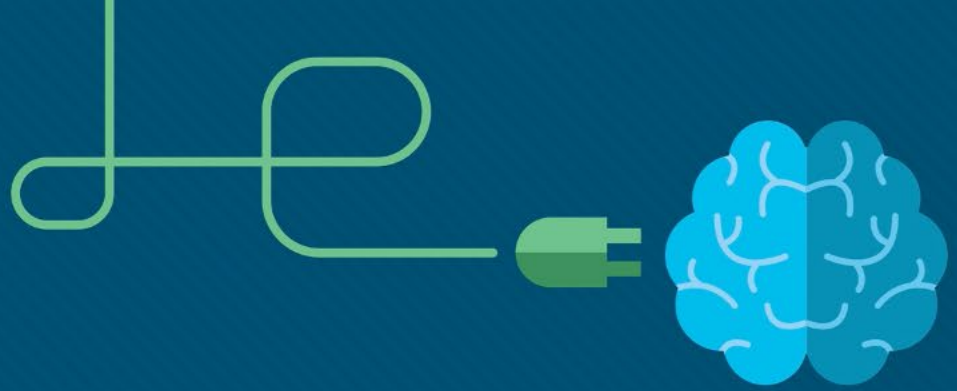


Module 3: Attacking the Foundation

Cybersecurity Essentials 3.0

Module Objectives

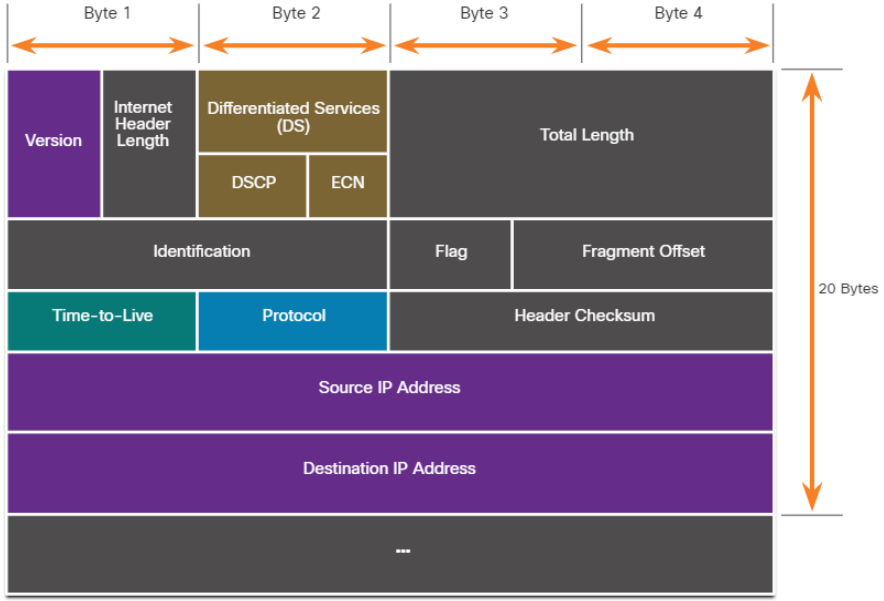
Module Title: Attacking the Foundation

Module Objective: Explain how TCP/IP vulnerabilities enable network attacks.

Topic Title	Topic Objective
IP PDU Details	Explain the IPv4 and IPv6 header structure.
IP Vulnerabilities	Explain how IP vulnerabilities enable network attacks.
TCP and UDP Vulnerabilities	Explain how TCP and UDP vulnerabilities enable network attacks.

3.1 IP PDU Details

IPv4 and IPv6



IP designed as a Layer 3 connectionless protocol:

- Delivers packets from host to destination over an interconnected system of networks.
- NOT designed to track and manage the flow of packets.
- If required, performed primarily by TCP at Layer 4.

IP does not validate whether the source IP address in a packet came from that source.

- Threat actors can send packets using a spoofed source IP address and tamper with other fields in the IP header to carry out their attacks.
- Security analysts must understand the different fields in IPv4 and IPv6 headers.

