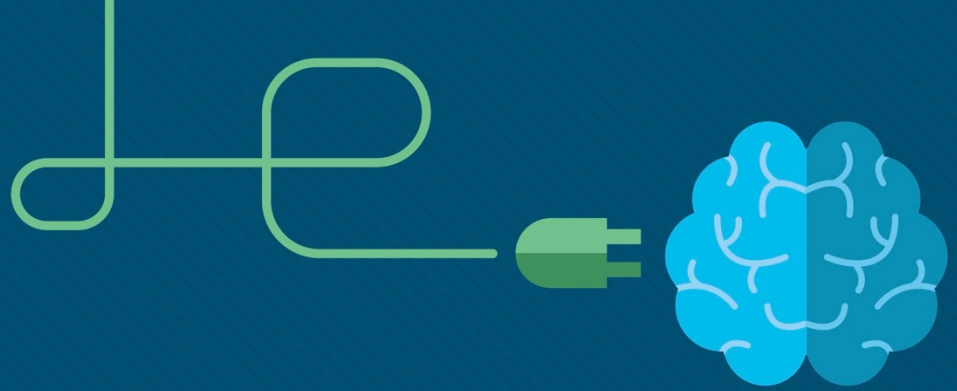


Chapter 6: Network Attacks: A Deeper Look

Information Security

Dr. Ayman Aljarbouh

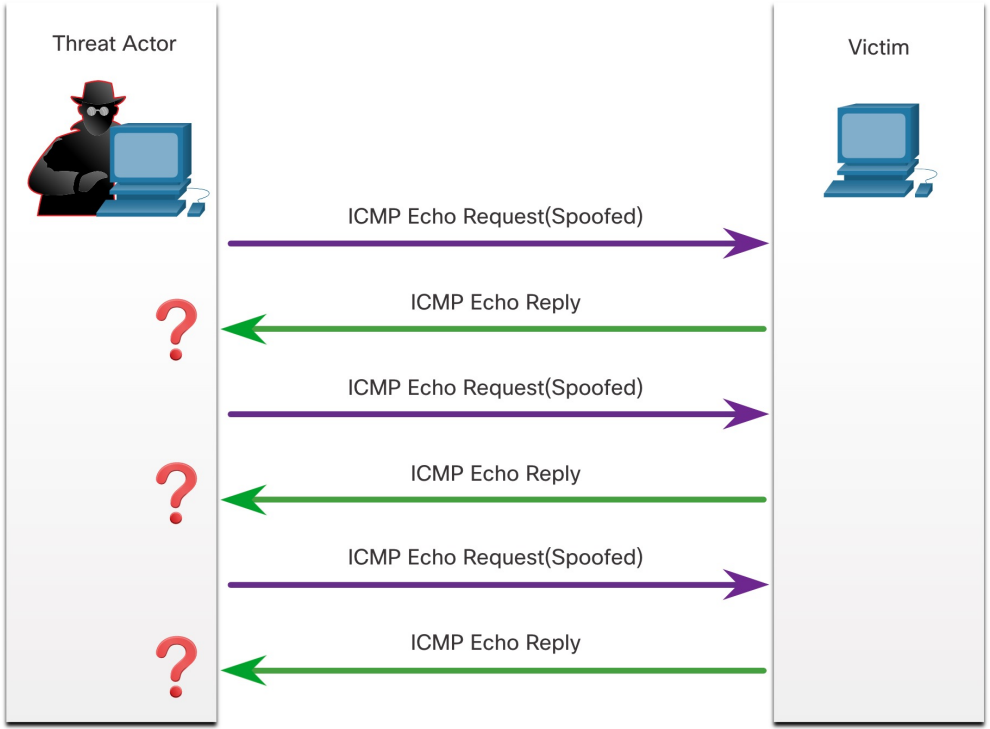
Module Objectives

Module Title: Attacking the Foundation, Attacking What We Do

Module Objective: Explain how TCP/IP vulnerabilities enable network attacks. Explain how common network applications and services are vulnerable to attack.

