13.3.8 Session and Spoofing Attack Facts

Session and spoofing attacks generally take advantage of the old TCP/IP protocols associated with IPv4. IPv6 mitigates many of these security vulnerabilities. But until IPv6 is fully adopted, you must be familiar with session and spoofing attacks so you can protect your system from them.

Session Attacks

In a *session attack*, the attacker takes over the TCP/IP session or captures information that can be used at a later date. The following table describes common session attack methods.

Attack	Description
Man-in-the-Middle	A *man-in-the-middle* attack is used to intercept information between two communication partners. With a man-in-the-middle attack: - An attacker inserts himself in the communication flow between the client and server. The client is fooled into authenticating to the attacker. - Both parties at the endpoints believe they are communicating directly with each other, while the attacker intercepts and/or modifies the data in transit. The attacker can then authenticate to the server using the intercepted credentials. Man-in-the-middle attacks are commonly used to steal credit card numbers, online bank credentials, and confidential personal and business information.
TCP/IP (session) Hijacking	*TCP/IP hijacking* is an extension of a man-in-the-middle attack where the attacker steals an open and active communication session from a legitimate user. - The attacker takes over the session and cuts off the original source device. - The TCP/IP session state is manipulated so that the attacker is able to insert alternate packets into the communication stream. Countermeasures for hijacking include using: - IPsec or another encryption protocol - Certificate authentication - Mutual authentication - Randomizing sequencing mechanisms - Packet time stamps - Packet sequencing
HTTP (Session) Hijacking	*HTTP (session) hijacking* is a real-time attack in which the attacker hijacks a legitimate user's cookies and uses the cookies to take over the HTTP session.
Replay Attack	In a *replay attack*, the attacker uses a protocol analyzer or sniffer to capture authentication information going from the client to the server. The attacker then uses this information to connect at a later time and pretend to be the client. To prevent a replay attack, use a secure authentication method, such as Kerberos.

Spoofing Attacks

Spoofing is used to hide the true source of packets or redirect traffic to another location. Spoofing attacks:

- Use modified source and/or destination addresses in packets.
- Can include site spoofing that tricks users into revealing information.

The following table describes common spoofing attack methods.

Attack	Description
IP Spoofing	IP spoofing changes the IP address information within a packet. It can be used to: - Hide the origin of the attack by spoofing the source address. - Amplify attacks by sending a message to a broadcast address and then redirecting responses to a victim who is overwhelmed with responses.
MAC Spoofing	MAC spoofing is when an attacking device spoofs the MAC address of a valid host currently in the MAC address table of the switch. The switch then forwards frames destined for that valid host to the attacking device. This method can be used to bypass: - A wireless AP with MAC filtering on a wireless network

	- Router ACLs - 802.1x port-based security
ARP Spoofing	ARP spoofing (also known as *ARP poisoning*) uses spoofed ARP messages to associate a different MAC address with an IP address. ARP spoofing can be used to perform a man-in-the-middle attack as follows: 1. When an ARP request is sent by a client for the MAC address of a device, such as the default gateway router, the attacker's system responds to the ARP request with its own MAC address. 2. The client receives the spoofed ARP response and uses that MAC address when communicating with the destination host. For example, packets sent to the default gateway are sent to the attacker instead. 3. The attacker receives all traffic sent to the destination host. The attacker can then forward these packets on to the correct destination using its own MAC address as the source address. ARP spoofing can also be used to perform Denial of Service (DoS) attacks by redirecting communications to fake or nonexistent MAC addresses.
DNS Spoofing	DNS spoofing (also known as *DNS poisoning*) takes advantage of the DNS server's ability to resolve a domain into its respective IP address. This attack: - Exploits DNS vulnerabilities, resolving a domain typed on a browser into a fake IP address. - Redirects connection to a potentially malicious server. Pharming is a cyber attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. The term "pharming" is based on the words "farming" and "phishing".

Countermeasures that prevent spoofing include the following:

- Firewall and router filters that prevent spoofed packets from crossing into or out of your private secured network. Filters drop any packet suspected of being spoofed.
- Certificates that prove identity.
- Reverse DNS lookup to verify the source email address.
- Encrypted communication protocols, such as IPsec.
- Ingress and egress filters that examine packets and identify spoofed packets. Ingress filters examine packets coming into the network, while egress filters examine packets going out of the network. Any packet suspected of being spoofed on its way into or out of your network is dropped.