



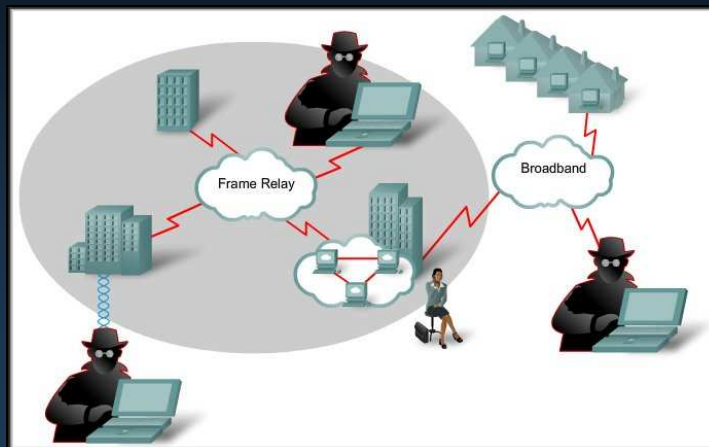
Chapter 4

Network Security

Part I

Introducing Network Security

Introduction to Network Security



Introducing Network Security

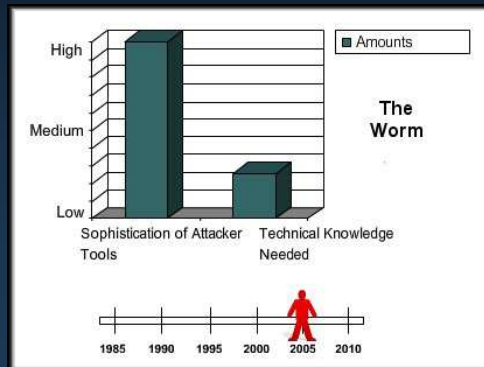
- Why is Network Security important?
 - Rapid growth in both size and importance.
 - Consequences of compromised security:
 - Loss of privacy.
 - Theft of information.
 - Legal liability.

Introducing Network Security

- Why is Network Security important?
 - We will discuss:
 - Different types of threats.
 - Development of organizational security policies, mitigation techniques,
 - Cisco software tools to help secure networks.
 - Managing Cisco IOS software images.
 - Cisco software images and configurations can be deleted. Devices compromised in this way pose security risks.

Introducing Network Security

- **Increasing Threat to Security:**
 - Over the years, attack tools have evolved.
 - Threats become more sophisticated as the technical expertise required to implement attacks diminishes.



CCNA4-5

Chapter 4-1



Netwo

ooks for
o that th

ise

systems that they are

- **Hacker:**
 - A general term that h
describe a computer



CCNA4-6

Chapter

rk Security



- **Spam**
 - An e-
- **Phisher:**
 - Uses e-mail or other means for providing information.



CCNA4-7

Chapter 4-1

Introducing Network Security

• T

Google™
Canada

attack software	
brute force attack software	764,000 results
dictionary attack software	709,000 results
dos attack software	1,510,000 results
denial of service attack software	30,400,000 results
ddos attack software	485,000 results
facebook hack attack software	462,000 results
ping attack software	304,000 results
dos attack software download	1,460,000 results
man in the middle attack software	14,000,000 results
server attack software	4,120,000 results
	close

[Advanced Search](#)
[Language Tools](#)

CCNA4-8

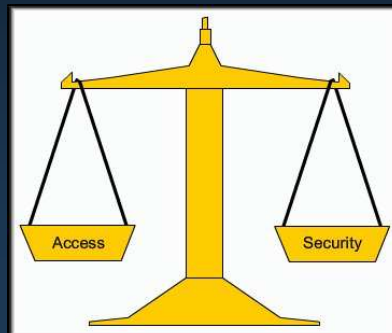
Chapter 4-1

Introducing Network Security

- **Types of computer crime:**
 - Text and Curriculum lists the most commonly reported acts of computer crime that have network security implications.
 - They fall into four general categories, or a combination thereof, that effective and vigilant security management can address.
 - Insider Abuse
 - Denial of service
 - System Penetration
 - Password sniffing

Introducing Network Security

- **Open versus Closed Networks:**
 - The challenge is to find the correct balance.
 - Networks must be **accessible** to be of any use.
 - Networks must be **secure** to protect corporate and personal information.



Introducing Network Security

- **Developing a Security Policy:**
 - First step an organization should take to protect its data and a liability challenge.
 - A security policy meets these goals:
 - **Informs users, staff, and managers** of their requirements for protecting information assets.
 - Acceptable and unacceptable use.
 - **Specifies the mechanisms** through which these requirements can be met.
 - Managing security violations.
 - **Provides a baseline** from which to acquire, configure, and audit computer systems for compliance.
 - Basis for legal action.

Common Security Threats

- Three common factors - Network Security:
 - **Vulnerability:**
 - It is the degree of weakness which is inherent in every network and device.
 - Routers, switches, desktops, and servers.
 - **Threats:**
 - They are the people interested in taking advantage of each security weakness.
 - **Attack:**
 - The threats use a variety of tools, and programs to launch attacks against networks.

