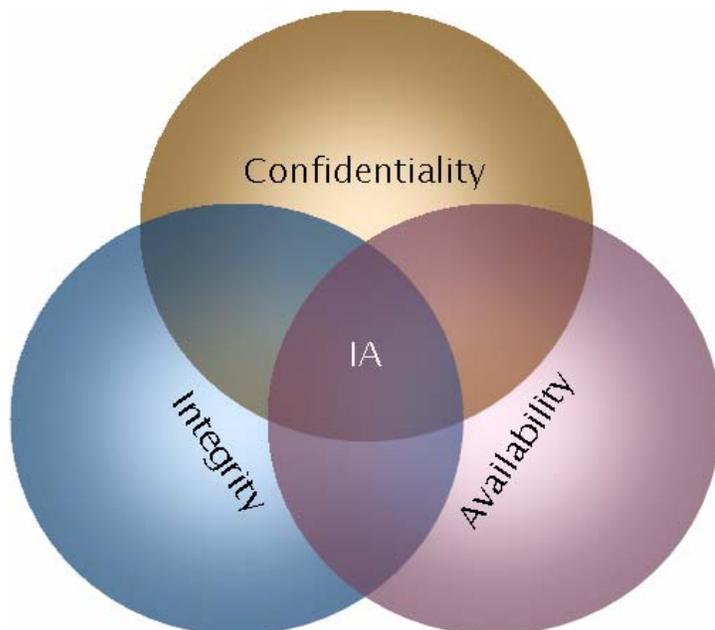


United States Army Signal Center
and Fort Gordon

Leader College for Information Technology
School of Information Technology



Information Assurance Division

Network Manager
Security Course

Contents at a Glance

Introduction & Orientation	7
Network Threats	8
Incidents, Violations, & Vulnerabilities	14
System Availability & Fault Tolerance	15
Cryptography/Encryption	17
Wireless Network Security	27
Securing Cisco Routers	30
Firewalls	36
Symantec Enterprise Firewall (SEF)	38
Real Secure	41
Reading Assignment 1	43
Reading Assignment 2	45
Reading Assignment 3	47
Reading Assignment 4	49
P.E. – PKI	51
P.E. – 3COM Access Point	55
P.E. – 3COM Wireless Adapter Installation	59
P.E. – AirCrack	63
P.E. – Cisco 1: Privilege Levels	67
P.E. – Cisco 2: Password Management	69
P.E. – Cisco 3: Banner Creation Configuration	71
P.E. – Cisco 4: Standard ACL Configuration #1	73
P.E. – Cisco 5: Standard ACL Configuration #2	75
P.E. – Cisco 6: Spoofing Filter	77
P.E. – Cisco 7: Extended Access List Configuration	79
P.E. – Firewall 1: Getting Started with SEF 8.0	81
P.E. – Firewall 3: Allowing & Controlling Outbound Access	85
P.E. – Firewall 3: Allowing & Controlling Outbound Access	85
P.E. – Firewall 4: Monitoring Logs	87
P.E. – Firewall 5: Monitoring Active Connections	89
P.E. – Firewall 6: HTTP & FTP Control	91
P.E. – Firewall 7: Rules	93
P.E. – RealSecure 1: Initialization	95
P.E. – RealSecure 2: Setup of the IDS Device	97
P.E. – RealSecure 3: Port Scans	99
P.E. – RealSecure 4: Web Watcher Template	101
P.E. – RealSecure 5: Capture Authentication Traffic	103
P.E. – RealSecure 6: RealSecure Reports	105
Classroom Network Diagram	107
Classroom Firewall Diagram	108

Table of Contents

Introduction & Orientation.....	7
Course Information	7
Course Objectives	7
Course Ground Rules	7
Course Outline	7
Network Threats	8
Threats	8
RISK = COST x THREAT x VULNERABILITY	8
Threat Methods	8
Attacks	8
Social Engineering – You ARE the weakest link.	9
Information Leakage	10
Virus	10
Worm	11
Rootkit	11
Internal vs. External	11
Pre-Hacking: Footprinting	11
Pre-Hacking: Scanning	12
Pre-Hacking: Enumeration	13
Enumeration on a Windows Platform	13
Username Enumeration	13
Common Port Numbers	13
Incidents, Violations, & Vulnerabilities.....	14
Lesson Objectives	14
Definition of an Incident	14
Definition of a Violation	14
Security Incident Report	14
The Army Reporting Structure	15
Definition of a Vulnerability.....	15
System Availability & Fault Tolerance.....	15
Lesson Objectives	15
Backups	15
Types of Backups	15
RAID	16
Power	16
Recovery Basics	16
Recovery Planning	17
Recovery Essentials	17
Cryptography/Encryption	17
Lesson Objectives	17
Governing & Investigating	17
Cryptographic Firsts.....	17
Definitions.....	17
Ciphers	18

Cipher Methods	18
Algorithms	18
CIA(N)	18
Conventional Encryption	18
Point-to-Point with Conventional Key	19
Advantages of Conventional Key Communications:	19
Disadvantages of Conventional Key Communications:	19
Public Key Encryption	19
Public keys can be used for authentication:	19
Point-to-Point w/Public Key	19
Department of Defense Certificate Authority	20
Hashing	20
Digital Signatures	20
PKI (w/Hybrid Crypto)	21
Crypto Supported Services	22
Encryption Weaknesses	22
Network Attacks	22
Cryptoanalysis	22
Cryptoanalytic Attacks	22
Strategies: Link Encryption	23
Strategies: End-to-End	23
Key Distribution	23
DES	23
AES	24
Kerberos	24
RSA	24
DH Algorithm	25
Certificate Authorities	25
SSL	25
EFS	25
DMS & the CAC	26
Fortezza Smart Cards	26
PGP	26
Email Security	26
Email Security Standards	26
Wireless Network Security	27
IEEE 802.11x Standards	27
Common Wireless LAN Vulnerabilities	27
DoD Policy	28
Army Best Business Practice (BBP)	28
Standard for implementing a wireless LAN	28
FIPS 140-2	29
Wi-Fi Protected Access Version 2 (WPA2)	29
Not approved for Army use	29
DoD References	29
Army References	29

Securing Cisco Routers	30
Lesson Objectives	30
Cisco 2621XM Router	30
Controlling Access	30
Access Modes	31
Configuration Modes	31
Saving the Configuration	31
'?' if You Need Help:	31
Privilege Levels (Default)	32
Privilege Levels (Custom)	32
Configuration Files	32
Physical Port Access Control	32
Virtual Port Access Control	32
Password Protection	33
Banners	33
Session Timeout Setting	34
Access Lists	34
Standard Access Lists	34
Extended IP Access List	35
Removing Access Groups/Lists	35
Firewalls	36
Lesson Objectives	36
Definition	36
Types of Firewalls	36
Proxy	36
Network Address Translation	37
Port Address Translation	37
Firewall Capabilities	38
Potential Weaknesses	38
Symantec Enterprise Firewall (SEF)	38
Industry-tested firewall	38
Virtual private networking	39
Content filtering	39
High availability/load balancing	39
Anti-spam support	39
Antivirus	39
Intrusion detection and prevention	39
Policy - Rules	39
Report type contents	40
Real Secure	41
Lesson Objective:	41
Overview	41
Attack Detection	41
Distributed Architecture	41
Sensors	41
Workgroup Manager	41
Features	41

Typical Implementation	42
Authentication	42
Encryption	42
TCP Ports	42
Reading Assignment 1	43
Reading Assignment 2	45
Reading Assignment 3	47
Reading Assignment 4	49
P.E. – PKI	51
P.E. – 3COM Access Point	55
P.E. – 3COM Wireless Adapter Installation	59
P.E. – AirCrack	63
P.E. – Cisco 1: Privilege Levels	67
P.E. – Cisco 2: Password Management	69
P.E. – Cisco 3: Banner Creation Configuration	71
P.E. – Cisco 4: Standard ACL Configuration #1	73
P.E. – Cisco 5: Standard ACL Configuration #2	75
P.E. – Cisco 6: Spoofing Filter	77
P.E. – Cisco 7: Extended Access List Configuration	79
P.E. – Firewall 1: Getting Started with SEF 8.0	81
P.E. – Firewall 3: Allowing & Controlling Outbound Access	85
P.E. – Firewall 3: Allowing & Controlling Outbound Access	85
P.E. – Firewall 4: Monitoring Logs	87
P.E. – Firewall 5: Monitoring Active Connections	89
P.E. – Firewall 6: HTTP & FTP Control	91
P.E. – Firewall 7: Rules	93
P.E. – RealSecure 1: Initialization	95
P.E. – RealSecure 2: Setup of the IDS Device	97
P.E. – RealSecure 3: Port Scans	99
P.E. – RealSecure 4: Web Watcher Template	101
P.E. – RealSecure 5: Capture Authentication Traffic	103
P.E. – RealSecure 6: RealSecure Reports	105
Classroom Network Diagram	107
Classroom Firewall Diagram	108

Introduction & Orientation

Course Information

- Title: System Administrator / Network Manager Security Course, Course Number 7E-F66/531-F21 (CT)
- Office: Information Assurance Division, Rm 205, Cobb Hall, Bldg 25801
- Email: ia@gordon.army.mil
- Website: <http://ia.gordon.army.mil>

Course Objectives

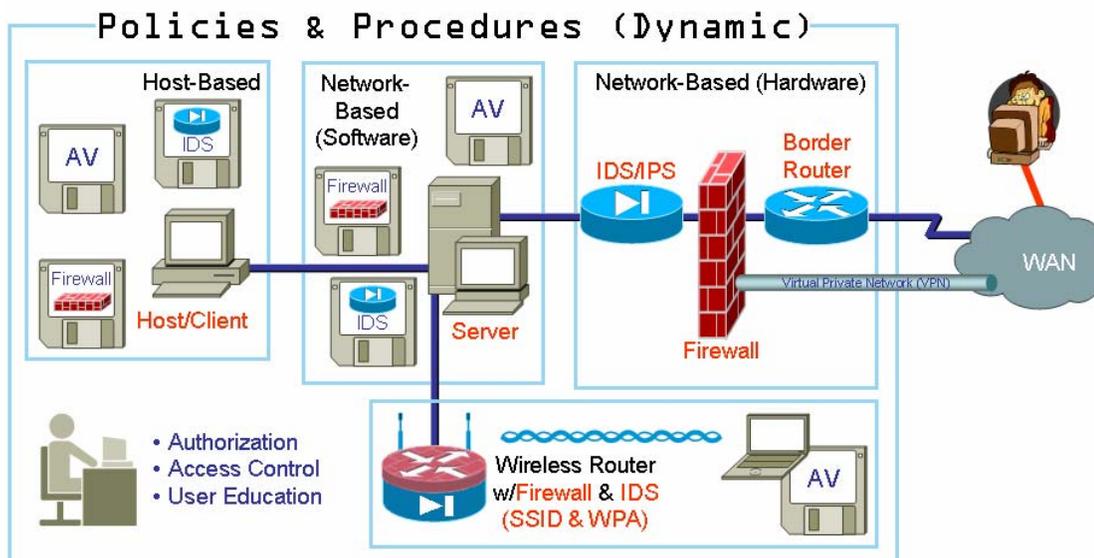
To train DoD personnel to recognize vulnerabilities and defeat potential threats within the network; operate and maintain firewalls using routers and bastion hosts; secure wireless access points; and, install an intrusion detection system

Course Ground Rules

- Course materials are yours to keep
- Ask questions at any time
- Respect the opinions of others
- Products mentioned or demonstrated are not being endorsed
- Smoking area outside in the quadrangle only
- Parking in student lot only (close-up to the building is staff only)
- Cell phones, food, & open containers are not allowed in classroom
- Do NOT hack your fellow students

Course Outline

- Network Vulnerabilities
- Reporting
- Hackers
- Fault Tolerance
- Encryption / Cryptography
- Router Security
- Wireless Security
- Firewall Security
- Intrusion Detection Systems



Network Threats

Threats

- A circumstance or event that could exploit or cause harm by violating security.
- Threat Assessment: Consideration of the likelihood and possible impact of the threat
- Threat Objectives:
 - Information Leakage
 - Integrity Violations
 - Denials of Service
 - Viruses, Worms, & Rootkits
 - Illegitimate Uses

RISK = COST x THREAT x VULNERABILITY

- The cost (or value) of the data (or loss of the data) on our networks is determined by the owner of the data. The SA can do nothing about it.
- Threats are always present. The SA can't control external threats. Internal threats can be mitigated to some extent, but not eliminated.
- Vulnerabilities are manageable and repairable: they can be reduced to near-zero.

Threat Methods

- Hackers
- Masquerading, forging, spoofing
- Playback, replay
- Bypassing security controls
- Authorization violations, misuse of authority
- Network attacks
- Traffic analysis, network scanning
- War dialing, war driving, sidewalk surfing
- Malicious Code
- Backdoors & Trojan horses
- Media scavenging, dumpster diving
- Social engineering
- Phishing, pharming, & spear-phishing

Attacks

- Buffer Overflow
 - The most common DoS attack involves sending more traffic to a network address than the programmers who planned its data buffers anticipated someone might send.
 - Sending e-mail messages that have attachments with 256-character file names to Netscape and Microsoft mail programs
 - Sending oversized ICMP packets (also known as the "ping of death")
 - Sending to a user of the Pine e-mail program a message with a "From" address > 256 characters
- SYN Attack
 - When a session is initiated between a TCP client and server, a small buffer space is set up to handle the "hand-shaking" exchange of messages that sets up the session. These packets include a SYN field that identifies the sequence in the message exchange.
 - An attacker can send a number of connection requests very rapidly and then not respond to the replies. This leaves the first packet in the buffer so that other, legitimate connection requests can't be handled. The packet in the buffer is

eventually dropped, but the effect of many of these bogus connection requests is to make it difficult for legitimate requests to be processed.

- Teardrop Attack
 - A packet received at a router that is too large to be forwarded to a network has to be fragmented into smaller packets. This is an automatic function of IP. Each fragmented packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled.
 - In the teardrop attack, the attacker puts a confusing offset value in fragments after the first one. If the receiving operating system does not have a plan for this situation, it can cause the system to crash.
- Smurf Attack
 - The attacker sends an IP ping request to a receiving site (typically a router).
 - The ping packet specifies that it be broadcast to a number of hosts in the receiving site's local network.
 - The packet also indicates that the request is from a site other than the one that originated it.
 - The result will be lots of ping replies flooding back to the target.
 - If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.
- Land Attack
 - The attacker puts the target's IP address in both the source and destination fields of every packet.
 - There is not legitimate reason to do this.
 - The packets are then sent to the target system, which is usually not configured to deal with packets from itself.
 - The result is that the system crashes.

Social Engineering – You ARE the weakest link.

- "People are the weakest link. You can have the best technology, firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything." Kevin Mitnick, *The Industry Standard*, 09/28/00
- Social Engineering Definitions:
 - an outside hacker's use of psychological tricks on legitimate users of a computer system in order to obtain information needed to gain access to the system.
 - getting needed information (for example, a password) from a person rather than breaking into a system.
 - a cracker's clever manipulation of the natural human tendency to trust.
 - The Jargon File: "a term used among crackers & samurai for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security."
 - lying to get what you want
- 3 Phases of Social Engineering:
 - Phase 1 – Reconnaissance. Learn as much about the target as you possibly can before initiating contact.
 - Phase 2 – Who's Who? Verify what you've learned
 - Phase 3 – Trust Me. Use what you learned to lie your way into what you want.

- Reconnaissance:
 - The telephone is the weapon of choice:
 - When it rings, someone answers it.
 - The person who answers it only knows what you tell them about yourself.
 - If things go wrong, hang up.
 - Dumpster-diving for fun and profit:
 - Telephone & Equipment Manuals
 - Internal Phone Directories
 - E-Mails
 - Discarded Floppies
- Who's Who:
 - Having gleaned information that only an employee should know, it is now time to verify what you have learned.
 - "The Gatekeeper" is your friend.
 - Through seemingly harmless conversations, try to learn nicknames, supplier names, REAL business hours, types of equipment in use, etc. Almost anything will help.
- Trust Me:
 - Put it all in play.
 - Use those seemingly insignificant bits of information to convince the gatekeeper that you are standing before his/her desk with nothing but the best of intentions in mind.
- Social Engineering Examples: Using information found in the dumpster, a hacker attempts the following:
 - Scenario 1: The secretary to the CFO gets a call from Todd in Tech Support. "Uh-oh", he says, "You're not in London! Someone is dialing in from London on your account. Don't worry about it, though. I'll change your password. Wait a second, he's on there now. I'll need your current password so I can knock him off line and then change it."
 - Scenario 2: "Ted" shows up with a toolbox and a printer toner cartridge. He says he's from Printers-R-Us and passes across a business card to that effect. He says "My boss said Big Earl left a voice mail about fixing his printer. I didn't think I could get to it today, but my last job was just down the street. Would it be OK to take a quick look at it?"