Topic Title	Topic Objective
IP Vulnerabilities	Explain how IP vulnerabilities enable network attacks.
TCP and UDP Vulnerabilities	Explain how TCP and UDP vulnerabilities enable network attacks.
Enterprise Services	Explain how network application vulnerabilities enable network attacks

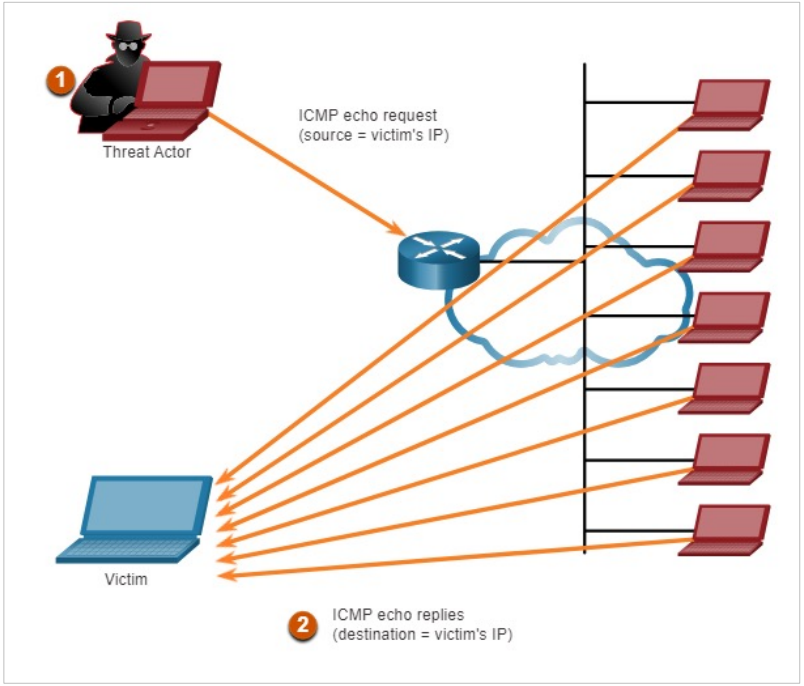
ICMP Attacks



- ICMP was developed to carry diagnostic messages and to report error conditions when routes, hosts, and ports are unavailable. ICMP messages are generated by devices when a network error or outage occurs.
- Common ICMP messages of interest to threat actors include:
  - **ICMP echo request and echo reply** – This is used to perform host verification and DoS attacks.
  - **ICMP unreachable** – This is used to perform network reconnaissance and scanning attacks.
  - **ICMP mask reply** – This is used to map an internal IP network.
  - **ICMP redirects** – This is used to lure a target host into sending all traffic through a compromised device and create a MITM attack.
  - **ICMP router discovery** – This is used to inject bogus route entries into the routing table of a target host.

Amplification and Reflection Attacks

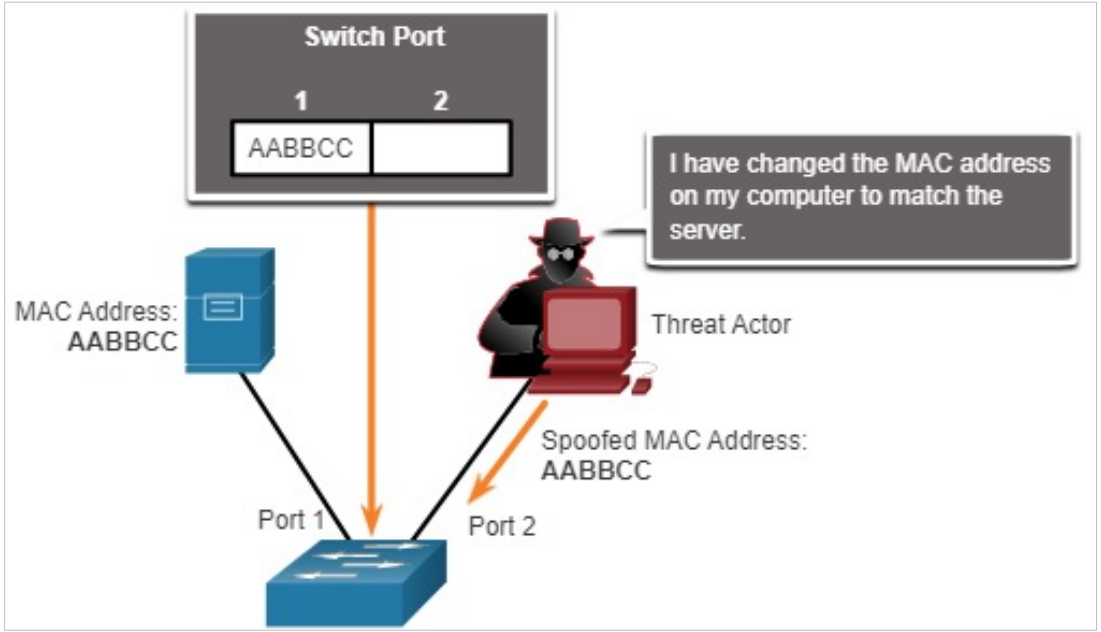
- Threat actors often use amplification and reflection techniques to create DoS attacks.
- The figure shows how an amplification and reflection technique called a Smurf attack is used to overwhelm a target host.
  - **Amplification** - The threat actor forwards ICMP echo request messages to many hosts. These messages contain the source IP address of the victim.
  - **Reflection** - These hosts all reply to the spoofed IP address of the victim to overwhelm it.
- Threat actors also use resource exhaustion attacks.



