KEMENTERIAN PENDIDIKAN MALAYSIA

UTeM
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FTMK
FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI



/ myftmk

http://ftmk.utem.edu.my

Chapter 12

INTRODUCTION TO NETWORK SECURITY

by

Nazrulazhar Bahaman

nazrulazhar@utem.edu.my

Learning Outcome

- Explain about computer network viruses, worms and Trojan Horses
- Describe the techniques used to mitigate viruses, worms, and Trojan Horses.
- Explain how reconnaissance attacks are launched.
- Explain how access attacks are launched.
- Explain how Denial of Service attacks are launched.
- Describe the techniques used to mitigate reconnaissance attacks, access attacks, and DoS attacks.

Types of Attacks

There are **FOUR** categories of attacks:

- **Malicious Codes Attacks** – Worm, Virus, and Trojan horse
- **Reconnaissance Attacks**
- **Access Attacks**
- **Denial of Service (DoS) Attacks**

Malicious Codes Attacks -
Viruses, Worms and Trojan Horses

Malicious Codes Attacks

Primary Vulnerabilities for End User Devices

- A virus is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation.
- A worm executes arbitrary code and installs copies of itself in the infected computer's memory, which infects other hosts.
- A Trojan horse is different only in that the entire application was written to look like something else, when, in fact, it is an attack tool.

Virus
Human Virus vs Computer Virus

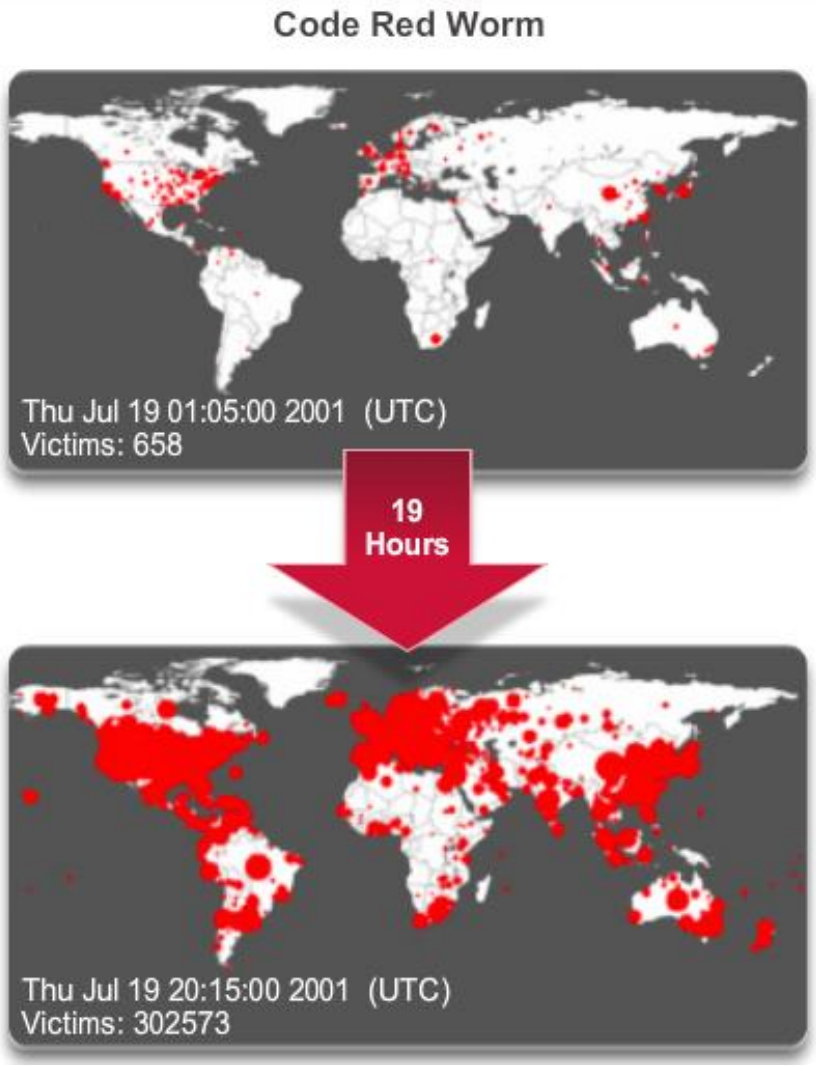
- Vital Information Resources Under Siege (VIRUS)

Human Virus

Computer Virus

Worms Characteristics

- Worms are a particularly dangerous type of hostile code.
  - They replicate themselves by independently exploiting vulnerabilities in networks.
  - Worms usually slow down networks.
- Worms do not require user intervention, and can spread extremely fast over the network.



Worms
SQL Slammer Worms

- In January 2001, the SQL Slammer Worm slowed down global Internet traffic as a result of DoS.
- Over 250,000 hosts were affected within 30 minutes of its release.
- The worm exploited a buffer overflow bug in Microsoft's SQL Server.
  - A patch for this vulnerability was released in mid-2002, so the servers that were affected were those that did not have the update patch applied.

Worms
Worm Components

- Enabling vulnerability
  - A worm installs itself using an exploit vector on a vulnerable system.
- Propagation mechanism
  - After gaining access to devices, a worm replicates and selects new targets.
- Payload
  - When the device is infected with a worm, the attacker has access to the host, often as a privileged user.
  - Attackers could use a local exploit to escalate their privilege level to administrator.

Worms
Exploit and Comparison

- Probe phase:
  - Vulnerable targets are identified using ping scans.
  - Application scans are used to identify operating systems and vulnerable software.
  - Hackers obtain passwords using social engineering, dictionary attack, brute-force, or network sniffing.
- Penetrate phase:
  - Exploit code is transferred to the vulnerable target.
  - Goal is to get the target to execute the exploit code through an attack vector, such as a buffer overflow, ActiveX or Common Gateway Interface (CGI) vulnerabilities, or an email virus.
- Persist phase:
  - After the attack is successfully launched in the memory, the code tries to persist on the target system.
  - The goal is to ensure that the attacker code is running and available to the attacker even if the system reboots.
  - Achieved by modifying system files, making registry changes, and installing new code.

Worms
Exploit and Comparison

- Propagate phase:
  - The attacker attempts to extend the attack to other targets by looking for vulnerable neighboring machines.
  - Propagation vectors include emailing copies of the attack to other systems, uploading files to other systems using file shares or FTP services, active web connections, and file transfers through Internet Relay Chat.
- Paralyze phase:
  - Actual damage is done to the system.
  - Files can be erased, systems can crash, information can be stolen, and distributed DDoS attacks can be launched.

Trojan Horses

Trojan Horse Concept

- A Trojan horse is a program that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.
- Trojan horses can appear to be useful or interesting programs, or at the very least harmless to an unsuspecting user, but are actually harmful when executed.
- Trojan horses are not self-replicating which distinguishes them from viruses and worms.

