

0 1 1 0 0 1 0 1 0 1 1 0 1 0 0 1
National Computer Forensics Institute
1 1 0 0 0 0 1 0 1 1 1 0 0 1 1 0
0 1 1 0 1 1 0 1 1 0 0 0 0 1 0 1
0 0 1 0 1 0 1 1 0 0 1 1 0 1 1
NITRO
1 1 1 1 0 1 1 1 1 1 1 1 0 1 1 1
1 0 1 0 1 1 1 0 1 0 1 0 1 1 1 0
1 0 0 1 1 1 0 0 1 1 0 1 1 1 0 1
0 0 1 1 0 0 1 1 1 0 1 1 0 0 1 0
0 1 1 0 1 0 0 0 0 1 1 1 1 1 0 0
1 1 0 1 1 0 0 0 1 1 0 0 1 0 0 0
1 0 1 1 1 0 0 1 1 0 1 0 1 0 0 1
Network Intrusion
0 1 1 0 1 0 1 0 1 1 0 1 0 1 1
Responder Program
0 0 1 0 1 1 0 0 0 1 1 0 1 1 1 0
0 0 0 0 1 1 0 0 0 1 1 0 1 1 1 0
0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
Volume 1 of 2
1 0 1 0 0 0 1 1 0 0 1 0 1 1 1 0
0 1 1 0 1 1 0 0 0 1 1 0 0 0 0 1

Course Introduction

Classification	<i>Information contained in this instruction is UNCLASSIFIED. However, certain methodologies are Law Enforcement Sensitive.</i>
Introduction	NITRO is a three-week course consisting of 14 days of lessons, incremental practical exams and a final practical exam.
Objective of this Course	NITRO is designed to introduce the officer to basic network intrusion investigation techniques.
Learning Outcomes	After completing this course the trained officer should be able to successfully conduct a network intrusion investigation.
Course Protocols	<p>Information contained in each section of this student book is presented in sequential order so that knowledge gained from later lessons is built on a foundation of what was learned earlier. Other course protocols include the following:</p> <ul style="list-style-type: none">• Practical exercises – Instructors will provide directives and handouts for practical exercises completed in the lab.• Appendices – Include course related materials provided by the instructors.
Practical Exercises	<p>Practical exercises in NITRO are hands-on. Each exercise is instructor-directed. In the exercises, students will:</p> <ul style="list-style-type: none">• Perform network wiring and connecting activities• Conduct manual log analysis• Use automated log analysis tools• Perform “Live” network gathering and analysis activities <p>In addition, every morning the students will have an opportunity to ask questions and/or review materials discussed on the previous day. This allows instruction to remain fresh and aids students with building practical connections to the training.</p>

This page intentionally left Blank

Network Intrusion Responder Program (NITRO)

NITRO Book I

- Windows Operating System
- Introduction to Networks
- Network Connectivity and Protocols
- IP Addresses and Subnets
- Common Network Crimes
- Phases of an Intrusion

NITRO Book II

- Report Writing
- Legal Issues
- Fundamentals of Log Analysis
- Log Sources
- Log Analysis
- LiveWire Investigations
- Appendices

This page intentionally left blank.

Network Intrusion Responder Program (NITRO)

Table of Contents – Book I

Topic	Page
Module 1 – Windows Operating System	1-1
Lesson 1 – Windows Operating System Basics	1-3
File Systems	1-4
Operating System Installation.....	1-8
Operating System Updates.....	1-11
Module 2 – Introduction to Networks	2-1
Lesson 1 – Networks Basics.....	2-3
Introduction to Networks	2-4
Network Types.....	2-6
Network Categories	2-9
Lesson 2 – Network Technologies	2-11
Introducing Network Technologies	2-12
Lesson 3 – Network Topologies.....	2-15
Topologies Defined.....	2-16
Lesson 4 – Network Architecture.....	2-25
Introduction to Network Architecture.....	2-26
Ethernet	2-27
Token Ring.....	2-29
Fiber Distributed Data Interface (FDDI)	2-30
Asynchronous Transfer Mode (ATM)	2-31
Broadband	2-32
Lesson 5 – The OSI Model.....	2-35
OSI Model Overview	2-36
OSI Model Layers.....	2-39

Topic	Page
Module 3 – Network Connectivity and Protocols	3-1
Lesson 1 – Network Connectivity	3-3
Network Connectivity	3-4
Network Transmission Media.....	3-5
Network Devices.....	3-10
Wireless Media	3-18
Lesson 2 – Network Configuration Models	3-23
Introduction to Network Models.....	3-24
Lesson 3 – Network Protocols.....	3-27
Protocols	3-28
TCP/IP.....	3-29
Other Protocols	3-31
Lesson 4 – Wireless Networks	3-35
About Wireless Networks	3-36
Types of Wireless Networks.....	3-37
Hardware Components.....	3-38
Security Concerns	3-40
Vulnerabilities.....	3-45
Module 7 – IP Addresses and Subnets	4-1
Lesson 1 – IP Addresses.....	4-3
IP Address Basics	4-4
IP Address Classes.....	4-6
More about IP Addresses	4-9
Lesson 2 – Ports	4-13
Overview of Ports	4-14
How Ports are Used	4-16
Configuring TCP/IP	4-19
Lesson 3 – Subnets.....	4-21
Subnet Overview.....	4-22
Subnet Masks	4-24

Topic	Page
Virtual LAN	4-25
Lesson 4 – Network Security	4-27
Data Encryption	4-28
Anti-Virus Software	4-29
Firewalls.....	4-30
IDS	4-37
Logs.....	4-39
Network Security Summary.....	4-41
Module 5 – Common Network Crimes	5-1
Lesson 1 – E-mail Scams	5-3
Overview of E-mail Scams	5-4
Attack Methodologies	5-5
Investigative Response.....	5-7
Lesson 2 – Online Fraud	5-9
Online Fraud Overview.....	5-10
Attack Methodologies.....	5-11
Investigative Responses	5-13
Lesson 3 – Identity Theft.....	5-15
Identity Theft	5-16
Investigative Responses.....	5-18
Lesson 4 – Social Threats.....	5-19
Social Threats.....	5-20
Attack Methodologies	5-21
Investigative Responses	5-22
Lesson 5 – Internal Threats	5-23
Internal Threats Overview	5-24
Investigative Responses	5-26
Lesson 6 – Malicious Code	5-27
Malicious Code Attacks.....	5-28
Investigative Responses	5-29

Topic	Page
Lesson 7 – Denial of Service Attacks	5-31
Denial of Service.....	5-32
Investigative Responses	5-33
Lesson 8 – Extortion.....	5-35
Extortion on the Internet	5-36
Investigative Responses	5-38
Lesson 9 – Network Attacks	5-39
Network vs. System Level Attacks	5-40
Investigative Responses	5-41
Lesson 10 – Terrorism.....	5-43
Extortion on the Internet	5-44
Investigative Responses	5-45
Module 6 – Phases of an Intrusion	6-1
Lesson 1 – Defining an Intrusion	6-3
Definition of an Intrusion.....	6-4
Goals of an Intrusion.....	6-5
Attacker Profiles	6-6
Phases of an Intrusion	6-9
Lesson 2 – Reconnaissance	6-11
Goals	6-12
Strategies.....	6-13
Techniques – General Web Browsing and Searching.....	6-14
Techniques – Public Records and Archives Search.....	6-15
Techniques – Target Web Site Examination	6-18
Techniques – Identifying Physical Attack Vectors.....	6-20
Techniques – Live Host Identification.....	6-22
Techniques – Identifying Available Protocols/Ports	6-23
Techniques – Type and Version Identification	6-25
Techniques – Vulnerability Scans	6-26
Lesson 3 – Network Attacks	6-29

Topic	Page
Goals	6-30
Strategic Categories	6-31
Strategies – Authentication Attacks.....	6-32
Techniques – Factor Guessing/Cracking	6-33
Techniques – Credential Recover/Reset	6-37
Techniques – Credential Injection	6-39
Techniques – Credential Theft.....	6-40
Strategies – Unexpected Input	6-41
Techniques – Excessive Input.....	6-42
Techniques – Excessive Input / Buffer Overflows	6-43
Techniques – Unexpected Input Content / XSS Attacks	6-44
Lesson 4 – Entrenchment	6-45
Goals	6-46
Strategies.....	6-47
Techniques – Log Cleaning	6-48
Techniques – Automatic Execution	6-50
Techniques – Hooking	6-52
Techniques – File Type Manipulation	6-54
Techniques – Naming Conventions and Placement.....	6-55
Techniques – Remote Connectivity	6-58
Techniques – File System Date/Time Stamp Manipulation	6-62
Privilege Escalation	6-63
Lesson 5 – Infiltration and Extraction.....	6-67
Sniffers.....	6-68
Trust Relationships	6-69
Data Extraction	6-70

Module 1

Windows Operating System

Overview

Windows XP Professional is both a popular and widely used Operating System. This lesson explains how to select a file system and install an operating system. You will learn how to patch your Windows XP system with the latest critical updates after installation.

Purpose of this Module

You need to be familiar with the file systems used within Microsoft Windows Operating Systems, as well as how to install a Windows operating system and apply patches.

Objectives

After successfully completing this module, you will be able to:

- Explain the procedure for installing Windows XP Professional
- Compare and Contrast the FAT32 and NTFS File System
- Describe how to install updates on Windows XP

In this Module

The following table shows the contents of this module.

Topic	See Page
Lesson 1 – Windows Operating System Basics	1-3

This page intentionally left blank.

Lesson 1 – Windows Operating System Basics

Introduction This lesson provides an overview of File System / Operating System Basics including selecting a file system.

Purpose of this Lesson You will gain an understanding of how to install and patch a Windows based operating system.

Objectives After completing this lesson, you will be able to:

- Give a brief overview of file systems
- Explain how to install Windows XP Professional
- Identify how Updates are installed on Windows XP

In this Lesson The following table shows the contents of this lesson.

Topic	See Page
File Systems	1-4
Operating System Installation	1-8
Operating System Updates	1-11

File Systems

File System Characteristics

Before installing Windows onto your workstation, you need to take an accurate assessment of how the workstation will be used. This will allow you to make the best choices during installation to avoid trouble later.

Users installing Microsoft Windows NT-based operating systems (NT, 2000, XP, 2003, and Vista) have a choice between using FAT or NTFS file systems. Although Windows Vista does not allow the system partition to use a FAT file system, additional partitions can use the FAT16 and FAT32 file systems.

NTFS has several advantages over FAT file systems. NTFS provides security and better overall performance than FAT file system. NTFS also uses a journaling mechanism which logs disks transactions. In the case of a power failure, journaling file systems often do a better job at data recovery.

While FAT does not provide security, it is compatible with older Windows Operating systems such as Windows 95, Windows 98, and Windows ME. Most USB thumb drives and storage devices are released pre-formatted with the FAT file system. This allows operating systems such as Linux and Mac OS X to read and write to the device.

FAT File System Characteristics

Each partition or logical drive contains a File Allocation Table, or FAT. The FAT manages a list of where files exist on the particular drive. This list is constantly being updated with new information as files are saved, deleted, renamed or moved. It is critical that this list stay up to date and intact to allow the operating system to access files.

FAT16 used a 16-bit length number to identify the various clusters on a hard drive. This limited the addressable capacity of a hard drive to 65,526 clusters, or 2 Gigabytes of data. Those using FAT16 on drives that were larger than 2 GB were required to create multiple partitions on the drive – each smaller than 2 GB. For example, a 4 GB hard drive would have to be partitioned into two 2 GB volumes, each receiving its own unique drive letter.

FAT32 uses a 32-bit length number to identify all of the clusters on a hard drive. This increase allows the file system to address approximately 268,400,000 clusters, or approximately 2 terabytes.

File Systems, continued

NTFS

Windows 2000 and Windows XP can operate in a FAT32 or FAT16 environment, but most users opt for the default file system, NTFS (New Technology File System). NTFS is more stable than the FAT system and offers such benefits as file compression and data encryption; these options are not readily available on a FAT-based system. In addition, MS Windows 2000, Windows 2003, and Windows XP Professional support *dynamic volumes*, which allow partitions to be added or extended without resulting in data loss.

The Windows 2000/XP Disk Management tool allows you to add, delete or modify partitions. In addition, it can be used to display general volume information including: file system type, the amount of available space and the drives total capacity. It can also be used to convert a partition from FAT16/32 to NTFS. In addition, the command prompt can also be used to convert partitions up to the NTFS standard. The following command converts the FAT formatted D: to the NTFS standard:

```
convert <drive letter> /fs:ntfs
```

Note: FAT partitions can be converted to NTFS while preserving the data; however, NTFS partitions cannot be converted to either of the FAT file systems.

There are a number of ways that a partition can be formatted or reformatted to the NTFS file system. The Disk Management tool, described previously, can be used to format the partition. In addition, the partition can be formatted via My Computer. The new partition(s) display when the My Computer folder is opened. Right clicking on the partition will result in a context-sensitive menu with Format as an option. Lastly, the Format command can be executed via the command line. The command “format [drive letter] /fs:ntfs” will format an existing partition to the NTFS standard.

Note: The format command can also be used to prepare a partition with the FAT (/fs:FAT) and the FAT32 (/fs:FAT32) file systems.

File Systems, continued

NTFS File System Characteristics

NTFS uses the Master File Table (MFT) to track files and their associated locations on a particular volume. The MFT is similar to FAT in that it maps the location of directories and folders and is updated whenever a file is accessed, changed, deleted or added to the volume.

There are, however, significant differences. The File Allocation Table can be thought of as a static fixed-sized chart that cannot change in size. However, the MFT is much more dynamic than the FAT. The MFT is a relational database that can grow in size if necessary. The MFT is created when the drive (or volume) is formatted for the NTFS specifications.

Since the MFT has the capability of growing, a certain amount of contiguous space is reserved for MFT expansion. This area is sometimes called the “MFT Zone.” Initially, this zone is approximately 12 percent of the total volume capacity; however, the MFT can grow past that size if needed. Most NTFS volumes are no larger than 2 terabytes in size. However, the dynamic nature of the MFT allows an NTFS volume to reach 16 Exabyte’s, which is equivalent to approximately 16,000,000 terabytes in capacity!

File Systems, continued

File Systems for Operating Systems The following table describes the default type of file systems used by each operating system.

Operating System	Type of Primary File System	Characteristics of File System
DOS	FAT16	<ul style="list-style-type: none"> Limited to 2GB partitions
Windows for Workgroups	FAT16 w/ limited VFAT	<ul style="list-style-type: none"> 32-bit file access
Windows 95a	VFAT	<ul style="list-style-type: none"> 32-bit file access Supports long file names
Windows 95b (OSR2), Windows 98, Windows ME	FAT32	<ul style="list-style-type: none"> Supports larger disk capacity up to 2TB Uses smaller cluster sizes for more efficient storage Windows 2000 supports FAT32 with disk volumes up to 32GB
Windows NT	NTFS	<ul style="list-style-type: none"> Improved reliability, to avoid data loss and improve fault tolerance Security and Access Control to manage who can read or write data Supports long file names Supports larger sized partitions, up to 16 Exabytes
Windows 2000, XP	NTFS	<ul style="list-style-type: none"> Improved Security Internal Data Encryption Disk Quotas
Unix,	UFS, FFS	<ul style="list-style-type: none"> Among oldest file systems
Mac OS X	HFS+	<ul style="list-style-type: none"> Supports 16 terabyte file and volume size 2.1 billion files per folder
Linux (kernel versions prior to 2.4.16)	Ext2fs	<ul style="list-style-type: none"> Security and Access Control Supports partitions up to 4TB Supports long file names
Linux (kernel versions since 2.4.16)	Ext3fs	<ul style="list-style-type: none"> Faster than ext2fs Greater data control. Information will not be lost on unclean shutdowns
OS/2	HPFS	<ul style="list-style-type: none"> Less fragmentation of data

Operating System Installation

Relevance

You will install Microsoft XP Professional SP2 as a means to introduce you to a modern desktop operating system that you will use later in this course.

**Procedure:
Installing
Windows XP Pro
SP2**

Use this procedure to properly install Microsoft Windows XP Professional SP2 for use on machines that do not have an operating system pre-installed.

Step	Action
1	Turn on your desktop PC and insert the provided Windows XP SP2 CD. Allow the PC to boot from the CD-ROM. When prompted, press any (space bar is fine) key to begin installation from the CD.
2	The CD will begin copying files to the hard drive. This process can take about five minutes to complete. Afterwards, a menu displays.
3	The Windows XP Professional Setup screen will appear. Press Enter to proceed to the End User Licensing Agreement.
4	Read over the License Agreement carefully. Press F8 if you agree to the terms of the License. If XP was pre-installed, the install will detect the existing installation and display a menu asking to overwrite it.
5	Press the ESC key to continue installing Windows XP. The partitioning screen will display.
6	Highlight the <i>Partition1</i> on disk0, id0 (the partition where you want to load XP) and press D for delete. Press Enter, and then press L to delete the partition.
7	Press C to create a new partition. Use the default size value to make a partition to use up the entire hard drive.
8	Highlight Partition1 and press Enter to format it. Format the partition using NTFS. The computer will reboot. Allow it to boot from the hard drive instead of the CD. Hint: Do not press a key when prompted to 'press any key' The Regional and Language Options screen will soon display.

Operating System Installation, continued

Procedure: Installing MS Windows XP Pro SP2, continued

Step	Action
9	Click Next to proceed to the Personalize Your Software screen.
10	When requested, type in your name, or organization assigned user name. Click Next to proceed to the End User Licensing Agreement screen.
9	Type in the Windows XP license key as it is noted on the supplied Windows XP Installation CD. Click Next to proceed to the Computer Name and Administration Password screen.
10	When requested for a Computer Name field, type in a unique value that doesn't exist anywhere else on your network. Refer to your instructor or network administrator for an appropriate value. For the administrator password, type in a unique password that is not easily guessed or determined. In the classroom, refer to your instructor for an appropriate password. Type password again to confirm it. Click Next to proceed to the Date and Time Setup screen.
11	Change the time zone to CST -06:00, Central Standard Time Zone and click Next to continue the installation. This setting can be changed at any time in the future to your local time zone. After copying files, the Networking Settings screen displays.
12	If connecting this computer into your organization's network, refer to your local administrator for appropriate network information to use in the next few steps. This procedure will assume you're in a classroom network. Click on Typical Settings and click Next for the Workgroup or Computer Domain screen.

Operating System Installation, continued

Procedure: Installing MS Windows XP Pro SP2, continued

Step	Action
13	Click No . For the workgroup, type: WORKGROUP Click Next to continue the installation. After copying files, the machine should reboot. Afterwards, the install will proceed to the “Welcome to Microsoft Windows” screen. Click Next .
14	On the “Help Protect Your PC” screen, choose the green shield for help protect my PC, and then click Next .
15	The system will check for Internet connectivity. The following screen will ask “Will this computer connect to the Internet directly, or through a network?” Choose “Yes, this computer will connect through a local area network or home network.”
16	Click Next to proceed to the “Ready to register with Microsoft?” screen.
17	At the “Ready to register with Microsoft?” screen, select “No, not at this time.” Click Next to proceed to the “Who will use this computer?” screen.
18	Type your name in the Your Name field and click Next to proceed to the “Thank You!” screen.
19	Click Finish to have Windows restart and bring up the desktop.

Operating System Updates

Patching

After installing an Operating System, it should be patched with the latest critical updates. Installing updates on a regular basis is vital as new threats and vulnerabilities are always being developed. Users who utilize the Windows Update site can choose to use Express or Custom settings.

Express Settings will install all high priority updates without allowing the user to decide which updates will be installed. Custom settings will allow the user to choose which updates their operating system will receive.

Alternatively, you could wait until Windows performs its automatic update function. This is set to occur during the middle of the night, on every night.

The Danger of Automatic Patching

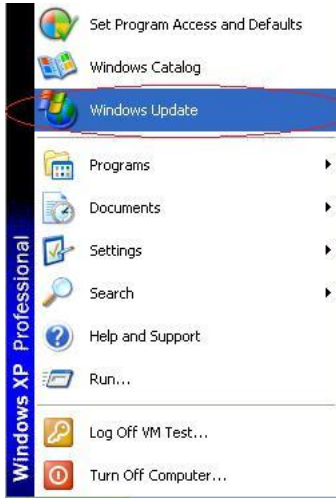


By default, Windows XP will automatically download and install new patches on a weekly basis. While this is a great setting for maintaining the security of a computer, there is also a negative drawback to it. If a critical update is released, your computer will automatically install it and reboot, closing all open applications in the process. Any open documents and case work will be closed, with the potential for the loss of hours, or even days of work. Even worse, this update occurs, by default, at 0300 hours at night. You could set up a forensic workstation to begin a 12-hour text search, only to come in the next morning to see a blank desktop screen.

To disable this setting, select Start > Control Panel > System Properties. Locate and select the tab for "Automatic Updates" to view the patching options. The recommended value for a workstation is "Download updates for me, but let me choose when to install them." With this option set, you will notice an update icon in your system tray notifying you that new updates have been downloaded. You can then choose a safe time to apply the updates, without worrying about the loss of work.

Operating System Updates, continued


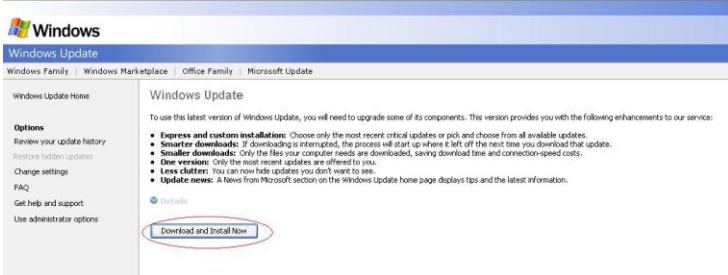
Procedure:
Updating an
Operating System

The following procedure will walk you through manually updating your Windows XP system using Microsoft's online Windows Update Web site.

Step	Action
1	<p>Click on the Start Button, and choose Windows Update, as seen below:</p> 
2	<p>The system will check for Internet connectivity. Right click on the ActiveX Warning and select "Install ActiveX Control..." as seen below.</p>  <p>Click Install at the Internet Explorer Warning.</p>
3	<p>Click Install Now at get the latest Windows Update Software screen.</p> 

Operating System Updates, continued

Procedure: Updating an Operating System, continued

Step	Action
4	<p>At the Express or Custom Screen, select Express.</p> 
5	<p>At the Next screen, click Download and Install Updates Now, as seen below.</p> 
6	<p>Click Restart Now after the installation is complete. At this point, you have not installed any updates, just the Windows Installer. This application is required to install the rest of Microsoft's updates.</p>
7	<p>Go back to the Windows Update Site to get updates, by clicking on the Start Button and selecting Windows Update.</p>
8	<p>Click Express.</p>
9	<p>Click Install Now. Read over the License Agreement and click I agree if you agree to it.</p>

This page intentionally left blank.

Module 3

Network Connectivity and Protocols

- Overview** Previously you learned about the different types of networks as well as the OSI model that supports data transport between two end systems. This module introduces the various network topologies and explains how networks interconnect.
- Purpose of this Module** Networks come in many configurations or topologies. You need to be able to recognize common network topologies and understand how they function.
- Objectives** After successfully completing this module, you will be able to:
- Identify network connection configurations
 - Name network connection devices and their functions
 - Recognize connection hardware and describe their characteristics
 - Describe different network topologies
- In this Module** The following table shows the contents of this module.

Topic	See Page
Lesson 1 – Network Connectivity	3-3
Lesson 2 – Network Configuration Models	3-23
Lesson 3 – Network Protocols	3-27
Lesson 4 – Wireless Networks	3-35

This page intentionally left blank.

Lesson 1 – Network Connectivity

Introduction This lesson identifies the various physical components used to connect computers and devices within a network environment.

Purpose of this Lesson You will learn how computers and stand-alone devices interconnect to form a network. You will also discover how to connect clients and servers on a LAN to other networks. An introduction to wireless networks is also included.

Objectives After successfully completing this lesson, you will be able to:

- Name the various types of transmission cabling used to wire a network
- Identify network interface cards and adapters
- Explain how modems work to provide remote access
- Identify the various types of wireless media

In this Lesson The following table shows the contents of this lesson.

Topic	See Page
Network Connectivity	3-4
Network Transmission Media	3-5
Network Devices	3-10
Wireless Media	3-18

Network Connectivity

Building Network Connections

A network connects stand-alone computers, workstations, printers, and other shared resources using many different types of connection devices. For example, you need at least the following components to build a LAN:

- Network interface cards (NIC) for each computer
- Transmission media including cabling and connectors

In order to connect locally to the Internet, the world's largest network, you would need:

- Modem connected to an Internet Service Provider's modem
- Or a NIC connected to a DSL or cable modem
- Or a USB cable modem.
- Or a NIC connected to an Optical Network Terminal (ONT)
- Phone wire or UTP cabling as appropriate

Network Devices

To connect one network to other networks, you need some combination of the following devices, which are described in detail later in this lesson:

- Routers to provide transmission pathways between two or more networks
- Hubs to establish a central connection point for several network devices on the same network
- Repeaters to ensure integrity of signals over long distances
- Switches to direct traffic through the network more efficiently than with traditional hubs
- Multi access units/multi-station access units (MAUs/MSAUs) to set up token ring in a star-wired ring topology
- Bridges to connect two separate segments of a network

The following sections describe numerous network components and in which topologies and architectures you are likely to find them being used.

Network Transmission Media

Types of Network Transmission Media

Network data transmission is classified two ways: cable and wireless.

- With cable, communication travels via electric currents or light pulses (for fiber optics) through different types of cabling.
- Wireless connections use radio waves, microwaves, and light spectrum energy to transmit data.

Bandwidth

A discussion of network transmission would not be complete without a description of bandwidth. The capacity of transmission media is measured in bandwidth. *Bandwidth* is the amount of data a communication channel can handle.

The bandwidth of a channel, often referred to as its capacity, is denoted differently for analog transmissions (phone, radio, and television communications) and digital transmissions. Analog transmissions are measured in cycles per second called hertz (Hz). Digital transmissions are measured bits per second (bps) and the capacity is called the data transfer rate.

