL

18. Notice all of the options under **Secure communications** are now available. Select **Edit**.
19. Check the box for **Require secure channel (SSL)**, click **OK**
20. Click **OK** on the **Default Web Site Properties** window. (If asked about Inheritance Overrides, click OK)
21. In your web browser (IE) type [http://\(Your IP address/](http://(Your IP address/)

What response did you get 

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

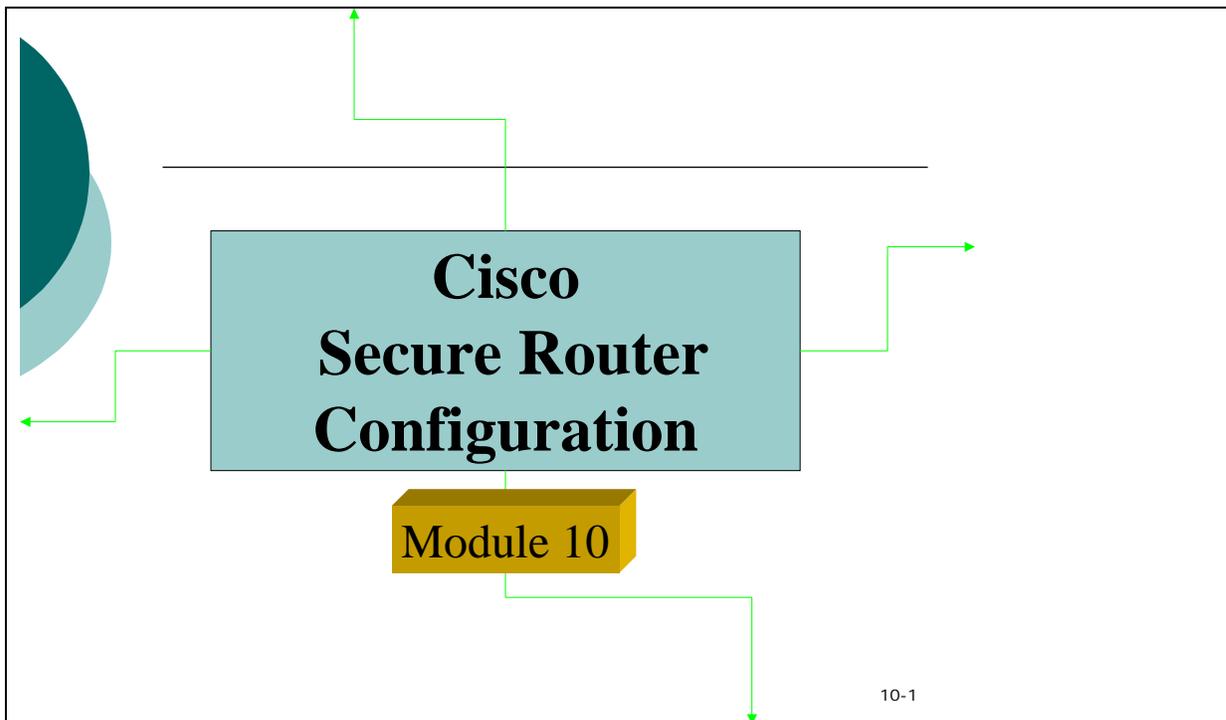
What can you do in order to view this page 

What are two indicators that you have a secure connection  (do not count any boxes you clicked away)

If you were presented with a dialogue box that stated that some items on the page were secure and some were not, then it asked you if you'd like to view the insecure items: If you selected "Yes", then the lock will not display, and you should see all the items on the page. If you selected "No", then the lock should be there, and you will see some items missing from the page.

IIS Summary & Security Tips

1. Do not ever use the "default web" always create a brand new web in a completely different path on the hard drive if possible.
2. Do not use ANY ISAPI filters unless you MUST.
3. Remember there is a new IIS hole bound to come out at least once a month.
4. Guard yourself from the attacks that are yet to come. Basically it does not matter how many service packs or hot fixes you install there will always be that one new hole that comes out that bites you where it hurts. Remember to look for things that are out of the ordinary, you should never have a request to your website that has "../..../..../..../..../" somewhere within it. There are a lot of "path attacks" against various ISAPI filters... they all have the same basic characteristics so look for patterns.
5. Consider obscurity -- Obscurity isn't good security but it is better than using defaults. There is nothing wrong with not installing software in their default directories to foil script kiddies or the easily discouraged hacker. Don't save orders to orders.txt. Don't put logs in a directory named logs. With so many other sites for a hacker to hack sometimes a little obscurity can be enough to save you.
6. Your site is never secure -- Don't brag about how secure your site is on your privacy page. Don't even mention how secure you are because you will start believing it yourself and let your guard down.
7. Training is the key for web administrators/developers. They should be able to test their own content. If not get signed up for more training.
 - a) HTML 4/ XML / HDML / C / C++ / Visual Basic / Active X / Java / Perl
8. Purchase the Internet Information Server Resource Kit and read the chapter on Security.



Overview

- Password Protection, Privilege Levels
- Configuring Passwords and Privileges
- Traffic Filtering and Firewalling

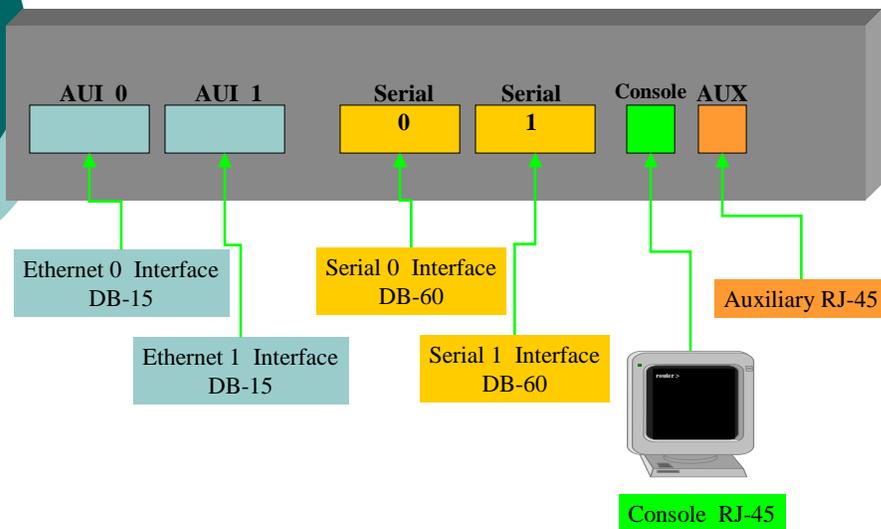
10-1

Cisco 2500 Series Router

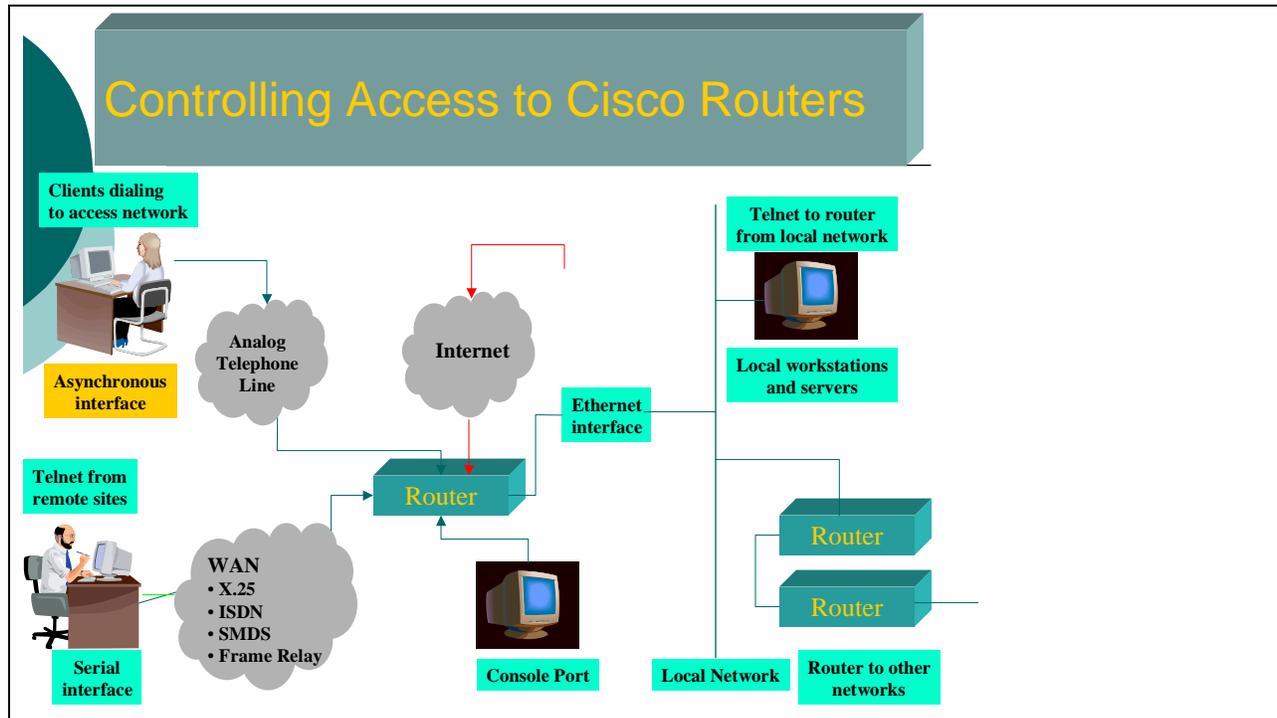
- Primary function is to route network traffic
- Secondary function is to provide packet filtering capabilities for network traffic control and security
- Best suited for small network environments

10-1

Back of Model 2514 Router



10-1



Two Types of Password Access Control Password & Secret

Sniffers can examine packets (and read passwords), you can increase access security by configuring the Cisco IOS software to encrypt passwords. Encryption prevents the password from being readable in the configuration file

- **Enable** password is **NOT** encrypted
- **Secret** password is encrypted (MD5)

When enable password and enable secret are both set, users must enter the enable secret password

10-1

Access to router

Terminal Session to Console port, COM 1, 9600bps

```
User Access Verification  
Password: _
```

Telnet Session to IP 172.24.xxx.xxx

Access password is **student**

10-1

Access to Router/Configuration Modes

- Non privileged mode access >

```
User Access Verification  
Password:  
Router>_
```

- Privileged level access #

```
User Access Verification  
Password:  
Router>enable  
Password:  
Router#
```

10-1

Access to Router/Configuration Modes

- Global configuration mode access

```
Router # config t  
Router (config) #
```

- Interface configuration mode access

```
Router (config) # int e0  
Router (config-if) #
```

10-1

Note: If you need help

Router # ?

Exec commands:

atmsig	Execute Atm Signalling Commands
cd	change current device
connect	Open a terminal connection
dir	List files on given device
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
help	Description of the interactive help system
lock	Lock the terminal
login	Log in as a particular user
logout	Exit from the EXEC
name-connection	Name an existing network connection

10-1

Access to Router

- Privileged level access #
- 16 different privilege levels 0-15
- 15 is the default fully privileged level

Establishing default fully privileged level password

```
Router (Config) # enable password student  
OR  
Router (Config) # enable secret instructor
```

10-1

Access to Router

Establishing intermediate privilege level passwords

```
Router (Config) # enable password level 5 student  
OR  
Router (Config) # enable secret level 5 instructor
```

10-1

Defining Level Command Access

- New levels will have normal user exec mode access by default
- To define access privileges to the ping and trace command for level 5, use the following command:

```
Router (Config) # privilege exec level 5 ping  
Router (Config) # privilege exec level 5 trace
```

10-1

After defining level command access and setting passwords, the next step is to control console, auxiliary and vty (telnet) access.

To verify that the changes we have made are active, type the following command:

```
Router # show running-config
```

To view the original settings when the router booted up, type the following command:

```
Router # show startup-config
```

10-1

Controlling Console, Aux & Vty Access

- Restrict access to console port

```
Router (Config) # line console 0  
Router (Config-line) # login  
Router (Config-line) # password student
```

- Restrict access to auxiliary port

```
Router (Config) # line aux 0  
Router (Config-line) # login  
Router (Config-line) # password dialup
```

Controlling Console, Aux & Vty Access

- Restrict telnet access to vty terminals
- Each ethernet access port on a Cisco router is called a virtual terminal (vty)
 - Cisco routers can have a maximum of 5 virtual terminal ports numbered 0 - 4

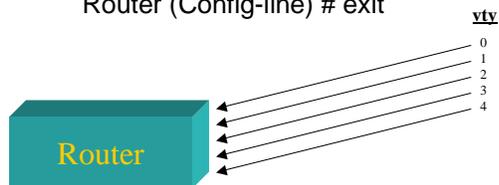
```
Router (Config) # line vty 0 4  
Router (Config-line) # login  
Router (Config-line) # password student
```

10-1

Controlling Console, Aux & Vty Access

Tip: You may wish to limit the amount of available vty ports (default of 5 may be too many). Use the "transport input none" command to accomplish this.

```
Router (Config) # line vty 0 1
Router (Config-line) # transport input none
Router (Config-line) # exit
```



10-1

Controlling Console, Aux & Vty Access

Tip: As administrator you may wish to protect one of the remaining vty ports for your private use only. Do the following to reserve your own vty port.

```
Router (Config)# line vty 2 3
Router (Config-line)# login
Router (Config-line)# Password telnet_users
Router (Config-line)# exit
Router (Config)# line vty 4
Router (Config-line)# login
Router (Config-line)# password MyBackDoor
```

10-1

Protecting Console, Aux & Vty Access

Now that we've set passwords on all the access ports we have to protect the password passwords from being discovered. The following command will encrypt the enable password password. **Note: The enable secret password is already encrypted.**

```
Router (Config) # service password-encryption
```

10-1

Cisco Password Hacks



- Programs are readily available on the Internet which are capable of decrypting user passwords on Cisco routers
 - Not capable of decrypting enable secret ????
 - Can decrypt passwords using the standard Cisco encryption scheme
- It is very important to maintain strict control of configuration files

10-1

Banner Notifications

- Banners are required by policy
- Create banner notifications on Cisco routers with the "banner" command

```
Router (Config) # banner motd @ Type Text Here @
```

- The @ is a delimiting character. It can be any character that is not in your banner.

- To view banner type

```
Router # show run
```

10-1

Setting Session Timeouts

- The default time-out for an unattended console is 10 minutes. It is recommended that this default be changed to a shorter period to minimize the chance of a possible compromise.

- Change the timeout period to five minutes or less.

```
Router (Config) # line console 0  
Router (Config-line) # exec-timeout 5 00
```

10-1

Mid-Break Summary

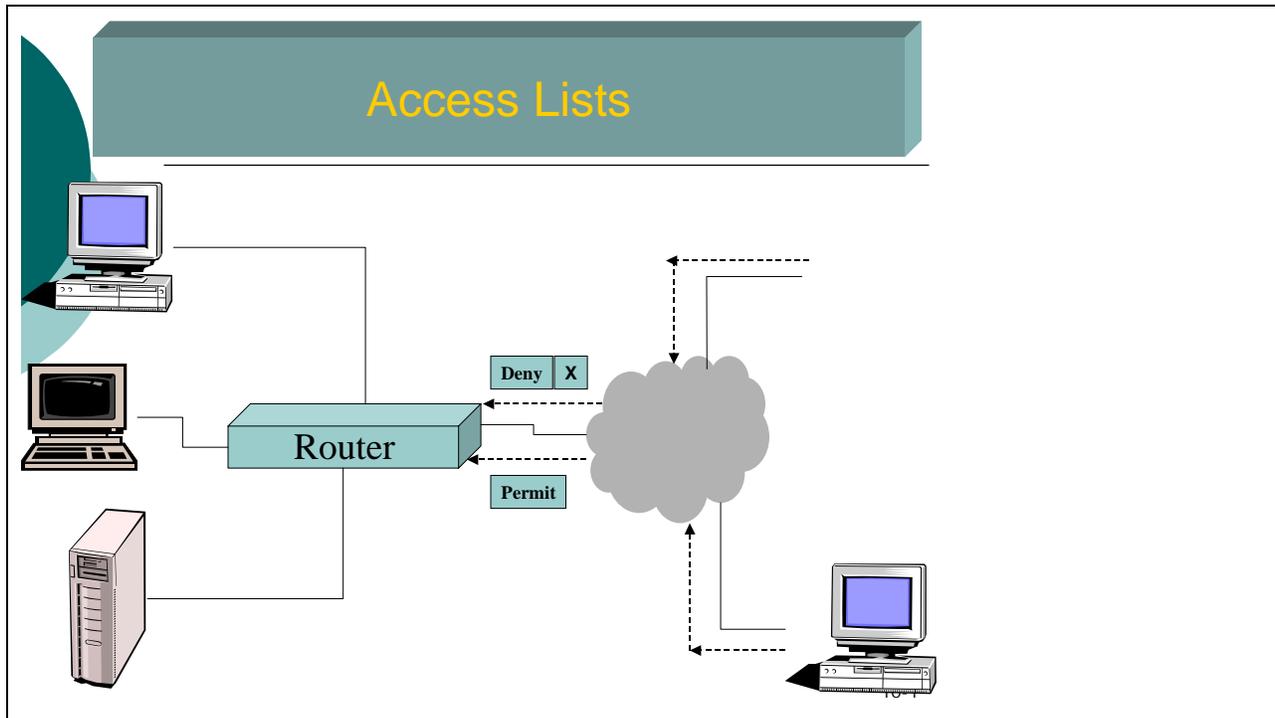
We talked about the following security controls:

1. Password password & Secret Password
2. Password restrictions for privilege level access.
3. Setting command access for privilege levels.
4. Access control to Console, Aux and Vty ports.
5. Creating a warning banner for implied notification.
6. Setting a session timeout for inattentive administrators

10-1

Access Lists

10-1



Why Use Access Lists?

