CCNA Security

Chapter One

Modern Network Security Threats

Lesson Planning

- This lesson should take 3-6 hours to present
- The lesson should include lecture, demonstrations, discussion and assessment
- The lesson can be taught in person or using remote instruction

Major Concepts

- Rationale for network security
- Data confidentiality, integrity, availability
- Risks, threats, vulnerabilities and countermeasures
- Methodology of a structured attack
- Security model (McCumber cube)
- Security policies, standards and guidelines
- Selecting and implementing countermeasures
- Network security design

Lesson Objectives

Upon completion of this lesson, the successful participant will be able to:

1. Describe the rationale for network security
2. Describe the three principles of network security
3. Identify risks, threats, vulnerabilities and countermeasures
4. Discuss the three states of information and identify threats and appropriate countermeasures for each state
5. Differentiate between security policies, standards and guidelines

Lesson Objectives

6. Describe the difference between structured and unstructured network attacks
7. Describe the stages and tools used in a structured attack
8. Identify security organizations that influence and shape network security
9. Identify career specializations in network security

What is Network Security?

National Security Telecommunications and Information Systems Security Committee (NSTISSC)

Network security is the protection of information and systems and hardware that use, store, and transmit that information.

Network security encompasses those steps that are taken to ensure the confidentiality, integrity, and availability of data or resources.

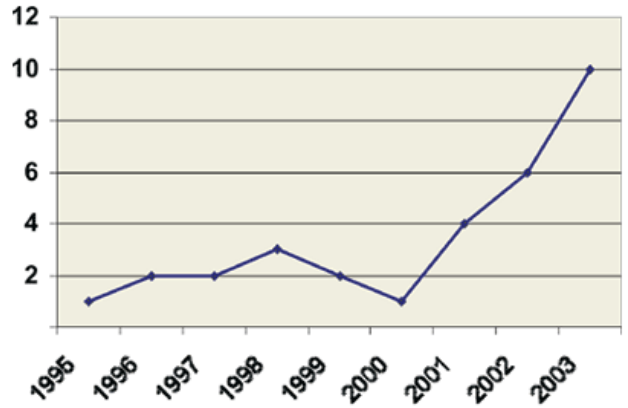
Rationale for Network Security

Network security initiatives and network security specialists can be found in private and public, large and small companies and organizations. The need for network security and its growth are driven by many factors:

1. Internet connectivity is 24/7 and is worldwide
2. Increase in cyber crime
3. Impact on business and individuals
4. Legislation & liabilities
5. Proliferation of threats
6. Sophistication of threats

Cyber Crime

- Fraud/Scams
- Identity Theft
- Child Pornography
- Theft of Telecommunications Services
- Electronic Vandalism, Terrorism and Extortion