Cabling

Most networks use cabling to connect devices. There are three main types of cabling used on most networks:

1. Twisted-pair
2. Coaxial
3. Fiber optic

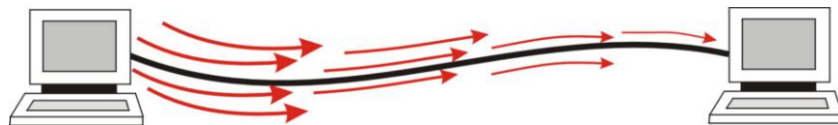
Network Transmission Media, continued

Attenuation

Before addressing the types of transmission media, it is important to understand a key point in the limitations of any media.

Signals carried over cabling are susceptible to attenuation. *Attenuation* is the weakening of signals as they travel away from their source. This is why there are specific limits to cable distances. The signal can only travel a limited distance before becoming indecipherable.

Attenuation



Twisted-pair Cabling

Twisted-pair cabling is inexpensive and used extensively with LANs and telephone connections. The cable consists of individually insulated metal wires that are twisted together and placed in a plastic encasement. The wires are twisted to prevent crosstalk, which is noise interference from other wires within the same cable. The twists also help prevent electromagnetic interference, or EMI, from nearby electrical or magnetic fields.

There are two types: unshielded twisted-pair (UTP) and shielded twisted-pair (STP). The shielded cable has an additional internal shield covering the wires that protects against electromagnetic interference (EMI). Electromagnetic waves can also be intercepted allowing for eavesdropping on signals.

Neither STP nor UTP offer the greater distances or more reliable interference protection of coaxial or fiber optic cables.

Twisted pair cables can be used in any topology, including bus and ring.

Network Transmission Media, continued

Categories of Twisted-pair Cable

There are several categories of twisted-pair cable. They reduce crosstalk and EMI, but suffer from rapid attenuation and are susceptible to eavesdropping. As a result of attenuation, all unshielded twisted pair cables have a maximum effective distance of 100 meters.

- Cat 3 twisted-pair cable is an older type and supports speeds up to 10 Mbps. Commonly used in 10baseT Ethernet networks
- Cat 5 twisted-pair cable supports speeds up to 100 Mbps. Commonly used in 100baseX Fast Ethernet networks.
- Cat 5e twisted-pair cable supports speeds up to 1 Gbps. Commonly used in 1000baseX Gigabit Ethernet networks.
- Cat 6 twisted-pair cable supports speeds up to 1 Gbps. Commonly used in 1000baseX Gigabit Ethernet networks.

Connectors

An RJ-45 connector is used on the ends of twisted pair cabling to connect components in an Ethernet network. It has an eight-wire modular plug that is similar in appearance to the RJ-11 and RJ-12 (standard phone wire) connectors.

Network Transmission Media, continued

Coaxial Cable

Coaxial cable offers greater protection against EMI than twist-pair cabling. Coaxial design has a copper core surrounded by insulation and then a braided metal shield. A plastic or rubber encasement comprises the outside layer.

Coaxial cabling is widely used for cable television and computer networks. The two types used for networks are:

- Thinnet coaxial cable: Used with 10base2 Ethernet
- Thicknet coaxial cable: Used in 10base5 Ethernet

Other characteristics include the following:

- To build a token ring network or bus Ethernet, thinnet is used to connect one device using a T-connector
- Cable must be grounded and terminated
- Peak transfer rate is 16 Mbps
- Effective range is approximately 185 meters for thinnet and 500 meters for thicknet
- Suffers from high attenuation

Coaxial cables can be used in any topology including bus and ring.

Connectors

The BNC connector is the acronym for British Naval Connector, Bayonet Neill Canceilman, or Bayonet Nut Connector. This type of connector is used to secure Thinnet coaxial cable and is found in 10Base2 Ethernet systems.

A BNC connector has a male-type plug found at each end of the cable. The BNC connector has a center pin connected to the center cable conductor and a metal sheath connected to the exterior cable shield. A rotating ring is then used to secure the connection. BNCs come in T-connectors, barrel connectors, and terminators.

Network Transmission Media, continued

Fiber Optic Cable Fiber optic cable uses glass or plastic fibers to transmit data modulated onto light waves. Each cable contains two strands in separate jackets. Fibers can be either single-mode allowing only one transmitted signal, or multi-mode allowing multiple transmitted signals simultaneously. The diameter of the optic core of a multi-mode fiber is visibly larger than that of a single mode fiber. Another notable difference between single-mode and multi-mode fiber is the distance they can carry a signal. A single-mode fiber, driven by laser light can carry a signal approximately forty-three miles without regeneration. The multi-mode fiber is limited to approximately one and a half miles.

Data does not have to be converted to analog before being transmitted. Instead, it is sent in its original digital format. Fiber optic cables offer greater bandwidth; therefore, can carry more data than metal cables. They are also less susceptible to signal interference making them a popular choice for LANs or transoceanic cabling.

Fiber optic cables are much thinner and lighter than wire cables, but also more fragile to handle and more difficult to cut. One main disadvantage of fiber optic cables is that they are expensive to install. Despite the increased cost, phone companies are replacing old lines with fiber optic cables and many think they will be the first choice for future communication cabling.

Connectors

Fiber optic cable uses several different types of connectors depending on the application. The one thing that they have in common is that the end of the fiber extends past the connector. The end can be damaged easily; therefore, you should always cap them when not in use.



Examples of ST (single twist) and SC (single click) fiber optic connectors

Network Devices

NICs

The NIC is an adapter in a computer that enables the computer to connect to a network. Each NIC is made for the network type it will support, such as Ethernet, Token Ring, FDDI, etc. Some cards are formatted as separate plug-ins to the MB while others are integrated into the MB. Most cards work with specific cable types.

MAC Address

NICs are manufactured with a hardwired code that is unique to each card. This code is called the *MAC address*. The first six hexadecimal characters of the address represent the manufacturer of the card, while the last six represent the serial number of the individual card. When the NIC is installed in a computer or other device, the MAC address is essentially the computer's physical address on a network. The MAC address is used to identify the right destination for transmitting data packets across a network.

Example: 3F-73-A4-48-D7-8F

Laptop and notebook computers can have a NIC built into the MB or use a NIC in the form of a PC card. A slot on the side of the laptop holds the PC card and provides high-speed access to the processor and memory.

There are several NICs for both Ethernet and Token Ring. NICs used for FDDI are called Dual Access Stations (DAS) as they connect the computer to each of two separate token rings.

How NICs Work

When a computer makes a request to communicate with the network, the OS sends the request to the NIC. The NIC converts the request into the proper type of data packets to be transmitted over the network. It then monitors network traffic flow and sends the packets at the appropriate time when there is an opening.

In addition to preparing and sending packets, the NIC also checks the MAC addresses of passing network transmissions. If they are addressed to the computer, the NIC then copies the packet for the computer. NICs decide whether to read incoming data packets based on the MAC address. (Data Link Layer 2)

Network Devices, continued

Modems

Modems handle communication that is transmitted over telephone lines between computer systems. Most modems have fax capabilities.

PCs are digital devices and the telephone system is analog. The modem is the component that converts or modulates the PC's digital code to analog so it can be sent over phone cables. Likewise when receiving information, the modem converts or demodulates analog signals to digital code before transmitting data to the PC. The transmission mode takes two separate forms:

- *Asynchronous Mode:* This mode of transmission sends data intermittently one character at a time. A start bit and a stop bit frame each character.
- *Synchronous Mode:* This mode of transmission relies on software to negotiate the protocol used. The blocks of data are much larger (128 up to 1024 bytes or more) than with asynchronous mode communications. The receiving modem must respond with either an acknowledgement (ACK) of receipt or a negative acknowledgement (NAK).

Modems do not decide whether or not to send the data packets. They simply make the conversion between analog and digital. (Physical Layer 1)

Network Devices, continued

Hubs

A *hub* contains ports where network computers and devices can connect with each other. A hub provides a central point of connection for all network nodes attached to it. The type of connector needed by each node depends on the network architecture and cabling used (i.e., Ethernet, Fast Ethernet, etc). Most hubs are small boxes with multiple ports; however, some hubs are cards that can plug into a server.

A hub is used to join several nodes together at a single site. Its main functions are to connect nodes, to organize cabling, and to transmit signals to anything that is attached to it, including other segments of the network. The types of hubs are:

1. *Passive Broadcast Hub*: Broadcasts data packets to every node on the hub. Performs no signal regeneration.
2. *Active Broadcast Hub*: Broadcasts data packets to every node on the hub. Enhances signal transmission by regenerating signals and filtering noise.

An intelligent hub is essentially an active hub that contains network management functions that are used to gather information on network traffic and error detection. Most intelligent hubs allow you to monitor individual ports and close a port if problems arise.

Hubs do not decide when or where to send data packets. They simply broadcast the data to all ports. (Physical Layer 1)

Token Ring MAU/MSAU

The Multi-Station Access Unit (MAU/MSAU) is a special device used to link nodes on token ring networks. The nodes are connected to the MAU and then data packets are routed in a ring within the MAU. Using this star-wired ring topology makes it very easy to add and remove nodes from the network.

MAUs or MSAUs decide where to send data packets and create a point-to-point connection based on the sending and receiving node's MAC addresses. (Data Link Layer 2)

Network Devices, continued

Repeater

Repeaters combat attenuation by boosting the signal during transmission.

To boost signals, analog repeaters amplify the signal and digital repeaters regenerate the signal. These devices can relay signals between networks that use different types of protocols or cabling.

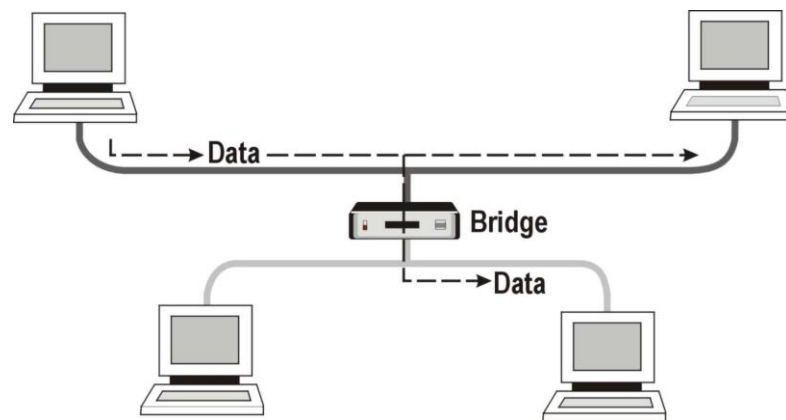
The difference between an active and a passive hub is that an active hub also functions as a repeater to regenerate or amplify the signal.

Repeaters do not decide when to send data. They simply receive data packets in one port, regenerate or amplify them, and send them back out the other port. (Physical Layer 1)

Bridge

A *bridge* is a unit that joins two separate segments of the same network. It also can be used to divide an overloaded network by creating separate broadcast (collision) domains. A bridge can also connect two networks that are dissimilar, such as connecting an Ethernet with a Token Ring network.

Bridge Example



A bridge decides whether data packets should be sent from one collision domain, across the bridge, into the second collision domain, based on the MAC address of the sending and receiving nodes. If the sending and receiving nodes are on the same segment, the bridge simply ignores, or drops the packets. (Data Link Layer 2)

Network Devices, continued

Switches

Switches are devices that meet the demand for faster connections and more bandwidth in networks. Although switches visibly resemble hubs, they also help increase the speed of the network by providing dedicated bandwidth to each port. In contrast, hubs share the bandwidth among all ports.

A switch functions like a cross between a bridge and a hub. Switches cut down on the amount of broadcast traffic on the network segment by switching network packets from the incoming port and sending them directly to the port for the receiving computer.

By decreasing the amount of broadcasts on the network, you also lower the number of collisions on the network segments, improving overall performance. Like intelligent hubs, switches can be managed, allowing individual port configuration and monitoring from across the network.

Switches direct data packets between ports based on sender and receiver MAC addresses. Switches have the ability to broadcast to all ports when necessary, but differ from hubs in that they can limit traffic to the sender and receiver ports without broadcasting.
(Data Link Layer 2)

Token Ring Switches are available that replace the MultiStation Access Units at speeds of 100/16/4 Mbps.

There are also Layer 3 switches that direct data based on *network addresses*, covered later in the Networking module.

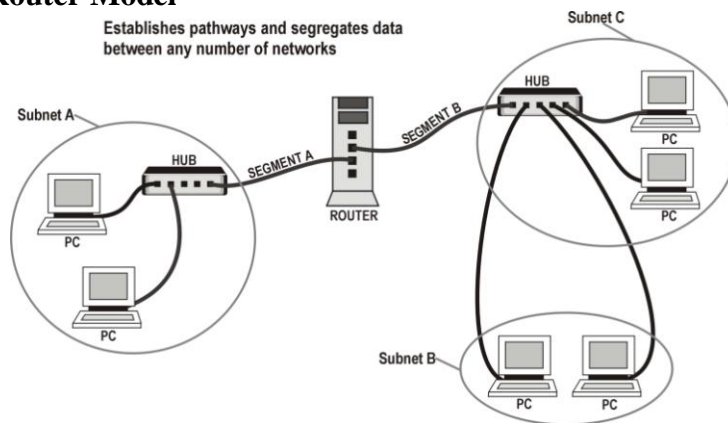
Network Devices, continued

Routers

Routers link separate networks or LAN segments and establish pathways for data packet transmissions. Each network has an IP network address. The router uses this address to transmit packets to the correct destination. Other characteristics include the following:

- Transmit data packets across different types of networks
- Fragment data packets to fit different frame sizes of various networks
- Can be configured to segregate secure data and prevent it from being sent to specified networks
- Collects and assembles information from remote routers about network routes. This information is used to identify reliable pathways.
- Does not broadcast data packets
- Routers read each data packet looking for the network address (IP address) to send to. Once it determines the best route to forward the packet, it replaces the sender's MAC address with its own.
- Each port on a router is in essence a separate NIC, with its own unique MAC address. Therefore, as packets move from one router to another, the MAC address changes from router to router. The original source and destination IP addresses will remain the same, regardless of how many routers a packet encounters.

Router Model



Network Devices, continued

Routing Activity

Routers on networks exchange information about paths to computers attached to them through a process known as *convergence*. This convergence information is stored in routing tables, which contain the network portion of the host computer's IP address.

Routing assumes that addresses convey at least partial information about where a host is located. This permits routers to forward packets without having to rely on a complete listing of all possible destinations.

Routing involves two basic activities:

- Path determination
- Switching

Path determination enables a routing protocol to determine the best direction to route a packet. It is complex because the determination will differ based on the routing protocol used.

Switching involves the router forwarding the packets independently through the network. The router forwards the packets based on the IP address. (Network Layer 3)

If the IP address is not in the router's routing table, the router will drop the packet.

Network Devices, continued

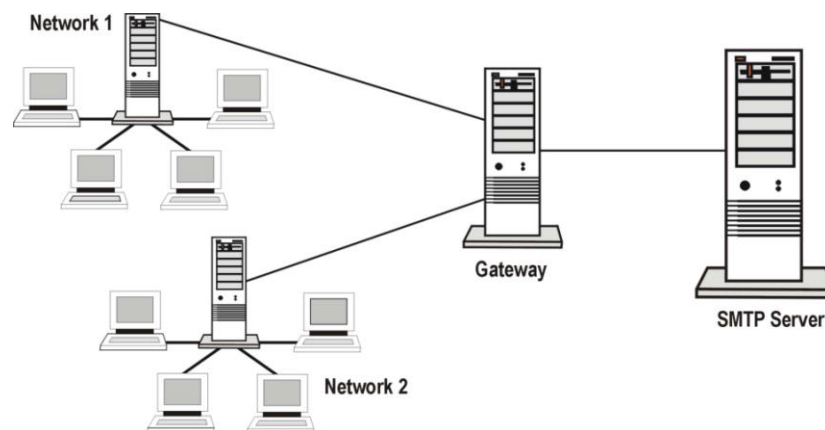
Gateway

A *gateway* is a server or software program that is the entrance to a network. For example, a gateway is used to route communications from a PC to a Web server outside the network.

A gateway can translate different protocols on a network thereby enhancing the traffic flow. Gateways can also serve as proxy servers and firewalls.

Gateways have the ability to look at data inside the packets and perform high-level decisions about that data, beyond simply looking at a MAC or network address. (OSI Layers 4 – 7)

Gateway Example



Network Device Summary

All of the above hardware can be implemented in Ethernet or token ring networks with the exception of hubs and MAUs. Hubs use broadcast technology and are only used in Ethernet, while MAUs use point-to-point and are only used in token ring. FDDI uses an FDDI concentrator, which is similar to a MAU.

Much of the hardware above is used to divide a network into manageable segments. The main difference between them is their basis for passing data on to other devices, or at which layer of the OSI model they function. For example, a hub automatically broadcasts all packets to all nodes, whereas a switch reads the packet header for a valid MAC address and only forwards data to the port associated with that address.

Wireless Media

Wireless Media Defined

Wireless technology offers data communications between two or more computers without the use of traditional network wire or cabling. Data is transmitted over frequencies in the air rather than through a cable. The IEEE 802.11 standard defines all aspects of radio frequency wireless networking.

The two types of wireless systems are the following:

1. Fixed wireless describes computing devices or networks that are in fixed locations, such as in a building, office, or home. These devices rely on electrical power.
2. Mobile wireless refers to portable computing devices, such as cell phones, PDAs, and wireless notebooks that use battery power and can transmit and receive from any location.

How Wireless Communication Works

Wireless Access Points (WAPs), or base stations, are the devices clients use to connect to a wireless network. Wireless devices transmit and receive signals without electrical or optical conductors. Wireless communication uses the Earth's atmosphere as the physical data path.

Wireless networking uses the technology in radio frequency (RF) transmissions to send network packets across airwaves. Typical indoor ranges are 150-300 feet and outdoor ranges are quoted up to 1,000 feet.

RF technology is used in both LANs and WANs. For transmission, laptop computers have transceivers in PC-card slots that first connect to a wireless access point (WAP) and then to the wired network. Desktop PCs use either an ISA/PCI wireless or USB transceiver. Data transfer speeds can be slower than wired connections.

Wireless Media, continued

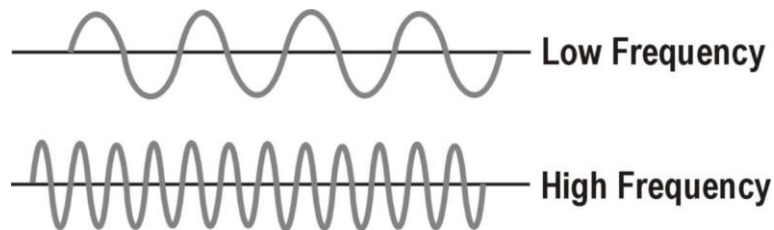
Wireless LAN

A wireless LAN, called a WLAN, transmits over the air and does not require arranging devices for line of sight transmission. In a WLAN, WAPs are connected to an Ethernet hub or server. These send radio frequency signals through walls over an area up to a thousand feet.

Desktop PCs send and receive transmissions via an ISA or PCI card. Laptops use PC cards or wireless modems that connect to an Ethernet port.

Wireless Signals

Wireless signals operate at a frequency rate that is gauged by the number of oscillations per time unit a signal makes. The faster the cycle rate the higher the frequency as shown in the following illustration. High frequency has more oscillations per second than low frequency.



Wireless signal frequencies are measured in hertz (Hz) and most current wireless communications involve megahertz (MHz) and gigahertz (GHz). These higher hertz rates mean greater bandwidth and more data capacity.

Types of Wireless Signals

Current wireless technology employs the following methods for transmitting signals:

- Radio frequency (RF) signals
- Microwaves
- Infrared signals

Wireless Media, continued

Radio Frequency The majority of wireless communication is transmitted over radio frequency. RF bands used widely today include:

- High Frequency (HF): 3 – 30 MHz
- Very High Frequency (VHF): 30 – 300 MHz
- Ultra High Frequency (UHF): 300 MHz – 3 GHz
- Super High Frequency (SHF): 3 GHz – 30 GHz

The types of devices that use RFs between 10KHz and 1GHz include short wave radio, VHF television, FM radio, and UHF radio and television.

Types of RFs Wireless communications rely on three types of RFs.

RF	Characteristics
Low Power, Single-Frequency	Used to carry signals short distances. This method is susceptible to massive attenuation and vulnerable to eavesdropping.
High-Power, Single-Frequency	Used over long distances. They can resist attenuation, but are vulnerable to eavesdropping.
Spread Spectrum	Uses multiple frequencies simultaneously and continuously to change signal patterns. This change of frequencies makes this method less susceptible to illegal monitoring. There are two types of spread spectrum RFs: <ul style="list-style-type: none">• Direct Sequence Modulation: Transmits encoded data and white noise across a subnet of radio frequencies. It is the most common RF used.• Frequency Hopping: Switches between pre-established frequencies several times per second.

Wireless Media, continued

Microwave Wireless Media

Microwaves are electromagnetic waves that use the same frequencies as RFs. There are two basic forms of microwave communication. Both are susceptible to weather conditions, jamming frequencies, eavesdropping, and latency.

- Terrestrial: Sends data over land such as for line-of-sight transmissions between buildings
- Satellite: Sends data across great distances via satellites

Infrared Wireless Media

Infrared transmissions use optical transceivers to communicate between transmitter and receiver. They operate using line-of-sight or reflection and require an unobstructed pathway between devices. The two categories of infrared media are as follows:

- Point-to-Point Infrared: Uses tightly focused beams directed at specific receiver (s) such as one computer transmitting to another within the same area.
- Broadcast Infrared: Signals are diffused over a wide area to a number of receivers such as data sent to several computers within a room. Data transfer is slow.

This page intentionally left blank.

Lesson 2 – Network Configuration Models

Introduction

The network configuration models presented in this lesson include client/server network, server/server network, peer-to-peer network, server-centric network, enterprise network, and remote access service (RAS) network.

Purpose of this Lesson

You will learn to recognize common network configurations. This information will be helpful for computer crime investigations involving networks.

Objectives

After successfully completing this lesson, you will be able to:

- Identify the six main network configurations
- Describe the key characteristics of each network configuration
- Explain how remote access service networks function

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Introduction to Network Models	3-24

Introduction to Network Models

Introduction

Network models are determined by the size and needs of the organizations they support. The following network models will be defined in this lesson:

- Peer-to-peer network
- Client/server network
- Server-centric network, which includes:
- Enterprise network
- Server/server network
- Remote access service (RAS) network

Peer-to-Peer Network Model

The *peer-to-peer network model* links computers and has them function as both workstations and as servers to share resources. Each PC can act as a server for other linked PCs. They can share drives, printers, and other common devices while running applications.

A peer-to-peer network is easy to set up and is often found in small offices. Limited user security can be configured to include password access. However, it is not ideal for a large network where a server-based network can provide more security.

Introduction to Network Models, continued

Client/Server Network Model

In a *client/server network*, individual workstations send requests to a central server and the server provides all resources. This separation of duties makes for a powerful system that offers the following:

- Fast processing time for running applications
- Increased disk space for sharing files
- Network security including mandatory user login to access network resources

This model has advantages over the peer-to-peer network. First, it provides a more organized system where files are easier to locate. Second, it has better security features because all user login files are stored in one location on the server.

As a network grows, the need for security increases. In the client/server model, every user has a user profile that includes a login name and password. These encrypted files are stored on the server and are accessed each time users log onto their workstations. User validation must occur before network access is granted.

Server-centric Network Model

In the *server-centric network*, each server has defined roles and offers access to specific shared resources. To handle requests from users on this network, each server requires user login authentication before processing the request.

Enterprise Network Model

An *enterprise network* connects all departmental and individual networks throughout an organization into one network. This configuration allows users to exchange and access files and resources across the organization.

It integrates all systems types. Therefore, Windows PCs, Apple Macintoshes, UNIX, and mainframes can be linked in an enterprise network. This interconnectivity is achieved with the Internet protocol TCP/IP and other Web technologies.

A designated server maintains system security. Users login once for access across the network.

Introduction to Network Models, continued

**Server/Server
Network Model**

In the *server/server network*, one server provides services to other servers in the network. The types of services provided include domain name service (DNS) address resolution and dynamic host configuration protocol (DHCP) IP address request and issue.

**Remote Access
Service**

Remote Access Service (RAS) enables users to access the network from any outside location by using a modem or an Internet connection.

Lesson 3 – Network Protocols

Introduction

Network protocols are guidelines that define how computers transmit and receive data. These rules for transmission follow the guidelines established by the OSI model. Protocols ensure that all devices attempting to communicate on a network are following the same rules. In this lesson, you will explore commonly used protocols.

Purpose of this Lesson

Gaining an understanding of the role of network protocols is essential to knowing how devices communicate across networks.

Objectives

After successfully completing this lesson, you will be able to:

- Define network protocol
- Describe the characteristics of TCP/IP, IPX/SPX, NetBEUI, PPP, and PPTP

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Protocols	3-28
TCP/IP	3-29
Other Protocols	3-32

Protocols

Introduction

Protocols define the rules for transmitting data between computers or other devices. Protocols determine the size of the data packets, what type of information is included in each packet, and what actions take place if the communication does not reach its destination. Protocol guidelines:

- Provide data compression, when necessary
- Determine the process to begin and to end a communication
- Govern message routes and data speeds
- Provide error checking procedures to ensure error-free message delivery
- Offer translation services for different types of computers and networks

Protocols vary depending on the network's environment. Those explained in this lesson include:

- TCP/IP
- IPX/SPX
- NetBEUI/NetBIOS
- PPP/PPTP

TCP/IP

Introduction to TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is considered the standard protocol for the Internet. While the TCP/IP protocol can be used for internal networks without Internet access, TCP/IP must be used for a device to gain Internet access.

TCP/IP is a suite of communications protocols governing how data travels between devices and networks throughout the Internet. Developed in 1969 to interconnect networks of research agencies around the country, TCP/IP was designed to work on all network topologies and to communicate over fiber optics, twisted-pair, or coaxial cable.

Within TCP/IP, the TCP functions (Transport Layer 4) are:

- Divide data into manageable packet sizes
- Reassembles data at destination
- Verifies packet arrival at destination

Within TCP/IP, the IP functions (Network Layer 3) are:

- Defines how much data can be carried by each packet
- Packages and addresses the data to be sent
- Enables various types of networks to read and route data packets

TCP/IP, continued

TCP/IP Message Routing

TCP/IP is a routable protocol and enables computers on different networks to communicate as if they were on the same network. The IP part of this protocol provides the routing capability.