By default, if there are no access lists... all packets will be allowed to any part of your network. You can enhance security and improve network performance by providing control over the traffic forwarded through or blocked from your network

Cisco access lists default to an implicit deny statement for everything that has not been permitted. This supports a deny all and allow only as needed security policy.

10-1

Standard Access Lists (1-99)

Allow filtering by:

- Source Address / Wildcard

10-1

Standard Access List (1-99) example

Creating a Standard Access List

Command	Purpose
Router(config)# access-list <i>access-list-number</i> {deny permit} <i>source</i> [<i>source-wildcard</i>] [log]	Define a standard IP access list using a source address and wildcard.
Router(config)# access-list <i>access-list-number</i> {deny permit} any [log]	Define a standard IP access list using an abbreviation for the source and source mask of 0.0.0.0 255.255.255.255.

Wildcard mask - 32-bit quantity used in conjunction with an IP address to determine which bits in an IP address should be ignored when comparing that address with another IP address

All or none
Wildcard Masks



0 no wildcard

255 wildcard

10-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Standard Access List (1-99) example

Applying a Standard Access List to a virtual terminal line
access-class

Command	Purpose
Router(config-line)# access-class <i>access-list-number</i> { in out }	Restrict incoming and outgoing connections between a particular virtual terminal line (into a device) and the addresses in an access list.

Applying a Standard Access List to an interface
access-group

Command	Purpose
Router(config-if)# ip access-group { <i>access-list-number</i> <i>name</i> } { in out }	Control access to an interface.

10-1

Standard Access List (1-99) example

Case 1

Create an access list that will only allow IP source addresses 192.168.12.42 and 192.168.12.55 to enter an interface.

Case 2

Create an access list that will deny only the IP source networks 192.168.12.0 and 192.168.13.0 from entering an interface.

Case 1 Solution

```
Router (config) # access-list 1 permit 192.168.12.42 0.0.0.0  
Router (config) # access-list 1 permit 192.168.12.55 0.0.0.0
```

Case 2 Solution

```
Router (config) # access-list 2 deny 192.168.12.0 0.0.0.255  
Router (config) # access-list 2 deny 192.168.13.0 0.0.0.255  
Router (config) # access-list 2 permit any
```

Access Lists

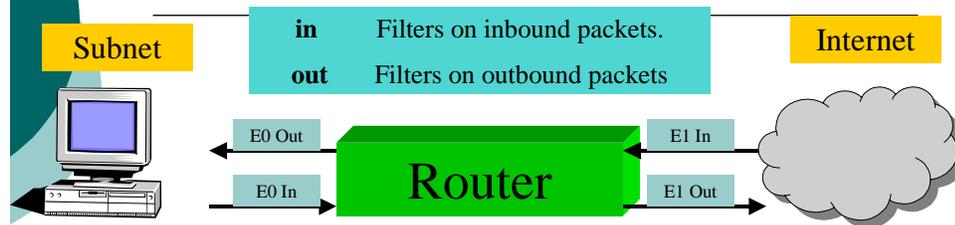
Access lists are processed in sequential order



Access lists cannot be edited on the router. For long access lists, create offline on a text editor, then copy and paste on the router

10-1

Standard Access List (1-99) example



Note: You can only apply one of each type of access list per group and/or class, per interface. Remember, traffic flows both ways on an interface.

Applying Case 2 access-list

```
Router (config) # interface ethernet 1  
Router (config-if) # ip access-group 2 in
```

10-1

Extended Access Lists (100-199)

Allow filtering by:

• Protocol

• Source /
Wildcard

• Destination /
Wildcard

• Port

10-1

Extended Access Lists (100-199)

```
Router (config) # access-list [access-list-number] {permit | deny} [protocol] [source] [source-wildcard-mask] [destination] [destination-wildcard-mask] [operator] [port]
```

Access-list-number = 100-199

Protocol = IP, TCP, UDP, ICMP

Source = Source IP Address

Source-Wildcard-Mask = Assign Wildcard Bits

Destination = Destination IP Address

Destination-Wildcard-Mask = Assign Wildcard Bits

Operand = lt (Less than) gt (Greater than) eq (equal to) neq (Not equal to)

Port = Port numbers and/or range of port numbers you wish to specify

Established = For the TCP protocol only: to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Extended Access Lists (100-199)

Case 1 Create an access list that will allow access to TCP port 80 on an interface and deny all UDP traffic.

Case 2 Create an access list that will deny the TCP protocol on ports 135 and 139 from entering an interface and allow all other protocols and ports.

Case 1 Solution

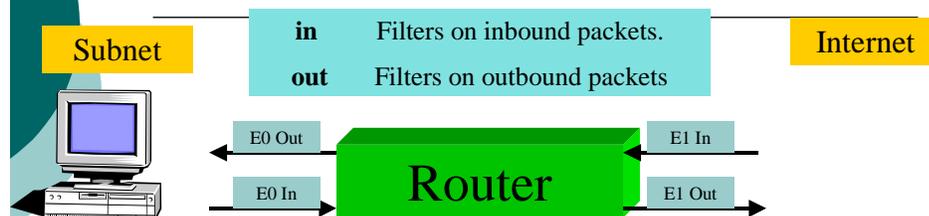
```
Router (config) # access-list 101 deny udp any any  
Router (config) # access-list 101 permit tcp any any eq 80
```

Case 2 Solution

```
Router (config) # access-list 102 deny tcp any any eq 135  
Router (config) # access-list 102 deny tcp any any eq 139  
Router (config) # access-list 102 permit ip any any
```

10-1

Extended Access Lists (100-199)



Note: you can only apply one of each type of access list per group and/or class, per interface. Remember, traffic flows both ways on an interface.

Applying Case 2 access-list

```
Router (config) # interface ethernet 1  
Router (config-if) # ip access-group 102 in
```

10-1

To view access lists

```
Router# show access-lists
```

10-1

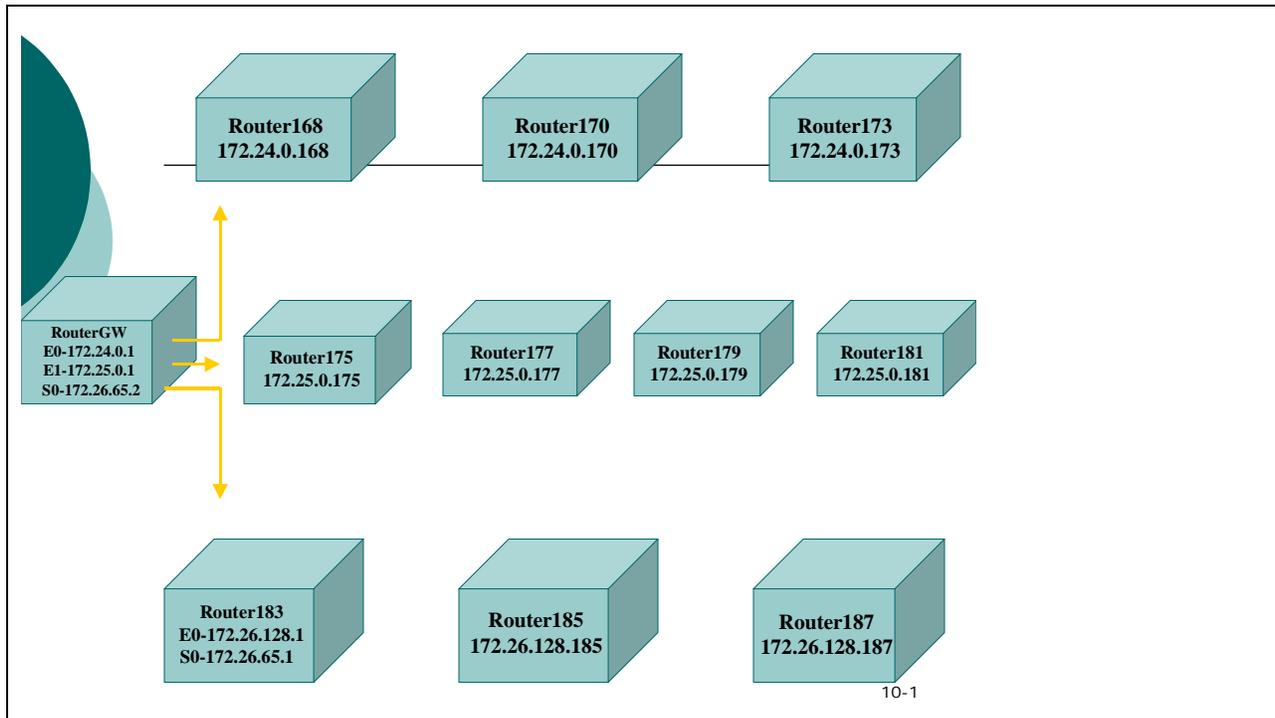
Removing access groups and access lists

```
Router # config t  
Router (config) # int e1  
Router (config-if) #no ip access-group 2 in  
Router (config-if) #exit  
Router (config) #no access-list 2  
Router (config) #<Ctrl> <Z>
```

It is important to remove the list from the interface before removing the access-list itself. If the access-list were to be deleted before it is removed from the interface, corruption of data could occur

10-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY



Questions



10-1

Router Security

Lesson 3

This practical exercise is intended as a supplement to material learned during the Router lecture. Students will become familiar with concepts and commands necessary to operate and secure a Router. Students will become familiar with creating and applying Standard and Extended Access-lists.

Objectives

1. Inspect and change router configurations.
2. Setup and maintain Standard Access-lists.
3. Setup and maintain Extended Access-lists.
4. Recover lost passwords.

Practical Exercise 1

Privilege Levels

The purpose of this PE is to guide you through configuration of privilege level passwords on a router and to familiarize you with the user mode.

1. From the user mode (>) Enter the command: ?
Notice the limited amount of commands. This is privilege level-1. All privilege levels from 1-14 will only have privilege level 1 commands unless other commands are added. Privilege level (0) can also be edited.
2. Open Notepad, then copy and paste all of the commands in the list to it. Save this list as **priv-lvl-1.txt**.
3. Enter the command: **enable**
(Password is student)
What mode have you just entered?
What privilege level are you now at?
4. Enter the command: ?
Do the same as in step 2 above and save to **priv-lvl-15.txt**. Now compare the lists. Which list gives you the most commands?
5. Enter the command: **show running-config**
6. Enter the command: **configure Terminal**
What mode are you now in?
7. Enter the command: ?
Compare this list to the commands in priv-lvl-15.txt. As you can see, the command list is different for each mode.
8. Enter the command: **enable password level 6 cisco**
Explain what this command sets for the router:
9. Enter the command: **privilege exec level 6 debug**
privilege exec level 6 reload
What have these commands done?
10. Enter the command: **CTRL-Z** (This means hold down the control key, and press Z)
Enter the command: **show running-config**
Verify your changes by looking for the privilege commands in the configuration.
11. Enter the command: **Exit**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Press **ENTER** to get back to the > prompt.
What privilege level are you in now?

12. Enter the command: **Enable 6**

Are you prompted for a password ?

Which password works with this command?

What type of prompt do you have now?

13. Enter the command: **?**

Are there any extra commands added? (Compare to priv-lvl-1.txt)

14. Enter the command: **Exit**

Practical Exercise 2

Password Management

You can control access to your router and to the use of privileged commands through the use of passwords. We will be setting passwords for console, VTY, and the enable secret. We will also encrypt all the passwords on the router.

Setting the console terminal password.

1. Set the console password to **con_user** by entering the following commands:

```
Router>enable  
Password: student  
Router#config t  
Router (config) #line console 0  
Router (config-line) #login  
Router (config-line) #password con_user  
Router (config-line) #<CTRL-Z>
```

2. Type **exit** and ensure that the password has been changed by logging back into the router.

Setting the password for telnet connections.

3. Set the vty 0-4 passwords to **telnet_user** by entering the following commands:

```
Router#config t  
Router (config) #line vty 0 4  
Router (config-line) #login  
Router (config-line) #password telnet_user  
Router (config-line) #<CTRL-Z>
```

4. Now **exit** and verify the password was successfully changed by telnetting to the Router. (Remember, if you decide to telnet from the console, you will have to enter the console password first)

Take a look at the running configuration file:

```
Router# show running-config
```

Are the passwords you just set viewable in clear-text?  S/NO

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Encrypting all passwords.

5. Encrypt the passwords by entering the following command:

```
Router#config t  
Router (config) #service password-encryption  
Router (config) #<CTRL-Z>
```

Let's take another look at the running configuration file:

```
Router# show running-config
```

Are the passwords you just set viewable in clear-text? **YES** 

Changing the Secret password.

6. Set the Secret password to **Roscoe** by entering the following commands: (The Enable Secret password will override the Enable password for privileged level access)

```
Router#config t  
Router (config) #enable secret Roscoe  
Router (config) #<CTRL-Z>
```

7. Now **exit** and verify the password was successfully changed. (Remember the console password from earlier, you will still need it before you can check your new Enable Secret.)

Take a third look at the running configuration file:

```
Router# show running-config
```

Is there a difference between the encrypted **Password** password and the **Secret** password?

 **S/NO** Explain:

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise 3

Banner Creation Configuration

The purpose of this lab is to show you how to use the banner commands to create specific login banners.

Create a login banner that is viewable while gaining terminal access to your router.

You must be in global configuration mode to configure a banner.

Router (config) # **banner motd** @ <Hit Enter>

"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, INCLUDING 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. UNAUTHORIZED USE 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 THESE PURPOSES."
@ < Hit Enter>

Router (config) #

Now exit and log back in to verify the functionality of your banner. Have another person telnet into your router to verify the functionality of it.

After verifying the functionality of the banner, continue to PE 4.

Practical Exercise 4

Standard Access List (SAL) Configuration

Objective: Configure a SAL to block a network and activate the access-group for inbound traffic.

1. Choose one network in your classroom to be a trusted network. Once you have the IP and wildcard mask figured out for that network, use them in the following commands to ensure that they are the only network allowed to send data into yours. You also need to decide which interface(s) to apply the access-list to. Fill in the blanks below, enter the Global Configuration, and type the following: (note that steps **d** and **e** may not be necessary if you only need to apply this to one interface)
 - a. Router (config) # **access-list 1 permit** _____
 - b. Router (config) # **interface** _____
 - c. Router (config-if) # **ip access-group 1 in**
 - d. Router (config-if) # **interface** _____
 - e. Router (config-if) # **ip access-group 1 in**
 - f. Router (config-if) # **Ctrl Z**
2. Once you have applied your access list, try to “**PING**” one of the IPs in a blocked network. Were you successful? **Yes** / 
3. Now “**PING**” one of the IPs you allowed. Were you successful?  / **No**
4. Use the “**show access-list**” command from the Privileged Mode prompt to look at your access-list.
5. Once the **instructor** has verified that the access list is working you need to remove the access list. Fill in the blanks below, and use these commands. Remember: If you only applied to one interface, then some of these steps aren’t needed.

Router (config) # int _____
Router (config-if) # no ip access-group 1 in (This removes the list from the interface)
Router (config-if) # int _____
Router (config-if) # no ip access-group 1 in (This removes the list from the interface)
Router (config-if) # exit
Router (config) # no access-list 1 (This deletes the entire list)
Router (config) # <Ctrl-Z> (This means press the “control” and “z” keys together)

It is important to remove the list from the interface before removing the access-list itself. If the access-list were to be removed before it is removed from the interface, corruption of data could occur.

6. After removing the access-lists, try to “**PING**” one of the routers in the other networks. Were you successful?  / **No**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise 5

Standard Access List (SAL) Configuration #2

Objective: Configure a SAL to block two specific IP address within trusted networks, and activate the access-group on your router.

Choose 2 networks in the classroom to be the **only trusted networks**.

Choose 1 computer IP address **from each** of those networks to be **untrusted systems**.

We need to develop an access list with the following definitions being true:

- A. Permit access from any trusted networks.
- B. Deny access from all untrusted addresses.

You now have the required information to create the SAL. Keep the untrusted addresses from entering your router and allow the trusted networks access to your router. All other networks that have not been defined as trusted are to be considered untrusted. Fill in the blanks with the appropriate commands.

Fill in the blanks, and then enter the commands into your router from Global Configuration Mode. (All lines and blanks may or may not be necessary)

```
Router (config) # access-list _____  
Router (config) # interface _____  
Router (config-if) # ip access-group _____  
Router (config) # interface _____  
Router (config-if) # ip access-group _____  
Router (config-if) # Cntrl Z
```

After applying your access list, have the untrusted addresses try to access your router. (Telnet and/or Ping) Were they successful? **Yes** / 

The **instructor** will verify that your access list is working.

Now, pick the first network you allowed and deny the other host on that network. (Hint: A text editor might prove useful)

The following instructions will walk you through the basics on it:

Router#**sh run**

(From this prompt you may copy/paste the ACL to notepad, and edit the ACL to add the new host that you want to deny.)

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Now, remove the old ACL, and put the new one back in its place. (note that all of these commands may not be necessary if you only placed an ACL on one interface.)

This removes it: (Fill in the blanks first, then perform the steps on your router)

```
Router#confi t  
Router (config) # int ____  
Router (config-if) # ____ip access-group ____ in (Remove the list from the first interface)  
Router (config-if) # int ____  
Router (config-if) # ____ip access-group 1 in (Remove the list from the second interface)  
Router (config-if) # exit  
Router (config) # ____access-list ____ (Delete the entire list)
```

Time to add it back:

```
Router (config) #  
(From this point, recall how you placed the access list the first time, and do it again.)
```

Configure an ACL for your VTY connections. Use the second trusted network and only allow VTY connection from that network.