***Note**: Newer forms of amplification and reflection attacks such as DNS-based reflection and amplification attacks and Network Time Protocol (NTP) amplification attacks are now being used.*

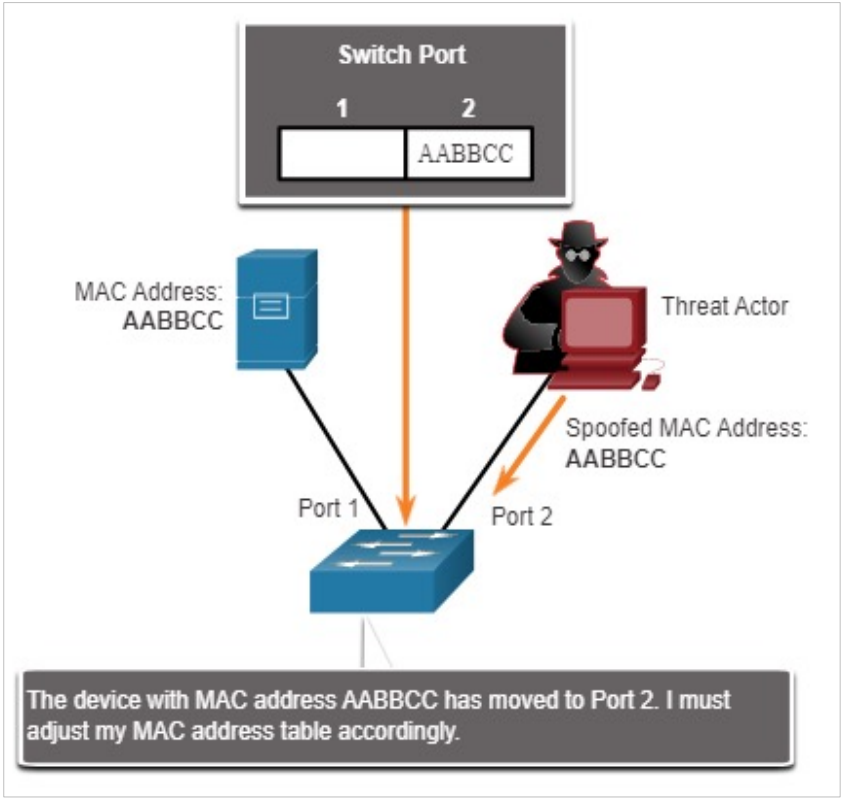
Address Spoofing Attacks

- MAC address spoofing attacks are used when threat actors have access to the internal network.
- Threat actors alter the MAC address of their host to match another known MAC address of a target host, as shown in the figure.
- The attacking host then sends a frame throughout the network with the newly-configured MAC address.
- When the switch receives the frame, it examines the source MAC address.



