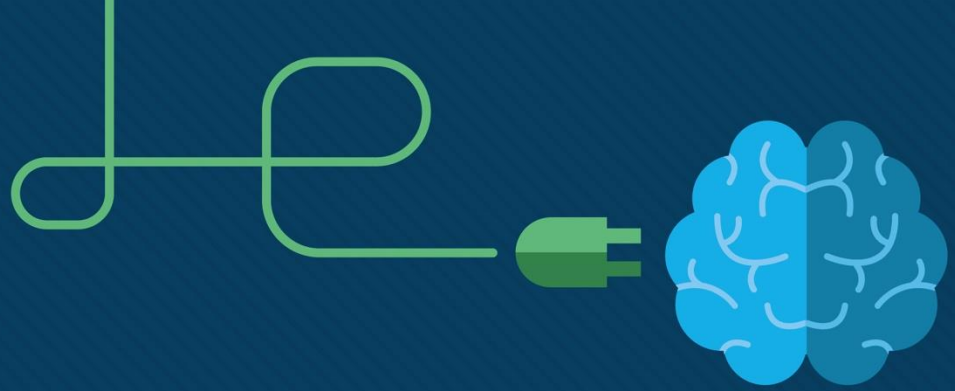


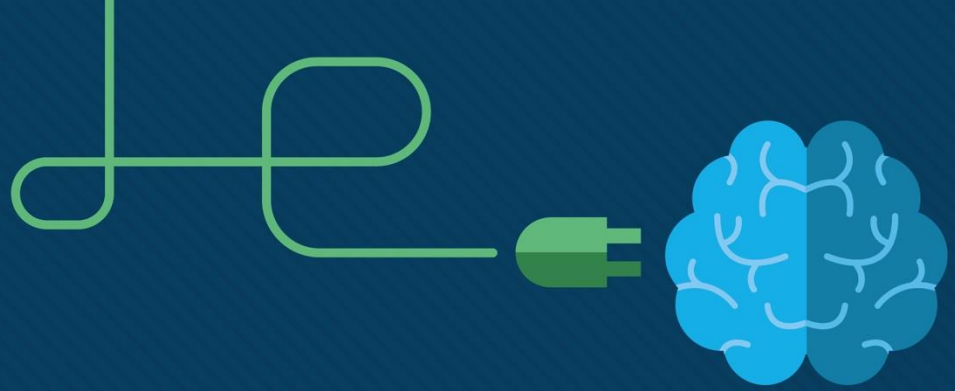
Chapter 6: Principles of Network Security

Instructor Materials

CCNA Cybersecurity Operation v1.1

Chapter 6: Principles of Network Security

CCNA Cybersecurity Operation v1.1
Planning Guide



Chapter 6: Principles of Network Security

CCNA Cybersecurity Operation v1.1

Chapter 6 - Sections & Objectives

- 6.1 Attackers and Their Tools
  - Explain how networks are attacked.
    - Describe the evolution of network security.
    - Describe the various types of attack tools used by Threat Actors.
- 6.2 Common Threats and Attacks
  - Explain the various types of threats and attacks.
    - Describe malware.
    - Explain common network attacks.

6.1 Attackers and Their Tools

Threat, Vulnerability, and Risk

- Threat
  - Potential danger to an asset such as data or the network.
- Vulnerability and Attack Surface
  - Weakness in a system or its design that could be exploited by a threat.
  - Attack surface describes different points where an attacker could get into a system and could get to the data (Example – operating system without security patches)
- Exploit
  - Mechanism used to leverage a vulnerability to compromise an asset.
  - Remote – works over the network.
  - Local – threat actor has user or administrative access to the end system.
- Risk
  - Likelihood that a threat will exploit a vulnerability of an asset and result in an undesirable consequence.

Hacker vs. Threat Actor

- White Hat Hackers
  - Ethical hackers who use their programming skills for good, ethical, and legal purposes.
  - Perform penetration tests to discover vulnerabilities and report to developers before exploitation.
- Grey Hat Hackers
  - Commit crimes and do unethical things but not for personal gain or to cause damage.
  - May compromise network and then disclose the problem so the organization can fix the problem.
- Black Hat Hackers
  - Unethical criminals who violate security for personal gain, or for malicious reasons, such as attacking networks.

Note: Threat actors is a term used to describe grey and black hat hackers.

Evolution of Threat Actors

- Script Kiddies
  - Inexperienced hackers running existing tools and exploits, to cause harm, but typically not for profit.
- State-Sponsored
  - White or black hats who steal government secrets, gather intelligence, and sabotage networks.
  - Targets are foreign governments, terrorist groups, and corporations.
- Cybercriminals
  - Black hats stealing billions of dollars from consumers and businesses.
- Hacktivists
  - Grey hats who rally and protest against political and social ideas.
  - Post articles and videos to leak sensitive information.
- Vulnerability Broker
  - Discover exploits and report them to vendors, sometimes for prizes or rewards.

