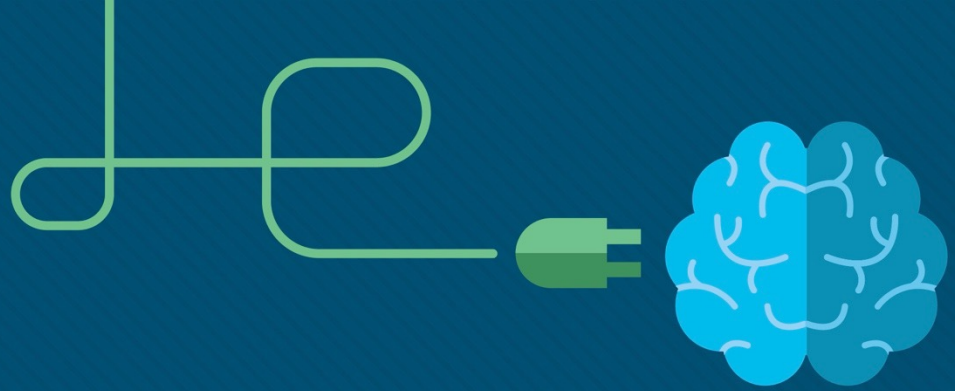


Chapter 5: Principles of Network Security

Information Security

Dr. Ayman Aljarbouh

5.2 Common Threats and Attacks

Module Objectives

Module Title: Common Threats and Attacks

Module Objective: Explain the various types of threats and attacks.

Topic Title	Topic Objective
Common Network Attacks - Reconnaissance, Access, and Social Engineering	Explain reconnaissance, access, and social engineering network attacks.
Network Attacks - Denial of Service, Buffer Overflows, and Evasion	Explain Denial of Service, buffer overflow, and evasion attacks.

Types of Network Attacks

- Malware is a means to get a payload delivered
- Network attacks are classified into three categories :

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

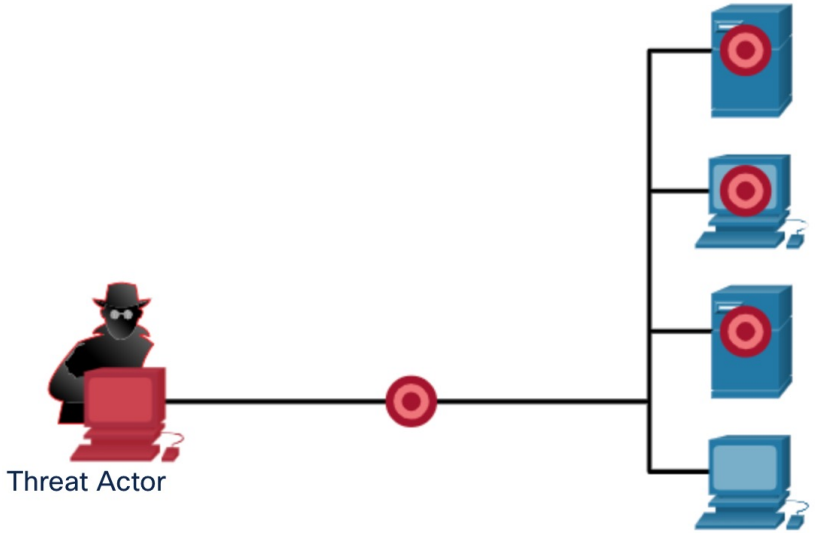
Reconnaissance Attacks

- 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.
- Recon attacks precede intrusive access attacks or DoS attack and employ the use of widely available tools.

Reconnaissance Attacks (Contd.)