Vulnerabilities

- **Three primary Vulnerabilities or Weaknesses:**
 - **Technological** weaknesses.
 - Computer and network technologies have intrinsic security weaknesses.

Network security weaknesses:

TCP/IP protocol weakness ←

- Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) and Internet Control Message Protocol (ICMP) are inherently insecure.
- Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP), and Syn Floods are related to the inherently insecure structure upon which TCP was designed.

Operating system weakness ←

- Each operating system has security problems that must be addressed.
- UNIX, Linux, Mac OS, Mac OS X, Windows NT, 9x, 2K, XP, and Vista.
- They are documented in the Computer Emergency Response Team (CERT) archives at <http://www.cert.org>.

Network equipment weakness ←

- Various types of network equipment, such as routers, firewalls, and switches have security weaknesses that must be recognized and protected against. Their weaknesses include password protection, lack of authentication, routing protocols, and firewall holes.

CCNA4-13

Chapter 4-1

Vulnerabilities

- **Three primary Vulnerabilities or Weaknesses:**
 - **Configuration** weaknesses.
 - Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate.

Configuration Weakness	How the weakness is exploited
Unsecured user accounts	User account information may be transmitted insecurely across the network, exposing usernames and passwords to snoopers.
System accounts with easily guessed passwords	This common problem is the result poorly selected and easily guessed user passwords.
Misconfigured Internet services	A common problem is to turn on JavaScript in Web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites. IIS, FTP, and Terminal Services also pose problems.
Unsecured default settings within products	Many products have default settings that enable security holes.
Misconfigured network equipment	Misconfigurations of the equipment itself can cause significant security problems. For example, misconfigured access lists, routing protocols, or SNMP community strings can open up large security holes.

CCNA4-14

Chapter 4-1

Threats to Physical Infrastructure

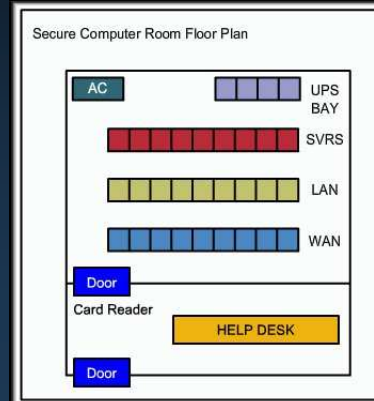
- **Four classes of Physical Threats:**

- **Hardware Threat:**

- Physical damage to servers, routers, switches, cabling plant, and workstations.

- **Security Measures:**

- Lock up equipment and prevent unauthorized access.
 - Monitor wiring closet access – electronic logs.
 - Security cameras



CCNA4-15

Chapter 4-1

Threats to Physical Infrastructure

- **Four classes of Physical Threats:**

- **Environmental Threat:**

- Temperature or humidity extremes.

- **Security Measures:**

- Temperature control.
 - Humidity control.
 - Positive air flow.
 - Remote environment alarms.



CCNA4-16

Chapter 4-1

Threats to Physical Infrastructure

- **Four classes of Physical Threats:**

- **Electrical Threat:**

- Voltage spikes, insufficient voltage (brownouts), unconditioned power (noise), and total power loss.

- **Security Measures:**

- UPS systems.
- Generators.
- Preventive maintenance.
- Redundant power supply.
- Remote alarms.



CCNA4-17

Chapter 4-1

Threats to Physical Infrastructure

- **Four classes of Physical Threats:**

- **Maintenance:**

- Poor handling of key electrical components, lack of critical spare parts, poor cabling, and poor labeling.

- **Security Measures:**

- Neat cable runs.
- Label the cables.
- Electrostatic discharge procedures.
- Stock critical spares.
- Control console port access.

