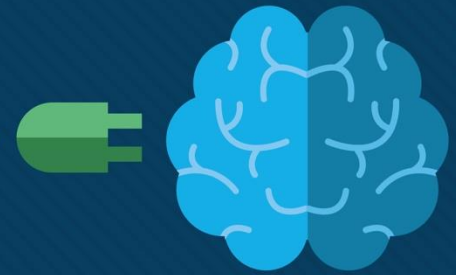
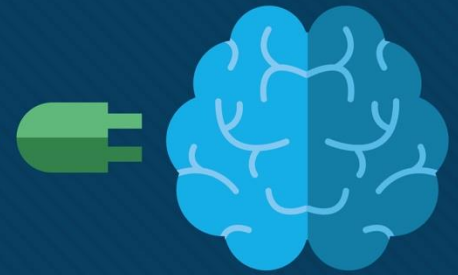


Chapter 2: Attacks, Concepts and Techniques

Introduction to Cybersecurity v2.1



Chapter 2: Attacks, Concepts and Techniques

Introduction to Cybersecurity v2.1

Chapter 2 - Sections & Objectives

- 2.1 Analyzing a Cyberattack
  - Explain the characteristics and operation of a cyber attack.
    - Explain how a security vulnerability is exploited.
    - Identify examples of security vulnerabilities.
    - Describe types of malware and their symptoms.
    - Describe methods of infiltration.
    - Describe methods used to deny service.
- 2.2 The Cybersecurity Landscape
  - Explain trends in the cyberthreat landscape.
    - Describe a blended attack.
    - Describe the importance of impact reduction.

2.1 Analyzing a Cyberattack

Finding Security Vulnerabilities

- An *exploit* is the term used to describe a program written to take advantage of a known vulnerability.
- An *attack* is the act of using an exploit against a vulnerability.
- Software vulnerability
  - Errors in OS or application code
  - SYNful Knock – Vulnerability in Cisco IOS
    - allows attackers to gain control of the routers
    - monitor network communication
    - infect other network devices.
  - Project Zero – Google formed a permanent team dedicated to finding software vulnerabilities.

- Hardware vulnerability
  - Hardware design flaws
  - Rowhammer - RAM memory exploit allows data to be retrieved from nearby address memory cells.

Categorizing Security Vulnerabilities

- Buffer Overflow
  - Data is written beyond the limits of a buffer
- Non-validated Input
  - Force programs to behave in an unintended way
- Race Conditions
  - Improperly ordered or timed events
- Weaknesses in Security Practices
  - Protect sensitive data through authentication, authorization, and encryption
- Access-control Problems
  - Access control to physical equipment and resources
  - Security practices

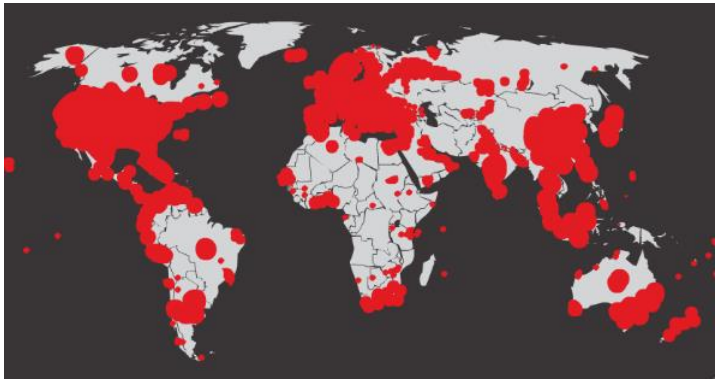
Types of Malware

- Malware is used to steal data, bypass access controls, cause harm to, or compromise a system.
- Types of Malware
  - **Spyware** - track and spy on the user
  - **Adware** - deliver advertisements, usually comes with spyware
  - **Bot** - automatically perform action
  - **Ransomware** - hold a computer system or the data captive until a payment is made
  - **Scareware** - persuade the user to take a specific action based on fear.

