

Zitian Yue

PERSON-IN-THE-MIDDLE VIA ARP SPOOFING:

- The MAC address of my Kali's main interface is: 00:0c:29:a2:cf:b9
- The IP address of my Kali's main interface is: 192.168.124.128
- The MAC address of Metasploitable's main interface is: 00:0c:29:7e:03:38
- The IP address of Metasploitable's main interface is: 192.168.124.129
- The routing table of Kali is displayed below

```
(kali㉿kali)-[~]
$ netstat -r
Kernel IP routing table
Destination        Gateway            Genmask           Flags     MSS Window  irtt  Iface
default            192.168.124.2     0.0.0.0           UG        0  0        0     eth0
192.168.124.0      0.0.0.0           255.255.255.0     U         0  0        0     eth0

(kali㉿kali)-[~]
$ netstat -rn
Kernel IP routing table
Destination        Gateway            Genmask           Flags     MSS Window  irtt  Iface
0.0.0.0            192.168.124.2     0.0.0.0           UG        0  0        0     eth0
192.168.124.0      0.0.0.0           255.255.255.0     U         0  0        0     eth0
```

- The ARP cache of Kali is displayed below

```
(kali㉿kali)-[~]
$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.124.254          ether    00:50:56:f5:70:8c   C                 eth0
192.168.124.129          ether    00:0c:29:7e:03:38   C                 eth0
192.168.124.2            ether    00:50:56:fd:64:a3   C                 eth0

(kali㉿kali)-[~]
$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.124.254          ether    00:50:56:f5:70:8c   C                 eth0
192.168.124.129          ether    00:0c:29:7e:03:38   C                 eth0
192.168.124.2            ether    00:50:56:fd:64:a3   C                 eth0
```

- The routing table of Metasploitable is displayed below

```
msfadmin@metasploitable:~$ netstat -rn
Kernel IP routing table
Destination        Gateway            Genmask           Flags     MSS Window  irtt  Iface
192.168.124.0      0.0.0.0           255.255.255.0     U         0  0        0     eth0
0.0.0.0            192.168.124.2     0.0.0.0           UG        0  0        0     eth0
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination        Gateway            Genmask           Flags     MSS Window  irtt  Iface
192.168.124.0      *                  255.255.255.0     U         0  0        0     eth0
default            192.168.124.2     0.0.0.0           UG        0  0        0     eth0
```

- The ARP cache of Metasploitable is displayed below

```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.124.128          ether    00:0c:29:a2:cf:b9   C                 eth0
192.168.124.2            ether    00:50:56:fd:64:a3   C                 eth0
192.168.124.254          ether    00:50:56:f5:70:8c   C                 eth0
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.124.128          ether    00:0c:29:a2:cf:b9   C                 eth0
192.168.124.2            ether    00:50:56:fd:64:a3   C                 eth0
192.168.124.254          ether    00:50:56:f5:70:8c   C                 eth0
```

- According to the routing table of Metasploitable, it will need to communicate with 192.168.124.2 first. Then based on the ARP cache of Metasploitable, the MAC address where the interface sends packets will be 00:50:56:fd:64:a3.

- j. The captured packets by Wireshark are displayed below

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.124.129	45.79.89.123	TCP	74	60359 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=2480399 TSecr=0 WS=32
2	0.046148043	45.79.89.123	192.168.124.129	TCP	60	80 → 60359 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.046148428	192.168.124.129	45.79.89.123	TCP	60	60359 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
4	0.046206423	192.168.124.129	45.79.89.123	HTTP	212	GET / HTTP/1.1
5	0.046525689	45.79.89.123	192.168.124.129	TCP	60	80 → 60359 [ACK] Seq=1 Ack=159 Win=64240 Len=0
6	0.094370509	45.79.89.123	192.168.124.129	HTTP	785	HTTP/1.1 200 OK (text/html)
7	0.094439474	192.168.124.129	45.79.89.123	TCP	60	60359 → 80 [ACK] Seq=159 Ack=732 Win=6579 Len=0
8	0.095403897	192.168.124.129	45.79.89.123	TCP	60	60359 → 80 [FIN, ACK] Seq=159 Ack=732 Win=6579 Len=0
9	0.095498391	45.79.89.123	192.168.124.129	TCP	60	80 → 60359 [ACK] Seq=732 Ack=160 Win=64239 Len=0
10	0.141275365	45.79.89.123	192.168.124.129	TCP	60	80 → 60359 [FIN, PSH, ACK] Seq=732 Ack=160 Win=64239 Len=0
11	0.141289795	192.168.124.129	45.79.89.123	TCP	60	60359 → 80 [ACK] Seq=160 Ack=733 Win=6579 Len=0