When a message is sent, it is divided into packets. Every client and server in TCP/IP network has a unique IP address. Therefore, each packet carries the IP addresses of both the source and destination computer. TCP/IP determines the right travel path between the two computers and then transmits the packets. When a packet reaches its destination, a confirmation is sent to the source computer. This confirmation is why TCP/IP is considered to be so reliable.

During the packets' journey, TCP/IP employs its suite of protocols to enable different types of networks to exchange data. The protocols that are part of this suite include the following:

- Simple Mail Transfer Protocol (SMTP) – Used to send email between hosts on the network
- File Transfer Protocol (FTP) – Used to transfer files over the network
- Simple Network Management Protocol (SNMP) – Used to monitor network activities
- Telnet – Allows a user to log onto a remote computer and run a program
- Domain Name Service (DNS) – Matches domain names of host computers with their corresponding IP addresses

TCP/IP, continued

TCP/IP Model

The TCP/IP model consists of four layers:

1. Application layer
2. Transport layer
3. Network layer
4. Link layer

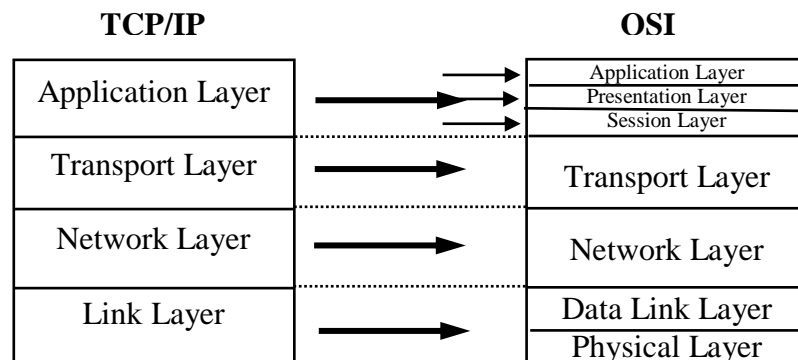
Encapsulation is a TCP/IP process for handling data packets. As data travel down the TCP/IP model when a network device transmits packets, each layer of the TCP/IP model adds leading information, or headers.

De-capsulation is the process of removing the headers as the data travels up the TCP/IP model on the receiving network device.

TCP/IP vs. OSI Model

When comparing the two, OSI is considered to be a conceptual model of how communications should flow from one network to another. It provides a standard for other protocols to use.

On the other hand, TCP/IP represents the actual implementation of how internetwork communications occur. In the TCP/IP Model, the Application layer absorbs the functions of OSI's Presentation and Session layers. The functions of the Data Link and Physical layers are combined. The following illustration shows how the layers of both TCP/IP and OSI model compare to each other.



Other Protocols

IPX/SPX Protocol Internetwork Packet Exchange (IPX) and its related protocol Sequenced Packet Exchange (SPX) are internetworking protocols for Novell Netware. Both are easy to configure for small networks and are compatible with other network operating systems.

IPX is a connectionless network protocol that operates on the network layer. With it, data packets are sent without any prior knowledge of the current state of the recipient system. Therefore, packet delivery cannot be guaranteed.

SPX, on the other hand, is a connection-oriented protocol that ensures the proper delivery of packets by establishing a virtual connection between sender and receiver before packets are sent. Therefore, SPX guarantees delivery of packets and provides error correction and packet sequencing.

NetBIOS and NetBEUI Protocol NetBIOS is the standard networking protocol for Windows networks. NetBIOS provides a programming interface for applications on the Session layer. It is also combined with NetBIOS Extended User Interface (NetBEUI), which serves as the default transport protocol for Windows networks.

Each computer on a NetBEUI network has a unique NetBIOS name (no more than 15 characters). NetBEUI is non-routable; therefore, it cannot pass data through the router to leave the connected LAN. It broadcasts many packets which makes it difficult to scale. For these reasons, it is best suited for small LANs because it is easy to configure with low overhead. NetBEUI is fast and self-tuning.

Other Protocols, continued

PPP and PPTP Protocols

Point-to-Point protocol (PPP) is designed for simple links between two peers. It offers full-duplex operation to both peers and packets are delivered in order (circuit-switched).

In addition, PPP is used to link a PC to the Internet. It creates the session between the PC and the ISP. PPP works well with many protocols including IPX.

Point-to-Point Tunneling protocol (PPTP) enables other protocols to transmit over an IP network. For example, it is used to encapsulate NetWare IPX packets and send them over the Internet. It is also used to carry TCP/IP, IPX/SPX, and NetBEUI traffic.

This page intentionally left blank.

Lesson 4 – Wireless Networks

Introduction

This lesson presents basic information about wireless networks. Topics covered include:

- How wireless networks work
- The different types of wireless networks
- The components that makeup a wireless network
- Security concerns

Purpose of this Lesson

This lesson expands on the earlier lesson on wireless media by providing insight on wireless networks and how they can be used with good and bad intentions.

Objectives

After successfully completing this lesson, you will be able to:

- Explain what a wireless network is and how it works
- Explain the 802.11 standard
- Explain the difference between infrastructure and ad-hoc modes
- Discuss security concerns of implementing wireless networks

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
About Wireless Networks	3-36
Types of Wireless Networks	3-37
Hardware Components	3-38
Security Concerns	3-40
Vulnerabilities	3-45

About Wireless Networks

Definition

As the name implies, a wireless network does not require cables to connect computers and peripherals. Instead, network communications are transmitted across the airwaves using infrared and various forms of radio technology. As discussed earlier, wireless technology uses radio frequencies between 2 and 5 gigahertz and is growing in popularity. It has an effective range between 300 and 1,500 feet.

802.11

Wireless network technology has evolved as a result of a standard published by the Institute of Electrical and Electronics Engineers (IEEE) in 1997. This standard, known as 802.11, established global rules for wireless networking at a speed of 2 megabits per second.

Two years later, in 1999, the IEEE ratified 802.11b, an extension of the original standard that increased the throughput from 2 megabits per second to 11 megabits per second. 802.11b is backward compatible with the original slower speed standard (802.11) and operates at a frequency of 2.4 gigahertz. Additional extensions to the original 802.11 standard have been ratified which include 802.11a and 802.11g, which both offer throughput as high as 54 megabits per second. 802.11g, although faster, is backward compatible with 802.11b. Both operate at 2.4 gigahertz.

Further development of the 802.11 standard continues with 802.11n, which claims to be twice as fast as 802.11g, and 802.11i which addresses the many security concerns over the current 802.11 standards. 802.11n incorporates Multiple Input Multiple Output (MIMO) antennas.

Hot Spots

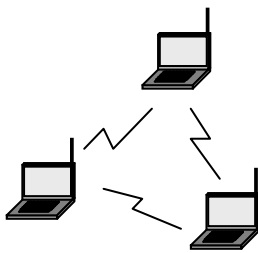
Both desktop and notebook computers on today's market offer 802.11 networking capability. This feature is often packaged under the label *Wi-Fi* and *Centrino*, an Intel trademark. To expand the wireless market, Intel has partnered with companies like Hilton Hotels & Resorts, Borders Group, and McDonalds to develop a concept called *hot spots*. These enable users of wireless-enabled notebooks and PDAs to connect to the Internet while using the other services the business offers. The strategy is two-fold: wireless hardware sales increase, and the hosting businesses attract more customers.

Types of Wireless Networks

Introduction

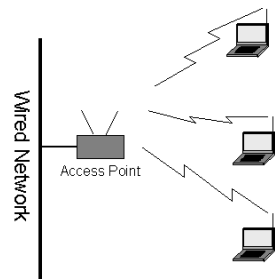
In general, there are two types of wireless networks: ad-hoc and infrastructure. The type of network simply indicates how the wireless devices are configured to communicate. The configuration can be changed very easily from one type to the other, making wireless networking flexible and easy to use. The two types of wireless networks are discussed below.

Ad-Hoc



When a group of wireless computers are configured to communicate with each other in a peer-to-peer configuration, the result is an independent wireless network. The combination of wireless computers and modern operating systems allow the network to be flexible enough for other wireless computers to join the network with ease. This feature provides an easy setup, ideal for groups who wish to collaborate on a project. It is from the ad-hoc nature of this independent network that this wireless network type gets its name.

Infrastructure



A more common use of wireless networking that takes full advantage of wireless device mobility is the infrastructure wireless network. Wireless computers configured to communicate in an infrastructure wireless network look for other wireless devices that are also attached to a wired network. These devices, called access points, are usually attached directly to a hub or switch in a wired network. Their primary function is to provide wireless computers with access to the wired network. Once connected to the wired network, wireless devices can use all of the resources available on that wired network, including Internet access.

Hardware Components

Introduction

A wireless local area network (WLAN) is rarely wireless. Although notebook computers, PDAs, and other devices communicate wirelessly, there are usually key components that are connected to the network by some form of cable. The shared resources, such as the Internet gateway, printers, file servers, etc., are all typically interconnected with cables. So how does the wireless notebook computer access the Internet gateway, or the shared files residing on a file server?

This part of the lesson on wireless networks will discuss the various components that are used in wireless networking and where they might be found. The function and properties of these devices will also be discussed.

Wireless NIC

The network interface card (NIC) is an essential part of any wireless network. Like its cable-based counterpart, the wireless NIC functions as the interface between the PC and the media used to connect the PC to a network. These NICs typically have visible antennae as shown in the examples pictured below.



(The wireless NIC images from left to right are 3COM 3CRDW696 Wireless NIC; LINKSYS Wireless NIC 802.11B; CNET PCI Wireless Network Card CWP-854.)

Hardware Components, continued

Wireless Access Points (WAP)

The wireless NIC must connect to the wired network through another device that has both wired and wireless connectivity. This device, the wireless access point (WAP), is generally a small hardware device that is connected by cable to a hub or switch that is part of the wired network. The WAP can also be a wireless cable/DSL router that provides routing protection and functionality to your broadband Internet service. The WAP is usually equipped with one or two visible antenna. These antennae receive signals from the wireless NIC and convert it to a format compatible with the cable that connects the WAP to the network. A single WAP can support connections from multiple wireless devices. Here are several examples of WAPs.



(The Wireless Access Points images from left to right are Linksys WAP54G-UK Wireless Access Point; AirPlus XtremeG 2.4GHz Wireless Access Point; Motorola WA840G Wireless Access Point; Netgear 802.11b Wireless Access Point.)

Security Concerns

Introduction

The very principles that facilitate wireless network communications also make them extremely vulnerable to eavesdropping and attack. In a broadcast network, data transmissions are sectioned into packets that are broadcast to all devices attached to the network. When packets are broadcast over wireless connections, they can easily be intercepted and examined. As a result of the packet interception, the data being transmitted can be viewed and reassembled by the intercepting party.

WEP

Networking devices manufactured under the 802.11 standards employ a method of encryption called *wired equivalent privacy* or simply *WEP*. This provides encryption of communications based on either a 64 bit or a 128-bit key. In essence, both the wireless computer and the WAP must use the same key in order for them to communicate. Encryption and encryption keys will be covered in greater detail in the Security section of this lesson.

Wireless devices have the ability to turn WEP on or off. Unfortunately, the default state of WEP for most devices is off, meaning the end user is required to understand WEP and how to configure it before the first step toward securing a wireless network is taken.

Although WEP is intended to secure wireless networks, its flaws are well documented, making it slightly better than no security at all. With the right combination of hardware and software, along with 25,000 to 50,000 captured data packets, a WEP key can be cracked within minutes.

Security Concerns, continued

WPA

Since WEP has been determined to be inadequate in securing wireless networks, the Wi-Fi Alliance, in cooperation with several members of the IEEE 802.11i task group, developed Wi-Fi Protected Access (WPA) to address wireless security concerns pending the release of the IEEE 802.11i standard.

While WEP uses a static key for encrypted transmission (the major flaw in WEP), WPA uses dynamic keys so that the same encryption key is never used twice. The difference is that under WEP, captured packets can be analyzed using readily available programs from the Internet to determine the encryption key. Under WPA, the encryption key is derived from up to 500 trillion possibilities.

The result is a key that is virtually uncrackable, if a strong password is used. This would mean 12 or more characters, using upper case, lower case, numbers and special characters. Tests have shown that dictionary words used as passwords can be captured from the key exchange packets within minutes.

LEAP

Developed by Cisco Systems, the Lightweight Extensible Authentication Protocol (LEAP) is a protocol that provides authentication services on a wireless network. What makes LEAP different from WPA is the authentication process that occurs. When a wireless client attempts to access the network, the wireless access point (WAP) blocks all ports except for the authentication ports to allow the user to securely provide authentication credentials. Once these credentials are received, the WAP forwards the credentials to a special authentication server for validation. If the credentials are valid, a unique key is generated for the session and access to the network through the WAP is granted.

The key that is generated is per-user and per-session, complicating and hopefully frustrating any hacking attempts to discern the key from captured packets. To further secure the network, the time-out settings of the key can be adjusted to force devices to re-authenticate frequently. Each re-authentication results in a new session, which results in a new key. Subsequently, the keys change so frequently and the sessions become so short that packet sniffing becomes useless as a means of deriving session keys.

Security Concerns, continued

SSID

The term SSID is used to refer to the Service Set Identifier, a unique, user configurable name that must be used to communicate with a WAP. Most wireless access points have an SSID that is indicative of the manufacturer or model of the device. For example, the Linksys brand of WAP uses the name LINKSYS as its default SSID, while Siemens uses the SSID SPEEDSTREAM to identify its SpeedStream model line. The SSID can be any combination of alpha and numeric characters with a maximum length of 32 characters.

When a WAP is powered on, it begins broadcasting its SSID to any wireless device within range. This feature, intended to simplify connectivity by mobile devices, can be disabled in some WAPs, thus eliminating the necessity for the notebook PC or PDA user to know the SSID before attempting to connect.

MAC Filtering

Enabling WPA and MAC filtering are methods that can be used to harden your wireless network against attack. The term MAC refers to the unique identifier address encoded into every network device. As each wireless device connects to a WAP in an attempt to communicate, its MAC address is read by the WAP. If MAC filtering is enabled, (this is disabled by default), the system administrator creates a list of MAC addresses for devices that are allowed to join the network and saves the list as part of the device's MAC filtering configuration. As each device attempts to connect, the MAC address of that device is validated against the list created by the administrator. If the connecting device's MAC address is not on the MAC filter list, the device is denied access. This can be circumvented through MAC spoofing, which is manually changing the transmitted MAC address of your device.

Security Concerns, continued

Detection Systems The security concerns of using 802.11 wireless networks have driven entrepreneurs and researchers to develop a myriad of solutions to the wireless security threat. Among these solutions are small inexpensive wireless network detectors like the two examples shown here. Both of these devices cost less than \$25 and only detect the presence of 802.11 wireless signals and signal strength.



Although useful for determining if 802.11 wireless activity is present in a given area, these devices are not well suited for determining the WAP SSID, the MAC address of the WAP, or any other information that can be detected using more sophisticated and expensive solutions.

(The Wireless Network Detectors shown above are Kensington Wireless Network Finder and Smart ID Wi-Fi Detector.)

Security Concerns, continued

Detection Systems, continued

Additionally, unauthorized or rogue wireless devices can appear on a network for short durations, making them hard to detect. To address this problem, a number of solutions providers have developed detection systems that are comprised of specialized software and customized sensors. These sensors are placed strategically throughout the network, constantly monitoring for rogue devices. When an unauthorized device is detected, its location is triangulated using the strategically placed sensors, and the network administrator is immediately alerted.

Once a rogue device has been identified and its approximate position determined, the network administrator could use a notebook computer or PDA equipped with a directional antenna to pinpoint the device. This can be accomplished by sweeping the antenna in a 360-degree rotation while monitoring signal strength.

A number of freeware applications are available to perform such functions. These include Net Stumbler for MS Windows and Pocket PC, and Kismet for Linux.

Vulnerabilities

Introduction

Despite the security that has been engineered into wireless (802.11) networks, they are still vulnerable to attack and unauthorized access. The vulnerabilities will be examined in this section, along with the issue of unintentional and accidental access.

War Driving

In the early 1980s, before the Internet emerged as the primary method for distributing files and information, corporations, universities, government agencies, and hobbyists configured computers to function as a central distribution point for various files, news, and information. These computers, called bulletin board systems (BBS), were equipped with modems that were set to automatically answer when a ring was detected, and to establish a connection with the calling computer. Once connected, the caller could login and access the files and data stored on the BBS.

Hackers in the late seventies and early eighties knew that there were thousands, if not hundreds of thousands of computers waiting to communicate with anyone who connected. The lure of an unexplored frontier and the treasures that awaited anyone who found them were driving forces for the hacker to find ways to discover them. As a result, hacker groups collaborated to develop software that could be configured to search for any BBS or modem-enabled mainframe computer by sequentially dialing every telephone number within a given area code and exchange.

As each number was dialed, the hacker's computer waited momentarily for the carrier signal of a modem on the other end. If no carrier was detected, the call was ended and the next number in the sequence dialed. Once a carrier was detected, the calling computer would save the telephone number to a log file, disconnect, and move onto the next number in the sequence. This process was called *war dialing* and eventually became the foundation for many hacking applications that would attempt to compromise long distance billing codes from companies like Sprint, MCI, Americall, and AT&T.

Vulnerabilities, continued

War Driving, continued

The concept of war dialing was applied to wireless networks, but without modems. Just as modems sat waiting for someone to connect, in a wireless network, the WAP waits for someone to connect as well. Anyone with the right hardware, software, and authentication configuration can connect. Even without the configuration information, the airwaves can be scanned for 802.11 signals, and SSIDs. Tools, such as the previously mentioned Net Stumbler and Kismet, can be used with a notebook computer to scan for, and identify wireless networks. The data that these programs collect includes the SSID (if broadcasted), which of the 14 wireless channels or frequencies are used (only 11 are used in the U.S.), whether or not WEP or WPA is enabled, and the MAC address of the WAP. This information can later be used to target specific networks for attack.

Today, wireless networks are used frequently in the business community and most businesses rely on some type of Internet connectivity. The possibility that these businesses have not secured their wireless access points has driven hackers to engineer ways to identify unsecured wireless networks. Their primary motive: free Internet access.

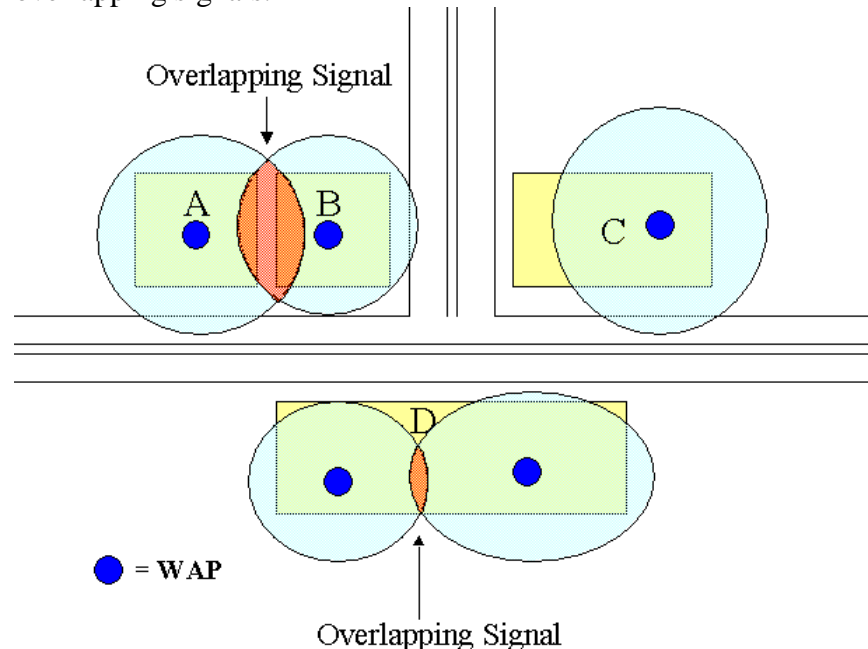
Hackers have developed software similar to the war dialer that attempts to connect to computers or WAPs. The name War Driving is derived from running these programs on a laptop with a wireless NIC and external antenna while driving along the major traffic routes in an effort to locate wireless networks. It is common for War Drivers to record the GPS coordinates of the wireless networks for use with mapping software and for publication to various sites on the Internet.

Vulnerabilities, continued

Overlapping Signals

One problem, of which wireless network administrators are usually aware, is that of overlapping signals. Wireless network signals typically radiate in an elliptical pattern. This can vary depending upon the physical structure in which the WAP is deployed because walls, floors, ceilings, and other obstacles affect radio waves.

In the illustration below, there are four buildings with wireless networks. Building C is far enough away from other buildings that overlapping signals are not an issue. Building D, because of its size, has two wireless access points deployed with minimal signal overlap. If the two signals are owned by two different businesses within building D, this could pose a significant problem. Likewise, buildings A and B have wireless access points generating overlapping signals.



Some examples of corrective action that can be taken to address overlapping signals are:

- Relocation of the WAP
- Reducing power output of the WAP

Vulnerabilities, continued

Accidental Access Because wireless signals can overlap, and because operating systems like Microsoft Windows XP are made to seek out network devices as well as advertise themselves as available network devices, a wireless end user operating in an overlapping signal area could possibly connect to the wrong network accidentally. If the wireless networks are configured to use WEP, the possibility of accidental access is eliminated.

Windows Vista has changed the way it tries to connect to access points as compared to XP. Vista will no longer try to connect to any open access point available the way XP may have. If the access point is not secured and is open, Vista requires that the users manually connect and accept the security warning each and every time it is to connect.

Vista has also improved its security by allowing the user to configure the wireless policies to know if the access point is configured to broadcast or not. For access points that are broadcasting their Service Set Identifier (SSID) information, Vista will not send out probe request trying to connect. If an access point is configured to not broadcast its SSID, then Vista will send out probe requests searching to the access point, thus exposing valuable information about the systems wireless configurations. From a client perspective, it is more secure to configure access points to broadcast their SSID.

These changes in Vista's wireless capabilities and default settings greatly increase the security over previous versions of Microsoft operating systems.

Vulnerabilities, continued

Known Attacks

Wireless network technology is constantly improving. Like most networking technologies, there are known vulnerabilities that lead to attack. The following examples of known wireless network attacks usually result from improperly managed or improperly secured wireless technology. The actual steps taken by a hacker are not detailed here as they are considered too complicated to be within the scope of the lesson.

Session Hijacking

An attacker monitors active sessions, connections between WAP and a remote station, for identifying information that can be used to facilitate his or her attack. Once enough information has been collected, the attacker sends a spoofed message to the workstation to be disconnected. The workstation responds by ending the session, allowing the attacker to masquerade as the disconnected workstation.

Man-in-the-Middle

This attack exploits the one-way authentication of the 802.11 design and allows the attacker to configure his or her computer to act as a wireless access point. The attacker's computer then waits for unsuspecting users to connect to the wireless network. As a result, the remote computers will pass the WEP key to the attacker's computer. The attacker's computer will then establish a connection with the real WAP and pass the remote computers packets transparently between the user and the WAP. The result is a captured WEP key that will allow the attacker access to the wireless network.

Vulnerabilities, continued

Known Attacks, continued

WEP Key Cracking

As previously mentioned, when WEP is enabled, an encrypted key is used to connect to, and transfer data across a wireless network. Only computers with the WEP key are allowed to communicate. Software tools, such as Aircrack-ng and WEPCrack, simplify the job of cracking the WEP key.

By monitoring the packets transmitted across the airwaves, the attacker can save the packets to a log file. After several thousand packets have been collected, cracking tools can analyze the collected packets to determine the WEP key. It's possible to crack a WEP key with 100% success.

WPA-PSK Cracking

WPA-PSK uses a pre-shared key for its encryption algorithm. This method is much more secure than using WEP, but it still is susceptible to cracking attacks. The attack method used to crack WPA-PSK is a dictionary attack, which uses a large database of common words and phrases to guess the password. Therefore, if the data from the transmitting access point and connected user is captured, the data can be run through a dictionary to find the correct key to unlock the data. It is recommended that administrators use a long key that would not be found in any dictionary, such as a complete phrase with additional special characters, etc.

Module 4

IP Addresses and Subnets

Overview

In this module, we will explain Internet Protocol (IP) addresses and how they are constructed. We will also introduce subnet masks.

Purpose of this Module

The purpose of this module is to introduce you to IP addressing and the classes of networks in IP addressing schemes. You will also learn about subnets and the IP addressing schemes for subnet masks.

Objectives

After successfully completing this module, you will be able to:

- Explain IP addresses and how they are constructed
- Name the classes of IP addresses and their characteristics
- Describe Domain Name Service functions
- Define subnetting
- Explain how subnet masking is used
- Name the types of firewalls used today and their characteristics

In this Module

The following table shows the contents of this module.

Topic	See Page
Lesson 1 – IP Addresses	4-3
Lesson 2 – Ports	4-13
Lesson 3 – Subnets	4-21
Lesson 4 – Network Security	4-27

This page intentionally left blank.

Lesson 1 – IP Addresses

Introduction

In a TCP/IP network, IP (Internet Protocol) addressing is essential to the physical routing of network communications. Every device on a LAN (Local Area Network) must have a unique IP address. Each address is essential for internetworking over WANs (Wide Area Networks).

Purpose of this Lesson

In this lesson, you will learn about the importance of IP addressing. You will discuss the three classes of IP addresses and explore the concepts of domain name services (DNS).

Objectives

After successfully completing this lesson, you will be able to:

- Define IP addresses
- Identify the various classes of IP addresses
- Explain the functions of DNS and Classless Inter-Domain Routing (CIDR)

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
IP Address Basics	4-4
IP Address Classes	4-6
More about IP Addresses	4-9

IP Address Basics

Network Addressing Overview

Locating computers on a network is an important function of all networks. With networks, there are two basic addressing schemes: a MAC address and an IP address.

- A Media Access Control (MAC) address is a unique hardware identification number that is specific for each network device. To send a data packet to a computer on a LAN, the sending device must first know the receiver's MAC address. MAC addresses exist at the Data Link Layer 2 of the OSI model.
- IP addresses identify every device attached to a TCP/IP network, including PCs, servers, switches, printers, and any other networked device. Each device has a unique IP address that identifies it for internetwork data packet routing. IP addresses exist at the Network Layer 3 of the OSI model.

Workstations can have either a permanent (static) IP address or one that is dynamically assigned each time a network connection is established. For clients on an isolated LAN, the administrator can assign unique static IP addresses. However, to communicate with the Internet, you must have a unique, registered IP address that is routable through the Internet.