Address Spoofing Attacks

- The switch overwrites the current CAM table entry and assigns the MAC address to the new port, as shown in the figure.
- It then forwards frames destined for the target host to the attacking host.
- Application or service spoofing is another spoofing example. A threat actor can connect a rogue DHCP server to create an MiTM condition.

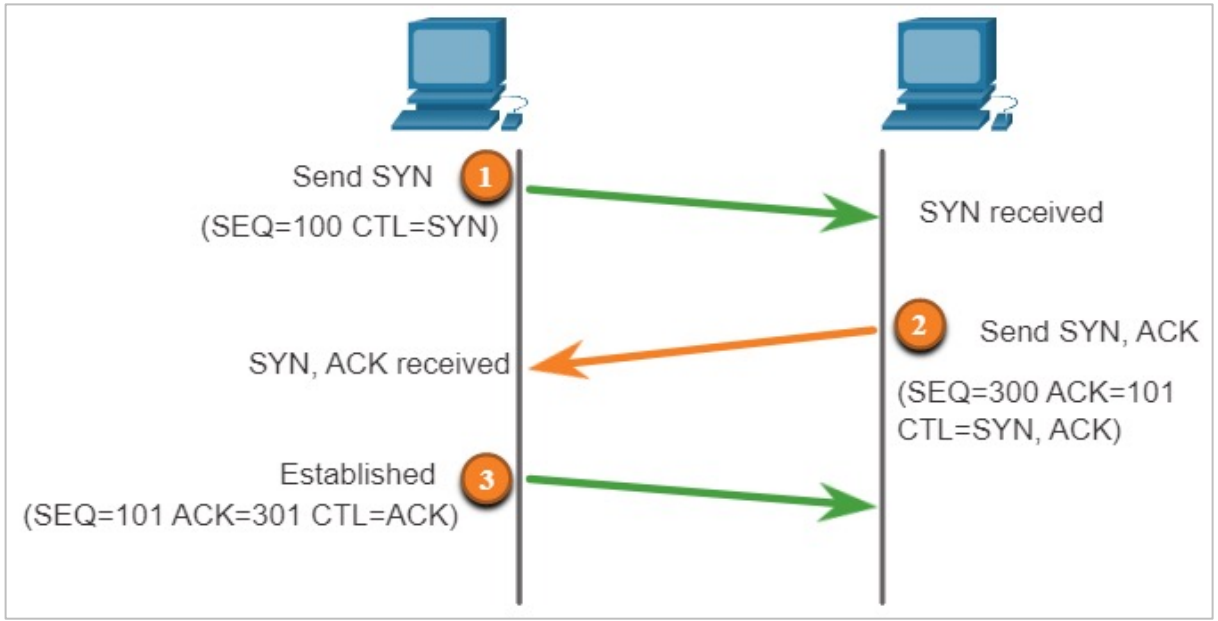


TCP Services

TCP Three-Way Handshake

A TCP connection is established in three steps:

- The initiating client requests a client-to-server communication session with the server.
- The server acknowledges the client-to-server communication session and requests a server-to-client communication session.
- The initiating client acknowledges the server-to-client communication session.