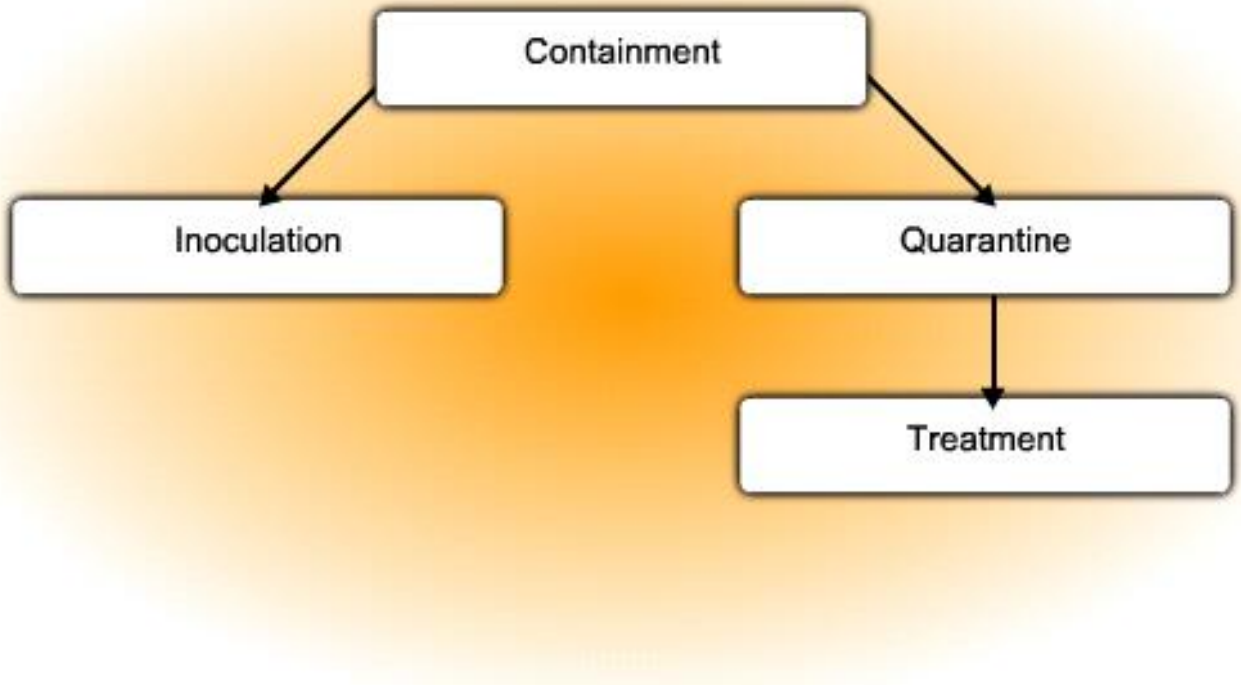
Trojan Horses

Trojan Horse Classification

- **Remote-access Trojan Horse** - Enables unauthorized remote access
- **Data sending Trojan Horse** - Provides the attacker with sensitive data, such as passwords
- **Destructive Trojan Horse** - Corrupts or deletes files
- **Proxy Trojan Horse** - User's computer functions as a proxy server
- **FTP Trojan Horse (opens port 21)** - Security software disabler Trojan Horse (stops antivirus programs or firewalls from functioning)
- **Security software disabler Trojan horse** - Stops antivirus programs or firewalls from functioning.
- **DoS Trojan Horse** - Slows or halts network activity

Worm Mitigation

- Worm attack mitigation requires diligence on the part of system and network administration staff.
- There is a four phase process to mitigate an active worm attacks.



Worm Mitigation - Cont.

- **Containment Phase**
  - Limits the spread of a worm infection to areas of the network that are already affected.
  - Compartmentalizes and segments the network to slow down or stop the worm to prevent currently infected hosts from targeting and infecting other systems.
  - Uses both outgoing and incoming ACLs on routers and firewalls at control points within the network.
- **Inoculation Phase**
  - Runs parallel to or subsequent to the containment phase.
  - All uninfected systems are patched with the appropriate vendor patch for the vulnerability.
  - The inoculation process further deprives the worm of any available targets.

Worm Mitigation - Cont.

- **Quarantine Phase**
  - Tracks down and identifies infected machines within the contained areas and disconnects, blocks, or removes them.
  - This isolates these systems appropriately for the Treatment Phase.
- **Treatment Phase**
  - Actively infected systems are disinfected of the worm.
  - Terminates the worm process, removes modified files or system settings that the worm introduced, and patches the vulnerability the worm used to exploit the system.
  - In more severe cases, completely reinstalling the system to ensure that the worm and its by products are removed.

Worm Mitigation
SQL Slammer Worm

- The SQL Slammer worm used UDP port 1434.
- This port should normally be blocked by a firewall on the perimeter.
- However, most infections enter internally and, therefore, to prevent the spreading of this worm, it would be necessary to block this port on all devices throughout the internal network.
- When SQL Slammer was propagating, some organizations could not block UDP port 1434 because it was required to access the SQL Server for legitimate business transactions.
- Permit only selective access to a small number of clients using SQL Server.

Reconnaissance Attacks

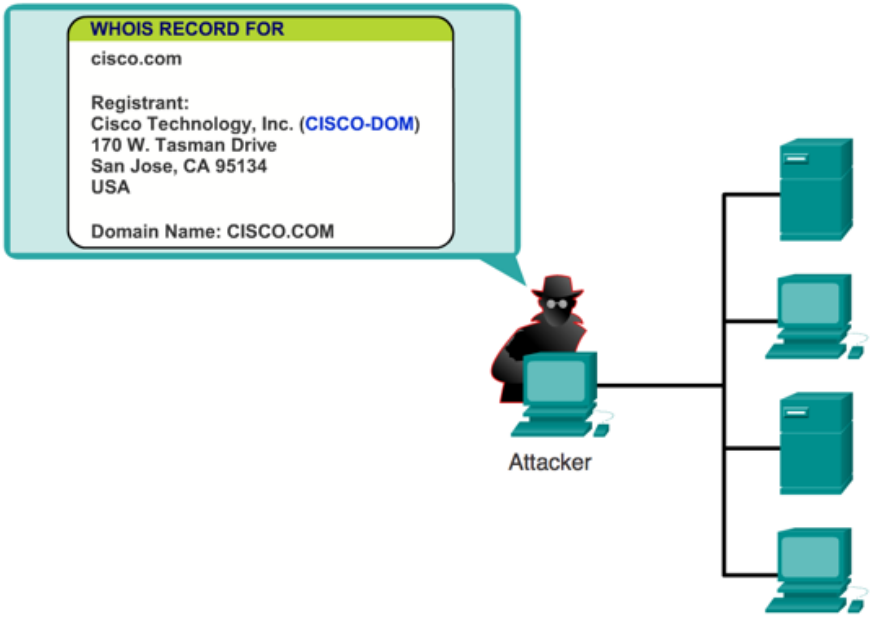
Reconnaissance Attacks

- Reconnaissance, also known as information gathering is the unauthorized discovery and mapping of systems, services, or vulnerabilities.
- In most cases, precedes an access or DoS attack.
- Reconnaissance attacks can consist of the following:
  - Internet information queries
  - Ping sweeps
  - Port scans
  - Packet sniffers

Reconnaissance Attacks

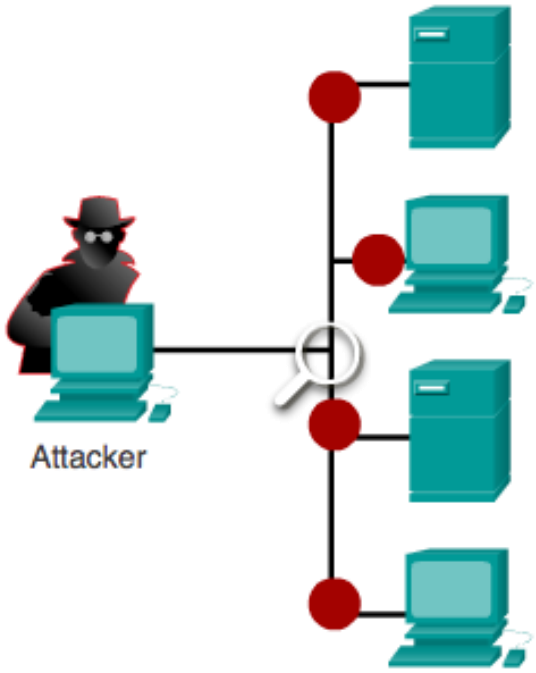
Internet Information Queries

- DNS queries can reveal information, such as who owns a particular domain and what addresses have been assigned to that domain.
- Use tools such as whois, nslookup, ...