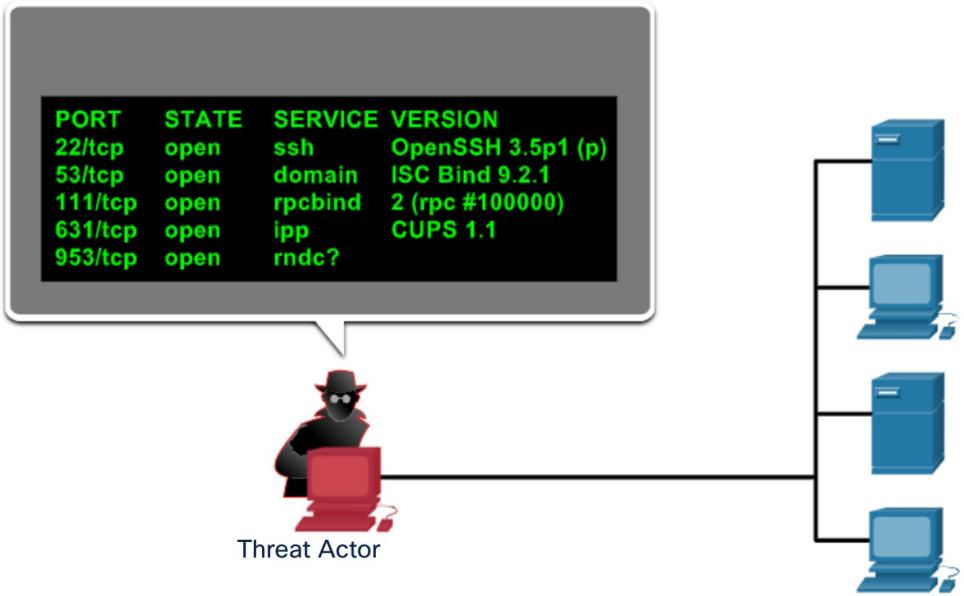
Internet Information Queries: Threat actor is looking for initial information about a target. Tools: Google search, public information from DNS registries using dig, nslookup, and whois.

Performing Ping Sweep: 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.



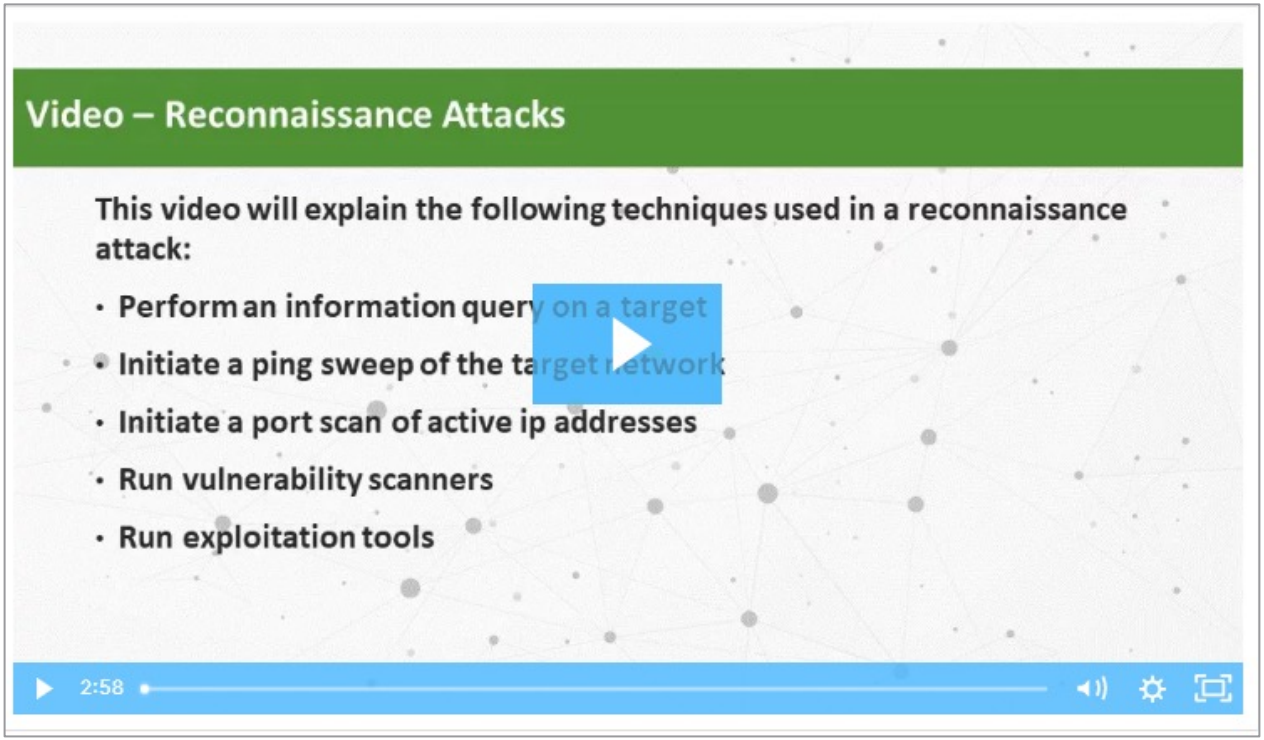
Reconnaissance Attacks (Contd.)

Performing Port Scan: 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.



Video - Reconnaissance Attacks

Watch the video to learn about the different techniques in a reconnaissance attack.



https://www.youtube.com/watch?v=jm47Qk6hf_A

Access Attacks

- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry into web accounts, confidential databases, and other sensitive information.

Password Attacks

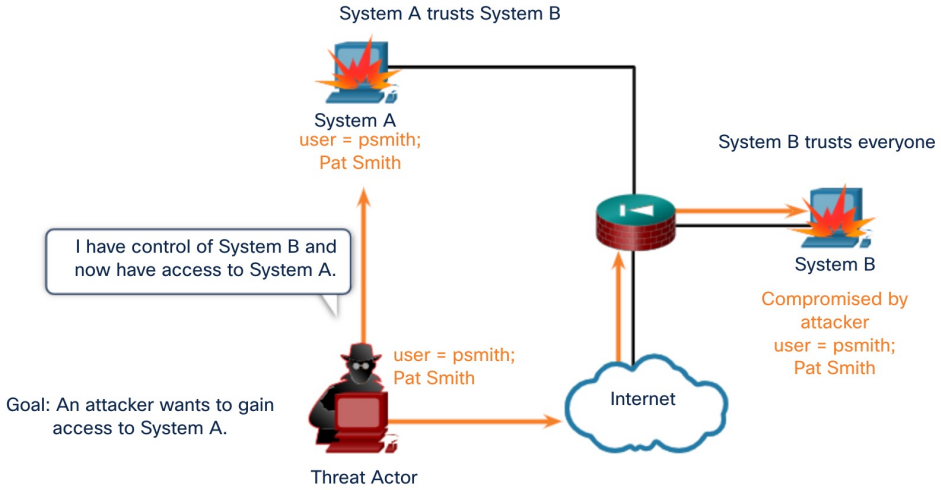
- The threat actor attempts to discover critical system passwords using a variety of password cracking tools.

Spoofing Attacks

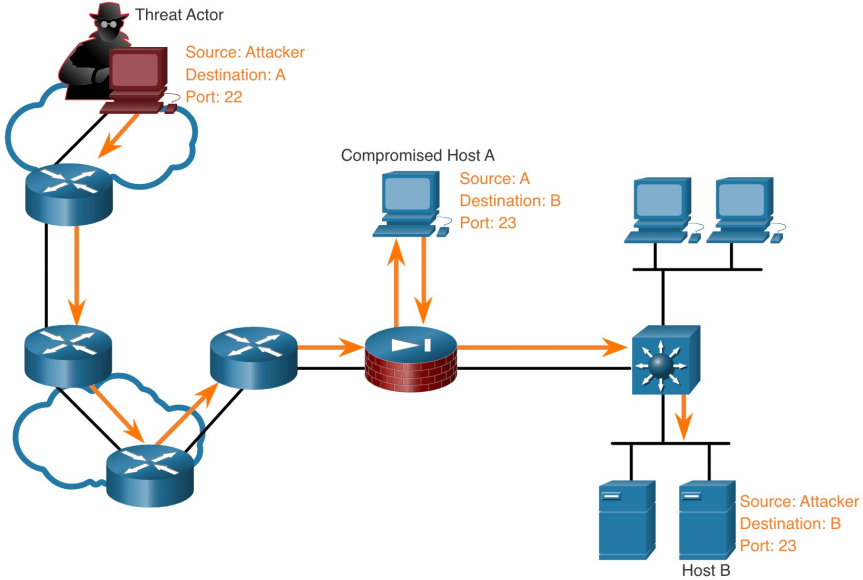
- The threat actor device attempts to pose as another device by falsifying data.
- Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing.
  - Trust exploitations
  - Port redirections
  - Man-in-the-middle attacks
  - Buffer overflow attacks

Access Attacks (Contd.)

Trust Exploitation: In a trust exploitation attack, a threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target.

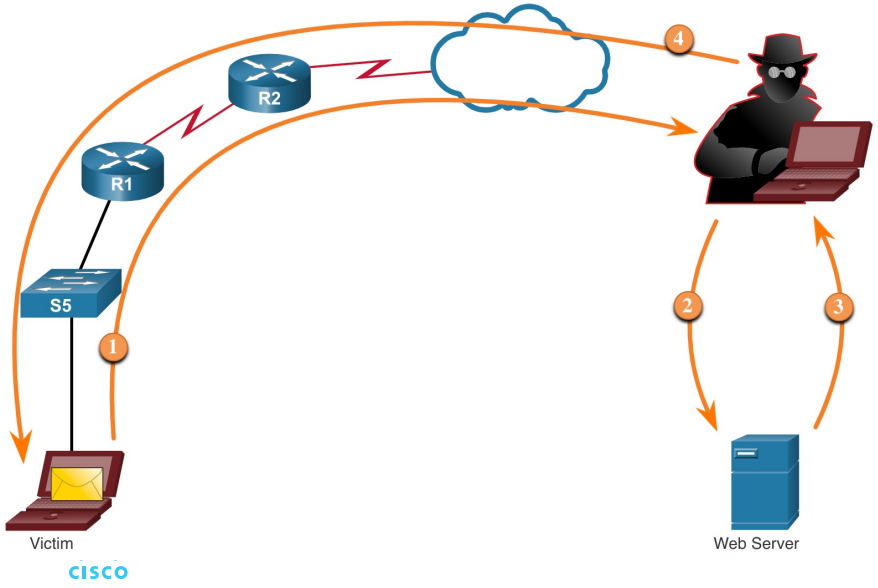


Port Redirection Example: The example shows a threat actor using SSH (port 22) to connect to a compromised Host A trusted by Host B. Hence, the threat actor can use Telnet (port 23) to access it.

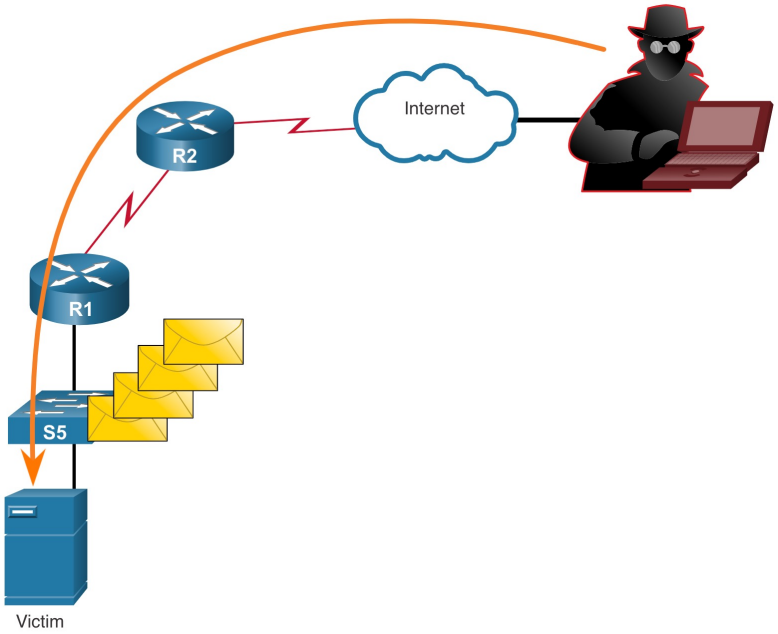


Access Attacks (Contd.)

Man-in-the-Middle Attack: The threat actor is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties.



Buffer Overflow Attack: The threat actor is sending many packets to the victim in an attempt to overflow the victim's buffer.



Video - Access and Social Engineering Attacks

Watch the video to see the demonstration of the types of access and social engineering attacks.

https://www.youtube.com/watch?v=F0wX7EShOcs

Social Engineering Attacks

- Social Engineering is an access attack that attempts to manipulate individuals into performing actions or divulging into confidential information.
- Some social engineering techniques are performed in-person or via the telephone or internet.
- Social engineering techniques are explained in the below table.

Social Engineering Attack	Description
Pretexting	A threat actor pretends to need personal or financial data to confirm the identity of the recipient.
Phishing	A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.
Spear phishing	A threat actor creates a targeted phishing attack tailored for a specific individual or organization.
Spam	Also known as junk mail, this is unsolicited email which often contains harmful links, malware, or deceptive content.

Social Engineering Attacks (Contd.)

Social Engineering Attack	Description
Something for Something	Sometimes called “Quid pro quo”, this is when a threat actor requests personal information from a party in exchange for something such as a gift.
Baiting	A threat actor leaves a malware infected flash drive in a public location. A victim finds the drive and unsuspectingly inserts it into their laptop, unintentionally installing malware.
Impersonation	In this type of attack, a threat actor pretends to be someone else to gain the trust of a victim.
Tailgating	This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area.
Shoulder surfing	This is where a threat actor inconspicuously looks over someone’s shoulder to steal their passwords or other information.
Dumpster diving	This is where a threat actor rummages through trash bins to discover confidential documents.

Strengthening the Weakest Link

- The weakest link in cybersecurity can be the personnel within an organization, and social engineering is a major security threat.
- One of the most effective security measures that an organization can take is to train its personnel and create a ‘security-aware culture’.

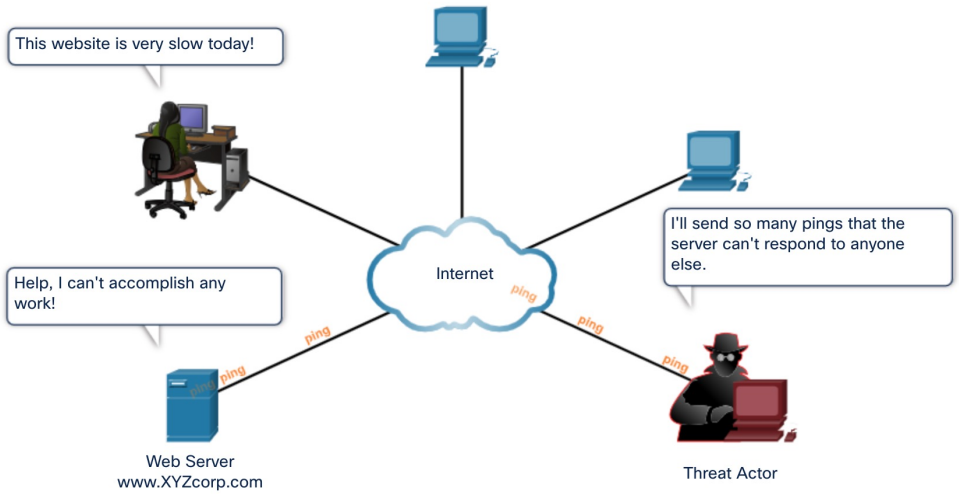
Video – Denial of Service Attacks

Watch the video to learn about Denial of Service attacks.

https://www.youtube.com/watch?v=WGm6PDcMLk0

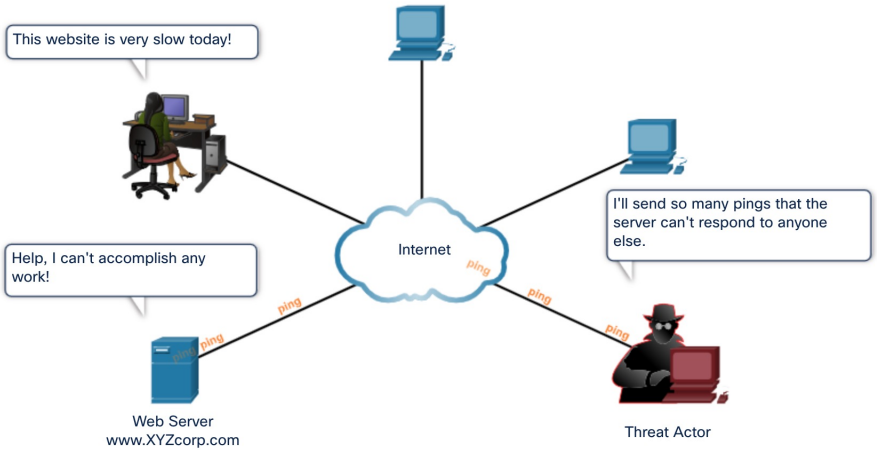
DoS and DDoS Attacks

- A Denial of Service (DoS) attack creates some sort of interruption in network services to users, devices, or applications. The two types of DoS attacks are as follows:
- **Overwhelming Quantity of Traffic** - The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle.
- **Maliciously Formatted Packets** - The threat actor sends a maliciously formatted packet to a host or application and the receiver is unable to handle it.

