Ex.No: 7	Experiment with Sniff Traffic using ARP Poisoning.

Aim:

To Experiment Sniff Traffic using ARP Poisoning.

ARP Poisoning:

Address Resolution Protocol (ARP) poisoning is an attack that involves sending spoofed ARP messages over a local area network. It's also known as ARP spoofing, ARP poison routing and ARPcache poisoning.

ARP poisoning is a type of man-in-the-middle attack that can be used to stop network traffic, change it, or intercept it. The technique is often used to initiate further offensives, such as sessionhijacking or denial-of-service.

The relationship between a given MAC address and its IP address is kept in a table known as theARP cache. When a packet heading towards a host on a LAN gets to the gateway, the gateway uses ARP to associate the MAC or physical host address with its correlating IP address.

The host then searches through its ARP cache. If it locates the corresponding address, it is used toconvert the format and packet length. Otherwise, ARP will send out a request packet that asks other machines on the local network if they know the correct address. When a machine replies with the address, the ARP cache is updated.

ARP Poisoning Countermeasures:

We can use several methods to prevent ARP poisoning, each with its own positives and negatives. These include static ARP entries, encryption, VPNs, packet sniffing, Poisoning detectionsoftware, OS security,etc.

Static ARP entries:

This solution involves a lot of administrative overhead and is only recommended forsmaller networks. It involves adding an ARP entry for every machine on a network into each individual computer.

Mapping the machines with sets of static IP and MAC addresses helps to preventspoofing attacks, because the machines can ignore ARP replies**.**

Encryption:

Protocols such as HTTPS and SSH can also help to reduce the chances of a successful ARP poisoning attack. When traffic is encrypted, the attacker would have to

go to the additional stepof tricking the target's browser into accepting an illegitimate certificate.

VPN: If it is just a single person making a potentially dangerous connection, such as using public wifi at an airport, then a VPN will encrypt all of the data that travels between the client and theexit server.

Operating System Security:

This measure is dependent on the OS been used. The following are the basic techniquesused by various operating systems.

- Linux: These work by ignoring unsolicited ARP reply packets.
- Microsoft Windows: The ARP cache behavior can be configured via the registry. The following list includes some of the software that can be used to protect networks against sniffing;

  AntiARP- provides protection against both passive and active sniffing

  Agnitum Outpost Firewall-provides protection against passive sniffing

  XArp- provides protection against both passive and active sniffing
- Mac OS: ArpGuard can be used to provide protection. It protects against both active and passive sniffing.

Sniff Traffic:

Network sniffing is the process of intercepting data packets sent over a network. This can bedone by the specialized software program or hardware equipment. Sniffing can be used to;

- Capture sensitive data such as login credentials
- Eavesdrop on chat messages
- Capture files have been transmitted over a network.

Types of Sniffing:

Passive sniffing is intercepting packages transmitted over a network that uses a hub. It is calledpassive sniffing because it is difficult to detect. It is also easy to perform as the hub sends broadcastmessages to all the computers on the network.

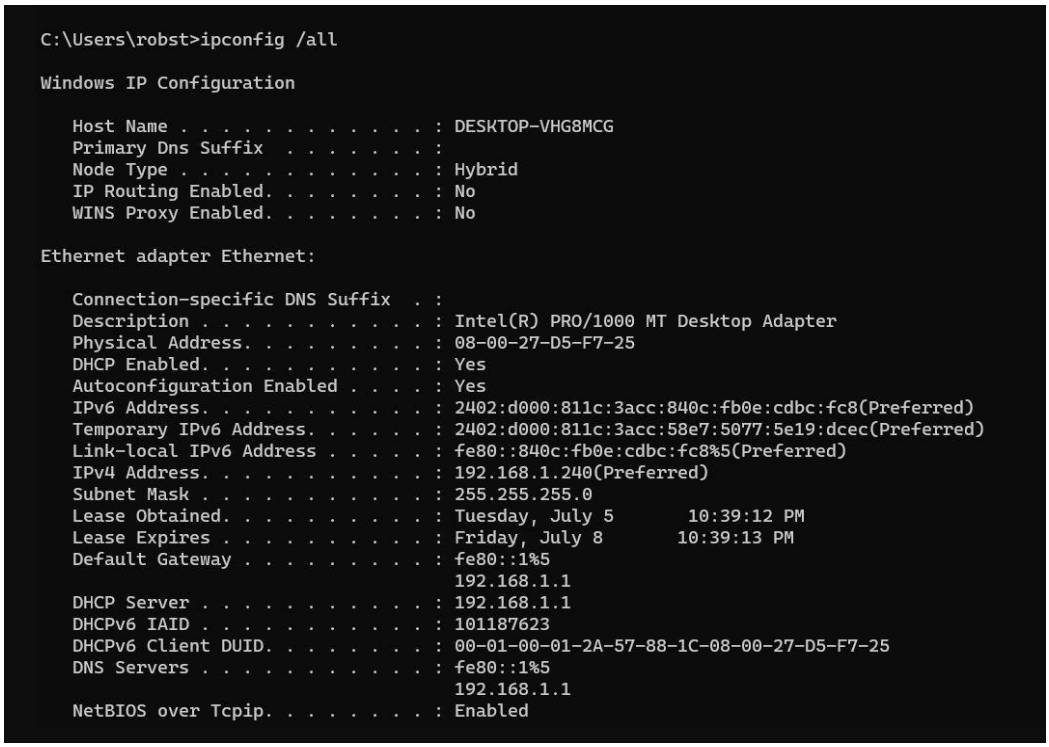
Active sniffing is intercepting packages transmitted over a network that uses a switch. There are two main methods used to sniff switch linked networks, ARP Poisoning, and MAC flooding**.**