Reconnaissance Attacks
Packet Sniffer

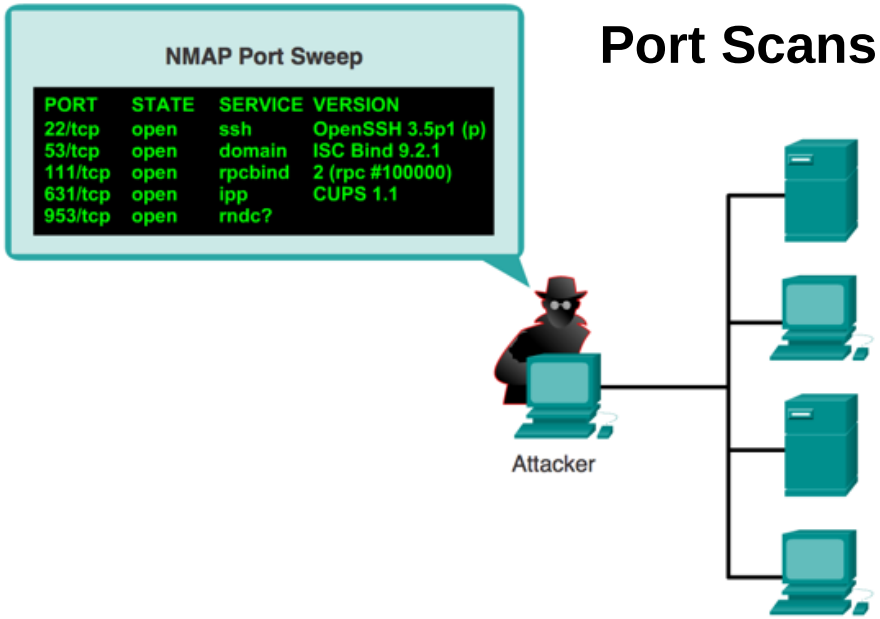
- A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN.
- Packet sniffers can only work in the same collision domain as the network being attacked.
- Promiscuous mode is a mode in which the network adapter card sends all packets that are received on the physical network wire to an application for processing.
- Wireshark is an example of a packet sniffer.



Reconnaissance Attacks

Ping Sweeps and Port Scans

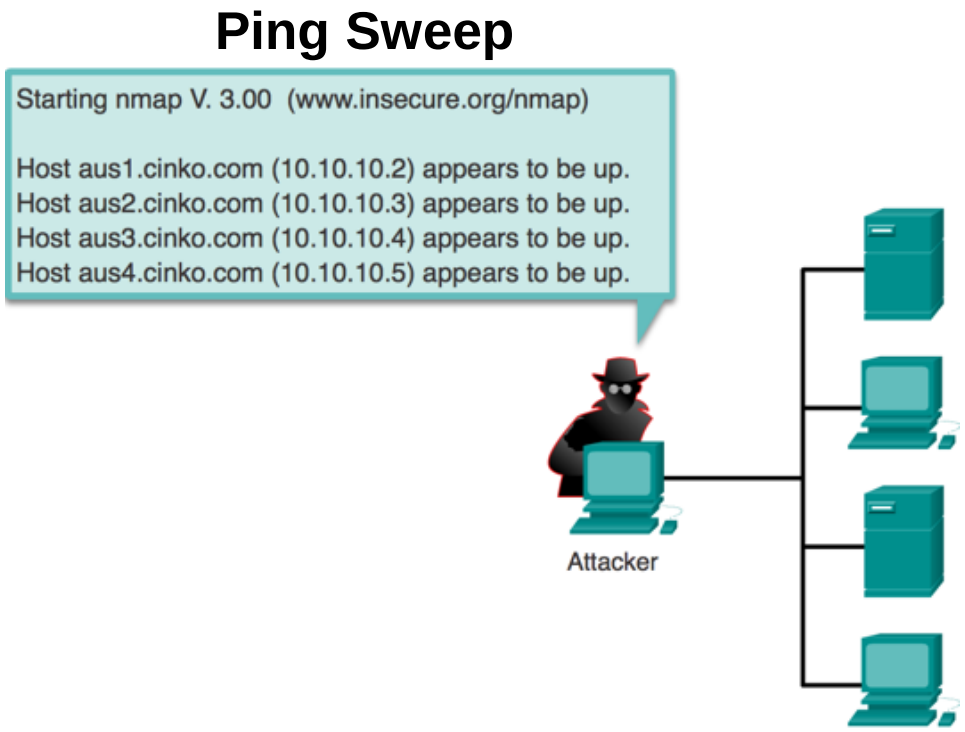
- A ping sweep, or ICMP sweep, scans to determine which range of IP addresses map to live hosts.
- A port scan consists of sending a message to each port, one port at a time. Response received indicates whether the port is used and can; therefore, be probed for weakness.



Reconnaissance Attacks

Ping Sweeps and Port Scans Cont.

- As legitimate tools, ping sweep and port scan applications run a series of tests against hosts to identify vulnerable services.
- The information is gathered by examining IP addressing and port data from both TCP and UDP ports.



Reconnaissance Attacks

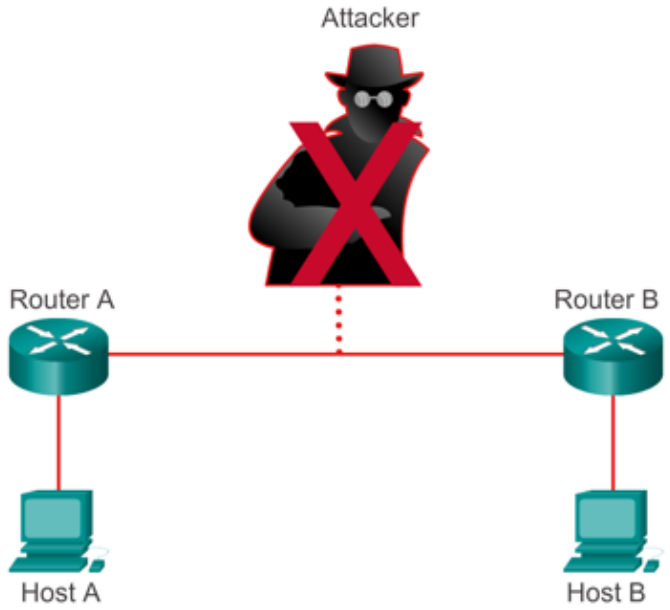
Mitigating Reconnaissance Attacks

- Reconnaissance attacks are typically the precursor to additional attacks, with the intent of gaining unauthorized access to a network or disrupting network functionality.
- A network security professional can detect when a reconnaissance attack is underway by receiving notifications from preconfigured alarms, such as the number of ICMP requests per second.

Reconnaissance Attacks

Mitigating Reconnaissance Attacks

- Implementing and enforcing a policy directive that forbids the use of protocols with known susceptibilities to eavesdropping.
- Using encryption that meets the data security needs of the organization without imposing an excessive burden on the system resources or the users.
- Use anti-sniffer tools to detect sniffer attacks.
- Using switched networks.
- Use a firewall and IPS.