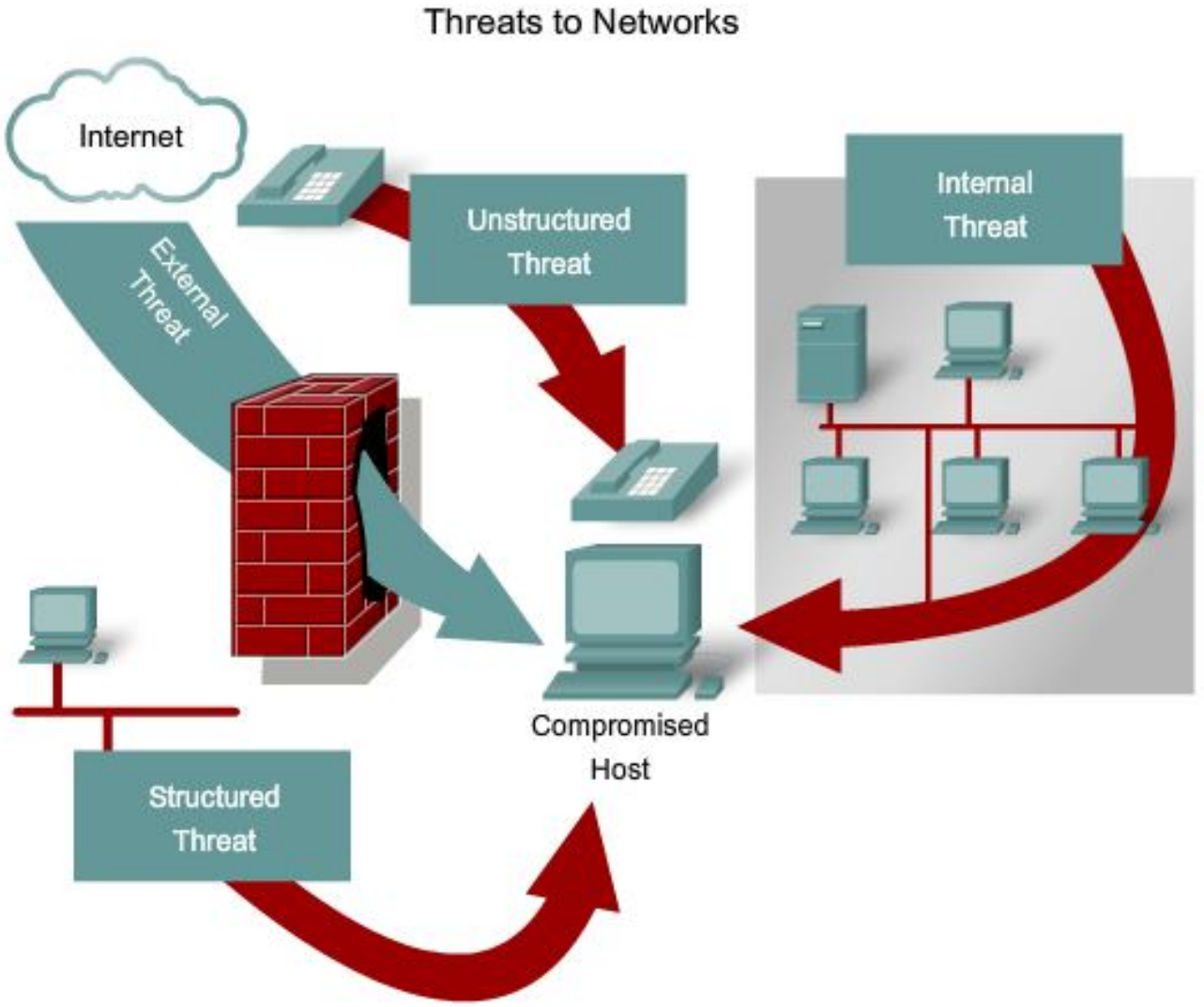
WASHINGTON, D.C. — An estimated 3.6 million households, or about 3 percent of all households in the nation, learned that they had been the victim of at least one type of identity theft during a six-month period in 2004, according to the Justice Department's Bureau of Justice Statistics

Business Impact

1. Decrease in productivity
2. Loss of sales revenue
3. Release of unauthorized sensitive data
4. Threat of trade secrets or formulas
5. Compromise of reputation and trust
6. Loss of communications
7. Threat to environmental and safety systems
8. Loss of time

Current Computer Crime Cases

Sophistication of Threats



Goals of an Information Security Program

- Confidentiality
  - Prevent the disclosure of sensitive information from unauthorized people, resources, and processes
- Integrity
  - The protection of system information or processes from intentional or accidental modification
- Availability
  - The assurance that systems and data are accessible by authorized users when needed

Risk Management

- Risk Analysis
- Threats
- Vulnerabilities
- Countermeasures

Types of Attacks

Structured attack

Come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.

Unstructured attack

Consists of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company.

Types of Attacks

External attacks

Initiated by individuals or groups working outside of a company. They do not have authorized access to the computer systems or network. They gather information in order to work their way into a network mainly from the Internet or dialup access servers.

Internal attacks

More common and dangerous. Internal attacks are initiated by someone who has authorized access to the network. According to the FBI, internal access and misuse account for 60 to 80 percent of reported incidents. These attacks often are traced to disgruntled employees.