Who is Attacking Our Network?

Cybercriminals

- Money-motivated threat actors.
- Buy, sell, and trade exploits, and private information and intellectual property.
- Steal from consumers, small businesses, as well as large enterprises and industries.

Cybersecurity Tasks

- Develop good cybersecurity awareness.
- Report cybercrime to authorities.
- Be aware of potential threats in email and web
- Guard important information from theft.
- Organizations must take action and protect their assets, users, and customers.
- Develop cybersecurity tasks and implement those tasks on a reoccurring basis.

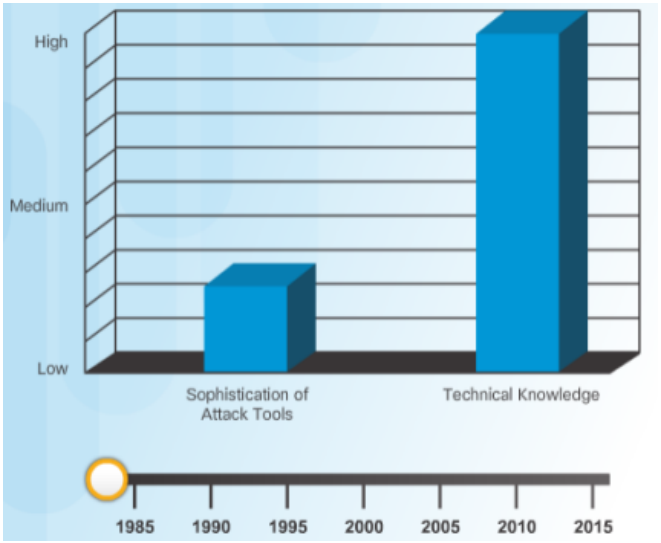
Cyber Threat Indicators

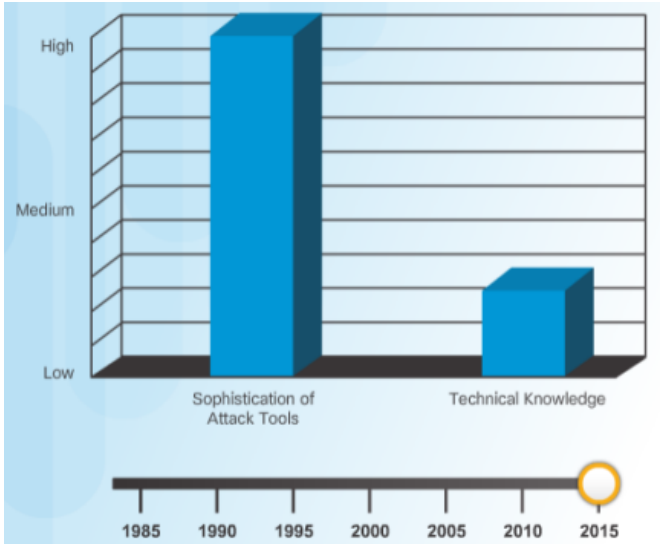
- Each attack has unique identifiable attributes that are known as cyber threat indicators or simply attack indicators.
- U.S. Department of Homeland Security (DHS) and United States Computer Emergency Readiness Team (US-CERT) use the Automated Indicator Sharing (AIS) system that enables sharing of verified attack indicators with public and private sector organizations

Clicking on the link in the email results in an attack.

Introduction of Attack Tools

- Attackers use tools to exploit a vulnerability.
- Sophistication of attack tools and technical knowledge to conduct attacks has changed since 1985.





Evolution of Security Tools

- Common Penetration Testing Tools
  - **Password crackers** - guesses to crack the password and access the system.
  - **Wireless hacking tools** - hack into a wireless network to detect security vulnerabilities.
  - **Network scanning and hacking tools** - probe network devices, servers, and hosts for open ports.
  - **Packet crafting tools** - probe and test a firewall's robustness using specially crafted forged packets.
  - **Packet sniffers** - capture and analyze packets within traditional Ethernet LANs or WLANs.
  - **Rootkit detectors** - directory and file integrity checker used by white hats to detect installed root kits.
  - **Fuzzers** - attempts to discover a computer system's security vulnerabilities.
  - **Forensic tools** - sniff out any trace of evidence existing in a particular computer system.
  - **Debugger tools** - reverse engineer binary files when writing exploits or malware analysis.
  - **Hacking operating systems** - designed operating systems preloaded with tools and technologies optimized for hacking.
  - **Encryption tools** - use algorithm schemes to encode the data to prevent unauthorized access to the encrypted data.
  - **Vulnerability exploitation tools** - determine whether a remote host is vulnerable to a security attack.
  - **Vulnerability scanners** - scan a network or system to identify open ports.