Fill in the blanks, and then enter the commands into your router from Global Configuration Mode. (All lines and blanks may or may not be necessary)

```
Router (config) # access-list _____  
Router (config) # access-list _____  
Router (config) #line vty _____  
Router (config-line) #access-_____ _____  
Router (config-if) # Cntrl Z
```

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

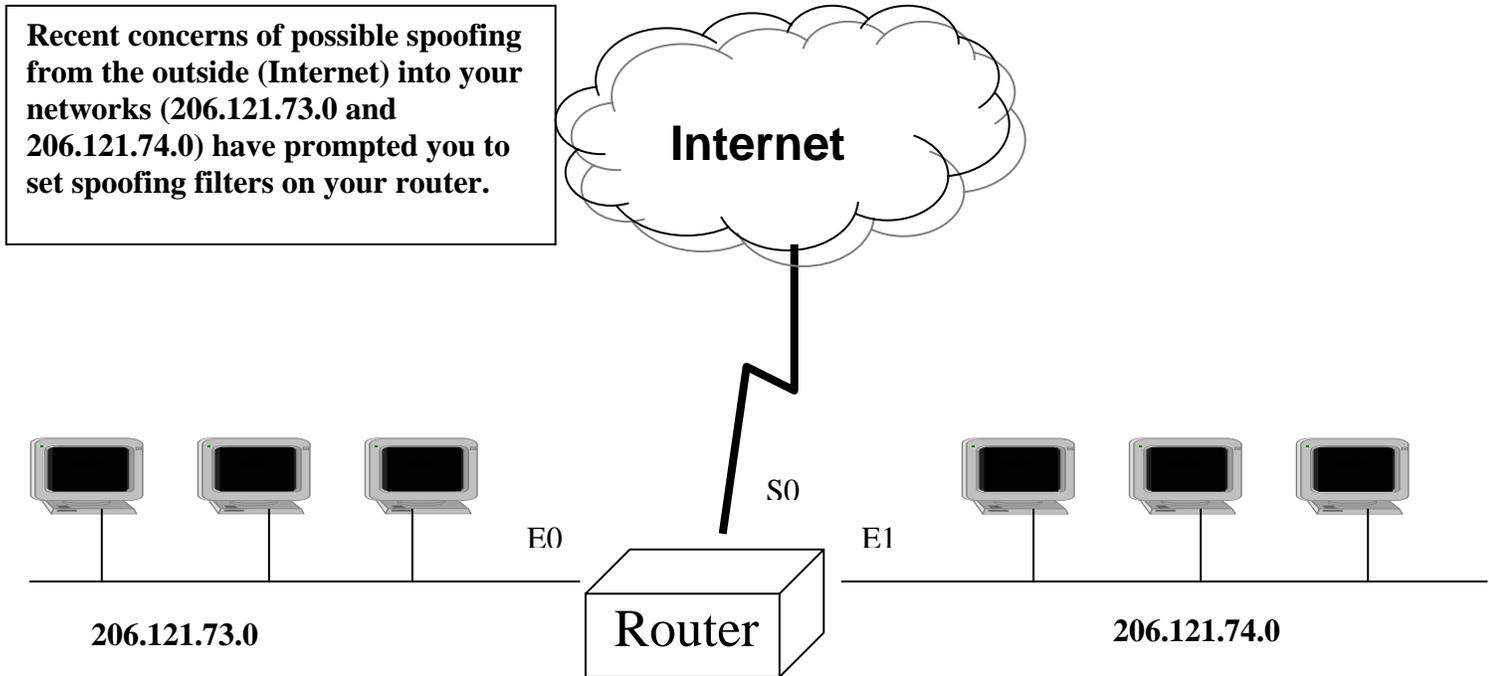
Practical Exercise 6

Spoofing Filter

Note: This will be covered in discussion. DO NOT APPLY THIS TO YOUR ROUTER!

Objective 1: Configure a SAL to prevent untrusted networks from spoofing inside addresses.

Objective 2: Configure a SAL to prevent your inside trusted networks from spoofing other outside networks.



What statements must be included in your access list to prevent your internal networks from being spoofed? (Only write out the entries that apply to the problem above, don't worry about the whole list.)

Router(config)# _____

Router(config)# _____

What port(s) will you apply the access-list to? _____ Will it be applied inbound or outbound? _____

Can you prevent inside users from spoofing out? _____ If so, show how?
(Remember, maximum security.)

Router(config)# _____

Router(config)# _____

What port(s) will you apply the access-list to? _____ Inbound or outbound? _____

NOTE: Answers may vary!

Practical Exercise 7

Extended Access List (EAL) Configuration

Objective: Configure an EAL to block certain TCP/IP services from specified networks, and apply the EAL on the interface(s) of the router.

1. Configure an EAL on your router for traffic coming in from connected networks.
 - A. Allow certain addresses to Telnet (port #23) to your network (pick a few IPs in the room).
 - B. Block all Telnet (port #23) traffic from all other networks.
 - C. Allow Pings (ICMP Echo Packets) from only certain addresses (pick a few IPs in the room).
 - D. Deny all other ICMP traffic to enter your router.
 - E. Once you have decided on the IPs, fill in the blanks below, and apply to your router.

Router # **config t**

(repeat the next step for all IP addresses you want to allow to telnet to your router)

Router (config)# **access-list 101 permit tcp** _____ **any eq 23**

(this will deny everybody else)

Router (config)# **access-list 101 deny tcp any any eq 23**

(specify the IPs you want to allow to ping to you)

Router (config)# **access-list 101 permit icmp** _____ **any**

(allow ICMP replies to work)

Router (config)# **access-list 101 permit icmp any any echo-reply**

(block all other ICMP)

Router (config)# **access-list 101 deny icmp any any**

(allow anything else not specified above to work)

Router (config)# **access-list 101 permit ip any any**

(repeat the next two lines for any interfaces this should be applied to)

Router (config)# **interface** _____

Router (config-if)# **ip access-group 101 in** (applies the access list 101 to the interface)

Router # <Ctrl> **Z**

2. Once you have completed loading your Extended Access List do the following:

Have someone you allowed telnet to your router.

Were they successful?  / **No**

Have someone that was not allowed telnet to your router.

Were they successful? **Yes** / 

Have someone you allowed ping your router.

Were they successful?  / **No**

Have someone you did not allow ping your router.

Were they successful? **Yes** / **No**

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Practical Exercise 8

Password Recovery Procedures

Objective: Recovery in case the Enable Secret password is lost or forgotten. This procedure works for all 2500 series routers running Cisco Release 10.0 and above.

- 1 Power cycle (turn off and then on) the router and within 10 seconds after the router starts to load, hold down the “**ctrl**” key and hit the “**break**” key several times. The system will stop the Boot Process and you will not get a router prompt.
- 2 Type **o/r 0x2142** at the > prompt to boot from Flash without loading the configuration.
Example: >**o/r 0x2142**
- 3 Reboot the router.
Example: >**i** (the router reboots but ignores its saved configuration)
- 4 Answer **NO** for “Would you like to enter the initial configuration dialog?”
- 5 Enter privileged mode.
Example: Router>**enable**
- 6 Load NVRAM to active memory.
Example: Router#**configure memory** (you might have to hit enter twice).
- 7 Type **show run** to show the configuration of the router. In this configuration you will see that all the interfaces are currently shutdown. You will also see the passwords in either encrypted or unencrypted format.
Example: Router#**show run**
- 8 Type **config t** to access the global configuration. Then change the enable-secret password and bring up the interfaces.

Example: Router#**config t**
Router(config)#**enable secret student** (change the password back to student)
Router(config)#**interface e0** (specifies the ethernet 0 interface)
Router(config-if)#**no shut** (turns on the interface)
NOTE: IF YOU ARE USING MORE THAN ONE INTERFACE, YOU WILL HAVE TO REPEAT THE COMMANDS ABOVE TO TURN ON THOSE PORTS AS WELL!
- 9 Enter the command to specify the original configuration setting.
Example: Router(config)# **config-register 0x2102**
- 10 Press <**Ctrl-z**> to return to privileged mode. Then save changes to NVRAM.
Example: Router(config)# <**Ctrl-z**> <**Enter**>
Router# **write mem** or **copy run start**

Reading assignment 3

Subject: **Firewalls, Proxies, and VPNs**

Pages: 55-69, 85-96, 138-142, 297-321

(Complete before day 4)

1.  Here are some typical locations for firewall placement?

2.  What are 2 strategies of multiple firewall deployment?
 - 1.
 - 2.

3.  What are their purposes?

4.  Name 3 types of proxies:
 - 1.
 - 2.
 - 3.

5.  Briefly explain each type:

6.  What are 2 types of NAT assignment?
 - 1.
 - 2.

7.  What are some other names used for PAT?

8.  What does NAT allow you to do with hosts in your network?

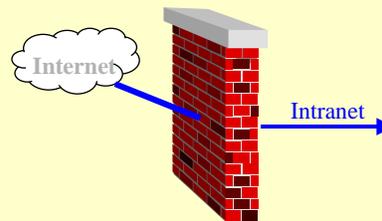


Firewalls

Module 11

What is a Firewall?

A firewall is any computer, router, or combination of both, that controls access between two networks, whether it is a commercial product or home-made box.

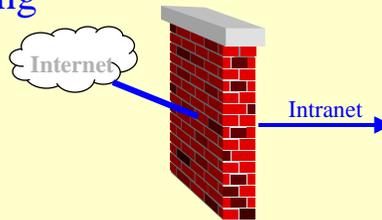


September 20, 2004

11-1

Firewall Types

- Static packet filtering
- Dynamic packet filtering
- Stateful packet filtering
- Proxy



September 20, 2004

11-1

Static Packet Filtering

Controls traffic by using information stored within the packet headers. Packets received are compared against the access control policy in effect. Packets will be either be forwarded or dropped depending on the active policy.

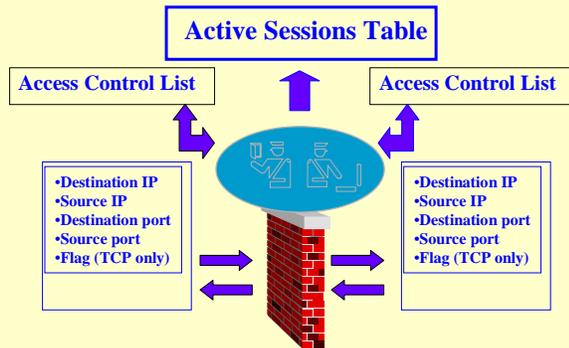


September 20, 2004

11-1

Dynamic Packet Filtering

Similar to static packet filtering except that it also maintains an active connections table that monitors the state of a communication session.

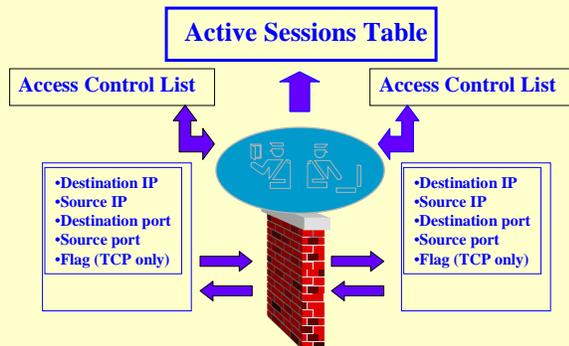


September 20, 2004

11-1

Stateful Packet Filtering

Similar to dynamic packet filtering except that it also maintains an active connections table that monitors the sequence of events for a communication session.

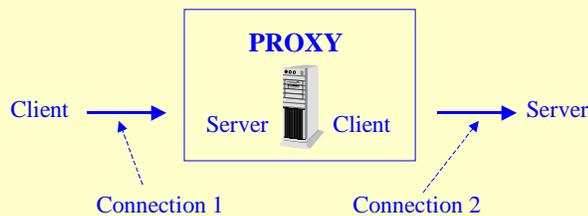


September 20, 2004

11-1

Proxy or Application Gateway

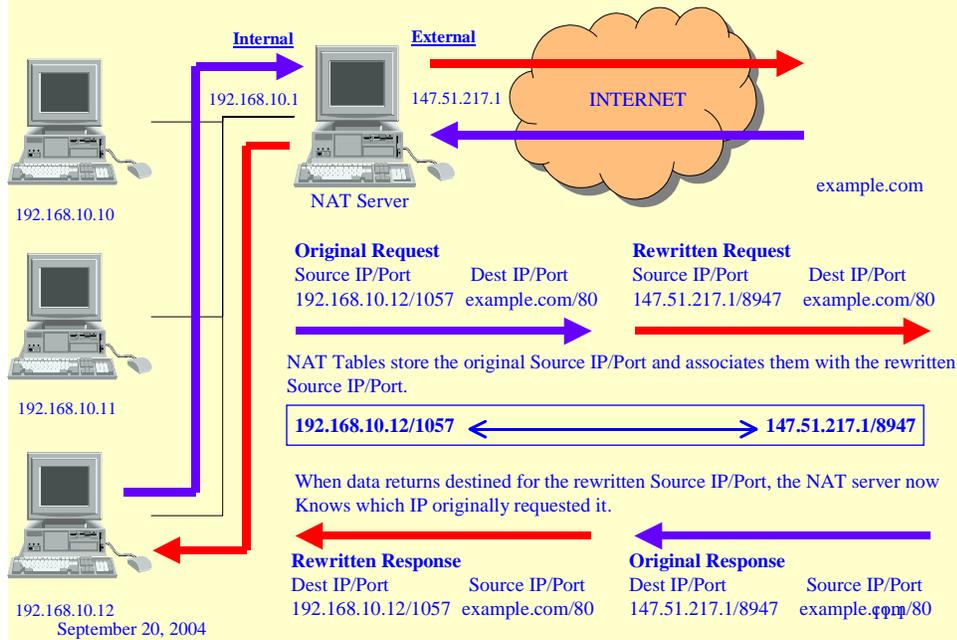
- Plays middleman between two network segments
- Source and destination never actually connect
- Stands in and speaks for each system on each side of the firewall



September 20, 2004

11-1

Network Address Translation



September 20, 2004

Firewall Capabilities

- Logging and Notification
Documents all traffic that passes through it and can provide alerts
- Virtual Private Networking (VPN)
As a “flowpoint” for external traffic, firewalls are a perfect place to implement VPNs for remote access
- Filter Java, ActiveX, and HTML Scripts
Remove Java/ActiveX applets from incoming HTTP datastream

September 20, 2004

11-1

Firewall Capabilities

- Address Processing
Provides the ability to control how systems are identified through the firewall
- Weak and Strong Authentication methods
 - ACE/Server
 - Cryptocard
 - S/Key
 - Gateway passwords
 - NT Domain authentication

September 20, 2004

11-1

Potential Firewall Weaknesses

- Have you compromised your own firewall?
- Tunneled Protocols and Firewalls
- Other ways to neutralize a firewall

September 20, 2004

11-1

Compromised Your Own Firewall?

- Where's your perimeter?
It's hard to prove you're protecting your assets when you can't even identify all of them
- Dial-in modem access commonly bypasses the firewall
- "Flavor of the day" protocols often allowed
Proxy-based firewall bypassed by opening ports for applications which don't yet have proxies available

September 20, 2004

11-1

Tunneled Protocols and Firewalls

- Anything can be tunneled over other protocols
e.g, Pointcast over HTTP, Telnet/NFS over e-mail
- Tunneling/Encapsulating traffic is routine
- Even if you only allow e-mail in and out, almost anything can “piggyback” over that channel

September 20, 2004

11-1

Other ways to neutralize a firewall

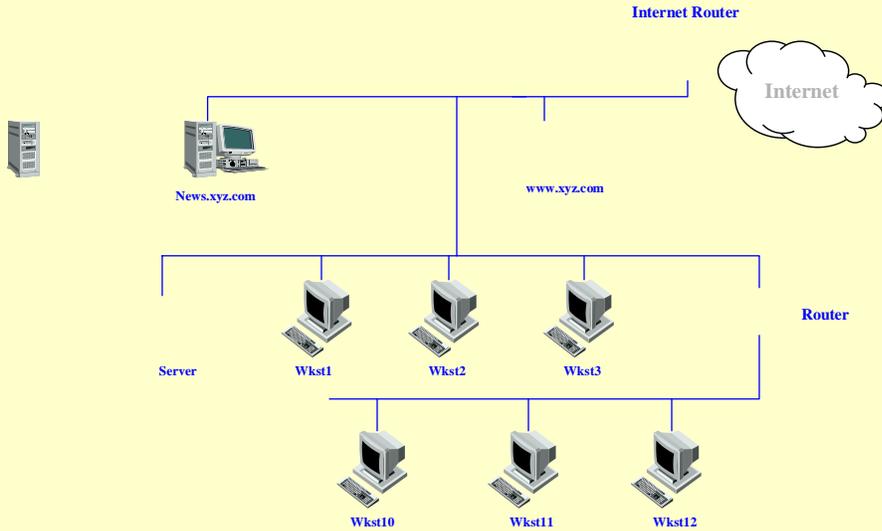
- Excessive Alarms
- Bypassing the firewall
If users get into the network in any way besides through the firewall, it does nothing to protect your systems
- Compromise an insider
Not every user, programmer, or system administrator is perfectly ethical. Firewalls do not protect from insider attacks!
- Trojan horses

September 20, 2004

11-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

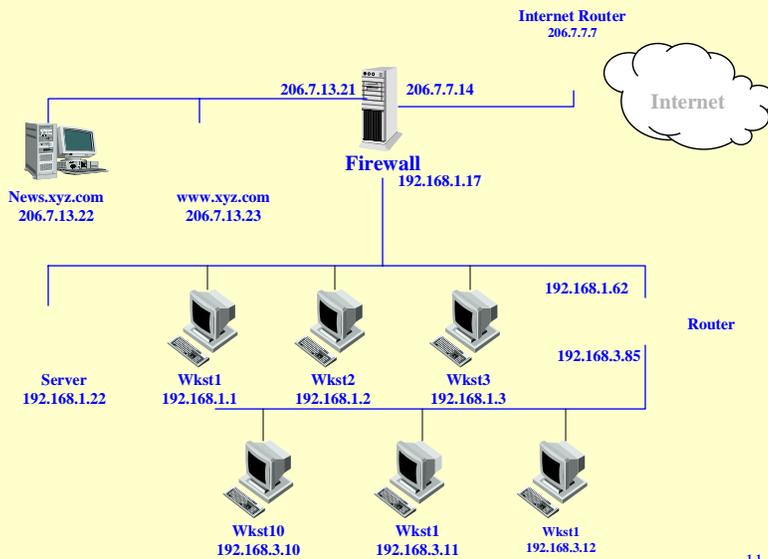
Network without a Firewall



September 20, 2004

11-1

Network with a Firewall



September 20, 2004

11-1

Summary

- Intelligent employment and configuration of Firewalls can significantly improve organizational security
- The goal is to allow inside and outside users access to as many services as possible without compromising the security of the network
- There are certain things which Firewalls cannot defend against

September 20, 2004

11-1

QUESTIONS?