The IPv4 Packet Header

IPv4 Header Field	Description
Version	It contains a 4-bit binary value set to 0100 that identifies this as an IPv4 packet.
Internet Header length	A 4-bit field containing 20 bytes is the minimum length of the IP header.
Differentiated Services or DiffServ (DS)	The DS field is an 8-bit field used to determine the priority of each packet. The six most significant bits of the DS field are the Differentiated Services Code Point (DSCP). The last two bits are the Explicit Congestion Notification (ECN) bits.
Total length	Specify the IP packet's length (IP header + user data). The total length field is 2 bytes, so the maximum size of an IP packet is 65,535 bytes; however, packets are much smaller in practice.
Identification, Flag, and Fragment offset	As an IP packet moves through the internet, it might need to cross a route that cannot handle the size of the packet. The packet will be divided, or fragmented, into smaller packets and reassembled later. These fields fragment and reassemble packets.

The IPv4 Packet Header (Cont.)

IPv4 Header Field	Description
Time-to-Live (TTL)	An 8-bit binary limits the lifetime of a packet. The packet sender sets the initial TTL value, which is decreased by one each time a router processes the packet. If the TTL field decrements to zero, the router discards the packet and sends an ICMP Time Exceeded message to the source IP address.
Protocol	It identifies the next-level protocol. This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol.
Header checksum	A calculated value based on the contents of the IP header determines any transmission-introduced errors.
Source IPv4 Address	It contains a 32-bit binary value that represents the source IPv4 address of the packet. The source IPv4 address is always a unicast address.
Destination IPv4 Address	It contains a 32-bit binary value that represents the destination IPv4 address of the packet.
Options and Padding	This field that varies in length from 0 to a multiple of 32 bits. If the option values are not a multiple of 32 bits, 0s are added or padded to ensure that this field contains a multiple of 32 bits.

Video - Sample IPv4 Headers in Wireshark

This video will cover the following:

- A demonstration of examining IPv4 headers in a Wireshark capture
- The network layer information in a Wireshark packet capture
- Identify source IP address, version, header length, DS field, flags, and TTL in each IPv4 packet.

The IPv6 Packet Header

IPv6 Header Field	Description
Version	This field contains a 4-bit binary value set to 0110 that identifies this as an IPv6 packet.
Traffic Class	This 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field.
Flow Label	This 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.
Payload Length	This 16-bit field indicates the length of the data portion or payload of the IPv6 packet.
Next Header	This 8-bit field is equivalent to the IPv4 Protocol field. It indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol.
Hop Limit	This 8-bit field replaces the IPv4 TTL field. This value decrements by a value of 1 by each router that forwards the packet. When the counter reaches 0, the packet discards, and an ICMPv6 Time Exceeded message is forwarded to the sending host, indicating that the packet did not reach its destination (the maximum hop limit).
Source IPv6 Address	This 128-bit field identifies the IPv6 address of the sending host.
Destination IPv6 Address	This 128-bit field identifies the IPv6 address of the receiving host.

Video - Sample IPv6 Headers in Wireshark

This video will cover the following:

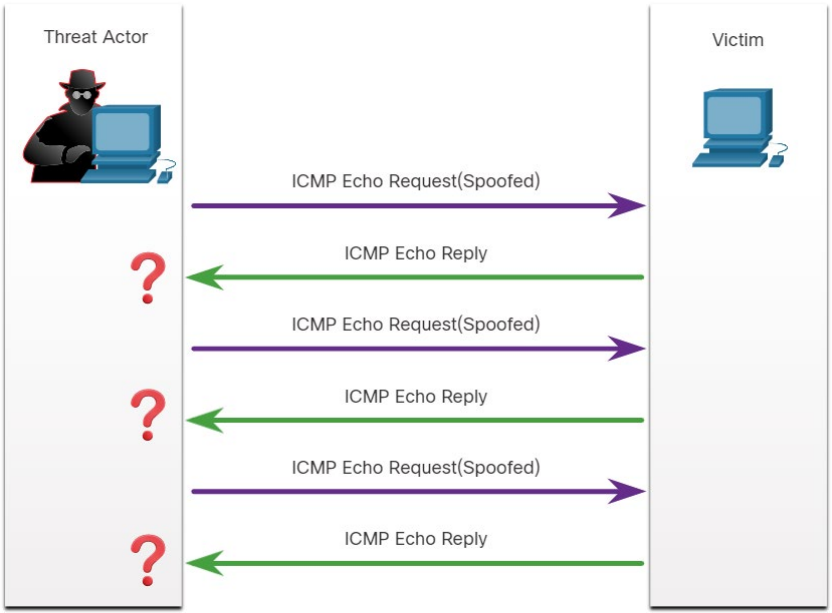
- Investigate a threat landscape and 3 vulnerabilities that can be exploited by threat actors
- Explore a vulnerability that results from a device that is not properly configured with security best practices