Categories of Attacks

Common Categories of Network Attacks

- **Eavesdropping** - capture and listen to network traffic.
- **Data modification** - alter the captured data in the packet without the knowledge of the sender or receiver.
- **IP address spoofing** - constructs an IP packet that appears to originate from a valid address inside the corporate intranet.
- **Password-based** - uses the stolen valid accounts to obtain lists of other users and network information.
- **Denial-of-Service** - prevents normal use of a computer or network by valid users.
- **Man-in-the-Middle** - hackers position themselves between a source and destination to monitor, capture and control communication.
- **Compromised-Key** - gain access to a secured communication without the sender or receiver being aware of the attack by obtaining the secret key.
- **Sniffer** - an application or device that can read, monitor, and capture network data exchanges and read network packets.

6.2 Common Threats and Attacks

Types of Malware

- Malware
  - Short for malicious software or malicious code.
  - Specifically designed to damage, disrupt, steal or inflict illegitimate action on data hosts or networks.

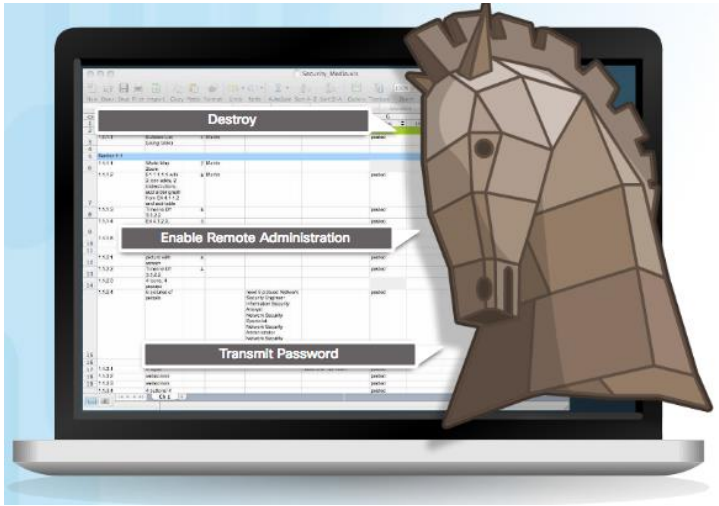
Viruses

- Type of malware that propagates by inserting a copy of itself into another program.
- Spread from one computer to another, infecting computers.
- Spread by USB memory drives, CDs, DVDs, network shares and email.
- Can lay dormant and activate at a specific time and date.
- Requires human action to insert malicious code into another program.
- Executes a specific unwanted, and often harmful, function on a computer.

Trojan Horses

- Malicious code that is designed to look legitimate.
- Often found attached to online games.
- Non-replicating type of malware.
- Exploits the privileges of the user that runs the malware.
- Can cause immediate damage, provide remote access to the system, or access through a back door.

Trojan Horse Classification

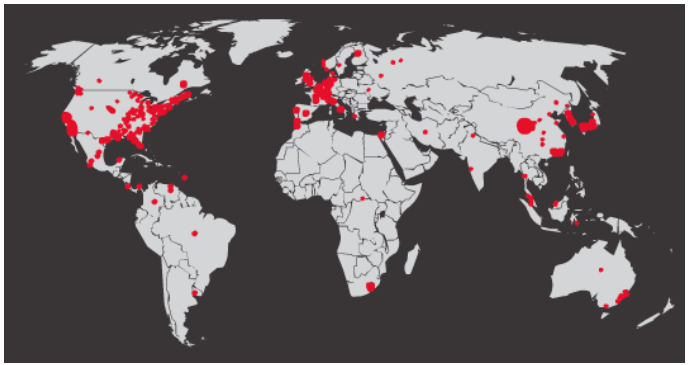


- **Remote-access Trojan horse** - Enables unauthorized remote access.
- **Data-sending Trojan horse** - Provides the threat actor with sensitive data, such as passwords.
- **Destructive Trojan horse** - Corrupts or deletes files.
- **Proxy Trojan horse** - Will use the victim's computer as the source device to launch attacks and perform other illegal activities.
- **FTP Trojan horse** - Enables unauthorized file transfer services on end devices.
- **Security software disabler Trojan horse** - Stops antivirus programs or firewalls from functioning.
- **DoS Trojan horse** - Slows or halts network activity.

Worms

- Executes arbitrary code and installs itself in the memory of the infected device.
- Automatically replicates itself and spreads across the network from system to system.
- Components of a worm attack include an exploiting vulnerability, delivering a malicious payload, and self-propagation.
- Virus requires a host program to run, worms can run by themselves.