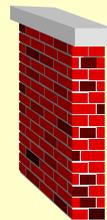
September 20, 2004

11-1



Symantec Enterprise Firewall

Module 12



Symantec Raptor Firewall

- A software product that provides enterprise-wide network security
 - Access control and service authorization both into and out of your network
 - Secure communication between two or more internal networks across the Internet
 - Suspicious activity monitoring with logging and automatic alerts

Symantec Raptor Firewall

- Application level firewall
- Runs on a dedicated network host
- Operates as a proxy for TCP/IP services
- All connections are checked against authorization rules
- All packets are re-packetized by the Firewall

September 20, 2004

12-1

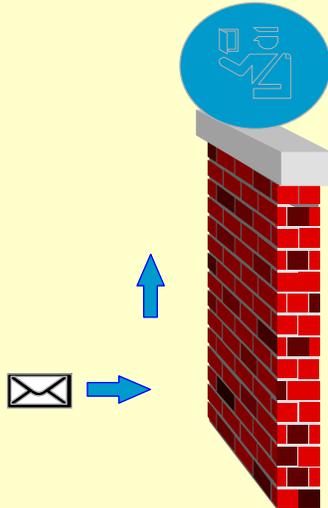
Hardware Requirements (NT/W2K)

- General
 - System must be listed with the NT Hardware Compatibility List (HCL)
 - Minimum 2 Network Cards (NIC)
 - Intel Pentium II Processor
- 256 MB memory (more recommended)
- 4 GB HD (more recommended)
- Bit mapped display console (min. 1024x768)

September 20, 2004

12-1

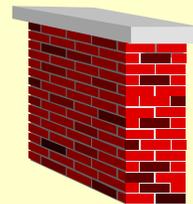
Proxy Service Daemons



- Examines all TCP/IP-based connection events in and out of the network it secures
- Allow or deny connection based on authorization rules
- Challenge for strong authentication as required
- Monitor direction of service (FTP) and URLs (HTTP)
- Can redirect certain services
- Log all session data

September 20, 2004

12-1



Planning and Configuration

September 20, 2004

12-1

(1) Perform an Audit

- Network Connection devices such as gateways, routers, bridges and repeaters
- Modems and modem pools
- Terminal servers and remote access servers
- Networking and applications software
- Information in files and databases

September 20, 2004

12-1

(2) Determine Use of Common Services

Your policy should only allow the types and degrees of access necessary to support business goals.

- Some services are used generally and widely
 - HTTP (web browsing)
 - SMTP (electronic mail)
- Other services are used more selectively
 - Telnet (remote login)
 - FTP put, FTP get (put or get files)

September 20, 2004

12-1

(3) Define your Users and Groups

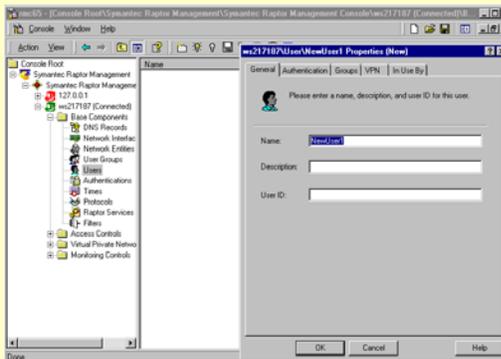
- Carefully defining the needs of specific groups and users makes it easy to create and maintain rules
- Get the buy-in of managers/leaders if you need to restrict services (HTTP, SMTP,FTP)
- Policies that are overly restrictive encourage violations
- Policies that are not restrictive enough may be vulnerable to compromise

September 20, 2004

12-1

USERS

- Several kinds of users
 - General
 - Trusted
 - Gateway
 - Dynamic
- Define your users as you would in NT or Solaris

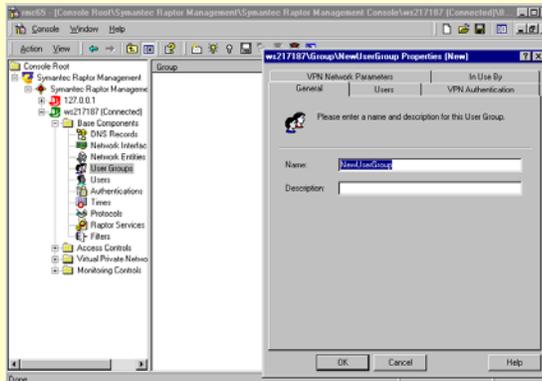


September 20, 2004

12-1

GROUPS

- You define your groups as you would in NT or Solaris
- Group ID is unique
- Allows users to telnet or ftp into internal servers



September 20, 2004

12-1

(4) Determine your Level of Authentication

- Determine the types of authentication to use for accessing users
- Outside-inside connections should require strong authentication
- Inside-outside connections can be transparent, or use gwpassword authentication

September 20, 2004

12-1

Authentication (cont)

- Validate a user's identity based on password response
- Authentication methods supported
 - Gateway - multi-use password like a standard login
 - S/KEY or Cryptocard - one-time use password generated by client/server software
 - ACE - one time use password generated by smart card
 - others

September 20, 2004

12-1

(5) Identify Key Host Systems

- Key Host Systems comprise all those used for specific purposes, both inside and outside of your network.
- Examples of internal systems:
 - Mail server
 - WWW server
 - Centrally used databases

September 20, 2004

12-1

(6) Outline Policy

- Sketch out your policy, in general
- Identify the services each group will need: - *Allow ftp gets from finance to HostA*
 - *Allow Web access from inside to Universe*
- Identify any exceptions. Examples:
 - *Deny all svcs from contractors to outside*
 - *Deny all svcs from temps to Universe*
- Begin writing rules...

September 20, 2004

12-1

Symantec Raptor Management Console

Symantec Raptor interface gets you started



September 20, 2004

12-1

Symantec Raptor Management Console

- The SRMC is the native Windows NT GUI used to manage the Symantec Raptor Firewall.
- For Unix systems, the GUI is named the Symantec Raptor Console for Unix (SRCU)

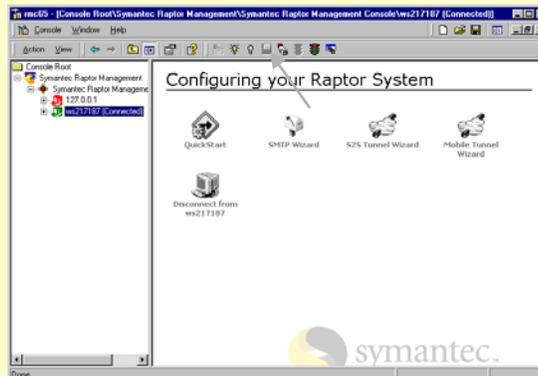


September 20, 2004

12-1

Symantec Raptor FILE | SAVE

- Changes don't take place on Firewall until you save!

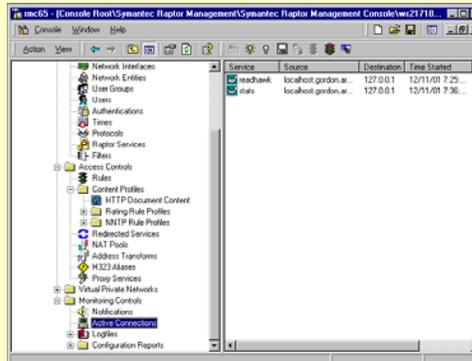


September 20, 2004

12-1

Monitor Active Connections

- Provides general information on ongoing connections through the GW
- Allows you to kill ongoing connections
- You can start and stop the GW

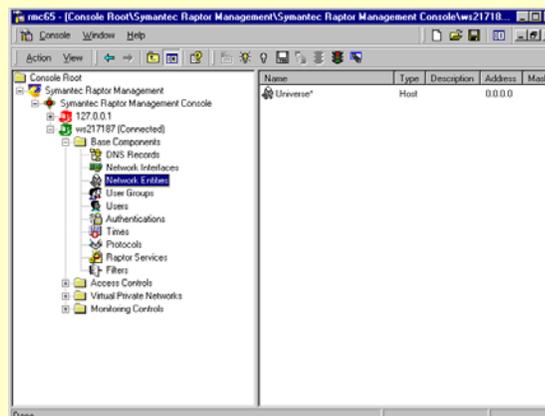


September 20, 2004

12-1

NET ENTITIES

- Create your NET ENTITIES as one of your first firewall admin steps
- Name is unique
- Can use IP or HOSTNAMES

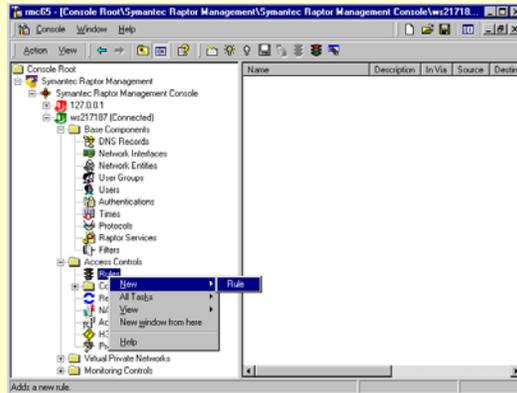


September 20, 2004

12-1

RULES

- Right-click on rules

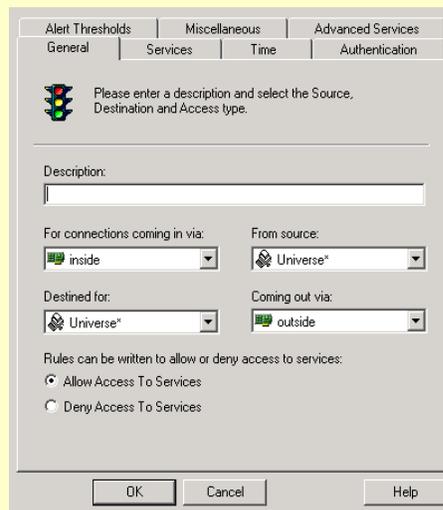


September 20, 2004

12-1

RULES

- Source & destination boxes can be filled with system or user-created entities
- * = system created
- Click Permit or Deny

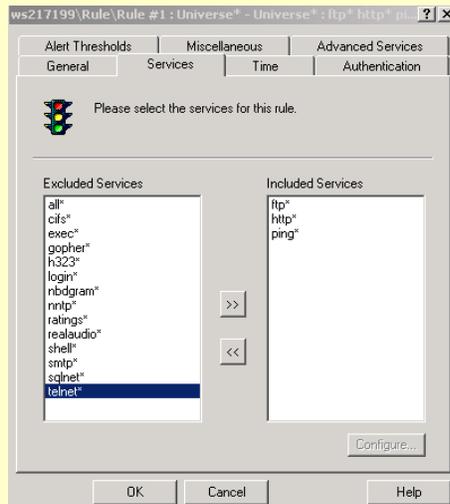


September 20, 2004

12-1

RULES

- Services

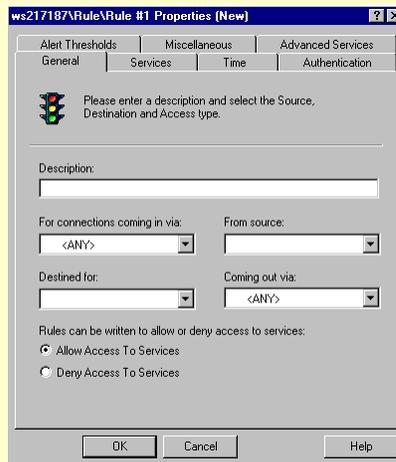


September 20, 2004

12-1

RULES

- Time tab
- Authentication
- Alerts
- Miscellaneous
- Advanced Services

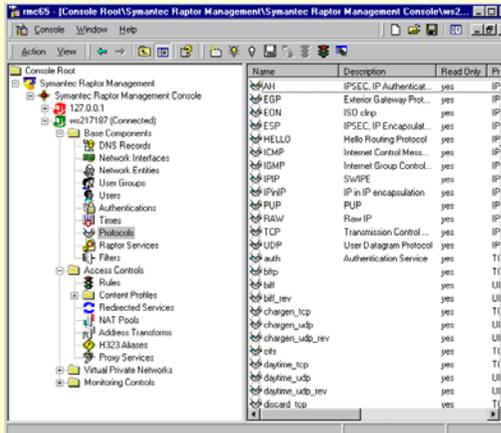


September 20, 2004

12-1

PROTOCOLS

- Symantec Raptor Firewall uses a set of standard application proxies to handle commonly used services.
- Other services are handled by the GSP.

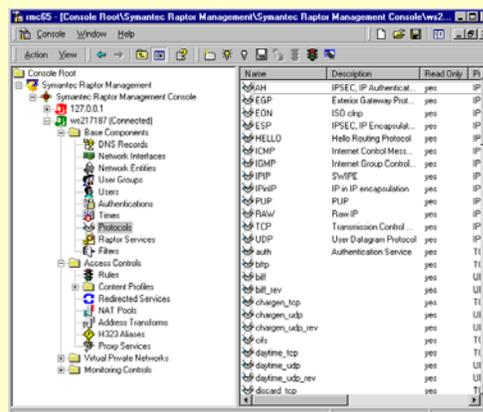


September 20, 2004

12-1

Custom Protocols

- Configures generic or “custom” services provided by the hosts on either side of FW
- They are now configured through Protocols. Just right click on **protocol** > **new** > **protocol**.

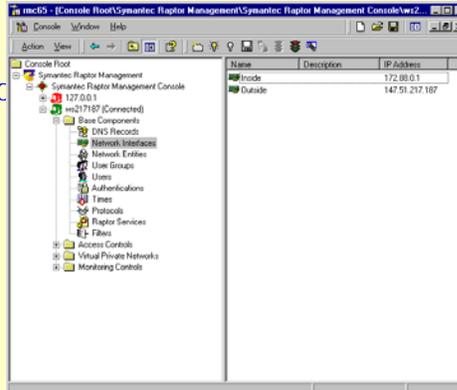


September 20, 2004

12-1

Network Interface Properties

- Shows all of the network interfaces
- Highlight interface to edit its properties



September 20, 2004

12-1

Illegal Address Support

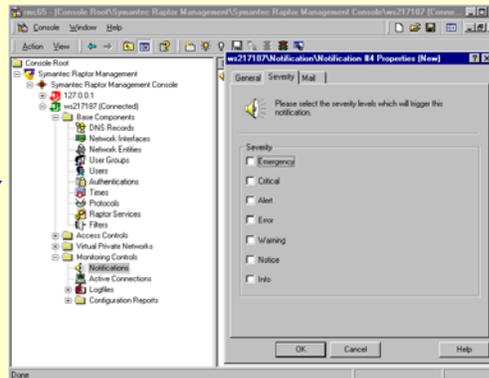
- Conforms to RFC 1597
 - Reserves a set of unallocated Class A and Class B network numbers
 - 10.0.0.0 thru 10.255.255.255
 - **172.16.0.0 thru 172.31.255.255**
 - 192.168.0.0 thru 192.168.255.255
 - These in turn can be mapped to internal illegal IP addresses

September 20, 2004

12-1

NOTIFICATIONS

- Notifies designated personnel to respond to alerts
- Allows you to specify the type of alert for the severity of the connection attempt

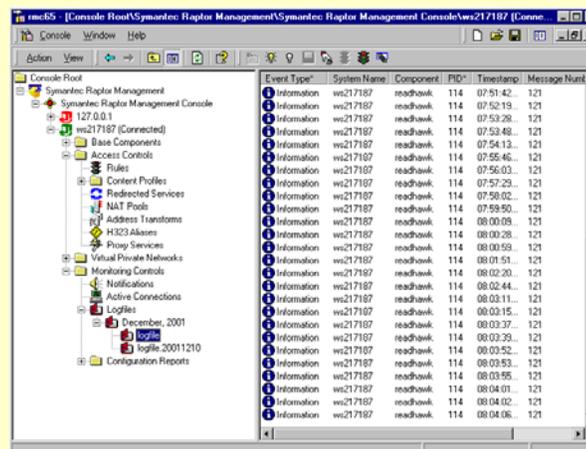


September 20, 2004

12-1

Logfile

Provides detailed information on all connections and connection attempts to the firewall



September 20, 2004

12-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY



QUESTIONS?

Firewall Security

Lesson 4

This practical is intended as a supplement to material learned during the Raptor Firewall lecture. Students will setup and configure the firewall to provide security and prevent unauthorized access to their internal network.

Objectives

1. Configure rules on the firewall
2. Check firewall for configuration management
3. Inspecting Logfile and Active Connections
4. Configure firewall for Virtual Private Networking

Symantes Raptor Practical Exercise #1 Setup of the Raptor Firewall 6.5

- *Your Raptor Firewall has been installed already*
- *The interface does not have to be activated for the firewall to run; Raptor Management Console (RMC) is used for configuration and management of the firewall*
- *Follow these instructions below and answer the questions—use only the firewall computers, and the “subnet” computers as instructed*

Remember: Anytime you make any changes, additions, and/or subtractions to the firewall console, press the save and reconfigure button on the power bar or they won't take effect.

