

ARP Spoofing

- 08:00:27:11:cf:53 (ifconfig | grep ether)
- 10.0.2.15 (used the very first IP address, command: ifconfig eth0 | grep 'inet')
- 08:00:27:1a:45:12 (ifconfig | grep HWaddr)
- 10.0.2.4 (ifconfig eth0 | grep 'inet addr:' | cut -d: -f2 | awk '{ print \$1}')
- Kali's routing table:

```
(kali@kali)-[~]
$ netstat -rn
Kernel IP routing table
Destination        Gateway            Genmask           Flags     MSS Window  irtt If
ace
default            10.0.2.1          0.0.0.0           UG        0 0        0 et
h0
10.0.2.0           0.0.0.0           255.255.255.0    U        0 0        0 et
h0

(kali@kali)-[~]
$ netstat -rn
Kernel IP routing table
Destination        Gateway            Genmask           Flags     MSS Window  irtt Iface
0.0.0.0            10.0.2.1          0.0.0.0           UG        0 0        0 eth0
10.0.2.0           0.0.0.0           255.255.255.0    U        0 0        0 eth0
```

- Kali's ARP cache:

```
(kali@kali)-[~]
$ arp
Address              HWtype  HWaddress           Flags Mask            Iface
10.0.2.3             ether   08:00:27:a9:6a:62   C             eth0
10.0.2.1             ether   52:54:00:12:35:00   C             eth0
```

- Metasploitable's routing table:

```
msfadmin@metasploitable:~$ netstat -nr
Kernel IP routing table
Destination        Gateway            Genmask           Flags     MSS Window  irtt Iface
10.0.2.0           0.0.0.0           255.255.255.0    U        0 0        0 eth0
0.0.0.0            10.0.2.1          0.0.0.0           UG        0 0        0 eth0
```

- Metasploitable's ARP cache:

```
msfadmin@metasploitable:~$ arp
Address              HWtype  HWaddress           Flags Mask            Iface
10.0.2.3             ether   08:00:27:A9:6A:62   C             eth0
10.0.2.1             ether   52:54:00:12:35:00   C             eth0
```

- i. The server MAC address, 52:54:00:12:35:00. This is because the gateway of reaching the default address (0.0.0.0) is through 10.0.2.1, as listed on the routing table. And by looking up the ARP cache, the associated MAC address is the one listed above.
- j. There is a response from Metasploitable, but no packets are captured from Wireshark on Kali.
- k. Did that
- l. Metasploitable's ARP cache:

```
msfadmin@metasploitable:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.2.1         ether    08:00:27:11:CF:53  C             eth0
10.0.2.2         ether    08:00:27:11:CF:53  C             eth0
10.0.2.3         ether    08:00:27:11:CF:53  C             eth0
```

After using Ettercap, all HWaddress values were changed to the one that is actually associated with Kali. This means that whenever Metasploitable tries to send packets to a certain IP address, it will use the Kali's MAC address to do so. Therefore all the outgoing packets will be directed to Kali.

