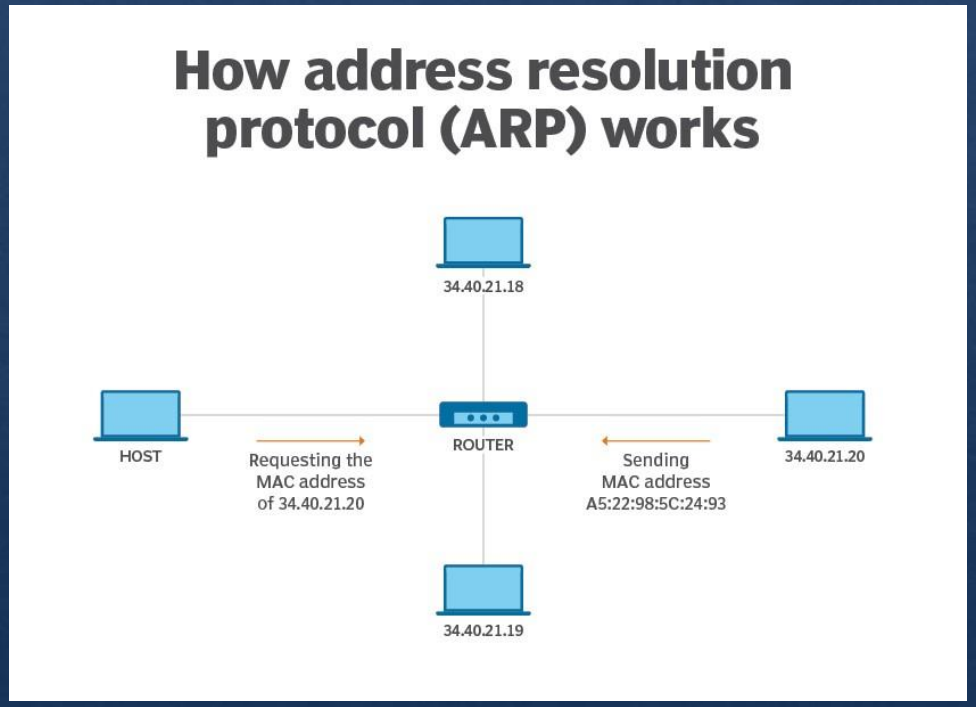
DETECTION OF ARP POISONING AND PROMISCUOUS MODE

BY
MANYAM ABHISHEK
KULADEEP MANTRI
ZAFEER KHAN
POKALKAR RISHITHA

CONTENTS:

HOW ARP WORKS?

- When one machine needs to communicate with another, it looks up its ARP table.
- If the MAC address is not found in the table, the **ARP_request** is broadcasted over the network.
- All machines on the network will compare this IP address to MAC address.
- If one of the machines in the network identifies this address, then it will respond to the **ARP_request** with its IP and MAC address.
- The requesting computer will store the address pair in its ARP table and communication will take place.



WHAT IS ARP POISONING?

- ARP stands for address resolution protocol.
- It is a type of attack in which a malicious actor sends falsified ARP messages over a local network.
- This results in linking of attacker’s mac address with ip address of server.
- Once mac address is connected to an authentic ip address then the attacker will receive any data which is intended for that ip.

FLAWS IN ARP:

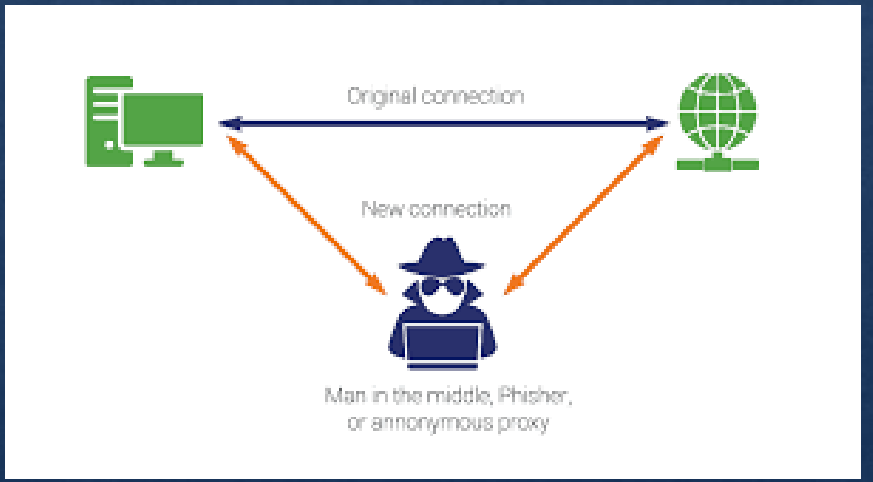
- There are two flaws in this protocol:

1.Problem with this protocol is lack of authentication i.e devices do not authenticate from where the requests or responses come from.

2.Other flaw is device can accept response from any device without actually sending a request to the device.

What is Man In The Middle Attack:

- In a scenario where host is looking for a router , host receives ARP responses from attacker saying that it is a router.
- Now all the ARP requests from host are redirected to the attacker which then forwards it to router.
- At the same time ARP responses are sent to router claiming that it is the host.
- So now all the ARP responses made for the host are forwarded to attacker and then it is forwarded to host.



PROMISCUOUS MODE:

- In a network, promiscuous *mode* allows a network device to intercept and read each network packet that arrives in its entirety.
- In an ethernet local area network (LAN), promiscuous mode is a mode of operation in which every data packet transmitted can be received and read by a network adapter.
- In promiscuous mode, a network adapter does not filter packets. Each network packet on the network segment is directly passed to the operating system (OS) or any monitoring application. If configured, the data is also accessible by any virtual machine (VM) or guest OS on the host system.

PRINCIPLES OF SNIFFING:

- Local networks are composed of ethernet.
- Messages sent through local network are expected to react the right person.
- When a server sends a packet to the devices NIC(Network Interface Card)manages to decide whether to receive or drop the packet.
- If we set NIC to promiscuous mode then all the packets are received regardless of destination.

DETECTION OF ARP POISONING:

- Attacker sends an ARP response which is received by the host system.
- After receiving the ARP response host checks the source ip address . And sends a broadcast message to that ip address which is received by both the attacker and the router.
- Then we retrieve the mac address and check whether the mac address sent from source matches with the mac address received.
- If both the mac addresses match then there is no problem. If the mac addresses are different then the problem is detected.


ARP POISONING
ARP POISONING
Specify interface
eth0
Exit
Start
Result :
YOU ARE SAFE

DETECTION OF PROMISCUOUS MODE:-

FF.FF.FF.FF.FF.FE

Ethernet address of destination	FF FF FF FF FF FF
Ethernet address of sender	00 11 22 33 44 55
Protocol type (ARP = 0806)	08 06
Hardware address space (Ethernet = 01)	00 01
Protocol address space (IPv4 = 0800)	08 00
Byte length of hardware address	06
Byte length of protocol address	04
Opcode (ARP request = 01, ARP reply = 02)	00 01
Hardware address of sender of this packet	<Own NIC's Device Address>
Protocol address of sender of this packet	<Own PC's IP Address>
Hardware address of target of this packet	00 00 00 00 00 00
Protocol address of target	<IP Address (A)>

prepare ARP packet with the following properties:

Detection:

- Send this packet(FF.FF.FF.FF.FF.FE) to the network.
- This packet is supposed to be blocked by hardware filter of target machine .if target machine reply ARP request , then it is in promiscuous mode.
- If there is no reply from target machine it could be either that the target machine is not in promiscuous mode or there is some filtering going on.


Promiscious Mode
Promiscious Mode
IP Address :
192.168.31.161
Exit
Start
Result :
OFF

Any Questions?

Thank you.