3.2 IP Vulnerabilities

IP Vulnerabilities

IP Attacks	Description
ICMP attacks	Threat actors use ICMP echo packets (pings) to discover subnets and hosts on a protected network, to generate DoS flood attacks, and to alter host routing tables.
Denial-of-Service (DoS) attacks	Threat actors attempt to prevent legitimate users from accessing information or services.
Distributed Denial-of-Service (DDoS) attacks	Similar to a DoS attack, but features a simultaneous, coordinated attack from multiple source machines.
Address spoofing attacks	Threat actors spoof the source IP address to perform blind spoofing or non-blind spoofing.
Man-in-the-middle attack (MiTM)	Threat actors position themselves between a source and destination to transparently monitor, capture, and control the communication. They could simply eavesdrop by inspecting captured packets or alter packets and forward them to their original destination.
Session hijacking	Threat actors gain access to the physical network, and then use an MiTM attack to hijack a session.

ICMP Attacks



ICMP carries diagnostic messages and reports error conditions when routes, hosts, and ports are unavailable.

- Messages are generated by devices when a network error or outage occurs.
- The ping command is a user-generated ICMP message (echo request) used to verify connectivity to a destination.

Threat actors use ICMP for reconnaissance and scanning attacks.

- It enables them to launch information-gathering attacks to map out a network topology, discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall.

Threat actors also use ICMP for DoS and DDoS attacks, as shown in the ICMP flood attack in the figure.

ICMP Attacks (Cont.)

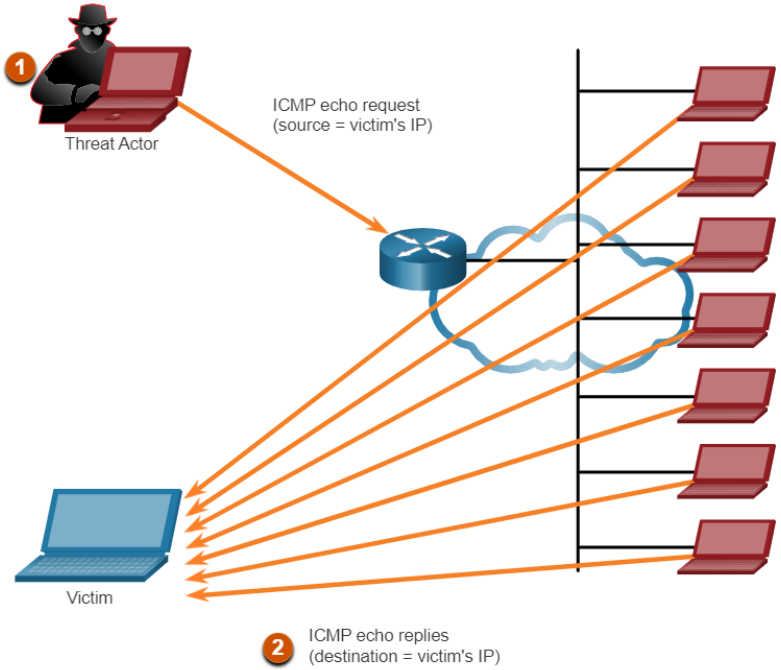
ICMP Message	Description
ICMP echo request and echo reply	Performs host verification and DoS attacks.
ICMP unreachable	Performs network reconnaissance and scanning attacks.
ICMP mask reply	Maps an internal IP network.
ICMP redirects	Lures a target host into sending all traffic through a compromised device and create a MiTM attack.
ICMP router discovery	Injects bogus route entries into the routing table of a target host.