- m. To Kali's MAC address, 08:00:27:11:cf:53, because that is the MAC address that Metasploitable associates with the server now. The ARP cache is like a phonebook that stores which IP address corresponds to which MAC address. Ettercap changed the MAC addresses to Kali's address, therefore even though Metasploitable wanted to communicate with the server, it actually communicated with Kali. Kali became the man in the middle!
- n. Did that
- o. Yes, yes, and yes. We can see the response on Metasploitable and also capture the packets on Wireshark. This means that the packets from Metasploitable are sent to Kali, Kali sends them to the server (intended destination), and then it forwards the packets it receives to Metasploitable. This way Kali observes the whole exchange and Metasploitable receives what it asked for. The picture below shows the whole captured exchange in Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.4	45.79.89.123	TCP	74	43291 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=266343 TSecr=0 WS=128
2	0.000000000	45.79.89.123	10.0.2.4	TCP	74	[TCP Retransmission] 43291 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=266343 TSecr=0 WS=128
3	0.052180541	45.79.89.123	10.0.2.4	TCP	60	80 → 43291 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
4	0.055621476	45.79.89.123	10.0.2.4	TCP	58	[TCP Retransmission] 80 → 43291 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
5	0.055818523	10.0.2.4	45.79.89.123	TCP	60	43291 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
6	0.055882200	10.0.2.4	45.79.89.123	HTTP	212	GET / HTTP/1.1
7	0.063654681	10.0.2.4	45.79.89.123	TCP	54	43291 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
8	0.063690925	45.79.89.123	10.0.2.4	TCP	212	[TCP Retransmission] 43291 → 80 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=158
9	0.108698849	45.79.89.123	10.0.2.4	HTTP	933	HTTP/1.1 200 OK (text/html)
10	0.111081628	45.79.89.123	10.0.2.4	TCP	933	[TCP Retransmission] 80 → 43291 [PSH, ACK] Seq=1 Ack=159 Win=32656 Len=879
11	0.111886508	10.0.2.4	45.79.89.123	TCP	60	43291 → 80 [ACK] Seq=159 Ack=880 Win=7032 Len=0
12	0.117117724	10.0.2.4	45.79.89.123	TCP	60	43291 → 80 [FIN, ACK] Seq=159 Ack=880 Win=7032 Len=0
13	0.119815501	10.0.2.4	45.79.89.123	TCP	54	[TCP Keep-Alive] 880 → 43291 [ACK] Seq=159 Ack=880 Win=7032 Len=0
14	0.119843592	10.0.2.4	45.79.89.123	TCP	54	[TCP Out-Of-Order] 43291 → 80 [FIN, ACK] Seq=159 Ack=880 Win=7032 Len=0
15	0.119740540	45.79.89.123	10.0.2.4	TCP	60	80 → 43291 [ACK] Seq=880 Ack=160 Win=32656 Len=0
16	0.127634347	45.79.89.123	10.0.2.4	TCP	54	[TCP Dup ACK 15=1] 80 → 43291 [ACK] Seq=880 Ack=160 Win=32656 Len=0
17	0.164317215	45.79.89.123	10.0.2.4	TCP	60	80 → 43291 [FIN, ACK] Seq=880 Ack=160 Win=32656 Len=0
18	0.167635401	45.79.89.123	10.0.2.4	TCP	54	[TCP Out-Of-Order] 43291 → 80 [FIN, ACK] Seq=159 Ack=880 Win=7032 Len=0
19	0.167826572	10.0.2.4	45.79.89.123	TCP	60	43291 → 80 [ACK] Seq=160 Ack=881 Win=7032 Len=0
20	0.212597000	10.0.2.4	45.79.89.123	TCP	54	[TCP Dup ACK 19=1] 43291 → 80 [ACK] Seq=160 Ack=881 Win=7032 Len=0

- p. About every 10 seconds, Kali's MAC address will claim to be the IP address of the target (Metasploitable, at 10.0.2.4), and telling all of its contacts that Metasploitable's IP address is at the MAC address of Kali. At the same time, Kali's MAC address will claim to be the IP address of all of the targets' contacts

(10.0.2.1 to 10.0.2.3), sending messages to Metasploitable and telling it that all of their associated MAC addresses are Kali's MAC address. As a result, the poisoning "floods" the ARP cache so that all of the IP addresses are linked to the MAC address of Kali and Kali becomes the person-in-the-middle.

- q. Check ARP cache for multiple IP addresses being associated with one MAC address. False positives would be generated in cases when a legitimate organisation/server has multiple IP addresses connected to the same MAC address.

Alternatively, check if ARP packages are being "flooded" frequently. As the poisoning seems to occur by repeatedly sending ARP packages. False positives could occur if there were legitimate reasons for a machine that is repeatedly setting up new connections with other machines and sending the ARP packages frequently.