Sniff Traffic using ARP Poisoning:

Step 1: Open the command prompt and Enter the command.

```
ipconfig /all
```

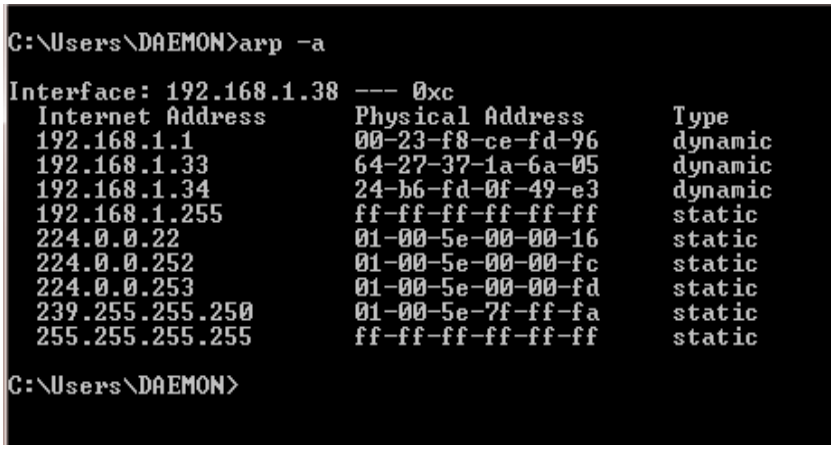
Detailed information about all the network connections available on your computer will be displayed. The results shown below are for a broadband modem to show the MAC address and IPv4format and wireless network to show IPv6 format.



Step 2: apr command calls the ARP configure program located in Windows/System32 directory

-a is the parameter to display to contents of the ARP cache.

```
arp –a
```



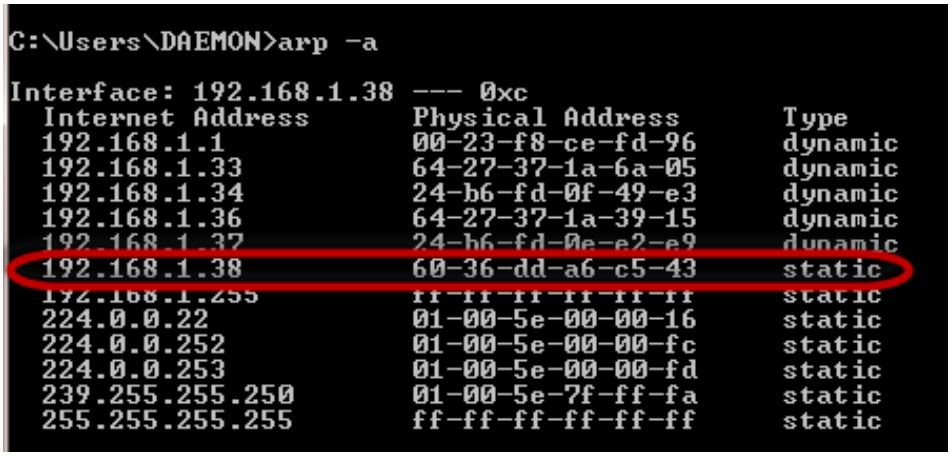
Step 3: Static entries are added manually and are deleted when the computer is restarted.

Step 4: After getting the IP/MAC address, enter the following command.

```
arp -s 192.168.1.38 60-36-DD-A6-C5-43
```

Step 5: To view the ARP cache

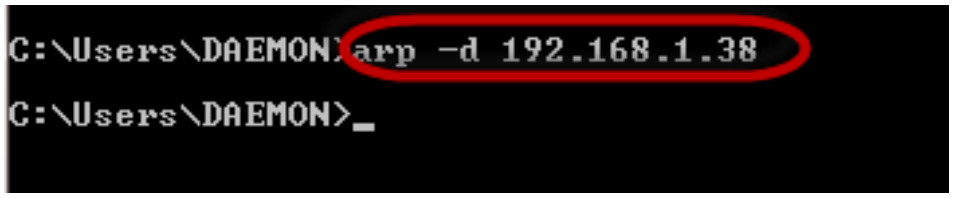
```
arp -a
```



The IP address has been resolved to the MAC address we provided and it is of a static type.

Step 6: Command to remove an entry.

```
arp -d 192.168.1.38
```



ARP poisoning works by sending fake MAC addresses to the switch.

Result:

Thus, the Sniff Traffic using ARP Poisoning have been executed successfully.