Video - Amplification, Reflection, and Spoofing Attacks

This video will cover the following:

- Explain the amplification, reflection, and spoofing attack
- Identify and address the difference between non-blind spoofing and blind spoofing attacks

Amplification and Reflection Attacks



- Threat actors often use amplification and reflection techniques to create DoS attacks.
- The example in the figure illustrates how an amplification and reflection technique called a Smurf attack is used to overwhelm a target host.

Address Spoofing Attacks

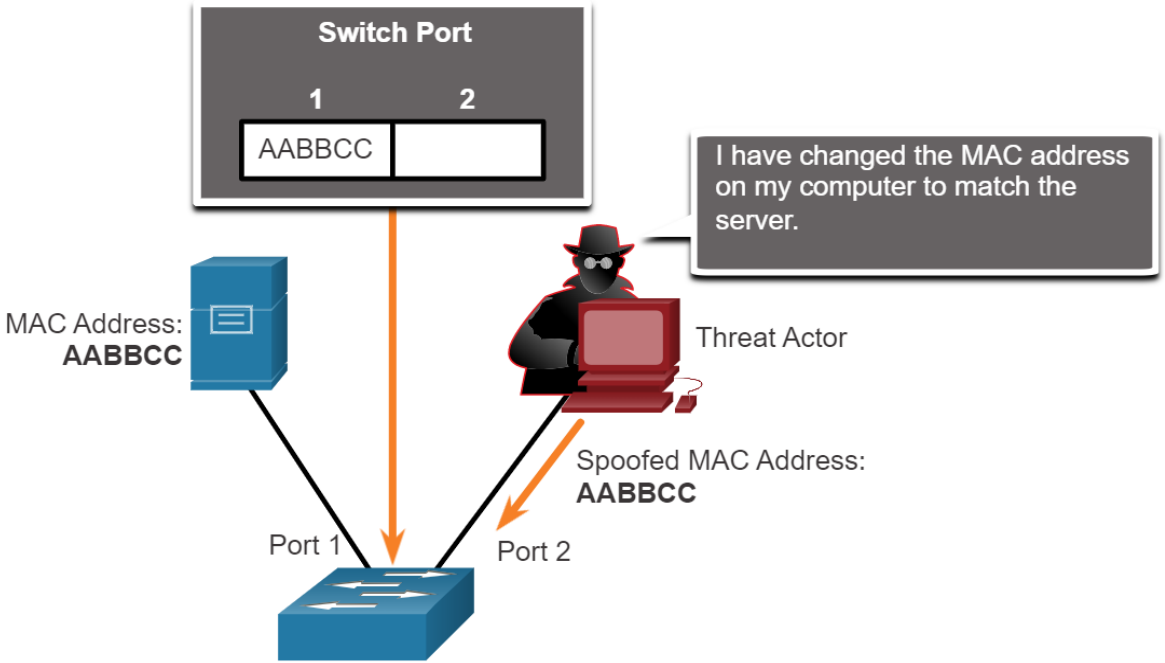
IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to hide the sender's identity or pose as another legitimate user.

Spoofing attacks can be non-blind or blind:

- Non-blind spoofing - The threat actor can see the traffic sent between the host and the target. The threat actor uses non-blind spoofing to inspect the reply packet from the target victim.
- Blind spoofing - The threat actor cannot see the traffic sent between the host and the target. Blind spoofing uses in DoS attacks.

MAC addresses spoofing attacks 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.

