Kabeer Ahmed SE-19028

LAB 10

Exercise:

1. Examine the client machine's ARP table and explain what you observed.

The ARP (Address Resolution Protocol) table is a list of IP addresses and their corresponding physical (MAC) addresses that a computer maintains in order to map the IP addresses to the physical addresses on a local network. To examine the ARP table on a Windows client machine, you can use the command prompt and type "arp -a" and press enter. On a Linux or macOS machine, you can use the terminal and type "arp -a" or "arp -n" command.
The ARP table will show you a list of IP addresses and their corresponding MAC addresses that the client machine has recently communicated with on the local network. The list will include entries for the client machine itself, as well as other devices on the network such as routers, switches, and other computers.
You may observe following in the ARP table:
The IP address of the client machine.
The MAC address of the client machine.
The IP address of other devices on the network.
The MAC address of other devices on the network.
The status of the entry (e.g. "dynamic" or "static") indicating whether the entry was learned through ARP or added manually.
The interface (e.g. Ethernet or Wi-Fi) that the entry is associated with.
It is important to note that the ARP table is only used for communication on the local network, and does not contain information about devices outside of the local network.

2. How many responses did the client receive for a certain ARP request?

To determine how many responses a client received for a certain ARP request, you can use the command prompt on Windows or terminal on Linux/macOS.

You can use the command "arp -a" or "arp -n" on the client machine to view the ARP table, which lists all the IP addresses and their corresponding MAC addresses that the client machine has recently communicated with on the local network.

You can observe the number of responses for a certain ARP request by looking at the number of IP addresses listed in the ARP table.

You can also use the command "arp -d" to clear the ARP table and "arp -s" to add a static entry to the ARP table, but these commands are not useful to check the number of responses for a certain ARP request.

It's important to note that the number of responses received for an ARP request may vary depending on the network conditions and the number of devices on the local network. Sometimes, the ARP request may not receive any response if the target host is down or not on the same network.

3. Are the responses being spoofed? Are there valid replies? How can you identify them?

ARP spoofing, also known as ARP cache poisoning, is a type of attack in which an attacker sends fake ARP messages to a network in order to map the attacker's IP address to the target's MAC address. This allows the attacker to intercept network traffic intended for the target host.

To determine if the responses to an ARP request are being spoofed, you can check the ARP table on the client machine using the command "arp -a" or "arp -n" and look for entries that have an unusual or unexpected MAC address associated with a known IP address. You can also use tools such as arpwatch, which monitor the ARP traffic on a network and alert when an unusual ARP packet is detected.

It's also possible to check the ARP table against the known IP and MAC addresses of the devices on the network. If an entry in the ARP table has a different MAC address than the one you expect, it may be an indication of ARP spoofing.

Another way to detect ARP spoofing is to use a tool such as Wireshark that can capture and analyze network traffic. Look for ARP packets with unusual source IP or MAC addresses.

To identify the valid replies, you can cross-reference the ARP table against the list of IP and MAC addresses of devices on your network. If an entry in the ARP table matches the IP and MAC address of a device on your network, it is likely a valid reply.

It's also important to keep in mind that the ARP table is only populated with the IP addresses and MAC addresses of devices that the client machine has recently communicated with, so if a device is not present in the ARP table, it does not necessarily mean that it is not on the network.

4. According to the trace, describe how this attack works.

Without more information about the trace, it is difficult to provide a specific description of how the attack works. However, in general, an ARP spoofing attack works by sending a large number of fake ARP messages to a network, which map the attacker's IP address to the target's MAC address. This allows the attacker to intercept network traffic intended for the target host, and in some cases even manipulate the data in transit.

The attacker can use various tools to perform ARP spoofing, such as arpspoof, Cain and Abel, Ettercap, and many others. These tools allow the attacker to flood the network with fake ARP messages and create a "man-in-the-middle" situation, in which the attacker can intercept and modify network traffic.

Once the attack is successful, the attacker can use the intercepted data to steal sensitive information, launch further attacks, or disrupt network communications. Depending on the nature of the attack, it may also be difficult to detect, as the attacker's IP and MAC addresses may appear legitimate to other devices on the network.

It's important to note that ARP spoofing is just one of the ways an attacker can carry out a man-in-the-middle attack and other methods such as DNS spoofing, SSL stripping, and more can be used.