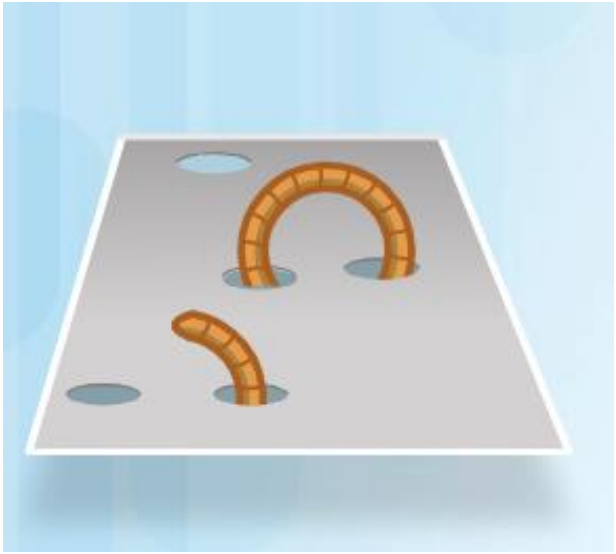
Initial Code Red Worm Infection – 658 servers



Code Red Worm Infection– 19 Hours Later 300,000 servers

Worm Components

- Worm attacks consist of three components:
  - **Enabling vulnerability** - Worm installs itself using an exploit mechanism, such as an email attachment, an executable file, or a Trojan horse, on a vulnerable system.
  - **Propagation mechanism** - After gaining access to a device, the worm replicates itself and locates new targets..
  - **Payload** - Any malicious code that results in some action is a payload which is used to create a backdoor that allows a threat actor access to the infected host or to create a DoS attack.



Ransomware

- Malware that denies access to the infected computer system or its data.
- Cybercriminals demand payment to release the computer system.
- Frequently uses an encryption algorithm to encrypt system files and data, cannot be easily decrypted.
- Email and malicious advertising are vectors for ransomware campaigns.
- Social engineering is also used, cybercriminals who identify themselves as security technicians call homes and persuade users to connect to a website that downloads the ransomware to the user's computer.

Other Malware

- Modern Malware
  - **Spyware** - Used to gather information about a user and send the information to another entity without the user's consent. Can be a system monitor, Trojan horse, Adware, tracking cookies, and key loggers.
  - **Adware** - Typically displays annoying pop-ups to generate revenue for its author. May analyze user interests by tracking the websites visited and send pop-up advertising pertinent to those sites.
  - **Scareware** - Includes scam software which uses social engineering to shock or induce anxiety by creating the perception of a threat. Generally directed at an unsuspecting user and attempts to persuade the user to infect a computer by taking action to address the bogus threat.
  - **Phishing** - Attempts to convince people to divulge sensitive information. Examples include receiving an email from their bank asking users to divulge their account and PIN numbers.
  - **Rootkits** - Installed on a compromised system. After it is installed, it continues to hide its intrusion and provide privileged access to the threat actor.

Common Malware Behaviors

- Computers infected with malware often exhibit one or more of the following:
  - Appearance of strange files, programs, or desktop icons.
  - Antivirus and firewall programs are turning off or reconfiguring settings.
  - Computer screen is freezing or system is crashing.
  - Emails are spontaneously being sent without your knowledge to your contact list.
  - Files have been modified or deleted.
  - Increased CPU and/or memory usage.
  - Problems connecting to networks.
  - Slow computer or web browser speeds.
  - Unknown processes or services running.
  - Unknown TCP or UDP ports open.
  - Connections are made to hosts on the Internet without user action.
  - Strange computer behavior.

Lab – Anatomy of Malware

Networking Academy

Lab – Anatomy of Malware

Objectives

Research and analyze malware

Background / Scenario

Malware, or malicious software, refers to a variety of malicious software programs that can be used to cause harm to computer systems, steal data, and bypass security measures. Malware can also attack critical infrastructure, disable emergency services, cause assembly lines to make defective products, disable electric generators, and disrupt transportation services. Security experts estimate that more than one million new malware threats are released each day. A McAfee Labs report indicates almost 500 million known malware threats at the end of 2015.

Note: You can use the web browser in virtual machine installed in a previous lab to research security related issues. By using the virtual machine, you may prevent malware from being installed on your computer.

Required Resources

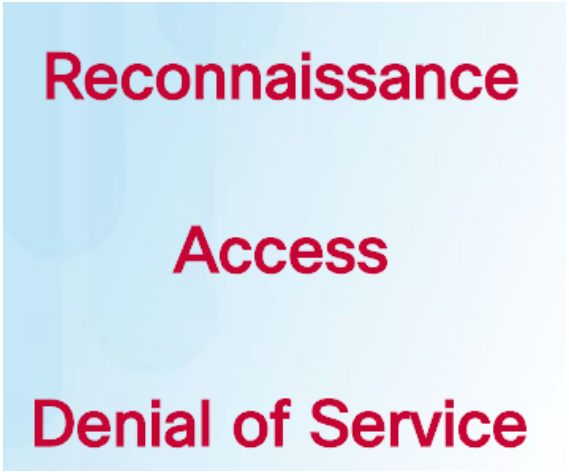
- PC or mobile device with Internet access

Conduct a Search of Recent Malware

a. Using your favorite search engine, conduct a search for recent malware. During your search, choose four examples of malware, each one from a different malware type, and be prepared to discuss details on what each does, how it each is transmitted and the impact each causes.

