Common network attacks

Types of Network Attacks

- This course classifies attacks in three major categories:

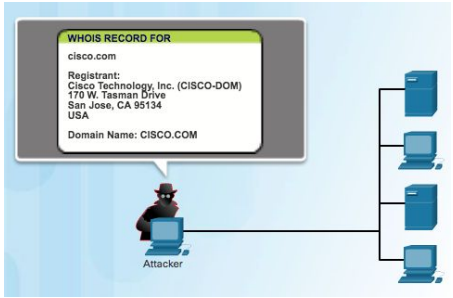
- By categorizing network attacks, it is possible to address types of attacks rather than individual attacks.

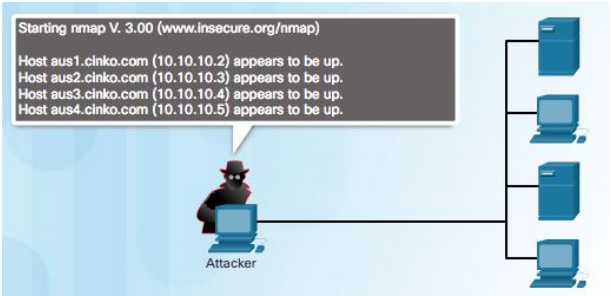
Reconnaissance Attacks

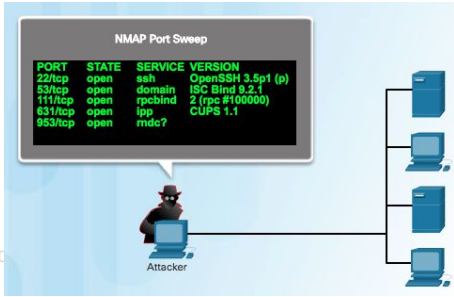
- Also known as information gathering, reconnaissance attacks perform unauthorized discovery and mapping of systems, services, or vulnerabilities.
- Analogous to a thief surveying a neighborhood by going door-to-door pretending to sell something.
- Called host profiling when directed at an endpoint.
- Recon attacks precede intrusive access attacks or DoS attack and employ the use of widely available tools.

Sample Reconnaissance Attacks

- Techniques used by threat actors:
  - **Perform an information query of a target** - Threat actor is looking for initial information about a target. Tools: Google search, public information from DNS registries using dig, nslookup, and whois.
  - **Initiate a ping sweep of the target networks** - Threat actor initiates a ping sweep of the target networks revealed by the previous DNS queries to identify target network addresses. Identifies which IP addresses are active and creation of logical topology.
  - **Initiate a port scan of active IP addresses** - Threat actor initiates port scans on hosts identified by the ping sweep to determine which ports or services are available. Port scanning tools such as Nmap, SuperScan, Angry IP Scanner, and NetScan Tools initiate connections to the target hosts by scanning for ports that are open on the target computers.







Access Attacks

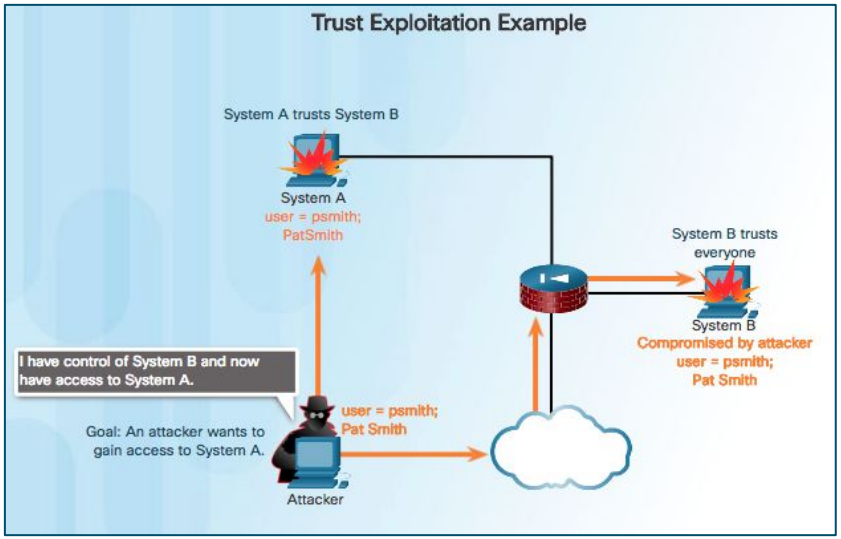
- Access attacks exploit vulnerabilities in authentication services, FTP services, and web services to retrieve data, gain access to systems, or to escalate access privileges.

