Many TCP/IP protocols are now considered insecure and vulnerable to various attacks

TCP/IP includes four main protocols: IP, TCP, UDP, ICMP

**IP vulnerabilities:** Ip address-based vulnerabilities that threaten network infrastructures

**Man-in-the-middle attacks**: Intercepts a communication between two systems

**Session hijacking** (detournement de session): the attacker gains physical access to the network, initiates an MITM attack, and hijacks that session

**Ip address spoofing**: attackers spoof the source IP address in an IP packet

**DoS, DDoS attacks**: attacker attempts to prevent legitimate users from accessing information or services

**Resource exhaustion attacks**: forms of DoS attacks

**ICMP Vulnerabilities**

ICMP can be used to launch information gathering attacks

* ICMP unreachable: used by attackers to perform network reconnaissance
* ICMP mask reply: may be used to map an IP network
* ICMP redirects: a router sends an IP redirect to notify the sender of a better route to the destination
* ICMP router discovery: allow hosts to locate routers that can be used as a gateway to reach IP-based devices on other networks
* Firewalk: active reconnaissance technique that employs techniques to analyze IP packet responses to determine the gateway ACL filters and map out the networks.

**Attack Surface:** is the total sum of all the vulnerabilities in a given computing device or network that are accessible to the attackers

Categories:

* Network attack surface: all vulnerabilities that reload to ports, protocols, channels, devices, network applications…
* Software attack surface: all function in any code that is running in a given system which is available to an unauthenticated user.
* Physical attacks surface:
* Human attack surface: takes advantage of human psychology

**Attacks vector**: is a path or route by which an attack was carried out

**Reconnaissance attacks**

Goal: discover information about targets like (ip address, accessible UDP and TCP ports on target systems, operating system on target system)

Methods for gathering network data:

* **Packet sniffers**: process of capturing data from local network searching for useful information
* **Ping sweeps**: attacker sends a set of ICMP echo packets to a network of machines looking for responses from live hosts.
* **Port scans**: software programs that survey host networks for open ports
* **Information queries**: can be sent via the internet to resolve hostnames from IP addresses or vice versa

**Access attacks**

Password attack: used to obtain system access

Malware: used to infect the victim’s system with malicious software

Spoofing/masquerading

**Man in the middle attacks**

* ARP poisoning: is achieve when an attacker poisons the ARP cache of two devices with the MAC address of the attacker’s NIC
* DNS-based MITM attack: used to supply false DNS information to a host
* DHCP-based MITM attacks: Dhcp server queries and responses are intercepted to help the attacker gain complete knowledge of the network (hostname, Mac address, ip address, dns server)

DOS/DDOS attacks

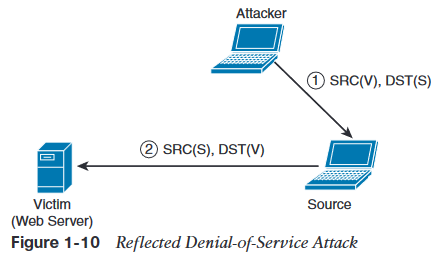
Goal:

**DOS**: uses one system or one network connection to perform a denial-of-service condition to a targeted system, network, or resource

**DDOS** attacks use multiple computers and networks connections that can be geographically dispersed to perform DOS condition against the victim

Three categories of DDOS:

* **Direct DDOS attacks**: occurs when the source of the attacks generates the packets, regardless of protocol, application and so on, that are sent directly to the victim of the attack.
* **Reflected DDOS attacks**



For example, if the attacker (A) decides he wants to attack a victim (V), he will  
send packets (for example, Network Time Protocol [NTP] requests) to a source (S) that thinks  
these packets are legitimate. The source then responds to the NTP requests by sending the  
responses to the victim, who was never expecting these NTP packets from the source.

**Amplification DDOS attacks**: is a form of reflected attack in which the response traffic is made up of packets that are much larger than those that were initially sent by the attacker. Many attackers use botnets to launch DDOS attacks

**Spoofing attacks**

Ip address spoofing, Mac address spoofing, application or service spoofing (ex: attacker enables a rogue DHCP server on a network)

DHCP Attacks

DHCP server spoofing: attacker runs DHCP server software and replies to DHCP request from legitimate clients

DHCP starvation: works by broadcasting of DHCP requests with spoofed MAC addresses to cause denial of service

ARP Poisoning