Types of Attacks

- Passive Attack
  - Listen to system passwords
  - Release of message content
  - Traffic analysis
  - Data capturing
- Active Attack
  - Attempt to log into someone else's account
  - Wire taps
  - Denial of services
  - Masquerading
  - Message modifications

Specific Network Attacks

- ARP Attack
- Brute Force Attack
- Worms
- Flooding
- Sniffers
- Spoofing
- Redirected Attacks
- Tunneling Attack
- Covert Channels

Internet queries

Ping sweeps

Port scans

Denial-of-Service Facts

- Commonly used against information stores like web sites
- Simple and usually quite effective
- Does not pose a direct threat to sensitive data
- The attacker tries to prevent a service from being used and making that service unavailable to legitimate users
- Attackers typically go for high visibility targets such as the web server, or for infrastructure targets like routers and network links

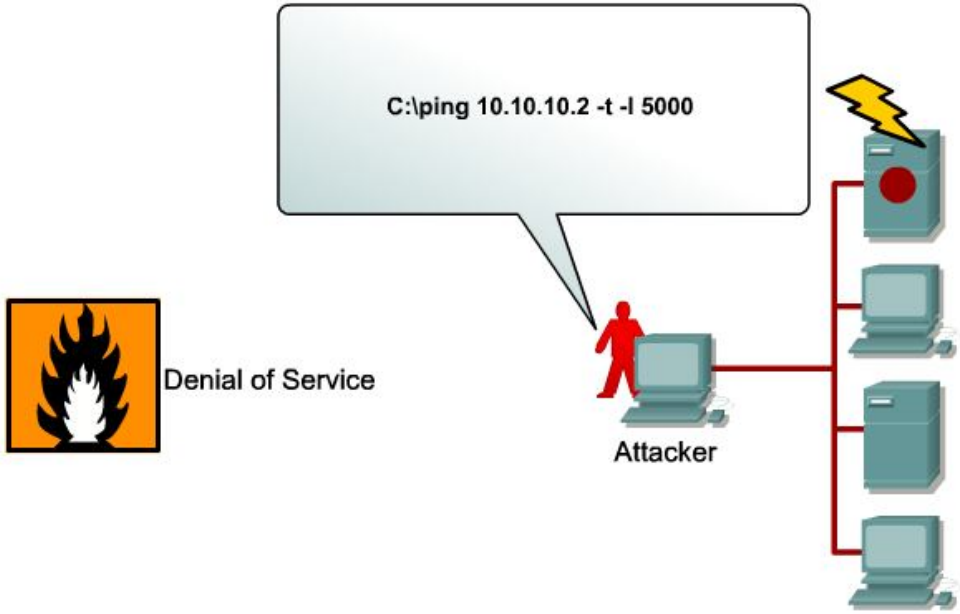
Denial-of-Service Example

If a mail server is capable of receiving and delivering 10 messages a second, an attacker simply sends 20 messages per second. The legitimate traffic (as well as a lot of the malicious traffic) will get dropped, or the mail server might stop responding entirely.

- This type of an attack may be used as a diversion while another attack is made to actually compromise systems
- In addition, administrators are likely to make mistakes during an attack and possibly change a setting that creates a vulnerability that can be further exploited

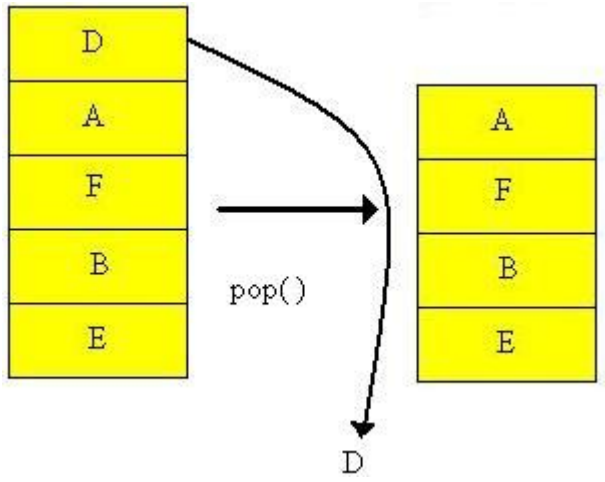
Types of Denial-of-Service Attacks

- Buffer Overflow Attacks
- SYN Flood Attack
- Teardrop Attacks
- Smurf Attack
- DNS Attacks
- Email Attacks
- Physical Infrastructure Attacks
- Viruses/Worms