Access Attacks

Access Attacks

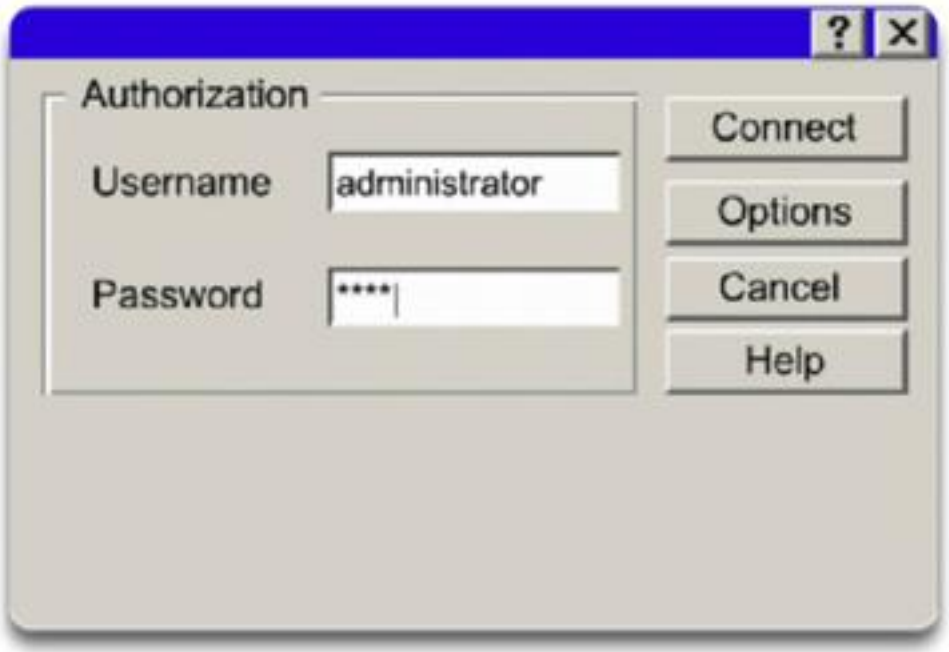
- Access attacks exploit known vulnerabilities in authentication services, FTP services and web services to gain entry to web accounts, confidential databases, and other sensitive information for these reasons:
  - Retrieve data
  - Gain access
  - Escalate their access privileges

Access Attacks
Types of Access Attacks

- Access attacks can be performed in a number of different ways
  - Password attacks
  - Trust exploitation
  - Port redirection
  - Man-in-the-middle attacks
  - Buffer overflow

Types of Attacks
Password Attacks

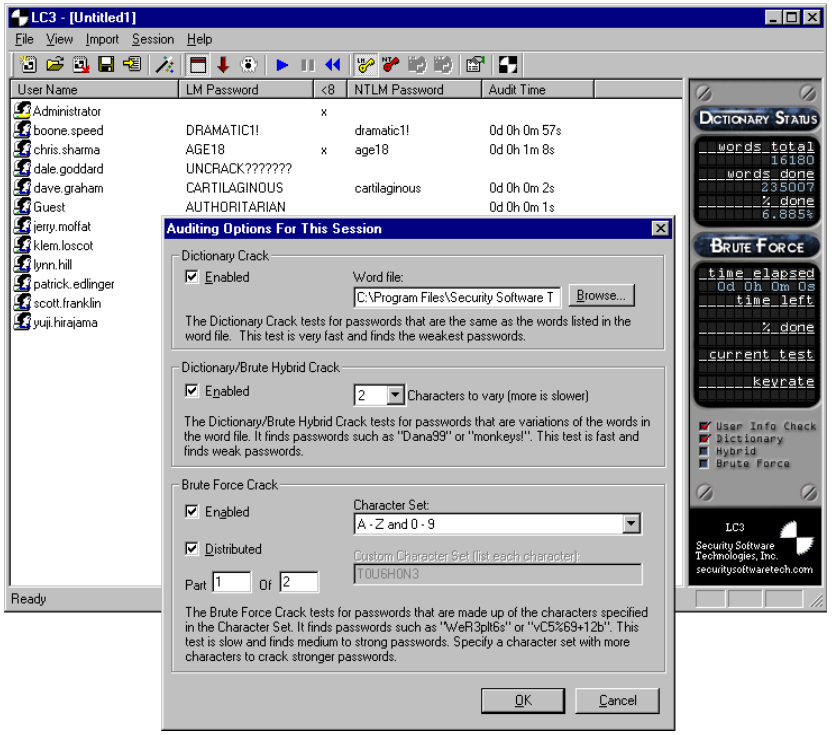
- Hackers implement password attacks using the following:
  - Brute-force attacks - An access attack method that involves a software program attempting to discover a system password by using an electronic dictionary.
  - Trojan horse programs
  - IP spoofing
  - Packet sniffers
  - Manipulating users



Types of Attacks

Password Attack Example

- L0phtCrack "loft-crack" takes the hashes of passwords and generates the plaintext passwords from them
- Passwords are compromised using one of two methods:
  - Dictionary cracking
  - Brute-force computation

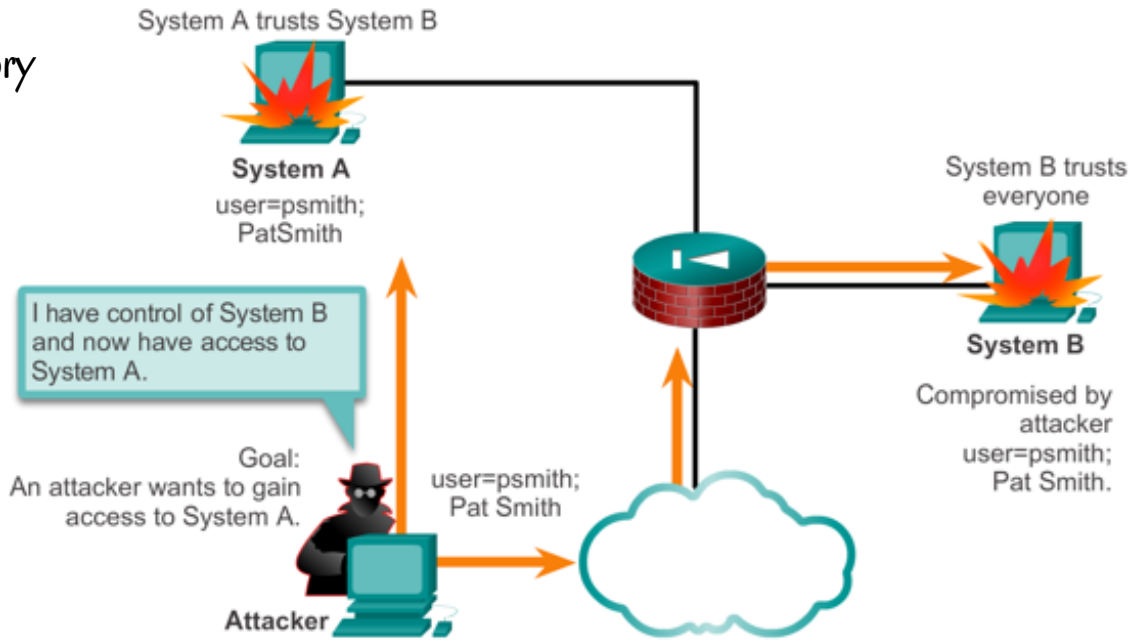


Types of Attacks
Trust Exploitation

- Trust exploitation refers to an individual taking advantage of a trust relationship within a network.
- An example of when trust exploitation takes place is when a perimeter network is connected to a corporate network.
  - These network segments often contain DNS, SMTP, and HTTP servers.
  - Because these servers all reside on the same segment, a compromise of one system can lead to the compromise of other systems if those other systems also trust systems that are attached to the same network.
- Another example of trust exploitation is a Demilitarized Zone (DMZ) host that has a trust relationship with an inside host that is connected to the inside firewall interface.
- The inside host trusts the DMZ host. When the DMZ host is compromised, the attacker can leverage that trust relationship to attack the inside host.