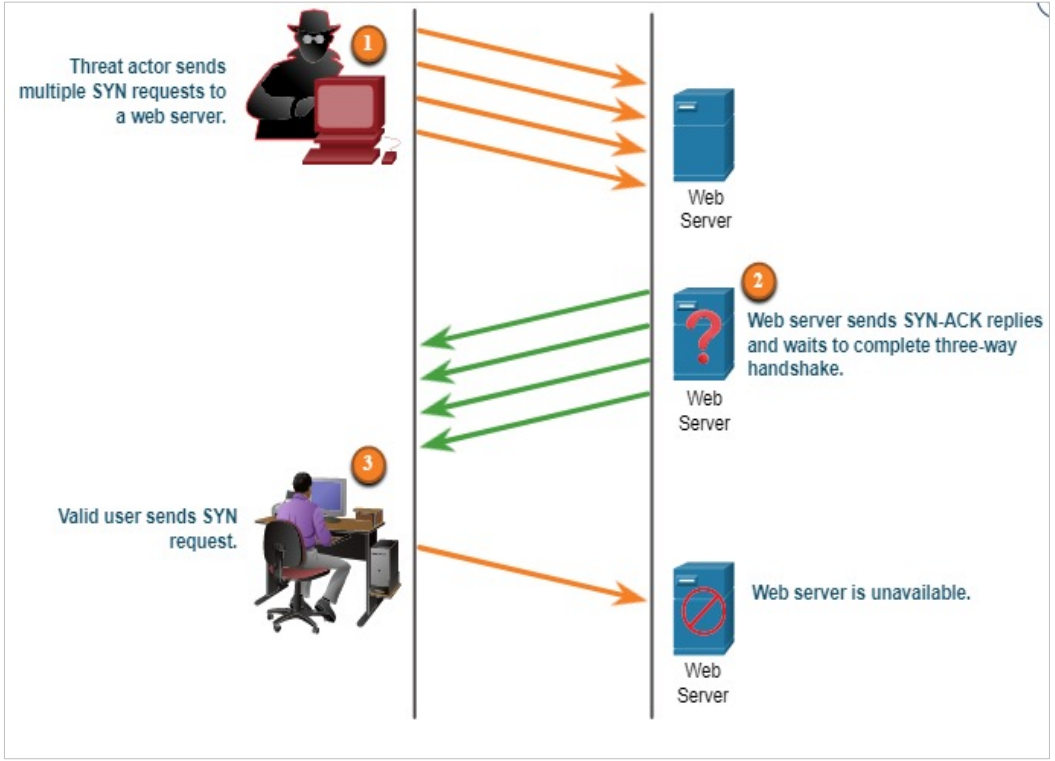


TCP Attacks

Network applications use TCP or UDP ports. Threat actors conduct port scans of target devices to discover which services they offer.

TCP SYN Flood Attack

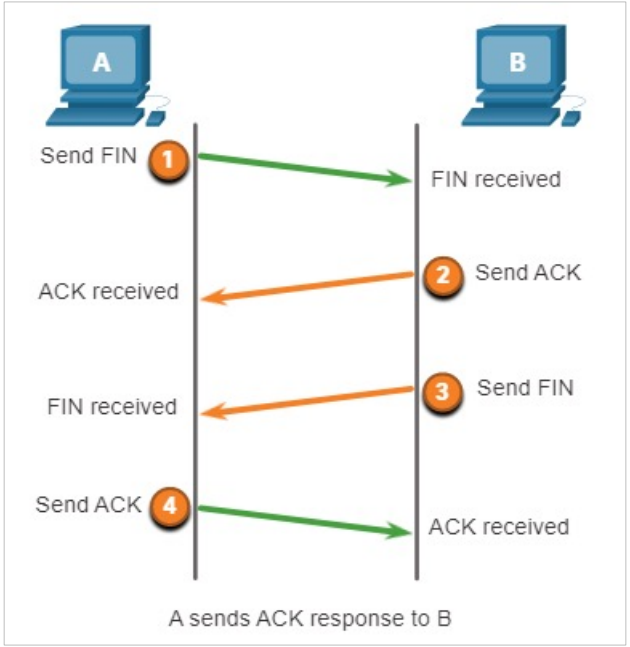
- The TCP SYN Flood attack exploits the TCP three-way handshake.
- The figure shows a threat actor continually sending TCP SYN session request packets with a randomly spoofed source IP address to a target.
- The target replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet. Those responses never arrive.
- The target host has too many half-open TCP connections, and TCP services are denied to legitimate users.