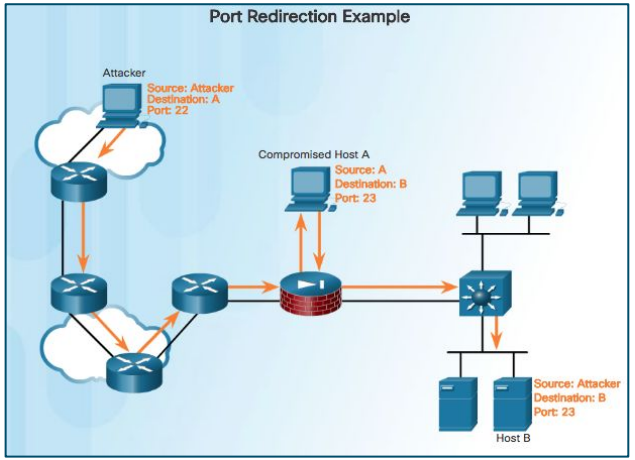
- There are at least three reasons that threat actors would use access attacks on networks or systems:
  - To retrieve data
  - To gain access to systems
  - To escalate access privileges

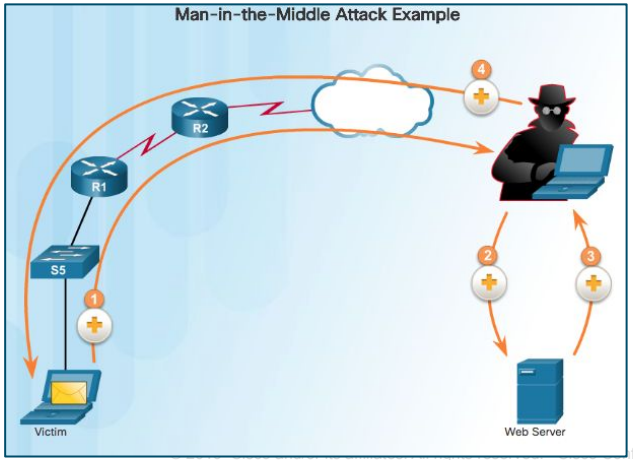
Types of Access Attacks

- **Password attack** - Attempt to discover critical system passwords using phishing attacks, dictionary attacks, brute-force attacks, network sniffing, or using social engineering techniques.
- **Pass-the-hash** - Has access to the user's machine and uses malware to gain access to the stored password hashes. The threat actor then uses the hashes to authenticate to other remote servers or devices.
- **Trust exploitation** - Use a trusted host to gain access to network resources.
- **Port redirection** - Uses a compromised system as a base for attacks against other targets.
- **Man-in-the-middle attack** - Threat actor is positioned in between two legitimate entities in order to read, modify, or redirect the data that passes between the two parties.
- **IP, MAC, DHCP Spoofing** - One device attempts to pose as another by falsifying address data.

Types of Access Attacks (Cont.)







Social Engineering Attacks

- Type of access attack that attempts to manipulate individuals into performing actions or divulging confidential information needed to access a network.
  - Examples of social engineering attacks include:
    - **Pretexting** - Calls an individual and lies to them in an attempt to gain access to privileged data. Pretends to need personal or financial data in order to confirm the identity of the recipient.
    - **Spam** - Use spam email to trick a user into clicking an infected link, or downloading an infected file.
    - **Phishing** - Common version is the threat actor sends enticing custom-targeted spam email to individuals with the hope the target user clicks on a link or downloads malicious code.
    - **Something for Something (Quid pro quo)** - Requests personal information from a party in exchange for something like a free gift.
    - **Tailgating** - Follows an authorized person with a corporate badge into a badge-secure location.
    - **Baiting** - Threat actor leaves a malware-infected physical device, such as a USB flash drive in a public location such as a corporate washroom. The finder finds the device and inserts it into their computer.
    - **Visual hacking** – Physically observes the victim entering credentials such as a workstation login, an ATM PIN, or the combination on a physical lock. Also known as “shoulder surfing”.