Types of Network Attacks

- This course classifies attacks in three major categories:



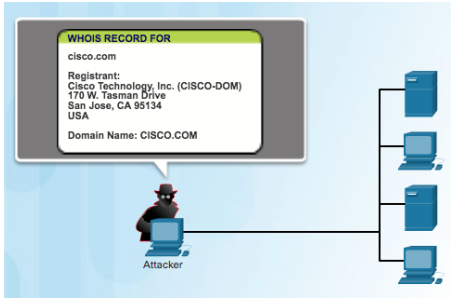
- By categorizing network attacks, it is possible to address types of attacks rather than individual attacks.

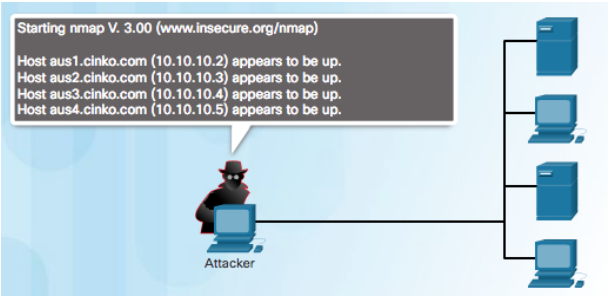
Reconnaissance Attacks

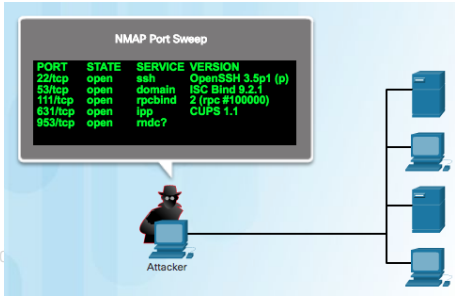
- Also known as information gathering, reconnaissance attacks perform unauthorized discovery and mapping of systems, services, or vulnerabilities.
- Analogous to a thief surveying a neighborhood by going door-to-door pretending to sell something.
- Called host profiling when directed at an endpoint.
- 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.



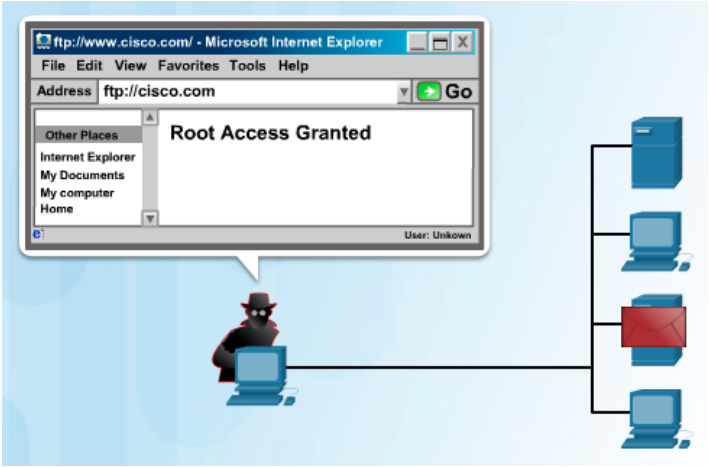




Access Attacks

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

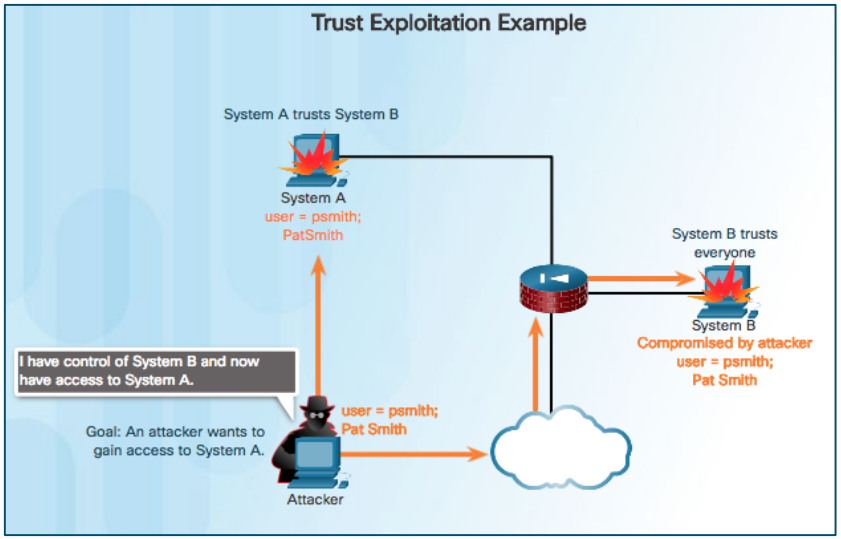
- There are at least three reasons that threat actors would use access attacks on networks or systems:
  - To retrieve data
  - To gain access to systems
  - To escalate access privileges