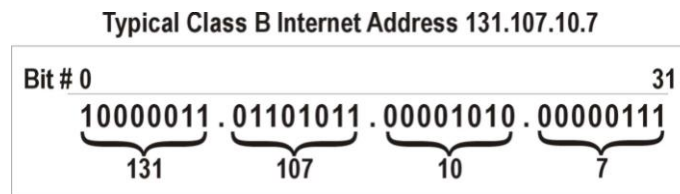
IP Address Basics, continued

What's in an IP Address

An IP address is a 32-bit numeric address written as four sets of numbers, called octets, separated by periods. For example, 131.160.10.240 is an example of a class B IP address. Each octet can range from 0 to a maximum of 255. A valid IP address cannot consist of all zeros or all ones.

For each networked device, the IP address consists of the network address (netid) and the host address (hostid). Each octet of the IP address contains eight bits equaling one byte. Therefore, an IP address has a total of four bytes. The following illustration indicates the various components of an IP address.

Example Class B IP Address 131.107.10.7



Binary IP Addressing

IP addresses are read as a set of four decimals. The computer can only read ones and zeros. Therefore, IP addresses are binary; meaning each of the four decimals is translated into eight binary numbers consisting of ones and zeros.

The binary numbering system used in IP addresses is based on the number 2, called Base2. Because each octet in an address is limited to eight bits, the corresponding binary numbers range from 2^0 to 2^7 (1 to 255). The following chart illustrates the use of Base2 in converting the decimal 131 to its binary number equivalent of 10000011.

Binary Conversion of Decimal 131								
Base2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal	128	64	32	16	8	4	2	1
Binary Number is 10000011	1	0	0	0	0	0	1	1

IP Address Classes

Classes of IP Addresses

IP addresses are divided into several class types. Class A, B, and C are used for government and commercial addresses. Class D and E are reserved for multicasting, which is the transmission of data to many recipients simultaneously. Class D and E are not commonly used.

Each class allows for a specific maximum number of subnets and end nodes.

IP Address Classes, continued

Classes of IP Addresses, continued

The following table describes the characteristics of each IP address class type.

Classes of IP Addresses Defined				
Class	First Octet	Maximum Networks	Maximum Hosts	Other Characteristics
A	1 – 126	126	16,777,214	Most often allocated to government and large institutions; Address Range: 1.X.X.X to 126.X.X.X
B	128 – 191	16,384	65,534	Most often allocated for commercial use and ISPs; Address Range: 128.X.X.X to 191.X.X.X
C	192 – 223	2,097,152	254	Most often allocated for commercial use and ISPs; Address Range: 192.X.X.X to 223.X.X.X
D	224 – 239	N/A	N/A	Reserved class used for multicasting; does not contain network or host IDs
E	240 – 247	N/A	N/A	Reserved class used for experimentation; does not contain network or host IDs

IP Address Classes, continued

Reserved IP Addresses

The following IP addresses are reserved for specific functions:

Description	IP Address Range
Reserved for non-routable networks	<ul style="list-style-type: none">• 10.0.0.0 to 10.255.255.255• 172.16.0.0 to 172.31.255.255• 192.168.0.0 to 192.168.255.255
Reserved for loopback NIC testing	127.0.0.1
Reserved for routing tables; refers to entire network	128.5.0.0
IDs an entire network	X.0.0.0 (Class A) X.X.0.0 (Class B) X.X.X.0 (Class C)
Broadcast	X.255.255.255 (Class A) X.X.255.255 (Class B) X.X.X.255 (Class C)

More about IP Addresses

New Methods for IP Addressing

Because the class system provides a finite number of IP addresses, the number of unassigned Internet addresses is running out. A new scheme called Classless Inter-Domain Routing (CIDR) has been introduced as a replacement for the system based on classes A, B, and C.

With CIDR, IP addresses are assigned in blocks. A single IP address can be used to identify many unique IP addresses. A CIDR IP address looks like a normal IP address except that it ends with a slash followed by a number. This end number is called the IP prefix length because it represents how many bits are used for the network partition of the address. An example of a CIDR address is 162.200.0.0/12.

The prefix length designates how many addresses are available for the network and the hosts in the CIDR address. In the previous example 162.200.0.0/12, the first 12 bits of the address identify the network and the remaining 20 bits identify the host.

10100010.1100|1000.00000000.00000000

$$2^{12} = 4098 \text{ Networks} \quad 2^{20} = 1,048,576 \text{ Hosts per Network}$$

CIDR addresses also reduce the size of routing tables and allows for more IP addresses for subnetting and supernetting within organizations.

IPv6

Internet Protocol version 6 (IPv6) is another new method for IP addressing that significantly increases the amount of available IP addresses. IP version 6 expands an IP address from 32 bits to 128 bits. This will provide over 3.4×10^{38} power new addresses. With IPv6, there will be enough IP addresses generated that every cell of a human body could be assigned one and there would still be addresses to spare.

Addresses for IPv6 are presented in hexadecimal format, such as FE80:325B:134C:5555:678D:9C4D:3EEE:2D5F. This format consists of eight groups of hexadecimal digits. Initially, many addresses will have zeros in the groups.

More about IP Addresses, continued

IPv6, continued

A shorthand notation exists that expresses the groups of zeros, :: (the colon-colon operator). For example, an IPv6 address, FE80::3E4F, is using the colon-colon operator. All the groups within the colons are zeros. Hence, the first group is FE80, the 2nd through 7th groups are all zeros and the 8th group is 3E4F.

IPv6 Special Addresses and Prefixes

Here are some special addresses and prefixes used in IPv6:

Address	Description
::FFFF:0:0/96	Used for IPv4 mapped addresses
FC00::/7	Unique local IPv6 unicast addresses. Routable only within set of cooperating sites. Replaced “site-local” used in earlier implementation of IPv6.
FE80::/10	Local link for use within a LAN. Similar to 169.254.x.x, the autoconfig IP address in IPv4.
FF00::/8	Multicast prefix. No address ranges reserved for broadcast. Applications are to use multicast.
::1 /128	Loopback or “localhost” address. Similar to 127.0.0.1 IPv4 loopback address.
FE80::/10 through FEB0::/10	Private address ranges. Similar to IPv4 private LAN addresses. Local link addresses. Stateless and autoconfigured for use within LAN segment.
FEC0::/10 through FEF0::/10	Private address ranges. Similar to IPv4 private LAN addresses. Local site addresses.
FF00::/8 prefix	Multi-cast prefix
(2000 to 3FFF)::/16 prefix	Global unicast prefix
2001::/16	Assigned to Regional Internet Registrar (RIR)
2002::/16	Assigned to 6to4 Transition Methods
3FFE::/16	Temporary address assigned to 6bone

More about IP Addresses, continued

Dual Stacks

As IPV6 is being implemented, routers and computers can be configured to use both IPv4 and IPv6. Routers which route both IPv4 and IPv6 packets are called dual-stack.

There is no need for a subnet mask address or NAT (Network Address Translation) with IPv6, although NAT can be implemented.

Pseudo-Interfaces

A network card can be configured with multiple IPv6 addresses. For example, one address can be just for the segment, another can be for the site, and a third can be for the Internet.

The IPv6 protocol assigns pseudo-interfaces or zone IDs for each of these. An address may look like ABCD::1234:B2C3 %4. The %4 would be its zone ID.

Domain Name Service

Most networks and Web sites have text-based domain names that people can remember, such as www.google.com. Because the Internet is based on numerical IP addresses, the *domain name service* (DNS) translates text domain names into numerical IP addresses before an Internet connection can be made.

For example, when you type the Web address to your favorite site, the DNS server receives your site request and translates it into the corresponding IP address.

Dynamic Host Configuration Protocol

Network administrators use Dynamic Host Configuration Protocol (DHCP) to assign dynamic IP addresses to individual devices on a network. Addresses are assigned from a pool of pre-registered addresses.

DHCP saves time by eliminating the steps to manually assign IP addresses to new network equipment. It also tracks all assigned addresses automatically.

With DHCP, a computer or other device can be assigned a different IP address every time it accesses the network. In some cases, a device can change its IP address between logon and logoff. ISPs frequently use DHCP for their dial-up and broadband users. DHCP6 will run in networks that have implemented IPv6.

This page intentionally left blank.

Lesson 2 – Ports

Introduction This lesson presents information about network ports, what they are, and how they are used, misused, and managed.

Purpose of this Lesson The purpose of this lesson is to provide a basic level of understanding about network ports.

Objectives After successfully completing this lesson, you will be able to:

- Discuss the definition of a port
- Explain how ports are used in network administration
- Discuss how hackers can identify open ports and what this means to network security

In this Lesson The following table shows the contents of this lesson.

Topic	See Page
Overview of Ports	4-14
How Ports are Used	4-16
Configuring TCP/IP	4-19

Overview of Ports

Ports

Imagine trying to engage in a telephone conversation with someone over a party line (a telephone circuit shared by more than one person) being used by thousands of people. At the very least, you would have great difficulty communicating with that person. Trying to filter out the thousands of other conversations would be impossible. Thankfully, the days of the party line have long passed and communicating by telephone is generally a two-way conversation between parties.

Understanding the person on the other end of the telephone connection is effortless because you are only listening to that one person and not the thousands of other conversations taking place over the phone system at any given time.

Communications over a computer network are similar to the telephone system in the sense that thousands of conversations between computers are occurring every second. In order for your computer to communicate with other computers, and more specifically, other applications, computers use a means of channeling communications, called service ports, or simply *ports*.

When a computer receives data from a network, the TCP/IP protocol stack must know the data's user application destination. For example, when a Web server sends a Web page to your computer, TCP/IP must know that the Web page data is supposed to go to your Web browser. Otherwise, your computer might receive the data, but you would never actually see it displayed.

TCP/IP maps data to an application using a port, which is a number that represents an application. Each data transmission is labeled with a source and a destination port. The source port identifies which application sent the data, and the destination port identifies which application should process the data at the receiving end.

Overview of Ports, continued

Well-Known Ports There are over 65,000 ports available to network applications. Ports 1 – 1023 usually map to specific applications, regardless of the computers involved. For this reason, they are often called *well-known ports*. Here are several examples:

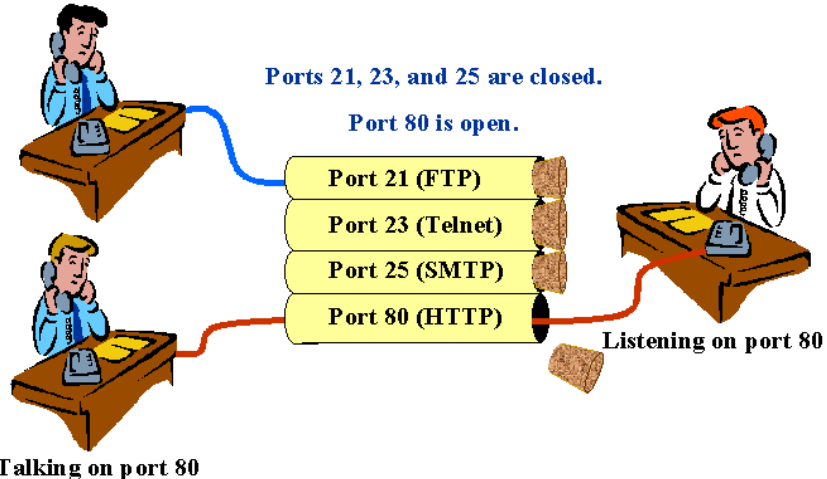
Service	Protocol	Port Number
World Wide Web (HTTP)	TCP	80
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
File Transfer Protocol (FTP) Control	UDP	21

Example

Referring to the graphic below, two applications (on the left) are attempting to communicate with similar applications on the receiving device (on the right) through well-known ports. While one application is communicating through port 80 (the standard port for World Wide Web traffic), another application is communicating through port 21, the well-known port for File Transfer Protocol.

As you can see in the graphic, the receiver has blocked port 21, 23, and 25, disallowing communications, while port 80 is open and transmitted data is received.

Talking on port 21



How Ports are Used

Port Use

With an understanding of how applications like Web servers and Web browsers exchange data through a specific port, you can expand on this knowledge to learn how ports are used.

At various layers of the OSI model, network hardware devices such as firewalls, routers and gateways offer the ability to protect your network by closing certain ports, or opening certain ports to provide access to specific types of information. Some network devices can open a port, but restrict the packets traveling through that port in such a way that certain instructions are blocked, while others are allowed to pass through unaltered.

For example, 21 (File Transfer Protocol) can be opened, but monitored to disallow any packets carrying the `put` command, an FTP command that writes to the FTP server's hard drive. Conversely, the `get` command, an FTP command to copy a file from the FTP server, would not be blocked. This allows files to be downloaded from the FTP server, but not uploaded.

How Ports are Used, continued

Port Management The network administrator usually performs management of ports in a network environment. A computer's ports can be enabled or disabled using features of the operating system.

Windows XP, for example, allows users to enable a built-in software firewall that automatically restricts port access. Terminating an active service on a server can also disable ports. For example, FTP service can be disabled using features of the operating system, thus disabling port 21.

Quite often, ports are managed through configuration of hardware devices called firewalls. Hardware devices that are configured by the network administrator can be managed locally by attaching a special cable from a PC to the network device and running standard communications software, such as Telnet or HyperTerminal.

These devices can also be managed remotely with Telnet. In many instances, they can be managed through a Web browser, such as Internet Explorer, and point the browser to the device's IP address.

Regardless of whether the management is performed locally or remotely, the device will most likely have an administration account that requires a login ID and password to configure the device.

The Windows XP firewall has rules that block inbound communication attempts. The Windows Vista firewall goes one step further with rules that block both inbound and outbound communication attempts.

How Ports are Used, continued

Port Misuse

Most government agencies and large corporations have published policies specifying port configurations for computer network devices. The blocking of certain ports is mandatory in many instances. These policies, intended to minimize the risk of intrusion, are standard.

Although policies exist to maintain a safe network, technical personnel with good intentions might “bend the rules” to accomplish a specific task, the completion of which is crucial to the mission of the organization. In bending the rules, technical personnel might be tempted to temporarily open an unauthorized port on a network device just long enough to accomplish the task at hand. In so doing, the policies protecting the network have been violated and the network has become vulnerable, albeit briefly.

Other examples of misuse might include opening ports for personal use that are required by such applications as instant messengers, file sharing programs, and Internet chat programs. These programs can be detrimental to maintaining a secure network.

Configuring TCP/IP

Procedure: Create a TCP/IP LAN via a Router with Microsoft Vista

Use these steps to configure your TPC/IP protocol to function correctly with the classroom router.

Step	Action
1	Right click on Network and then click Properties.
2	Left click on Manage Network Connections.
3	Right click on Local Area Connection and then click Properties.
4	Highlight Internet Protocol (TCP/IP) and then click Properties.
5	<p>Team 1 will use the IP range and subnet mask listed below:</p> <div style="text-align: center;"> 11.0.0.1 – 11.0.0.15 255.255.255.0 </div> <p>Team 2 will use the IP range and subnet mask listed below:</p> <div style="text-align: center;"> 134.120.0.21 – 134.120.0.25 255.255.0.0 </div> <p>Team 3 will use the IP range and subnet mask listed below:</p> <div style="text-align: center;"> 198.168.112.31- 198.168.112.35 255.255.255.0 </div> <p>Team 4 will use the IP range and subnet mask listed below:</p> <div style="text-align: center;"> 223.14.6.41 – 223.14.6.45 255.255.255.0 </div> <p>Note: There is no gateway address set at this time</p>

This page intentionally left blank.

Lesson 3 – Subnets

Introduction

Understanding subnets is important to computer crime investigations. When the crime scene includes a networked computer, you must know the subnet to which that computer belongs and identify all of the other computers on the same subnet. Within the subnet, the suspect computer has access to other connected computers where evidence may be stored.

Purpose of this Lesson

Networks can be logically divided into sub-networks (subnets) to enhance efficiency and security. This lesson introduces subnetting and the use of subnet masks.

Objectives

After successfully completing this lesson, you will be able to:

- Define subnetting and explain its benefits
- Explain the value of subnet masks
- Identify the components of a subnet mask

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Subnet Overview	4-22
Subnet Masks	4-24
Virtual LAN	4-25

Subnet Overview

Subnets Defined

To increase efficiency, Class A, B, and C networks can be subdivided into subnets. A *subnet* is a segment of a network that shares a common IP network address component with all other devices on the same subnet. On a TCP/IP network, all devices with the same IP address prefix belong to the same subnet.

Networks on the Internet only view other networks as single entities. They have no way of viewing another network's subnet structure. This helps reduce the size of routing tables.

When a data packet is sent over the Internet, it goes to the router of the destination network. The router then determines the destination node by deciphering the packet's subnet address.

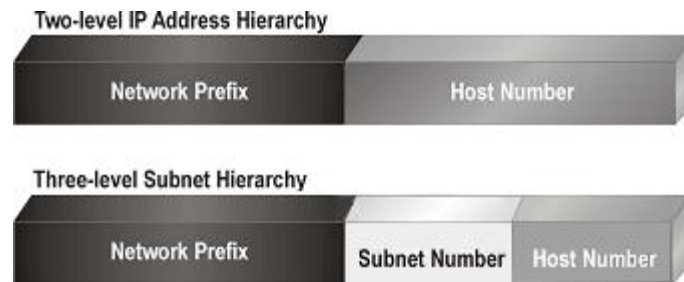
Advantages of Subnetting

- Enhances security by creating subnets that have restricted access
- Extends the capabilities of the network
- Enhances network performance because routers determine the destination network thereby eliminating traffic on other segments
- Allows subnets to be invisible to the outside world
- Provides flexibility by allowing administrators to deploy additional subnets without registering new network numbers
- Allows data route changes within a network without affecting the Internet routing table

Subnet Overview, continued

Subnet Addressing Like IP addresses, each subnet address is unique. As you recall, each IP address has four octets and the address is divided into two major segments: a network address and a host address. By comparison, a subnet address contains three segments: the network address, subnet address, and the host address as illustrated here.

IP Address vs. Subnet Address



Creating Subnets Network administrators create subnets as extensions of the network number. To create a subnet address, the administrator takes bits from the host number and reassigns them to the subnet field. Therefore, the more bits taken from the host number, the fewer host addresses that can be assigned to that subnet.

Note: Any user with administrator-level access can modify a computer's subnet configuration.

Subnet Masks

Definition

A *subnet mask* conceals a subnet from outside networks. As you recall, every subnet address consists of the network prefix, subnet number (including mask), and host number. The two main functions of a subnet mask are as follows:

- Identify the subnet of an IP address
- Notify communicating devices which part of an IP address is the network ID (including subnet) and which part is the host ID

Classes of Subnet Masks

There are three default classes of subnet masks. They are as follows:

- Class A - 255.0.0.0
- Class B - 255.255.0.0
- Class C - 255.255.255.0

Subnet Masks Components

Subnet masks use the same 32-bit, four-octet structure as IP addresses. Subnet mask addresses have three parts: network address, subnet address, and host address. A subnet mask has all ones in the network and subnet segments of the address and contains all zeros in the host segment.

With subnetting, part of the host address is used to identify the subnet. The subnet mask is the network address plus the bits reserved to identify the subnet.

Virtual LAN

Definition

Virtual LAN (VLAN) is another way to divide a local area network into logical subgroups. VLAN uses software to connect a group of computers and devices together instead of manually moving cables and wiring. It can be used to combine workstations and other devices into a single group regardless of their physical location. The result improves traffic flow within the workgroup.

VLANs are used in LAN switches. Network changes and additions are quickly implemented with the VLAN software making proprietary group solutions easy to create. VLANs operate at the Data Link Layer 2 and Network Layer 3 of the OSI model.

This page intentionally left blank.

Lesson 4 – Network Security

Introduction

Network security, an essential component for network management, strives to protect network resources through layered defenses. These defenses generally contain encryption, anti-virus software, firewalls, and Intrusion Detection System (IDS) devices. This lesson focuses on the network security methods available today.

Purpose of this Lesson

The purpose of this lesson is to gain an understanding of how networks are secured. You will learn about the types of evidence available in the form of logs. Various types of firewalls and Intrusion Detection Systems (IDS) are also introduced.

Objectives

After completing this lesson, you will be able to:

- Explain the various firewall architectures
- Name the types of firewalls used today and their characteristics
- Explain data encryption
- Define the security methods of IDS
- Identify various types of network logs

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Data Encryption	4-28
Anti-Virus Software	4-29
Firewalls	4-30
IDS	4-37
Logs	4-39
Network Security Summary	4-41

Data Encryption

Data Encryption *Data encryption* is the conversion of data into a form that cannot be easily deciphered. Encrypted text is called cipher text.

Decryption converts encrypted data into plain text that can be easily understood. Encryption provides a highly effective method for data protection. There are two types of encryption:

1. *Asymmetric encryption* uses two types of cryptographic keys to encode messages. The public key is known to everyone. The private key is only known to the recipient. These methods work because the public key relates to the private key in order to decrypt messages upon receipt.
2. *Symmetric encryption* uses the same key to encode and decode messages.

Anti-Virus Software

Viruses

A virus is a small piece of code that executes when opening a real program or file. For example, a virus might attach itself to a word processing file. When the file is opened, the virus code then attaches itself to the word processing program. Each time the program runs, the virus runs, too. It then has the chance to replicate by attaching to other programs or wreak havoc, such as deleting the entire contents of the hard drive.

E-mail Viruses

An e-mail virus spreads in e-mail messages, usually by automatically mailing itself to every address in the victim's e-mail address book.

Worms

A worm is a small piece of code that uses computer networks and vulnerabilities, known as security holes, to replicate itself. The worm scans the network for any machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

Trojan Horses

A Trojan horse is not a virus; it is a computer program. The program claims to do one thing, but instead does damage when you run it. For example, a Trojan horse may claim to be a game, but instead may erase your hard disk or create a backdoor. Trojan horses have no way to replicate automatically.

Boot Sector Viruses

Boot sector viruses spread by infecting the boot sector of the boot media, usually a hard drive or a floppy diskette. Once infected, every time the computer boots, the virus is loaded automatically into memory. Thereafter, it attempts to infect every other program and file opened.

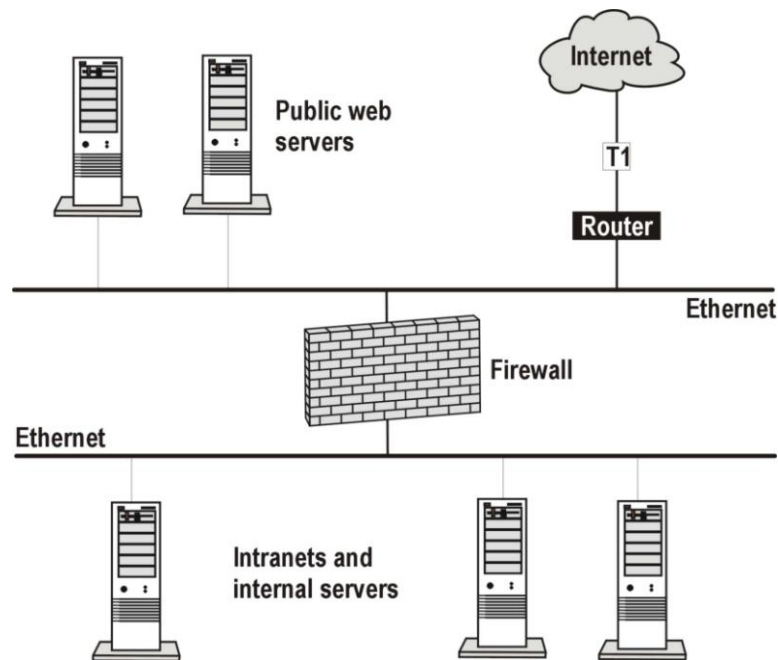
Firewalls

Introduction

A *firewall* is a method of securing a network from unauthorized access. Most often, firewalls protect against intruders who seek access via the Internet. Enterprises install firewalls to offer secure Internet access for employees and to separate and protect their intranet from unauthorized public Web site traffic. Firewalls can also be installed to protect an organization's internal departments or domains, such as a firewall that secures the accounting department.

Firewall protection can be software, hardware, or a combination of both. Each one performs specific security activities. Firewalls are access control devices that only detect failed attempts at access. If an intruder defeats the corporate firewall, the intrusion may or may not be logged, depending on the firewall configurations.

Intranet protected by firewall



Firewalls, continued

How Firewalls Work

All messages going in or out of the network pass through the firewall. Messages are checked using specified security criteria. The firewall blocks those that do not meet the criteria. Different types of firewalls work at various layers of the OSI model or the TCP/IP protocol. The following sections define each type of firewall.

Network Address Translation (NAT)

NAT allows you to use internal non-routable IP addresses on your intranet and connect to the Internet with one registered IP address. The registered IP address is assigned to the software or hardware device running NAT. This process allows any computer behind the NAT device to be invisible to the Internet because only the NAT device's registered IP address is being used.

OSI Model: NAT firewalls operate at Network Layer 3.

TCP/IP Model: NAT firewalls operate at Network Layer 2.

How NAT Works

The following table describes the NAT process for intranet messaging via the Internet.

Stage	Activity
1	The intranet computer sends data packet to NAT device.
2	The NAT device examines the packet header and records which intranet computer made the request.
3	The NAT device then replaces the IP address with its own registered IP address and sends the request to the Internet.
4	When the information packet returns, it goes to the IP address of the NAT device.
5	The NAT device then examines the packet, places the appropriate IP address for the intranet computer, and sends it the computer.

Firewalls, continued

Stateful Inspection *Stateful inspection* firewall architecture has the ability to look into the packet and allow only certain types of application commands while rejecting others. For example, a stateful packet-filtering firewall allows the FTP command `get` and rejects the `put` command.

Stateful inspection firewalls record the User Datagram Protocol (UDP) packet request that is permitted to cross the firewall in a state table. Incoming UDP packets are then examined and verified against the ones waiting for a response in the state table. If the information matches, the request is permitted to enter the network. Otherwise the packet is rejected.

OSI Model: Stateful inspection firewalls operate at Network Layer 3.

TCP/IP Model: Stateful inspection firewalls operate at Network Layer 2.

Firewalls, continued

Packet-filtering Firewalls

A *packet-filtering* firewall checks the header of each packet for specific information and then either accepts or rejects the packets based on user-defined rules. Checks are made for:

- Source and destination IP address
- Source and destination port numbers
- Protocol type
- Direction of the packet (inbound or outbound)

OSI Model: Packet-filtering firewalls operate at Network Layer 3.