Phishing Social Engineering Attacks

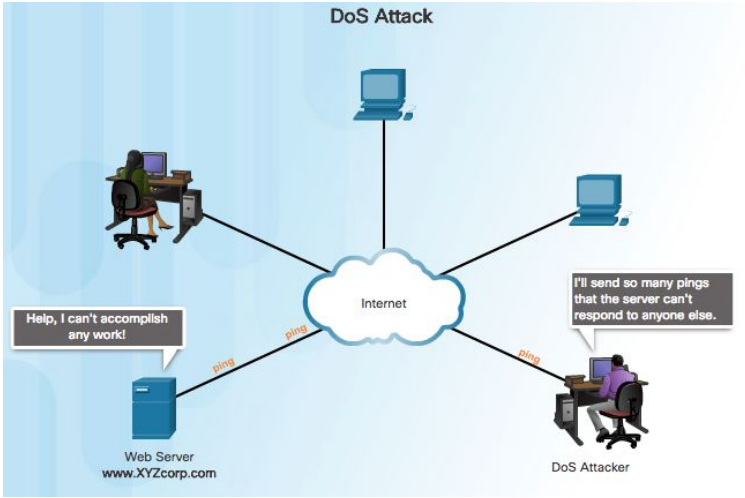
- Phishing
  - Common social engineering technique that threat actors use to send emails that appear to be from a legitimate organization (such as a bank)
  - Variations include:
    - **Spear phishing** - Targeted phishing attack tailored for a specific individual or organization and is more likely to successfully deceive the target.
    - **Whaling** – Similar to spear phishing but is focused on big targets such as top executives of an organization.
    - **Pharming** – Compromises domain name services by injecting entries into local host files. Pharming also includes poisoning the DNS by compromising the DHCP servers that specify DNS servers to their clients.
    - **Watering hole** – Determines websites that a target group visits regularly and attempts to compromise those websites by infecting them with malware that can identify and target only members of the target group.
    - **Vishing** – Phishing attack using voice and the phone system instead of email.
    - **Smishing** – Phishing attack using SMS texting instead of email.

Strengthening the Weakest Link

- People are typically the weakest link in cybersecurity
- Organizations must actively train their personnel and create a “security-aware culture.”

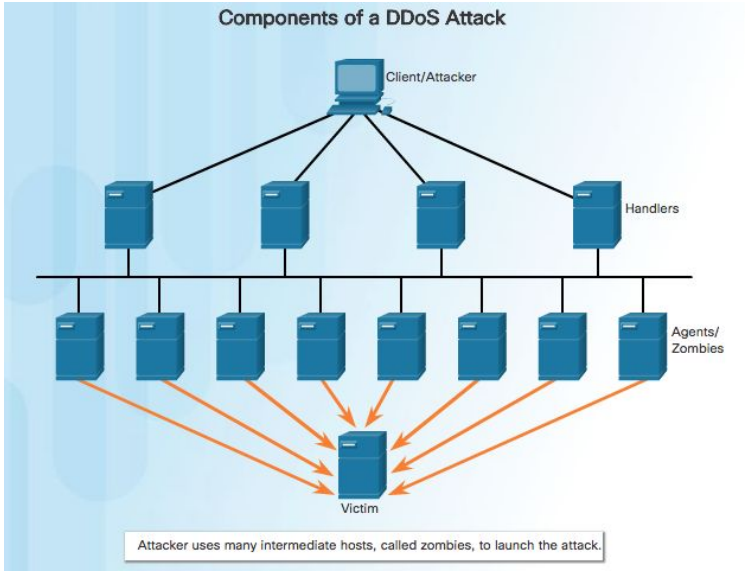
Denial of Service Attacks

- Typically result in some sort of interruption of service to users, devices, or applications.
- Can be caused by overwhelming a target device with a large quantity of traffic or by using maliciously formatted packets.
- A threat actor forwards packets containing errors that cannot be identified by the application, or forwards improperly formatted packets.

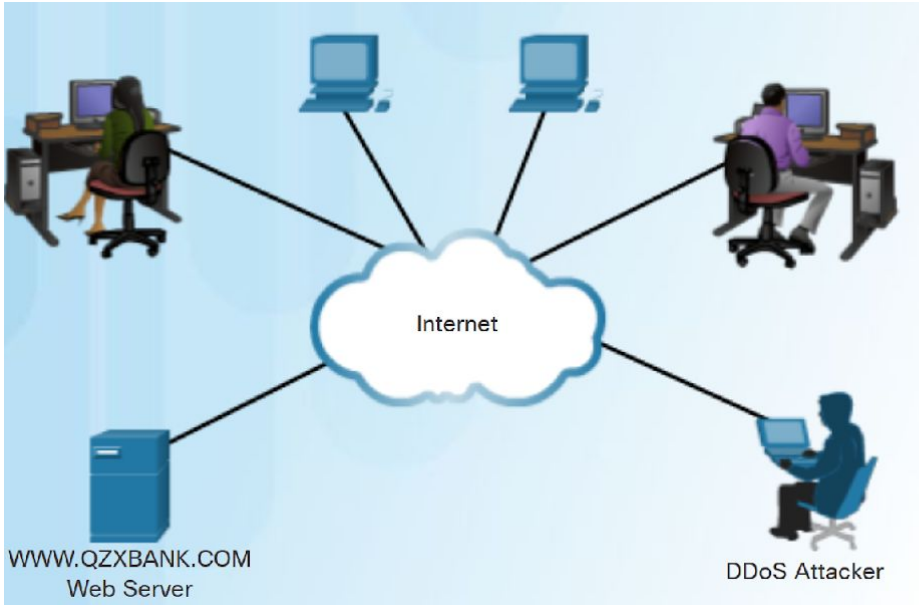


DDoS Attacks

- DDoS Attacks
  - Compromises many hosts
  - Originates from multiple, coordinated sources
- DDoS terms:
  - **Zombies** – Refers to a group of compromised hosts (i.e., agents). These hosts run malicious code referred to as robots (i.e., bots).
  - **Bots** – Bots are malware designed to infect a host and communicate with a handler system. Bots can also log keystrokes, gather passwords, capture and analyze packets, and more.
  - **Botnet** – Refers to a group of zombies infected using self-propagating malware (i.e., bots) and are controlled by handlers.
  - **Handlers** – Refers to a master **command-and-control** server controlling groups of zombies. The originator of a botnet can remotely control the zombies.
  - **Botmaster** – This is the threat actor in control of the botnet and handlers.



Example DDoS Attack

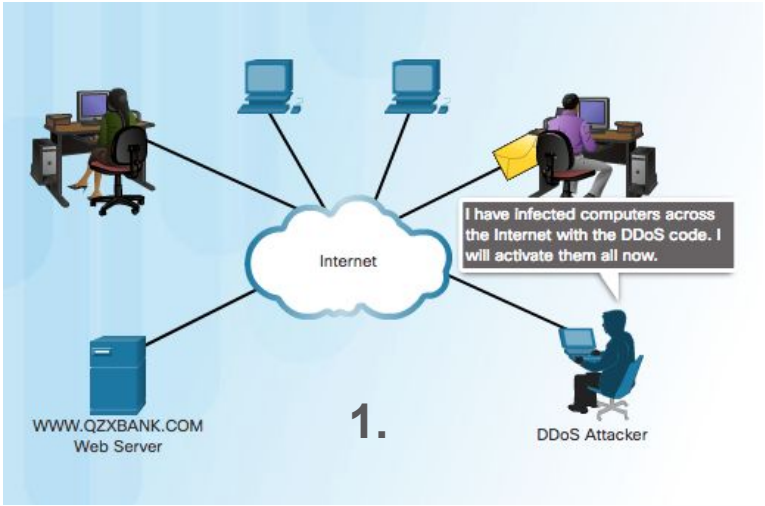


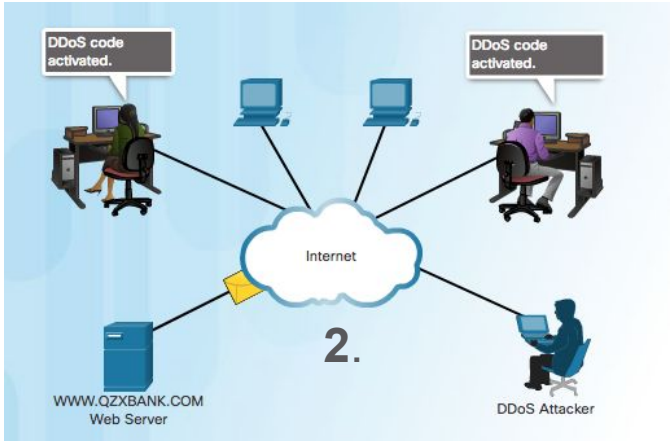
1. The threat actor builds or purchases a botnet of zombie hosts.

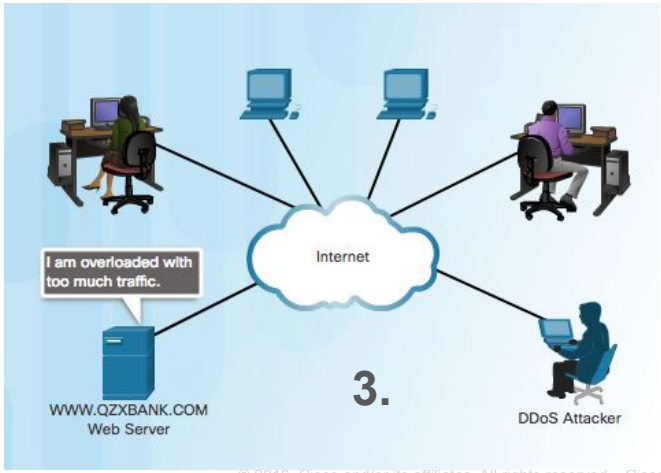
2. Zombie computers continue to scan and infect more targets to create more zombies.