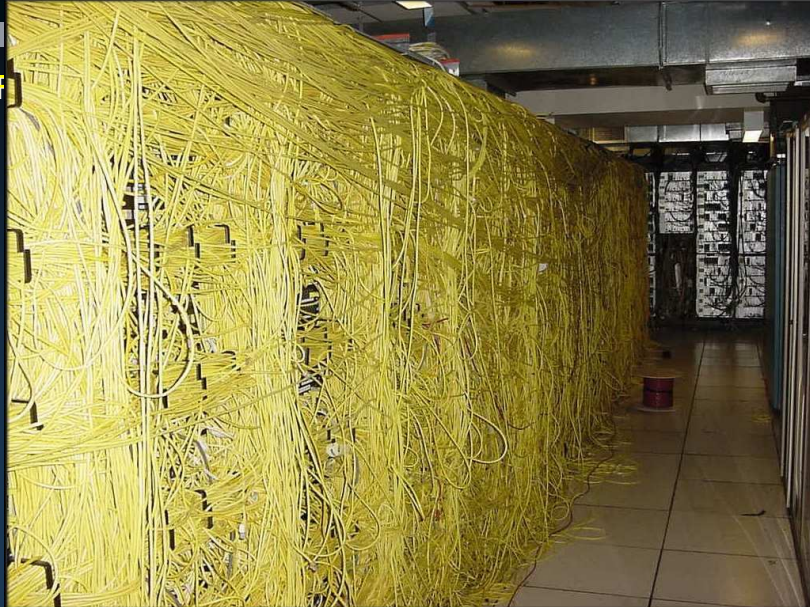


CCNA4-18

Chapter 4-1

Threats to Physical Infrastructure

- **F**

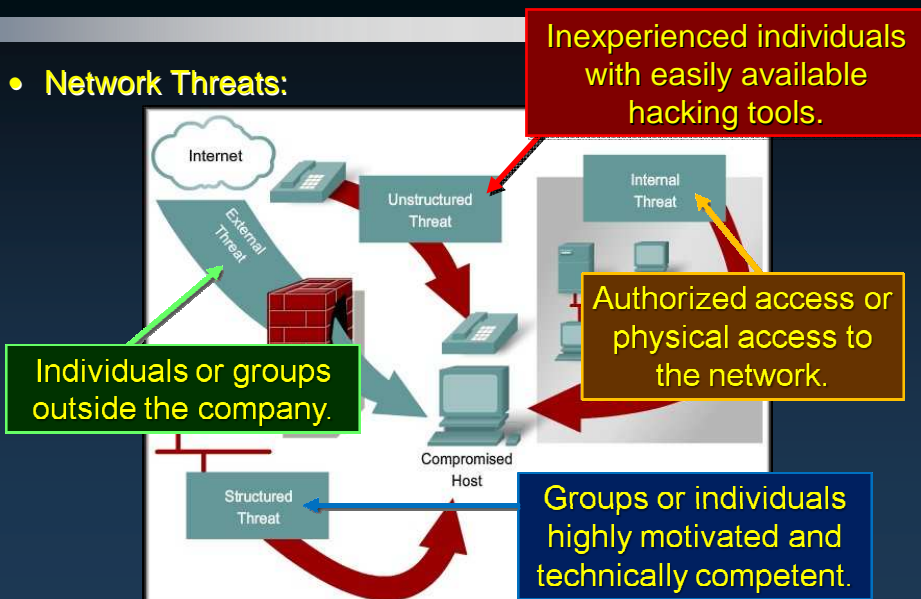


CCNA4-19

Chapter 4-1

Threats to Networks

- **Network Threats:**



CCNA4-20

Chapter 4-1

Social Engineering

- **The easiest hack involves no computer skill.**
 - If an intruder can trick a member of an organization into giving over information, such as the location of files or passwords, the process of hacking is made much easier.
- **Phishing:**
 - A type of social engineering attack that involves using e-mail in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords.
 - Phishing attacks can be prevented **by educating users and implementing reporting guidelines** when they receive suspicious e-mail.

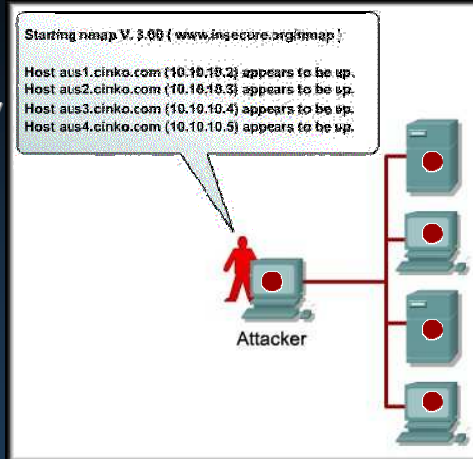
Types of Network Attacks

- **There are four primary classes of attacks:**
 - Reconnaissance
 - Access
 - Denial of Service
 - Malicious Code



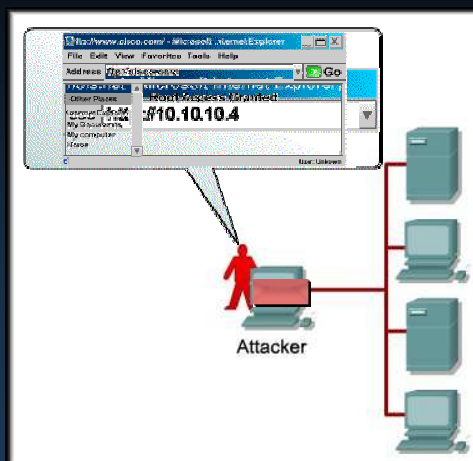
Types of Network Attacks

- **Reconnaissance:**
 - Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities.
 - In most cases, it precedes another type of attack.



Types of Network Attacks

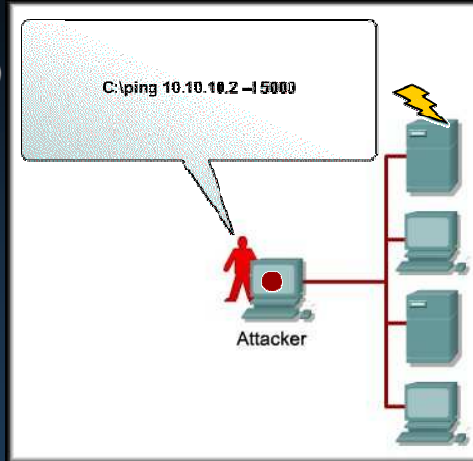
- **System Access:**
 - System access is the ability for an intruder to gain access to a device for which the intruder does not have an account or a password.
 - Usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.





