Detection of ARP Poisoning

And

Promiscuous Mode

CONTENTS

ABSTRACT

Address Resolution Protocol (**ARP**) is responsible for parsing an IP address into a corresponding MAC address. **ARP** attacks still threaten the Internet of Things (IoT) .
Among various types of attacks on an Ethernet network, “sniffing attack” is probably one of the most difficult attacks to handle. Sniffers are programs that allow a host to capture any packets in an Ethernet network, by putting the host‟s Network Interface Card (NIC) into the promiscuous mode. This documentation discusses about the tools used to detect the ARP poisoning and promiscuous mode.

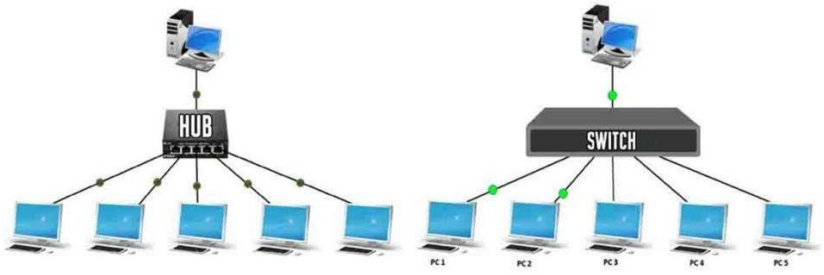
BASIC CONCEPTS

HUB

Hub is commonly used to connect segments of a LAN (Local Area Network). A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. Hub acts as a common connection point for devices in a network.

SWITCH

A switch operates at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI (Open Systems Interconnection) Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs. In networks, the switch is the device that filters and forwards packets between LAN segments.



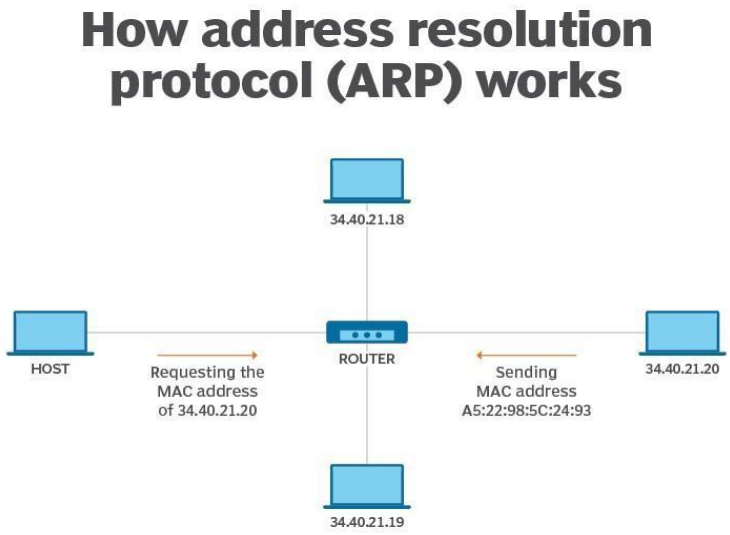
ARP POISONING

What is ARP spoofing?

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 the attacker's mac address with the ip address of the server. Once a mac address is connected to an authentic ip address then the attacker will receive any data which is intended for that ip. What is ARP spoofing?

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 are the 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 the device can accept responses from any device without actually sending a request to the device.

What is man in the middle attack (MITM)?

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

PROMISCUOUS MODE

What is 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.

DETECTION OF ARP POISONING AND PROMISCUOUS MODE

1. DETECTING ARP POISONING:

- Attacker sends an ARP response which is received by the host system.
- After receiving the ARP response, the 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.

SCRIPT:

```
from scapy.all import Ether, ARP, srp, sniff, conf

def get_mac(ip):
    p = Ether(dst='ff:ff:ff:ff:ff:ff')/ARP(pdst=ip)
    result = srp(p, timeout=3, verbose=False)[0]
    return result[0][1].hwsrc

def process(packet):
    if    packet.haslayer(ARP):
        if packet[ARP].op == 2:
            try:
                real_mac = get_mac(packet[ARP].psrc)
                response_mac = packet[ARP].hwsrc
                if real_mac != response_mac:
                    print(f"[!] You are under attack, REAL-MAC: {real_mac.upper()}, FAKE-
MAC: {response_mac.upper()}")
            except IndexError:
                pass
if _name_ == "_main_":
    import sys
    try:
        iface = sys.argv[1]
    except IndexError:
        iface = conf.iface
    sniff(store=False, prn=process, iface=iface)
```

Def Process():

This function is executed every time a packet is sniffed. We took advantage of this function to run a particular set of code which helps us in detection of arp poisoning.