Information Leakage

- Comments left in source code (primarily HTML)
- Verbose error messages
- Confidential data in plain sight
- System response prompts (password scenario)
- Steganography
- Covert channel communications

Virus

- A cracker program that searches out other programs and 'infects' them by embedding a copy of itself in them, so that they become Trojan horses. When these programs are executed, the embedded virus is executed too, thus propagating the 'infection'. This normally happens invisibly to the user.
- Unlike a worm, a virus cannot infect other computers without assistance. It is propagated by vectors such as humans trading programs with their friends.
- The virus may do nothing but propagate itself and then allow the program to run normally. Usually, however, after propagating silently for a while, it starts doing things

like writing cute messages on the terminal or playing strange tricks with the display (some viruses include nice display hacks).

Worm

- A program that propagates itself over a network, reproducing itself as it goes.

Rootkit

- A rootkit is a set of software tools frequently used by a third party (usually an intruder) after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system without the user's knowledge. Rootkits are known to exist for a variety of operating systems such as Linux, Solaris and versions of Microsoft Windows.
- A rootkit typically hides logins, processes, files, and logs and may include software to intercept data from terminals, network connections, and the keyboard. In many instances, rootkits are counted as trojan horses.

Internal vs. External

- Internal (Insider) Threats
 - System administrator, network manager, operator, programmer, user
 - Reasons for the potential threat:
 - Fired or disgruntled
 - Coerced, greedy, financially strapped
 - Lazy, untrained
 - For the thrill or challenge
- External (Outsider) Threats
 - Foreign intelligence agent, terrorist, criminal
 - Hacker

Pre-Hacking: Footprinting

- The act of creating a profile of the target
- Includes technologies used by the target:
 - Internet
 - Domain Name(s)
 - Static IP Addresses
 - TCP & UDP Services Running
 - System Architecture (SPARC/x86)
 - Firewall and Router ACLs
 - Intrusion Detection Systems (IDS)
 - User Names
 - Group Names
 - Intranet
 - Networking Protocols
 - Internal Domain Names
 - Internal Static IP Addresses
 - TCP & UDP Services running
 - System Architecture (SPARC/x86)
 - Firewall and Router ACLs
 - Intrusion Detection Systems (IDS)
 - User Names
 - Group Names
 - Remote Access
 - Analog/Digital Telephone Numbers
 - Type of Remote System

- Authentication Mechanisms
- Extranet
 - Connection Origination & Destination
 - Type of Connection
 - Access Control Mechanism
- The goal of footprinting is to put together a picture of the target:
 - Employee names & phone numbers
 - IP addresses
 - DNS servers
 - Mail servers
 - An outline of the software and hardware in use by the company.

Pre-Hacking: Scanning

- After creating a picture of the target network, the hacker next looks at each system individually to discover what is running on each one. This is called scanning.
- This is accomplished by using a variety of tools:
 - Ping Sweeps (ICMP Queries): A basic network scanning technique used to determine which of a range of IP addresses map to live hosts. If a given address is live, the host responds with an ICMP ECHO reply.
 - Port Scans
 - A series of messages sent to a computer in an attempt to learn what the computer's capabilities are and what services/programs are running.
 - Identify both the TCP and UDP services.
 - Identify the type of operating system.
 - Identify specific applications or versions of a particular service
 - Types of Scans
 - TCP connect scan – completes a full, three-way handshake (SYN, SYN/ACK, & ACK)
 - TCP SYN scan – also called a 'half-open' scan because a full TCP connection is not made (SYN, SYN/ACK, RST)
 - TCP FIN scan – sends a FIN packet which causes the target to respond with a RST for all ports that are closed. Usually works only on Unix systems.
 - TCP Xmas Tree scan – sends FIN, URG, and PUSH packets to the target. Usually, an NT system will respond with an RST for all closed ports.
 - TCP Null scan – causes the target system to turn off all flags and responds with an RST for all closed ports
 - UDP scan – usually unreliable; sends a UDP packet and waits for an 'unreachable' message indicating the port is closed.
 - Sweep – scans the same port on multiple hosts
 - Vanilla – attempts to scan all 65,536 ports
 - Strobe – scans a subset of all the ports
 - FTP Bounce – scan through an FTP server in an attempt to hide the scanner's identity
 - Port Scan Results
 - port number (21, 23, 80, etc.)
 - state (open/closed)
 - protocol (TCP/UDP)
 - service (FTP, SMTP, HTTP, finger, etc.)
 - Countermeasures include using an Intrusion Detection System (IDS), & shutting down all unnecessary services

- Automated Discovery Tools
 - There are literally hundreds of automated discovery tools available to the hacker. These tools, coupled with the many differences in IP stack implementations across the various vendor operating systems makes it virtually impossible to prevent the discovery of information in an intranet.
 - For protection against discovery on an internet connected network the deployment of a good firewall or proxy application is the best solution.

Pre-Hacking: Enumeration

- Involves active connections to systems
- Is very risky from a hacker's standpoint
- Is the point at which the hacker is either breaking the law, or is on the brink of doing so.
- Information gained can be grouped as follows:
 - network resources and shares
 - users and groups
 - applications and banners

Enumeration on a Windows Platform

- Standard NET command options such as 'view'
- Standard Windows XP/2003 command WHOAMI
- A multitude of external hacking tools which probe the operating system (eDump, GetMAC, NetDOM, NetViewX, etc.)
- Countermeasures include:
 - Installing service packs, security rollups, hotfixes
 - Auditing the system regularly
 - Applying the Windows STIG
 - Using a Host-based intrusion detection system (Tripwire, Tiger, SARA, etc.)
 - Filtering TCP & UDP ports 135-139 on perimeter

Username Enumeration

- Almost half the puzzle
- NBTSTAT
- sid2user & user2sid (Once SID is gained, can determine which is administrator account)
- These will work even if RestrictAnonymous is enabled
- An effective countermeasure is blocking port 139 from all perimeter access

Common Port Numbers

- 20 TCP File Transfer Protocol (FTP) Data
- 21 TCP File Transfer Protocol (FTP) Control
- 22 TCP Secure Shell (SSH)
- 23 TCP Telnet
- 25 TCP Simple Mail Transfer Protocol (SMTP)
- 53 TCP Domain Name Service (DNS)
- 69 UDP Trivial File Transfer Protocol (TFTP)
- 80 TCP HyperText Transfer Protocol (HTTP)
- 110 TCP Post Office Protocol (POP)
- 161 UDP Simple Network Management Protocol (SNMP)
- 443 TCP HTTP over Secure Socket Layer (SSL/TLS)

Incidents, Violations, & Vulnerabilities

Lesson Objectives

- Detect and report incidents and violations
- Identify information system vulnerabilities

Definition of an Incident

- An 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:
 - suspected intrusion
 - unauthorized access attempt
 - unexplained file modification
 - unexplained output
 - security system failure
 - abnormal system response
 - malicious software
 - network intrusion alert
 - anything “alarming”

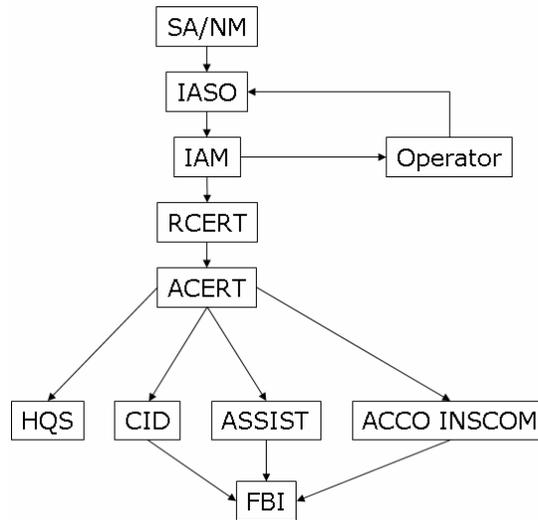
Definition of a Violation

- A failure to comply with the policies and procedures established which could reasonably be expected to result in the loss or compromise of classified info:
 - removal of classified information
 - wrongful disclosure of classified information
 - introduction of high-risk software
 - introduction of malicious code
 - sharing passwords

Security Incident Report

- Report incident to IASO
 - Information system name and/or number
 - Location
 - Date & Time
 - Description
 - Impact
 - Any pertinent information
- IASO investigates and advises IAM
- IAM advises the community
- ACERT advises IAM and IASO
 - further guidance
 - further reporting requirements
 - Vulnerability assistance

The Army Reporting Structure



Definition of a Vulnerability

- A hardware, firmware, communication, or software weakness which leaves a computer processing system open for potential exploitation or damage
- To determine what current vulnerabilities have been identified and what the countermeasures are for them, visit www.sans.org

System Availability & Fault Tolerance

Lesson Objectives

- Discuss technologies for high system availability
- Discuss techniques for disaster prevention and system recovery
- Discuss contingency planning basics

Backups

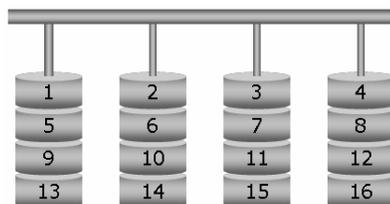
- Why Backup?
- What are some good software choices?
- What is your backup policy?
 - Media protection / retention schedule
 - Encryption, compression, error checking & correction
 - Automate your backups
 - Train your users
 - Maintain off site storage
 - Document your policies & procedures
 - Distribute policies & procedures to key personnel
- Backup - it's your last line of data protection.

Types of Backups

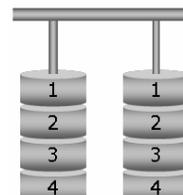
- FULL: the starting point for all other backups; contains all the data in the folders and files that are selected to be backed up
- INCREMENTAL: only the files that have changed are included
- DIFFERENTIAL: contains all files that changed since the last FULL backup

RAID

- RAID is short for Redundant Array of Independent (Inexpensive) Disks, a category of disk storage that employs two or more drives in combination for fault tolerance and performance.
- There are a number of RAID levels. The three most common are 0, 1, and 5.
- RAID 0
 - The data is broken down into blocks with each block written to a separate disk drive
 - I/O performance is greatly improved by spreading the I/O load across many channels and drives
 - No parity

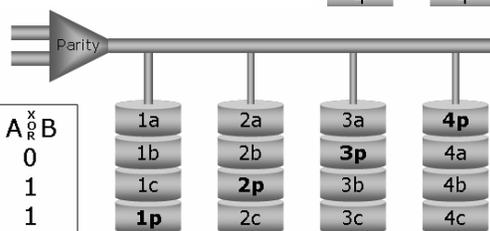


- RAID 1: Disk Mirroring - mirrors data across multiple disks. Data is duplicated on another set of drives. If one drive fails, then the data is still available on the other mirror.

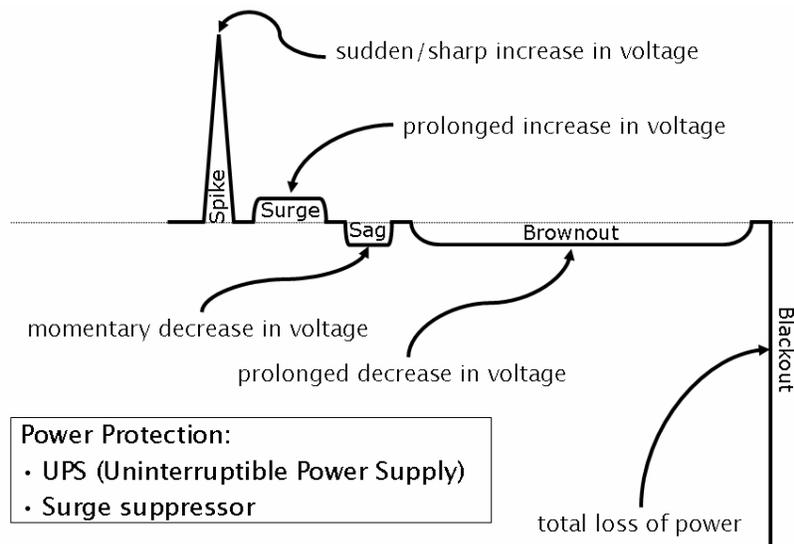


- RAID 5: Stripes data and parity information across all the drives in the array. Parity is written to the next available drive, not to a dedicated parity drive.

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0



Power



Recovery Basics

- Fault Tolerance: A network that is fully redundant and has maximum up-time is considered fault tolerant. In other words, should a component of the network fail, the network will continue processing requests and the failure will be transparent to clients.
- Develop & Test Contingency Of Operation Plan (COOP)
- Maintain system configuration information

Recovery Planning

- Planning is your road map to recovery:
- Minimize recovery period (down time)
- Minimize errors in decision making
- Minimize errors in implementation
- Identify critical assets and procedures
- Establish responsibilities
- Establish priorities
- Identify resources
- Obtain commitment from management

Recovery Essentials

- Develop a plan
- Train the plan
- Test the plan
- Update the plan

Cryptography/Encryption

Lesson Objectives

- Define government regulatory & investigation roles
- Discuss cryptography's historical background
- Define the basic concepts of cryptography
- Explain conventional encryption (symmetric)
- Explain public key encryption (asymmetric)
- Explain hashing & digital signatures
- Examine the Public Key Infrastructure (PKI)
- Illustrate some encryption weaknesses
- Examine various types of network attacks
- Illustrate network encryption strategies
- Discuss key distribution
- Discuss encryption standards & tools
- Discuss email encryption/security standards

Governing & Investigating

- The U.S. Department of Commerce is the governing approval authority for all encryption methods, tools, and applications that can be used, sold, and downloaded in the U.S.
- The National Security Agency (NSA) is responsible for investigating, monitoring, and decrypting traffic that could be terroristic in nature.

Cryptographic Firsts

- 1st recorded use was in 4000BC (hieroglyphs)
- 1st military use of cryptography was in 400BC
- 1st electromechanical ciphering machine was invented in 1920
- 1st commercial encryption algorithm was DES ('76)
- 1st commercial public key encryption was RSA ('78)

Definitions

- Cryptography: The science of secret writing
- Encrypt: Transform plaintext into ciphertext
- Decrypt: Transform ciphertext into plaintext
- Cryptanalysis: Decrypting ciphertext without the key by breaking the encryption.

- Algorithm: A math formula, recipe, or procedure used to encrypt and decrypt data
- Cipher: An algorithm used in the encryption and decryption transformations

Ciphers

- A substitution cipher replaces characters with other characters or symbols
"the enemy is nigh" = "wkh hqhp lv qljk"
- A transposition cipher rearranges characters, bits, or bytes
"the enemy is nigh" = "ene myisn ig hthe"
- The hybrid substitution & transposition cipher (modern) both replaces and rearranges characters, bits, or bytes
"the enemy is nigh" = "hqhpbivq lj kwkh"

Cipher Methods

- Stream Cipher:
 - Data is sequentially encrypted using a single bit from the encryption key
 - Requires no memory
 - Data is encrypted on-the-fly
 - Usually implemented in hardware
- Block Cipher
 - Transforms fixed-length blocks of plaintext into ciphertext of the same length
 - Requires memory
 - Data is encrypted block-by-block
 - Usually implemented in software
- Key: Parameter that controls a cryptographic algorithm (usually a sequence of bits)
 - Shorter key (40bit), faster encryption, less secure
 - Longer key (128bit), slower encryption, more secure
- Cryptoperiod: The time period for which the use of a key is authorized
 - The more ciphertext produced by a key and available to a cryptanalyst, the easier it is to break the key.
 - If the key is compromised, the amount of information compromised will be limited.

Algorithms

- Three primary algorithm types:
 - Symmetric – conventional or secret key encryption
 - Asymmetric – 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

CIA(N)

- Confidentiality: prevents unauthorized disclosure
- Integrity: prevents unauthorized modification
- Authentication: assures the identity of the originator
- Non-repudiation: prevents denial of participation in a communication session

Conventional Encryption

- Also known as Secret Key, Symmetric Key, and One-Key encryption
- Encryption & decryption processes use the same key
- Key must be protected against compromise
- Provides confidentiality & basic authentication service

- Does NOT provide non-repudiation service (For better authentication, use a Message Authentication Code (MAC))
- Normally uses a proven algorithm

Point-to-Point with Conventional Key

Advantages of Conventional Key Communications:

- Faster (smaller key lengths)
- Algorithm is straightforward and usually cannot be broken (it is not theoretical)

Disadvantages of Conventional Key Communications:

- No true means of authenticating sender (no digital signature capability)
- If the key is broken, all participants are compromised
- Does not scale well



Public Key Encryption

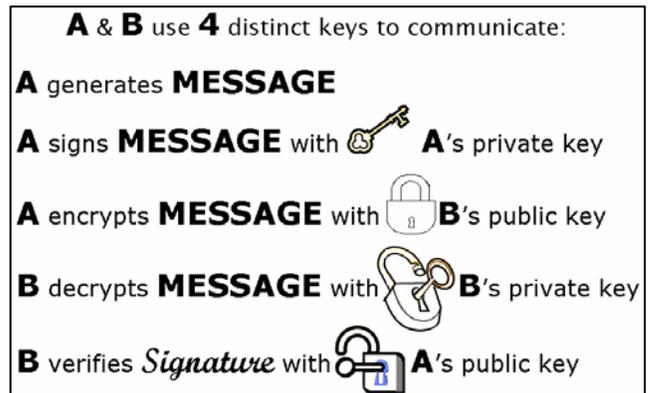
- Also known as Asymmetric Key, and Two-Key encryption
- Public Key: - Used to encrypt messages
 - Does not need to be protected against compromise
 - Available to public through a trusted third party or Key Distribution Center (KDC)
- Private Key: - Used to decrypt messages
 - Must be protected against compromise
 - Distributed by a trusted third party or KDC
- Sender and receiver do not use the same key to encrypt/decrypt messages.
- When something is encrypted with a public key, it cannot be decrypted with the same public key. For this reason, public keys can be shared without fear of compromise.