Types of Network Attacks

- **Denial of Service:**
 - Denial of service (DoS) is when an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users.
 - DoS attacks involve either crashing the system or slowing it down to the point that it is unusable.

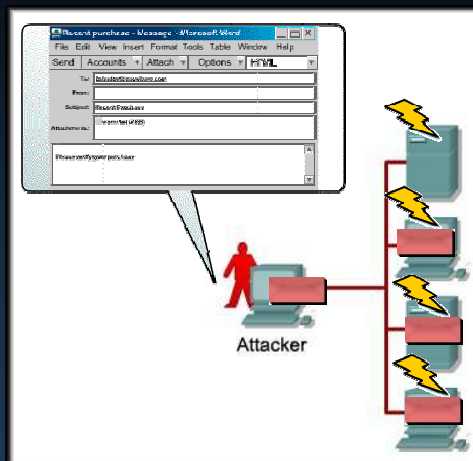


DoS MOST FEARED!



Types of Network Attacks

- **Worms, Viruses and Trojan Horses:**
 - Malicious software can be inserted onto a host to damage or corrupt a system, replicate itself, or deny access to networks, systems, or services.



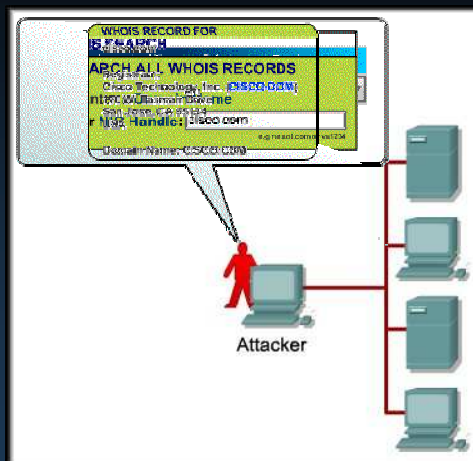
Types of Network Attacks

- **Reconnaissance Attacks:**
 - Reconnaissance is the unauthorized discovery or mapping of systems, services or vulnerabilities.
 - It usually precedes another type of attack.
 - **Can consist of:**
 - Internet Information Queries
 - Ping Sweeps
 - Port Scans
 - Packet Sniffers



Types of Network Attacks

- **Internet Queries:**
 - External attackers can use Internet tools, such as the **nslookup** and **whois** utilities, to easily determine the IP address space assigned to a given corporation or entity.

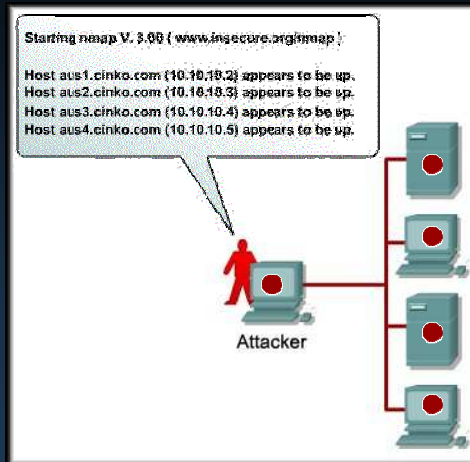




Types of Network Attacks

- **Ping Sweeps:**

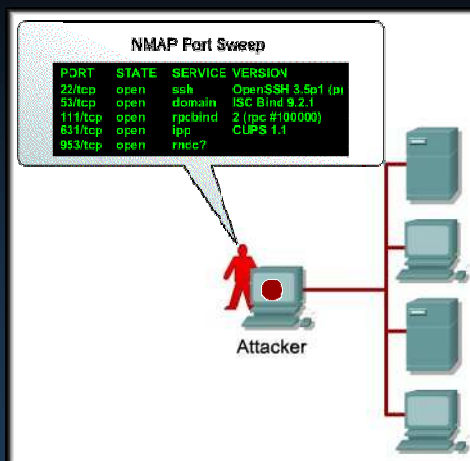
- After the IP address space is determined, an attacker can then ping the publicly available IP addresses to identify the addresses that are active.
- To help automate this step, an attacker may use a ping sweep tool, such as **fping** or **gping**.



Types of Network Attacks

- **Port Scans:**

- When the active IP addresses are identified, the intruder uses a port scanner to determine which network services or ports are active on the live IP addresses.
- A port scanner is software, such as **Nmap** or **Superscan**, that is designed to search a network host for open ports.

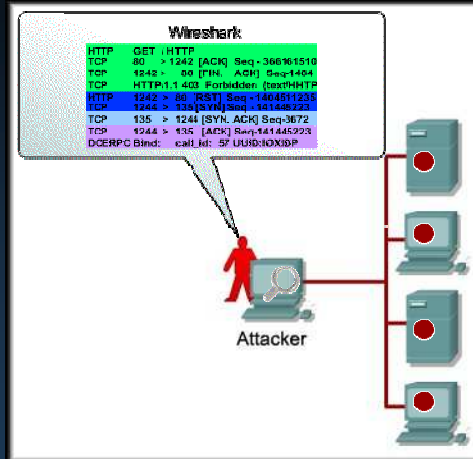




Types of Network Attacks

- **Packet Sniffers:**

- Internal attackers may attempt to "eavesdrop" on network traffic.
- **Wire Shark**
- Two common uses of eavesdropping are Information Gathering and/or Information Theft.