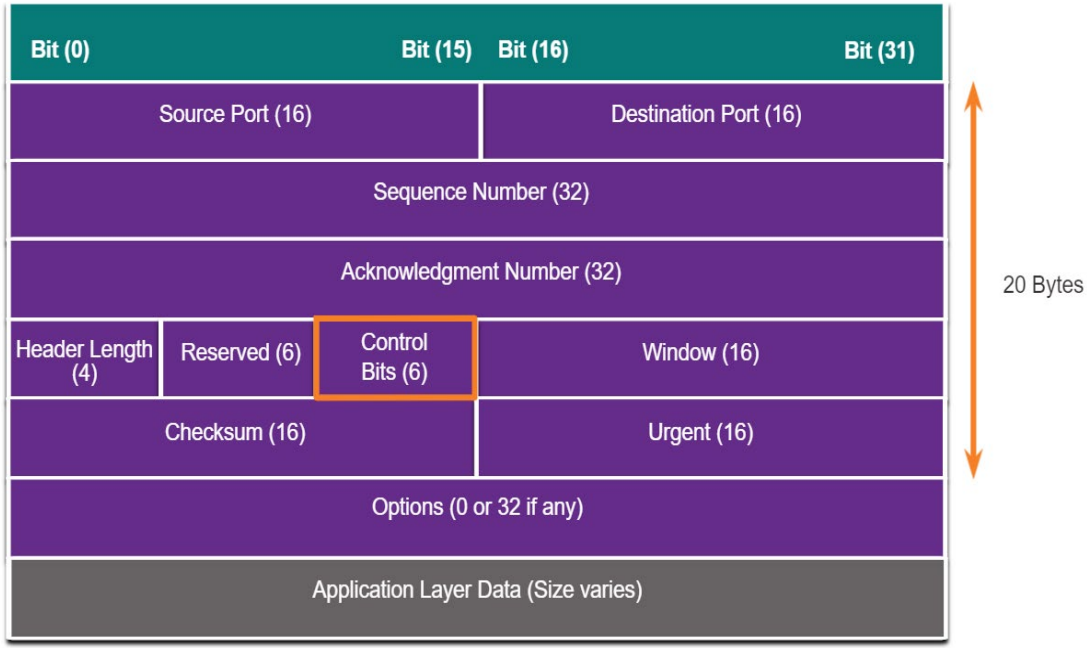
Address Spoofing Attacks (Cont.)



- 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.

3.3 TCP and UDP Vulnerabilities

TCP Segment Header



- TCP segment information appears immediately after the IP header.
- The fields of the TCP segment and the flags for the Control Bits field display in the figure.

TCP Services

TCP provides these services:

Reliable delivery

- TCP incorporates acknowledgments to guarantee delivery instead of relying on upper-layer protocols to detect and resolve errors.
- If a timely acknowledgment is not received, the sender retransmits the data.
- Requiring acknowledgments of received data can cause substantial delays.