Public keys can be used for authentication:

- What is signed with the sender's private key must be verified with the sender's public key.
- The sender's private key is used only to digitally sign, not to encrypt.
- Everyone can verify a private key.

Point-to-Point w/Public Key

- Public key algorithms are slower (100+ times longer to encrypt) than conventional algorithms due to the key lengths (1024 bits)
- Time & Date stamping can be used but requires a third-party system.
- Public Key algorithms provide C-I-A as well as a non-repudiation service
- The integrity of the PKI system is ensured through the use of
 - Certificate Revocation Lists (CRL)
 - Compromised Key Lists (CKL)



Department of Defense Certificate Authority

- <http://dodpki.c3pki.chamb.disa.mil>

Hashing

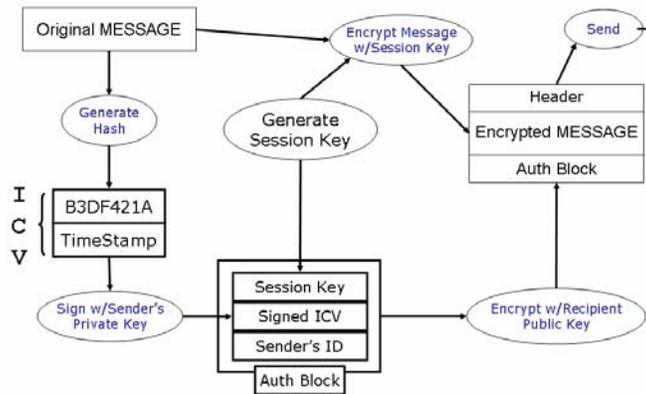
- Hashing is used for integrity purposes only. It is not used to encrypt or decrypt data, but only to provide proof that a message was not altered.
- Hashing is a ONEWAY function.
- Two common types of hashing are:
 - Integrity Check Value (ICV) uses SHA-1 (Secure Hash Algorithm v.1) 160-bits
 - Message Digest 2, 4, or 5 (MD2, MD4, MD5) which is 128bits in length
- Both sender and receiver share the same key, and arrive at the same hash value if the message has not been altered.
- Sender includes the hash value with the message so the receiver can compare the two.
- A good hash function has the following characteristics:
- The hash should be computed on the entire message.
- Message content is not disclosed by the hash value.
- It should be infeasible to create another message with the same hash value given the original message and hash.
- The hash value should display strong cryptographic dispersion.
- It should be impossible to compute the hash value of two messages combined given their individual hash values.
- Common Hash Functions:
 - MD2: Used with digital signature applications; Good for older 16-bit operating systems
 - MD4: Used with digital signature applications; Used on 32-bit operating systems
 - MD5: Extension of MD4; standard on most routers; slower, but more secure; 128-bit hashing function
 - SHA-1: Designed to be used in digital signatures and for more secure digital signature algorithm for federal government applications; 160-bit hashing function

Digital Signatures

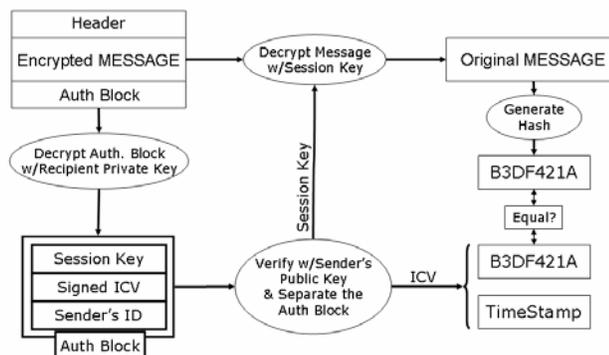
- Used to verify the sender of a message
- Made up of the Public Key, Private Key, Owner's ID
- An ICV or hash is attached to the message. It is this hash that is signed by the sender using the sender's private key.
- The receiver, using the sender's public key, retrieves the hash value and compares it with the value it generates.
- If the two hash values match, the message has not been altered; otherwise, the message is discarded.
- This is the basis for non-repudiation.

PKI (w/Hybrid Crypto)

- Most messages using PK are encrypted using conventional key because it is much faster.
- Attached to the message is an authentication block containing:
 - The conventional (secret) key
 - The hash value of the message signed using the sender's private key
 - A way to identify the sender (name)
- The authentication block is encrypted using the recipient's public key.



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



Crypto Supported Services

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

Encryption Weaknesses

- Mishandling, or human error
- Deficiencies in the cipher
- Cryptanalysis (discussed later)

Network Attacks

- Passive Method
 - Packet Sniffing: Capturing packets off the wire without interrupting the network
 - Content Analysis: Reconstruct entire session; most common attack against existing networks
 - Traffic Analysis: Using traffic flow to map a network's potential weak points; more difficult, less fruitful
 - Countermeasure: ENCRYPT ALL TRAFFIC
- Active Method
 - Jamming: Executing a DoS attack by using fake packets
 - SYN Flooding: Not completing 3-way handshake forcing the receiving system to re-request synchronization.
 - Smurfing: Large amounts of ICMP Echo (ping) traffic sent to a network IP broadcast address.
 - Packet Substitution: Replay or playback attacks in which valid, captured packets are retransmitted with a slight delay to confuse the receiving system. For example, recording the client/server handshake and later sending only the client's half of the handshake to the server from a different system and getting logged on without a password.
 - Countermeasure: Integrity & Strong Password Authentication

Cryptoanalysis

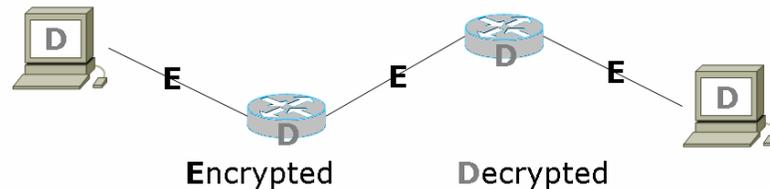
- Cracking codes
- Decoding secrets
- Violating authentication schemes
- Breaking cryptographic protocols
- Finding weaknesses in encryption algorithms

Cryptoanalytic Attacks

- Ciphertext Only – requires analysis using probabilities, distributions, and characteristics of the available ciphertext, plus any publicly known information
- Known Plain Text – knows some plaintext and ciphertext; only needs to determine the algorithm; can use probable plaintext analysis
- Chosen Plain Text – Loaded with a hidden key
- Adaptive Chosen Plain Text – Plain text samples chosen dynamically
- Chosen Ciphertext - Applicable to Public Key attacks
- Adaptive Chosen Ciphertext – The adaptive version of Chosen Ciphertext
- Man-in-the-Middle: Between parties on the same wire
- Timing Attacks: Measuring exact execution times

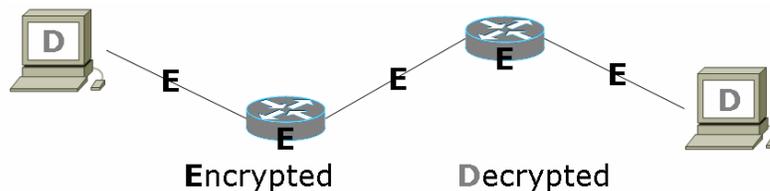
- Differential Power Analysis (DPA): Analyzes power consumption of devices like smartcards.
- Brute Force Attacks: Try all keys until one works
- Birthday Attack: Form of probability; used in attacking hashing functions

Strategies: Link Encryption



- Encrypts traffic as it leaves each node (exits the link)
- Decrypts traffic as it arrives at each node (enters link)
- Headers are encrypted, but the packet is in the clear in each node in the path
- Uses multiple keys – slows things down
- Plain text traffic potentially vulnerable at the nodes
- Example is any Trunk Encryption Device (TED)

Strategies: End-to-End



- Encrypted at source; decrypted at destination
- Plain text traffic not exposed anywhere enroute
- Routing info left in clear
- Target IP/Port address can be exposed
- More information exposed, key more exposed
- Vulnerable to traffic analysis attacks
- Example: VPN

Key Distribution

- Manual Key Distribution
 - Common in symmetric (conventional) encryption
 - Trusted couriers physically bring keys to site
 - Most secure method to distribute keys in a conventionally encrypted network
- Automatic Key Distribution
 - Encrypt with another key
 - Authentication of source is bonus of public key
 - Regular updates
 - Distribution normally from a key server or Key Distribution Center (KDC)

DES

- Data Encryption Standard

- Designated as a Federal Information Processing Standard (FIPS) and adopted by the National Institute of Standards & Technology (NIST) in 1976
- Broken in 1993 using “brute force” and “known plain text”
- Replaced by 3DES as an interim solution
- Conventional/symmetric encryption
- Most widely used block cipher
- Uses 56-bit key on 64-bit blocks
- Used by several OS to encrypt password files
- No flaw in the algorithm has ever been recorded

AES

- Advanced Encryption Standard
- Replacement for DES/3DES
- Developed in 2001
- Uses the Rijndael algorithm
- Key lengths of 128, 192, and 256 bits
- Being implemented in software
- Hardware implementation will be costly

Kerberos

- Used on Windows 2000/2003/XP
- Authentication Service
 - Uses conventional encryption
 - Based on users, not hosts
- Three parts to exchange:
 - Logon to the domain (realm) through a KDC
 - Request a type of service
 - Use a service
- Timestamps used in authenticators; system clocks must be within tolerance (5m default)
- Credentials cache is erased upon logoff or shutdown
- Smart Cards can be used, replacing the password login
- Kerberos is AUTHENTICATION NOT AUTHORIZATION

RSA

- Named after its inventors Ron Rivest, Adi Shamir, Leonard Adleman
- Developed in 1977; first patented PK algorithm
- Offers encryption and digital signatures
- Based on factoring large prime integers
- Very strong, but very slow
- Wide range of bit lengths from 512 to 4096
- In August, 1977, Martin Gardner in “Scientific American” magazine, issued a challenge to readers to break a ciphertext that he published (he also provided the key).
 - It took 17 years to claim the \$100 prize
 - In April, 1994, a team of 600 announced they had broken the cipher using spare time on computers spread across several continents

DH Algorithm

- Diffie-Hellman
- Developed in 1976; first PK algorithm; not patented until 1978
- Used as a secure key exchange or agreement protocol; not used for message encryption or digital signatures
- Uses large prime number factoring
- Very vulnerable to Man-in-the-Middle attacks

Certificate Authorities

- Maintain and issue public key certificates (either from 3rd party or your own server)
- Manages public keys for each entity in its domain
- Verifies identity; constructs the certificate; signs it; delivers it to the requester; maintains it over its entire lifetime
- Provides authentication and integrity services
- Before issuing a public key, a CA will check both the Certificate Revocation List (CRL) and Compromised Key List (CKL)

SSL

- Secure Sockets Layer (ppt)
- Supports web browsers and servers
- Uses one-way public key algorithm (by default)
- Server issues its public key
- Client generates session key using the browser
- Client sends session key to server encrypted with the server's public key (CA)
- Client and server exchange information using session key generated by client
- The server can require the client to authenticate but typically, does not.

EFS

- Encrypting File System
- Uses DESX algorithm for file encryption
- When file or folder is encrypted:
 - FEK (File Encryption Key) is generated
 - FEK used to encrypt file/folder contents
 - FEK stored encrypted as attribute with file/folder
- Uses public key in both DDF (Data Decryption Field) and DRF (Data Recovery Field)
- Conventional encryption used for speed
- Recovery Agent's public key used to encrypt the FEK which is attached to the file
- Uses two certificates (file owner & recovery agent)
- Uses CA; if none available, builds one
- SSH
- Secure Shell
- Used to secure terminal sessions and logins in Unix/Linux operating systems
- Establishes connections between clients and servers
- Used mostly in email, the web, file sharing, FTP, and telnet
- Provides three components:
 - Transport Layer Protocol
 - User Authentication Protocol
 - Connection Protocol

DMS & the CAC

- The Defense Messaging System (DMS) and the Common Access Card (CAC) use a CA scheme
- DMS Encryption
 - PK 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
 - PK 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

Fortezza Smart Cards

- A Fortezza card is a cryptographic module packaged on a PCMCIA smart card
- Fortezza cards have:
 - A clipper chip which is the cryptographic processor
 - A clock for timestamps
 - Permanent memory for certificates (PK 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 10 times in a row

PGP

- Pretty Good Privacy
- Uses Peer Trust instead of a CA
- Uses RSA as its PK algorithm (2048 bits)
- Is secure and a de facto standard in Europe
- Uses IDEA (128 bits) for its conventional algorithm
- Digital signatures are available as are integrity checks using MD5 for hashing
- Major disadvantage: no 3rd party checks

Email Security

- Email security can prevent:
 - Faking/Altering mail
 - Spoofing mail
 - Interception/Stealing mail

Email Security Standards

- Privacy Enhanced Mail (PEM)
- Pretty Good Privacy (PGP)
- MIME Object Security Services (MOSS)
- Secure Multipurpose Internet Mail Extensions (S/MIME)
- Message Security Protocol (MSP)

Wireless Network Security

IEEE 802.11x Standards

(Institute of Electrical & Electronic Engineers)

- IEEE 802.11a
 - (Wi-Fi) Up to 54Mbps in the 5GHz band
 - WEP & WPA
 - Products that adhere to this standard are considered "Wi-Fi Certified"
 - Eight available channels
 - Less potential for RF interference than 802.11b and 802.11g
 - Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments.
 - Relatively shorter range than 802.11b
 - Not interoperable with 802.11b
- IEEE 802.11b
 - (Wi-Fi) Up to 11Mbps in the 2.4GHz band
 - WEP & WPA
 - Products that adhere to this standard are considered "Wi-Fi Certified"
 - Not interoperable with 802.11a
 - Requires fewer access points than 802.11a for coverage of large areas
 - Offers high-speed access to data at up to 300 feet from base station
 - 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels
- IEEE 802.11g
 - (Wi-Fi) Up to 54Mbps in the 2.4GHz band
 - WEP & WPA
 - Products that adhere to this standard are considered "Wi-Fi Certified"
 - May replace 802.11b
 - Improved security enhancements over 802.11b
 - Compatible with 802.11b
 - 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels
- IEEE 802.11i
 - Security fix not a new bandwidth specification
 - Supports 802.1x authentication, TKIP, & AES
 - Referred to as WPA2
 - Improved security enhancements over 802.11x
 - Compatible with 802.11x
- IEEE 802.11n
 - boost 802.11a and 802.11b speeds to 108 Mbps and higher
 - Backward compatible with 802.11x products
 - Standard not finalized

Common Wireless LAN Vulnerabilities

- No configured security or poor security – installed with default settings such as SSID broadcast or WEP standard in effect.
- No set physical boundaries – radio waves are difficult to restrict
- Physically insecure locations
- Untrained users setting up unauthorized workstations and access points – wireless capable laptops brought in by users; untrained help desk staff

- Rogue access points – illicit access points; access points that do not support required security features; wardriving
- Lack of network monitoring – IDS improperly used
- Insufficient network performance – saturated access points
- MAC address filtering – total reliance on MAC filtering can be breached via MAC spoofing and identity threat
- Inadequate encryption standards - WEP
- Off hours traffic/war driving – hackers sitting in parking lots gathering data or driving from place to place looking for connections
- Unauthorized data rates – an access point that appears to be accepting traffic at rates slower than those governed by the protocol could indicate unauthorized access
- Easy to eavesdrop - packets easily captured by anyone
- Man in the middle attacks – hackers pretending to be legitimate access points and then using captured data to access the real access points
- Unsecured holes in the network – faulty design of wireless LANs which allow access behind the firewall
- Denial of Service (DOS) attacks – flooding the network with data packets forcing users to disconnect continually; microwaves, cordless phones, etc.

DoD Policy

- Wireless devices, services, and technologies that are integrated or connected to DoD networks are considered part of those networks and must comply with DoD 8500.1 and 8500.2 and be accredited in accordance with DoDI 5200.40
- For data, strong authentication, nonrepudiation, and personal identification is required for access to a DoD IS. Encryption of unclassified data for transmission to and from wireless devices is required. Encryption must be implemented “end to end”. Encryption must also meet FIPS 140-2 requirements.