Types of Network Attacks

- **Packet Sniffers:**

- A common method for eavesdropping is to capture TCP/IP or other protocol packets and decode the contents.
- Three of the most effective methods for counteracting eavesdropping are as follows:
 - **Using switched networks** instead of hubs so that traffic is not broadcast to all endpoints or network hosts.
 - **Using encryption** that meets the data security needs without imposing an excessive burden on system resources or users.
 - **Forbid the use of protocols** with known susceptibilities to eavesdropping. (e.g. SNMP vs SNMP v3)

Types of Network Attacks

- **Access Attacks:**
 - Access attacks exploit vulnerabilities in authentication, FTP, and web to gain entry to accounts, confidential, and sensitive information.
 - The more common are:
 - Password Attacks
 - Trust Exploitation
 - Port Redirection
 - Man-in-the-Middle

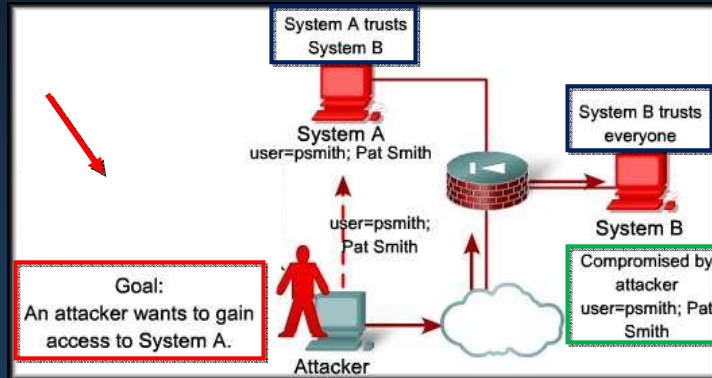
Types of Network Attacks

- **Password Attacks:**
 - Packet sniffer to yield user accounts and passwords that are transmitted as clear text.
 - Dictionary Attacks or Brute-Force Attacks:
 - Repeated attempts to log in to a shared resource.
 - Tools such as **L0phtCrack** or **Cain**.
 - **Rainbow Tables:**
 - A rainbow table is pre-computed series of passwords which is constructed by building chains of possible plaintext passwords.
 - Password attacks can be mitigated by educating users to use long, complex passwords.



Types of Network Attacks

- **Trust Exploitation:**
 - The goal of a trust exploitation attack is to compromise a trusted host, using it to stage attacks on other hosts in a network.

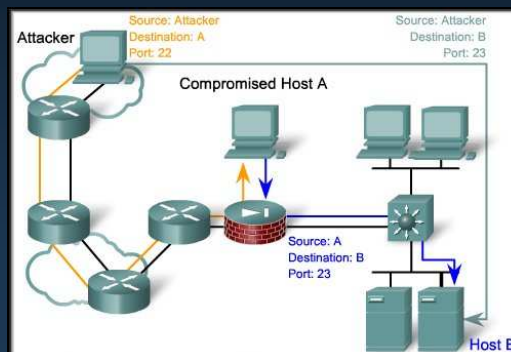


CCNA4-35

Chapter 4-1

Types of Network Attacks

- **Port Redirection:**
 - Port redirection is a type of trust exploitation attack that uses a compromised host to pass traffic through a firewall. Traffic that would normally be stopped.
 - Utility - **netcat**
 - Port redirection can be mitigated through the use a host-based Intrusion Detection System (**IDS**). (e.g. Snort)



CCNA4-36

Chapter 4-1

Types of Network Attacks

- **Man-in-the-Middle:**

- A man-in-the-middle (MITM) attack is carried out by attackers that manage to position themselves between two legitimate hosts.
- There are many ways that an attacker gets positioned between two hosts.
- One popular method, the **transparent proxy**:
 - In a transparent proxy attack, an attacker may catch a victim with a **phishing e-mail** or by defacing a website.
 - Then the URL of a legitimate website has the attacker's URL prepended.

<http://www.attacker.com/http://www.legitimate.com>

Types of Network Attacks

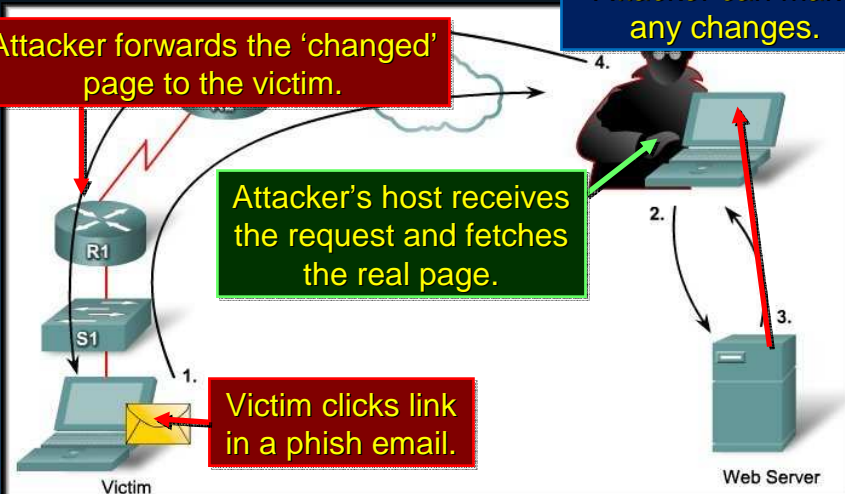
- **Man-in-the-Middle:**

Attacker forwards the 'changed' page to the victim.