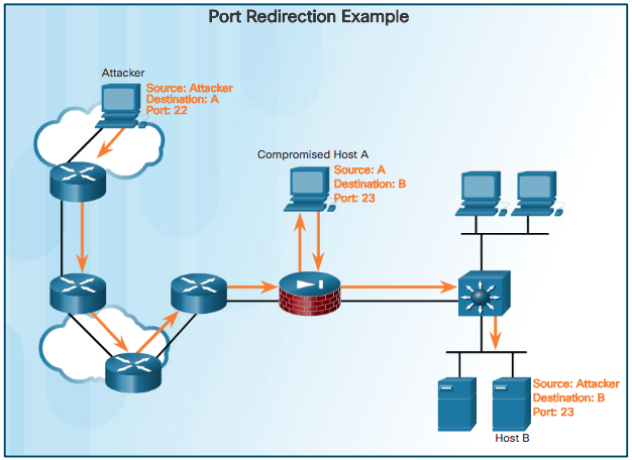


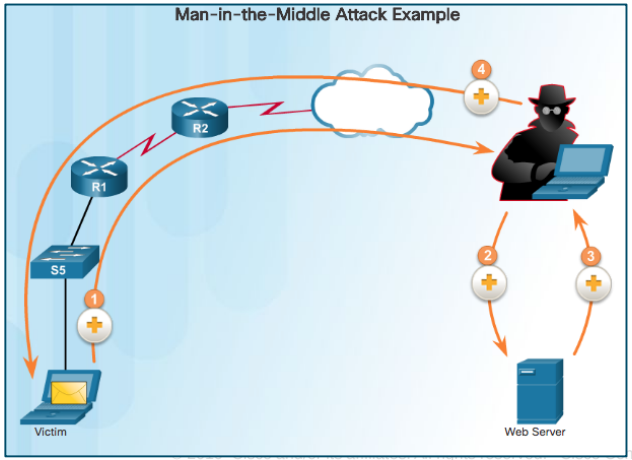
Types of Access Attacks

- **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.”

Lab – Social Engineering

Networking Academy

Lab - Social Engineering

Objectives

Research and identify social engineering attacks

Background / Scenario

Social engineering is an attack with the goal of getting a victim to enter personal or sensitive information, this type of attack can be performed by an attacker utilizing a keylogger, phishing email, or an in-person method. This lab requires the research of social engineering and the identification of ways to recognize and prevent it.

Required Resources

- PC or mobile device with Internet access

Step 1: Read the following article.

Navigate to the following website and read it thoroughly to answer the following questions in step 2.

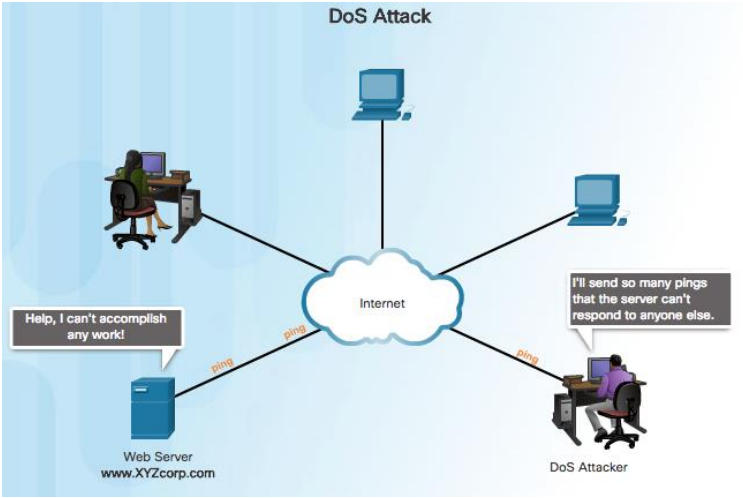
https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972

Step 2: Answer the following questions.

a. What are the three methods used in social engineering to gain access to information?

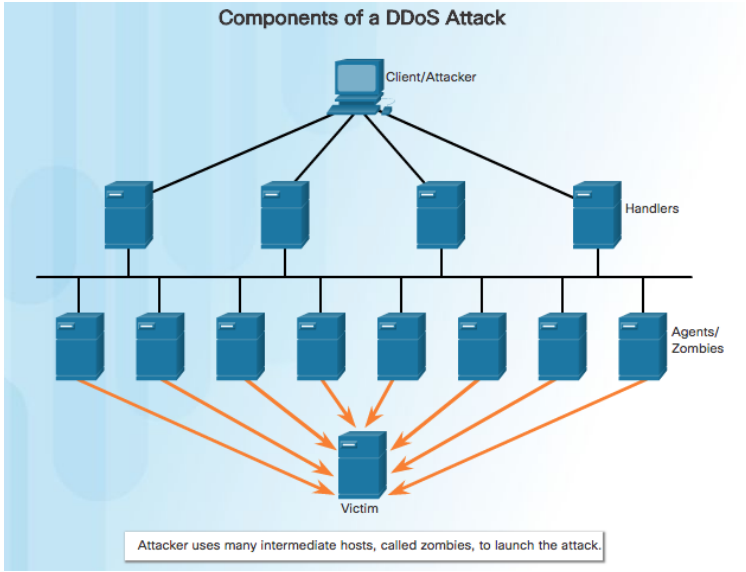
Denial of Service Attacks

- 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.