Army Best Business Practice (BBP)

- Wireless LANs and PEDs (Personal Electronic Device) with LAN connectivity must meet the same certification and accreditation security requirements as the wired LAN
- Wireless solutions will be engineered to preclude backdoors/trapdoors into the Army LAN
- All bridges must comply with FIPS 140-2 compliance
- Strong authentication required
- ESSID (Extended Service Set Identifier)/SSID (Service Set Identifier – a configurable name associated with an access point to identify the wireless network it supports) broadcast option turned off
- Wireless solutions must meet IA requirements
- Wireless as well as wired infrastructure must be accredited
- Encryption strength will be 128 bit 3DES or AES as a minimum
- Wireless devices used to extend the LAN environment shall support IA related security software, have a host based firewall, an approved anti-virus product installed, management application, and require user-unique authentication as absolute minimums

Standard for implementing a wireless LAN

- Must be certified FIPS 140-2 level 1 end to end encryption; 3DES/AES only
- Must protect OSI layer 2 (Data Link) with an approved FIPS 140-2 encryption module
- Must be able to detect and suppress rogue access points – set up access controls to only allow authorized devices and users access to the wireless network
- Must incorporate a location aware protection scheme – security policies are enforced based on location, connection interface, and wireless access points

FIPS 140-2

- Standard that describes requirements IT products must meet for use with sensitive unclassified information (SUI)
- Has 4 levels of security
 - Level one: The lowest level of security. No physical security mechanisms are required in the module beyond the requirement for production grade equipment.
 - Level two: Tamper evident physical security or pick resistant locks. Provides for role based authentication. It allows software cryptography in multi-user timeshared systems when used in conjunction with a trusted operating system.
 - Level three: Tamper resistant physical security. Level 3 provides for identity based authentication.
 - Level four: Physical security provides an envelope of protection around the cryptographic module. Also protects against fluctuations in the production environment.
- Covers areas related to the secure design and implementation of a cryptographic module
- Establishes encryption requirements for 128-bit 3DES, AES or better

Wi-Fi Protected Access Version 2 (WPA2)

- Uses strong AES encryption based on Rijndael algorithm
- Has 128-, 192-, 256-bit key sizes
- 802.1x for user authentication and key distribution
- Has two strong authentication features
 - Wireless robust authentication protocol (WRAP)
 - Counter with cipher block chaining message authentication code protocol (CCMP)

Not approved for Army use

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access Version 1 (WPA)
- Temporal Key Integrity Protocol (TKIP)
- Encryption based on the RC4 encryption algorithm
- Encryption must be FIPS 140-2 compliant

DoD References

- DISA Wireless Security Technical Implementation Guide April 2004
- DISA Wireless LAN Security Framework Jan 2004
- DISA Wireless Security Checklist Nov 2004
- FIPS PUB 140-2 May 2001
- NIST Wireless Guidance SP 800-48 Dec 2002
- DoDD 8100.2 April 2004 "Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)"
- DoD 8500.1 "Information Assurance"
- DoD 8500.2 "Information Assurance Implementation"
- DoDI 5200.40 "DITSCAP"
- DoDD 8510.1-m "DITSCAP Application Manual"

Army References

- AR 25-2 "Information Assurance"
- AR 380-53 "Information Systems Security Monitoring"
- Army BBP Wireless Security Standards June 2004

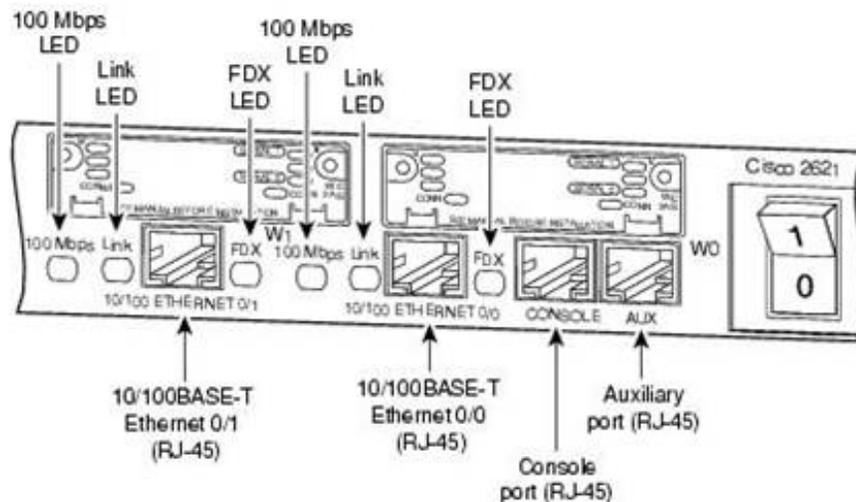
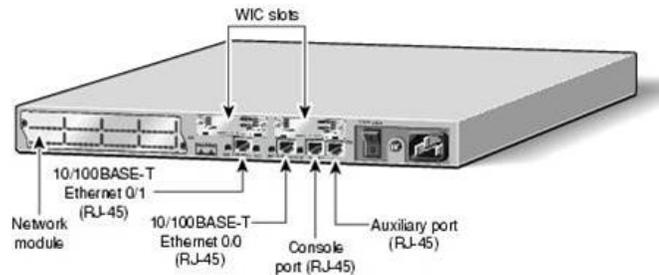
Securing Cisco Routers

Lesson Objectives

- Protecting Passwords
- Configuring Passwords
- Privilege Levels
- Configuring Privilege Levels
- Traffic Filtering and Firewalling

Cisco 2621XM 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 networks



Controlling Access

- Connect using either the console port or through a telnet session.
- Connections to the console port require initial settings of n,8,1,9600bps
- Telnet to an IP address of the router: telnet 172.24.xxx.xxx

User Access Verification

Password:

- When you enter passwords on a Cisco device, the password is not echoed to the screen so others cannot read it.

Access Modes

- User exec mode access:

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

- Privileged mode access:

```
User Access Verification
Password: -----

Router>enable
Password: -----
Router#:
```

Configuration Modes

- Global Configuration Mode:

```
Router#configure terminal
Router(config)#:
```

- Interface Configuration Mode:

```
Router(config)#interface fastethernet 0
Router(config-if)#:
```

- Line Configuration Mode:

```
Router(config)#line console 0
Router(config-line)#:
```

Saving the Configuration

- Current versions of the CISCO IOS still support the wr command. Future versions probably will not.
- To write the running-configuration to the startup-configuration file, you can use wr:

```
Router#wr
```

- Cisco's preferred method of copying the running-configuration to the startup-configuration is to use the copy command:

```
Router#copy running-config startup-config
```

'?' if You Need Help:

```
Router#?
Exec commands:
atmsig          Execute ATM Signaling 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
.....        .....
```

Privilege Levels (Default)

- By default, the Cisco IOS command-line interface (CLI) has two levels of access: user EXEC mode (level 1), and privileged EXEC mode (level 15)
- Upon initial login, the user is placed in user EXEC mode (level 1).
- To gain access to privileged EXEC mode (level 15), use the 'enable' command and password.
- The enable password is not encrypted.
- The enable secret password is encrypted.
- If the secret password is set, it must be used.
- The hash of the secret password (MD5) is stored in the configuration file.

Privilege Levels (Custom)

- By default, newly-created access levels will have normal user EXEC access.
- Additional command access is added to each level using the 'privilege exec' command.
- Create new level 5:

```
router(config)#enable password level 5 student *OR*
```

```
router(config)#enable secret password level 5 instructor
```

- Add the 'ping' and 'trace' commands to level 5:

```
router(config)#privilege exec level 5 ping
```

```
router(config)#privilege exec level 5 trace
```

- Add multiple commands to level 5:

```
router(config)#privilege exec level 5 T1 controller*
```

```
router(config)#privilege exec level 5 ATM*
```

- To display the current privilege level:

```
router#show privilege
```

```
current privilege level is 5
```

Note: the '?' lists commands applicable to the current privilege level

Configuration Files

- To view the configuration currently in effect:

```
router#show running-config
```

- To view the configuration stored in memory which will be loaded upon router restart:

```
router#show startup-config
```

Physical Port Access Control

- To restrict access to the console port:

```
Router(config)#line console 0
```

```
Router(config-line)#login
```

```
Router(config-line)#password student
```

- To restrict access to the auxiliary port:

```
Router(config)#line aux 0
```

```
Router(config-line)#login
```

```
Router(config-line)#password dialup
```

Virtual Port Access Control

- Virtual ports, called 'vty' ports, are used for telnet/ssh remote access.
- Cisco routers come equipped with 5 vty ports, numbered 0 – 4.

- To restrict access to ALL vty ports:
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password student
- To restrict access to a single vty port:
Router(config)#line vty 2
Router(config-line)#login
Router(config-line)#password student
- To reduce the number of vty ports available:
Router(config)#line vty 0 1
Router(config-line)#transport input none
- This command effectively turns off vty ports 0 and 1, reducing the number of available vty ports to three: 2, 3, & 4
- To insure at least one vty port is always available for your admin use:
Router(config)#line vty 0 3
Router(config-line)#login
Router(config-line)#password telnet_users
Router(config-line)#
Router(config-line)#line vty 4
Router(config-line)#login
Router(config-line)#password AdminBackDoor

Password Protection

- By default, the various port passwords are stored in the configuration file in plain text.
- Anyone using either the 'show running-config' or 'show startup-config' command can read them. To eliminate this problem:
Router(config)#service password-encryption
- This command encrypts all passwords other than the secret password and replaces the plain text versions with their hash values.
- Programs are readily available which are capable of decrypting Cisco user (level 7) passwords.
- The Cisco 'enable secret' (level 5) password is hashed using MD-5 and only the hash is placed in the config file. This makes it impossible to crack.

Banners

- "banner exec" displays a banner on terminals with an interactive EXEC. Specifies a message to be displayed when an EXEC process is created (a line is activated or an incoming connection is made to a VTY line).
Router#banner exec
- "banner incoming" specifies a banner used when you have an incoming connection to a line from a host on the network.
Router#banner incoming
- "banner login" displays a login banner. Specifies a message to be displayed before the username and password login prompts. The "no" form of this command deletes the login banner.
Router#banner login

- “banner motd” specifies a message-of-the-day (MOTD) banner. The “no” form of this command deletes the MOTD banner.
- When someone connects to the router, the MOTD banner appears first followed by the login banner and prompts. After the user successfully logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

```
Router#banner motd
Router(config)#banner motd @ text here @
Router(config)#banner login #text here #
Router(config)#banner exec ~ text here ~
Router(config)#banner incoming & text here &
Router(config)#
```

Session Timeout Setting

- Default timeout for an unattended console session or vty connection is 10 minutes. This complies with AR 25-2.
- Should local policy dictate a shorter period of time, the “exec-timeout” command can be used. Example: (sets timeout to 5 minutes and 0 seconds):

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

Access Lists

- Why use access lists?
 - By default, a router routes incoming packets providing a route exists.
 - We do not necessarily want all packets reaching their destinations.
 - Access lists allow us to block or filter incoming packets by making decisions based on certain criteria contained within the packets themselves.
 - All Cisco IP access lists contain an implicit deny statement as the last entry. An empty access list will block every packet on the port by default.
- IP Access Lists
 - Basic IP access lists are processed one-line-at-a-time. Once a match occurs between the packet and an entry in the list, the list terminates.
 - Standard IP access lists can be numbered 1-99 and 1300-1999
 - Extended IP access lists can be numbered 100-199 and 2000-2699
 - The other access list numbers are for protocols other than IP

Standard Access Lists

- Filter by source address only
- To define a standard ACL using a source address and wildcard mask:

```
Router(config)#access-list access-list-number { deny | permit } source [ source-wildcard ] [ log ]
```
- To define a standard ACL using an abbreviation for the source address and source mask of 0.0.0.0 255.255.255.255:

```
Router(config)#access-list access-list-number { deny | permit } any [ log ]
```
- To apply an standard ACL to a vty line:

```
Router(config-line)#access-class access-list-number { in | out }
```
- To apply an standard ACL to an interface:

```
Router(config-if)#access-group { access-list-number | name } { in | out }
```

- Only one of each type of access list (in/out) per group or class can be applied per interface.
- Standard ACL Example 1: Create and employ an access list that will allow only IP addresses 192.168.12.42 and 192.168.12.55 to enter an interface.

```
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
Router(config)#interface fa0/0
Router(config-if)#ip access-group 1 in
```

- Standard ACL Example 2: Create and employ an access list that will deny only the IP source networks 192.168.12.0 and 192.168.13.0 from entering an interface.

```
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
Router(config)#interface fa0/1
Router(config-if)#ip access-group 2 in
```

Extended IP Access List

- Filter by source & destination address and wildcard masks; protocol & Port
 - Router(config)#access-list access-list-number { deny | permit } [protocol]
{ source [source-wildcard] | destination [destination-wildcard] } [operator] [log]
- Protocol: IP, TCP, UDP, ICMP
- Operand: lt = less than; gt = greater than; eq = equal; neq = not equal to
- Port: number or name
- Extended ACL Example 1: Create and employ an access list that will allow access to TCP port 80 on an interface and deny all UDP traffic.

```
Router(config)#access-list 101 deny udp any any
Router(config)#access-list 101 permit tcp any any eq 80
Router(config)#interface fa0/0
Router(config-if)#ip access-group 101 in
```

- Extended ACL Example 2: Create and employ an access list that will deny the TCP protocol on ports 135 and 139 from entering an interface and allow all other protocols & ports.

```
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
Router(config)#interface fa0/1
Router(config-if)#ip access-group 102 in
```

Removing Access Groups/Lists

- Remove the list from the interface before removing the access-list. If the access-list is deleted before it is removed from the interface, data corruption could occur.

```
Router#configure terminal
Router(config)#interface fa0/1
Router(config-if)#no ip access-group 2 in
Router(config-if)#exit
Router(config)#no access-list 2
```

Firewalls

Lesson Objectives

- Define what a firewall is
- Examine types of firewalls
- Define Network Address Translation (NAT)
- Examine firewall capabilities and weaknesses
- Illustrate the proper network placement of a firewall

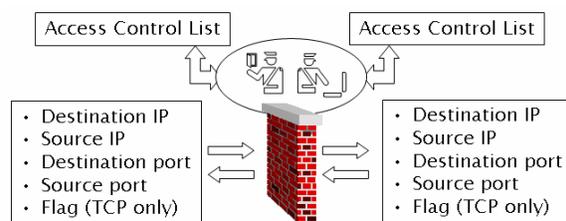
Definition

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

Types of Firewalls

- Static Packet Filtering

Controls traffic by using information in the packet header. Packets are compared against the access control list. Packets will be either forwarded or dropped depending on the active policy.

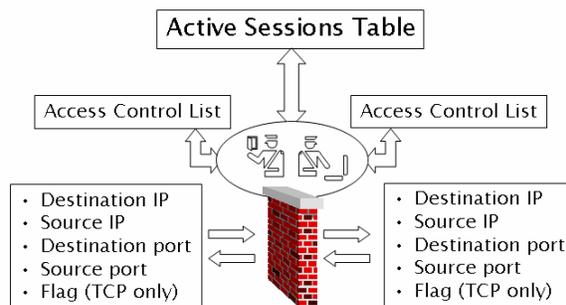


- Dynamic Packet Filtering

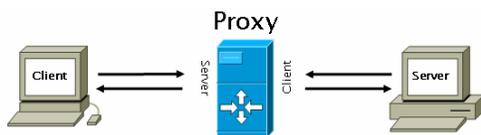
Similar to static packet filtering except that it maintains an active sessions table that monitors the state of a communication session.