DoS - Buffer Overflow Attacks

The most common DoS attack sends more traffic to a device than the program anticipates that someone might send Buffer Overflow.



DoS - SYN Flood Attack

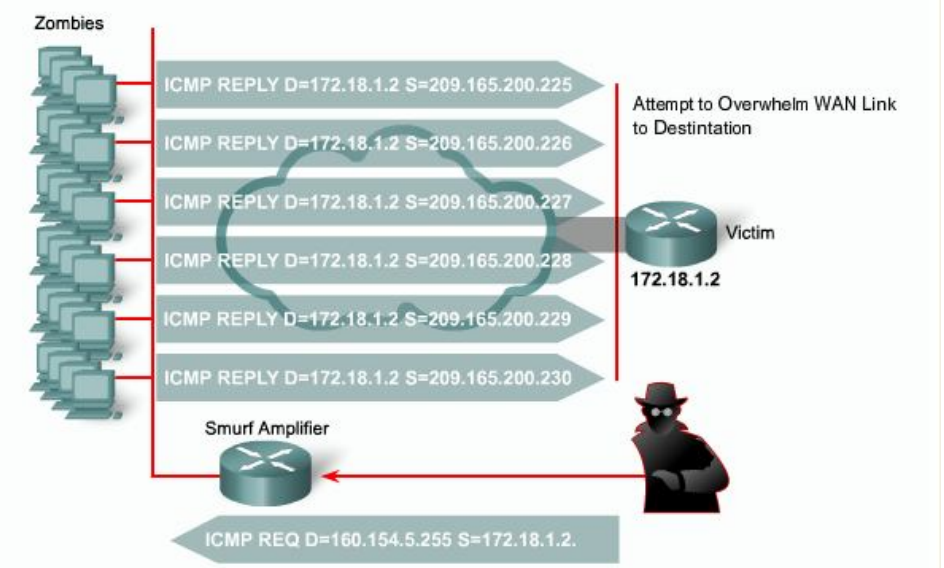
- When connection sessions are initiated between a client and server in a network, a very small space exists to handle the usually rapid "hand-shaking" exchange of messages that sets up a session.
- The session-establishing packets include a SYN field that identifies the sequence order.
- To cause this kind of attack, an attacker can send many packets, usually from a spoofed address, thus ensuring that no response is sent.

DoS - Smurf Attack

The attacker sends an IP ping request to a network site.

The ping packet requests that it be broadcast to a number of hosts within that local network.

The packet also indicates that the request is from a different site, i.e. the victim site that is to receive the denial of service.