Attacker can make any changes.

Attacker's host receives the request and fetches the real page.

Victim clicks link in a phish email.



Types of Network Attacks

- **Denial-of-Service Attacks:**

- An attacker disables or corrupts networks, systems or services with the intent to deny service to intended users.
- **DoS** attacks are the most publicized form of attack and also among the most difficult to eliminate.

Resource overloads	Malformed data
Disk space, bandwidth, buffers	Oversized packets such as ping of death
Ping floods such as smurf	Overlapping packet such as winuke
Packet storms such as UDP bombs and fraggle	Unhandled data such as teardrop

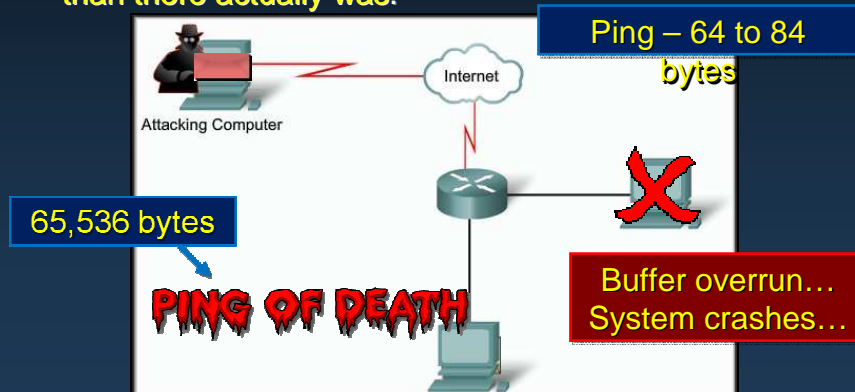
- Ping of Death
- SYN Flood
- DDos
- Smurf

Types of Network Attacks

- **Denial-of-Service Attacks:**

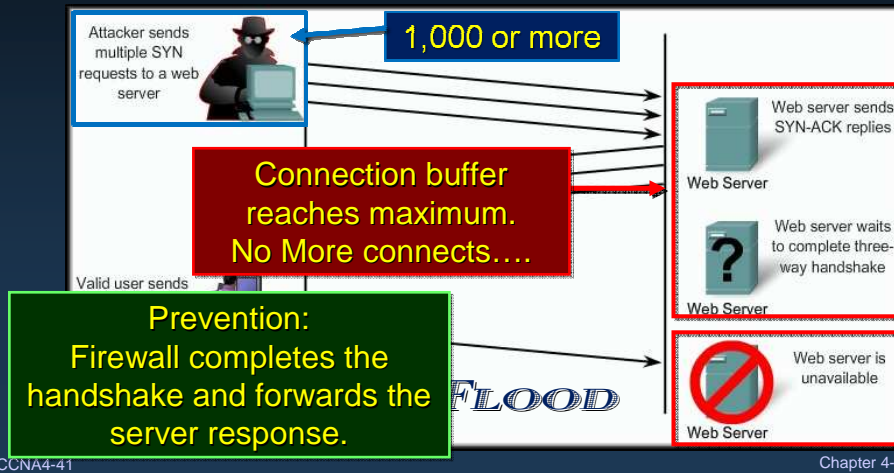
Older OS – most networks no longer susceptible.

- This attack modified the IP portion of a ping packet header to indicate that there is **more data in the packet than there actually was.**



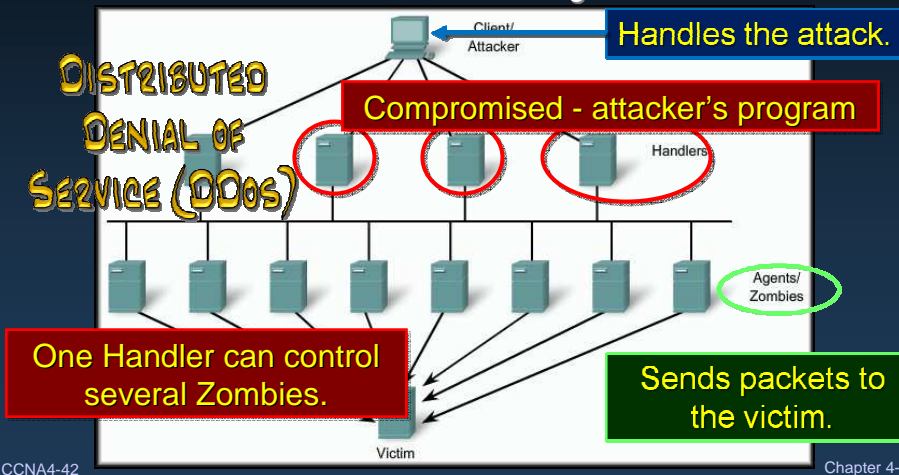
Types of Network Attacks

- Denial-of-Service Attacks:
 - This attack exploits the TCP three-way handshake.