TCP Attacks

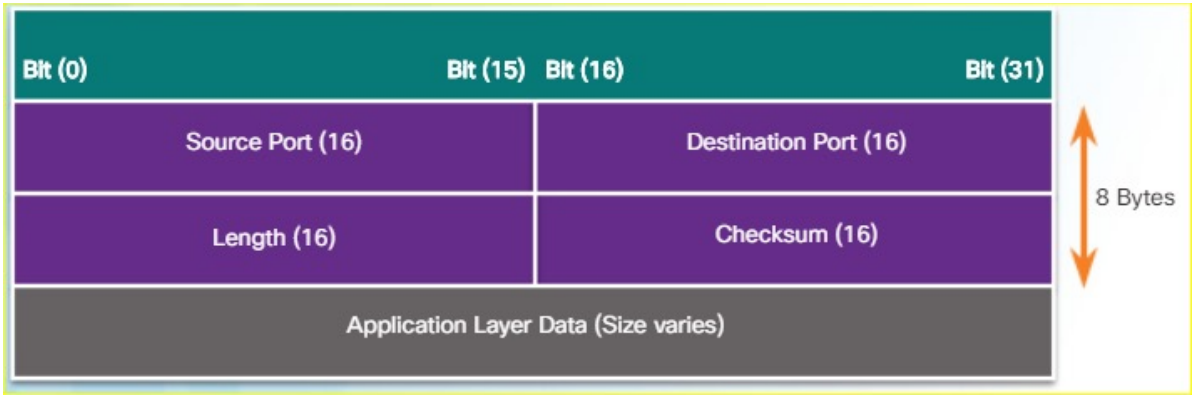
TCP Reset Attack

- A TCP reset attack can be used to terminate TCP communications between two hosts.
- A threat actor could do a TCP reset attack and send a spoofed packet containing a TCP RST to one or both endpoints.
- Terminating a TCP session uses the following four-way exchange process:
- When the client has no more data to send in the stream, it sends a segment with the FIN flag set.
- The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.
- The server sends a FIN to the client to terminate the server-to-client session.
- The client responds with an ACK to acknowledge the FIN from the server.



UDP and UDP Attacks

- UDP is a simple protocol that provides the basic transport layer functions. UDP is commonly used by DNS, TFTP, NFS, and SNMP. It is also used with real-time applications such as media streaming or VoIP. UDP is a connectionless transport layer protocol.
- By default, UDP is not protected by any encryption. The lack of encryption allows anyone to look at the traffic, change it, and send it on to its destination.
- UDP protocol attacks target the lack of protocol behaviors (UDP):
  - UDP checksum attack
  - UDP flood attack
  - UDP DoS attacks



HTTP and HTTPS

- Browsing the Web is possibly the largest vector of attack. Security analysts should have in depth knowledge of how web attacks work.
  - **Malicious iFrames** – an iFrame allows a page from a different domain to be opened inline within the current page. The iFrame can be used to launch malicious code.
  - **HTTP 302 cushioning** – allows a web page to redirect and open in a different URL. Can be used to redirect to malicious code.
  - **Domain shadowing** – malicious web sites are created from subdomains created from a hijacked domain.

Email

- Email messages are accessed from many different devices that are often not protected by the company's firewall.
  - **Attachment-based attacks** – email with malicious executable files attached.
  - **Email spoofing** – phishing attack where the message appears to come from a legitimate source.
  - **Spam email** – unsolicited email with advertisements or malicious content.
  - **Open mail relay server** – massive amount of spam and worms can be sent by misconfigured email servers.
  - **Homoglyphs** – phishing scheme where text characters (hyperlinks) look similar to real text and links.

Web-Exposed Databases

- Web applications commonly connect to a relational database. Because relational databases often contain sensitive data, databases are a frequent target for attacks.
  - **Command injection attacks** – insecure code and web application allows OS commands to be injected into form fields or the address bar.
  - **XSS Cross-site scripting attacks** – insecure server-side scripting where the input is not validated allows scripting commands to be inserted into user generated forms fields, like web page comments. This results in visitors being redirected to a malicious website with malware code.
  - **SQL injection attacks** – insecure server-side scripting allows SQL commands to be inserted into form fields where the input is not validated.
  - **HTTP injection attacks** – manipulation of html allows executable code to be injected through HTML div tags, etc.

New Terms and Commands

• Internet Control Message Protocol (ICMP) • TCP SYN Flood attack • TCP Reset attack • Amplification and Reflection attacks • Address Spoofing attacks	• iFrame • Domain Shadowing • Cross-Site Scripting (XSS) • SQL Injection • HTTP 302 cushioning • Homoglyphs

Lab 23 - Attacking a mySQL Database

In this lab, you will complete the following objective :

- View a PCAP file from a previous attack against a SQL database.

Lab 24 - Reading Server Logs

In this lab, you will complete the following objectives:

- Reading Log Files with **cat**, **more**, and **less**
- Log Files and Syslog
- Log Files and **journalctl**