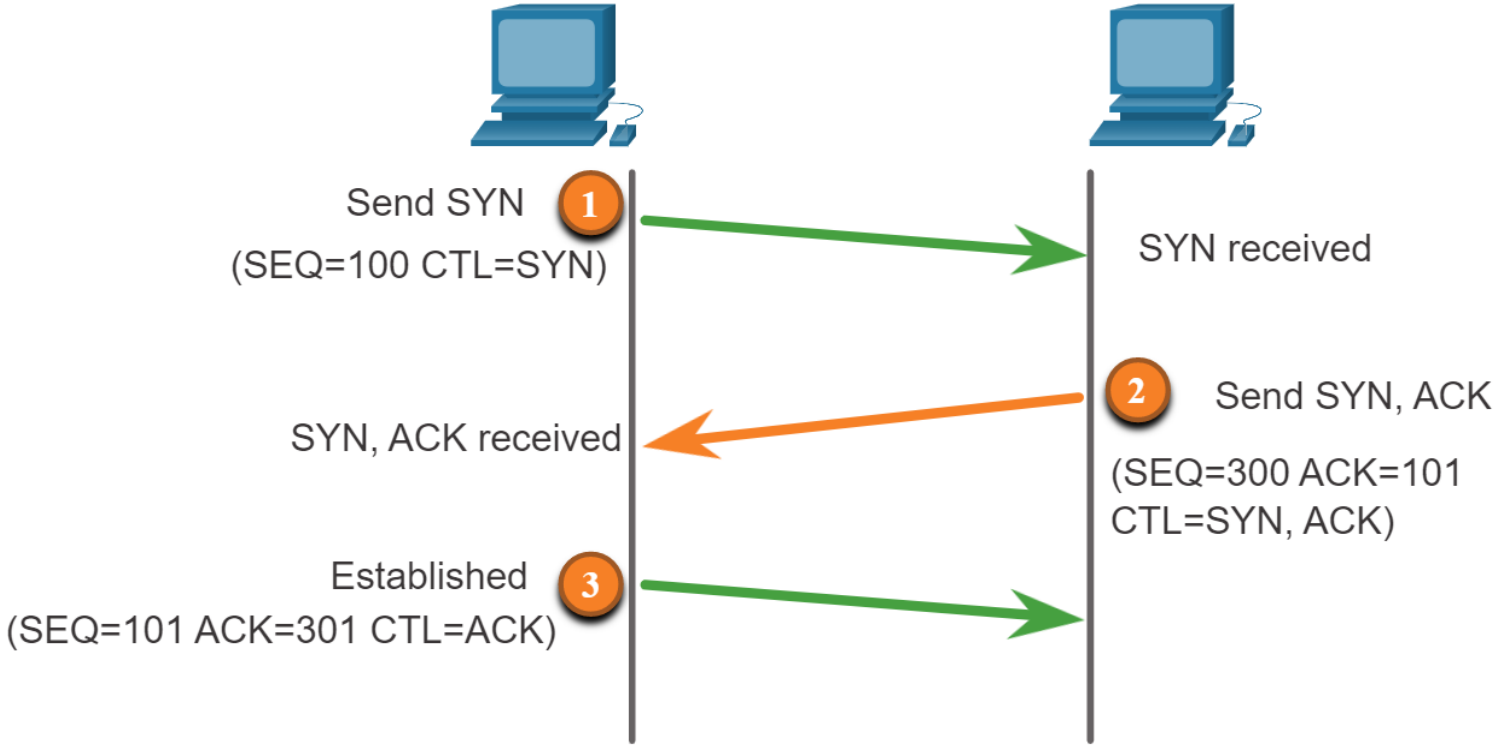
Flow control

- TCP implements flow control to address this issue. Rather than acknowledge one segment at a time, multiple segments acknowledge concurrently.

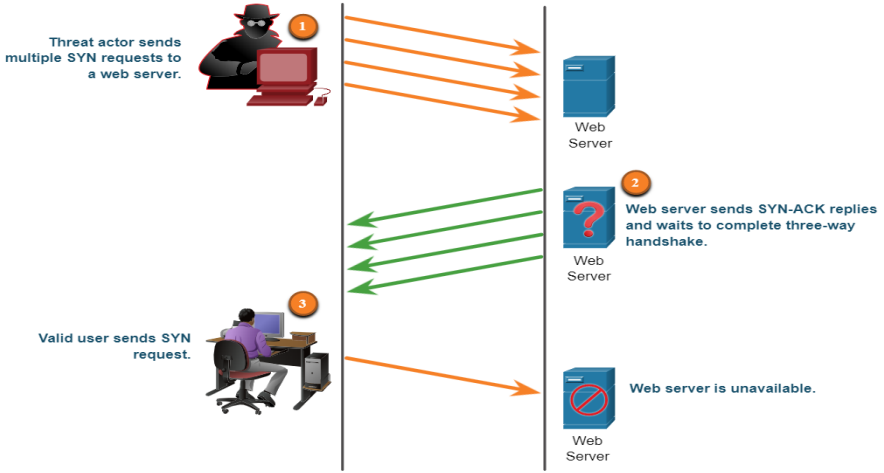
Stateful communication

- TCP stateful communication between two parties occurs during the TCP three-way handshake.
- Before data transferring using TCP, a three-way handshake opens the TCP connection.
- If both sides agree to the TCP connection, data can be sent and received by both parties using TCP.

TCP Services (Cont.)