1. Start the firewall configuration console:
 - **START > PROGRAMS > SYMANTEC RAPTOR MANAGEMENT CONSOLE > RAPTOR MANAGEMENT CONSOLE** (Note: If there is an icon on your desktop you can use that also to start the RMC).
2. In the **Getting Connected** window, click on the **Connect To Localhost** icon. The **Welcome to the Symantec Raptor Management Console** box will appear. The name will always be **Localhost** and the **Management Port** will always be 418. Type in **student** in the password box and click on the OK button.
3. To verify the connection, look at the left column and look at the name (**Your Computername**) and in parenthesis you should see the word **Connected**.
4. Right-click (**Your Computername**) (**connected**), and choose **Properties** and the **General Tab**. What is the: System ID _____
License Key _____

When finished, click on the **OK** button

NOTE: This license key is from the company, and is related to the Volume ID serial number of the hard drive that it is installed on.

5. On the Symantec Raptor Management Console, expand the (**Your Computername**) (**connected**) and the **Base Components** folder. Click on **Network Interfaces**. You will see two network adapters. One **Outside NIC** and one **Inside NIC**.

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Symantec Raptor Firewall Practical Exercise #2
Checking Connectivity

- *Your Raptor Firewall is still properly installed*
- *Follow these instructions below and answer the questions—use both the firewall computers AS WELL AS the “subnet” computers (**the subnet pc is the computer behind the firewall**)*
- *Write down abbreviated responses in your answers only*
- *Use Command Prompt for ping, telnet, and FTP.*

1. From the **Firewall Computer** check out the firewall’s interface status by doing the following steps:

Do you get a reply when you  **the Instructor’s computer**
YES / NO

Do you get a reply when you  **the subnet computer’s network interface card:**
YES / NO

2. From the **Subnet Computer**, type the following commands:

Do you get a reply when you  **the internal interface of the firewall computer:**
YES / NO

Do you get a reply when you  **the external interface of the firewall computer:**
YES / NO
Why? _____

Do you get a reply when you  **the Instructor’s computer:**
YES / NO
Why? _____

Do you get an address when type in  **lookup www.gordon.army.mil**
YES / NO

If you got an IP address, what was it? _____

(This is an example of an information leak, the instructor will discuss it with the class)

Symantec Raptor Firewall Practical Exercise #3 Inside vs. Outside Transparencies

- *Your Raptor Firewall is still properly installed*
- *Write down abbreviated responses in your answers only*
- *REMEMBER: Any and all changes must be saved using the save button and reconfigured using the reconfigure button on the power bar before they can take place.*

Expand the **Access Controls** folder and highlight rules, right click and choose **New > Rule**.

- In the **Description Box**, type in **Outside**.
- Select **Inside** in the **For Connections Coming in Via Box**.
- Select **Universe** as your **From Source**:
- Select **Universe** as your **Destined For**:
- Select **Outside** in the **Coming Out Via Box**.
- Check the block to Allow access to Services:
- Select Services Tab:
- Add **ping**, **telnet**, and **http** protocols as **Included** services
- Click **OK** when finished
- **Save the current configuration and reconfigure the firewall.**

1. From your subnet computer try to telnet to the **Installation Gateway Router** (Instructor will provide you with the IP). Do not attempt to login, you are just verifying that telnet works. Do you get through? **YES/NO**
2. Next, ping the **Instructor's computer**. Is the ping successful? **YES/NO**
3. Open up Internet Explorer. In the address bar, enter the Instructors IP Address. Do you get a website? **YES/NO**
4. Open up a command prompt. From the command prompt FTP to the instructors computer. Do you get an FTP login prompt? **YES/NO**
5. Explain why the above steps did/didn't work:

6. Modify the rule you created by double-clicking it, and selecting the Services tab. Add **FTP** to the list of **Included** services.

Symantec Raptor Firewall Practical Exercise #4

Filtering, Logfile, and Active Connections

→ *Your Raptor Firewall is still properly installed*

1. To start this Practical Exercise, you will need to filter the logfiles. Raptor Eagle logs all data entering and leaving through the firewall. The only data that you will need to see for this Practical Exercise is:

- File Transfer Protocol Daemon/ftpd
- Hypertext Transfer Protocol/httpd
- Telnet Data/telnetd
- Ping Sweeps/pingd

Expand the **Monitoring Controls** and **Logfiles** folders and click on the month and year that you are in and then click on the **Logfile** folder. You will see data already picked up by the firewall (see figure 1)

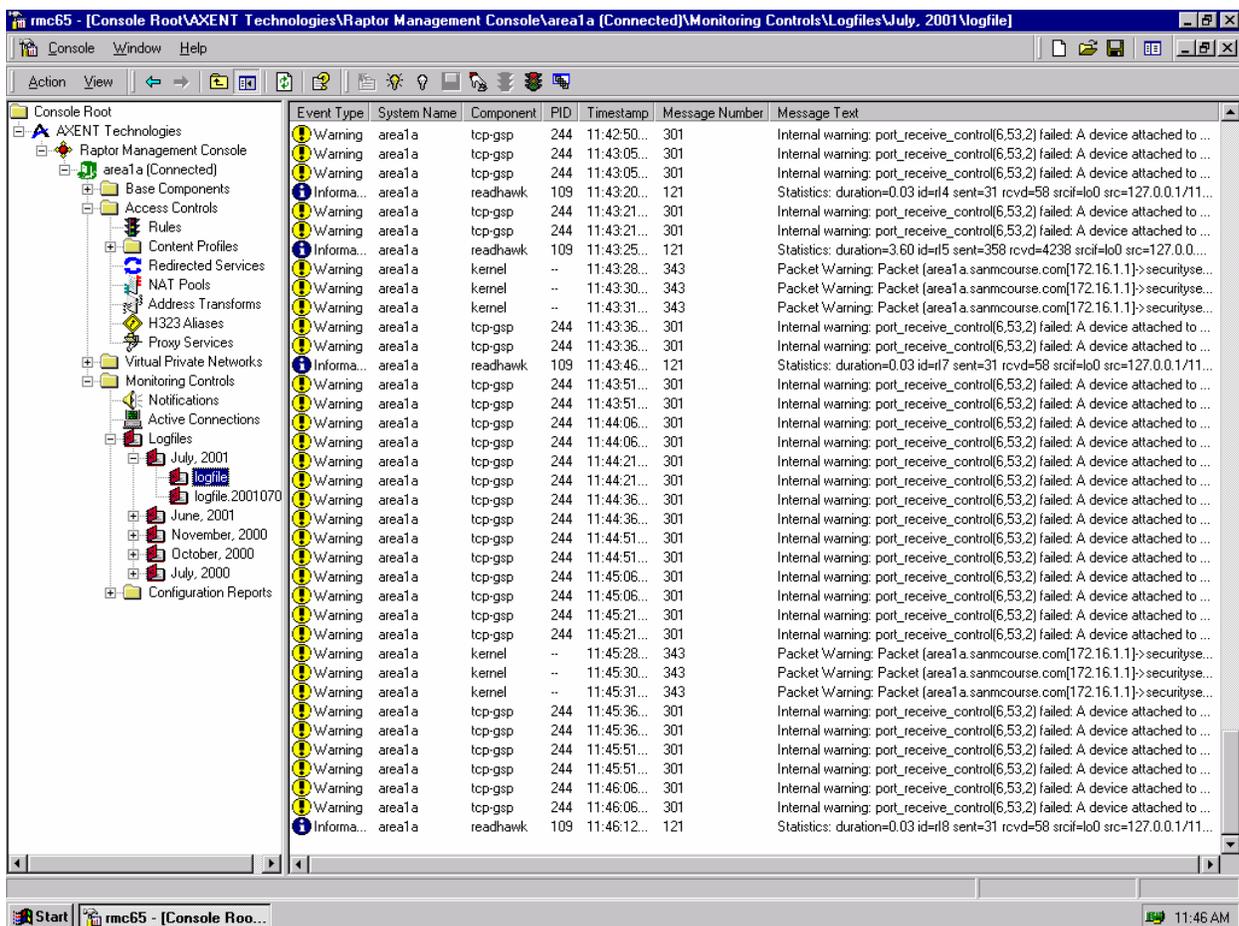


Figure 1 – Logfiles

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Figure 3 – Filter Event Properties Box

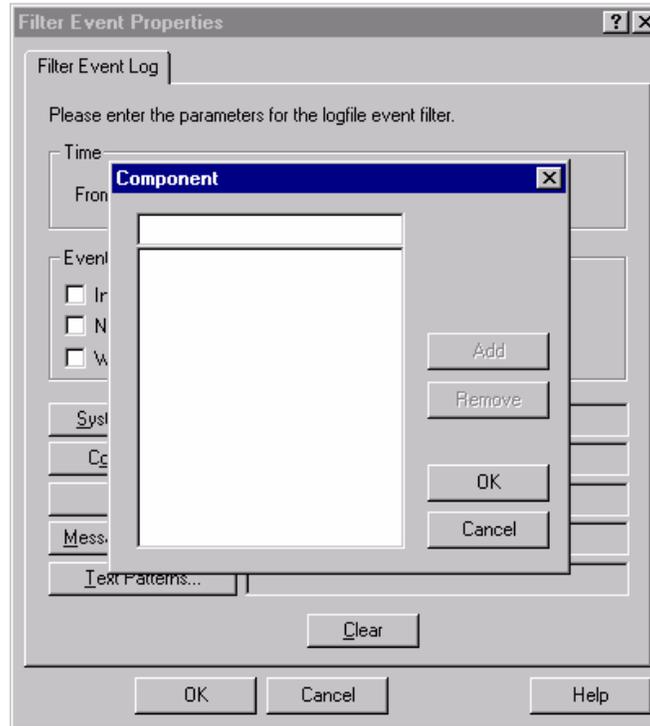


Figure 4 – Components Box

In the box with the blinking cursor, you will type in **ftpd** (This is case-sensitive) and click the add button (see figure 5). Do the same again, but this time add **httpd**, **telnetd**, and **pingd**. When finished, click OK, (then OK again) and only those components will show up throughout the rest of the Firewall Practical Exercise.

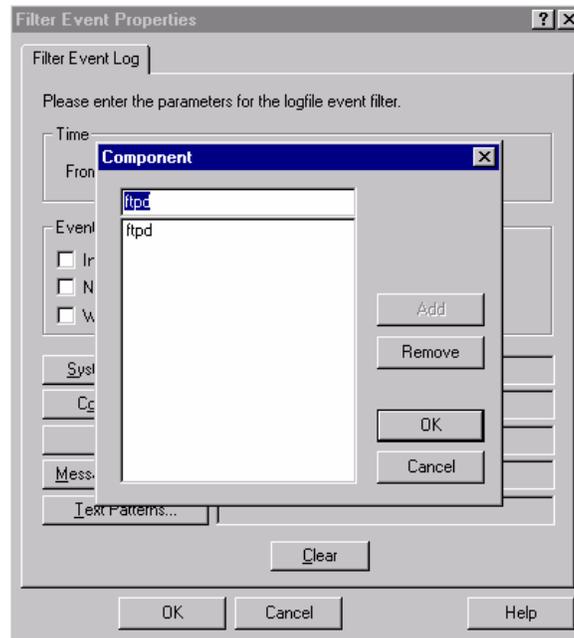


Figure 5 – Add Component

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

1. Double-click the log entries for Telnet and Ping connections that were conducted earlier. Fill in the following fields below:

Src IP/Port: _____ Dest IP/Port: _____

Bytes Transferred: _____ Time: _____ Protocol: _____ Rule: _____

2. Click on Active Connections, Are there any active connections at this time  YES/NO

4. Using the subnet computer **ftp to the instructors computer from the Command Prompt:** (Login as anonymous. Just press enter when asked for a password.)

Watch "Active Connections". Do you see an FTP connection open  YES/NO

Do you get a log entry for this FTP action  YES/NO

5. From the subnet machine, download a file from the FTP server by doing the following commands from the **FTP>** prompt:

get present.rtf [enter]

You should see a new entry in the firewall's logfile. What message does it contain 

-
6. In that same log entry, what does "IP address/20" mean 

-
7. What IP/Port is the original source (src), what IP/Port does the FTP connection use going through the firewall (svrsrc), and what IP/Port does it use to connect to the FTP server (dst) 

Are these the same ports used on every connection 

This is Address Translation in action. Which IP/Port do you think you would find in the FTP server's logfiles for this connection?

Why?

Symantec Raptor Practical Exercise #5 Logfile and Active Connections (cont.)

→ *Your Raptor Firewall is still properly installed*
→ *Continue to answer the following questions*

1. Click on Active Connections and double click on the **FTP** session, press the **KILL CONNECTION** button, observe your active connection window and see if the session has been terminated. Did it work? **YES/NO**

2. List the directory on the subnet machine (dir or ls) then log out using the quit command. What response is on the subnet machine because of the firewall's connection kill 

3. Look at the Logfile. What message can you find because of this termination of the **FTP** session from the firewall 

4. Have the subnet computer **ftp to the instructors computer** again, and log in as anonymous as before. Look at the **ACTIVE CONNECTIONS** window. Did the firewall prevent the user from re-connecting  **YES/NO**
Why or why not 

5. Do you get an entry on the Logfile because of this FTP action? **YES/NO**

6. Which rule does it indicate was responsible for allowing/denying the FTP connection?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Symantec Raptor Practical Exercise #6
HTML Browsing and FTP Stuff

- *Your Raptor Firewall is still properly installed*
- *Start up IE 6.0 on your subnet machine*
- *Answer the following questions*

1. On the subnet computer, start Internet Explorer and type in **http://www.gordon.army.mil**. Look at the firewall's Logfile.

2. Can you find an entry showing where one of the images on the page was downloaded 
YES/NO

3. What option was used to retrieve it 

4. What port on the web server is being used 

5. How did you figure that out 

6. Notice that you can see each and every file, image, or object retrieved as the Subnet PC accessed the page. Even though each of these objects were individual connections, you will rarely ever see them show up in "Active Connections". This is because they complete so quickly. However, your log files will contain a full and complete listing of absolutely everything done through the firewall.

Symantec Raptor Practical Exercise #7
HTML Browsing and FTP Stuff (cont)

- *Your Raptor Firewall is still properly installed*
- *Start up IE 5.01 on your subnet machine*
- *Answer the following questions*

1. Point the subnet PC's browser back to the URL <http://www.gordon.army.mil>
2. Highlight on **RULES** and double click on the current rule (rule #1) and choose the **Services Tab**. Remove the **HTTP** protocol from the internal interface, thereby stopping all **HTTP** traffic—remember to **SAVE** and **RECONFIGURE**.
3. Refresh the subnet PC's browser on the same URL.

What occurs  did you get an error message as expected 

4. Add the HTTP* rule back into your **RULES** set. (**Remember to SAVE and RECONFIGURE**)
5. Modify your existing rule to the internal interface so that the internal user cannot get files using ftp. Double click on **Rule #1** and the **Services Tab**. Highlight FTP and click on the configure button. Remove the checkmark for **Allow FTP Gets**. Close the box and **SAVE AND RECONFIGURE**.
6. Have the subnet computer **ftp to the instructors computer** at the **Command Prompt** and type the following command: **get fw.ppt**

What error message do you get 

What does the Logfile tell you in this situation 

WHEN FINISHED, DELETE ALL THE RULES YOU HAVE CREATED (Save and Reconfigure Firewall). CONTINUE TO NEXT EXERCISE.

Symantec Raptor Practical Exercise #8 RULES RULES RULES!

→ Setup your Raptor NT firewalls to have the following properties:

1. Create a network entity called “subnetPC” that defines your subnet computer sitting behind the firewall. Expand the Base Components folder, highlight Network Entities and right click and choose New > Host.
 - In the **Name Box**, type in **SubnetPC**.
 - Leave the Description Box blank.
 - Select **Host** for type.
 - Click on **Address Tab** and in the address box, type in your subnet PC’s IP address
 2. Create another new host called “Hotmail”
 - In the **Name Box**, type in Hotmail
 - Leave the Description Box blank
 - Select **Host** for type
 - Click on the **Address Tab** and in the address box, type in **www.hotmail.com**
 3. Create another new host called “Microsoft”
 - In the **Name Box**, type in Microsoft.
 - Leave the Description Box blank
 - Select **Host** for type
 - Click on the **Address Tab** and in the address box, type in **www.microsoft.com**
 4. Create a new group this time called “Denied Websites”
 - In the **Name Box**, type in Denied Websites
 - Select **Group** for type
 - Click on the **Members Tab** and include Hotmail and Microsoft as members.
 5. Configure a set of rules that will allow the subnet PC to access all websites EXCEPT Microsoft and Hotmail. (Hint: you will need a minimum of 2 rules for this.)
 6. Have your subnet PC try to access the **Microsoft** and **Hotmail** web sites. Now try <http://www.cert.org>. Did the rules work properly  YES/NO?

 7. After successfully testing the rules above, you are now permitted to allow your subnet computer to access www.hotmail.com. Modify the rules to permit the subnet computer access. The user should get to the Hotmail website, but when they try to log in, it is not successful. You may get a message that says, “**Page Cannot Be Displayed**”. What configuration setting in the firewall rules will fix the problem  you can substitute AKO if you don’t have a Hotmail account.
-
-

NOTE! If IE is caching web pages, exit and restart IE.

When finished, remove all rules and network entities that were created by you and save your changes before continuing to the next practical exercise.

Symantec Raptor Practical Exercise #9
Virtual Private Networking

Creating a VPN Between Two Computers

NOTE! This is just an overview of what a VPN is and what things have to be accomplished! The procedures start on the next page!

Virtual private networking (VPN) works by encapsulating an encrypted and/or authenticated IP packet in a second packet. Encrypting the original packet ensures the privacy of your communication over the public network. At its destination, the outer packet is stripped off and the original packet is decrypted and passed on to its ultimate destination.