Initial Code Red Worm Infection

Types of Malware (Cont.)

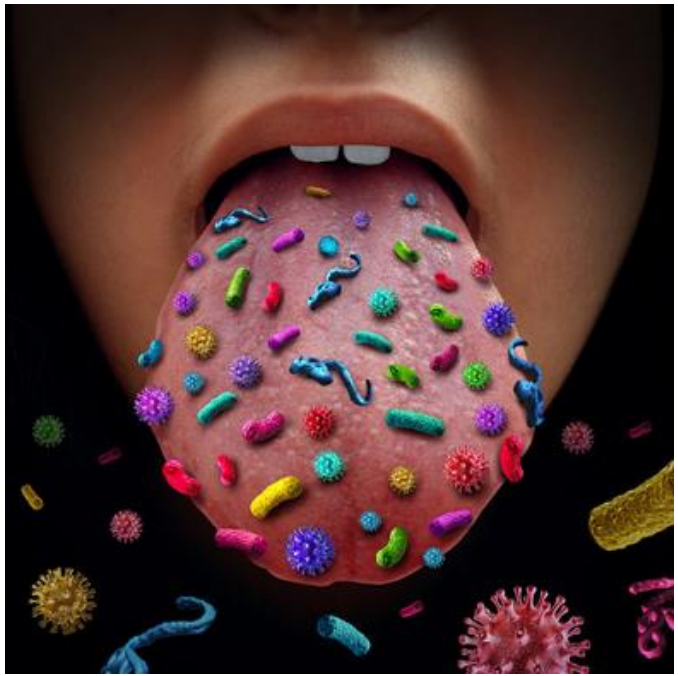
- Types of Malware (Cont.)
  - **Rootkit** - modify the operating system to create a backdoor
  - **Virus** - malicious executable code that is attached to other executable files
  - **Trojan horse** - carries out malicious operations under the guise of a desired operation
  - **Worm** - replicate themselves by independently exploiting vulnerabilities in networks
  - **Man-in-The-Middle** or **Man-in-The-Mobile** – take control over a device without the user's knowledge



Code Red Worm Infection 19 Hours Later

Symptoms of Malware

- There is an increase in CPU usage.
- There is a decrease in computer speed.
- The computer freezes or crashes often.
- There is a decrease in Web browsing speed.
- There are unexplainable problems with network connections.
- Files are modified.
- Files are deleted.
- There is a presence of unknown files, programs, or desktop icons.
- There are unknown processes running.
- Programs are turning off or reconfiguring themselves.
- Email is being sent without the user's knowledge or consent.



Social Engineering

- Social Engineering – manipulation of individual into performing actions or divulging confidential information
  - **Pretexting** - an attacker calls an individual and lies to them in an attempt to gain access to privileged data.
  - **Tailgating** - an attacker quickly follows an authorized person into a secure location.
  - **Something for something (Quid pro quo)** - an attacker requests personal information from a party in exchange for something

Wi-Fi Password Cracking

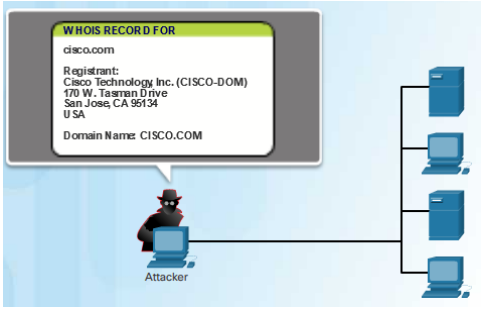
- Wi-Fi Password Cracking – Password discovery
  - **Social engineering** - The attacker manipulates a person who knows the password into providing it.
  - **Brute-force attacks** - The attacker tries several possible passwords in an attempt to guess the password.
  - **Network sniffing** - The password maybe discovered by listening and capturing packets send on the network.