Types of Attacks
Trust Exploitation

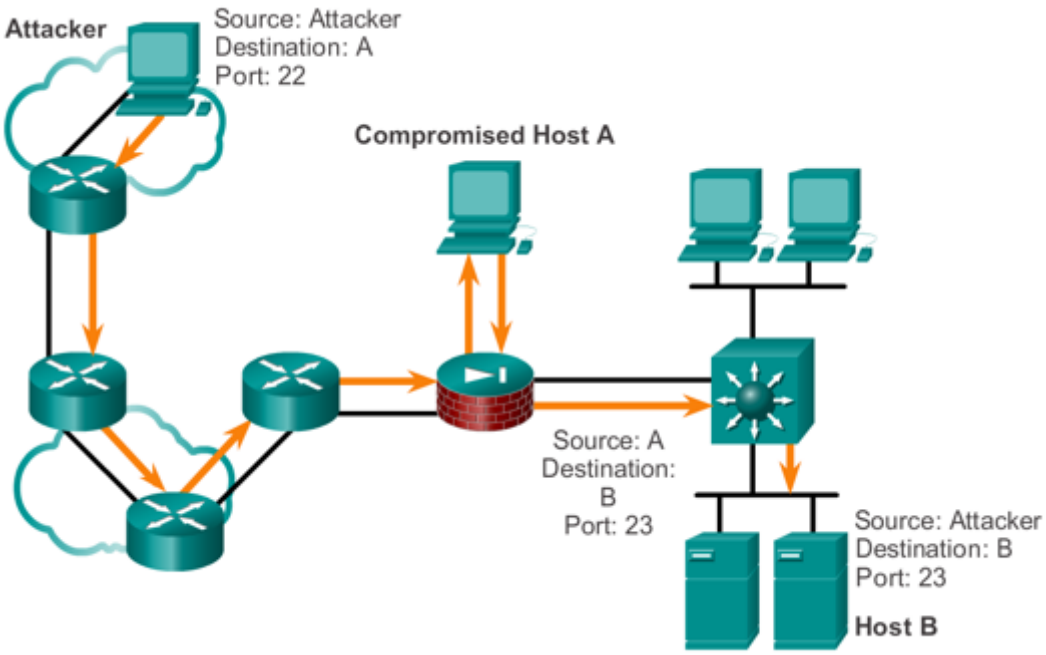
- A hacker leverages existing trust relationships.
- Several trust models exist:
  - Windows:
    - Domains
    - Active directory
  - Linux and UNIX:
    - NIS
    - NIS+



Types of Attacks
Port Redirection

- A port redirection attack is a type of trust exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise have been dropped.
- Port redirection bypasses the firewall rule sets by changing the normal source port for a type of network traffic.
- You can mitigate port redirection by using proper trust models that are network-specific.
- Assuming a system is under attack, an IPS can help detect a hacker and prevent installation of such utilities on a host.

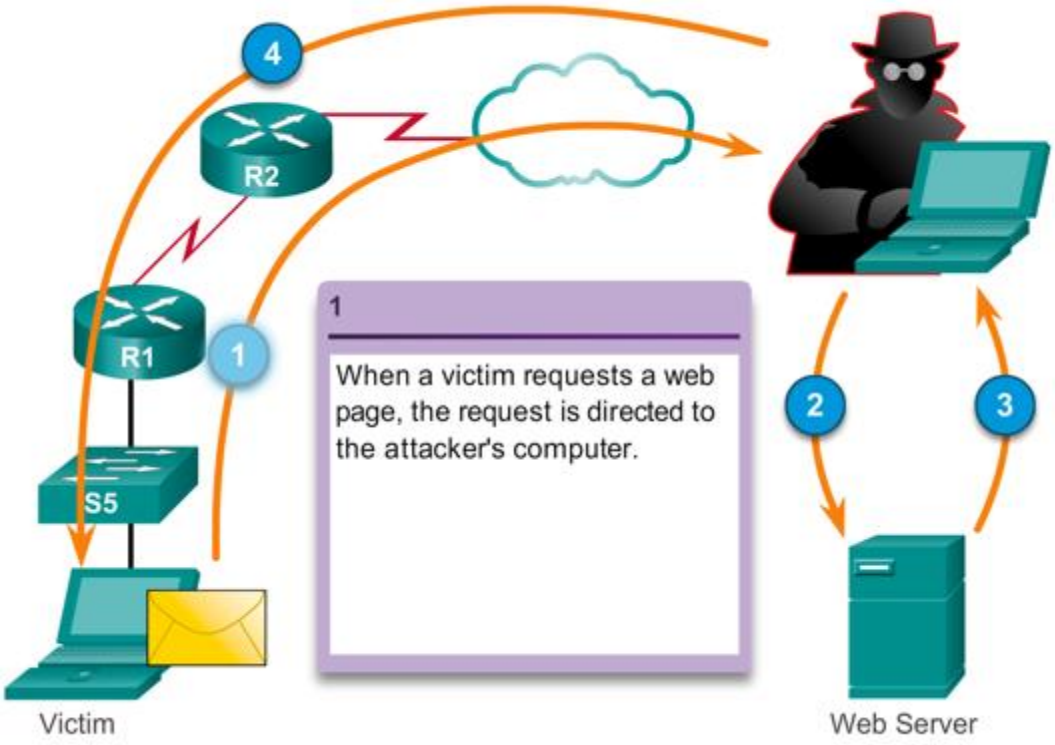
Types of Attacks
Port Redirection Cont.



Types of Attacks
Man-in-the-Middle Attacks (MITM)

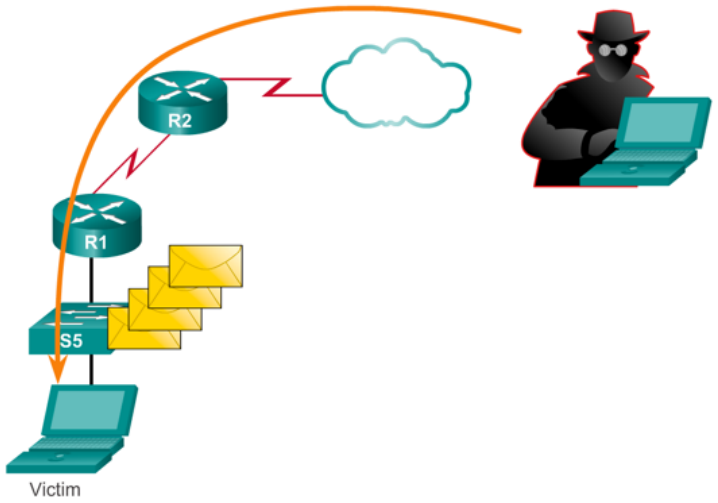
- MITM attacks have these purposes:
  - Theft of information
  - Hijacking of an ongoing session to gain access to your internal network resources
  - Traffic analysis to obtain information about your network and network users
  - DoS
  - Corruption of transmitted data
  - Introduction of new information into network sessions
- An example of a MITM attack is when someone working for your ISP gains access to all network packets that transfer between your network and any other network.

Types of Attacks
Man-in-the-Middle Attacks (MITM) Cont.