We compare two mac addresses from source and the packet we received to determine if there is an attack going on in our network.

Def get_mac():

This function takes the source ip of the packet as argument and sends the packet using „srp“ function. We determine the source mac address using this function.

Sniff function (scapy) :

Scapy has a sniff function that is great for getting packets off the wire, but there's much more to show off how great this function really is! sniff has an argument prn that allows you to pass a function that executes with each packet sniffed.

2. DETECTING PROMISCUOUS MODE:

- Send this packet (01.00.00.00.00.00) to the network.
- This packet is supposed to be blocked by the hardware filter of the target machine .If the target machine replies to an ARP request, and then it is in promiscuous mode.
- If there is no reply from the target machine it could be either that the target machine is not in promiscuous mode or there is some filtering going on.

SCRIPT:

```
from scapy.all import Ether, ARP, srp, sniff, conf

def get_mac(ip):
    promisc_test = Ether(dst='01:00:00:00:00:00')/ARP(pdst=ip)
    result = srp(promisc_test,timeout=3,verbose=True)[0]
    return result[0][1].hwsrc
if __name___== "__main__":
    import sys
    ip=sys.argv[1]
    while 1:
        try:
            t=get_mac(ip)
            print("promisc")
```

```
except:
    print("safe")
```

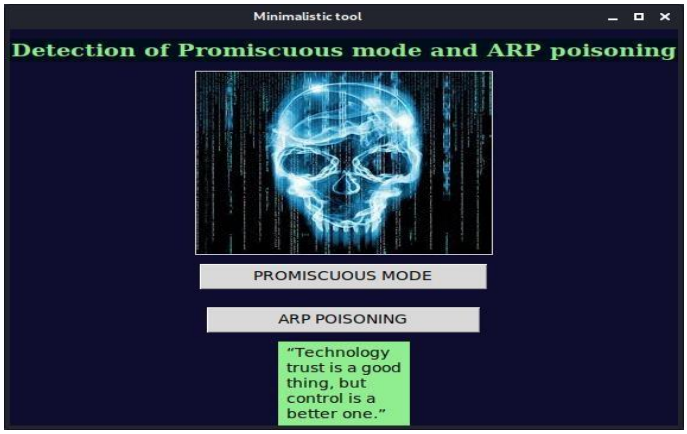
Def get_mac():

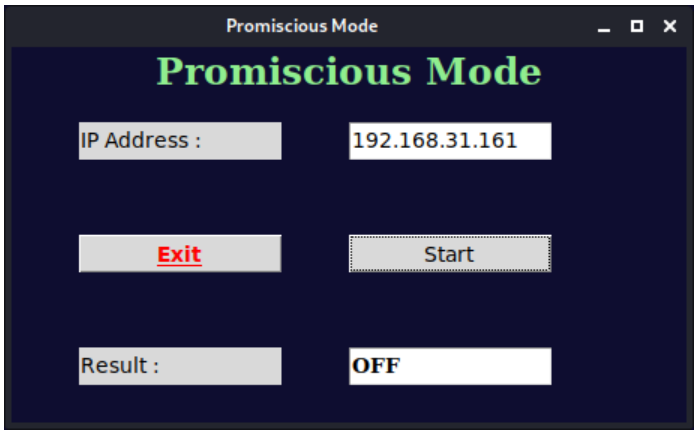
This function takes the target ip as an argument and sends a special packet which will only be received by a machine with promiscuous mode on. The target system responds to the packet, hence proving that it has promiscuous mode on.

Try and catch block:

get_mac() function returns a mac address if the packet is received by the target machines which will not trigger any exception in our code hence proving that the attacker is in promiscuous mode. If nothing is returned by the get_mac() function,it will trigger an exception in the try block indicating that no user is in promiscuous mode.

RESULT





REFERENCES

http://www.securityfriday.com/promiscuous_detection_01.pdf

https://security.radware.com/ddos-knowledge-center/ddospedia/arp-poisoning/