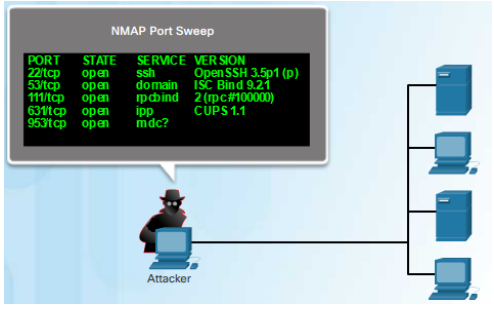
Phishing

- Phishing
  - malicious party sends a fraudulent email disguised as being from a legitimate, trusted source
  - trick the recipient into installing malware on their device or sharing personal or financial information
- Spear phishing
  - a highly targeted phishing attack

Vulnerability Exploitation

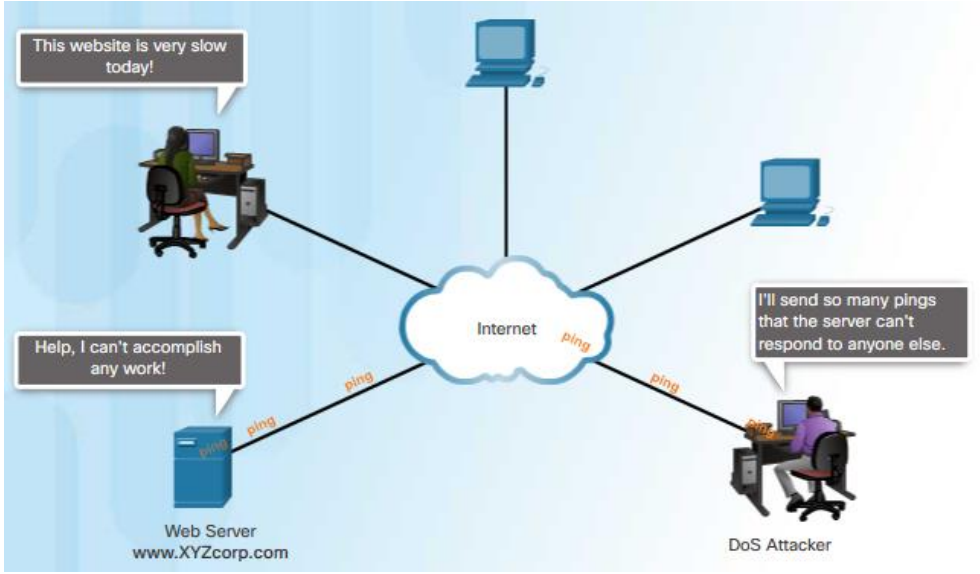
- Vulnerability Exploitation – scan to find vulnerability to exploit
  - **Step 1** - Gather information about the target system using port scanner or social engineering
  - **Step 2** - Determine learned information from step 1
  - **Step 3** - Look for vulnerability
  - **Step 4** - Use a known exploit or write a new exploit
- Advanced Persistent Threats – a multi-phase, long term, stealthy and advanced operation against a specific target
  - usually well-funded
  - deploy customized malware