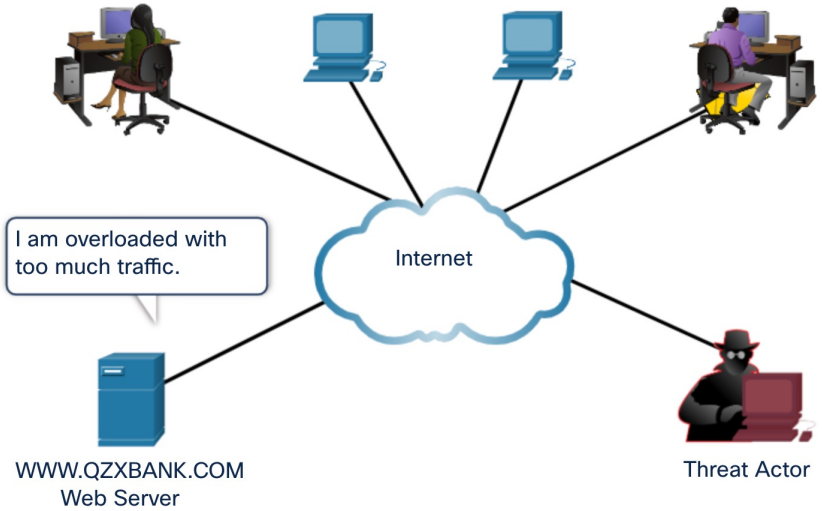


DoS and DDoS Attacks (Contd.)

DoS Attack: DoS attacks are a major risk because they interrupt communication and cause significant loss of time and money.



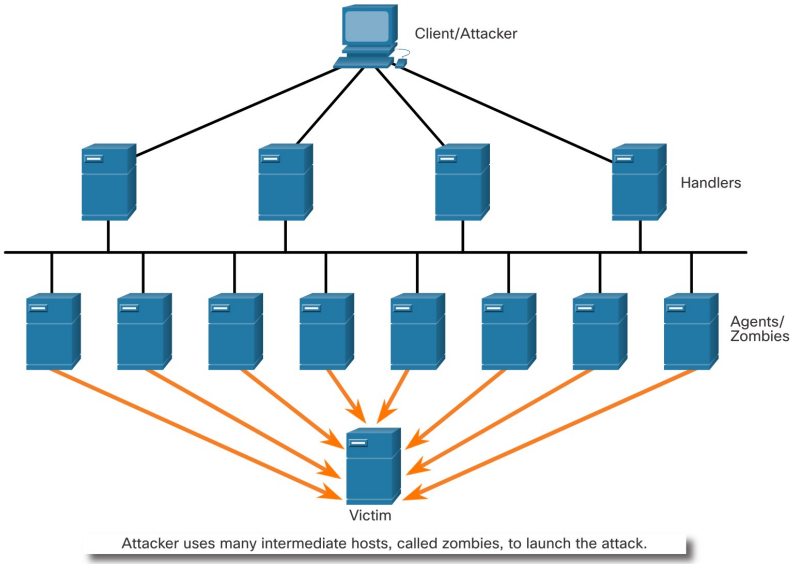
DDoS Attack: Similar to a DoS attack, but it originates from multiple, coordinated sources.



Components of DDoS Attacks

The following terms are used to describe the components of a DDoS:

Component	Description
zombies	A group of compromised hosts. These hosts run malicious code.
bots	Bots are malware that is designed to infect a host and communicate with a handler system.
botnet	A group of zombies that have been infected using self-propagating malware and are controlled by handlers.
handlers	A master command-and-control (CnC or C2) server controlling groups of zombies.
botmaster	Enables unauthorized file transfer services on end devices.