On Metasploitable, I see an HTTP response that gives the content of the website in form of HTML as shown below

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>CS338 Sandbox</title>
  </head>

  <body>
    <h1>CS338 Sandbox</h1>
    <h2>Fun with security, or maybe insecurity</h2>

    <p>This page should be the page you retrieve for the "Getting started with Wireshark" assignment. Here's my head, as advertised:
    <div></div>
  </p>
</body>
</html>
```

On Kali, I see the transmissions of packets of HTTP protocols are captured. My Metasploitable's interface sends an HTTP request to the IP address of <http://cs338.jeffondich.com/> and receives the HTTP response which provides the service of GET.

- k. I have successfully executed these steps. More detailed analysis will be provided later.
- l. The APR cache of Metasploitable now is displayed below

```
msfadmin@metasploitable:~$ arp -n
```

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.124.128	ether	00:0C:29:A2:CF:B9	C		eth0
192.168.124.2	ether	00:0C:29:A2:CF:B9	C		eth0
192.168.124.254	ether	00:0C:29:A2:CF:B9	C		eth0

It shows that every host's MAC address is now the same as my Kali's main interface's MAC address: 00:0c:29:a2:cf:b9.

- m. Since every host has same MAC address now, Metasploitable will send the TCP SYN packet to the IP address of 192.168.124.128 which is my Kali's main interface. Metasploitable will base its sending on the MAC address which points to the Kali's main interface. Therefore, Kali will now function as the medium of information transmission for Metasploitable and cause the PITM problem.
- n. I did this step.
- o. The captured packets by Wireshark are displayed below

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.124.129	45.79.89.123	TCP	74	42258 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3929254 TSecr=0 WS=32
2	0.007640820	192.168.124.129	45.79.89.123	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 42258 → 80 [SYN] Seq=0 Win=5840 Len=0
3	0.053878246	45.79.89.123	192.168.124.129	TCP	60	80 → 42258 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4	0.055790904	45.79.89.123	192.168.124.129	TCP	58	[TCP Out-Of-Order] 80 → 42258 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5	0.055989671	192.168.124.129	45.79.89.123	TCP	60	42258 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
6	0.056012028	192.168.124.129	45.79.89.123	HTTP	212	GET / HTTP/1.1
7	0.067892555	192.168.124.129	45.79.89.123	TCP	54	42258 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
8	0.067987325	192.168.124.129	45.79.89.123	TCP	212	[TCP Retransmission] 42258 → 80 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=158
9	0.068724484	45.79.89.123	192.168.124.129	TCP	60	80 → 42258 [ACK] Seq=1 Ack=159 Win=64240 Len=0
10	0.075767113	45.79.89.123	192.168.124.129	TCP	54	[TCP Dup ACK 9] 80 → 42258 [ACK] Seq=1 Ack=159 Win=64240 Len=0
11	0.115000195	45.79.89.123	192.168.124.129	HTTP	785	HTTP/1.1 200 OK (text/html)
12	0.123610401	45.79.89.123	192.168.124.129	TCP	785	[TCP Retransmission] 80 → 42258 [PSH, ACK] Seq=1 Ack=159 Win=64240 Len=731
13	0.123816072	192.168.124.129	45.79.89.123	TCP	60	42258 → 80 [ACK] Seq=159 Ack=732 Win=6579 Len=0
14	0.125267332	192.168.124.129	45.79.89.123	TCP	60	42258 → 80 [FIN, ACK] Seq=159 Ack=732 Win=6579 Len=0
15	0.135913391	192.168.124.129	45.79.89.123	TCP	54	[TCP Keep-Alive] 42258 → 80 [ACK] Seq=159 Ack=732 Win=6579 Len=0
16	0.136007530	192.168.124.129	45.79.89.123	TCP	54	[TCP Out-Of-Order] 42258 → 80 [FIN, ACK] Seq=159 Ack=732 Win=6579 Len=0