- Stateful Packet Filtering

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

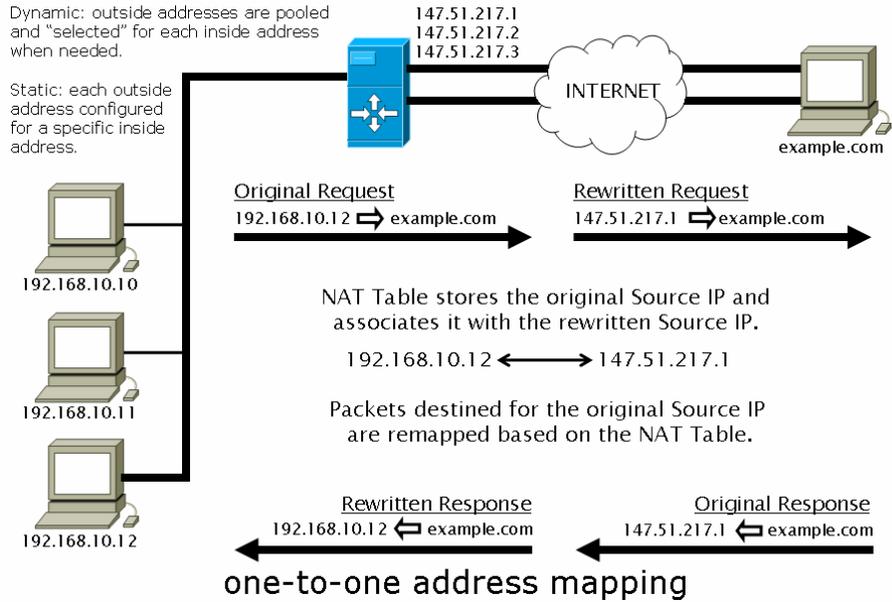


Proxy

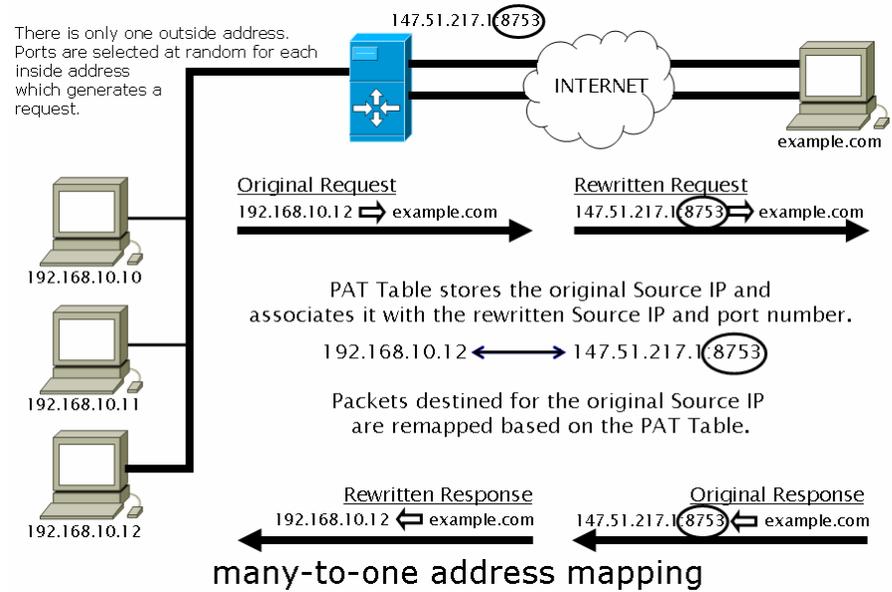


- Plays middleman between two network segments (is an active participant in the communications)
- Source and destination never actually connect
- Stands in and speaks for each system on each side of the firewall

Network Address Translation



Port Address Translation



Firewall Capabilities

- Logging and Notification
Documents all traffic that passes through it and can provide alerts
- Virtual Private Networks (VPN)
As a "flowpoint" for external traffic, firewalls are a perfect place to implement VPNs for remote access
- Filter Java, ActiveX, & HTML Scripts
Remove Java/ActiveX applets from incoming HTTP datastream
- Address Processing
Provides the ability to control how systems are identified through the firewall
- Weak & Strong Authentication Methods
 - ACE/Server
 - Cryptocard
 - S/Key
 - Gateway passwords
 - NT Domain authentication

Potential Weaknesses

- Did you compromise your own firewall?
- Where is your perimeter?
It's hard to prove you're protecting your assets when you can't even identify all of them.
- Dial-in 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
- Tunneled protocols and the firewall
- Anything can be tunneled over other protocols
e.g., Pointcast over HTTP, Telnet/NFS over email
- Tunneling/Encapsulating traffic is routine
- Even if you only allow email in and out, almost anything can "piggyback" over that channel
- Other ways to weaken a firewall
- Excessive alarms
- Bypassing the firewall
If users get into the network in any way other than through the firewall, it's defeated
- Compromised by an insider
- Trojan Horses

Symantec Enterprise Firewall (SEF)

Industry-tested firewall

- protects at the network layer and at the application layer with full application inspection proxies that provide protection against a variety of application-based attacks
- The core of the firewall component is the Symantec driver which incorporates several security features including fragment reassembly, header and datagram validation, and SYN flood protection.
- A security guard that checks the credentials and integrity of both incoming and outgoing packets and determines whether those packets go on to more sophisticated checks
- Symantec's application proxies reduce overhead, create access to services that may not exist on the security gateway, and provide security by creating a virtual air gap between the client and the server.

Virtual private networking

- The security gateway incorporates a robust VPN component, letting organizations securely extend their network. The VPN component is a standards-based solution that establishes encrypted connections from remote locations. The security gateway uses IPsec tunnels to send encrypted and encapsulated traffic across public networks to other IPsec-compliant endpoints.
- Advanced Encryption Standard (AES), Triple DES and DES are supported as well as MD5 and SHA1 for packet integrity.

Content filtering

- Symantec security gateways include a strong content filtering component that lets administrators simply and efficiently deny access to Web sites and Web site content.
- You can make manual entries to the Web site database.

High availability/load balancing

- The security gateway includes support for high availability and load balancing (HA/LB).
- The integrated HA/LB technology is based on a share nothing model.
- Symantec's implementation is network-based, where the network provides the means of communication between all nodes in a cluster. Every node in the cluster shares responsibility in maintaining the state of the cluster over a controlled network.

Anti-spam support

- SMTP proxy to prevent the security gateway from functioning as an SMTP relay. You can impose hard and soft limits on the number of recipients in an email. Additionally, you can check email sources, and if they don't resolve, block them. Optionally, you can elect to use one of the public real-time blackhole lists (RBL) when deciding to accept or reject an email.

Antivirus

- Updates both virus definitions and the engine without service interruption
- The antivirus component incorporates bloodhound technology for heuristic detection of known and unknown viruses.
- The antivirus component detects malicious viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats.

Intrusion detection and prevention

- Symantec security gateways monitor network traffic for suspicious behavior and respond to detected intrusion in real-time.
- Symantec's intrusion detection and prevention component provides a common, highly coordinated approach to detect attacks at very high speeds within the network environment.
- the intrusion detection and prevention component collects evidence of malicious activity with a combination of protocol anomaly detection (PAD), traffic rate monitoring, protocol state tracking, and IP packet reassembly.

Policy - Rules

- Similar to rules themselves, the rule parameters also have a priority as to which takes precedence. For similarly configured rules, the following order is checked:
- Rules that define a time period take precedence over those with no defined time period (<ANYTIME>) when the connection request arrives during that time period. If the connection request arrives outside of the defined time period (trying to access the

network on the weekend when WorkingHours is defined, for example), then the rule with <ANYTIME> takes precedence.

- Rules with more source network bits defined rank higher than those with fewer. Therefore, a rule specific to a host is picked before a rule that defines a subnet, and both of these are chosen before a rule that uses the *universe entity. In cases where there is no difference between the number of network bits, entity names are used, with longer names taking priority over shorter ones.
- Rules with source interface restrictions (eth0, eth1, and so forth) have a higher priority than those with no interface restrictions.
- Rules with more destination network bits defined rank higher than those with fewer. Therefore, a rule specific to a host is picked before a rule that defines a subnet, and both of these are selected before a rule that uses the *universe entity. In cases where there is no difference between the number of network bits, entity names are used, with longer names taking priority over shorter ones.
- Rules with destination interface restrictions are higher in priority than those with no interface restrictions.
- Rules that explicitly deny traffic supersede matching rules.
- Rules with user restrictions overrule those with no restrictions.
- Rules with authentication override those with no authentication.
- This order also defines top-down priority. That is, a rule with a time period takes precedence over a similar rule with authentication.

Report type contents

- Authentication Method report: Configured authentication methods
- Address Transform report: Configured address transforms
- Advanced Option report: Configured advanced option information
- Content Filtering report: Configured content filtering information
- DNS Record report: Configured DNS records
- Filters report: Configured filters and filter groups
- Global IKE Policy report: Configured Global IKE policy information
- H.323 Alias report: Configured H.323 information
- IP Route report: Configured routing information
- License Features report: Configured licensing information
- LiveUpdate report: Configured LiveUpdate information
- Local Administrator report: Configured local administrator information
- Logical Network Interface report: Configured logical nic information
- Machine Account report: Configured machine account information
- NAT Pool report: Configured NAT pools
- Network Entity report: Configured network entities
- Network Interface report: Configured network interface information
- Network Protocol report: Configured protocol information
- Notification report: Configured security gateway notification information
- Proxy Services report: Configured proxy information
- Redirected Service report: Configured service redirects
- Rule report: Configured security gateway rules
- VPN Tunnel report: Configured VPN tunnel information
- VPN Tunnel Policy report: Configured VPN policy information
- Service Group report: Configured service group information System Parameters by Location

Real Secure

Lesson Objective:

Walkthrough the set-up and activation of RealSecure

Overview

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

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 (WinNuke, remote registry accesses, anonymous logins)

Distributed Architecture

- RealSecure uses a distributed architecture and has two major components:
 - the Sensor
 - the Workgroup Manager
- Although not recommended due to performance issues, you can install both components on the same computer.

Sensors

- Software components that are installed on UNIX or Win2K/NT hosts
- Installed on key network segments to protect critical data
- Examine all network traffic on their segment
- Monitor network packets and look for signatures that could indicate an attack against your network.

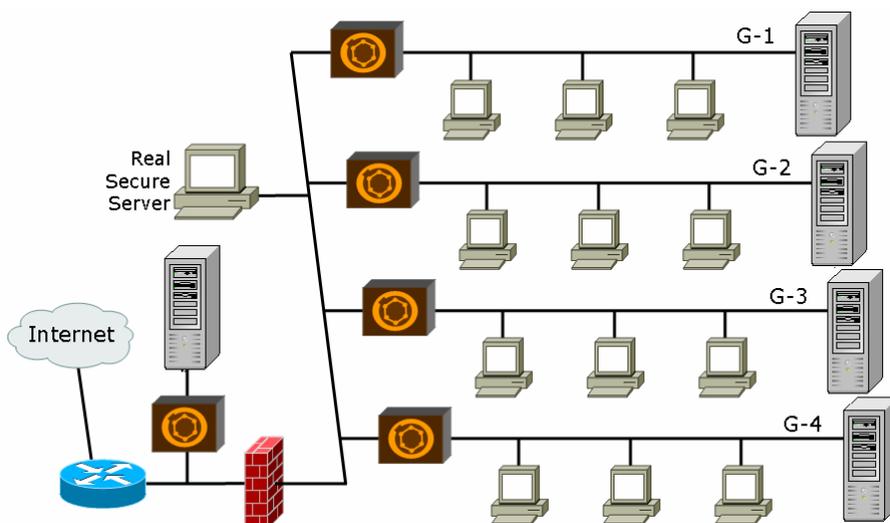
Workgroup Manager

- Central management point
- Receives alarms from Sensors
- Controls the Sensors and configurations
- Aggregates data and generates reports about network activity

Features

- 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

Typical Implementation



Authentication

- Each end of the communications channel has its own private/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

Encryption

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

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).

Reading Assignment 1

Subjects: Encryption, Signatures, Hashes, & Certificate Authorities

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

1. What services do digital signatures provide? _____

2. Define "non-repudiation". _____

3. Name some of the differences between RSA and DSA. _____

4. What other names are used for a hash? _____

5. What the purpose of using a hash? _____

6. Name and define two assurances provided by message digests. _____

7. Name three non-keyed digests and their sizes. _____

8. List and describe the two major PKI frameworks: _____

9. What is a Certificate Authority? _____

Reading Assignment 2

Subjects: Defense in Depth & Router Introduction

Book: Inside Network Perimeter Security, Pages: 7-18, 27-36

1. Briefly define each of the following terms in your own words:

border router: _____

firewall: _____

IDS: _____

VPN: _____

DMZ: _____

screened subnet: _____

proxy firewall: _____

configuration management: _____

2. List the range of numbers used to define standard and extended access lists and describe the differences between the two types.

3. Describe "implicit deny" with respect to an access list and indicate where in an access list it occurs.

4. Why use an ACL on a router when there's usually a high-tech firewall right behind it?

5. What is a range of IP addresses called which is specifically denied by an ACL?

6. An ingress filter is used to protect a _____ from packets with invalid

_____ .

7. An egress filter is used to protect _____ from packets with invalid _____ originating from your network.

Reading Assignment 3

Subjects: Firewalls, Proxies, & VPNs

Book: Inside Network Perimeter Security, Pages: 95-100, 135-136, 252-257, 320-323

1. Where are some typical locations for firewall placement? _____

2. Name two strategies for multiple firewall placement:

a. _____

b. _____

3. What are the purposes of each? _____

4. Name three types of proxies:

a. _____

b. _____

c. _____

5. Briefly explain each type: _____

6. Name two types of NAT assignment:

a. _____

b. _____

7. What are some other names used for PAT? _____

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

Reading Assignment 4

Subjects: Network Intrusion Detection Systems

Book: Inside Network Perimeter Security, Pages: 201-216

1. How does an IDS capture traffic? _____

2. What are two methods used by IDS to generate alerts?

a. _____

b. _____

3. Briefly describe each method (from question 2):

a. _____

b. _____

4. Name three actions an IDS can take upon detection of an event:

a. _____

b. _____

c. _____

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

6. How do switches affect the placement of an IDS? _____

7. Define "false positive": _____

8. Define "false negative": _____

9. Name two methods a hacker might employ to avoid detection by an IDS:

a. _____

b. _____

P.E. – PKI

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.

Your IP Address	Email Address	Your IP Address	AP IP Address
10.0.1.2	wo012@ia1.gov	10.0.6.2	wo062@ia1.gov
10.0.1.3	wo013@ia1.gov	10.0.6.3	wo063@ia1.gov
10.0.2.2	wo022@ia1.gov	10.0.7.2	wo072@ia1.gov
10.0.2.3	wo023@ia1.gov	10.0.7.3	wo073@ia1.gov
10.0.3.2	wo032@ia1.gov	10.0.8.2	wo082@ia1.gov
10.0.3.3	wo033@ia1.gov	10.0.8.3	wo083@ia1.gov
10.0.4.2	wo042@ia1.gov	10.0.9.2	wo092@ia1.gov
10.0.4.3	wo043@ia1.gov	10.0.9.3	wo093@ia1.gov
10.0.5.2	wo052@ia1.gov	10.0.10.2	wo102@ia1.gov
10.0.5.3	wo053@ia1.gov	10.0.10.3	wo103@ia1.gov

You will need a partner for this exercise.

1. Open *My Computer*, double-click on "C:", locate and highlight the "Temp" folder.
 - 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 Plug-in", "PGP Outlook Express Plug-in", 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 full name.
 - b. Enter your **classroom email address** from the list **at the top of this page**.
 - 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 **passphrase that you can remember and confirm** it by entering it again in the confirmation box. Click "Next". (If you are warned that your pass phrase is a potential security hazard, click "Next".)
 - g. If asked to move the mouse to create some random data, do so, then click "Next".
 - h. Once your key is generated, click "Next".
 - i. Your Digital Certificate will be generated. What three pieces of information does your digital certificate consist of (**not displayed on screen – presented in lecture**)?
-
- j. **DO NOT** check "send my key to the root server now". Click "Next", and then "Finish".
 - k. Now, manually start PGPTray by clicking on *Start* ⇒ *All Programs* ⇒ *PGP* ⇒ *PGPTray*. Nothing will open, but you should see a small lock icon in your taskbar tray.
 - l. Close the "My Computer" window.
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 (**10.0.0.100**), and set the port to **389**. Click "OK".
 - e. Select the server you just added, and click the "**Set as Root**" button.
 - f. Delete the other servers in the list. (Use the "**Remove**" button).
 - g. Check every box in the "Synchronize with server" section and Click "OK".
 - h. Right-click on your key pair in PGPkeys and select "Send to". Select the server you just added to your list to have your key sent to it.
 - i. You will receive a message "Key(s) successfully uploaded to server." From now on, the classroom server will make your keys available to anyone who asks for them. Click "OK".
 4. Once your partner has reached this step, add his/her key to your keyring:
 - a. Click the magnifying glass on the toolbar. A search window will open. Do not enter 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. Send your partner an encrypted email.
 - a. Open Outlook Express (user name **wxxxx@ia1.gov** / password "**student**").
 - b. Click "Create Mail", & enter your partner's *complete* email address in the "To:" field.
 - c. For the subject, enter "Encryption Test Message 1".
 - d. Write out a message in the body of the email.
 - e. Click 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 2.j). Make sure you use the **PGP buttons** for this exercise. The others will not work.

- f. This version of PGP does not copy text directly from the email window. In order for it to encrypt (or decrypt) your message, you must first copy it to the clipboard. With the cursor inside the text area of Outlook Express, press CTRL^A (hold down the Control Key and then press the 'A' key) and then CTRL^C. These key combinations first highlight all the text and then copy it all to the clipboard. You will have to follow this procedure every time you want to encrypt or decrypt a message.
 - g. Click each of them once.
 - h. Click "Send".
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 pass phrase? If so, why? _____

7. When your partner reaches this point in the PE, check 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 opens the message in its own window. Click the "▶▶" button if there is one, and then click the button labeled "Decrypt PGP message". Are you prompted for your pass phrase? Why, or why not?

10. Once the pass phrase 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. "(Invalid)" indicates that the key used to verify the signature is not yet a trusted key. Let's assign this key some trust. Open PGPkeys, select your partner's key, right-click on it, and select "Sign..."

14. 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?

15. Click "Allow signature to be exported", and click "OK".

16. Enter your pass phrase, 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.

17. Open your Outlook Express 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?

18. Send your partner a signed, unencrypted email. Which key did you just use?

19. 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 pass phrase? _____

Which key did you use to authenticate the signature? _____

20. 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 pass phrase this time? Why?

21. 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? _____

22. 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.

P.E. – 3COM Access Point

During this PE students will be working in teams. Only one student may access the wireless access point at a time. You may take turns performing the procedures or one can perform the steps with the partner(s) looking on.

This PE was designed to be used with the 3Com 108 Mbps 11g PoE Access Point. Procedures should be similar with other brands or models.