Types of Attacks
Buffer Overflow Attacks

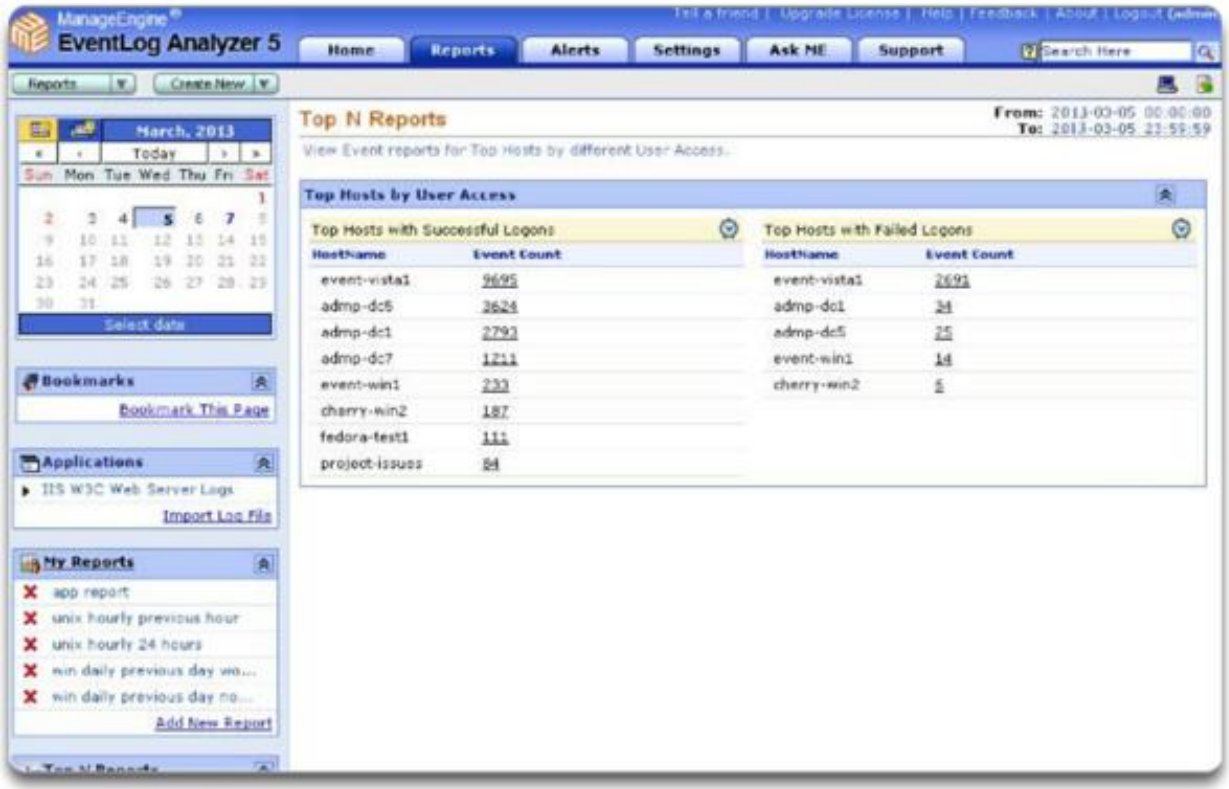
- A program writes data beyond the allocated buffer memory.
- Buffer overflows usually arise as a consequence of a bug in a C or C++ program.
- A result of the overflow is that valid data is overwritten or exploited to enable the execution of malicious code.
- The overflow can be used to modify the values of program variables and cause the program to jump to unintended places, or even replace valid program instructions with arbitrary code.



Access Attacks

Mitigating Access Attacks

- Access attacks in general can be detected by reviewing logs, bandwidth utilization, and process loads.
- The network security policy should specify that logs are formally maintained for all network devices and servers.



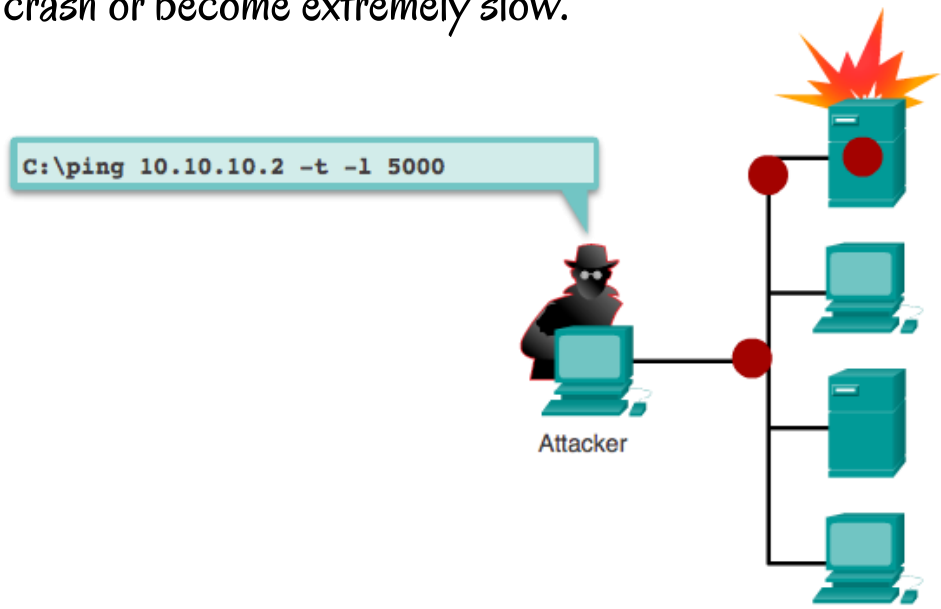
Mitigating Access Attacks

- Techniques to mitigate access attacks include:
  - Strong password security
  - Principle of minimum trust
  - Cryptography
  - Applying operating system and application patches
- Practices that help to ensure a strong password policy:
  - Disable accounts after a specific number of unsuccessful logins. This practice helps to prevent continuous password attempts.
  - Do not use plaintext passwords. Use either a one-time password or encrypted password.
  - Use strong passwords. Strong passwords are at least eight characters and contain uppercase letters, lowercase letters, numbers, and special characters.

DoS Attacks

DoS Attacks
DoS Attack

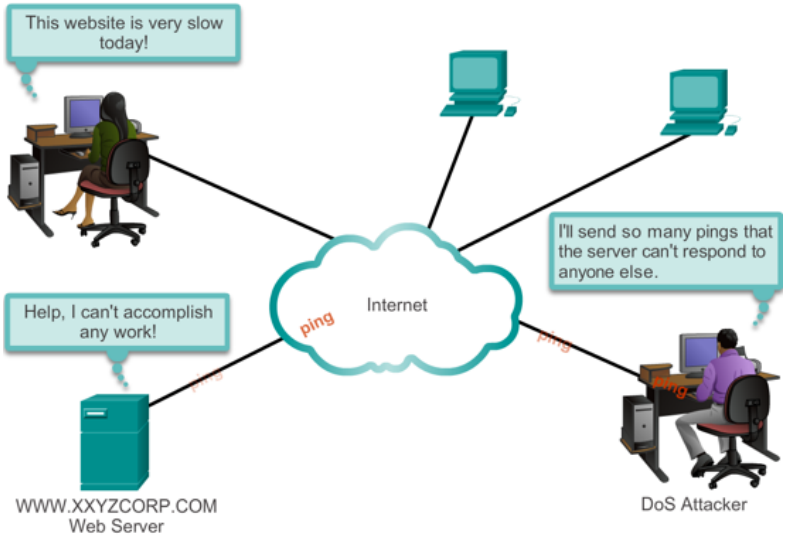
- A DoS attack is a network attack that results in some sort of interruption of service to users, devices, or applications.
- There are two major reasons a DoS attack occurs:
  - A host or application fails to handle an unexpected condition, such as maliciously formatted input data, an unexpected interaction of system components, or simple resource exhaustion.
  - A network, host, or application is unable to handle an enormous quantity of data, causing the system to crash or become extremely slow.