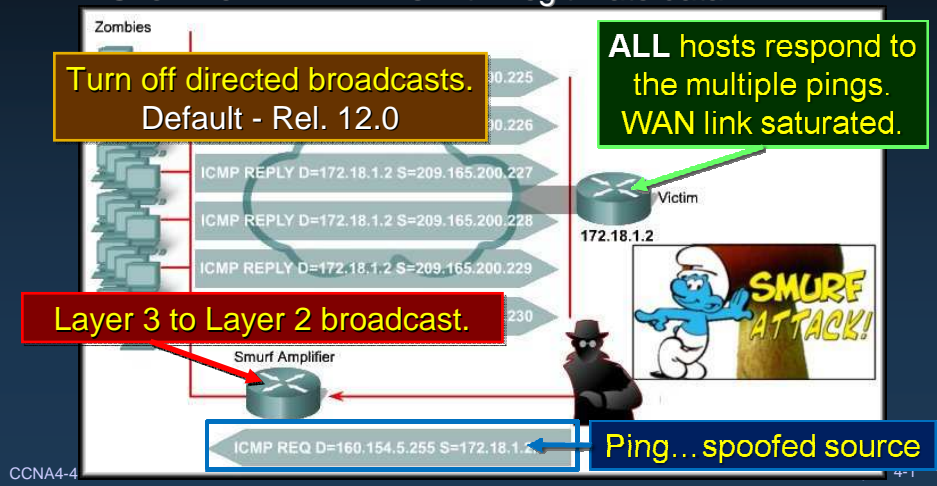
Types of Network Attacks

- Denial-of-Service Attacks:
 - Overwhelm network links with illegitimate data.



Types of Network Attacks

- Denial-of-Service Attacks:
 - Overwhelm WAN links with illegitimate data.



Types of Network Attacks

- Malicious Code Attacks:
 - Worm:
 - Executes code and installs copies of itself in the memory of the infected computer, which can, in turn, infect other hosts.



Types of Network Attacks

- Malicious Code Attacks:

- Virus:

- Malicious software that is **attached to another program** for the purpose of executing a particular unwanted function on a workstation.



CCNA4-45

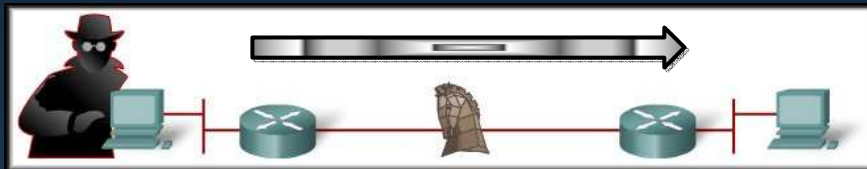
Chapter 4-1

Types of Network Attacks

- Malicious Code Attacks:

- Trojan Horse:

- Different from a worm or virus only in that the **entire application was written to look like something else**, when in fact it is an attack tool.



CCNA4-46

Chapter 4-1

General Mitigation Techniques

- **Device Hardening:**
 - Default usernames and passwords should be changed.
 - Access to system resources should be restricted to only the individuals that are authorized.
 - Any unnecessary services should be turned off.
- **Antivirus Software.**
- **Personal Firewalls.**
- **OS Patches.**

General Mitigation Techniques

- **Intrusion Detection and Prevention:**
 - **Intrusion Detection Systems (IDS):**
 - Detect attacks against a network and send logs to a management console.
 - **Intrusion Prevention Systems (IPS):**
 - Prevent attacks against the network and should provide the following active defense mechanisms in addition to detection:
 - **Prevention**.....Stops the detected attack from executing.
 - **Reaction**.....Immunizes the system from future attacks from a malicious source.

General Mitigation Techniques

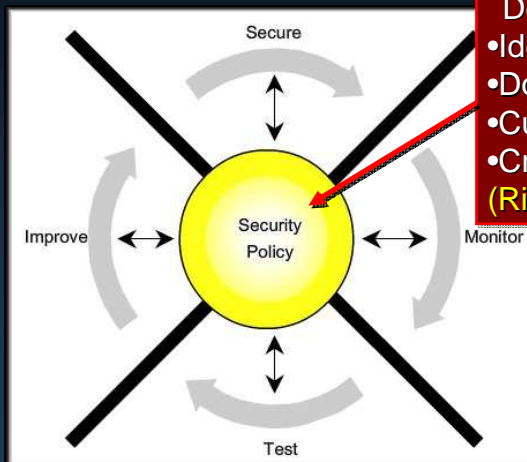
- **Common Security Appliances and Applications:**
 - A firewall by itself is no longer adequate for securing a network.
 - Integrated approach with a firewall, intrusion prevention, and VPN.
 - Follows these building blocks:
 - **Threat Control:** Regulates network access, prevents intrusions, by counteracting malicious traffic.
 - **Secure Communications:** Secures network endpoints with a VPN.
 - **Network Admission Control (NAC):** Provides a roles-based method of preventing unauthorized access.

CCNA4-49

Chapter 4-1

The Network Security Wheel

- A continuous process and an effective approach.