1. Log into Windows XP as the Administrator.
2. You will be accessing a single Access Point (AP). The access point you are going to use depends on the IP address of the computer you are logged into. From the following chart, determine which IP address and SSID you will be using:

Your IP Address	AP IP Address	SSID
10.0. 1 .x	10.0.0.20 1	206A 1
10.0. 2 .x	10.0.0.20 2	206A 2
10.0. 3 .x	10.0.0.20 3	206A 3
10.0. 4 .x	10.0.0.20 4	206A 4
10.0. 5 .x	10.0.0.20 5	206A 5

Your IP Address	AP IP Address	SSID
10.0. 6 .x	10.0.0.20 6	206A 6
10.0. 7 .x	10.0.0.20 7	206A 7
10.0. 8 .x	10.0.0.20 8	206A 8
10.0. 9 .x	10.0.0.20 9	206A 9
10.0. 10 .x	10.0.0.2 10	206A 0

Enter the IP address and SSID of the AP you will be using:

IP: _____ SSID: _____

3. You will first have to connect to the Access Point via the wired LAN before you can use the wireless LAN. Open Internet Explorer and browse to <http://10.0.0.2xx>, where the "xx" value is the value from the table.
4. You should be prompted for a User-ID and a password. The default User-ID is "admin" and the password is "password". The configuration screen for web access should appear.
5. One of the first things to do is to change the default login as this is a potential backdoor. On the left side of the screen is a darker blue menu frame: click on "Management". This opens the management console.
6. You will notice that this screen gives you options to change the User-ID, the password, and the method for connection. The first thing you will change is the method of connection. Under "Admin Connections", *uncheck* "http" and "telnet". When configuring your access point, you want to make sure that the new password is not traversing the network unencrypted; so, *check* "https". Click "Save" in the upper right portion of the screen, then click "Apply/Restart" in the lower left corner. The device will restart and you will have to reconnect using "https" instead of "http". Click "Ok" in any windows that appear and then exit the browser.
7. Open a new browser window and browse to <https://10.0.0.2xx>. (Once again, the xx values represent the address of the AP).
8. Click "Ok" to accept the security alert (things will slow down a bit).
9. Click "Yes" to accept the security certificate.

10. The User-ID and password are still "admin" and "password".
11. Re-open the management console by clicking on the "Management" link in the blue menu on the left.
12. Change the password and User-ID. To do this, check the "Change Admin Password" box and replace "admin" with "access". Then enter the new password "\$1-2threFOR" in both the password fields. Click on "Save". The login box will reappear after a slight delay.
13. Login using the new User-ID and password.
14. The next step is to change the Service Set Identifier (SSID). The SSID is the public name of the network. The default SSID on this device is "3COM". It is a 32 character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the Basic Service Set (BSS). When one access point is connected to a wired network and a set of wireless clients it is referred to as a BSS. An Extended Service Set (ESS) is when two or more BSSs form a single sub-network. On the left side of the screen, click on "Security Profiles".
15. Highlight the top choice of "*3Com[3Com]None[2.4GHz]". The asterisk means that this is the SSID that is enabled.
16. In the "Current Profiles" area of the window, click on "Configure".
17. In the SSID block, enter the new SSID (from Step 2). Make sure and enter it correctly, paying attention to case.
18. Click the arrow by the "Wireless Security System" drop-down box that shows "none". You have 9 choices:
 - None no encryption
 - WEP* Wired Equivalent Privacy (not FIPS 140-2 compliant)
 - WPA-PSK TKIP* (Temporal Key Integrity Protocol) 128 bit encryption improvement over WEP
 - WPA2-PSK AES (Advanced Encryption Standard) with a passkey. It is capable of using key sizes of 128, 192, or 256 bits.
 - WPA-PSK and WPA2-PSK..... TKIP or AES with a passkey*
 - WPA with Radius TKIP with Radius authentication
 - WPA2 with Radius AES with Radius authentication
 - WPA and WPA2 with Radius TKIP or AES with Radius authentication
 - 802.1x WEP with EAP (Extensible Authentication Protocol) authentication
- *WEP and TKIP use the RC4 Stream cipher whereas AES uses a block cipher.
19. Click on "WPA-PSK and WPA2-PSK".
20. Enter the network key: "weektwowirele" [without the quotation marks].
21. Click on the drop-down box for "WPA Encryption" (WPA stands for Wi-Fi Protected Access).
22. The drop down box value should show the encryption value as "TKIP + AES". This means that the encryption will default to either TKIP or AES depending on the highest capability of the client that is connecting. AES is the encryption method we want to use.

AES (Advanced Encryption Standard) ensures that the minimum key strength is 128 bits with block encryption. 192 and 256 key lengths are possible but 128 is the minimum that can be used. This level of encryption is required in order to be compliant with FIPS 140-2 and is, in fact, the basis of the new 802.11i standard.

23. Check the box for "Group Key Update". This causes the AP to periodically update the key for all associated group members. The value of "60" [minutes] is fine for our purposes. Click on "Save" and "Apply/Restart".
24. Click "Ok" in the warning dialog.
25. Close your browser window and open a new one. Reconnect using SSL. You may have to wait a minute or two for the AP to restart.
26. Click "Ok" in response to the security alert.
27. Click "Yes" to accept the security certificate.
28. When prompted for the login, use the new user-id and password.
29. Click on the "Management" link again.
30. Click on the "Log Settings" tab. In a real network setting, you would want to capture log entries. The access point does not have much of a log storage capability. The access point keeps a record of device activity such as system startup and client association/disassociation. The maximum internal log file size is 30KB. Once this size is reached, the log file is purged and all log records are lost. You have two choices for sending your logs to another server. If you have more than one syslog server and they alternate times, choose the broadcast mode. If you have a dedicated syslog server you should enable "syslog" and have it log to that server. The syslog method is similar to how a UNIX system does remote logging. We won't change logging at this time.
31. Click on the "Access Control" link on the left menu frame. You will see that you can enable access control via a physical MAC address.
32. Click on the "Trusted Stations" tab. You can set up a trusted station list based on individual MAC addresses.
33. Click on the "Wireless" link in the left menu frame. In the "Basic" tab, under "AP Mode", you will notice that "Broadcast SSID" is selected. Deselect "Broadcast SSID" and click "Save". By default, the Access Point will broadcast its SSID every few seconds to allow clients to dynamically discover and roam between WLANs. Knowing your SSID allows a hacker to be one step closer to accessing your site. The SSID will still be detectable by sniffing Wi-Fi Protocol traffic but why make it any easier.
34. Click "Apply/Restart" in the menu frame. You may have to wait a minute or two to log back in.
35. In the blue menu frame on the left, click on "System". This is where you would reconfigure the access point for a particular address on your network. You can see places to enter the IP, subnet mask, gateway and DNS settings.
36. Click "Ok".
37. Close your browser window. Your wireless access point should be setup and should meet the DoD requirements of FIPS 140-2.

END OF PE

P.E. – 3COM Wireless Adapter Installation

1. Boot up your system into Microsoft Windows XP.
2. Login as the administrator.
3. Disable the onboard LAN connection:
 - a. Execute "*Start ⇒ Control Panel*".
 - b. Click on "Network and Internet Connections".
 - c. Click on "Network Connections".
 - d. Right-click on "Local Area Connection".
 - e. Left-click on "Properties".
 - f. Highlight "Internet Protocol TCP/IP" and click on "Properties".
 - g. Note the IP address/Mask setting: _____
 - h. Left-click on "Ok" twice to close the windows.
 - i. Right-click on "Local Area Connection".
 - j. Left-click on "Disable".
 - k. Close the "Network Connections" window.
4. Place the USB adapter installation CD in the CD-ROM drive. The Wireless Utility Installation Wizard should start. If it doesn't, click "*Start ⇒ Run*", then type "*d:\setup.exe*" (where 'd' is the letter of your CD-ROM drive).
5. Use the wizard to install the utility:
 - a. Left-click on "Install Wireless Product". (It will take a few moments...)
 - b. Click on "Next".
 - c. Accept the license and click "Next".
 - d. Click "Next" to accept location.
 - e. Click "Next" to accept the folder.
 - f. If a message appears telling you the utility has not passed Windows logo testing, click "Continue Anyway" to complete installation. The windows logo message may appear twice and you may have to click "Continue Anyway" once more.
 - g. Click "Finish" to complete the installation.
6. After a slight delay, a box will appear asking you to plug in the wireless USB adaptor. Plug the USB adapter cradle into a USB port on the computer; then install the adapter into the cradle. Push in the cradle button so that the connection is made. The 'found new hardware wizard' should appear.

7. Click on "No" in response to the "Can Windows connect to Windows Update" question and then click on "Next". If a message appears telling you the utility has not passed Windows logo testing, click "Continue Anyway" to complete installation. Windows will install the driver for the USB adapter.
8. Click "Finish" to complete the installation. The new hardware found message may reappear and you may have to repeat this step by reinstalling the software.
9. Click "Finish" to complete the Windows part of the installation and then on "Exit" to close the 3COM installation program.

At some point during the installation, you may see a popup window indicating that a wireless network is within range. Close the window – you will not be connecting yet.

10. Setup TCP/IP on the new wireless adapter:
 - a. Execute "*Start ⇒ Control Panel*".
 - b. Click on "*Network and Internet Connections*".
 - c. Click on "*Network Connections*".
 - d. Right-click on "*Wireless Network Connection*".
 - e. Left click on "*Properties*".
 - f. Highlight "*Internet Protocol TCP/IP*" and click on "*Properties*".
 - g. Add 2 to the IP address from item #3.g. (For example, adding 2 to the IP address x.x.x.2 produces x.x.x.4; adding 2 to x.x.x.3 produces x.x.x.5). Enter this IP address and subnet mask (which *doesn't* change from item #3.g) into the appropriate fields on the setup screen. Use 10.0.0.1 for both the gateway and DNS addresses.
 - h. Click "Ok" to accept changes and then close the Connections Properties Window.
11. To configure the wireless connection using the 3Com Office Connect Wireless Utility, either double-click the "3Com Wireless 108Mbps USB Utility" icon on the desktop or from the start menu, click "*Programs ⇒ 3Com OfficeConnect Wireless Utility ⇒ 3Com Wireless 108Mbps 11g USB Adapter ⇒ 3Com Wireless 108Mbps 11g USB Utility*". The program may flash on the screen and then disappear – you will have to click on the icon that has appeared in the tray (located in bottom right of screen) to run the program.
12. For the wireless stations on the network to be able to successfully associate with the Access Point, their settings must be configured to match those of the Access Point. If the Access Point's security is disabled, any wireless station that knows the SSID would be able to associate with it. In the 3Com OfficeConnect Wireless Utility, click on "Profile Manager" in the left part of the window.

13. Click on "New".
14. Fill in the profile name with the SSID assigned to your Access Point.
15. Fill in the SSID1 field with the SSID assigned to your Access Point (remember that the SSID is case sensitive).
16. Click the "Advanced" tab and select "Infrastructure" from the Network Type drop down box. The wireless station must be set to "Infrastructure Mode" and not "Ad Hoc" mode. "Ad hoc" mode is for peer to peer wireless communications.
17. Click the security tab.
18. Under "Set Security Options" select "WPA-PSK" and click "Configure". You configured the Access Point for WPA-PSK and WPA2-PSK so we could utilize the AES encryption and authentication features. Using WPA-PSK will match the Access Point setting for AES. Not all wireless clients package AES with the WPA-PSK setting. Make sure you consult your documentation to determine if the client adaptor can use AES or if it only uses TKIP.
19. The wireless security on the station must be set to WPA-PSK and the pre-shared key entered in the Access Point must also be entered on each wireless station. Enter the passphrase. The pre-shared key is "weektwowirele".
20. Click "OK"
21. Click "OK"
22. On the profile manager screen, with the profile for your access point highlighted, click "Activate". The status screen should appear with the link status showing "Authenticated". Security type should read "PSK-AES". The tray icon for the utility should show a small flashing green square instead of the red one.

The next 6 steps (23 -28) are performed on the Access Point:

23. Open a browser window and try to connect to the access point.
<https://xxx.xxx.xxx.xxx> (where xxx is the various octets of the Access Point IP)
24. Accept the certificate. Enter User-ID ("access") and Password ("\$1-2threFOR").
25. When the Access Point status screen appears, click on the "stations" tab for a list of associated machines. When a wireless device connects, it is called associating.
26. Click on the "log" tab for info on authentication and accreditation. Do not click on the "Clear" button or you will lose your log data.

27. Click on the "profiles" tab for total client connection info.
28. Click "Logout" on the left menu pain and then "OK" to logout of the access point. Close the browser window.
29. In the wireless client adapter utility, click on "Site Survey". The Access Point connection that you made should show up on the list.
30. Close the utility window and open a command prompt.
31. Ping the access point and some of the routers (10.0.1.1, 10.0.2.1, 10.0.3.1, etc.) to verify network connectivity. All connectivity should be supplied by the Access Points and their LAN interconnections. Your wireless connections to your one Access Point are referred to as a "Basic Service Set" (BSS). The fact that all of the Access Points and their wireless clients are connected via a LAN makes the network an "Extended Service Set" (ESS).
32. Close the command prompt window.
33. Put everything back to normal:
34. Disable the onboard LAN connection:
 - a. Execute "*Start ⇒ Control Panel*".
 - b. Click on "*Network and Internet Connections*".
 - c. Click on "*Network Connections*".
 - d. Right-click on "*Wireless Connection*".
 - e. Left-click on "*Disable*".
 - f. Right-click on "*Local Area Connection*".
 - g. Left-click on "*Enable*".
 - h. Close the "*Network Connections*" window.
35. Disconnect the USB cradle and adapter from the computer, place them back into the box along with the install CD and return them to the instructor.

END OF PE

P.E. – AirCrack

This practical exercise is designed to illustrate the advantage of increased encryption key length. Most home users use what is known as Wired Equivalency Protocol (WEP). This protocol has an important function: it outlines a way to encrypt the data packets that travel over IEEE 802.11 networks. Unfortunately, WEP encryption is based on a symmetric stream cipher (RC4). As is true for all stream ciphers, it's important that each packet have a different WEP secret key. The WEP standard specified the use of different keys for different data packets, which is a very good idea. This approach relied on the use of initialization vectors (IVs). Originally, these IVs were intended to be unique for each packet, but the space of possible vectors was too small to avoid duplications. As a result, the IVs had to be reused. When IVs are reused, an attacker can use them to recover the plain text. You will be using this vulnerability to decipher encrypted wireless communications during this PE.

You will first examine captured data that used a 40-bit WEP key and then examine captured data that used a 104-bit key. The differences will be readily apparent.

This PE requires the use of Linux tools to crack the key. Pay close attention to the exact format of the commands used.

1. Insert the Linux boot disk and restart your computer.
2. Your computer will boot-up in Linux and prompt you to log in:

livedcd login: **root** and hit **ENTER**
3. The prompt will change to "root@livedcd: ~#". Welcome to the command line.
4. A CDROM is considered by Linux to be an external file system. In Linux, an external file system must be mounted to a directory within the Linux native file system in order for the operating system to see it. To do this, you will use the "mount" command:
 - a. First, create a directory in which to mount the drive:

Type: **mkdir /mnt/hda1**
 - b. Next, mount the drive to the new directory:

Type: **mount -t ntfs /dev/hda1 /mnt/hda1**

If you've executed this correctly, the prompt should return and you should not receive any messages. If you *do* receive a message, try executing the commands again. If you are still unsuccessful, notify the instructor.
5. The capture files are located in a directory on the XP drive called "CAP". Change to that directory:

Type: **cd /mnt/hda1/cap**
6. Type: **ls -l**

You will see two files: one, "07-min-40bit.cap", contains 7 minutes of traffic which was

encrypted using a 40-bit key and the other, "15-min-104bit.cap", is a 15 minute capture of 104-bit traffic. We will use a Linux tool called "AirCrack" to try and break (or "crack") the encryption of the initialization vectors used in sending the packets.

7. First, you'll try cracking the 40-bit traffic:

Type: **aircrack -n 64 ./07min-40bit.cap**

- a. Was the key successfully cracked? _____
- b. Did it take a long time? _____

8. Next, you'll try cracking the 104-bit traffic:

Type: **aircrack -n 64 ./15min-104bit.cap**

What was the result this time? _____

9. What conclusions can you draw at this point? _____

10. The 104-bit sampling provided twice as much data as the 40-bit sample but still proved to be beyond the capabilities of basic AirCrack. (Substituting the -f command line option for the -n option will cause Aircrack to successfully discover the key because it was encoded with WEP. Had it been encoded with WPA, it would be impossible for Aircrack to discover the key.) 128-bit AES encryption is required in order to be in compliance with FIPS 140-2. Would this stand up to AirCrack?
- _____

11. Lets take a look at one of the captures and locate the initialization vector that is being decrypted:

- a. Type: **startx**

The X-windows program will start. You will be in what is known as the KDE Window Manager. In the lower left corner you'll see a "K" in a gear sprocket. This is equivalent to the Microsoft Windows "Start" button.

- b. **Left-click** on the "K".
- c. A menu will pop up. **Highlight** the "Security Toolbox".
- d. **Left-click** on "Network traffic analyzer (Ethereal)".
- e. Once Ethereal has completed loading, **left-click** on the "File" menu.
- f. **Left-click** on "Open".
- g. **Double-click** on "Filesystem" to open up the file system.
- h. In the right window pain, **double-click** on "mnt".