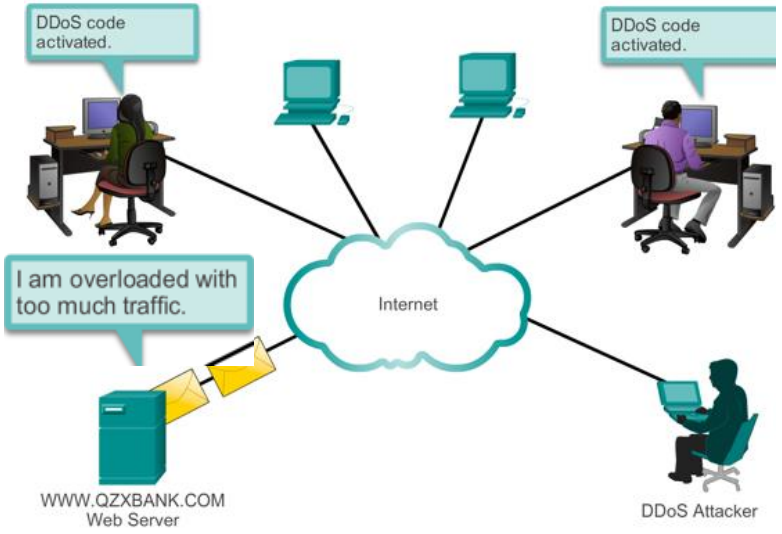


DoS Attacks

DoS and DDoS

- A Distributed DoS Attack (DDoS) is similar in intent to a DoS attack, except that a DDoS attack originates from multiple coordinated sources.

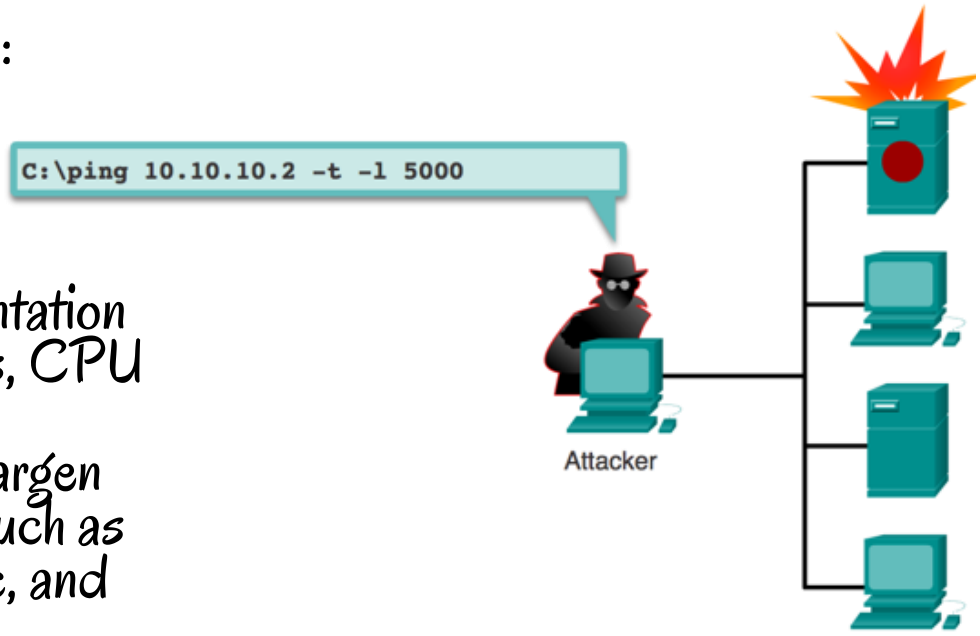




DoS Attacks

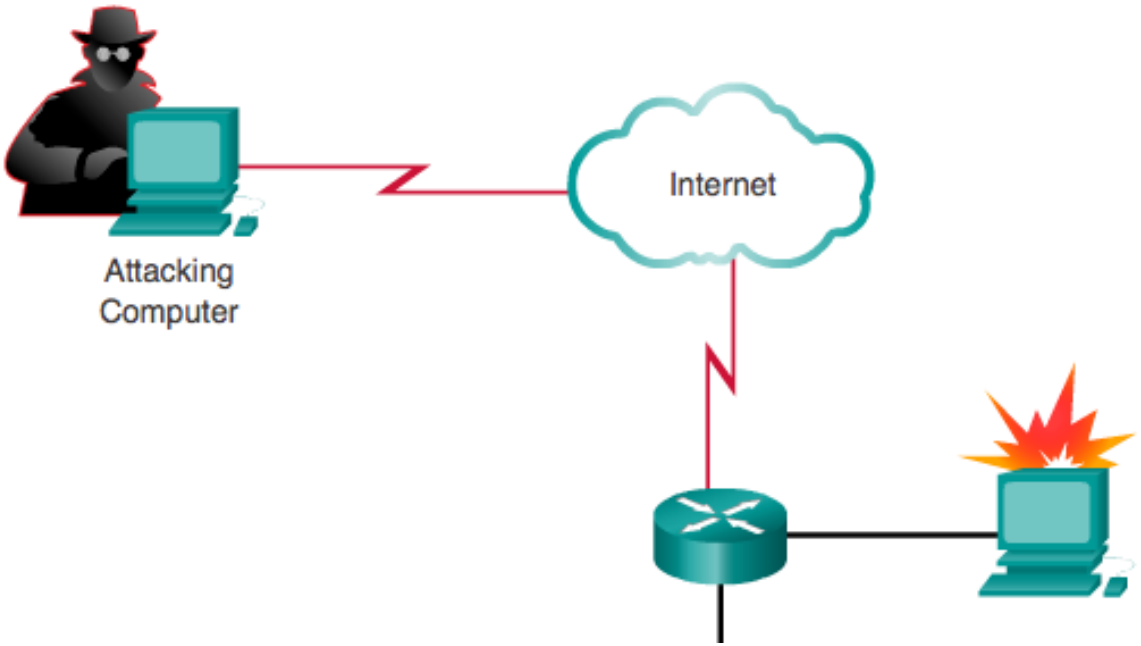
Types of DoS Attacks

- Among the most difficult to completely eliminate because they require so little effort to execute.
- Types of DoS attacks include:
  - Ping of death
  - Smurf Attack
  - TCP SYN flood attack
- Others include packet fragmentation and reassembly, E-mail bombs, CPU hogging, Malicious applets, Misconfiguring routers, the chargen attack, out-of-band attacks, such as WinNuke, Land.c, Teardrop.c, and Targa.c.