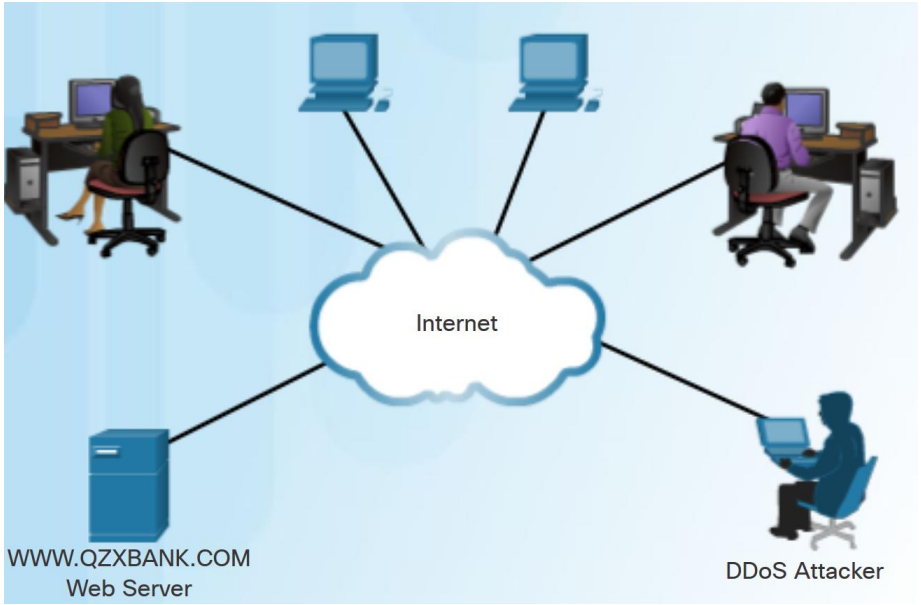


DDoS Attacks

- 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

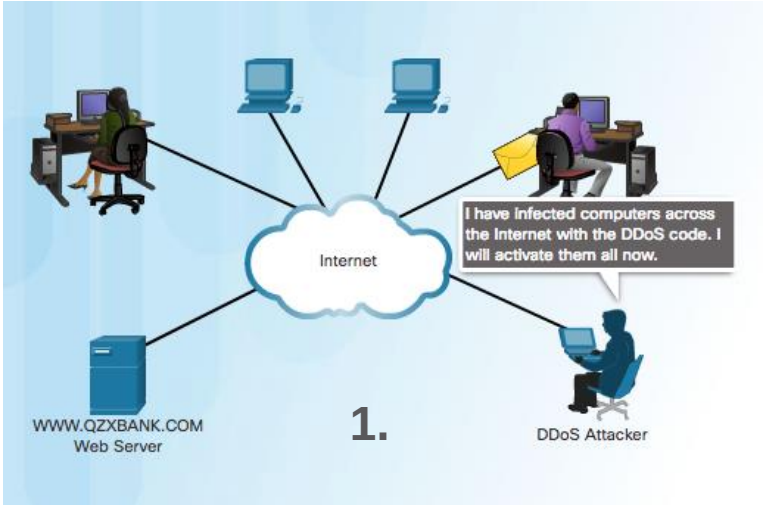


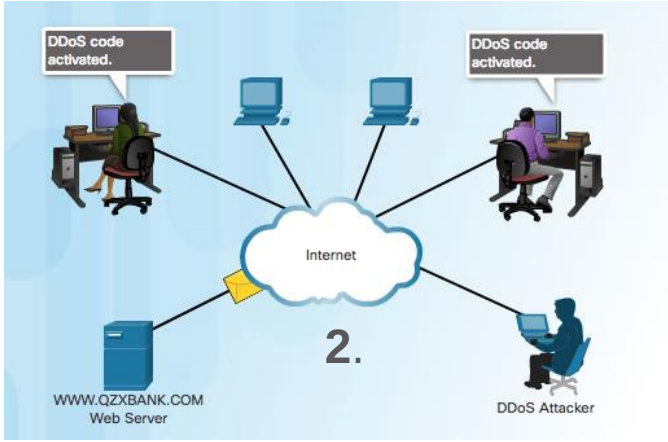
1. The threat actor builds or purchases a botnet of zombie hosts.