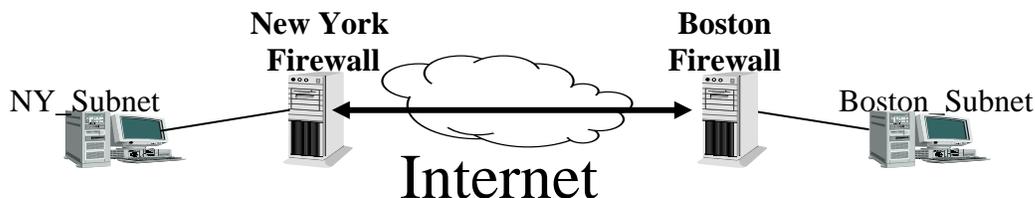
This PE will provide you with an example of a common VPN configuration (computer to computer). You will be required to set up the VPN tunnel on two different firewall computers (**New York** and **Boston**). The PE will provide you with the steps for both firewalls.

- In this PE, the Gateway for the entities (subnets) New York and Boston are the outside interfaces of New York and Boston Firewall computers.

In order to establish the VPN, the administrators of both firewalls will have to perform the following actions:

- Create a secure subnet entity called **NY_Subnet**, which has only a single computer with a gateway entry of New York's gateway address.
- Create a secure subnet entity called **Boston_Subnet**, which has only a single computer with a gateway entry of Boston's gateway address.
- Define a secure tunnel using the same values for both Firewalls.
- Configure rules to allow ping from subnet to subnet entities.
- If you are actually trying to do these steps now, then you haven't been reading the instructions.

Success will be verified when the Subnet computers can ping each other



Symantec Raptor Practical Exercise #9 Virtual Private Networking (cont)
--

Please read this PE very carefully! Any mistakes and your VPN will not work. Both New York and Boston teams will perform the following steps:

Exchange your 3 IP addresses with the other team. (Subnet PC IP, Inside Firewall IP, and Outside Firewall IP.)

Creating a VPN Policy

NOTE: IF ANYTHING IS “GRAYED OUT” THEN LEAVE IT AS-IS

1. Expand the **Virtual Private Networks** folder and right click on **VPN Policies**. Chose **New > VPN Policy**.
2. Enter **NY_end** as the name under the **General Tab**
3. Leave the Description blank
4. Select **swIPe** from the **Encapsulation Protocol** drop down box
5. Choose the **swIPe tab** and choose **rc2** as your **Algorithm** from the drop down box
6. Click on the OK button
7. Create another policy called **Boston_end** under the **General Tab**
8. Leave the Description blank
9. Select **swIPe** from the **Encapsulation Protocol** drop down box
10. Choose the **swIPe tab** and choose **rc2** as your **Algorithm** from the drop down box
11. Click on the OK button.

Creating Network Entities. We will create 4 network entities (2 security gateways and 2 hosts).

12. Expand the **Base Components** folder and highlight **Network Entities**. Right click on **New > Security Gateway**.
13. Enter name **New_York** and the type is **Security Gateway**
14. On the **Security Gateway Tab** enter New York Outside NIC IP Address
15. Place a **checkmark** in the box for **Enable IKE (Internet Key Exchange/ISAKMP)**
16. Under the **IKE Parameters**, Type in Boston Outside NIC IP Address in the **Phase 1 ID Address Box**.
17. Click on the **Shared Secret** radio button, then **Reveal**. Click OK
18. Right click **Network Entities > New > Security Gateway**
19. Enter name **Boston** and the type is **Security Gateway**
20. On the **Security Gateway Tab** enter Boston Outside NIC IP Address
21. Place a **checkmark** in the box for **Enable IKE (Internet Key Exchange/ISAKMP)**
22. Under the **IKE Parameters**, Type in New York Outside NIC IP Address in the **Phase 1 ID Address Box**.
23. Click on the Shared Secret radio button.
24. Click OK
25. Right click on **Network Entities** and choose **New > Host**

Symantec Raptor Practical Exercise #9 Virtual Private Networking (cont)
--

26. Enter name **Boston_Sub** and the type is **Host**
27. On the **Address Tab** enter Boston Subnet PC's IP Address and leave the MAC address blank.
28. Click OK
29. Right click on **Network Entities** and choose **New > Host**
30. Enter name **NY_Sub** and the type is **Host**
31. On the **Address Tab** enter New York Subnet PC's IP Address and leave the MAC address blank.
32. Click OK

Creating Secure Tunnel:

This Tunnel must be identical on both sides. The students that are sitting at the Boston Firewall will be the ones that create and distribute the Key to the New York Firewall!

Boston Firewall will perform the following steps: (New York will skip to next block)

33. Expand the **Virtual Private Networking** folder and click **Secure Tunnel > right mouse click > New > Secure Tunnel**
34. **Enter Name of Tunnel:** BostonSecure-Tunnel
35. **Enter Description:** tunnel from Boston to New York
36. **Enter Local Entity:** Boston_Sub
37. **Enter Local Gateway from drop-down box:** Boston
38. **Enter Remote Entity:** NY_Sub
39. **Enter Remote Gateway from drop-down box:** New_York
40. **Select Boston_end from the VPN Policy box.**
41. **Keys Tab:** Press the **Reveal Key** button, and then press **Generate Key** to reveal the code. Copy the code displayed on a piece of paper.
42. **SPI's Tab:** Generate SPI by pressing the **Generate SPI's** button (click once). Write this on the same paper as the key.

NOTE: Once the Key and the SPI is generated and written down, pass it to the student running the New York Firewall Computer.

Symantec Raptor Practical Exercise #9 Virtual Private Networking (cont)
--

New York will perform the following steps: (Boston will skip to next block)

43. Expand the **Virtual Private Networking** folder and click **Secure Tunnel > right mouse click > New > Secure Tunnel**
44. **Enter Name of Tunnel:** BostonSecure-Tunnel
45. **Enter Description:** tunnel from Boston to New York
46. **Enter Local Entity:** NY_Sub
47. **Enter Local Gateway from drop-down box:** New_York
48. **Enter Remote Entity:** Boston_Sub
49. **Enter Remote Gateway from drop-down box:** Boston
50. **Select Boston_end from the VPN Policy box.**
51. **KeysTab:** The key will be given to you from the student on the **Boston Firewall** Computer. Type it in the proper field.
52. **SPI Tab:** The SPI will be given to you from the student from the **Boston Firewall** Computer. Type it in the proper field. **Click OK.**

Creating Rules:

When you start to create rules, once again you must work as a team to coordinate as you did in Creating a Secure Tunnel.

Boston will perform the following steps: (New York will skip to next block)

53. Expand the Access Controls folder and right click on **Rules > New > Rule**
54. For Connections Coming in Via box, select **BostonSecure-Tunnel**
55. Select **NY_Sub** for From Source.
56. Select **Boston** for Destined For.
57. Select **INSIDE** for Coming Out Via.
58. Services Tab > allow ping
59. Click OK

60. Right click on **Rules > New > Rule**
61. For Connections Coming in Via box, select **INSIDE**
62. Select **Boston** for From Source.
63. Select **NY_Sub** for Destined For.
64. Select **BostonSecure-Tunnel** for Coming Out Via.
65. Services Tab > allow ping
66. Click OK

Symantec Raptor Practical Exercise #9 Virtual Private Networking (cont)
--

New York will perform the following steps: (Boston should prepare to test the VPN)

67. Expand the Access Controls folder and right click on **Rules > New > Rule**
68. For Connections Coming in Via box, select **BostonSecure-Tunnel**
69. Select **Boston_Sub** for From Source.
70. Select **New_York** for Destined For.
71. Select **INSIDE** for Coming Out Via.
72. Services Tab > allow ping, Click OK
73. Right click on **Rules > New > Rule**
74. For Connections Coming in Via box, select **INSIDE**
75. Select **New_York** for From Source.
76. Select **Boston_Sub** for Destined For.
77. Select **BostonSecure-Tunnel** for Coming Out Via.
78. Services Tab > allow ping
79. Click OK

Test the VPN for conductivity:

At the Command Prompt, ping from your **subnet computer** (Boston or New York) to the distant end (New York or Boston) **subnet computer**.

Do this from both Subnet Computers. If you get a positive reply, **SUCCESS!! Notify the Instructor.**

If you cannot ping from one subnet computer to the other, check your keys. Make absolutely sure you both have the same key on both ends on the Keys Tab of the Secure Tunnel. Once you verify that, if it still doesn't work, **VERIFY THE KEY AGAIN!** Once you are positive beyond the shadow of a doubt that the keys are not the issue, look very closely at all of the assigned network entities. Verify that each and every entity you assigned has the right IP address. If these troubleshooting steps don't fix the problem, notify the instructor.

Reading assignment 4

Subject: **Network Intrusion Detection Systems**

Pages: 161-184

(Complete before day 5)

1.  How does an IDS capture information off of the network it is monitoring?

2.  What are 2 methods used by IDS' to generate alerts?
 - 1.
 - 2.

3.  Briefly describe each of them:

4.  Name 4 actions an IDS can take upon detection of an event:
 - 1.
 - 2.
 - 3.
 - 4.

5.  Where are IDS' typically placed in a network?

6.  How do switches affect your IDS placement?

7.  Define a "False Positive":

8.  Define a "False Negative":

9.  Name two methods hackers sometimes employ to avoid detection by an IDS:
 - 1.
 - 2.

RealSecure

Module 13



13-1

RealSecure Overview

- Real-time intrusion detection and response system
- Packet “greper” looks for signatures in the data stream.
- Active response, notification, and storage options
- Monitors the network traffic for “attacks” and “misuse”

13-1

Attack Detection

- 400+ different network danger signs:
 - Denial of service attacks
 - Network probes (port scans, SATAN scans)
 - Brute force attacks, password cracking attempts
 - Windows attacks, including WinNuke, remote registry accesses, and anonymous logins

13-1

Distributed Architecture

- RealSecure uses a distributed architecture and has two major components:
 - the Sensor
 - the Workgroup Manager

Note: Although not recommended due to performance issues, you can install both components on the same computer.

13-1

RealSecure Sensors

- The Sensor is a software component that is installed on a UNIX or Win2K/NT host.
- Sensors are installed on key network segments where you have critical data to protect.

13-1

RealSecure Sensors

- Sensors then examines all of the network traffic on their local segment.
- Sensors monitor network packets and look for signatures that could indicate an attack against your network

13-1

Sensor Specs

- OS
 - Windows 2000 or Windows NT
 - Solaris 2.6 and later
 - Linux
- System
 - 400MHz PII +
 - 256+ MB RAM
- Disk Space
 - 2 GB + (for logfiles and database entries)

Note: The Network card must support promiscuous mode.

13-1

Workgroup Manager

- The Workgroup Manager represents the central management points
- Receive alarms from Sensors
- Control the Sensors and configurations
- Aggregate data and generate reports about network activity.

13-1

Workgroup Manager Specs

- OS
 - Windows 2000 Server or Pro w/SP1
 - Windows NT w/SP4 thru SP/6a
- System
 - 400MHz PII +
 - 256+ MB RAM
- Disk Space
 - 2 GB + (for logfiles, database entries)

13-1



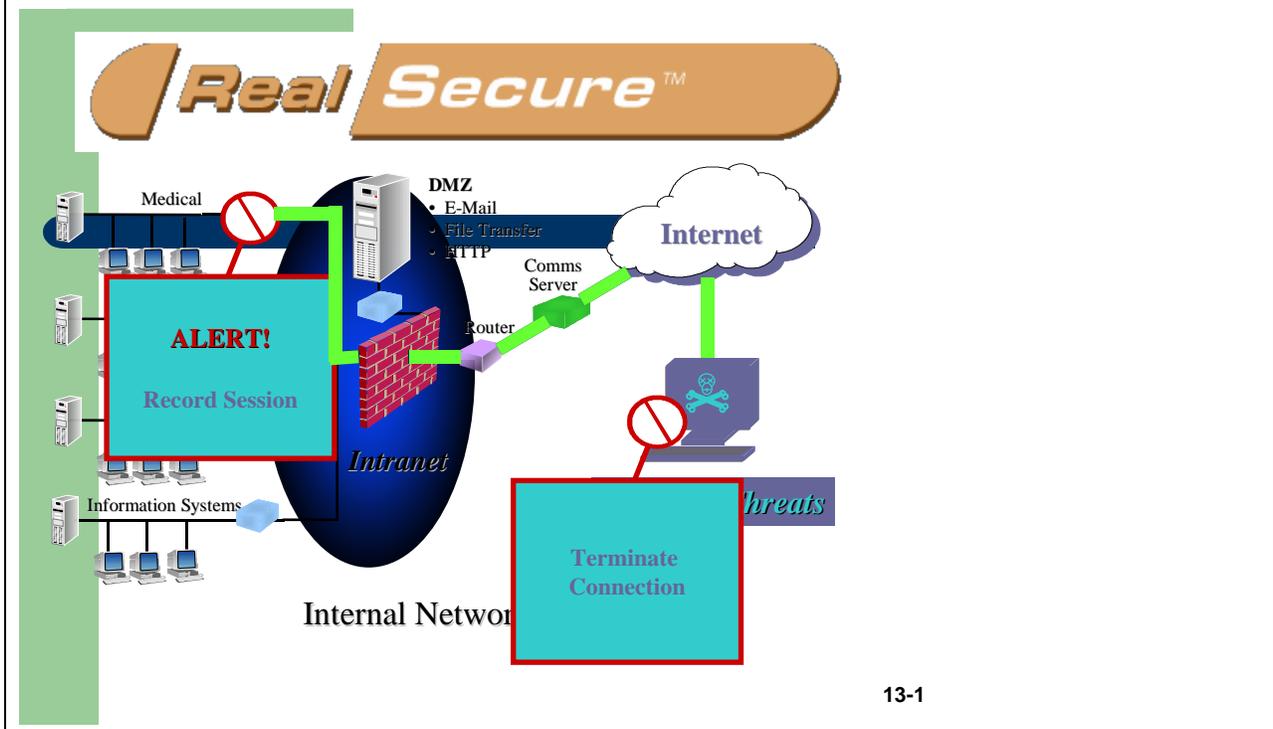
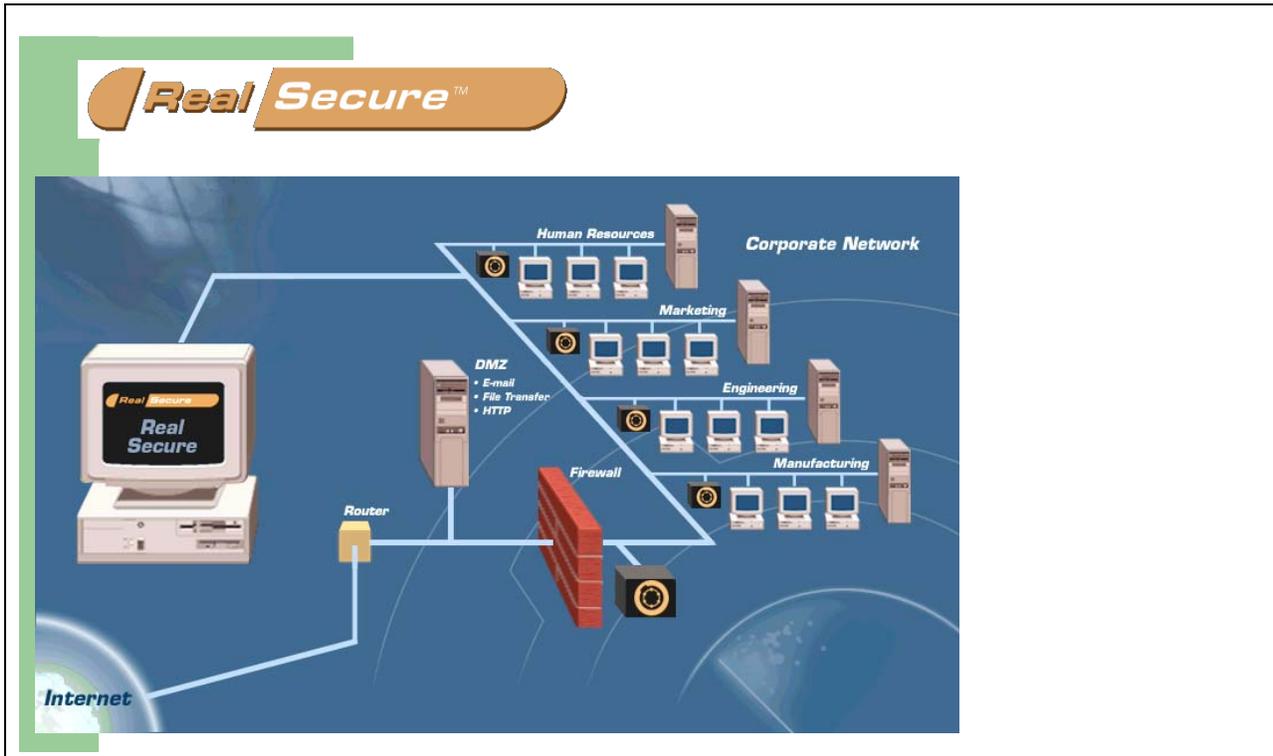
Features

Benefits

Operates 24 hours per day	Continuous network protection
Distributed client-server architecture	Centralized view of enterprise security status
Non-obtrusive solution	Avoids central point of failure
Industry's widest variety of attack signatures	Administrator not required to be a security expert
Customizable by the administrator	Can be configured to meet the needs of the organization
Six-to-eight updates per year	Always has latest attack patterns
Centralized configuration control	Allows configuration of all Detectors from one location