TCP/IP Model: Packet-filtering firewalls operate at Network Layer 2.

Advantages

- Good performance
- NAT shields internal addresses from external users
- No code modifications are needed
- Closes ports when not in use
- Stateful inspection checks the packets and only allows those through that were requested

Disadvantages

- Subject to IP spoofing or port spoofing
- Cannot filter or authenticate URL information
- Little or no auditing or alert mechanisms
- Rules need to be entered for stateful inspection type firewalls and then changed

Firewalls, continued

Circuit-level Firewall

A circuit-level firewall validates TCP and UDP sessions before opening a connection. After the validation, it passes everything through until the session has ended.

A circuit-level firewall establishes a virtual circuit between the client and the host on a session-by-session basis. The firewall maintains a table of connections that includes session and sequencing information. When the session ends, the table information is removed and the virtual connection is closed. Only packets associated with the session are allowed through. If the packet is valid according to the session table, the packet is passed through without any further security checks.

The circuit-level firewall session consists of two connections: one between the client and the firewall and one between the firewall and server. All outgoing packets appear to have originated from the firewall in a method similar to NAT.

OSI Model: Circuit-level firewalls operate at Session Layer 5.

TCP/IP Model: Circuit-level firewalls operate at the Transport Layer 3.

Advantages

- Good performance because the packets are not examined after the initial connection is allowed
- No direct connection between client and the application server
- Similar to NAT's method of shielding internal IP address

Disadvantages

- Client programs need to be recompiled and relinked to a special library containing the set of rules for sessions
- Does not examine the application level information in the packets allowing them to be subverted by an inside user or outside hacker

Firewalls, continued

Application-Gateway Firewall

Application-gateway firewalls run a proxy server application that acts as an intermediary between two systems. The proxy server evaluates all requests from internal computers to connect to an external service, such as FTP, and determines whether to permit or deny the request based on the rules defined for the individual network.

The application-gateway running on the proxy server understands the protocols of the service it is evaluating and can deny any packets that do not comply with the protocol for that service. It also provides detailed audit records or session information, user authentication, URL filtering, and caching.

Application-gateway firewalls are application specific and require proxy addresses for FTP, HTTP, SMTP, etc. Because they work through a proxy, they also perform NAT services. In addition, these firewalls operate at the OSI model Application Layer and have the ability to look down through the packets to the application layer information and determine if the packet is altered or not complying with the appropriate protocol rules. These additional steps cause the application-gateway firewall to be slower than other types of firewalls.

OSI Model: Application-gateway firewalls operate at Application Layer 7.

TCP/IP Model: Application-gateway firewalls operate at the Application Layer 4.

Firewalls, continued

Application-Gateway Firewall Advantages

- No direct connection between the internal client and external server
- Can deny packets that do not comply with the protocol for a service, such as FTP, HTTP, SMTP, etc.
- Ability to screen data streams for potential threats, such as send mail attacks, and Java or ActiveX scripts riding on top of HTTP services
- Provide NAT services
- Transparent to the individual user
- Can implement features such as HTTP object caching, URL filtering and user authentication
- Provide audit logs for administrators to monitor for violations of security policy

Application-Gateway Firewall Disadvantages

- Slower than other firewall methods
- Vulnerable to operating system and application level bugs because they are highly dependant on the operating system, TCP/IP stacks, and runtime libraries
- New services require new proxy servers

IDS

Intrusion Detection Systems (IDS)

Unlike firewalls that attempt to block entry into the network, Intrusion Detection Systems (IDS) monitor the network for attacks. There are two basic types of IDSs:

- *Network-based IDS* monitors the entire network for signs of an intrusion
- *Host-based IDS* monitors an individual computer

IDS must be installed consistent with the network's type and topology.

Network-based IDS

A network-based IDS monitors the entire network and uses the information in the data packets to detect an intrusion. It analyzes the packets for an *attack signature*, a known pattern in the packet or packets that match a specific attack type.

The IDS analyzes the packets in real time using its recognition files. The most common method used by IDS pattern expression is byte code matching, also known as signature analysis or misuse detection.

An IDS looks for a substring of data within the network packets that matches known attack signatures. A match between a substring and an attack signature signals an attack on the network.

When an attack is identified, the IDS can be programmed to perform any of the following actions:

- Send an alert to the console
- Log the event and send an email
- Initiate a connection kill (TCP reset)
- Reconfigure a firewall or router, or use an SNMP trap

In the same way that you keep virus definition files up-to-date in your virus protection software, it is equally as important to keep a list of known attack signatures current.

IDS, continued

Host-based IDS

Host-based IDS is installed on an individual computer to monitor only that computer. Host-based IDSs are used to:

- Monitor logs
- Detect file access
- Detect attempts to install executables
- Monitor remote user activities

Host-based IDSs are specific to the operating system that is installed on the computer. On a computer with NT operating system, IDS will monitor the system, event, and security logs. On a computer with a Unix OS, it will monitor the syslog. The host-based IDS examines each log's entry to see if it matches any known attack patterns.

Some host-based systems can also monitor the ports on the computer. When certain ports are accessed, the host-based IDS takes action depending on the system's configuration. Security actions include:

- Log the event
- Alert the console and send an e-mail
- Initiate a SNMP trap
- Terminate the user login and disable the user account

Host-based IDSs can also detect attacks initiated from the local keyboard. Keyboard attacks should be rare if the computer is located in a secure area, the user logs off correctly, and user passwords are changed frequently.

Logs

Introduction

Logs are a record of network activity that provide system administrators with details of computer transactions and network traffic. Logs are routinely used for backup, recovery, and statistical purposes. They can also be used to detect failed and successful intrusions, abnormal network activity, and system activities.

Networks have many different types of logs that can be generated by both software and hardware devices. Logs can be an integral part of computer forensic investigations. Some of the more common logs that you may encounter are:

- System logs
- Firewall logs
- Router logs
- IDS logs

System Logs

Most networking operating systems have the ability to maintain log files. Those files can include system activities, application activities, and security activities. They can also be configured to maintain logs for Internet access, FTP sessions, etc.

For example, Windows NT/2000/XP maintains three main logs that can be accessed through the Event Viewer. Those logs are:

1. System log
2. Security log
3. Application log

The logs can be configured to capture both successful and failed logon attempts.

Logs, continued

Firewall Logs

All firewalls have the ability to capture failed network access and send the information to a log file. The firewall log file provides information on:

- Type of attempted access (Web access, FTP access, Telnet access etc.)
- Port that the attempted access originated from and was directed to
- Date and time of attempted access
- IP address from which the attempt came
- Application-level firewall logs can also provide you with detailed information of session information, user authentication, and security policy violations

Router Logs

Routers can log information about network traffic and any potential network problems that occur. They can also be configured to log abnormal activity that contains host information of a possible intruder and what was accessed on the network during the attempt.

Dial-up-access routers, such as those used by Internet Service Providers, can log dial-up connection information including the username, IP address assigned, date, time, and duration of the connection. This information can be very beneficial during an intrusion investigation.

IDS Logs

IDS can be configured to log a wide variety of information. IDS examines all packets on the network; therefore, IDS logs can contain large amounts of log information that can be of useful to the investigator. Some of the information that can be obtained from IDS logs include:

- Intrusions
- Intrusion attempts
- Unauthorized access to a computer
- Attempts to access unauthorized data
- Attempts to manipulate privileged files
- Attempts to render a network system inoperable

Network Security Summary

Network Security Summary

Most network administrators implement a layered approach to network security:

- Intrusion Detection to provide real-time monitoring of the network
- Firewalls to restrict unauthorized access to the network
- Anti-virus protection to reduce the risk of infection
- Encryption to prevent stolen data packets from being read
- Logs to record activity and provide documentation should a breach of security occur

This page intentionally left blank.

Module 5

Common Network Crimes

Overview

Similar to physical crimes, network-based crimes fall into categories. These categories for common network crimes include e-mail scams, online fraud, identity theft, social threats, internal threats, malicious code, denial of service attacks, extortion, network attacks, and terrorism. In this module, we will examine and discuss the characteristics of the most commonly perpetrated crimes involving network communications.

Purpose of this Module

This module examines ten of the most common network-based crimes that you may encounter as an investigator. You will learn about typical methodologies used for each crime and some of the traditional investigative responses.

Objectives

After completing this module, you will be able to:

- Describe each of the crimes
- Discuss the methodologies of each crime
- Explain the traditional responses to these crimes

In this Module

The following table shows the contents of this module.

Topic	See Page
Lesson 1 – E-Mail Scams	5-3
Lesson 2 – Online Fraud	5-9
Lesson 3 – Identity Theft	5-15
Lesson 4 – Social Threats	5-19
Lesson 5 – Internal Threats	5-23
Lesson 6 – Malicious Code	5-27
Lesson 7 – Denial of Service Attacks	5-31
Lesson 8 – Extortion	5-35
Lesson 9 – Network Attacks	5-39
Lesson 10 – Terrorism	5-43

This page intentionally left blank.

Lesson 1 – E-Mail Scams

Introduction

Today's criminals use the Internet and know a majority of victims do not look closely at e-mail headers or question the authenticity of the sender. E-mails contain headers that document who sent an e-mail and from which IP address and server. This information can be used to help detect suspicious e-mails sent by unreliable sources.

Purpose of this Lesson

The purpose of this lesson is to describe the ways that e-mail can be used for illicit purposes.

Objectives

After completing this lesson, you will be able to:

- Describe e-mail scams
- Explain how e-mail scams are perpetrated
- Explain how investigators typically respond to these attacks

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Overview of E-mail Scams	5-4
Attack Methodologies	5-5
Investigative Response	5-7

Overview of E-Mail Scams

Definition

A scam is defined as a fraudulent business act. Using the postal system for fraudulent means has been around since the 1660s. It was a simple step for surface-mail scammers to make the leap to the Internet when e-mail became popular.

Why E-mail Scams Work

E-mail scams work because people often do not look at e-mail headers. If they did, they could compare the information in the header to see if it matches the sender.

For example, a common scam is an e-mail purportedly sent by a bank that is in fact sent by a scammer. Upon careful inspection of the header, a user could notice that the e-mail stating it is from a bank has a header that shows the origination to be from an individual's e-mail address.

These e-mail scams often use HTML-encoded graphics to display logos and other items that give the illusion of authenticity. They use copyrighted images to hide the fact that the communication is not from the stated source. An attacker could also easily hide code in HTML formatted e-mail. This code could launch trojans or other malicious code, such as a virus, when the e-mail is viewed.

Just like the chain letters that the U.S. Postal Service combats daily, chain e-mails and solicitations for money using every imaginable story and trick are prevalent on the Internet.

Attack Methodologies

The Nigerian or 419 Scam

The Nigerian Scam, which is also known as the 419 or Advance Fee Fraud Scam, is a true legend among e-mail frauds. Here are the typical components of the scam:

- *Foreign Nation*: Virtually all of the e-mails originate from a country other than the United States. Countries that have no agreements with the U.S. pertaining to prosecution of these frauds are the most popular.
- *Government connected source*: Usually the person making the request will claim to either be a government official or a relative of a deposed leader or potentate.
- *Large sums of money*: The requests always involve large, usually multi-million dollar, sums of money.
- *Money Access*: Usually the person making the request has a reason why he or she cannot get to the money, but the recipient, being an upstanding American, can.
- *Advance Fee*: The sender will request that a sum of money be deposited to an account in the other country. The recipient transfers the money to the account and waits for the big payoff. Of course, the requestor has ran off with the money and is outside the reach of U.S. law enforcement.

Origins of 419

The Nigerian government has taken a harder line against these frauds. Section 419 of the Nigerian Criminal Code outlaws this activity.

According to Nigerian law, it is also illegal to try to remove funds from Nigeria. People who have gone to Nigeria to try and recover their money back have been imprisoned for doing so.

Attack Methodologies, continued

Phishing

Phishing is when a perpetrator sends e-mail that appears legitimate in an attempt to gain financial or personal information on the recipient. This information can then be used for other network crimes.

Examples

There are many types of phishing attacks. Here are some examples:

eBay/PayPal – The recipient receives an e-mail that appears to be from eBay online auctions. In the e-mail, the recipient is told to change his password for security reasons. The e-mail includes a form to enter the current and new passwords, in addition to other personal identification information. The recipient fills out the form and sends it back to the attacker, who can now use that information to empty the person's account or steal his identity.

Banks – The recipient receives an e-mail with the bank logo and other items that the attacker copied from the bank's real Web site. The e-mail offers a low refinance rate or interest loan. The recipient is asked to fill out a form with personal information that would usually be on a loan request. If the recipient fills out the form, the attacker now has more than enough information to steal the person's identity. In some cases, these attackers obtain a loan from the bank using this information and leave the recipient holding the note.

Cross Site Scripting – The recipient receives an e-mail that appears to be from a legitimate entity. However, when the recipient logs into the site using his ID and PIN, he becomes a victim of a cross-site scripting attack. This attack, also known as an XSS attack, uses custom code to track information in a client's Web browser windows. The perpetrator has code in the e-mail that captures the information and passes the recipient to the real Web site. Then the attacker can enter the Web site at a later time and use the victim's account information.

Spam

At first you may not consider spam, which is an unsolicited advertisement or bulk e-mail, an attack. But consider the fact of how much bandwidth is consumed and how much storage space is used by spam each day. It is estimated that spam costs companies in the U.S. over \$12 billion dollars a year.

Investigative Response

Capture	As you investigate e-mail scams, it is important to know how to view the complete original message. Most e-mail clients and Web-based clients have either a menu option or a button that you can click to view the complete original message.
Preservation	In some cases, you may have to obtain the original e-mail and/or the Internet Service Provider logs from the server. This usually requires for you to present a preservation letter to the ISP's point-of-contact for law enforcement.
Warrants	Once preservation letters have been delivered, you need to secure the warrants to seize the data. Note that in some cases the data you are trying to obtain may already be deleted from the ISP's server by the time you investigate the crime.
Reporting	First and foremost you should refer to your agency's Standard Operating Procedures for internal reporting methods for these offenses. Depending on your agency, you may be required to report offenses up the chain to State and/or Federal enforcement agencies. In the case of offenses that reach outside the borders of the United States, you should seek assistance from international enforcement groups.
Education	Where possible, provide victims with information on classes or other places where they can find assistance with learning how to protect themselves from e-mail fraud attacks.

This page intentionally left blank.

Lesson 2 – Online Fraud

Introduction

Virtually all major businesses rely upon a Web presence to sell products or bring customers into stores. Many companies establish “virtual storefronts” that allow an entire business to run without a brick and mortar store, relying completely upon the Internet. Many virtual businesses are created by single individuals to sell goods over Web sites and auction sites such as eBay, as well as through e-mail. Due to the large variety of online businesses there are numerous ways in which a victim can be defrauded in the world of e-commerce.

Purpose of this Lesson

The purpose of this lesson is to learn the common types of online fraud.

Objectives

After completing this lesson, you will be able to:

- Describe some of the common online fraud techniques
- Discuss the methodologies used in these cases
- Explain some of the responses to these attacks

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Online Fraud Overview	5-10
Attack Methodologies	5-11
Investigative Responses	5-13

Online Fraud Overview

Online Fraud

Defining online fraud can be fairly easy. It is any form of fraud that is practiced on the Internet. Such fraud generally involves creating elaborate situations in which to deceive online users into giving money to criminals. Explaining all the possible ways in which this can occur can be much harder.

In this section, we will describe some of the common fraud attacks. As new online frauds are constantly developed, you will probably see numerous new attacks in the field.

Common Attack Vectors

The attack vectors in an online fraud case can include:

- *Price too good to be true:* In many of the online auction frauds you will find that a popular item is priced much lower than normal. When the victim buys the item nothing is sent once the winning bid is paid.
- *Short time to decide:* The attacker may make the offer available only for a short period of time, thereby making the victim act before he or she has time to think it through.
- *Fine print:* Lawyers aren't the only ones that like to put clauses in small type. Many times attackers will put important information in very small type, or change the type to a color that is only a few shades different than the background color, making the type very hard to read.
- *Hijacked sites:* Some attackers will take over a Web site, known as hijacking, and use the site for their own gain until the real owner discovers and fixes the site.
- *Box-of-rocks:* Just like older postal frauds, online criminals will offer a product, collect the money and send a box of worthless goods, or even rocks instead of the promised item.
- *Stall tactics:* If the criminal thinks that the victim is not Internet savvy, the criminal may try to stall to get more money. He may also stall the resolution of the problem until the victim gives up in frustration.

Attack Methodologies

Bogus Web Sites

An attacker or criminal can generate a new Web site in a matter of minutes. There are numerous Web site providers that will accept a credit card or PayPal money transfer and provide the criminal with a domain name in less than a day. Additionally, through a process known as domain tasting, a new domain name can be registered for a five-day “test” period for free through many domain name registrars. This site can then be very quickly populated with whatever fraudulent information or services the criminal wants. The criminal can potentially be making money within 48 hours. When the criminal is no longer willing to accept the risk of detection for the fraudulent site, he erases the site and moves to a new provider with a modified name the next day.

If the criminals used bogus names and addresses, then they are virtually untraceable using normal investigative techniques. In many cases, you will find that the criminal has used numerous forms of obfuscation to hide his identities and locations. The only way you may be able to locate the criminal is to literally follow the money through banking records.

Auctions

eBay is a global marketplace and it is also a haven for fraud. eBay, and other online auction services, have made great improvements in addressing fraud and trying to keep it to a minimum. In many cases, these auction sites will use insurance money to pay back the victim rather than have the negative publicity impact business.

Putting a picture of an expensive, desirable item on an auction page and then selling it for less than fair market value is a popular fraud scenario. Often, product descriptions and images are simply copied from other auctions to give a legitimate look to the fraudulent auction.

Advertising pictures of a similar item that is in much better condition is another popular tactic. Frauds can also offer one item but show pictures of another. Notably, popular video game systems have appeared on eBay with pictures of the actual console but small text stating that bidders will receive only an empty box.

In these cases, depending on the wording of the auction advertisement, there may be no recourse for the victim. It is important to thoroughly read any disclaimers about what you are buying.

Attack Methodologies

Bogus Charities

The most famous of the bogus charities in recent years is the Web site that collected hundreds of thousands of dollars in the name of victims of the September 11th terrorist attacks. The money actually went to a scammer's bank account and the 9/11 victims never saw a penny of it.

Playing to a person's sympathies is a popular fraud tactic and it is seen in many different forms on Web pages. Some have been bold enough to actually put small disclaimers at the bottom of the page notifying anyone willing to read it that the money would not actually go to the charity.

Investigative Responses

Capture	As you investigate online fraud, it is important to capture the fraudulent site as soon as possible. Most fraudulent sites are gone in a very short amount of time and the evidence will be lost.
Preservation	In some cases, you may have to obtain the original site files and/or the Internet Service Provider logs from the server. This usually requires you to present a preservation letter to the ISP's point-of-contact for law enforcement.
Warrants	Once preservation letters have been delivered, you should obtain the warrants to seize the data. Note that in some cases the data you are trying to obtain may already be deleted from the ISP's server by the time you investigate the crime.
Reporting	First and foremost you should refer to your agency's Standard Operating Procedures for internal reporting methods for these offenses. Depending on your agency, you may be required to report offenses up the chain to State and/or Federal enforcement agencies. In the case of offenses that reach outside the borders of the United States, you should seek assistance from international enforcement groups.
Education	Where possible, provide victims with information on classes or other places where they can receive assistance with learning how to protect themselves from fraud attacks.
Recording Observations	Observations can be recorded in many different forms, including written notes, office documents, and databases. You should use the approved and tested method used by your organization. This course uses a spreadsheet template for recording this data.

This page intentionally left blank.

Lesson 3 – Identity Theft

Introduction

In 2007, there were an estimated 8.4 million reported cases of identity theft in the U.S. That number is down from the reported 10.1 million in 2003. Even with the decline the identity theft problem is ever present in society today.

Purpose of this Lesson

The purpose of this lesson is to learn how identity theft is perpetrated online.

Objectives

After completing this lesson, you will be able to:

- Discuss some of the common online identity theft techniques
- Explain the methodologies used in these cases
- Describe some of the responses to these attacks

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Identity Theft	5-16
Investigative Responses	5-18

Identity Theft

Overview

As you have seen in the previous lessons in this module, there are numerous ways in which a criminal can gain enough information to assume someone else's identity. The most sophisticated criminals will use numerous social engineering methods to gather information on a victim. As investigators, we use some of the same offline sources to gather information on subjects:

- *Search engines:* Using Google, Dogpile, Yahoo or other search engines to search for a name, address, phone number, license plate, etc.
- *Public information sites:* County tax records, marital records, vehicle license information and many other forms of public records are searchable online.
- *Group sites:* MySpace, Facebook, and many other community sites can be a good source of information. People tend to put pictures of themselves on these sites and do not notice things in the background like addresses and license plates that can be used to gather even more information.
- *Commercial sites:* Many companies and agencies are taking employee information off their Web sites, but some are not. It is possible to find information on people from press releases and company phone and e-mail lists.
- *Membership sites:* Many clubs and membership groups have lists of members with phone numbers and addresses, and sometimes even birth dates on their Web sites.

The Internet is a vast research engine that allows someone to look for information on virtually any topic. Information on people is as easy to find as any other piece of information.

Identity Theft, continued

Attack Methodologies

If the criminal can find one piece of information on a target victim, the criminal can use any number of tools or sites on the Internet to gather information very easily. Here are just a few examples of ways in which this can be done.

In this example we are using the Google search engine, but you can use these methods with any search tool.

Information Type	Description
Name	Simply type the name enclosed in single quotes to narrow the search to the full name on any page that Google has seen. If the name is too common or if too many results are returned, use the plus sign to link the name to a city. For example: 'John Smith' + 'Austin, TX'
Phone	Entering the phone number into the search box will return sites that list the address associated with the phone number and the name to which the number is registered. '555-1212'
Social Security Number	The number of returns found from searching for a social security number is diminishing, but it is sometimes possible to find sites that have this information.
Address	Searching for an address usually returns the registered owner of the property and his or her contact information. Searching for an address in Google Earth shows you the exact location of the property and in most cases a satellite photo.
License plate	A search for a license plate can in some states return the name and address of the registered owner.

Pretexting

In recent years there has been a growth in occurrences of pretexting, the act of using small bits of information about a subject to gather more details from businesses and vendors.

With this attack, an attacker can call a business or service and pretend to be the victim. Using information already gathered, the attacker can then persuade the business to disclose further information, or even change information in the account to allow the attacker full control of the account.

Investigative Responses

Capture	As you investigate ID theft, it is important to gather as much original information as possible.
Preservation	In some cases, you may have to obtain the original Web or e-mail content and/or the Internet Service Provider logs from the server. This usually requires you presenting a preservation letter to the ISP's point-of-contact for law enforcement.
Warrants	Once preservation letters have been delivered, you should acquire the warrants to seize the data. Note that in some cases the data you are trying to obtain may already be deleted from the ISP's server by the time you investigate the crime.
Reporting	First and foremost you should refer to your agency's Standard Operating Procedures for internal reporting methods for these offenses. Depending on your agency, you may be required to report offenses up the chain to State and/or Federal enforcement agencies. In the case of offenses that reach outside the borders of the United States, you should seek assistance from international enforcement groups.
Education	Where possible, provide victims with information on classes or other places where they can get assistance on learning how to protect themselves from e-mail fraud attacks.

Lesson 4 – Social Threats

Introduction

The Internet has created a layer of perceived anonymity for criminals. This has led to an increase in social threats perpetrated on the Internet.

Purpose of this Lesson

The purpose of this lesson is to learn how social threats are perpetrated online.

Objectives

After completing this lesson, you will be able to:

- Describe some of the common online social threats
- Discuss the methodologies used in these cases
- Explain some of the responses to these attacks

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Social Threats	5-20
Attack Methodologies	5-21
Investigative Responses	5-22

Social Threats

Predators

The Internet provides a communication shield that allows people to hide or disguise their true identity. Because users are not seen, they have the ability to misrepresent themselves and lead others to believe they are different than they really are. This has been utilized by predators effectively for years now. Children especially are vulnerable to online predators because they are excited with the technology of the Internet and anxious to make friends quickly.

The problem is not just restricted to young people. Anyone that frequents chat rooms or other online communities is accessible to predators.

Stalkers

Just like predators, stalkers search for victims online and then begin the stalking process. As you saw in previous lessons, the amount of information available to a stalker or predator can be significant.

In some cases, the stalker will not actually be known to the victim until the cycle elevates to dangerous levels. Many stalking cases are discovered after the stalker has been monitoring the victim for some time.

Cyberbullying

The term cyberbullying is a term used in reference to children, not adults. When the Internet is used to bully, harass, embarrass, or demean a child it is considered cyberbullying.

Cyberbullying is a complex topic because the ways it can be perpetrated is only limited by a child's imagination. It should be noted that the roles of the bully and the victim may reverse one or more times during the attack. The investigator may have to review data over a long period of time to determine the start and cause of the attack.

Also note that in extreme cases cyberbullying has led to murder and suicide.

Attack Methodologies

E-mail

E-mail is the preferred initial method for many of the social threat attackers. It is a simple matter to spoof an e-mail or send e-mail from an anonymous source. This causes stress for the victim because he or she thinks the e-mail is from a bad source or unknown origin.

The e-mails may start innocuously and seem like they are from a secret admirer. They usually escalate to disturbing topics and threats depending on the attacker's desires.

Chat

If the attacker can engage the victim in a chat room, he or she can start a conversation that, like e-mail, can seem harmless at first but usually escalates to disturbing levels and even open threats.

It is also possible for the attacker to use wording in chat rooms in such a way as to turn the others in the chat room against the victim. This tactic is common in cases of cyberbullying.

Texting

The ability to send messages and images to and from cell phones is a popular tactic for social threats. Taking pictures of victims in public settings without their knowledge and then sending it to them can cause mental anguish to the victim. In this situation, the victim knows that the criminal was close enough to take the picture. This creates a sense of personal space violation for the victim.

Using text on a cell phone is also a control issue for the attacker, who believes he can reach the victim anywhere and at any time.

Impersonation

Attackers can use identity theft or simple impersonation to publish information on Web sites, forums and chat rooms that appears to be from the victim. This is done to enlist more people in the attack via proxy.