DoS Attacks
Ping of Death

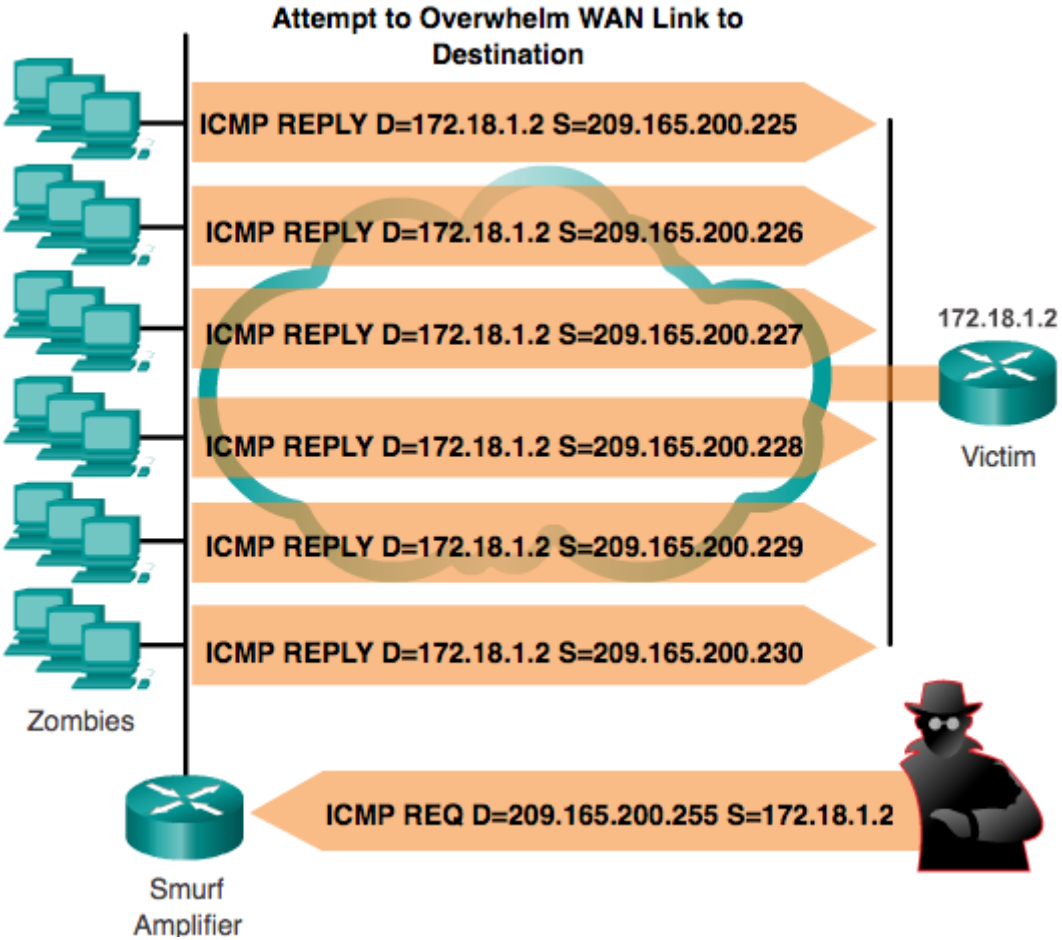
- Legacy attack that sent an echo request in an IP packet larger than the maximum packet size of 65,535 bytes. Sending a ping of this size can crash the target computer.
- A variant of this attack is to crash a system by sending ICMP fragments, which fills the reassembly buffers of the target.



DoS Attacks
Smurf Attack

- A Smurf Attack is a DDoS attack in which large numbers of ICMP packets with the intended victim's spoofed source IP are broadcast to a computer network.
- This attack sends a large number of ICMP requests to directed broadcast addresses, all with spoofed source addresses on the same network as the respective directed broadcast.
  - If the routing device delivering traffic to those broadcast addresses forwards the directed broadcasts, all hosts on the destination networks send ICMP replies, multiplying the traffic by the number of hosts on the networks.
  - On a multi-access broadcast network, hundreds of machines might reply to each packet.

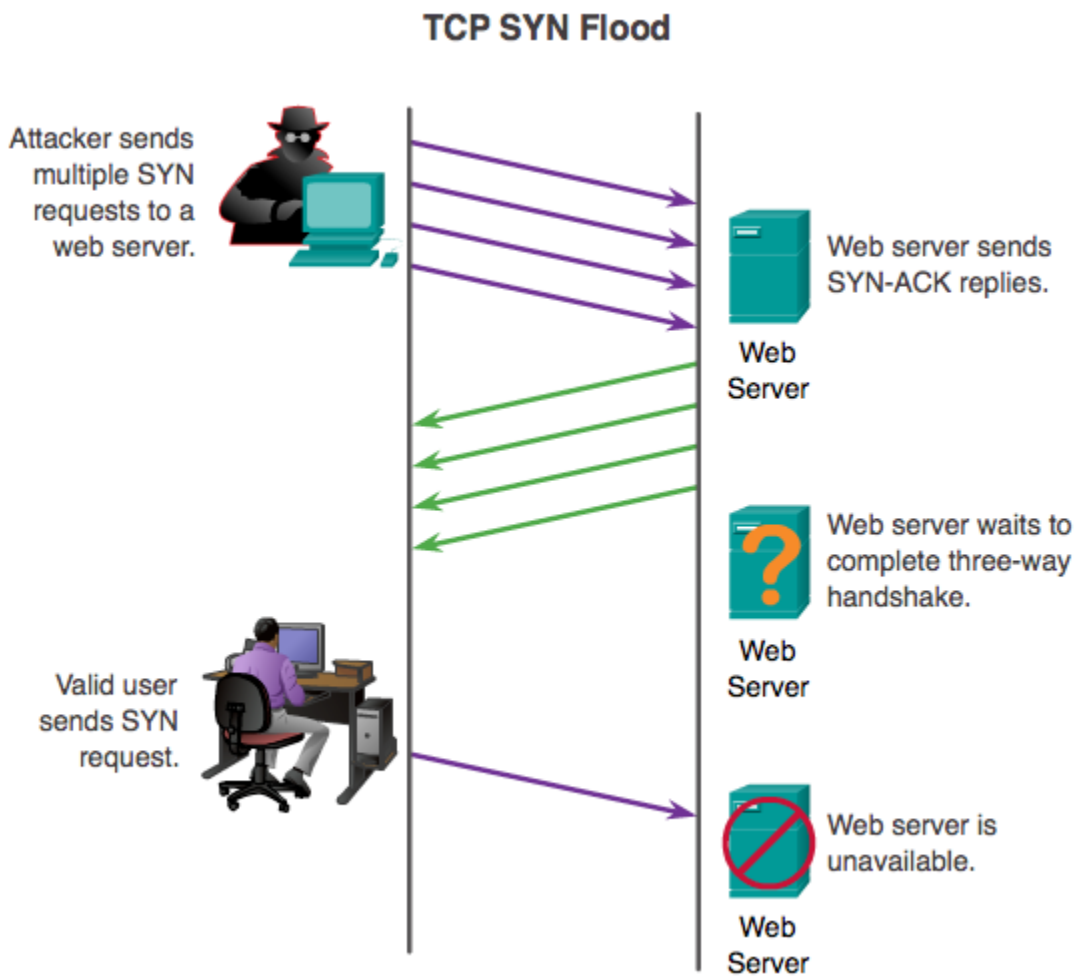
DoS Attacks
Smurf Attack Cont.



DoS Attacks
SYN Flood Attack

- A flood of TCP SYN packets is sent, often with a forged sender address.
  - Each packet is handled like a connection request, causing the server to spawn a half-open (embryonic) connection by sending back a TCP SYN-ACK packet and waiting for a packet in response from the sender address.
  - However, because the sender address is forged, the response never comes.
  - These half-open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests until after the attack ends.

DoS Attacks
SYN Flood Attack Cont.



DoS Attacks
Symptoms of a DoS Attack

- There are five basic ways that DoS attacks can do harm:
  - Consumption of resources, such as bandwidth, disk space, or processor time.
  - Disruption of configuration information, such as routing information.
  - Disruption of state information, such as unsolicited resetting of TCP sessions.
  - Disruption of physical network components.
  - Obstruction of communication between the victim and others.

DoS Attacks

Mitigating DoS Attacks

- IPS and firewalls (Cisco ASAs and ISRs)
- Antispoofing technologies
- Quality of Service-traffic policing

DoS Attacks
Mitigating DoS Attacks Cont.

- Anti-DoS features on routers and firewalls:
  - Proper configuration of anti-DoS features on routers and firewalls can help limit the effectiveness of an attack.
  - These features often involve limits on the amount of half-open TCP connections that a system allows at any given time.

- Anti-spoof features on routers and firewalls:
  - Proper configuration of anti-spoof features on your routers and firewalls can reduce your risk of attack.
  - These features include an appropriate filtering with access lists, unicast reverse path forwarding that looks up the routing table to identify spoofed packets, disabling of source route options, and others.

THE END