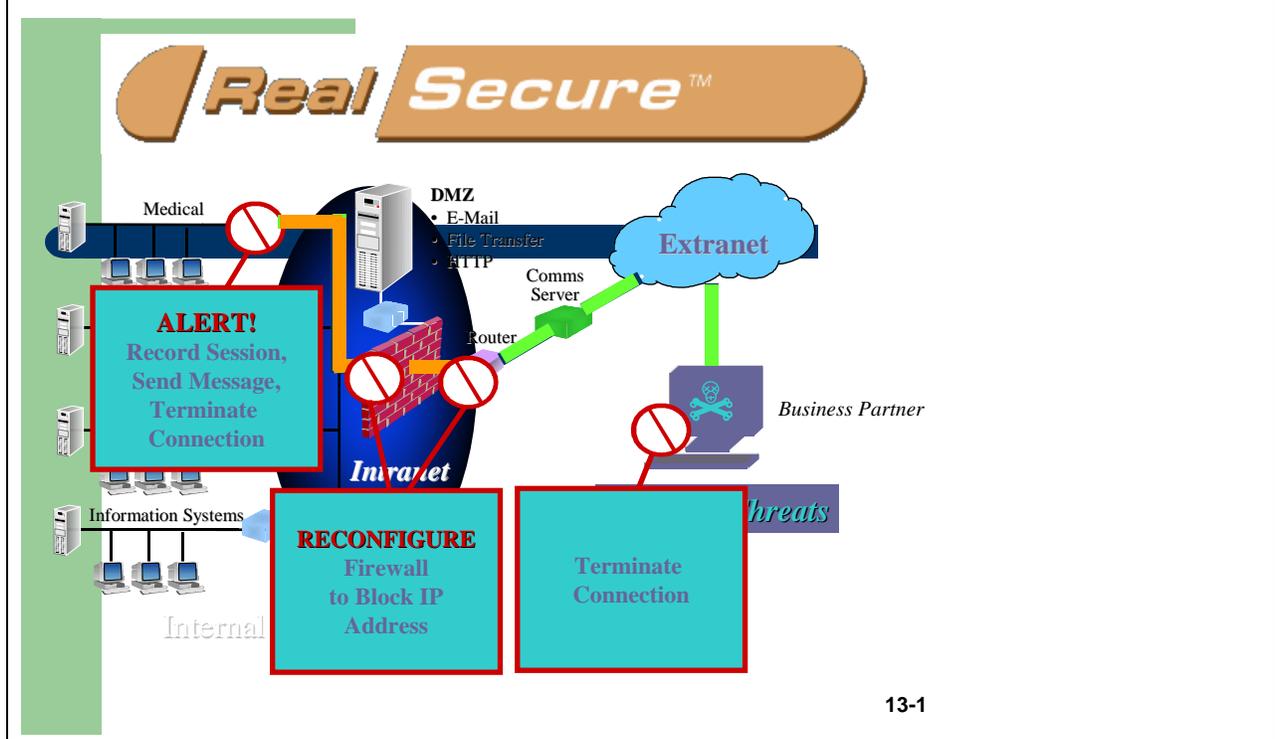
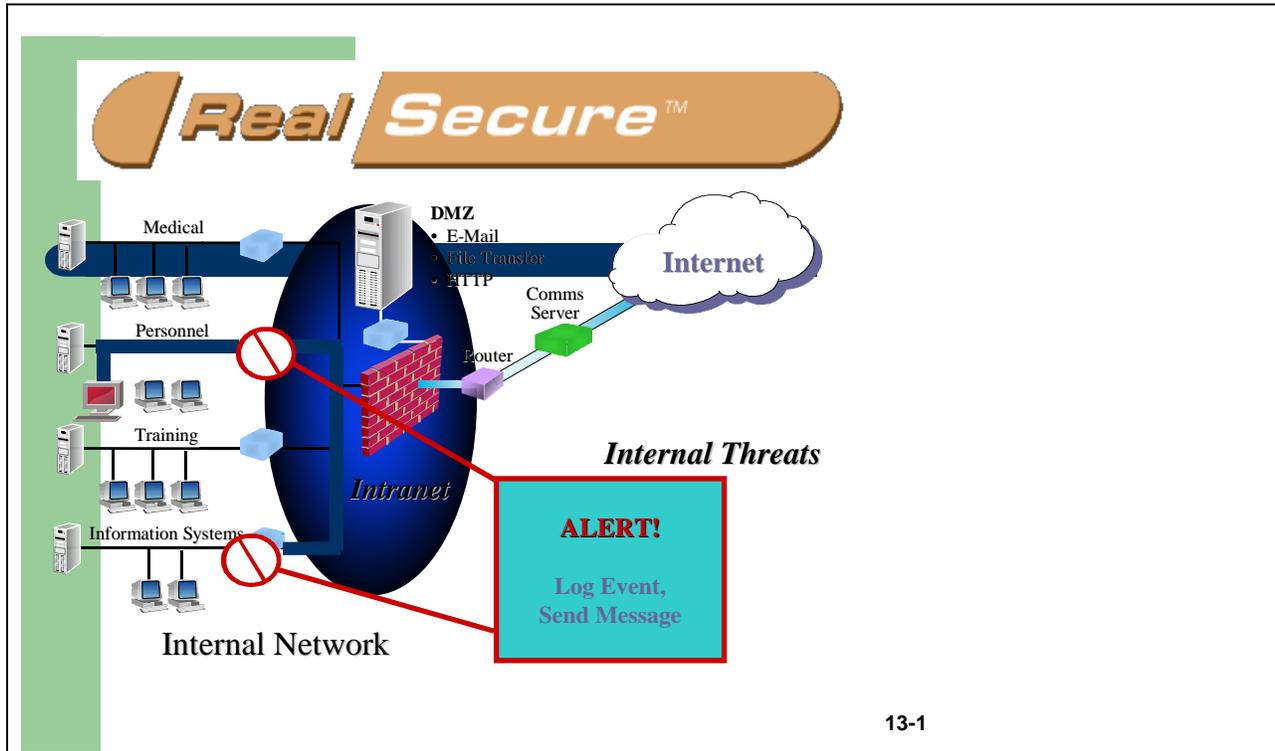
13-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY



13-1

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY



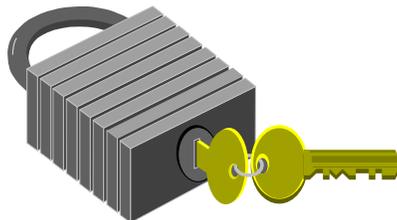
Authentication

- Each end of the communications channel will have its own private and public key pair.
 - Keys are generated at product installation.
 - For the highest level of security, public keys should be distributed among the components of the RealSecure system manually.
 - Ultimately, RS will use X.509 certificates to exchange public keys.

13-1

Encryption

- During installation, the administrator can select either weak (40 bit) or strong (128 bit) for the Sensor and the Workgroup Manager.



13-1

TCP Ports

- TCP 2998 for management control data
- Dynamically assign an additional TCP port for exchange of event and log data (typically TCP 901).
- Override these defaults with your own preferences (ports already open through your firewalls, for example).

13-1

RealSecure Walk-through

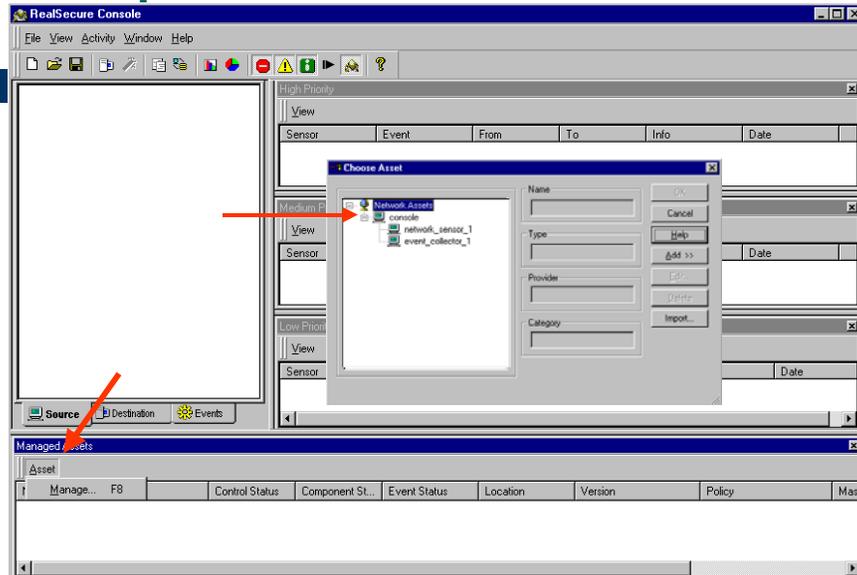
The screenshot displays the RealSecure Console interface. On the left, a tree view shows 'Active Events' categorized by IP addresses and protocols like IPDuplicate, SNMP, Windows, Netbios, and HTTP. The main pane is divided into three sections: 'High Priority', 'Medium Priority', and 'Low Priority', each containing a table of event logs with columns for Sensor, Event, From, To, Info, and Date. At the bottom, a 'Managed Assets' table lists network sensors and event collectors.

Sensor	Event	From	To	Info	Date
147.51.217.170	IPDuplicate	147.51.217.55	147.51.217.176	MAC1 - 00:50:DA:5E:6B:99	2001/10/02 13:02:13
147.51.217.170	IPDuplicate	147.51.217.55	147.51.217.170	MAC1 - 00:50:DA:5E:6B:99	2001/10/02 13:02:13
147.51.217.170	IPDuplicate	147.51.217.55	147.51.217.169	MAC1 - 00:50:DA:5E:6B:99	2001/10/02 13:02:13
147.51.217.170	IPDuplicate	147.51.217.55	147.51.217.171	MAC1 - 00:50:DA:5E:6B:99	2001/10/02 13:02:13

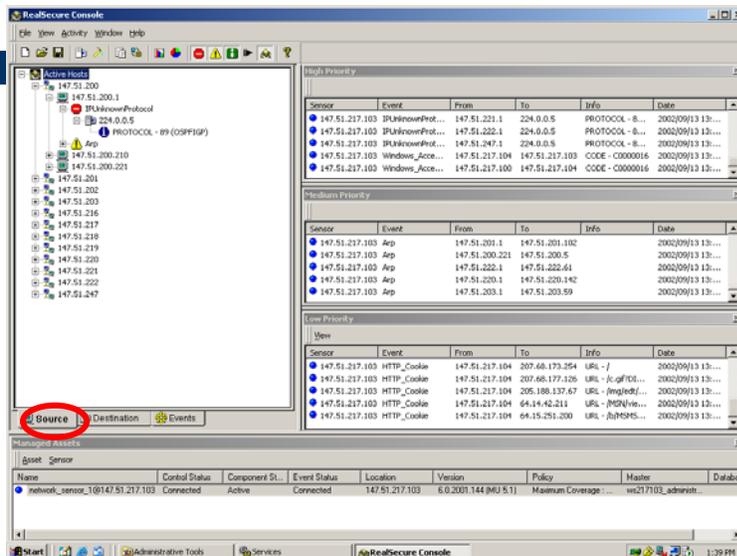
Name	Control Status	Component St...	Event Status	Location	Version	Policy	Master	Databas
network_sensor_1@147.51.217.170	Connected	Active	Connected	147.51.217.170	6.0.2001.144	Maximum Coverage : ...	vs217170_administr...	
147.51.217.170	Connected	Active	Connected	147.51.217.170	6.0.2001.144		Unassigned	
event_collector_1@147.51.217.170	Connected	Active	Connected	147.51.217.170	6.0.2001.144		vs217170_administr...	

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Fire up the Sensor



Activity Tree - Source



Activity Tree - Destination

The screenshot displays the RealSecure Console interface. On the left, the 'Active Destinations' tree is expanded to show a list of IP addresses. The 'Destination' tab is selected and highlighted with a red circle. The main area shows event logs for three priority levels:

Priority	Sensor	Event	From	To	Info	Date
High	147.51.217.103	IPUnknownProt...	147.51.222.1	224.0.0.5	PROTOCOL - 8...	2002/09/13 13:...
High	147.51.217.103	IPUnknownProt...	147.51.247.1	224.0.0.5	PROTOCOL - 8...	2002/09/13 13:...
High	147.51.217.103	Windows_Acce...	147.51.217.104	147.51.217.103	CODE - C0000016	2002/09/13 13:...
High	147.51.217.103	Windows_Acce...	147.51.217.100	147.51.217.104	CODE - C0000016	2002/09/13 13:...
High	147.51.217.103	Windows_Acce...	147.51.217.100	147.51.217.103	CODE - C0000016	2002/09/13 13:...
Medium	147.51.217.103	App	147.51.216.1	147.51.216.70		2002/09/13 13:...
Medium	147.51.217.103	App	147.51.220.1	147.51.220.21		2002/09/13 13:...
Medium	147.51.217.103	App	147.51.219.1	147.51.219.20		2002/09/13 13:...
Medium	147.51.217.103	App	147.51.217.1	147.51.217.60		2002/09/13 13:...
Medium	147.51.217.103	App	147.51.201.1	147.51.201.107		2002/09/13 13:...
Low	147.51.217.103	HTTP_Cookie	147.51.217.104	207.66.173.254	URL - /	2002/09/13 13:...
Low	147.51.217.103	HTTP_Cookie	147.51.217.104	207.66.177.126	URL - /c.gif/00...	2002/09/13 13:...
Low	147.51.217.103	HTTP_Cookie	147.51.217.104	205.188.137.67	URL - /img/edf...	2002/09/13 13:...
Low	147.51.217.103	HTTP_Cookie	147.51.217.104	64.14.42.211	URL - /MSN/ve...	2002/09/13 13:...
Low	147.51.217.103	HTTP_Cookie	147.51.217.104	64.15.251.200	URL - /b/MSMS...	2002/09/13 13:...

Activity Tree - Events

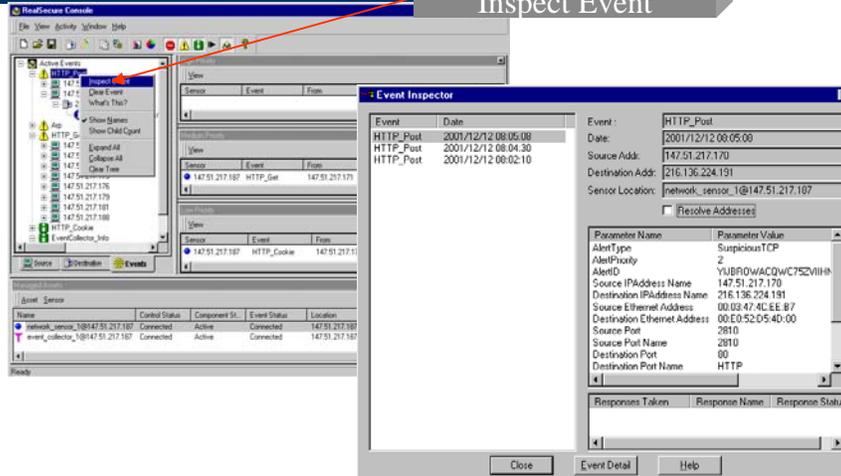
The screenshot displays the RealSecure Console interface. On the left, the 'Active Events' tree is expanded to show a list of event types and URLs. The 'Events' tab is selected and highlighted with a red circle. The main area shows event logs for three priority levels:

Priority	Sensor	Event	From	To	Info	Date
High	147.51.217.103	IPUnknownProt...	147.51.222.1	224.0.0.5	PROTOCOL - 8...	2002/09/13 13:...
High	147.51.217.103	IPUnknownProt...	147.51.247.1	224.0.0.5	PROTOCOL - 8...	2002/09/13 13:...
High	147.51.217.103	Windows_Acce...	147.51.217.100	147.51.217.104	CODE - C0000016	2002/09/13 13:...
High	147.51.217.103	Windows_Acce...	147.51.217.100	147.51.217.103	CODE - C0000016	2002/09/13 13:...
Medium	147.51.217.103	App	147.51.217.1	147.51.217.60		2002/09/13 13:...
Medium	147.51.217.103	App	147.51.201.1	147.51.201.107		2002/09/13 13:...
Medium	147.51.217.103	App	147.51.220.1	147.51.220.24		2002/09/13 13:...
Medium	147.51.217.103	App	147.51.220.1	147.51.220.24		2002/09/13 13:...
Medium	147.51.217.103	App	147.51.201.1	147.51.201.114		2002/09/13 13:...
Medium	147.51.217.103	App	147.51.201.1	147.51.201.109		2002/09/13 13:...
Low	147.51.217.103	HTTP_Cookie	147.51.217.104	207.66.173.254	URL - /	2002/09/13 13:...
Low	147.51.217.103	HTTP_Cookie	147.51.217.104	207.66.177.126	URL - /c.gif/00...	2002/09/13 13:...
Low	147.51.217.103	HTTP_Cookie	147.51.217.104	205.188.137.67	URL - /img/edf...	2002/09/13 13:...
Low	147.51.217.103	HTTP_Cookie	147.51.217.104	64.14.42.211	URL - /MSN/ve...	2002/09/13 13:...
Low	147.51.217.103	HTTP_Cookie	147.51.217.104	64.15.251.200	URL - /b/MSMS...	2002/09/13 13:...