- i. **Double-click** on "hda1".
 - j. **Double-click** on "CAP".
 - k. **Highlight** the "07min-40bit.cap file".
 - l. **Click** "Open" (in the lower right-hand corner of the window).
12. The contents of the capture file should be displayed. You may get a message stating the capture stopped in the middle of a packet, if so **left-click** "Ok" -- this is normal.
 13. **Highlight** one line from an Intel source (NIC card).
 14. In the middle window, **left-click** on the directional arrow next to "IEEE 802.11". This will open up the data for viewing.
 15. **Left-click** on the directional arrow next to "WEP parameters".
 16. When this opens up, you should see the initialization vector. This hexadecimal value is what is being decrypted to find the key.
 17. Close the program by **left-clicking** the "x" in the upper right corner of the window.
 18. **Left-click** on the "K" button in the lower left corner of the screen and **select** "Logout".
 19. **Left-click** on "End Session" to return to the shell prompt.
 20. At the #prompt type: **reboot**
 21. Take out the Linux CDROM **during reboot** and log back in to XP Pro.

END OF PE

P.E. – Cisco 1: Privilege Levels

This Practical Exercise must be performed through HyperTerminal.

1. From the user mode (>) Enter the command: ? Notice the number 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. Type: **enable** (Password is **student**)
What mode have you just entered? _____
At what privilege level are you now? _____
4. Type: ?
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. Type: **show running-config**
6. Type: **configure Terminal**
What mode are you now in? _____
7. Type: ?
Compare this list to the commands in *priv-lvl-15.txt*. As you can see, the command list is different for each mode.
8. Type: **enable password level 6 cisco**
Explain what this command sets for the router: _____

9. Type: **privilege exec level 6 debug**
Type: **privilege exec level 6 reload**
What have these commands done? _____

10. Type: **CTRL^Z** (This means hold down the control key, and press Z)
Type: **show running-config**

Verify your changes by looking for the privilege commands in the configuration.

11. Type: **Exit**

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

12. Type: **Enable 6**

Are you prompted for a password? _____

Which password works with this command? _____

What prompt do you have now? _____

What privilege level are you in now? _____

13. Type: **?**

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

14. Type: **Exit**

END OF PE

P.E. – Cisco 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.

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>
Router(config)#exit
```

Check the new password by logging back into the router.

2. Set the vty passwords to **telnet_user** by entering the following commands:

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

Verify the password was successfully changed by telneting to the Router.

3. Take a look at the running configuration file:

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

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

4. Encrypt the passwords by entering the following commands:

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

5. Take another look at the running configuration file:

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

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

6. Set the Secret password to **Roscoe** by entering the following commands:

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

7. Verify the password was successfully changed. Take a third look at the running configuration file:

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

Is there a difference between the way the enable password is encrypted and the enable secret password is encrypted? **YES / NO**

If so, what is the difference? _____

If not, why would you use one over the other? _____

END OF PE

P.E. – Cisco 3: Banner Creation Configuration

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

For this P.E., you may either abbreviate the DoD banner depicted here, or cut-and-paste it into a text editor and transfer it to the router using HyperTerm. Do not take the time to type the entire banner into the router.

1. 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 ENSURING 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)#
```

2. 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.

END OF PE

P.E. – Cisco 4: Standard ACL Configuration #1

The objective of this P.E. is to configure a standard access control list to block a network and then activate it 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 it is the only network allowed to send data into your network. You also need to decide which interface to apply the access-list to. Fill in the blanks below, enter global configuration mode and type the following:

```
Router (config)#access-list 1 permit _____
```

```
Router (config)#interface _____
```

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

```
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 / NO**
3. Now PING one of the IPs you allowed. Were you successful? **YES / NO**
4. Use the show access-list command from the privileged mode prompt to look at your ACL.
5. Once the instructor has verified that the access list is working, remove it.

```
Router(config)#int
```

```
Router(config-if)#no ip access-group 1 in
```

```
Router (config-if)#exit
```

```
Router (config)#no access-list 1
```

```
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 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? **YES / NO**

END OF PE

P.E. – Cisco 5: Standard ACL Configuration #2

The objective of this P.E. is to configure a standard ACL to block two specific IP address within trusted networks, and activate the access-group on your router.

1. Choose *two* networks in the classroom to be the only trusted networks. Choose *one* IP address from each of these networks to be untrusted systems.
2. Develop an access list with the following definitions being true:
 - *Permit* access from any *trusted* network
 - *Deny* access from any *untrusted* address
3. 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, then enter the commands into your router. (All lines and blanks may or may not be necessary)

```
Router(config)#access-list _____  
Router(config)#access-list _____  
Router(config)#access-list _____  
Router(config)#access-list _____  
Router(config)#access-list _____  
Router(config)#interface _____  
Router(config-if)#ip access-group 1 in  
Router(config-if)#Ctrl^Z
```

4. After applying your access list, have the untrusted addresses try to access your router (telnet and/or ping).

Were they successful? **YES / NO**

The instructor will verify that your access list is working.

5. Now, pick the first network you allowed and deny the other host on that network. The following instructions illustrate one method of modifying an existing ACL.

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

Copy/paste the ACL to a text editor (Notepad in Windows, or vi editor in Unix) and edit it to add the new host you want to deny.

Now, remove the old ACL, and put the new one back in its place: (Fill in the blanks first, then perform the steps on your router)

Router(config)#int _____

Router(config-if)#_____ ip access-group _____ in (Remove the list from the first interface)

Router(config-if)#exit

Router(config)#_____ access-list _____ (Delete the entire list)

6. Now, refer back to step three and repeat that step for the new ACL.
7. 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 not be necessary.)

Router(config)#access-list _____ _____ _____ _____

Router(config)#access-list _____ _____ _____ _____

Router(config)#line vty _____

Router(config-line)#access-class _____ in

Router(config-line)#Ctrl^Z

END OF PE

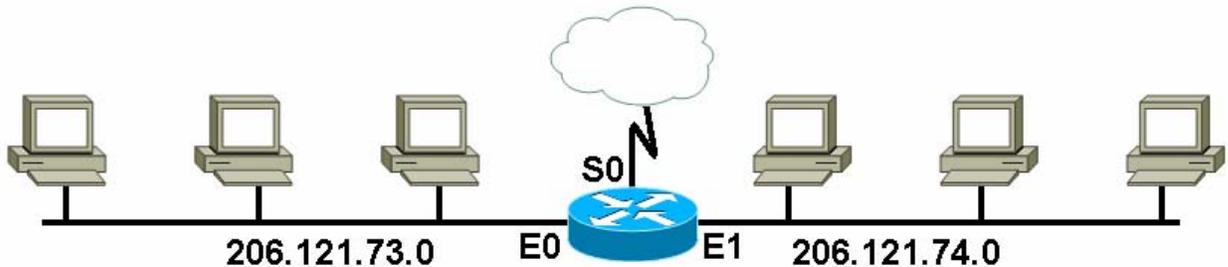
P.E. – Cisco 6: Spoofing Filter

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

P.E. Objectives:

- Configure a standard access list to prevent untrusted networks from spoofing inside addresses.
- Configure a standard access list to prevent your inside trusted networks from spoofing other outside networks.

Recent concerns of possible spoofing from the outside (Internet) into your networks (206.121.73.0 and 206.121.74.0) have prompted you to set spoofing filters on your router.



1. 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)# _____

2. What interface(s) will you apply the access-list to? _____

3. Will it be applied inbound or outbound? _____

4. Can you prevent inside users from spoofing out? _____

5. If so, how? (Remember, maximum security.)

Router(config)# _____

Router(config)# _____

6. What interface(s) will you apply the access-list to? _____

7. Will it be applied inbound or outbound? _____

NOTE: Answers may vary!

END OF PE

P.E. – Cisco 7: Extended Access List Configuration

The objective of this P.E. is for you to configure an extended access list to block certain TCP/IP services from specified networks, and apply it to the interface(s) of the router.

1. Configure an extended access list on your router.

- Allow certain addresses to Telnet (port #23) to your network (pick a few IPs).
- Block all Telnet (port #23) traffic from all other networks.
- Allow Pings (ICMP Echo Packets) from only certain addresses (pick a few IPs).
- Deny all other ICMP traffic to enter your router.
- 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 in to your router)

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

(the next command 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 _____

(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 to which this should be applied)

Router(config)#interface _____

(applies the access list 101 to the interface)

Router(config-if)#ip access-group 101 in

Router#<Ctrl> Z

2. Test the ACL:

Have someone you allowed telnet to your router.

Were they successful? YES / NO

Have someone that was not allowed telnet to your router.

Were they successful? YES / NO

Have someone you allowed ping your router.

Were they successful? YES / NO

Have someone you did not allow ping your router.

Were they successful? YES / NO

END OF PE

P.E. – Firewall 1: Getting Started with SEF 8.0

- Your Symantec Firewall has been installed already.
- The interface does not have to be activated for the firewall to run.
- Symantec Gateway Management Interface (SGMI) is used for configuration and management of the firewall
- Follow the instructions below and answer the questions. Use the firewall computers, and the “subnet” computers as instructed

Remember: Anytime you make changes, additions, and/or subtractions to the firewall, press the *Apply* button and *Activate Changes* from the *Action* drop down.

1. Start the firewall application: Double-click the *Symantec Gateway Management Interface* icon on the desktop
2. A browser will open. The url will be *https://localhost:2456/index.html*. Click “Yes” after reading the contents of the Security Alert. You will then be presented with a Log On screen. Enter “admin” for User Name and “student” for the Password. Click on the “Log On” button.
3. Verify the Security gateway is running. *This information is available on the main SGMI screen as well as in the upper right hand portion of the screen.*

If you see the message “CHANGES PENDING” in red, alert the instructor.

4. What is the current Active Configuration? _____
(This information is available on the main SGMI screen.)
5. Select the *System* folder in the left column. Select the *Features* tab:

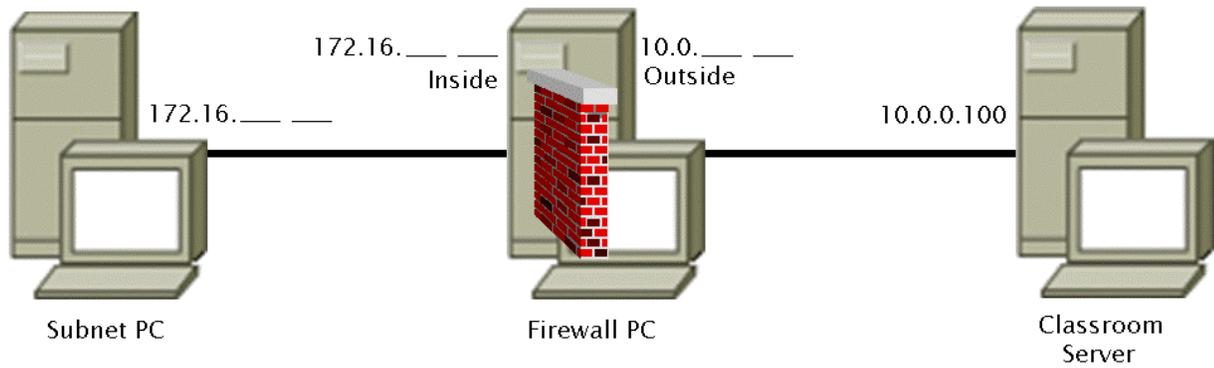
What does it say about the license we are using? _____

Select the *System* folder. Click on *Network Interfaces*. You should see two network adapters. The IP address 172.16.xx.xx is the Inside NIC and the IP address 10.0.x.x. is the Outside NIC.

<p>ON THE BACK OF THIS PAGE, ENTER THE INSIDE AND OUTSIDE ADDRESSES ON THE DIAGRAM. REFER TO THIS DIAGRAM THROUGHOUT THE <u>REMAINDER</u> OF THE P.E.s.</p>
--

If you do not see both interfaces, alert the instructor.

END OF PE



P.E. - Firewall 2: Checking Connectivity

- Follow the instructions below and answer the questions. Use both the firewall computer and the Subnet computer (the Subnet computer is the computer behind the firewall).
 - The diagram on the back of the previous page illustrates the mini-network you'll be working with.
 - Write down abbreviated responses in your answers only.
 - Use the Command Prompt for ping.
1. On the firewall computer, check out the firewall's interface status by performing the following steps: (You should receive a response to each ping command.)

Enter the response to the command **ping localhost** :

Enter the response to the command **ping 10.0.0.100** :

Write the response to pinging the Subnet computer's NIC (172.16.xx.xx):

2. On the subnet computer, enter the following commands to determine the status of its interfaces:

Enter the response to pinging the internal firewall interface (172.16.xx.xx):

Write the response to pinging the external firewall interface (10.0.xx.xx):

Write the response to the command "ping 10.0.0.100" (classroom server):

3. Why did we receive the above responses?

END OF PE

P.E. – Firewall 3: Allowing & Controlling Outbound Access

Changes must be saved using *Apply* and *Activate Changes* before they will take effect.

1. Select the *Policy* folder, choose the *Service Groups* tab.
2. Click on *New Service Group*. Once the *new_service_group* is created, select it and then click on *Properties*. Make the following changes:
 - General Tab
 - Service Group Name: Ping
 - Ratings Profile: None (default)
 - Caption: Exercise 3
 - Protocols Tab
 - Locate "ping" in the *Available Protocols* pane, select it, and click on the >> button. You should now see "ping" in *Included Protocols* pane.
3. Repeat Step 2 to create another Service Group. Make the following changes:
 - General Tab
 - Service Group Name: Outbound
 - Ratings Profile: None (default)
 - Caption: Exercise 4-8
 - Protocols Tab
 - Locate "ping", "ftp", "http", "telnet" and "dns_udp" in the *Available Protocols* pane, select each, and click on the >> button. You should now see them in *Included Protocols* pane.
4. Click *Apply*. Notice at the top of your screen that "**Changes Pending*" is displayed. That will be displayed until *Activate Changes* has concluded.
5. Select *Rules* tab. Select *New Rule*. Once the *new_rule* is created, select it and then click on *Properties*. Make the following changes:
 - Rule Name: Exercising
 - Arriving through: Inside
 - Source: Universe
 - Destination: Universe
 - Leaving through: Outside
 - Service Group: Ping
 - Action: Allow (default)
 - Caption: (leave blank)
6. Click "*Apply*". On the *Action* Drop Down, scroll down to *Activate Changes*.
7. On the *Activate Changes* window click "*Next*" twice. Wait for the *Close* option to appear. Select "*Close*". Changes you made are now in effect.
8. On the Subnet computer, ping the classroom server (10.0.0.100). Did you receive a reply? Why? or why not?

9. On the subnet computer: telnet to the Gateway Router (155.8.216.1). What response did you receive? _____

Why did you get that response? _____

10. On the *subnet computer*: telnet to the outside NIC of the firewall (10.0.xx.xx). Do you get a hostname prompt? _____

Why did you get that response? _____

11. Select the *Location Settings* folder, choose the *Network Entities* tab.

12. Click on *New Network Entity*, choose *New Host Network Entity*. Once the *new_host_network_entity* is created, click *Properties*. Make the following changes:

- Entity Name: WOxxx (use your subnet computers name)
- IP Address: 172.16.xx.xx (use subnet computers IP)

13. Click "Ok", click "Apply".

14. Go back to step 5 and change the rule named Exercising. Click on *Properties*. Change the following items only:

- Source: WOxxx (use your subnet computers name)
- Service Group: Outbound

15. Repeat steps 6 and 7 to apply and activate changes.

16. Repeat steps 8, 9 and 10 from Subnet PC. Record your results.

Ping the classroom server. Did you receive a reply? _____

Are you able to telnet to the gateway router? _____

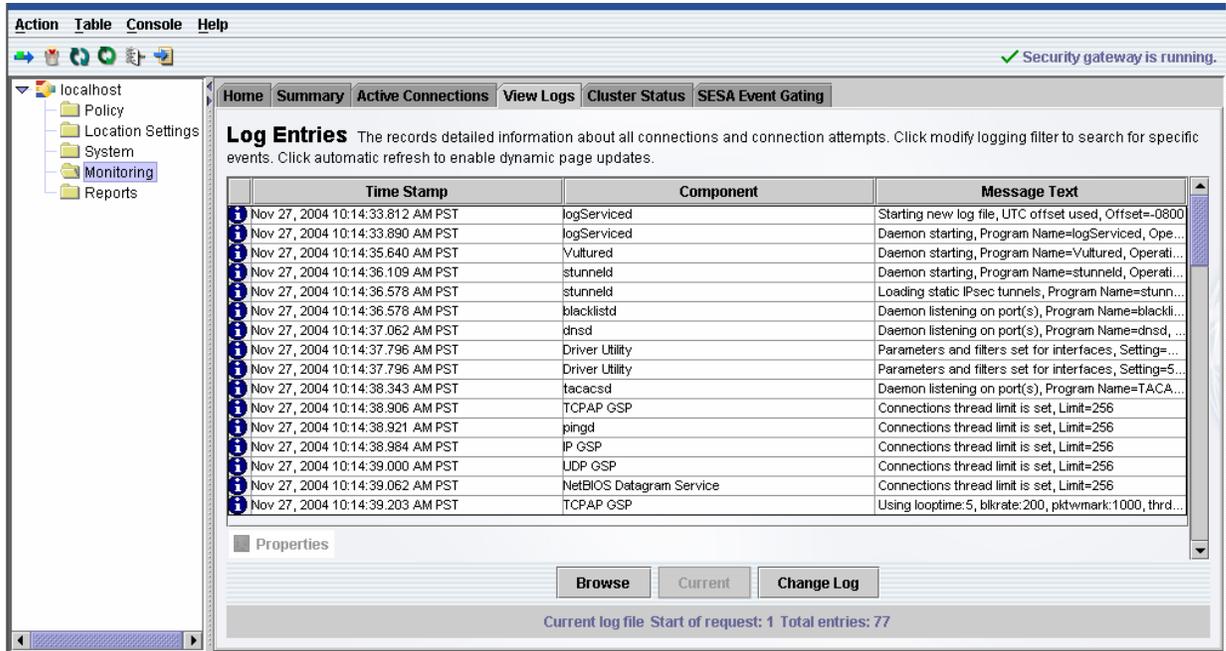
Can you telnet to the outside firewall NIC? _____

Why did you get the responses this time around? _____

END OF PE

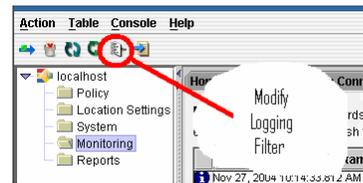
P.E. – Firewall 4: Monitoring Logs

1. Select the *Monitoring* folder and choose *View Logs* tab. You will see data already picked up by the firewall.

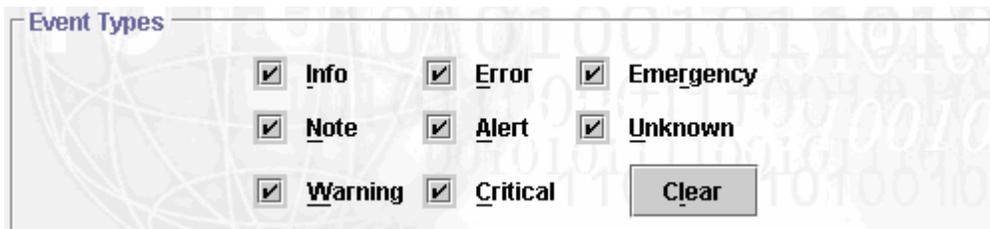


2. Go to the *Table* drop down and select *Show Columns*. Select *Log Sequence*, *Time Stamp*, *Event Type*, *System Name*, *Component*, & *Message Text*. Close the window.