17	0.136343020	45.79.89.123	192.168.124.129	TCP	60	80 → 42258 [ACK] Seq=732 Ack=160 Win=64239 Len=0
18	0.143060704	45.79.89.123	192.168.124.129	TCP	64	[TCP Fin ACK] 73211 → 42258 [FIN] Seq=732 Ack=160 Win=64239 Len=0

On Metasploitable I see an HTTP response which gives the information about the web page of <http://cs338.jeffondich.com/>. It shows that packets of TCP and HTTP protocols are transmitted between Metasploitable and cs338.jeffondich.com. Some TCP protocols are “normal” as building the connection between these two IP addresses while there are some weird TCP protocols communicating about the problem of retransmission. The HTTP protocols are requests and responses regarding the information of web page <http://cs338.jeffondich.com/>.

- p. The captured packets by Wireshard are displayed below

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	VMware_a2:cf:b9	VMware_7e:03:38	ARP	42	192.168.124.254 is at 00:0c:29:a2:cf:b9
2	0.000121552	VMware_a2:cf:b9	VMware_f5:70:8c	ARP	42	192.168.124.129 is at 00:0c:29:a2:cf:b9 (duplicate use of 192.168.124.254
3	0.010548204	VMware_a2:cf:b9	VMware_7e:03:38	ARP	42	192.168.124.2 is at 00:0c:29:a2:cf:b9
4	0.010609922	VMware_a2:cf:b9	VMware_fd:64:a3	ARP	42	192.168.124.129 is at 00:0c:29:a2:cf:b9 (duplicate use of 192.168.124.2 de
5	0.021017866	VMware_a2:cf:b9	VMware_7e:03:38	ARP	42	192.168.124.1 is at 00:0c:29:a2:cf:b9
6	0.021072460	VMware_a2:cf:b9	VMware_c0:00:08	ARP	42	192.168.124.129 is at 00:0c:29:a2:cf:b9 (duplicate use of 192.168.124.1 de
7	1.032104134	VMware_a2:cf:b9	VMware_7e:03:38	ARP	42	192.168.124.254 is at 00:0c:29:a2:cf:b9
8	1.032195554	VMware_a2:cf:b9	VMware_f5:70:8c	ARP	42	192.168.124.129 is at 00:0c:29:a2:cf:b9 (duplicate use of 192.168.124.254
9	1.043078223	VMware_a2:cf:b9	VMware_7e:03:38	ARP	42	192.168.124.2 is at 00:0c:29:a2:cf:b9
10	1.043160816	VMware_a2:cf:b9	VMware_fd:64:a3	ARP	42	192.168.124.129 is at 00:0c:29:a2:cf:b9 (duplicate use of 192.168.124.2 de
11	1.053653240	VMware_a2:cf:b9	VMware_7e:03:38	ARP	42	192.168.124.1 is at 00:0c:29:a2:cf:b9
12	1.053721637	VMware_a2:cf:b9	VMware_c0:00:08	ARP	42	192.168.124.129 is at 00:0c:29:a2:cf:b9 (duplicate use of 192.168.124.1 de
13	2.064768507	VMware_a2:cf:b9	VMware_7e:03:38	ARP	42	192.168.124.254 is at 00:0c:29:a2:cf:b9
14	2.064865834	VMware_a2:cf:b9	VMware_f5:70:8c	ARP	42	192.168.124.129 is at 00:0c:29:a2:cf:b9 (duplicate use of 192.168.124.254
15	2.075197484	VMware_a2:cf:b9	VMware_7e:03:38	ARP	42	192.168.124.2 is at 00:0c:29:a2:cf:b9
16	2.075258058	VMware_a2:cf:b9	VMware_fd:64:a3	ARP	42	192.168.124.129 is at 00:0c:29:a2:cf:b9 (duplicate use of 192.168.124.2 de
17	2.085618454	VMware_a2:cf:b9	VMware_7e:03:38	ARP	42	192.168.124.1 is at 00:0c:29:a2:cf:b9
18	2.085678135	VMware_a2:cf:b9	VMware_c0:00:08	ARP	42	192.168.124.129 is at 00:0c:29:a2:cf:b9 (duplicate use of 192.168.124.1 de

It shows that Kali at MAC address of 00:0c:29:a2:cf:b9 is constantly sending packets of ARP protocols to all other hosts stating that the corresponding IP addresses are at the MAC address of 00:0c:29:a2:cf:b9 which is same as Kali's. Therefore, the Metasploitable will respond to the command arp with one MAC address for all hosts.

- q. I would have my detector to check whether the situation of repetitive MAC address for hosts exists. I would also have my detector to extract actual MAC address and then compare it with detected ones to ensure that my device is sending packets to expected servers. Finally, I would have my detector to monitor ARP packets transmission for unusual activities between my device and other servers.