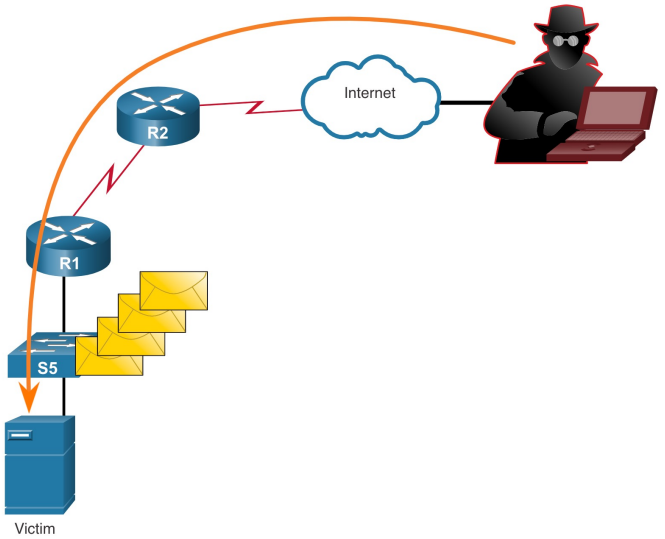
Video Demonstration – Mirai Botnet

- Mirai is a malware that targeted IoT devices configured with default login information.
- The botnet was used as part of a Distributed Denial of Service (DDoS) attack.

https://www.youtube.com/watch?v=6V5BeXypd6U

Buffer Overflow Attack

- The threat actor uses the buffer overflow DoS attack to find a system memory-related flaw on a server and exploit it.
- For instance, a remote denial of service attack vulnerability was discovered in Microsoft Windows 10, where the threat actor created malicious code to access out-of-scope memory.
- Another example is **ping of death**, where a threat actor sends a ping of death, which is an echo request in an IP packet that is larger than the maximum packet size.
- The receiving host cannot handle a packet size and it would crash.
- **Note:** It is estimated that one third of malicious attacks are the result of buffer overflows.



Evasion Methods

The evasion methods used by threat actors include:

Evasion Method	Description
Encryption and tunneling	This evasion technique uses tunneling to hide, or encryption to scramble, malware files. This makes it difficult for many security detection techniques to detect and identify the malware. Tunneling can mean hiding stolen data inside of legitimate packets.
Resource exhaustion	This evasion technique makes the target host too busy to properly use security detection techniques.
Traffic fragmentation	This evasion technique splits a malicious payload into smaller packets to bypass network security detection. After the fragmented packets bypass the security detection system, the malware is reassembled and may begin sending sensitive data out of the network.

Evasion Methods (Contd.)

Evasion Method	Description
Protocol-level misinterpretation	This evasion technique occurs when network defenses do not properly handle features of a PDU like a checksum or TTL value. This can trick a firewall into ignoring packets that it should check.
Traffic substitution	In this evasion technique, the threat actor attempts to trick an IPS by obfuscating the data in the payload. This is done by encoding it in a different format. For example, the threat actor could use encoded traffic in Unicode instead of ASCII. The IPS does not recognize the true meaning of the data, but the target end system can read the data.
Traffic insertion	Similar to traffic substitution, but the threat actor inserts extra bytes of data in a malicious sequence of data. The IPS rules miss the malicious data, accepting the full sequence of data.

Evasion Methods (Contd.)

Evasion Method	Description
Pivoting	This technique assumes the threat actor has compromised an inside host and wants to expand their access further into the compromised network. An example is a threat actor who has gained access to the administrator password on a compromised host and is attempting to login to another host using the same credentials.
Rootkits	A rootkit is a complex attacker tool used by experienced threat actors. It integrates with the lowest levels of the operating system. When a program attempts to list files, processes, or network connections, the rootkit presents a sanitized version of the output, eliminating any incriminating output. The goal of the rootkit is to completely hide the activities of the attacker on the local system.
Proxies	Network traffic can be redirected through intermediate systems in order to hide the ultimate destination for stolen data. In this way, known command-and-control not be blocked by an enterprise because the proxy destination appears benign. Additionally, if data is being stolen, the destination for the stolen data can be distributed among many proxies, thus not drawing attention to the fact that a single unknown destination is serving as the destination for large amounts of network traffic.

New Terms and Commands

• Denial of Service (DoS) • Distributed Denial of Service (DDoS) • Buffer Overflows	• Mirai Botnet • Reconnaissance Attack • Access Attack • Social Engineering

Lab 20 – Social Engineering

In this lab, you will research examples of social engineering and identify ways to recognize and prevent it.

Lab 21 – Explore Social Engineering Techniques

In this lab, you will explore social engineering techniques, sometimes called human hacking, which is a broad category for different types of attacks.