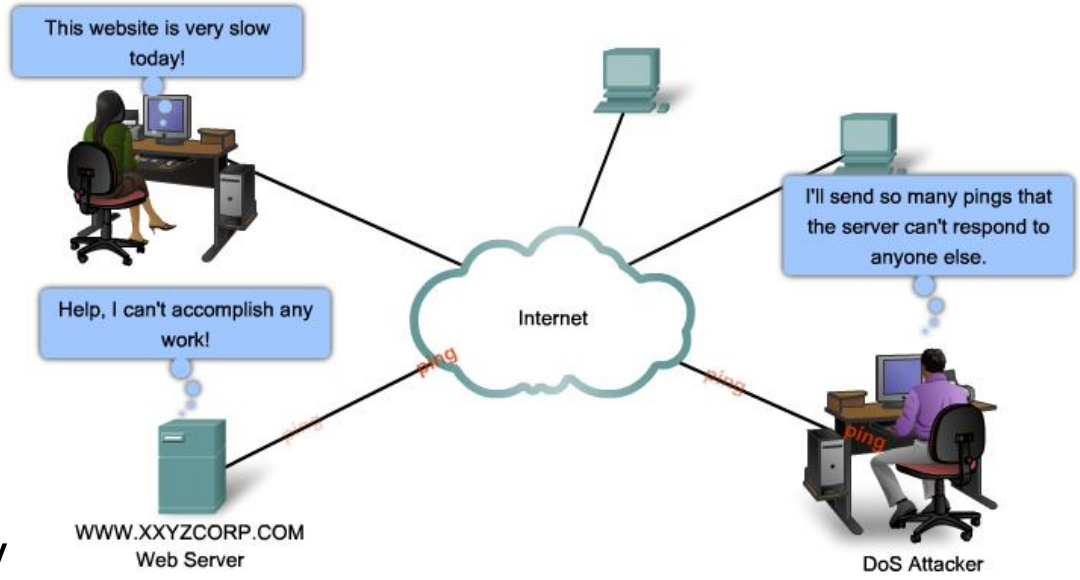


This is called IP Spoofing--the victim site becomes the address of the originating packet.

The result is that lots of ping replies flood back to the victim host. If the flood is big enough then the victim host will no longer be able to receive or process "real" traffic.

DoS - DNS Attacks

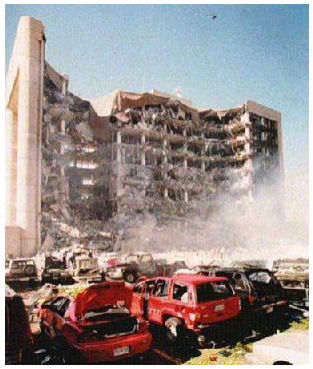
- A famous DNS attack was a DDoS "ping" attack. The attackers broke into machines on the Internet (popularly called "zombies") and sent streams of forged packets at the 13 DNS root servers via intermediary legitimate machines.



- The goal was to clog the servers, and communication links on the way to the servers, so that useful traffic was gridlocked. The assault is not DNS-specific--the same attack has been used against several popular Web servers in the last few years.

DoS - Physical Infrastructure Attacks

- Someone can just simply snip your cables! Fortunately this can be quickly noticed and dealt with.
- Other physical infrastructure attacks can include recycling systems, affecting power to systems and actual destruction of computers or storage devices.



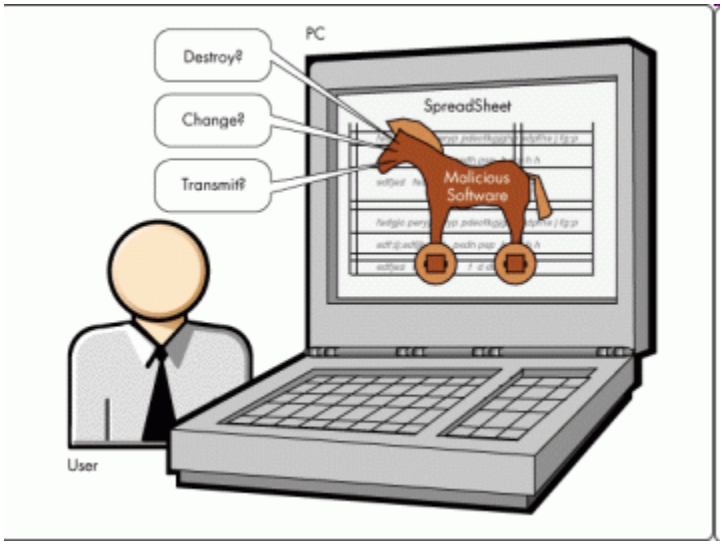
DoS - Viruses/Worms

- Viruses or worms, which replicate across a network in various ways, can be viewed as denial-of-service attacks where the victim is not usually specifically targeted but simply a host unlucky enough to get the virus.
- Available bandwidth can become saturated as the virus/worm attempts to replicate itself and find new victims.