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

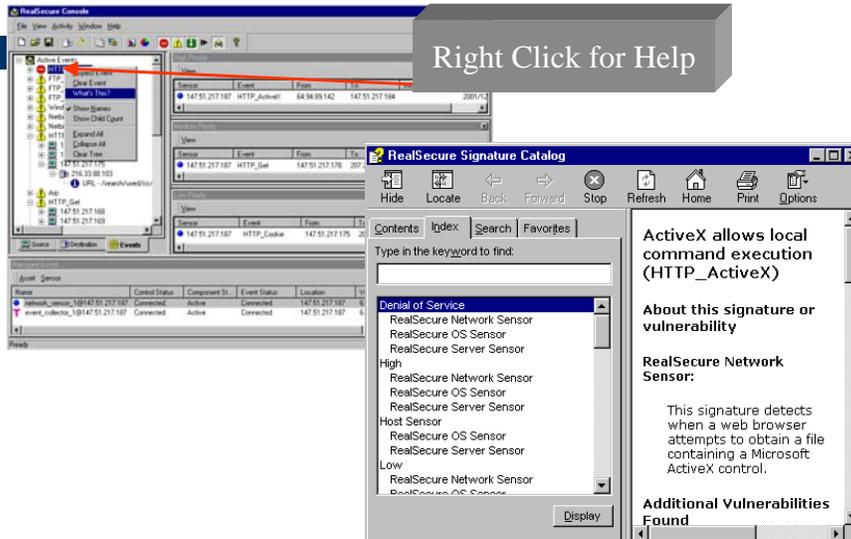
Inspecting Events

Right Click, then
Inspect Event

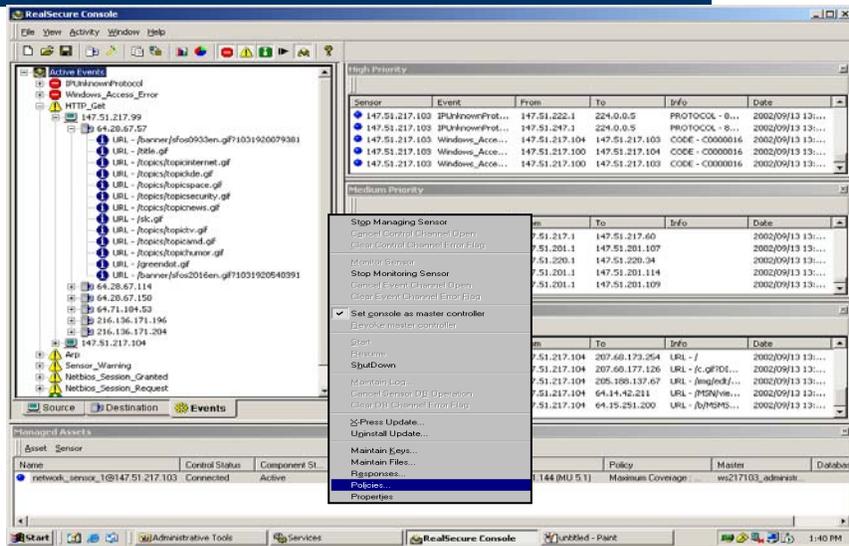


Priorities & Help

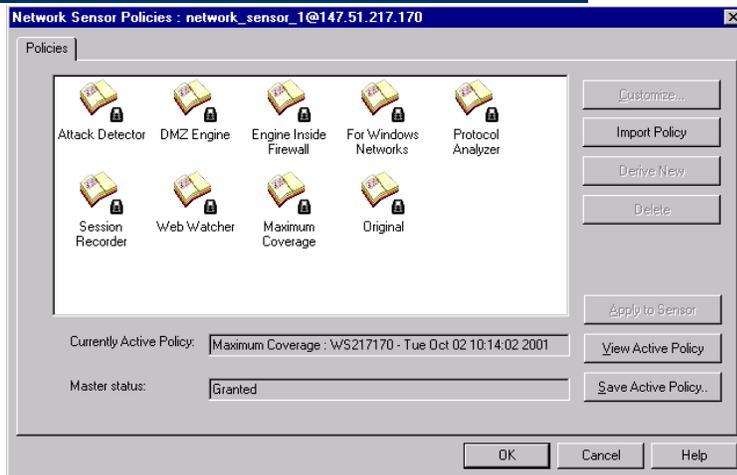
Right Click for Help

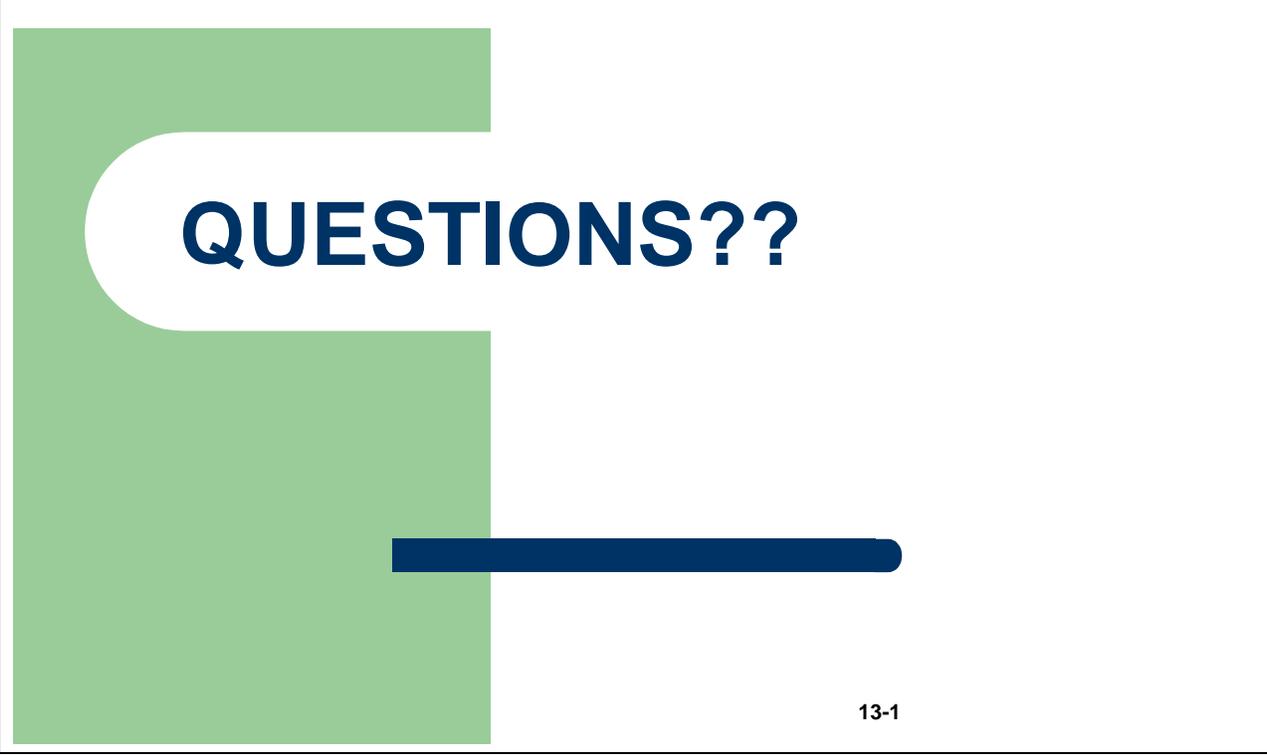


Sensor Engine Policies



Network Sensor Policies





QUESTIONS??

13-1

Intrusion Detection Systems (RealSecure)

Lesson 5

This practical exercise is intended as a supplement to material learned during the IDS and RealSecure lecture. Students will be expected to be familiar with concepts and basic operations related to the RealSecure Intrusion Detection System.

Objectives

1. Setup and operate Realsecure
2. Apply and modify policies
3. Observe real-time attacks

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

RealSecure Practical Exercise #1
Initialization

- *Your ISS RealSecure IDS device has been installed already*
- *Follow the instructions below and answer the questions*

1. Check on the status of the RealSecure application on your W2K server system:
 - **Start > Settings > Control Panel > Administrative Tools > Services**

Is the RealSecure daemon (issdaemon) on? If not, START IT UP!!

What is the STARTUP setting 

Would you want to have the STARTUP as “automatic”  *Why* 

2. Press **CTRL – ALT – DELETE**, then click **Task Manager** to bring up current processes.

What processes are running for RealSecure? (Hint: they start with “iss”)

3. Click on Start, Search, “For Files or Folders”
 - Search for a file named “iss.key” (There may be more than one, but they are identical)
 - Open up the file using Notepad
 - Scroll to the bottom of the “iss.key” file and write down the IP range and the key expiration date—save this for the next PE:

RealSecure Practical Exercise #2
Setup of the IDS Device

- Π *Your ISS RealSecure IDS device has been installed already*
- Π *The console is your configuration tool; the sensor runs in the background. Several sensors can be monitored per console*
- Π *Follow the instructions below and answer the questions*

1. Start the RealSecure application (console):

- √ **Start > Programs > ISS > RealSecure 6.0**

2. RealSecure console screen will appear; then:

- √ Click on **View > Options** (pull-down menu)

This is the location of the key files on your hard drive.

- √ Click on **View > Display Key** (pull-down menu)

What is the Key expiration date? What is the key's IP range?

3. Start your detectors!

- √ Go to the bottom-left window and click on the **Assets > Manage** option on the pull-down menu
- √ Expand the tree, highlight **Network Sensor** and hit **OK** button
- √ **If the daemon is not reached, your key is invalid or your RealSecure daemon is not running Notify Instructor**

What is the current component status 

What is the type of policy coverage 

Do you think this policy type can cause a problem monitoring the network  *Why* 

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

RealSecure Practical Exercise #3
Port Scan and WinNuke

- *Your ISS RealSecure IDS device has been installed already*
- *Follow these instructions below and answer the questions*

1. Wait for the instructor to try a port scan against a target in the classroom:

Did you detect the scan? 

Were you able to determine which ports were scanned? If so, what ports did the instructor scan? 

What was the source of the scan?

2. Highlight the Event Name and **Right Click**, then **Inspect Event**

What Alert Priority was it? Is this appropriate?  

3. Now, wait for the instructor to conduct a Win Nuke attack against the a target in the classroom:

Did you pick up this attack? 

What kind of event was this attack? 

What priority was it? (High, Medium, Low) Is this appropriate?  

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

RealSecure Practical Exercise #4
Web Watcher Template

- *Your ISS RealSecure IDS device has been installed already*
- *Follow these instructions below and answer the questions*

1. Go to the bottom-left window and highlight the **Network Sensor**, then right-click > **Policies**
2. Highlight **Web Watcher** and click on the **Apply to Sensor** button
3. Highlight Web Watcher and click on the view
4. Expand tree and highlight HTTP:

List the following events:

	PRIORITY	RESPONSE	DESCRIPTION
√ HTTP_JAVA			
√ HTTP_PHF			
√ HTTP_PHP_READ			
√ HTTP_SHELL			
√ HTTP_WEBSITE_UP			

5. Now, wait for the instructor to repeat his two attacks—Port Scan and Win Nuke—against the a target in the classroom:

Did you pick up these attacks 

Why did (or didn't) you detect these attacks 

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

RealSecure Practical Exercise #5
Capture Authentication Traffic

- *Your ISS RealSecure IDS device has been installed already*
- *Make sure that the **Max Coverage** policy is active*
- *Follow these instructions below and answer the questions*

1. Set your IDS policy back to “Maximum Coverage”
2. Wait for the instructor to go to his web browser – he’ll try to log a web site that requires a username and password 
3. Now, highlight the HTTP_COOKIE event:
What kind of event (“What’s this?”) is HTTP_COOKIE 

4. Highlight any URL under the HTTP_COOKIE event:
What kind of info do you get here 

What does HTTP_GET signify 

5. Look at HTTP_AUTHENTICATION
Can you read the password sent from the instructor’s browser 

What would it take to safeguard the password via the web 

What does the HTTP_AUTHENTICATION events signify 

What are the source and destination of this event?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

RealSecure Practical Exercise #6 RealSecure Reports
--

- *Your ISS RealSecure IDS device has been installed already*
- *Follow the instructions below and answer the questions*

1. On the RealSecure Console (upper left), click on **View > Reports** on the main pull-down menu.

Note: If asked to SYNCHRONIZE LOGS, click on **File > Synchronize All Logs**. Then try #1 again.

What were the top 5 events?

What were the top 5 destinations?

What were the top 5 source locations?

What were some of the most active source and destination IP's?

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

Appendix A – Public Key Example

-----Here is a copy of my public key:-----

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1.0.7 (GNU/Linux)

```
mQGIBD1SuUURBACHB8cgzc8UuPC23VZ5Zta10/DFf8vIAHU45d8stZ8PR3oWrK5U
30xg02DCeqJSwCGNd7yCOhy5KMJg26r5H/688GYCpA7Q043gZiMyRibDVWaONo/p
/4zKDFDw/4OHZ7tiGwPalpmasc0AmdVIR2cJ3jjwbNIZk8TQ64n/YWiL/wCgwW+w
sVxXerOPKefeidlZkBKqs6sEAI6q8Y8RP22tqrJR5NsfJkOV7JGU/nfQwMP0l+Lm
o4CjBcY4/9UjXYTXmzJUJ3tc4PD+cm+1cH8T04IlobdJV1JZ4JjS/eixJCxvYtAs
U0fq1Mj9Cwee4R1k6gMI0hbunTTSXD7W55loRYZMRLdNELLYENGDQwIQeNgKyf02
wBEjA/0cdTumFOZmSVt+RY8nbkzSMOZpoW4xOkUg83vP/ZuvMlkpdonDD2yOBfh9
RzpellV5TAYr2iAUJcXwCHbvHYei0ZptHCK0aXKLnKE4Af9YYSggJtCXGQrsMOIW
zYUiKWMHUegdVwRA31Igm7ILCgjtG77V8oRpESn63XNGJGWl07Q2Q2hhcmx1cyBK
b25lcyAoQzItUHJvdGVjdCkgPGxpbnV4Y2h1Y2tAcGhvZW5peGJveC5vcmc+iFkE
ExECABkECwcDagMVAgMDFgIBAh4BAheABQI9UrlHAAoJEK8V6KhJF2a26HAAAnR+S
bYtIY19Ayeo1EsFKJDGFHFojAJ0QLHeALOSWlrUj3SX8UXo2O+mbMLQ8Sm9uZXMs
IENoYXJsZXMGtS4gKFNBL05NLVn1Y3VyaXR5KSA8am9uZXNjbUBnb3Jkb24uYXJt
eS5taWw+iF8EExECAB8CGwMECwcDagMVAgMDFgIBAh4BAheAAhkBBQI9Usa2AAoJ
EK8V6KhJF2a2RI8AnAgPwetWLqfBabbZ/byF0lX/QYTCAKCQnx15mN9e4+1biseC
Nqm/dAl+YrkBDQ9UrlGEAQA22hNqWGRBhAdKvopGkr8yQlsD7egdyHYSLXN/A7o
uMGAEYBEpuS0eeTBbn0p13oXsW6MM6v1kjW9LJuz3GUqBUCx0qjvZ2IJdV9a3eyz
cfLsT0pGiH0Fo+8dZCX+G4neGTLsRVie9qBT/3l4hZ6QeMLKpwtvXXtzFMSrfMmH
SYcAAwUD/jj/89QwKbcCkqJePJ2f8aKOKaHw2nZRX+JYckkmm+BTOff10e3uycL9
/tS1xwFRLWEL2wv30GBHfm6tHOQqVY99gHMzPtMWMeoVws3wYQDY54eLtqUyuhKH
RvUAjNjqWWv93Pkm5j92kqXferi9lhMvRPnEfhWHqUdGtUHxdinziEYEGBECAAYF
Aj1SuUYACgkQrxXoqEkXZrapwQCfYvRzfkD9CdRLhin3Bic9oLazGYUANRmXmBP/
6PNlWRI09R5nQgayPqni
=uyZt
```

-----END PGP PUBLIC KEY BLOCK-----

-----example test message-----

This is a test message for classroom usage of the PKI example

Charles Jones

-----signed test message-----

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

This is a test message for classroom usage of the PKI example

Charles Jones

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.7 (GNU/Linux)

```
iD8DBQE9hY9GrxXoqEkXZrYRals1AJ9tTx9o0ROy/Ex2Th/C4zAOgynBtACguOqr
ojHGB5rTYeE3H2xua7ONjiw=
=oVki
```

-----END PGP SIGNATURE-----

PRACTICAL EXERCISES
C2 PROTECT/SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY

-----encrypted test message-----

-----BEGIN PGP MESSAGE-----

Version: GnuPG v1.0.7 (GNU/Linux)

hQEOAzeF/JeNCXxyEAQAtK8KNr46viwTh1E+sklvwrc/KKz0X5h5tpXSCbsvAOBi
BNpeJGdoxQVi jVA7nGzroGPIF9WDsJCdbnu7Cg/K6m9Tq2/FnZTk7t9a21xw/T0h
Z3mM+96urKZIKeH3uLK/hvhIW3CWSfunrM+IUhBT6AewGv7RQjUQtyKmgg2uKmQE
AKbwdklSFEOPdQLILwWV8Y4IgrGgghJk6HTAiHbyvFlKDPtHOSO3fwMzfAKJf3ex
ZznCj6+wcG1oLUDppxxGRbJyc1LqsLzNUozhWbJL2tbFziMgg0HzD7uw1h40hKRR
Mh49ZU4/6Pt3/ENqZiIoek5x0cdeAm+Mc45jxt01001A0sB7AYkURk1e/3Q8X8V6
dBvzWLyFt8ynUkXB+NO7A0dv97fclvrUjF6B2kRNADCfg9yhg2rQreVAuSrGrUg3
+CtWXl3boGK9NrabLz9wKG3mZfmHKHV/GhRyE7FFqBUYKqMCL7ptpKodyFcDAAtX
0HmxtEU6ycJb0tDwHv4p0/dCA8DqAGP43JKgoe/81+rQWK/tvHspk/v1VdF5ZwLO
7szgX0rMr59eyP52FoDzXXd8otjOCqCn4QyCLd7sisI8EUxVculM6/cSqVuj/RQ2
22DF8yWn4yVziTSi6qP/htXJQo2JAY9H86q4Jld7xH4XiWdJW/RuoQgeYtnXhok3
/QZ9YmGFZ3TLppcax4MksGc+qwnPRPMLU82+PZceFht154Rtdvqyuu9Uvzt4vQvv
QUUDENa2uTCx72apaUrD

=xOMA

-----END PGP MESSAGE-----