1. Explain Reconnaissance attacks.

A reconnaissance attack is an attempt to learn more about the intended victim before attempting a more intrusive attack, such as an actual access or DoS. The goal of reconnaissance is to discover the following information about targeted computers or networks:

* IP addresses, sub-domains, and related information on a target network
* Accessible UDP and TCP ports on target systems
* The operating system on target systems

The following lists the four main subcategories or methods for gathering network data:

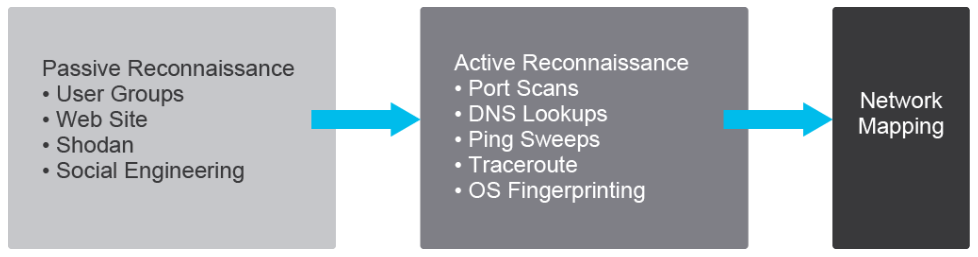
* **Packet sniffers:** Packet sniffing, or packet analysis, is the process of capturing any data that are passed over the local network and looking for any information that may be useful to an attacker. The packet sniffer may be either a software program or a piece of hardware with software installed in it that captures traffic that is sent over the network, which is then decoded and analyzed by the sniffer. Tools, such as Wireshark, Ettercap, or NetworkMiner, give anyone the ability to sniff network traffic with a little practice or training.
* **Ping sweeps:** A ping sweep is another kind of network probe. In a ping sweep, the attacker sends a set of ICMP echo packets to a network of machines, usually specified as a range of IP addresses, and sees which ones respond. The idea is to determine which machines are alive and which aren't. Once the attacker knows which machines are alive, he can focus on which machines to attack and work from there. The fping command is one of the many tools that can be used to conduct ping sweeps.
* **Port scans:** A port scanner is a software program that surveys a host network for open ports. As ports are associated with applications, the attacker can use the port and application information to determine a way to attack the network. The attacker can then plan an attack on any vulnerable service that they find. Examples of insecure services, protocols, or ports include but are not limited to port 21 (FTP), port 23 (Telnet), port 110 (POP3), 143 (IMAP), and port 161 (SNMPv1 and SNMPv2) because protocols using these ports do not provide authenticity, integrity, and confidentiality. NMAP is one of the many tools that can be used for conducting port scans.
* **Information queries:** Information queries can be sent via the Internet to resolve hostnames from IP addresses or vice versa. One of the most commonly used queries is the nslookup command. You can use nslookup by opening a Windows or Linux command prompt window on your computer and entering the nslookup command, followed by the IP address or hostname that you are attempting to resolve.

1. What is Passive and Active Reconnassaince?

Active recon: Direct interaction with target

Passive recon: No direct interaction with target

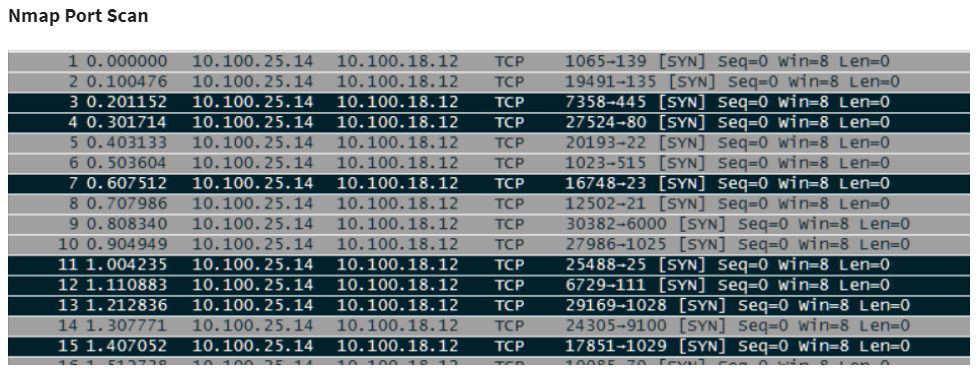
Initially, an attacker attempts to gain information about targeted computers or networks that can be used as a preliminary step toward a further attack seeking to exploit the target system. A reconnaissance attack can be active or passive.



1. Explain Nmap port scan.

Port scanning tools like Network Mapper can cycle through all well-known ports to provide a complete list of all services that are running on the hosts. Nmap is an Open Source tool that is specialized in network exploration and security auditing. Design and operation of port scans uses two components: a host address and a port number that is used by host services. An attacker can attempt to connect to a device on a specified array of ports, such as 21 (FTP), 23 (Telnet) and 25 (SMTP). With the information received from these scans, an attacker can find open ports that could allow access to a network and launch more sophisticated attacks.

The port scan example that is shown below is based on the portscan.pcap packet capture. Packets traveling between a local computer at 10.100.25.14 and a remote computer 10.100.18.12 are being sent to a different port number on the destination machine (for example, 21, 23, 25, 80). These ports happen to be commonly exploited ones, such as 21 (FTP), 23 (Telnet), 25 (SMTP), HTTP (80). When you see a remote computer sending packets to many commonly exploited ports, you can typically assume that a port scan is taking place.



Note: Nmap supports a range of scanning options. The SYN scan (-sS option) is the default and most popular scan option. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections. For more information, refer to https://nmap.org.