3. When ready, the botmaster uses the handler systems to make the botnet of zombies carry out the DDoS attack on the chosen target.

Example DDoS Attack (Cont.)

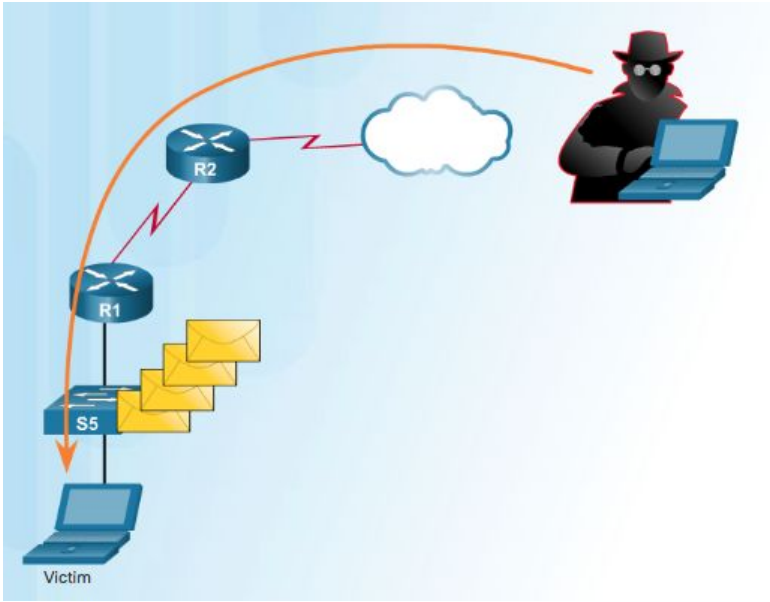






Buffer Overflow Attack

- The goal is to find a system memory-related flaw on a server and exploit it.
- Exploiting the buffer memory by overwhelming it with unexpected values usually renders the system inoperable.
- For example:
  - Threat actor enters input that is larger than expected by the application running on a server.
  - The application accepts the large amount of input and stores it in memory.
  - It consumes the associated memory buffer and potentially overwrites adjacent memory, eventually corrupting the system and causing it to crash.



Evasion Methods

- Threat actors learned long ago that malware and attack methods are most effective when they are undetected.
- Some of the evasion methods used by threat actors include encryption and tunneling, resource exhaustion, traffic fragmentation, protocol-level misinterpretation, traffic substitution, traffic insertion, pivoting, and rootkits.
- New attack methods are constantly being developed; therefore, network security personnel must be aware of the latest attack methods in order to detect them.

Lecture Summary

- Network attacks can be classified as one or more of the following:
  - Reconnaissance
  - Access attacks
  - Social engineering
  - DoS
  - Buffer overflow
- Threat actors use a variety of evasion methods including:
  - Encryption and tunneling
  - Resource exhaustion
  - Traffic fragmentation
  - Protocol-level misinterpretation
  - Traffic substitution
  - Traffic insertion
  - Pivoting
  - Rootkits

New Terms and Commands

- Access attacks
- Adware
- Attack indicators
- Baiting
- Black Hat Hackers
- Botmaster
- Botnet
- Bots
- Buffer overflow attack
- Countermeasure
- Cybercriminals
- Debuggers
- Encryption Tools
- Exploit
- Forensic Tools
- Fuzzers
- Gray Hat Hackers
- hacker
- Hacking Operating Systems
- Hacktivists
- Handlers
- Impact
- Man-in-the-middle attack
- Network Scanning
- Packet Crafting Tools
- Packet Sniffers Tools
- Pass-the-hash
- Password Crackers
- Pharming
- Phishing
- Pretexting
- Quid pro quo
- reconnaissance
- Risk

New Terms and Commands

- Risk acceptance
- Risk avoidance
- Risk limitation
- Risk transfer
- Rootkit Detectors
- Scareware
- Script Kiddies
- Smishing
- Social engineering
- Spear phishing
- Spoofing
- Spyware
- State-Sponsored Hacking
- Tailgating
- Threat
- Trojan horse
- virus
- Vishing
- Visual hacking
- Vulnerability
- Vulnerability Broker
- Vulnerability Exploitation Tools
- Vulnerability Scanners
- Watering hole
- Whaling
- White Hat Hackers
- Wireless Hacking Tools
- worm
- Zombies