Develop a **Security Policy**.

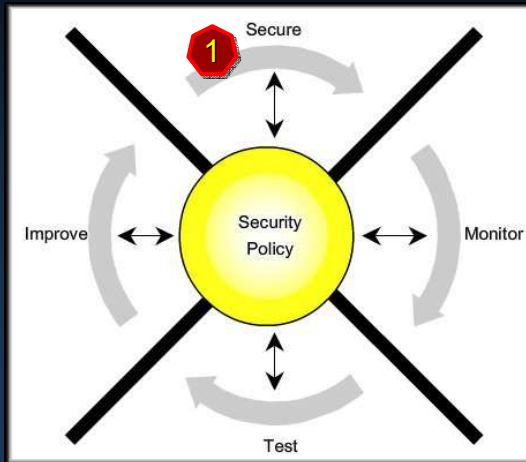
- Identify objectives.
- Document resources.
- Current infrastructure.
- Critical resources
(**Risk Assessment**).

CCNA4-50

Chapter 4-1

The Network Security Wheel

- A continuous process and an effective approach.



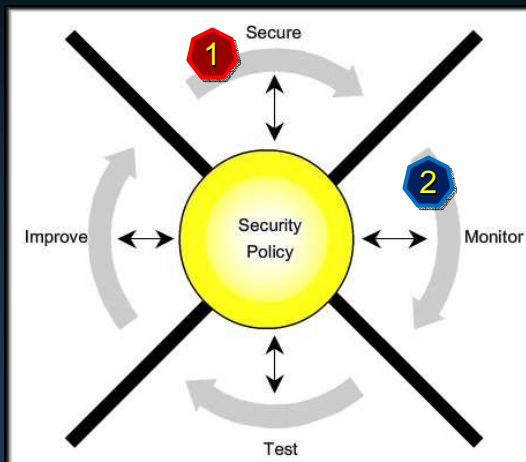
- Threat Defense
- IPS
- OS Patches
- Disable unnecessary services.
- Filter traffic
- VPNs (encrypted)
- Trusts
- User Authentication
- Policy Enforcement

CCNA4-51

Chapter 4-1

The Network Security Wheel

- A continuous process and an effective approach.



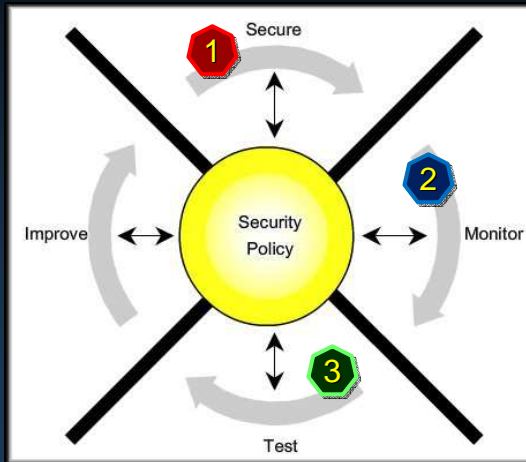
- Active and passive methods.
- Active:
 - Audit host logs
- Passive:
 - IDS

CCNA4-52

Chapter 4-1

The Network Security Wheel

- A continuous process and an effective approach.



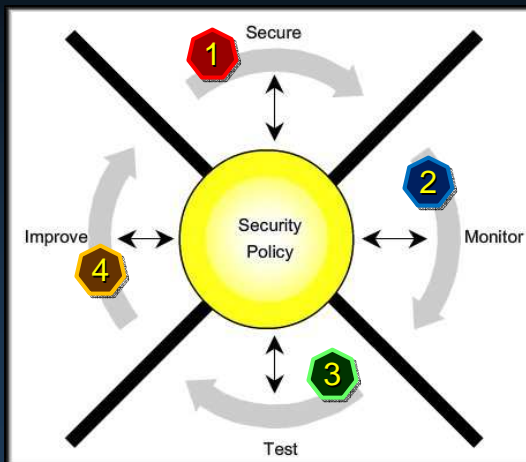
- Verify the methods implemented in Steps 1 and 2.
- Vulnerability assessment tools:
 - SATAN
 - Nessus
 - Nmap

CCNA4-53

Chapter 4-1

The Network Security Wheel

- A continuous process and an effective approach.



- Using the information from steps 2 and 3, implement improvements.

CCNA4-54

Chapter 4-1

The Enterprise Security Policy

- **A living document:**
 - The document is never finished and is continuously updated as technology and employee requirements change.
- **Essential Functions:**
 - Protects people and information.
 - Sets the rules for expected behavior by users, system administrators, management, and security personnel.
 - Authorizes security personnel to monitor, probe, and investigate.
 - Defines and authorizes the consequences of violations.

The Enterprise Security Policy

- **Attributes:**
 - Provides a means to audit existing network security and compare the requirements to what is in place.
 - Plan security improvements, including equipment, software, and procedures.
 - Defines the roles and responsibilities of the company executives, administrators, and users.
 - Defines which behavior is and is not allowed.
 - Defines a process for handling network security incidents.
 - Enables global security implementation and enforcement by acting as a standard between sites.
 - Creates a basis for legal action if necessary.