TCP Attacks



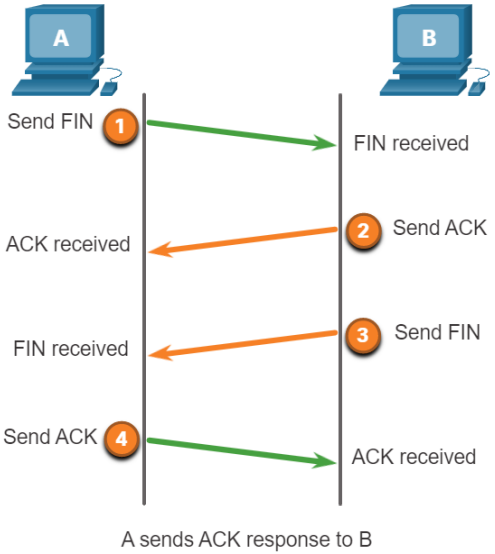
The TCP SYN Flood attack exploits the TCP three-way handshake.

- The threat actor sends TCP SYN session request packets with a randomly spoofed source IP address to a target.
- Targeted device replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet.
- Responses never arrive.
- Eventually, the target host denies legitimate users because it is overwhelmed with half-open TCP connections.

TCP reset attack

- It terminates TCP communications between two hosts. TCP uses a four-way exchange to close the TCP connection using a pair of FIN and ACK segments from each TCP endpoint.
- A TCP connection abruptly terminates when it receives an RST bit, which tears down the TCP connection and informs the receiving host to stop using the TCP connection immediately.

TCP Attacks (Cont.)



A sends ACK response to B

Terminating a TCP session uses the following four-way exchange process:

1. 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, then terminates the session from client to server.
1. The server sends a FIN to the client to terminate the server-to-client session.
2. The client responds with an ACK to acknowledge the FIN from the server.

TCP session hijacking

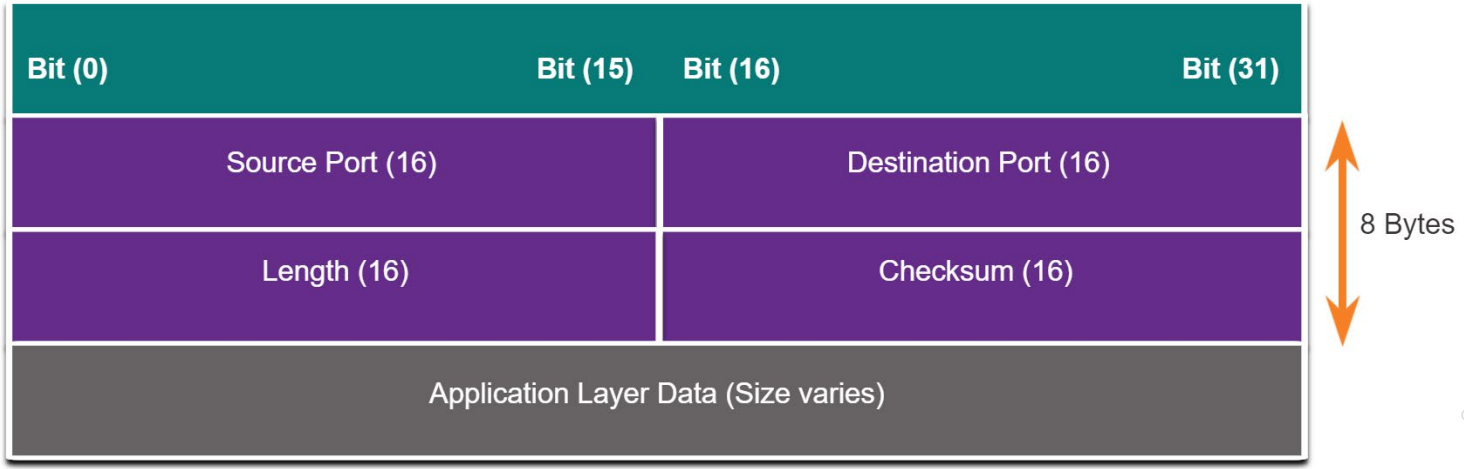
- A threat actor takes over an already-authenticated host as it communicates with the target.
- The threat actor must spoof the IP address of one host, predict the following sequence number, and send an ACK to the other host.
- If successful, the threat actor could send, but not receive, data from the target device.