Investigative Responses

Capture	As you investigate social threats, it is important to gather original Web content and e-mail messages. Most e-mail clients and Web-based clients have either a menu option or a button that you can click to view the original content.
Preservation	In some cases you may have to obtain the original e-mail or Web site files and/or the Internet Service Provider logs from the server. This usually requires you to present a preservation letter to the ISP's point-of-contact for law enforcement.
Warrants	Once preservation letters have been delivered, you must obtain the warrants to seize the data. Note that in some cases the data you are trying to obtain may already be deleted from the ISP's server by the time you investigate the crime.
Reporting	First and foremost you should refer to your agency's Standard Operating Procedures for internal reporting methods for these offenses. Depending on your agency, you may be required to report offenses up the chain to State and/or Federal enforcement agencies. In the case of offenses that reach outside the borders of the United States, you should seek assistance from international enforcement groups.
Education	Where possible, provide victims with information on classes or other places where they can obtain assistance on learning how to protect themselves from social threats.

Lesson 5 – Internal Threats

Introduction

Without a doubt, the greatest network threat is the internal threat. Persons with knowledge of the internal workings of a system or company have the greatest capability to cause damage.

Purpose of this Lesson

The purpose of this lesson is to learn how internal threats are perpetrated.

Objectives

After completing this lesson, you will be able to:

- Describe some of the common internal threats
- Discuss the methodologies used in these cases
- Explain some of the responses to these attacks

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Internal Threats Overview	5-24
Investigative Responses	5-26

Internal Threats Overview

Inappropriate Usage

With inappropriate usage of a computer or network, a person violates acceptable computing use policies. Observations that may lead to this classification include:

- Web browsing sessions to Web sites containing unauthorized workplace viewing material
- Inappropriate e-mails sent to coworkers or from a work account
- Installing unauthorized software onto workplace resources

Embezzlement

Embezzlement is the theft or inappropriate use of money and goods provided to a person in trust. Property that is entrusted to an employee which is then used wrongly is an example of embezzlement. Here are other examples of embezzlement:

- Taking equipment home and using it without proper permission
- Installing copies of company software on personal machines
- Using other network assets without proper permission

Extortion

Disgruntled IT managers and others with access to sensitive information within an organization have changed access codes and then held the information hostage in exchange for money, and usually a promise of no prosecution. This is an example of extortion. A fact surprising to many in law enforcement is that these attempts have worked, and continue to work, because companies do not want negative publicity. This is especially true with banks and financial institutions.

Internal Threats Overview, continued

Espionage

If a person is hired by a company or agency to obtain information and pass it on to a competitor or rival government, he or she is guilty of espionage. Like other forms of insider threats, espionage is particularly effective if a dissatisfied employee can be identified and manipulated.

If the information is classified by the U.S. Government, then the charge may be elevated to treason.

Sabotage

When employees feel like they are unappreciated, or have been slighted by the company, they may seek to impact their supervisor or the company in retaliation. The retaliation may come in the form of modified data that negatively affects the company, or in the form of a program that may cause a slowing or stoppage of data within the company.

Some of these attacks are executed in such a way that the employee will make a show of coming in and fixing the problem in order to elevate his status within the organization.

Investigative Responses

Capture

As you investigate internal threats, it is important to obtain as much information from the company or agency as possible. Human resource offices usually have the most to offer an investigator. You should also gather as much original evidence files and material as soon as possible.

Preservation

In some cases, you may have to obtain the original evidence and/or the Internet Service Provider logs from the servers. This usually requires you presenting a preservation letter to the ISP's point-of-contact for law enforcement.

Warrants

Once preservation letters have been delivered, you should obtain on the warrants to seize the data. Note that in some cases the data you are trying to obtain may already be deleted from the ISP's server by the time you investigate the crime.

Reporting

First and foremost you should refer to your agency's guidance or Standard Operating Procedures for internal reporting methods for these offenses. Depending on your agency, you may be required to report offenses up the chain to State and/or Federal enforcement agencies. In the case of offenses that reach outside the borders of the United States, you should seek assistance from international enforcement groups.

Education

Where possible, provide victims with information on classes or other places where they can obtain assistance on learning how to protect themselves from internal threats.

Lesson 6 – Malicious Code

Introduction

Malicious code is the generic term for attacks that use scripts or programs to exploit security vulnerabilities. Worms, trojans, viruses, and backdoors are all examples of malicious code.

Purpose of this Lesson

The purpose of this lesson is to learn how malicious code is perpetrated.

Objectives

After completing this lesson, you will be able to:

- Describe some of the common malicious code threats
- Discuss the methodologies used in these cases
- Explain some of the responses to these attacks

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Malicious Code Attacks	5-28
Investigative Responses	5-29

Malicious Code Attacks

Viruses	A virus is malicious code that is attached to another object, such as an application or document. The virus itself will not run until the object is opened in some way.
Trojans	A trojan horse program appears to be a useful utility or game program that you want, but instead it delivers a malicious program as soon as the utility or game starts.
Worms	A worm is a program which does not need a host program to run or replicate itself. Typically worms use the network to transmit copies of itself to other computers thereby replicating and consuming network bandwidth.
Spyware	Spyware is often recognized as software that monitors the user without his or her knowledge. This definition is certainly true in most cases. However, most spyware can control and direct users as well. This is done by slowing the loading of Web pages that the creators of the spyware do not want the user to see. Some may also divert traffic to a competitor's Web page instead of the intended target.
Adware	Like spyware, adware monitors what the user does. With this information, the creators of the adware display advertisements that they think may be of interest to the user. Programs that display ads until you pay the shareware fee are considered adware as well. Most adware reports back to its owners on the users' activities.
Rootkits	Once an attacker has gained access to a machine, he or she usually installs a rootkit. Rootkits come in different versions depending on what it is the attacker wants to accomplish. Most rootkits install versions of operating system utilities and commands that hide the existence of the attacker on the machine and give the attacker easy access at the same time.

Investigative Responses

Capture

As you investigate malware, it is important to obtain as much of the original evidence data from the victim's machine as possible. Keep in mind that these files may be considered viral. Therefore, you should treat the files with care in order not to infect your forensic systems.

Preservation

In some cases, you may have to obtain the original content and/or the Internet Service Provider logs from the server. This usually requires for you to present a preservation letter to the ISP's point-of-contact for law enforcement.

Warrants

Once preservation letters have been delivered, you should obtain the warrants to seize the data. Note that in some cases the data you are trying to obtain may already be deleted from the ISP's server by the time you investigate the crime.

Reporting

First and foremost you should refer to your agency's Standard Operating Procedures for internal reporting methods for these offenses. Depending on your agency, you may be required to report offenses up the chain to State and/or Federal enforcement agencies. In the case of offenses that reach outside the borders of the United States, you should seek assistance from international enforcement groups.

Education

Where possible, provide victims with information on classes or other places where they can obtain assistance on learning how to protect themselves from malware attacks.

This page intentionally left blank.

Lesson 7 – Denial of Service Attacks

Introduction For some attackers, simply making a resource unavailable is the satisfaction of the attack. The Denial of Service attack is the goal of these criminals.

Purpose of this Lesson The purpose of this lesson is to learn how a Denial of Service attack is perpetrated.

Objectives After completing this lesson, you will be able to:

- Describe some of the common Denial of Service threats
- Discuss the methodologies used in these cases
- Explain some of the responses to these attacks

In this Lesson The following table shows the contents of this lesson.

Topic	See Page
Denial of Service	5-32
Investigative Responses	5-33

Denial of Service

DoS Attack

Denial of Service (DoS) attacks are a common method to attack Web sites and servers. These attacks inundate a Web site with traffic that crashes the server, making the Web site's content and services unavailable. DoS attacks often target major e-business sites in an attempt to prevent customers from accessing the site for hours, or even days, at a time.

Here are several ways in which a Denial of Service attack is accomplished:

- Flooding the target computer with more information than it can handle, causing a system crash or reset
- Interfering with the communications channel in such a way that others cannot access the system
- Starting a number of processes that consumes all available resources on the target system, making the system unable to respond to requests
- Changing access codes to prevent authorized users from accessing the system

Distributed Denial of Service Attack

When multiple systems attack a target system it is called a Distributed Denial of Service Attack. The multiple systems usually are other compromised systems that are controlled by the same attacker. DDoS attacks are normally facilitated by a large botnet that is created for such a purpose, or is leased out from a botnet owner to an attacker for a specific attack.

Investigative Responses

Capture	As you investigate DoS attacks, it is important to gather as much of the original attack information as you can. Ideally, network traffic captures are some of the best sources of investigational data. However, this kind of evidence is rarely available.
Preservation	In some cases, you may have to obtain the original traffic and/or the Internet Service Provider logs from the server. This usually requires for you to present a preservation letter to the ISP's point-of-contact for law enforcement.
Warrants	Once preservation letters have been delivered, you should obtain the warrants to seize the data. Note that in some cases the data you are trying to obtain may already be deleted from the ISP's server by the time you investigate the crime.
Reporting	First and foremost you should refer to your agency's Standard Operating Procedures for internal reporting methods for these offenses. Depending on your agency, you may be required to report offenses up the chain to State and/or Federal enforcement agencies. In the case of offenses that reach outside the borders of the United States, you should seek assistance from international enforcement groups.
Education	Where possible, provide victims with information on classes or other places where they can obtain assistance on learning how to protect themselves from DoS attacks.

This page intentionally left blank.

Lesson 8 – Extortion

Introduction

Creating a sense of fear in a victim and then asking for money to make the fear stop is the goal of an extortionist. The Internet has allowed this old-school criminal activity to continue in a modern medium.

Purpose of this Lesson

The purpose of this lesson is to learn how extortion is perpetrated online.

Objectives

After completing this lesson, you will be able to:

- Describe some of the common extortion threats
- Discuss the methodologies used in these cases
- Explain some of the responses to these attacks

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Extortion on the Internet	5-36
Investigative Responses	5-38

Extortion on the Internet

Direct Threats

One of the oldest methods of extorting money through the Internet is the e-mail threat. The criminal typically sends an e-mail to the victim stating that a murder contract has been taken out on him by an enemy. Then the criminal offers to stop the contract if the victim is willing to pay a certain amount. The criminal usually offers to supply enough information to allow the victim to contact the police and have the enemy arrested.

Other versions of this attack are direct threats against a loved one, a pet or an object of value to the victim. The threat can be anything from causing the object damage or taking the object and demanding a ransom for its return.

Threats Against Tangible or Non-Tangible Data

A criminal can also use extortion by denying access to the owner of an information system by changing the access control of the system. This is sometimes seen as part of an insider threat when an administrator of a system locks the user out of the system and demands something in return for granting access.

Other forms of this type of attack include when the criminal removes data from a system and offers a disk or other media with the missing data in exchange for something. Quite often the data being held in this type of case is something that would be potentially embarrassing or damaging to the victim if it were released to others.

Extortion on the Internet, continued

Threats Against a Web Entity

Yet another type of extortion is when an attacker takes control of a Web server, disables it, and then locks the owners out. The attacker requests a ransom for the key to re-open the system.

Historically, a criminal seldom succeeds in collecting money by holding a Web server for ransom. The usual goal is simply to cause a disruption of service that makes life difficult for the site owner. Only in a few cases has money actually changed hands, and in many of those, the owner still had to rebuild the server to close the vulnerability.

Protection

In some cases, the money is asked for before an attack takes place. This is called “protection” by the attacker and only occasionally is actually paid by the victim. Usually the attack takes place anyway.

Investigative Responses

Capture	As you investigate extortion, it is important to obtain as much of the original evidence as possible.
Preservation	In some cases, you may have to obtain the original e-mail, Web content and/or the Internet Service Provider logs from the server. This usually requires for you to present a preservation letter to the ISP's point-of-contact for law enforcement.
Warrants	Once preservation letters have been delivered, you should obtain the warrants to seize the data. Note that in some cases the data you are trying to obtain may already be deleted from the ISP's server by the time you investigate the crime.
Reporting	First and foremost you should refer to your agency's Standard Operating Procedures for internal reporting methods of these offenses. Depending on your agency, you may be required to report offenses up the chain to State and/or Federal enforcement agencies. In the case of offenses that reach outside the borders of the United States, you should seek assistance from international enforcement groups.
Education	Where possible, provide victims with information on classes or other places where they can obtain assistance on learning how to protect themselves from extortion.

Lesson 9 – Network Attacks

Introduction

Up to this point most of the attacks have been aimed at a person or a specific system or group of systems. Now we will look at the attacks that target the equipment and systems that comprise an entire network.

Purpose of this Lesson

The purpose of this lesson is to learn how network attacks are perpetrated.

Objectives

After completing this lesson, you will be able to:

- Describe some of the common network attacks
- Discuss the methodologies used in these cases
- Explain some of the responses to these attacks

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Network vs. System Level Attacks	5-40
Investigative Responses	5-41

Network vs. System Level Attacks

Attacking a Network

When criminals want to damage a company or agency as much as possible they will attack the network itself. Such attacks will not only disrupt an organization's Internet presence, but also all of its internal communications and productivity. These attacks come in the form of:

- Attacks against routers for the network
- Attempts to compromise Domain Name Servers on the network
- Attacks against firewalls and Intrusion Detection Systems
- Attacks against wireless networking equipment
- Attacks against access control systems for the network

These attacks have the potential to disrupt the communications on the target network. The criminal can disrupt the daily work flow of the target network by changing the equipment that systems use to lookup traffic routing, or sabotaging equipment that allows communication on and with the target network.

Investigative Responses

Capture	As you investigate network attacks, it is important to attempt to obtain any network traffic captures during the attack. In many cases, this information may not be available.
Preservation	In some cases, you may have to obtain the original attack data and/or the Internet Service Provider logs from the server. This usually requires for you to present a preservation letter to the ISP's point-of-contact for law enforcement.
Warrants	Once preservation letters have been delivered, you should obtain the warrants to seize the data. Note that in some cases the data you are trying to obtain may already be deleted from the ISP's server by the time you investigate the crime.
Reporting	First and foremost you should refer to your agency's Standard Operating Procedures for internal reporting methods for these offenses. Depending on your agency, you may be required to report offenses up the chain to State and/or Federal enforcement agencies. In the case of offenses that reach outside the borders of the United States, you should seek assistance from international enforcement groups.
Education	Where possible, provide victims with information on classes or other places where they can receive assistance on learning how to protect themselves from network attacks.

This page intentionally left blank.

Lesson 10 – Terrorism

Introduction

Historical accounts vary but it is generally agreed that terrorism has been on the Internet since its early inception. In modern times, the Internet is widely used by terrorist organizations to communicate and plan attacks and events on a global scale.

Purpose of this Lesson

The purpose of this lesson is to learn how terrorist attacks are perpetrated across the Internet.

Objectives

After completing this lesson, you will be able to:

- Describe some of the common terrorist attacks
- Discuss the methodologies used in these cases
- Explain some of the responses to these attacks

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Internet Terrorist Methodologies	5-44
Investigative Responses	5-45

Internet Terrorist Methodologies

Various Categories

Terrorism is the act or threats of force against civilian populations to create a political or ideological objective. This electronic definition of terrorism falls into many categories and includes crimes we have already reviewed. Terrorists use any methodology available to them and the lines between terrorism and extortion can be easily blurred. However, if you keep in mind that terrorism is the systematic creation of fear in a group of people rather than an individual, terrorism will be easier to detect.

The group can be defined in the simplest terms as being aimed at religious, political and moral groups. If the attacks are designed to instill fear and aimed at a religious group, a political faction, or any other group that is defined by a common relationship, you have a terrorist attack.

Internet Uses

There are several ways in which terrorist organizations use the Internet. Their Web sites are used as psychological warfare, propaganda machines, fundraising opportunities and as messaging centers for coordinating activities. They also use Internet connections for data mining and launching network attacks.

Attacks

Terrorists will use any and all attack vectors if they think it will further their cause. These attacks include:

- Denial of Service attacks against perceived enemies
- Site defacements of Web sites that are counter to their cause
- Spam e-mail attacks against enemies and propaganda e-mail
- Phishing attacks for banking information to help fund activities

The only real difference between many of the attacks you have learned about and terrorist activities are the end uses of the information.

Investigative Responses

Capture	As you investigate terrorist attacks, it is important to obtain as much original evidence as possible.
Preservation	In some cases you may have to obtain the original E-mail or web content and/or the Internet Service Provider logs from the server. This usually requires you presenting a preservation letter to the law enforcement point-of-contact.
Warrants	Once preservation letters have been delivered, you should start on the warrants to seize the data. Note that in some cases the data you are trying to obtain may already be gone from the ISP's server by the time you investigate the crime.
Reporting	First and foremost you should refer to your agency's guidance or Standard Operating Procedures for methods of internal reporting of these offenses. Depending on your agency you may be required, or requested, to report offenses up the chain to State and/or Federal enforcement agencies. In the case of offenses that reach outside the borders of the United States, you should seek assistance from international enforcement groups.
Education	Where possible, provide the victims with information on classes or other places where they can get assistance with learning how to protect themselves from terrorist attacks.

This page intentionally left blank.

Module 6

Phases of an Intrusion

Overview

Network intrusions can be technically complex and difficult to identify. To find traces of an intrusion, it is necessary to understand how intruders conduct their attacks on a system. Many times the hacker will take a very methodical approach by gathering information about a network, probing the network, probing a particular system, attacking the system, and escalating his privileges. Once a hacker becomes entrenched in a system, he can use that system to mine information and launch more attacks against other systems.

Purpose of this Module

The purpose of this module is to provide an overview of the various phases and classifications of an intrusion. You will examine common profiles of an attacker and recognize evidence left behind during the various stages of an intrusion.

Objectives

After completing this module, you will be able to:

- Define a network intrusion
- Explain the phases and goals of an intrusion
- Examine the different attack profiles
- Explain the type of information an attacker can gather with and without actively engaging the target
- Evaluate the goals, strategies, and techniques of various types of attacks
- Evaluate the goals, strategies, and techniques for entrenchment
- Evaluate the goals, strategies, and techniques for extraction

In this Module

The following table shows the contents of this module.

Topic	See Page
Lesson 1 – Defining an Intrusion	6-3
Lesson 2 – Reconnaissance	6-11
Lesson 3 – Network Attacks	6-29
Lesson 4 – Entrenchment	6-45
Lesson 5 – Infiltration and Extraction	6-67

This page intentionally left blank.

Lesson 1 – Defining an Intrusion

Introduction

Technically complex network intrusions can be difficult to identify. To understand how to find traces of an intrusion, you need to understand how intruders conduct their attacks on a system.

Purpose of this Lesson

The purpose of this lesson is to learn the basics of how network intrusions are conducted.

Objectives

After completing this lesson, you will be able to:

- Define a network intrusion.
- Discuss the vulnerabilities that attackers look for in a target

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Definition of an Intrusion	6-4
Goals of an Intrusion	6-5
Attacker Profiles	6-6
Phases of an Intrusion	6-9

Definition of an Intrusion

Intrusion

An intrusion is the act of executing unauthorized actions against an information system and/or its resources.

An intrusion is considered to have taken place when someone gains unauthorized access to a computer. This is an intrusion on a single device and that device is now considered to be compromised. A network intrusion is broader and includes the compromise of multiple devices on a single or multiple networks.

Vulnerability

A vulnerability is a weakness in an information system that could allow unauthorized actions to be taken against that system.

Exploit

An exploit is a tool used by an attacker to perform malicious attacks through vulnerabilities in a system.

For example, an error in an operating system that allows arbitrary code execution is a vulnerability. The program that the attacker writes to perform the attack against that operating system error is an exploit.

Threats and Threat Agents

A threat is a possible source of danger for an information system. A threat agent is a specific person or event that executes unauthorized actions against a system. Listed below are possible threats and threat agents:

- Threats - Insider
 - Disgruntled employee
 - Uninformed employee
- Threat Agents
 - Contractors
 - Recruited or placed agent
- Outsider
 - Hackers
 - Political activist “Hactivist”
 - Information “brokers”
 - Foreign Governments or Corporations
- Natural disasters

Goals of an Intrusion

Goals of an Intrusion

There are several goals of a successful network intrusion. Each can stand alone or can be combined into a blended attack. They can be classified as the following:

- *Denial of Server (DoS)* – An attack that makes a computer resource unable to communicate on the network.
- *Unauthorized Access* – The act of gaining access to any computer resource without the express permission of the owner of that resource.
- *Inappropriate Usage* – The act of using a computer resource in a manner that has been deemed not appropriate for that resource.
- *Other* – These are broad goals that may be difficult to categorize:
 - Suspicious Activity – Any activity that does not conform to the normal prescribed activity
 - Malware – Software designed to infiltrate, monitor, or possibly damage a computer without the owner's consent.

Note: During your cases, you may encounter a combination of two or more goals.

Attacker Profiles

Intruder Types

There are many types of attackers and many reasons why networks and systems are attacked. However, most intruders fit loosely into one of a few categories, which differentiate attackers by skill, resources, and motivation. Understanding these basic intruder profiles may help you identify other compromised systems. The basic intruder profiles are categorized as:

- Advanced
- Intermediate
- Beginner

Advanced

An advanced attacker is very skilled and motivated. Individuals who fit into this category will generally exercise the highest levels of caution and care and will exhibit the following attributes:

- Slow and precise
- Attempt to evade intrusion detection
- Attempt to hide the signs of their presence
- Attempt to mask the source of their attack
- Piggy back on another attacker's data stream
- Misdirection that points to another source
- Program in one or more languages and will modify or create new exploit code or methods to support their objective
- Working knowledge of common system and network architectures
- Have the greatest ability to cause damage throughout a network

This category of attacker can be found in organized crime, terrorist organizations, foreign governments or next door. Their motivation varies, as it tends to match the motivations of the organization. However, intellectual challenge is a common motivation because compromising a network can be like completing a complex puzzle.

Some of the other terms used in this category are: Professional, State Sponsored, Elite.

Attacker Profiles, continued

Intermediate

Intermediate attackers attempt to follow the same methodology as the advanced group, but simply do not possess the necessary skills, knowledge or experience. They exhibit the following attributes:

- Moderate speed and precision
- May attempt to evade intrusion detection
- Attempt to remove signs of their presence, but are more likely to miss something
- Attempt to mask the source of their attack
- May have some programming skills and will be able to perform minor modifications of exploit code to suit their objectives.
- Working knowledge of common system and network architectures

A system administrator attempting to further his or her knowledge and abilities provides an example of an immediate hacker. Other terms used are Amateur and Enthusiast.

Beginner

Beginners are users who are just getting into this arena. They are learning the art and rely on the success and failures of others to teach them the basics. They have a tendency to rely on other people's code and scripts to do their work. Because they do not have a basic understanding of the intrusion phases, their focus is usually on one or two of them. Beginners exhibit the following attributes:

- Usually fast and imprecise
- Will not usually attempt to evade intrusion detection, unless that is a function of the tool they are using
- Will not attempt to hide the signs of their presence, unless that is a function of the tool they are using
- May attempt to mask the source of their attack
- Normally cannot program well, if at all, and will not be able to modify exploit code to support objectives. Instead, the objectives change to suite the code at their disposal.

The motivations for this classification of attacker tend to be game-oriented. A system will be attacked for as little as bragging rights. Other terms used for this attacker are script kiddy, kiddiot, and packet monkey.

Attacker Profiles, continued

Insiders

An insider is a person who has already been authorized to use a network or system, due to his or her part in the organization. Insiders are often underestimated or overlooked as the source of an attack because network security focuses on protecting the network perimeter from outside hackers.

Virtually any disgruntled employee using a valid account could decide to take unauthorized actions against a network. The level of skill is highly varied, but the employee's motivations often include some form of sabotage or retribution.

Phases of an Intrusion

Phases of an Intrusion

There are several traditional phases of a successful network intrusion. Not every intrusion will include all of these phases because the specific actions of the attacker will depend on his or her objectives and abilities. These phases are briefly described below and will be explained in more detail throughout this module.

- *Reconnaissance* – Gathering information about a target
- *Attack* – Gathering, compiling, and launching exploits
- *Entrenchment* – Ensuring continued access to the target system and hiding traces of that access
- *Extraction* – Data theft or enabling channels for outbound attackers to new targets

This page intentionally left blank.

Lesson 2 – Reconnaissance

Introduction

Reconnaissance is the act of gathering the information about a target in order to conduct an intrusion or to continue one already in progress.

Purpose of this Lesson

The purpose of this lesson is to explain how attackers can footprint a target computer system or network before initiating an attack.

Objectives

After completing this lesson, you will be able to:

- Explain the purposes and methods of reconnaissance
- Explain the difference between direct and indirect methodologies
- Discuss some specific tools and techniques used to conduct reconnaissance

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Goals	6-12
Strategies	6-13
Techniques – General Web Browsing and Search	6-14
Techniques – Public Records and Archives Search	6-15
Techniques – Target Web Site Examination	6-18
Techniques – Identifying Physical Attack Vectors	6-20
Techniques – Live Host Identification	6-22
Techniques – Identifying Available Ports/Protocols	6-23
Techniques – Type and Version Identification	6-25
Techniques – Vulnerability Scans	6-26

Goals

Reconnaissance Goals

Reconnaissance is the process of gathering information about a potential intrusion target. This involves identifying any data that will assist in that intrusion. Data is gathered about:

- The target organization, including its main functions, staff members, assets, partner organizations, etc.
- Target individuals, including names, functions, contact information, credentials, etc.
- Target computers and networks, including addresses, functions, installed applications, operating systems, etc.
- Any other information that may be beneficial

Strategies

Direct versus Indirect

Reconnaissance strategies can be defined as “direct” or “indirect.” Direct techniques involve taking actions on or against information systems owned and/or operated by the targeted individual or organization. As such, these actions may be observed and logged by the target.

Indirect strategies are those that do not involve actions on or against target information systems, and therefore will not be observed and logged by the target in most cases.

Reconnaissance Strategies

Strategies used during reconnaissance include:

- Web browsing and searching
- Public records searches
- Target Web site examination
- Identify physical attack vectors
- Live host identification
- Identification of open communication channels
- Operating system and application identification
- Operating system and application vulnerability scans

Techniques – General Web Browsing and Searching

General Web Browsing and Search

General Web searches can be a valuable tool during the information gathering phase, especially when the searches are conducted using data obtained through other reconnaissance methods.

For instance, a staff member's name may have been identified on the target's Web site. Searching for that name through a search engine, such as Google, may produce a home page with personal data or postings on newsgroups and discussion forums. This may in turn yield sensitive company data that should not have been posted on the Internet, such as the staff member's username and hints at passwords.