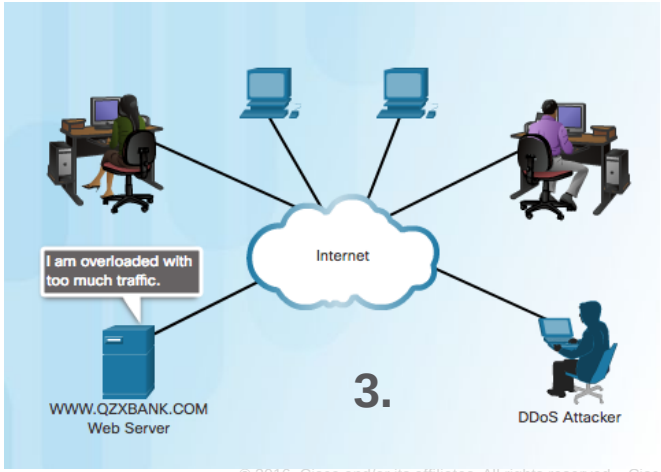
2. Zombie computers continue to scan and infect more targets to create more zombies.

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.)

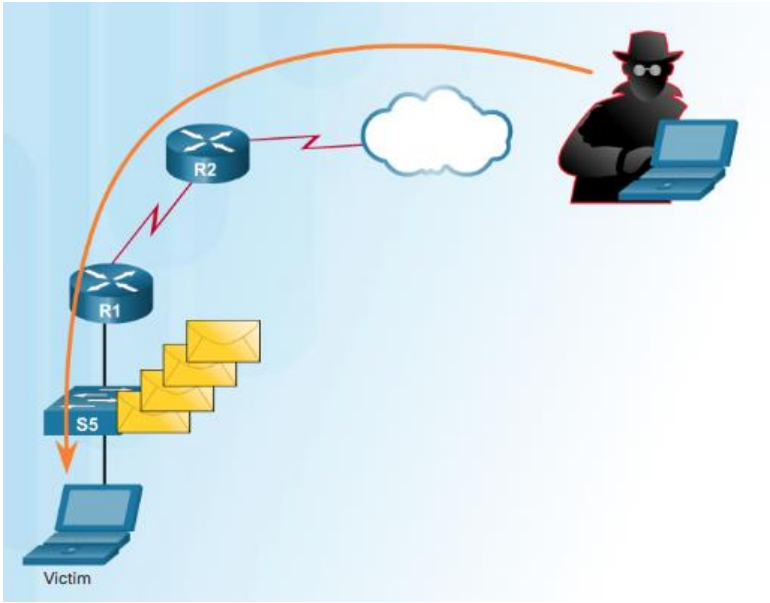






Buffer Overflow Attack

- 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.

6.3 Chapter Summary

Summary

- In this chapter you learned how networks are attacked, the types of threats and attacks used by threat actors.
- Threat actors are gray or black hat hackers who attempt to gain unauthorized access to our networks. Cybercriminals are threat actors who are motivated solely by financial gain.
- Threat actors use a variety of tools including password crackers, wireless hacking tools, network scanning and hacking tools, packet crafting tools, packet sniffers, rootkit detectors, forensic tools, debuggers, hacking operating systems, encryption tools, vulnerability exploitation tools, and vulnerability scanners.
- These tools can be used for eavesdropping, data modification, IP address spoofing, password cracking, DoS, man-in-the-middle, compromised key, network sniffing.

Summary (Cont.)

- Malware is software that is specifically designed to damage, disrupt, steal, or generally inflict some other “bad” or illegitimate action on data, hosts, or networks. The three most common types of malware are viruses, worms, and Trojan horses.
- A virus is a type of malware that propagates by inserting a copy of itself into another program.
- Worms are similar to viruses because they replicate and can cause the same type of damage. Whereas a virus requires a host program to run, worms can run by themselves.
- A Trojan horse is software that appears to be legitimate, but it contains malicious code which exploits the privileges of the user that runs it.
- The most dominate attack currently is ransomware which denies access to the infected computer system or its data until the owner pays the cybercriminal.

Summary (Cont.)

- 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 (Cont.)

- 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

Cybersecurity Operations Certification

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 2: Security Concepts**
  - 2.2 Compare and contrast the following concepts: Risk, Threat, Vulnerability, Exploit.
  - 2.3 Describe the following term: Threat Actor.

Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 6: Attack Methods**
  - 6.1 Compare and contrast an attack surface and vulnerability.
  - 6.2 Describe the following network attacks: Denial of Service, Distributed Denial of Service, Man in the middle.
  - 6.4 Describe the following attacks: Social Engineering, Phishing, Evasion Methods.
  - 6.5 Describe the following end-point based attacks: Buffer Overflows, Command and Control (C2), Malware, Rootkit, Port Scanning, Host Profiling.
  - 6.8 Compare and contrast remote exploit and a local exploit.


CISCO