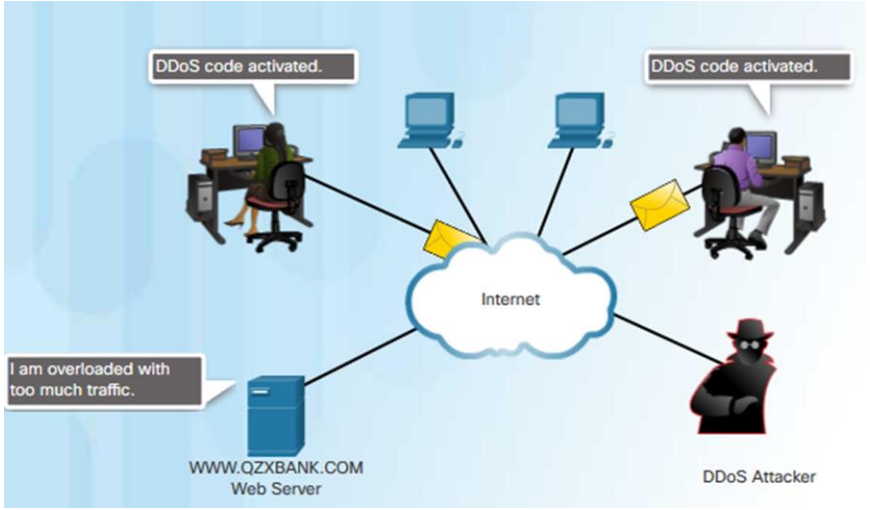
DoS

- DoS is a disruption of network services
  - **Overwhelming quantity of traffic** - a network, host, or application is sent an enormous quantity of data at a rate which it cannot handle
  - **Maliciously formatted packets** - maliciously formatted packet is sent to a host or application and the receiver is unable to handle it



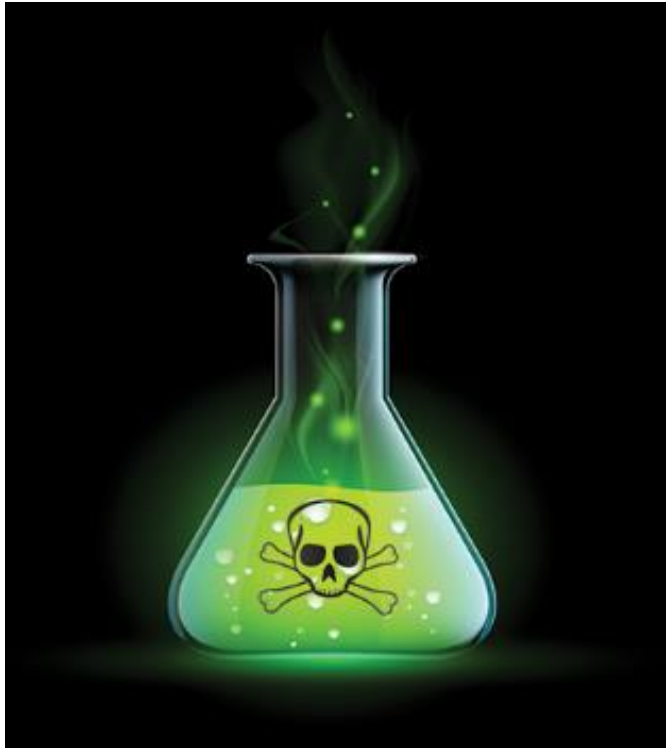
DDoS

- Similar to DoS, from multiple, coordinated sources
- Botnet - a network of infected hosts
- Zombie - infected hosts
- The zombies are controlled by handler systems.
- The zombies continues to infect more hosts, creating more zombies.



SEO Poisoning

- SEO
  - Search Engine Optimization
  - Techniques to improve a website's ranking by a search engine
- SEO Poisoning
  - Increase traffic to malicious websites
  - Force malicious sites to rank higher



2.2 The Cybersecurity Landscape

What is a Blended Attack?

- Uses multiple techniques to compromise a target
- Uses a hybrid of worms, Trojan horses, spyware, keyloggers, spam and phishing schemes
- Common blended attack example
  - spam email messages, instant messages or legitimate websites to distribute links
  - DDoS combined with phishing emails
- Examples: Nimbda, CodeRed, BugBear, Klez, Slammer, Zeus/LICAT, and Conficker

What is Impact Reduction?

- Communicate the issue
- Be sincere and accountable
- Provide details
- Understand the cause of the breach
- Take steps to avoid another similar breach in the future
- Ensure all systems are clean
- Educate employees, partners and customers

2.3 Chapter Summary

Summary

- Identify examples of security vulnerabilities.
- Explain how a security vulnerability is exploited.
- Describe types of malware and their symptoms, methods of infiltration, methods used to deny service.
- Describe a blended attack and the importance of impact reduction.


CISCO