Searches of online discussion forums, such as Usenet, may also reveal information about an organization's security weaknesses. IT professionals will often post networking questions to online forums in an attempt to solicit advice. Reading these postings can provide information about unresolved security problems.

Possible Artifacts

Searching and browsing 3rd party Web sites will typically not generate any artifacts on the information systems belonging to the target organization or individual. They will leave artifacts on the network that hosts the sites being browsed, most notably a record of URLs accessed during the attacker's research.

Techniques – Public Records and Archives Search

Public Records

Public records are any public source of data maintained by a third party. Relevant public records include:

- Domain Name Service (DNS)
- Whois
- Web site content archives
- Web site defacement archives
- Web server OS and Uptime
- Government business registration sites

DNS

DNS is used to maintain the public record of domain names and the IP addresses to which they correspond. When you Web browse to Microsoft.com, your computer first asks a DNS server how to find that domain name. DNS will respond with the IP addresses that are linked to Microsoft.com. Records kept by DNS include:

- IP address of the Web server(s) that hosts the Web site for a particular domain name
- IP address of the e-mail server(s) that hosts e-mail for a particular domain name
- IP addresses of the DNS servers that are authoritative for a domain name
- Host/domain names associated with an IP address

This information provides attackers with the IP addresses of various servers within an organization that provide specific services (Web, e-mail and DNS), which may be vulnerable to attack.

While DNS queries normally occur automatically when an application requires resolution of a domain name, they can be conducted manually with several applications, including nslookup, which is found natively on many systems.

Techniques – Public Records and Archives Search,

continued

Whois

There are several Regional Internet Registries (RIRs) that are responsible for leasing IP addresses to ISPs and other large organizations. “Whois” is an Internet utility that queries an RIR database for public information, which includes:

- Range of IP addresses assigned to an organization
- Geographical address used when the organization registered for the domain
- Names or handles, phone numbers, and e-mail addresses of the points of contact (POCs) for an organization

There are many Web sites that can be used to perform a whois query. For example www.arin.net/whois/ can be used to directly query the American Registry for Internet Numbers, which covers IP address assignments to the U.S. and Canada.

Web site Content Archives

The Wayback Machine (<http://www.archive.org>) provides archival storage for Web pages that are no longer available through the original provider. An organization may have realized that at some point it included sensitive information on its Web site and subsequently removed the entire Web site. The Wayback Machine offers the ability to check for previous, less security-conscious versions of an organization’s site. There may be other Web site archives available online.

Techniques – Public Records and Archives Search,

continued

Defacement Archives

Defacement archival sites provide information, archives, and statistics regarding Web defacements. An example is Zone-H (<http://www.zone-h.com>). Attackers can use Zone-h to find out if a target has previously been defaced, a record of that defacement, and a listing of the operating system and Web server in use by the compromised server. There may be other such archives available online.

Web Server OS and Uptime Archives

Netcraft (<http://news.netcraft.com>) is a site that provides network and server-specific search functionality. If you enter a domain name, Netcraft will determine the operating system and uptime of the server to which the domain name points. It will also attempt to discover the type of Web server application running and it will provide a record of the results for previous attempts to gather this information.

Government Business Registration Sites

For an organization to be recognized as a business for tax and liability purposes, the federal government and most state governments require several forms to be submitted. These forms may be considered public record and are often searchable on the Internet for information about a potential target.

For example, the U.S. Securities and Exchange Commission maintains the database EDGAR (Electronic Data Gathering, Analysis, and Retrieval) system. Organizations required to file with the SEC have publicly recorded information in the EDGAR database, which can be found at:

<http://www.sec.gov/edgar/searchedgar/webusers.htm>

Possible Artifacts

Searching third-party archive and public record sites will typically not generate any artifacts on the information systems belonging to the target organization or individual. They will leave artifacts on the network that hosts the sites being browsed, most notably a record of URLs accessed during the attacker's research.

It is also possible that queries made against a third-party DNS server will be forwarded to a DNS server owned or operated by the target organization.

Techniques – Target Web Site Examination

Target Web Site Examination

Web sites made available by a target organization can serve an attacker as either a source of general information or as a point of entry into a target network. During recon, the following tactics may be used when reviewing a site.

- Manual browsing
- Automated crawling
- URI prediction/guessing
- Source code review

Manual Browsing

Manually browsing a target Web site is a legitimate method for gathering intelligence about that site and about the organization that runs the site. The disadvantage of such browsing is that it is a direct technique that will leave traces on the target system and network. This can be mitigated by using a browsing pattern that mimics the way a legitimate user might browse the site.

Manual browsing can also be obfuscated by the use of various proxies or routing techniques. This could be through the use of TOR or another type of free proxy, but could also be routed through another previously compromised box. Many of the free proxies have well-known IP addresses and might be blocked by Web servers or firewalls.

Automated Crawling

Web crawlers, which are also known as Robots or Spiders, can be used to automatically browse a site and follow all available links. The results of the Web page download that results from each link is saved for later review. This technique is very obvious to anyone that bothers to read the logs of the target Web server or any associated reverse proxies.

Techniques – Target Web Site Examination, continued

URI Prediction

Not all pages in a Web site are accessible via a link. Pages that are not directly advertised on a site or linked can sometimes be found by guessing at the naming convention used by the site designer.

For instance, if there is a `www.examplesite.com/page1`, then it follows that there may be a `www.examplesite.com/page2`. Guessing these naming conventions can lead to the discovery of additional pages containing valuable data.

Guessing these resources can lead to error logs on the server. These can be generic errors or in the case of a folder that is restricted, security-related errors.

Source Code Review

Other than server side scripts, all HTML/XML markup language and client-side scripts are sent to the Web browser that requests the associated page. This code can be reviewed for information disclosure (e.g., in programmer comments), as well as for weaknesses in the code itself.

Possible Artifacts

Possible artifacts of target Web site examination include:

- Any record of URL requests from suspicious IP addresses or IP ranges in the logs of the Web server or any associated Web proxies.
- Logs that show a broad, systematic pattern of URL requests, which is characteristic of a site being crawled (as observed in Web servers and proxies).
- Logs that show failed URL access attempts that list non-existent files which are close in name to actual existing files. This is characteristic of an attempt to guess at a naming convention. (Again, as observed in Web servers and proxies.)
- IDS alerts referencing Web crawling or other abnormal URL access patterns.

Techniques – Identifying Physical Attack Vectors

Attack Vectors

An attack vector is a pathway through which an attack may be launched.

Physical Attack Vectors

The most common attack vector is via the public Internet, which is a mixture of physical mediums. There are times when specific vectors will be useful or even required, such as when the target cannot be reached via the Internet. Other vectors include:

- POTS (Plain Old Telephone System)
- Wireless
- Direct physical access to the device
- Mixed (any route across the Internet)

Identifying POTS Vectors

War-dialing is identifying computers listening for remote connections on a POTS line. This is done by feeding a set of telephone numbers to a computer program, which will use a modem to dial each of those numbers. If a modem response is received, then there is a computer listening at that number, and further attack actions may be taken against it.

War-dialing a telephone through the POTS system is growing less viable as more systems use dedicated Internet connections rather than dial-up modems.

Identifying Wireless Vectors

Attackers can use a computer with an 802.11 network interface to listen for frames transmitted from 802.11 compliant wireless networks. Because there are different 802.11 specifications, an attacker would have to ensure that their wireless NIC(s) supported all necessary versions. Other wireless specifications are not typically a viable vector, but cellular access to information systems is becoming more prevalent and Bluetooth can be used in very close range situations.

Techniques – Identifying Physical Attack Vectors, continued

Identifying Physical Vectors

An attacker could obtain direct physical access to a target device through obtaining unauthorized access to a building or a room. If the target device is owned by the organization to which the attacker is employed, physical access may already be available.

Possible Artifacts

Possible artifacts of an attempt to identify or test a physical attack vector include:

- Call records that show incoming calls to a phone number with a modem attached
- Standard physical security violations or suspicious activity (e.g., unknown persons in a building, tripped alarms, broken locks, etc.)
- Local console logins recorded in system logs during times when a building was empty, or when the individual to whom the user account was assigned was not present.
- 802.11 frames from an unknown source
- The presence of physical wiretap devices on a cable or device

Techniques – Live Host Identification

Live Host Identification

Live host identification is the process of finding target hosts and verifying that they are online and responding to communication requests. This can be done through several methods:

- ICMP (Internet Control Message Protocol) probes/sweeps
- TCP/UDP probes/sweeps
- Network monitoring

ICMP Probes/Sweeps

ICMP is a protocol used primarily for network troubleshooting, and is commonly used to test hosts to see if they are online. The ICMP “Echo Request” packet is used to sweep multiple IP addresses to elicit an “echo response” packet from available hosts. This is also called a “ping sweep.” In an effort to pass through firewalls that block ICMP Echo Requests, other ICMP packet types may be used to elicit a response from a target host.

TCP/UDP Sweeps

Modern networks sometimes block ICMP at external perimeter defenses, such as firewalls and routers. To circumvent this barrier, TCP and UDP packets can be sent instead.

Network Monitoring

Passively monitoring a network from a compromised system can also be used to identify other hosts inside a network. The amount of traffic collected and number of hosts identified will depend greatly upon where the sniffer is placed within the logical network architecture.

Possible Artifacts

Possible artifacts of live host identification include:

- IDS alerts referencing broad scans or sweeps
- Firewall logs that show blocked packets attempting to reach a large number of hosts in a short period of time
- Firewall logs that show traffic blocked based upon abnormal protocol options (unusual ICMP types, TCP ACK packets existing outside of a session, etc.)

Techniques – Identifying Available Protocols/Ports

Ports/Protocols

Once a physical vector is identified, and a target has been verified as being online, an attacker may choose to enumerate the logical methods by which the target computer is willing to communicate. These methods include:

- Accepted network and transport protocols (ICMP, TCP, UDP)
- Accepted application protocols (HTTP, FTP, SMTP, etc.)
- Accepted TCP/UDP port numbers

Identifying Accepted TCP/UDP Port Numbers

Also called “Port Scanning,” connection attempts can be sent to TCP and UDP ports to determine if there is an application listening on that port. Responses may include one of the following:

- A scanner will attempt to initiate a TCP session to multiple ports. If the remote computer responds to the request with a TCP syn/ack packet, then there is an application or OS service listening on that port.
- A scanner will send packets to UDP ports to test to see if they are opened. Since UDP is connectionless, these packets will either be empty, or contain data that is not valid for the protocol normally used with that port. If the port is opened, the application listening on that port will respond, if it is not open, an ICMP Destination Unreachable message will be sent.

Note: Firewalls may behave differently when they block a connection attempt, dropping packets (no response) instead of allowing the destination computer to respond.

Techniques – Identifying Available Protocols/Ports

Possible Artifacts Possible artifacts of port/protocol scans include:

- IDS alerts referencing port/protocol scans.
- Firewall logs showing blocked attempts to access a large number of ports on a single host, especially if they are in close sequence or if the requests occur during a short period of time.
- A TCP session that is initiated to an IP address and then immediately terminated, and not followed by any additional communication. This sequence would be observable in a sniffer log.
- A TCP session that is only half set up and then abandoned is potentially observable in a sniffer log.

Techniques – Type and Version Identification

Type and Version Identification

Once an open communication channel to a device has been established, the attacker may need to know the type and version of the listening application and/or operating system. This is because attack methods are highly dependant upon target versions and patch levels. Common methods for identifying this information include:

- Banner grabbing
- Packet printing

Banner Grabbing

Banner grabbing is the process of connecting to commonly available services that provide type and version information in their greeting messages.

Packet Printing

The TCP/IP stack is the part of the operating system that controls any TCP/IP network communication. Because the implementation of the stack is different on every operating system, this produces minor variances in the operating system's response to certain network requests.

Scanning tools that perform packet printing (or fingerprinting) check for these variances on a target host to identify its operating system. Common TCP/IP attributes that can be used for packet printing include:

- ICMP Error Messages
- TCP Sequence Numbers
- TCP Options
- TCP Timestamps
- TCP Retransmissions Timeouts
- Fragmentation Handling
- IPID Values

Possible Artifacts

Possible artifacts include:

- IDS alerts referencing scans
- Errors in the logs of the scanned application or service referencing communication problems or incomplete connection attempts

Techniques – Vulnerability Scans

Targets for Vulnerability Scans

Vulnerability scans are probes that test specific applications or operating system services for possible vulnerabilities by issuing application or service-specific commands that may reveal known weaknesses in the software. Commonly scanned services include:

- Web servers and FTP servers
- E-mail servers
- File and database servers
- Directory service servers
- RPC
- Print services
- Simple services

Vulnerability Scan Techniques

The purpose for scanning applications is tied to the nature of the program. For instance, a database server may be scanned for the ability to access data without authenticating, whereas an e-mail server may be scanned for its ability to be used as a spam relay.

Vulnerability scans look for the presence of known vulnerable application component files, as well as the ability to:

- Traverse into normally non-accessible directories on the host operating system
- Access unauthorized files
- Execute unauthorized code
- Make unauthorized calls to backend application or database servers
- Route unauthorized data, such as spam or another probe, through the server
- Trigger backchannel communication, a communication session originating from the target to the hacker

Techniques - Vulnerability Scans, continued

Possible Artifacts Possible artifacts of vulnerability scans include:

- IDS alerts referencing a possible vulnerability scan
- IDS alerts referencing any attack. Some vulnerability scans launch partial attacks to determine if they are possible, and this may trigger an IDS.
- Any extremely large volume of traffic that is also widely varied. This is characteristic of a comprehensive, multi-protocol, blatant vulnerability scan.
- Any other activity characteristic of any form of attack, as seen in the next lesson of this text.

This page intentionally left blank.

Lesson 3 – Network Attacks

Introduction

In the attack phase, an intruder takes the actions necessary to gain unauthorized access or privilege to a network, or damage a system.

Purpose of this Lesson

The purpose of this lesson is to explain how an attacker gains control of a system or data resource, or executes a denial of service attack against that resource.

Objectives

After completing this lesson, you will be able to:

- Explain the goals of an attack
- List the major strategies used to conduct an attack
- Explain some of the specific techniques that an attacker can use to obtain control or elevated privilege
- Explain some of the specific techniques that an attacker can use to damage the functionality of a system or network

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Goals	6-30
Strategic Categories	6-31
Strategies – Authentication Attacks	6-32
Techniques – Factor Guessing/Cracking	6-33
Techniques – Credential Recover/Reset	6-37
Techniques – Credential Injection	6-39
Techniques – Credential Theft	6-40
Strategies – Unexpected Input	6-41
Techniques – Excessive Input	6-42
Techniques – Excessive Input / Buffer Overflows	6-43
Techniques – Unexpected Input Content / XSS Attacks	6-44

Goals

Entrenchment Goals

An attack is an action taken to further one of the following goals:

- **Unauthorized Access:** Obtaining access to a resource (i.e., system, network, data, etc.) that is illegal, against policy, or otherwise unauthorized by the organization or individual owning that resource.
- **Access Privilege:** Obtaining the ability to manipulate a resource (i.e., change, delete, deactivate, etc.) to an extent not authorized by the organization or individual owning that resource.
- **Denial of Service:** Preventing a resource from being available to fulfill its purpose either temporarily or permanently.

Unauthorized access and privilege are often both goals of the same attack. In many instances, they can be achieved through a single attack technique. Other times, an initial attack is used to gain access, and subsequent attacks are used to obtain the proper privilege.

Terminology Note

The term “Denial of Service” (DoS) is often used to indicate an attack that is performed by flooding a network link or interface. The term “Distributed Denial of Service” (DDoS) is used when this attack is sourced from many different hosts.

This text uses the term denial of service in the general sense of any action that prevents a target from performing its normal actions within its normal time frame.

Strategic Categories

Entrenchment Strategic Categories

There are many different ways to compromise a system or network. Most attack strategies fall into one of the following broad categories, although there are exceptions:

- **Authentication Attacks:** Attacks against an authentication mechanism for the purpose of obtaining credentials to a system or network.
- **Unexpected Input:** Supplying input in a way that will cause an application or operating system to behave in an unauthorized fashion, either to gain unauthorized access or to disrupt the functionality of the target system.

Strategies – Authentication Attacks

Authentication Attack Strategies

Authentication attacks use the following strategies, which will be explained later in this lesson. In addition to these, an attacker may simply already be authorized to use an information system either based on explicitly granted credentials, or based on the fact that a system does not require authentication.

- Factor guessing/cracking: Attempting to determine the factors (e.g., passwords) that will allow the attacker to successfully authenticate to a system.
- Credential recovery/reset: Taking actions that will cause a system or administrator to either resend a set of credentials to an attacker, or simply send the current credentials to an attacker.
- Credential injection: Creation of new credentials that will allow authentication into a target system.
- Credential theft: Theft of credentials either through inadvertent disclosure or methods such as sniffing network traffic.

Authentication and Authorization

Authentication attacks focus on obtaining a set of credentials for a specific individual or account, or being authenticated as that person or account without credentials. What the attacker is able to do once this has been accomplished will depend on what the compromised/unauthorized account is allowed to do. If an attacker requires more authority on a system or network, then he or she will have to use another authentication attack or try a different attack strategy.

Techniques – Factor Guessing/Cracking

Authentication Factors

Authentication factor is a piece of data that is used to identify an individual, and authenticate him into an information system. Most authentication factors fit into one of the following categories:

- “Something you know”: Usernames, passwords, pass-phrases, answers to secret questions, etc.
- “Something you have”: USB tokens, smart cards, RFID tokens, cookies, encryption keys, etc.
- “Something you are”: Retinal patterns, thumbprints, DNA, etc.

Usernames and passwords are still the most common authentication factors.

Guessing/Cracking

One of the most direct ways to access an information system is through an already existing channel with legitimate credentials. Obtaining the credentials is sometimes as simple as guessing at the value, and attempting to authenticate. If the authentication fails, you guess again. This is sometimes called a “password attack.” However, the general method can be used for factors other than passwords.

Factor guessing or cracking techniques require taking the following actions:

1. The attacker generates a set of values that represent possible legitimate authentication factors.
2. The attacker tests those values against the authentication system or a stolen set of password hashes to determine which ones are correct, if any.

Techniques – Factor Guessing/Cracking, continued

Value Generation There are several techniques used to generate the values that will be tested against an authentication system:

- **Brute Force:** Guessing every possible value for a credential using any combination of acceptable characters. For instance, if attempting to guess a password, you might begin with “a” – “z”, then “aa”, then “ab”, etc.
- **Dictionary:** Using only words from a dictionary to generate a list of potential values. Some dictionary attacks will also allow for small variances such as common misspellings in the list of potential values.
- **Hybrid:** Using any combination of brute force and dictionary methods for value generation.
- **Pattern Recognition:** For server/administrator assigned factors (especially mathematically generated factors) that follow a pattern, an attacker could use the pattern to guess the values of other valid factors. Assigned factors include items like cookies and URLs. Patterns can also be recognized in user-created factors. For instance, administrators may always assign new users their last name as their initial password, forcing the user to change it upon first login.
- **Pre-generated Hashes:** When the authentication factor is a hash value of another piece of data, such as the hash of a password, a list of all possible hashes for a set of values can be pre-calculated. The term “rainbow table” is used to refer to some types of pre-generated hash sets.

The data type for the values depends on the authentication factors required by the system. ASCII characters are used for passwords and usernames, whereas long numbers or hash values might be used to represent codes found in tokens.

Techniques – Factor Guessing/Cracking, continued

Value Testing

Once an attacker has decided upon a value set, then those values must be tested against an authentication system. This can be done by:

- Manually typing the values in, one at a time.
- Using an automated tool such as THC Hydra to pass test values to the authentication system as fast as possible, or with a specific timing. Automated tools may be the only method available when attempting to emulate a token.
- Using hashes calculated against values in a set of data and comparing them to hashes stolen from an authentication system or used by an authentication system.

Value Testing and Session Length

When a session is underway and an individual or application is authenticated, that session will sometimes last for a specific amount of time. If credentials are successfully guessed/cracked, they may only be good for the length of a session already in progress.

This is more likely the case when the factor is a temporary token, such as a cookie. For example, an attacker could guess at the proper value of a cookie used for authenticating to Web mail. But the cookie may have expired if the interface to the account has been inactive for a certain period of time.

Techniques – Factor Guessing/Cracking, continued

Possible Artifacts	<p>Possible artifacts of authentication factor cracking or guessing include:</p> <ul style="list-style-type: none">• Large numbers of failed authentication attempts for a single account, as seen in the logs of the authentication system (e.g., The Windows Security Event Log, or the /var/log/secure file on a Linux or Unix system with SSH).• Failed authentication attempts for one or more non-existent user account names, as seen in the logs of the authentication system.• Failed authentication attempts that show a series of passwords that match a pattern indicative of an attack, such as the “aa”, “ab”, “ac”, etc. that might be seen in a brute force value set. Authentication logs do not always record the password that was entered, but they may be visible in a network sniffer log.• IDS logs referencing a password or authentication attack.• User accounts that are locked out due to an unusually high number of failures.• A list of passwords or password hashes found in a text file in an abnormal location.• The presence of password/hash dumping utilities such as pwdump (pwdump.dll).• Authentication attempts (successful or failed) at abnormal times, or for which the authorized user of the account does not recall.
---------------------------	--

Techniques – Credential Recovery/Reset

Credential Recovery and Reset Mechanisms

People lose their credentials (i.e., authentication factors). They tend to forget their passwords, lose their tokens and sometimes cannot remember their user names. To account for this, most authentication systems include a mechanism for either resetting a user's credentials to a new value, or for recovering a copy of lost credentials. These credential recovery and reset mechanisms include:

- Password reset links on Web sites that allow you to have your password, or a reset link e-mailed to the address attached to a given account.
- Password reset links on Web sites that will reset a password if you know the answer to a “secret question.”
- Help desk staff (available by phone or in person) that will reset or unlock an account.
- Operating system and directory user account management interfaces that allow an account with sufficient privilege to reset the credentials to any other account on the system or in the directory.

Techniques – Credential Recovery/Reset, continued

Credential Recovery/Reset Attack Techniques

Examples of credential recovery and reset attack techniques include:

- Requesting a password reset, and then capturing the password from network traffic as it is sent to the user.
- Registering a domain name previously belonging to another person, recreating a previously existing e-mail address at that domain name, and using that e-mail address as an authentication factor and recipient for reset credentials transmissions.
- Directly requesting an individual's credentials, while using personal information about that individual (birth date, mother's maiden name, etc.) as authentication factors necessary for the reset.

Possible Artifacts

Possible artifacts of attacks against credential reset and recovery mechanisms include:

- Successful authentication attempts for an account that was believed to be no longer in use, as seen in the logs of the authentication system
- Password resets for an account that was believed to be no longer in use
- Password resets for which the legitimate user of the account claims to not be responsible

Techniques – Credential Injection

Credential Injection / Modification

Almost all systems that include a mechanism for authenticating users and programs also include a mechanism for creating new accounts when necessary. If an attacker has access to this mechanism, he or she can use that mechanism to create new accounts. Techniques for accomplishing this include:

- Calling a help desk and requesting the creation of an account. This will usually require that the attacker masquerade as someone who can legitimately request such an action.
- Using an online mechanism to request an account. This can be done to gain initial access to information on Web sites that provide information as long as you register and sometimes pay. Some Web sites might require that you validate your identity for registration, using some type of personal information. Others allow you to input whatever information you choose to provide.
- Directly creating user accounts using an available administrative utility (e.g., the Active Directory Users and Computers console), or by directly inserting them into a list of users (e.g., /etc/passwd).

Possible Artifacts

Possible artifacts of credential injection and modification include:

- Existence of a user account in an account repository for which there is no legitimate authorized user.
- Existence of a user account in an account repository that does not match the account naming convention for the organization.
- Recorded logins of an account for which there is no legitimate authorized user as seen in OS or application security/authentication logs.
- Log entries referencing account creation.

Techniques – Credential Theft

Credential Theft	<p>Authentication factors may also be stolen. Possible techniques used to accomplish this include:</p> <ul style="list-style-type: none">• Capturing credentials as they are transmitted across a network. In order to sniff the traffic, this requires that the attacker have control or be present on one of the network mediums through which the credentials are sent.• Tricking an individual into revealing his or her credentials by contacting the individual in person. For example, an attacker might claim to be a system administrator or security representative that needs a user's credentials for some kind of troubleshooting or verification.• Tricking an individual into revealing credentials by sending an electronic request for the information. For example, an attacker might send an e-mail that has been falsified to appear to be from a legitimate bank or online service.• Physical tokens such as ID cards and USB tokens can be physically stolen.
Possible Artifacts	<p>Possible artifacts of credential theft include:</p> <ul style="list-style-type: none">• Reports of the theft of physical credentials by a user, or reports of the disclosure of credentials to someone the user believed was authorized to request such information.• Successful authentication requests at abnormal times, or for which the authorized user of the account does not recall.• Existence of e-mails in an e-mail repository or logged by a proxy that include requests for credentials, or links to Web pages where such requests are made.

Strategies – Unexpected Input

Unexpected Input Strategies

Strategies that use unexpected input to conduct an attack are listed below. Each will be described in further detail on following pages.

- **Excessive Input:** Sending more input than a system or application was expecting, or is able to handle.
- **Unexpected Input Content:** Sending input content that a system or application will process incorrectly due to the inability to recognize and/or properly control the input type.
- **Unexpected Input Timing:** Sending input at times that a system, application or communication session is temporarily vulnerable to interference.

Techniques – Excessive Input

Excessive Input

A basic attack method is to supply an excessive amount of input to an application, operating system, or network. The effect of this input could be to simply crash the target. Excessive input could break a control system and allow the attacker to perform additional unauthorized actions. Techniques for supplying excessive input include:

- Buffer Overflow Attacks
- Flooding

Input Size Validation

All attacks that use excessive input to influence target behavior take advantage of a lack of input validation. Properly coded applications should verify that any user-supplied input is of the proper size, and if not, truncate that input or simply produce an error message and/or stop the process. Likewise, network devices should terminate or block all communication from hosts that are supplying an excessive number of packets or service requests.

Techniques – Excessive Input/Buffer Overflow

Buffers

A *buffer* is a temporary storage area, usually in RAM, allocated for the manipulation of data within a process. For example, when logging into an e-mail server, there might be a 32-character space for your user name. This limitation is established in the code of the e-mail server application and controls how much input will be accepted from the user.

