13.13.2 Network Security Threat Facts

Common network attacks that you should be aware of include the following:

Attack	Description
Man-in-the-Middle	A *man-in-the-middle* attack is used to intercept information passing 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, as well as 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.
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.
Phishing	A *phishing* scam employs an email pretending to be from a trusted organization, asking to verify personal information or send a credit card number. In a phishing attack: - A fraudulent message (that appears to be legitimate) is sent to a victim. - The message requests that the target visit a fraudulent website (which also appears to be legitimate). Graphics, links, and websites look almost identical to legitimate websites they are trying to imitate. - The fraudulent website requests that the victim provide sensitive information, such as an account username and password. Common phishing scams include: - A Rock Phish kit uses a fake website that imitates a real website (such as banks, PayPal®, eBay®, or Amazon®). Phishing emails direct victims to the fake website where they enter account information. A single server can host multiple fake sites using multiple registered DNS names. These sites can be set up and taken down rapidly to avoid detection. - A *Nigerian scam*, also known as a *419 scam*, involves email which requests a small amount of money to help transfer funds from a foreign country. For their assistance, the victim is promised a reward for a much larger amount of money that will be sent at a later date. - In *spear phishing*, attackers gather information about the victim, such as identifying which online banks they use. They then send phishing emails for the specific bank that the victim uses. - *Whaling* is another form of phishing that is targeted to senior executives and high profile victims. - *Vishing* is similar to phishing but instead of an email, the attacker uses Voice over IP (VoIP) to gain sensitive information. The term is a combination of voice and phishing. To protect against phishing: - Check the actual link destination within emails to verify that they go to the correct URL and not a spoofed one. - Do not click on links in emails. Instead, type the real bank URL into the browser. - Verify that HTTPS is used when going to e-commerce sites. HTTPS requires a certificate that matches the server name in the URL that is verified by a trusted CA. You can also look for the lock icon to verify that HTTPS is used. If the website is using an invalid certificate, then an

	invalid SSL certificate warning appears when you try to access the website. - Implement phishing protections within your browser.
Zombie	A *zombie* is a computer that is infected with malware that allows remote software updates and control by a command and control center called a *zombie master*. A zombie: - Is also known as a *bot* (short for robot). - Is frequently used to aid spammers. - Can commit click fraud. The internet uses an advertising model called *pay per click* (PPC). With PPC, ads are embedded on a website by the developer. The advertiser then pays the website owner for each click the ad generates. Zombie computers can imitate a legitimate ad click, generating fraudulent revenue. - Can be used to perform denial of service attacks.
Botnet	A *botnet* refers to a group of zombie computers that are commanded from a central control infrastructure. A botnet is: - Under a command and control infrastructure where the zombie master (also known as the *bot herder*) can send remote commands to order all the bots they control to perform actions. - Capable of performing distributed denial of service attacks. - Detected through the use of firewall logs to determine if a computer is acting as a zombie and participating in external attacks.
Zero Day	A *zero day* attack (also known as a *zero hour* or *day zero* attack) is an attack that exploits computer application vulnerabilities before they are known and patched by the application's developer.

Spoofing is used to hide the true source of packets or to 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

Network attacks may also falsify source or destination addresses for network communications. This is called spoofing. Common methods of spoofing are listed in the table below:

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 occurs 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 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 instead to the attacker. 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.

Countermeasures to prevent spoofing use:

- Firewall and router filters to prevent spoofed packets from crossing into or out of your private secured network. Filters will drop any packet suspected of being spoofed.
- Certificates to prove identity
- Reverse DNS lookup to verify the source email address
- SecureDNS to identify emails with malicious domains. SecureDNS will redirect the user to a safe landing page or send the bad traffic to a sinkhole.
- Encrypted communication protocols, such as IPsec
- Ingress and egress filters to 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 will be dropped.