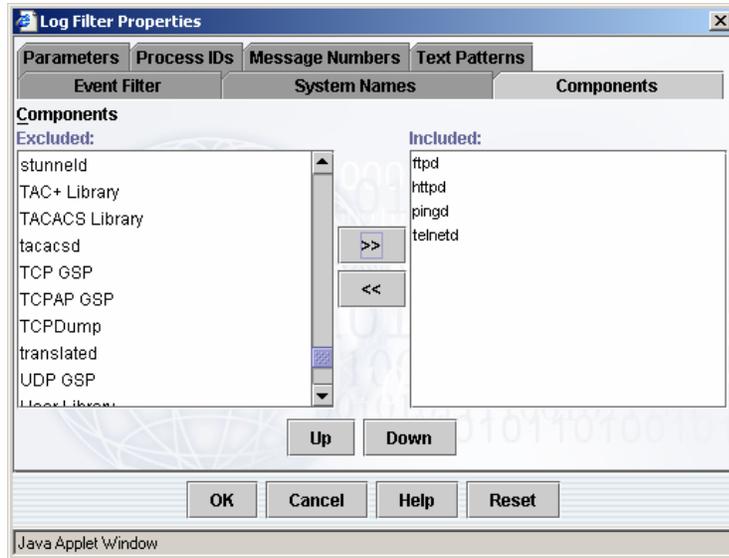
3. Click on *Modify Logging Filter* on the task bar (illustrated here).



4. Once the *Log Filter Properties* display is open, select the *Event Filter* tab. Place a checkmark in all options under *Event Types*:



5. Select the *Components* tab. In the *Components->Excluded* pane, highlight *ftpd*, and then click the ">>" button. Notice that *ftpd* now appears in the *Components->Included* window. Use the same procedure to add *httpd*, *telnetd*, and *pingd*. Click "OK". Now, only those components will show up in the logs throughout the rest of the Firewall Practical Exercises.



6. You should now be back at the **View Logs** tab.

Identify the log entries for the telnet and ping connections conducted earlier. Can you identify the IP addresses used in the connections? Can you determine the session duration of the telnet session?

7. On the subnet computer, type in "ftp 10.0.0.100" at a Command Prompt: (Login as "anonymous". Use any e-mail address for password). Run the **ls** command.

Watch the log entries on the firewall. What messages are posted in the logs related to this FTP action? _____

8. Still on the subnet computer, download a file from the FTP server by executing "get SalaryReview.pps" and pressing ENTER.

9. Can you identify the downloaded file in the firewall's log file?

10. What port does the FTP connection use going through the firewall and what port does it use to connect to the FTP server? Are these the same ports used on every connection?

11. From the subnet computer, connect to a few websites. See if the firewall administrator can track through the logs and discover your misuse of government resources.

END OF PE

P.E. – Firewall 5: Monitoring Active Connections

1. On the firewall computer, select the *Active Connections* tab and monitor the Subnet computers behavior.
2. From the subnet computer, ftp to 10.0.0.100. Log on as “anonymous” using any email address as the password.
3. On the firewall computer, select the FTP session in *Active Connections*. Click on the *Kill Connection* button.
4. On the subnet computer, execute the “ls” command. (You may have to execute this command a couple of times to insure that it shows up in the active session list.) Is the FTP session still active?

What message did you receive? _____

5. On the firewall computer, wait for the ftp connection to time out of *Active Connections*. Examine the log file. What message was entered into the log because the ftp connection was terminated at the firewall?

6. On the subnet computer, reestablish the ftp connection to 10.0.0.100.
7. On the firewall computer, look at the *Active Connections* window. Did the firewall prevent the user from re-connecting? Why or why not? (Notice the rule associated with this connection.)

8. On the firewall computer, be prepared to kill the subnet computer’s connection to www.foxnews.com as soon as it appears in the *Active Connections* window. Click on the *Automatic Refresh* icon on the toolbar:



9. From the subnet computer, connect to “www.foxnews.com”.
10. On the firewall computer, as soon as the http traffic pops up in the *Active Connections* window, kill the connection.
11. Did the page fail to load on the subnet computer? _____

END OF PE

P.E. – Firewall 6: HTTP & FTP Control

1. From the subnet computer, connect to `http://10.0.0.100`. What site are you visiting? (Look closely.)

2. On the firewall computer, go to the *Monitoring* folder and select the *View Logs* tab. What does the log file tell you?

3. On the subnet computer, in the web browser *Location* field, enter "`ftp://10.0.0.100`".

4. What response did you get? Were you successful in reaching the FTP server via the web browser? (If you do successfully reach it, do NOT download anything). _____

5. On the subnet computer, return to "`http://10.0.0.100`".

6. On the firewall computer, select the *Policy* folder; choose the *Service Groups* tab; click on *Outbound Service Group*; click *Properties* and select the *Protocols* tab. Remove the HTTP protocol from the *Included Protocols* window. (This should stop all HTTP traffic).

7. On the firewall computer, what should be your next step? _____

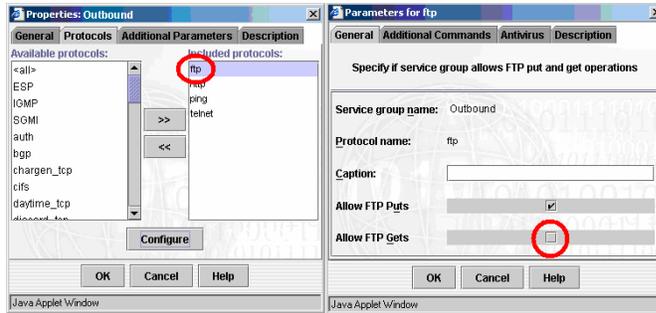
Do it.

8. On the subnet computer, refresh the browser session (clear the cache). Attempt to reconnect to "`http://10.0.0.100`". What happens?

Did you get an error message as expected? _____

9. On the firewall computer, add the HTTP protocol back into the *Outbound Service Group*.

10. Click on "FTP"; click the "Configure" button; remove the checkmark for *Allow FTP Gets*. (See screen shots below) Click OK twice & make sure to *Apply* and *Activate Changes*.



11. On the subnet computer, at the command prompt, execute "ftp 10.0.0.100". Log in as "anonymous" and use any email address as the password.

12. At the *ftp>* prompt, execute "get fw.ppt".

13. Was the command in step 12 successful? _____

14. On the firewall computer, what does the log file tell you about this activity?

END OF PE

P.E. – Firewall 7: Rules

1. On the firewall computer, select the *Location Settings* folder and click on the *Network Entities* tab.
2. On the firewall computer, create a new host network entity to block access to Yahoo Mail:
 - Click *New Network Entity*
 - Click *Host Network Entity*
 - Click *Properties*
 - Entity Name: Yahoo.Mail.Blocker
 - IP Address: mail.yahoo.com
 - Click "OK"
3. Still on the firewall computer, create a new host network entity to block access to "cnn.com".
 - Click *New Network Entity*
 - Click *Properties*
 - Entity Name: CNN.Blocker
 - IP Address: www.cnn.com
 - Click "OK"
4. On the firewall computer, create new rules that will deny the subnet computer (source) access to Yahoo Mail and CNN (destined for) while permitting access to all other web sites. Create the rules similar to the way you did before, but this time click on "Deny" rather than "Allow". Make sure to *Apply* and *Activate Changes*.
5. On the subnet computer, try to surf to "mail.yahoo.com" and "www.cnn.com".
Did the new rules work properly? _____
6. Now try "www.yahoo.com" and "www.cnn.com/TECH". How did the rules work
this time? _____

Remove ALL rules and apply and activate your changes.

END OF PE

P.E. – RealSecure 1: Initialization

1. Check the status of the RealSecure application:

Start ⇒ Control Panel ⇒ Administrative Tools ⇒ Services

Is the RealSecure daemon (issDaemon) on? _____ If not, start it.
(HINT: Right click issdaemon => select "Start")

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 ⇒ All Files and Folders*

Search for a file named "iss.key" (There may be more than one, but they are identical).

Open up the file using Notepad.

(HINT: Right click on the file => select "Open" => click on "Select the program from a list" => Select "Notepad" from the list.)

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:

(1.0.0.0 to 254.255.255.255 is example range.
Your IDS will display your network address range.)

END OF PE

P.E. – RealSecure 2: Setup of the IDS Device

- The console is your configuration tool
- The sensor runs in the background.
- Several sensors can be monitored per console

1. Start the RealSecure application (console):

Start ⇒ All Programs ⇒ ISS ⇒ RealSecure Workgroup Manager

2. The RealSecure console screen will appear:

Click on *View ⇒ Options*

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

Click on *View ⇒ Display License Key*

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

(HINT: Should be the same information from PE#1)

3. Start your detectors:

In the Managed Assets window, click on *Assets ⇒ Manage* option on the pull-down menu.

Expand the tree, highlight *Network_Sensor_1* and click on the "OK" button.

If the daemon is not reached, your key is invalid or your RealSecure daemon is not running. ** Notify the 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? _____

END OF PE

P.E. – RealSecure 3: Port Scans

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

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. Right-Click on *Event Name*, then *Inspect Event*.

What *Alert Priority* was it? _____ Is this appropriate? _____

3. The instructor will conduct either a Back Orifice or Smurf attack against a target in the classroom. Did you pick up this attack? _____

What kind of event was this attack? _____

What priority was it? _____ Is this appropriate? _____

END OF PE

P.E. – RealSecure 4: Web Watcher Template

1. Go to the Managed Assets window and right click on *Network Sensor*.
2. Select *Policies*.
3. Highlight *Web Watcher* and click on the *Apply to Sensor* button.
4. Click "Ok" on the message box.
5. Highlight *Web Watcher* and click on the view.
6. Expand the Security Events tree. You will have two options: Attacks & Audits.
7. Expand the Audit tree and highlight *HTTP*. List the following events:

Event	Priority	Description
HTTP_Java		
HTTP_Shockwave		
HTTP_Kazaa		
HTTP_ActiveX		
HTTP_Put		

8. The instructor will repeat the two attacks "Back Orifice" and "Smurf attack" against a target in the classroom. Did you pick up these attacks? _____

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

END OF PE

P.E. – RealSecure 5: Capture Authentication Traffic

1. Set your IDS policy back to "Maximum Coverage".

(HINT: Highlight "Maximum Coverage", then click "Apply to Sensor")

2. From the command prompt FTP into the instructor computer (10.0.0.100).

User: anonymous
Password: password

After completing the anonymous logon, exit the session.

3. Now, highlight the FTP_PASS event.

What kind of event ("What's this?") is FTP_PASS?

4. Highlight the FTP_PASS event again.

What kind of info ("inspect event") do you get here?

5. What is the alert priority?

6. What is the alert type?

7. Can you see the username and password for the FTP_PASS event?

8. What was the response taken?

END OF PE

P.E. – RealSecure 6: RealSecure Reports

On the RealSecure Console, click on *View* ⇒ *Reports* on the main pull-down menu. If prompted to *SYNCHRONIZE LOGS*, click on *File* ⇒ *Synchronize All Logs*. Then try again.

1. What were the top 5 events?

2. What were the top 5 destinations?

3. What were the top 5 source locations?

4. Enter the number of events the software has detected by priority:

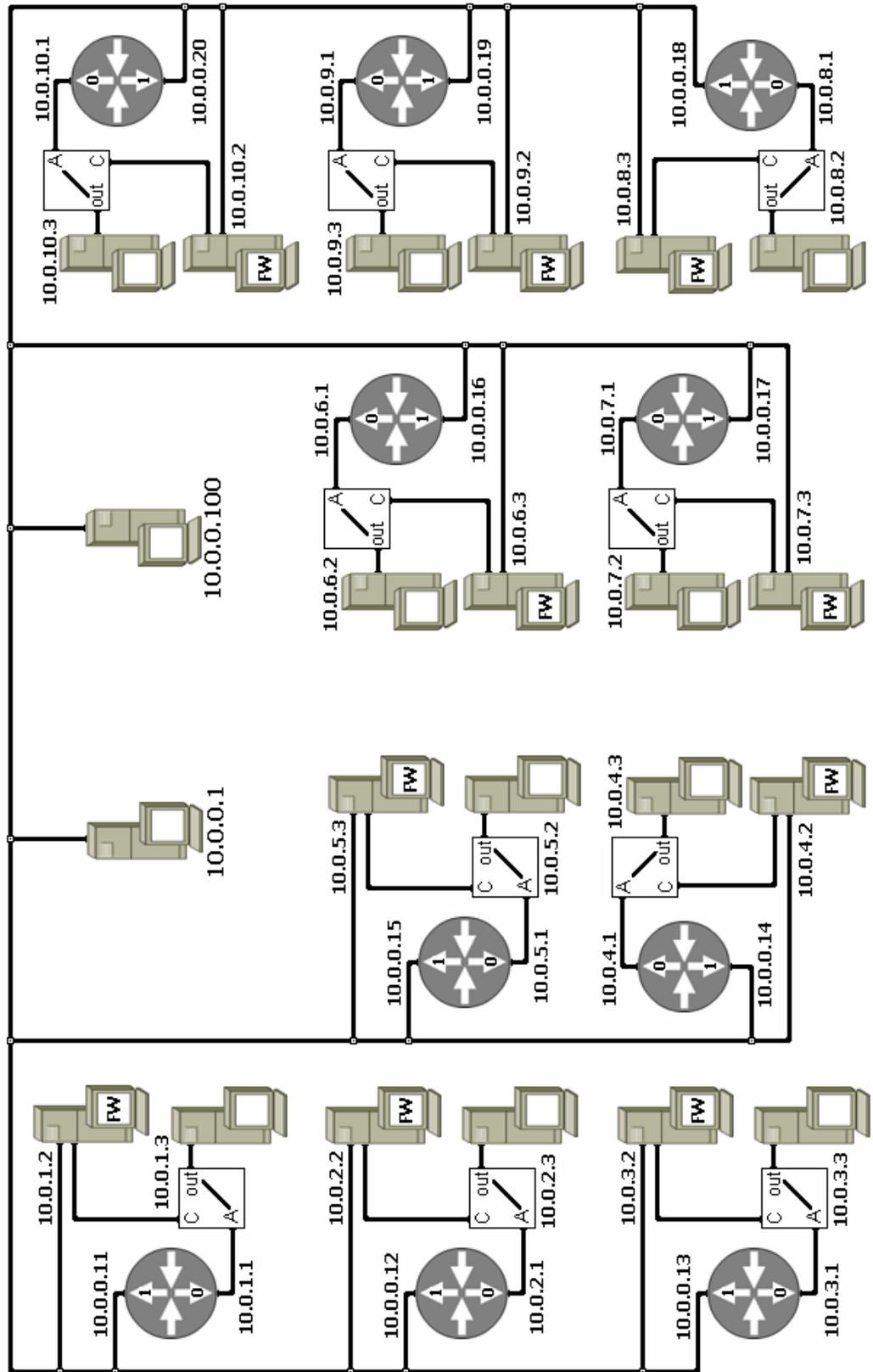
High: _____

Medium: _____

Low: _____

END OF PE

Classroom Network Diagram



Classroom Firewall Diagram