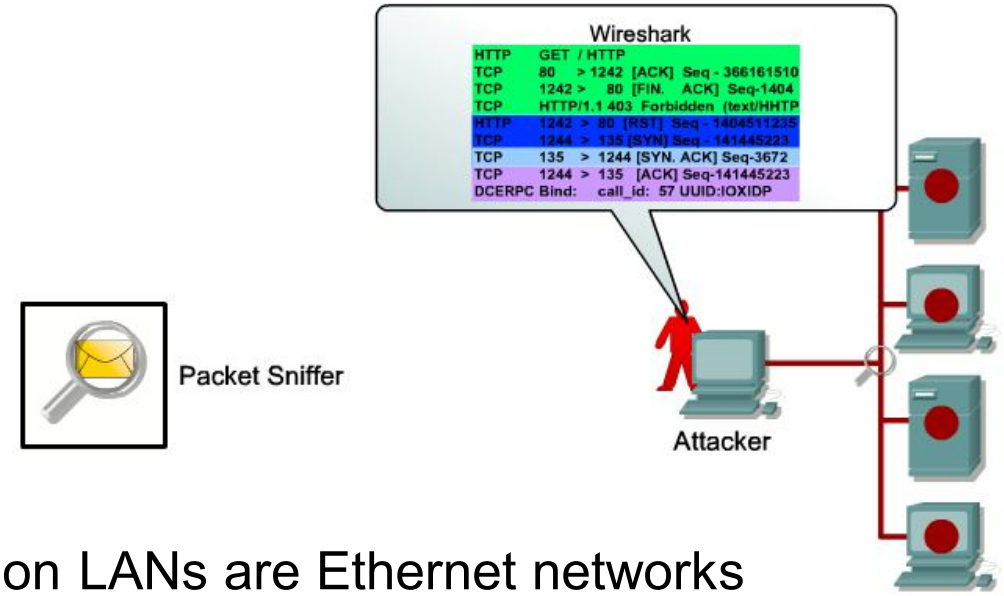
Image courtesy of: Tech Tips.com

Malicious Code Attacks

- Malicious code attacks refers to viruses, worms, Trojan horses, logic bombs, and other uninvited software
- Damages personal computers, but also attacks systems that are more sophisticated
- Actual costs attributed to the presence of malicious code have resulted primarily from system outages and staff time involved in repairing the systems
- Costs can be significant



Packet Sniffing Attacks



- Most organization LANs are Ethernet networks
- On Ethernet-based networks, any machine on the network can see the traffic for every machine on that network
- Sniffer programs exploit this characteristic, monitoring all traffic and capturing the first 128 bytes or so of every unencrypted FTP or Telnet session (the part that contains user passwords)

Stages of an Attack

- Today's attackers have a abundance of targets. In fact their greatest challenge is to select the most vulnerable victims. This has resulted in very well- planned and structured attacks. These attacks have common logistical and strategic stages. These stages include;
  - Reconnaissance
  - Scanning (addresses, ports, vulnerabilities)
  - Gaining access
  - Maintaining Access
  - Covering Tracks

Tools of the Attacker

- The following are a few of the most popular tools used by network attackers:
  - Enumeration tools (dumpreg, netview and netuser)
  - Port/address scanners (AngryIP, nmap, Nessus)
  - Vulnerability scanners (Meta Sploit, Core Impact, ISS)
  - Packet Sniffers (Snort, Wire Shark, Air Magnet)
  - Root kits
  - Cryptographic cracking tools (Cain, WepCrack)
  - Malicious codes (worms, Trojan horse, time bombs)
  - System hijack tools (netcat, MetaSploit, Core Impact)

Countermeasures

- DMZ/NAT
- IDS/IPS
- Content Filtering/NAC
- Firewalls/proxy services
- Authentication/Authorization/Accounting
- Self-defending networks
- Policies, procedures, standards guidelines
- Training and awareness