Buffer Overflow Attack

A buffer overflow attack purposely sends an entry too large for the buffer to hold. It sends it in such a way that a portion of the entry is written to the target computer where program instruction code is stored.

An attacker uses this method to intentionally cause the execution of his code. The result of this code execution could be anything, but will often be a denial-of-service, a command terminal session sent back to the attacker's computer or the injection of a DLL (dynamic link library) or other program code into the remote process.

Possible Artifacts

Possible artifacts of buffer overflow attacks include:

- Unexplained errors in the log files for the application or service that was attacked. If an OS service was attacked, then these log entries may exist in the operating system's main log files, or supplementary crash logs (such as Dr. Watson).
- Intrusion detection system alerts indicating a buffer overflow, shellcode or NOOPs.
- Sniffer logs that show large blocks of repetitive data, such as 0x90 or other hex values.
- Sniffer logs that show blocks of data that do not conform to normal rules for the network protocol being used.
- IDS alerts or sniffer logs showing common post-attack events such as reverse shells, DLL transfer, OS commands, etc.

Techniques – Unexpected Input Content / XSS Attacks

Web Scripting

Program code executed in the context of a Web page, either by the server or the client system, is called a Web script.

Cross-Site Scripting (XSS)

Cross-site scripting occurs when an attacker supplies a script that is executed by another system's Web browser or in another browser window accessing a different site. There are several ways of accomplishing this. Possible techniques include:

- An attacker posts a script to a Web site that will permanently store the script, and serve it to other systems when they request the Web page to which it was posted. This allows the attacker to run code in another person's browser. These are called "persistent" or "stored" XSS attacks.
- An attacker will embed script in a URL that, if loaded by another user, will cause a Web server to supply malicious code to the requesting browser to be executed in the context of the requested page. These are called "non-persistent" or "reflected" XSS attacks, and rely upon a user or browser to load the URL.

Possible Artifacts

Possible artifacts of XSS include:

- IDS alerts referencing an XSS attack.
- URLs containing scripting (such as the presence of the "<script>" tag), as seen in Web server and proxy server logs, or in Web browser history.
- Web pages containing embedded scripting, as seen in proxy server logs where the proxy records full page.
- Unusual character encodings in URLs as seen in Web server or proxy server logs, or in Web browser histories.

Lesson 4 – Entrenchment

Introduction

Continued, undetected control over a compromised system is required for any extended operations such as data mining and theft, or further penetration into a larger network.

Purpose of this Lesson

The purpose of this lesson is to explain how an attacker retains remote control of a system and hides or removes any traces of that control.

Objectives

After completing this lesson, you will be able to:

- Explain the goals of entrenchment
- List the major strategies used to conduct entrenchment
- Explain some of the specific techniques that an attacker can use to maintain remote access and control
- Explain some of the specific techniques that an attacker can use to hide traces of unauthorized activity

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Goals	6-46
Strategies	6-47
Techniques – Log Cleaning	6-48
Techniques – Automatic Execution	6-50
Techniques - Hooking	6-52
Techniques – File Type Manipulation	6-54
Techniques – Naming Conventions and Placement	6-55
Techniques – Remote Connectivity	6-58
Techniques – File System Date/Time Stamp Manipulation	6-62
Privilege Escalation	6-63

Goals

Entrenchment Goals

The access resulting from a successful attack can sometimes be tenuous. A buffer overflow may have resulted in a Windows command shell back channel that will be lost if the user decides to shut down or reboot the target system. An attack against Internet Explorer (IE) may last only as long as the IE window stays open. Despite these scenarios, an intruder may require extended access for more extensive operations.

Entrenchment is the process of solidifying access to a compromised system, and is used in pursuit of the following goals:

- **Attack Pivot Point:** The attacker requires continued control of the system to use it as a pivot point from which to attack other systems and networks.
- **Data Theft:** The attacker requires continued control of the system to perform data mining operations on that asset and any local storage media.
- **General Control Maintenance:** The attacker wants to maintain control of the system as an asset for various other uses as required or for a future undetermined use. For example, an attacker may simply want to maintain control of a network in order to disrupt it during a future conflict.

Entrenchment Goal Attributes

Regardless of goals above, entrenchment requires that the attacker retain some ability to remotely control or manipulate the target, and also for that method of control to remain undetected.

Strategies

Entrenchment Strategies

Activities conducted during entrenchment include:

- **Log Cleaning:** Removing records of unauthorized activities to hide attacker presence.
- **Automatic Execution:** Adding configuration changes that will cause unauthorized programs to start when the host OS boots, or restart if they are unexpectedly terminated.
- **Naming Conventions and Placement:** Naming unauthorized files, processes and configuration changes in such a way that they appear legitimate or otherwise benign.
- **File Type Manipulation:** Changing the attributes which identify a file's type, such as the signature and extension.
- **Hooking:** Intercepting calls to the operating system to interfere with any data returned, such as lists of files or processes.
- **Remote Connectivity:** Maintaining one or more channels through which a compromised system can be remotely controlled.

Entrenchment and Unauthorized Code

Because of the requirement for persistent control of a compromised system, entrenchment activities typically involve the installation of some sort of unauthorized code. This code will serve to perform one or more of the functions identified above including when a human attacker is not currently administering the system. Common types include backdoors, rootkits and trojans.

Techniques – Log Cleaning

Log Cleaning

To entrench properly, an attacker must remove records of unauthorized activity. A common record of unauthorized activity is a log entry. Log cleaning is the process of deleting individual log entries, or clearing entire log files to achieve this goal. This can be done manually, with specific log cleaner malware, or with a general-purpose rootkit.

Log Cleaning – Record Deletion

The most precise method of log cleaning is to delete individual log entries (records) that correspond to the activity that needs to be hidden. By deleting those records and leaving all others, there is a better chance that the act of log cleaning will go undiscovered.

Removing individual records is easy with text logs. The attacker simply needs to open the log in a text editor, delete the associated lines and save the file. Proprietary log formats are much more difficult to handle. To remove a record, either the attacker (or his or her tools) must understand the format of the log, and be able to identify the beginning and end of each entry. The log viewers that correspond to proprietary logs (e.g., The Windows Event Viewer) do not typically include a function for removing an individual line.

Note: If an attacker can open individual records, he or she may be able to change the content of an individual record instead of deleting it. This could be used to achieve the same goals.

Log Cleaning – Log Clearing

An alternative to deleting individual records is to clear an entire log. The log file itself is left, but all records within are removed. This is done in situations where the attacker is in a hurry or does not have a mechanism for deleting individual records. Some log viewing applications include a mechanism for clearing all records. Within the Windows Event Viewer, you can clear a log by right clicking on the log name and choosing “Clear All Events.”

The downside of log clearing is that it is quite noticeable. Therefore, record deletion is preferable. You may also find that an attacker may clear a log when he or she is not as concerned with hiding the intrusion as with removing any information that can be used to trace the attack back to its source, although this is not characteristic of entrenchment.

Techniques – Log Cleaning, continued

Log Cleaning – File Deletion

In lieu of record deletion or log clearing, an attacker may choose to delete an entire log file. This is the least desirable of log cleaning methods, as the deletion of an actual log file is the most noticeable, and may cause system errors or crashes. It is more useful when dealing with more obscure log files that are not as likely to be noticed. For example, an administrator is much less likely to notice that a Dr. Watson dump log has been deleted than a missing IIS Web server log file.

Log Cleaning – Possible Artifacts

Possible artifacts of log cleaning include:

- File system date/time stamps: File system date/time stamps may be changed during log cleaning. For example, if a log were cleared, the NTFS last written time would be updated on a Windows system at the time of the clearing, meaning that the attacker may have been active on the system at that time.
- Time gaps: Log files that have had specific entries removed may have abnormal time gaps between remaining entries.
- Empty or completely missing log files
- Log entry recording the deletion: For example, Event ID 517 corresponds to the clearing of all entries in the Windows Security Event Log for Windows 2000/XP/2003. It is only added when the administrator user account performs the deletion.
- Existence of malicious code on a system that includes log cleaning as one of its functions.

Techniques – Automatic Execution

Automatically Starting Malware

Computers, especially workstations, are often shut down or rebooted. Sometimes they simply lose power. Furthermore, individual processes are sometimes terminated by anti-virus software or by a suspicious user or administrator.

Starting Processes at Boot: Registry Entries

It is extremely common for malicious code to be installed to automatically start when Windows boots. The main mechanism for accomplishing this is by adding a Registry key that will start an executable file as a new process or load a library into another process.

There are dozens of Registry keys that can be used to run code. Some of the more common methods include creating “Run” keys for executables, installing a new service, or trojanizing a legitimate service by changing the ServiceDLL key to load a malicious DLL. See the appendices for a full listing of relevant Registry keys.

Run key:

HKLM\Software\Microsoft\windows\CurrentVersion\Run

Services:

HKLM\System\ControlSet***\Services\<service_name>\ImagePath

HKLM\System\ControlSet***\Services\<service_name>\Parameters\ServiceDLL

*** Represents a number, usually 001, 002 or 003. That number corresponds to one of the control sets used by the Registry for configuration. There is a typically a “current control set,” and another set representing the last known good configuration.

Techniques – Automatic Execution, continued

Directories

During boot, Windows checks certain directories and executes any files found there. Depending on the version of Windows, directories that are checked at boot may include:

- C:\Documents and Settings\All Users\Start Menu\Programs\Startup
- C:\Documents and Settings\<username>\Start Menu\Programs\Startup
- C:\Windows\Tasks

Job Scheduling

Most operating systems include a mechanism for scheduling executions to occur with various triggers, usually date/time. For Microsoft operating systems, this is the Windows Task Scheduler. For Linux/Unix derivatives, this is the “cron” daemon.

Possible Artifacts

Possible artifacts of malware configured to auto-start include:

- Existence of Registry entries that load unauthorized executables or libraries
- Unauthorized executables in auto-start directories
- Unauthorized executables specified in an INI file used by Windows or another automatically started program
- The existence of “.job” files on Windows which represent a Task Scheduler (Usually found in C:\windows\tasks or C:\winnt\tasks). The log file SchedLgU.txt also keeps a record of Tasks Scheduler job executions.
- Entries in the “crontab” file in Linux/Unix derivatives, which contain a list of scheduled cron jobs.
- Malicious code that is found on the system which adds automatic start configurations when executed.

Techniques – Hooking

Hooking

Hooking is the process of intercepting calls from one program to another to interfere with any data exchanged. This can be used to hide data such as processes, files and specific file contents.

The OS API

An API is an Application Programming Interface. Operating systems provide an API in order for programs to run on and interface with the operating system. Common functions that use this interface include operations such as:

- Directory listings
- File copy and move operations
- File editing operations
- Network sending and receiving
- Process and thread starting, stopping and enumeration

For example, when you use Windows Explorer to view the contents of a directory, this is done via a standard API call from explorer.exe to a Windows OS DLL file.

These operations are common during every day usage of any given OS. They are important during entrenchment, because these same API calls can be used to find malicious code. It is therefore important to prevent these calls from revealing signs of malware presence.

OS API Hooking

Rootkits can be used to hook these API calls by intercepting them at various points. Sensitive values can then be edited out of any returned values. For example, a call used to obtain a directory listing from C:\windows\system32 may be intercepted, and the name of the unauthorized .exe and .dll files that make up the rootkit and backdoor programs could then be removed from the results.

Techniques – Hooking

Possible Artifacts Possible artifacts of API hooking include:

- OS files that have been hooked through direct modification of the file on disk will have hashes that do not match those in hash sets of known-good executables.
- For live systems, the results of API directory listings and Registry key enumerations can be verified by directly checking the file system for the same data (e.g., looking for files by reading the file table itself rather than asking the OS). Mismatches indicate the potential presence of API hooks in memory. This technique is used by some rootkit detection programs such as Rootkit Revealer.
- Discovery of API hooks during the analysis of malicious code files found on a compromised system.

Techniques – File Type Manipulation

File Types

There are many different types of files found on a computer, such as text files, executables, database files, office documents, etc. When a user opens a file, the operating system first determines the file type. Depending on the operating system, this is done by checking either:

- **File Extension:** Series of letters at the end of a file name, separated from the actual name by a period. Used primarily by Windows variants to determine file type.
- **File Signature:** Series of bytes in the file, usually at the very beginning or end, that marks the file type. Used primarily by Linux/Unix variants to determine file type.

As an example, a GIF image file could be identified either by the “.gif” file extension, or by the characters “GIF89” found at the very beginning of the file.

File Type Manipulation

The attributes that define a file’s type can be manipulated to hide that file from general searches and from some specific forensic analysis strategies. Techniques for manipulating file type include:

- Changing the file extension to make the file appear to Windows or a casual observer as a different file type. For example, an executable may be disguised by changing its file extension from “.exe” to “.doc”.
- Changing the file signature to make it appear as a different file. For example, the “GIF89” at the beginning of an image could be changed to “MZ” to make it appear to be an executable to someone conducting file signature analysis.

Possible Artifacts

Possible artifacts of file type manipulation include:

- File signatures that do not match the extension, or vice versa.
- Files that have a matching signature and extension, but which cannot be read by the appropriate application.

Techniques – Naming Conventions and Placement

Naming Conventions and Placement

Some of the simplest methods for hiding unauthorized files, processes and configuration changes are to name them something that appears benign or to place them in a location where they are less likely to be noticed.

Naming Convention Strategies

Naming conventions used to hide activity include:

- Giving files/processes the same name as a legitimate file or process.
- Giving files/processes a name that is slightly modified from the name of a legitimate file or process. For example, a file may be named `lsas.exe`, which is similar to the legitimate file `lsass.exe`.
- Assigning a name that appears similar to the names of other files. For example, there are many DLLs in the System32 directory. Most of those DLLs have names that are not recognizable to most users and administrators. An attacker could assign an unauthorized DLL a random 8 character name, and it would probably go unnoticed.
- Use of special characters within names that will either cause the name to blend in with other files, or will cause the name to not be rendered in certain interfaces. For example, a directory could be created named `...`, which would blend in with the `.` and `..` directories that refer to the current and parent directories respectively.

Techniques – Naming Conventions and Placement,

continued

Placement Strategies

Placement strategies include:

- Placing unauthorized files in a directory where an average user is unlikely to look.
- Placing unauthorized files named a certain way into a directory with other files with similar names. For example, DLLs could be placed into System32 along with many of the other DLLs found on a Windows system. There they will be more difficult to identify.
- Using directory names that are normal, but are in the wrong location. For example, because the name “temp” is commonly used for directories, a new directory named temp created in any location would not stand out to most individuals.
- Storing files or file fragments in disk space not currently in use (slack or unallocated space).
- Fragmenting a file and inserting it into another file in small amounts so that the host file can still be opened and read (steganography).

Techniques – Naming Conventions and Placement,

continued

- Possible Artifacts** Recognizing naming conventions used to hide unauthorized activity relies heavily upon your knowledge of what is normal and not normal within the directory structure and running processes of an operating system. Common artifacts include:
- File names, Registry keys and process names that appear to be misspelled or in the wrong location.
 - Files with normal names that do not have the appropriate hash value or file signature.
 - A process that seems to be running in more than one instance when that is not typical, or when a process is a child of itself.
 - Abnormal capitalization patterns in names. For example, Winhex could be spelled wInhex.
 - The presence of programs on the system used for file hiding.
 - File names and directory locations discovered during the analysis of malicious code found on a compromised system.

Techniques – Remote Connectivity

Communicating with Compromised Machines

For extended operations, an intruder will require dependable access to compromised systems. This could be a legitimate channel that an attacker accesses with stolen credentials or a new channel created by the attacker.

Subverting Legitimate Communication Channels

If available, an attacker can use an already existing communication channel for remote access to a compromised system. Here are some examples:

- **SMB/CIFS and DCE/RPC:** Windows file sharing and remote procedure protocols can be used to move data to and from, or even configure a remote system. This requires that the attacker has credentials to that system. This is most useful for manipulating a system from another device within the same network, as these protocols are not allowed to traverse most Internet-facing network perimeters.
- **Remote administration applications:** Terminal Services, VNC and Remote Desktop are all examples of applications that allow someone to open a graphical interface to another system. The attacker can authenticate to these pre-existing applications with stolen credentials. Other applications such as SSH and telnet can also be used to administer a system through a command line interface.
- **VPN tunnels:** An attacker can utilize tunnels that already exist to or from a compromised system to jump to other devices and/or networks.

Techniques – Remote Connectivity, continued

Remote Backdoors A backdoor is a non-legitimate method for listening for remote connections from an attacker to a compromised system. This is typically accomplished by starting a process that listens for remote connection attempts. That attempt might be a normal TCP connection attempt, or it may involve a series of packets sent to specific ports in a specific order which will then cause a full listening socket to be opened (called “port knocking”).

Outbound Initiated Channels Sometimes, a compromised system may sit behind a firewall that prevents inbound remote connection attempts from reaching the system. As an alternative to a process listening for inbound connection attempts, a malicious code package may be configured to initiate communication outbound from the victim system/network to an external computer that is controlled by an attacker (called a “Command and Control Server”). These connections, called “Reverse Channels,” are frequently successful due to the fact that firewall egress rules are typically less stringent than ingress rules.

Techniques – Remote Connectivity, continued

Possible Artifacts: Artifacts of the usage of a legitimate communication channel by an attacker include:
Legitimate Channel Usage

- Unusual login times for an otherwise authorized account. They are shown in authentication logs such as /var/log/secure or the Windows Security Event Log.
- Login times for an authorized account that the user of that account claims he/she did not initiate.
- Authentication or subsequent activity that occurs too fast for a human to be manually directing the activity.
- The existence of malicious code on a compromised system that includes functions for connecting to remote administration applications such as SSH or VNC.

Possible Artifacts: Possible artifacts of the usage of unauthorized backdoor listeners include:
Backdoors

- Abnormal ports open on a system. These may be suspicious ports that correspond to known backdoors that are visible from a port scan or from the results of a command such as netstat.
- Suspicious processes attached to a listening port. These may be viewable from the output of programs such as tcpview or fport.
- Inbound connection attempts to workstations. Connection attempts blocked by firewalls or routers may show in the logs of those devices.
- Abnormal patterns of inbound packets or connection attempts. Again, blocked packets may be recorded in firewall or router logs. Otherwise this activity would be viewable in a recording of network traffic.
- The existence of malicious code on a compromised system that is found to start a listening service when executed.

Techniques – Remote Connectivity, continued

Possible Artifacts: Possible artifacts of the usage of reverse channels include:

**Outbound
Channels**

- DNS queries for known-bad domain names or DNS hosts, as seen in the logs of any available DNS servers, or their upstream forwarders.
- Outbound connection attempts to known-bad or suspicious IP addresses or IP ranges, which may be seen in firewall logs.
- Outbound connection attempts occurring over abnormal ports, which may be seen in firewall logs.
- Outbound connection attempts which exhibit abnormal content. For instance an outbound session that occurs over TCP port 80, but contains no HTTP headers or HTML. This may be observed in proxy server logs when traffic is rejected due to the appropriate content.
- The existence of malicious code on a compromised system that is found to beacon to a domain name or IP address when executed.

Techniques – File System Date/Time Stamp Manipulation

File System Date/Time Stamp Manipulation

An attacker may attempt to hide unauthorized activity by changing associated date/time stamps to make it appear as if the activity is unrelated.

Possible Artifacts

Artifacts of date/time stamp manipulation include:

- Date/time stamps for malicious code executables or DLLs that match the date/time stamps on Windows files that were created much earlier than other related activity.
- Date/time stamps for suspicious Registry keys that are set much earlier than other related activity.
- The existence of malicious code on a system that is found to modify date/time stamps on files or Registry keys when it is executed.

Privilege Escalation

**Escalation/
Advancement**

The Escalation or advancement phase of a network intrusion is where a hacker in possession of a system seeks to elevate privileges.

**What is
Advancement?**

Once hackers gain access to a system, they must advance from an unprivileged user account to a privileged to control the system.

Some of the ways in which privileges are escalated include:

- Through local system attacks
- Cracked or guessed passwords
- Running trojans on the system

Local Attacks

A local attack takes place either sitting directly at the system or remotely through a command prompt or GUI. A hacker with inside access has many options available to compromise systems that will not work over the network. The default installation of most operating systems has open doors through which attackers can escalate privileges. These doors are often overlooked, which makes advancement possible.

Some of the commonly used local attacks are:

- Physical abuse
- Editing the boot.ini to boot another kernel
- Path abuse
- Using boot media (Knoppix, Linux-on-a-Floppy)
- Null connections
- Session Hijacking

Physical Abuse

If hackers can restart a system, they can often boot into a debugger or recover console, which usually has administrator-level access. While at this prompt, the hacker can create user names and passwords, edit access control lists and install programs in start-up directories that will provide them with administrator-level access when the system restarts.

Privilege Escalation, continued

Boot Prompt Attacks

Most operating systems use boot loaders to load their default kernel. The boot loader allows other kernels to be chosen in case the system has difficulty booting. Accessing boot loader configuration files can be as easy as pressing a key upon boot.

Path Abuse

A path tells the operating system where to look for programs required to run. If the default path is changed or appended, hacker installed programs may be executed.

Boot Media

Booting from a CD can bypass logon screens and directly access the system allowing for the hacker to search, crack, and extract passwords. Complete operating systems like KNOPPIX or Linux-on-a-floppy exist, and if the default boot sequence allows for booting from a floppy, then placing a Linux-on-a-floppy diskette into the drive will allow hackers to mount and access the system. This allows them to swap out and edit files that provide root-level access.

Null Connections

During the reconnaissance phase, a hacker may have created a null connection while attempting to run services that provide administrator-level access. A system administrator may have blocked these service ports at the firewall, but left them open on local systems. Simply connecting to these ports with a dummy or null connection, while at a command prompt, can provide administrator-level access.

Session Hijacking

A hacker sniffing the network traffic can detect when a root user is connected to the network. He can either interrupt the existing session or wait until the session is almost terminated and block the end of transmission signal from being sent.

Privilege Escalation, continued

Local Password Cracking

Username and passwords are the security mechanisms used to authenticate to a system. If this authentication can be bypassed or defeated the system can be compromised.

Windows systems store encrypted passwords locally in the registry, and if a hacker can gain access to these files, he can run a brute force cracking program. A *brute force program* uses a dictionary to encrypt words with various encryption algorithms and seeks to match encrypted passwords with those stored in the registry.

Many times, hackers have physical access to a system. Having inside access to these systems might allow hacker control by simply pressing a key combination to bypass authentication mechanisms.

Some of the ways that passwords can be defeated on a local system are:

- Booting from a CD or floppy diskette, extracting the password files and cracking them offline
- Hijacking a connection with administrator privileges
- Logging onto the system as a service
- Brute force password attacks
- Sniffing clear text passwords
- Change entries in system critical files for services that authenticate login and login privileges

Some popular password cracking programs are:

- pwdumpX
- Crack
- John the ripper
- L0phtcrack
- LSADump

Privilege Escalation, continued

Trojans in Advancement

Trojans are programs that pretend to be normal or useful software tools. Many commands used by the system administrator for system and network control are often trojanized by hackers. They can also be batch files (.BAT) with the same name as the program and execute the program along with the Trojan.

Examples of commonly trojanized binary programs are:

- task manager
- login
- ipconfig
- secpol
- dir
- ntbackup

These executables are often trojanized because only the system administrator has a right to run them. For example, the system administrator creates a new user and assigns a password, but uses a trojanized program that captures the password and sends it back to the hacker.

A Trojan might also sabotage the installation of security patches informing the system administrator that updates were installed when in actuality they were not. Such vulnerabilities might allow the hacker to gain entry through unpatched security holes.

Lesson 5 – Infiltration and Extraction

Introduction

Once a hacker becomes entrenched in a system, he uses that system as a mainstay with which to gather data, mine for useful information, and launch attacks on other systems.

Purpose of this Lesson

This lesson explains how to infiltrate other systems and determine data extraction methods.

Objectives

After completing this lesson, you will be able to:

- Explain the purpose and methods of infiltration
- Explain the importance of trust relationships
- Determine the data types targeted by hackers and how these types are extracted

In this Lesson

The following table shows the contents of this lesson.

Topic	See Page
Sniffers	6-68
Trust Relationships	6-69
Data Extraction	6-70

Sniffers

Sniffers

A *sniffer* is a program that is used to monitor or capture network traffic. Hackers often eavesdrop seeking data, like usernames and passwords that they can use to access other systems. This collected data is usually stored on the compromised system in a hidden file.

Sniffers often run as disguised processes on systems. Some of the common ways they run as disguised processes include:

- Trojanized device drives
- Renamed programs that are configured to start at boot
- Trojanized applications

Trust Relationships

Trust Relationships

A *trust relationship* is a mechanism whereby users who are logged on and authenticated to one server are allowed to access resources on another server without the need to re-authenticate.

If server A trusts the users logged into server B, then server A has established what is called a one-way trust.

If server A trusts server B, and server B trusts server A, then they have established what is called a two-way or absolute trust.

Server A and B have a two-way trust. Server B also trusts server C. Server C can now access server A through what is called a pass through or transitive trust.

Server A ←----- Server B (One way trust)

Server A ←-----→ Server B (Two-way or absolute trust)

Server A ←-----→ Server B ←-----Server C (Transitive trust)

Some of the ways in which trust relationships are exploited are:

- Compromising a trusted system, domain or server
- Using or exploiting the LDAP service
- Forging or spoofing authentication credentials
- Spoofing source information
- Piggybacking off an already trusted system
- Hijacking a session from a trusted system

Data Extraction

Data Extraction

Data extraction is the process of obtaining data off a compromised system. Hackers must find a way to extract collected data in a stealthy manner so as to avoid detection. To help avoid detection, the desired data is filtered for relevancy and sent in a way that will not overload the system or trigger an IDS.

Hackers know that most traffic loggers, IDS, and sniffers are configured to only capture the beginning of most packets. Embedding data deep into packets often allows the hacker to extract the data without being detected.

Sometimes a hacker will schedule a job to send extracted data during times when network traffic is heavy. This technique attempts to avoid detection by using the network traffic volume against the system administrator; much like trying to find a needle in a haystack.

Some of the common ways data is extracted include:

- E-mail
- Masked as services like HTTP, DNS or ARP
- Backdoor connections
- Services run on a regular basis
- Ftp or telnet login by the attacker
- A print job run to a remote location or file