UDP Segment Header and Operation

- UDP commonly uses DNS, DHCP, TFTP, NFS, and SNMP.
- It uses real-time applications such as media streaming or VoIP.
- UDP is a connectionless transport layer protocol.
- It has a much lower overhead than TCP because it is not connection-oriented and does not offer the sophisticated retransmission, sequencing, and flow control mechanisms that provide reliability.
- The UDP segment structure is much smaller than TCP's segment structure.
- **Note**: UDP divides data into datagrams. However, the generic term "segment" is commonly used.

UDP Segment Header and Operation (Cont.)

- Although UDP usually is called unreliable, in contrast to TCP's reliability, this does not mean that applications that use UDP are always unreliable, nor does it mean that UDP is an inferior protocol.
- It means that these functions are not provided by the transport layer protocol and must implement elsewhere if required.
- The low overhead of UDP makes it very desirable for protocols that make a simple requests and reply transactions.
- For example, using TCP for DHCP would introduce unnecessary network traffic. If no response is received, the device resends the request.



UDP Attacks

Any encryption does not protect UDP. Encryption can be added to UDP but is not available by default.

- Lack of encryption means anyone can see the traffic, change it, and send it on to its destination.
- Changing the data in the traffic will alter the 16-bit checksum, but the checksum is optional and not always used.
- When the checksum uses, the threat actor can create a new checksum based on the new data payload and then record it in the header as a new checksum.
- The destination device will find that the checksum matches the data without realizing it is altered data. This type of attack is not widely used.

UDP Attacks (Cont.)

UDP Flood Attacks

- A UDP flood attack consumes all the resources on a network.
- The threat actor must use a tool like UDP Unicorn or Low Orbit Ion Cannon.
- These tools send a flood of UDP packets, often from a spoofed host, to a server on the subnet.
- The program will sweep through all the known ports to find closed ports, causing the server to reply with an unreachable ICMP port message.
- Because there are many closed ports on the server, this creates traffic on the segment, which uses up most of the bandwidth. The result is very similar to a DoS attack.

3.4 Attacking the Foundation Summary

What did I Learn in this Module?

- IP is a Layer 3 connectionless protocol. The IPv4 header consists of several fields, and the IPv6 header contains fewer fields.
- Different types of attacks target IP, like ICMP attacks, DoS attacks, DDoS attacks, Address spoofing attacks, Man-in-the-middle attacks (MiTM), and Session hijacking.
- ICMP carries diagnostic messages and reports error conditions when routes, hosts, and ports are unavailable.
- Threat actors use ICMP for reconnaissance and scanning attacks and DoS and DDoS attacks.
- Threat actors often use amplification and reflection techniques to create DoS attacks.
- They also use resource exhaustion attacks to consume the resources of a target host to crash or consume the network's resources.
- IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the sender's identity or pose as another legitimate user.
- Address spoofing attacks can be non-blind spoofing to hijack a session or blind spoofing to create a DoS attack. MAC address spoofing attacks deploy when threat actors have access to the internal network.

What did I Learn in this Module? (Cont.)

- TCP segment and UDP datagram information appear immediately after the IP header.
- TCP provides reliable delivery, flow control, and stateful communication.
- TCP stateful communication between two parties occurs during the TCP three-way handshake.
- Threat actors can conduct TCP-related attacks like TCP port scans, TCP SYN Flood attacks, TCP Reset Attacks, and TCP Session Hijacking attacks.
- The UDP segment (i.e., datagram) is much smaller than the TCP segment, making it desirable for use by protocols that make simple request and reply transactions, such as DNS, DHCP, SNMP, and others.
- Threat actors can conduct UDP flood attacks which sweep through all the known UDP ports on a server trying to find closed ports. Threat actor actions can create a DoS situation.