***IP vulnerabilities***

**ICMP attacks**

Actors use OCMP echo packets (pings) to discover subnets and hosts on a protected network, to generate DoS flood attacks, and to alter host routing tables

**DoS attacks**

Threat actors attempt to prevent lgitimate users from accessing info or services

**DDoS attacks**

Similar to DoS attacks, but features a simultaneous, coordinated attack from multiple source machines

**Address spoofing attacks**

Threat actors spoof the source IP in an attempt to perform blind spoofing or non- blind spoofing

**MiTM**

Actors position themselves between a source and destination to transparently monitor, capture and control the communication

**Session hijacking**

Threat actors gain access to the physical network, and then use an MiTM attack to hijack a session

***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. The ping command is a user-generated ICMP message, called an echo request, that is used to verify connectivity to a destination.

Threat actors use ICMP for reconnaissance and scanning attacks. This 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.

**ICMP echo request and echo reply** used to perform host verification and DoS attacks

**ICMP unreachable**

Used to perform network reconnaissance and scanning attacks

**ICMP mask reply**

Used to map an internal IP network

**ICMP redirects**

Used to lure a target host into sending all traffic through a compromised device and create a MiTM attack

**ICMP router discovery**

Used to inject bogus route entries into the routing table of a target host

**Amplification** - The treat actor forwords ICMP echo request message to many hosts. These message contain the sourse IP address of the victim.

**Reflection** - These hosts all reply to the spoofed IP address of the victim to overwhelm it.

***Address Spoofing Attacks***

IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user. The threat actor can then gain access to otherwise inaccessible data or circumvent security configurations. Spoofing is usually incorporated into another attack such as a Smurf attack.

**Non-blind spoofing** - The threat actor can see the traffic that is being sent between the host and the target. The threat actor uses non-blind spoofing to inspect the reply packet from the target victim. Non-blind spoofing determines the state of a firewall and sequence-number prediction. It can also hijack an authorized session.

**Blind spoofing** - The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks.