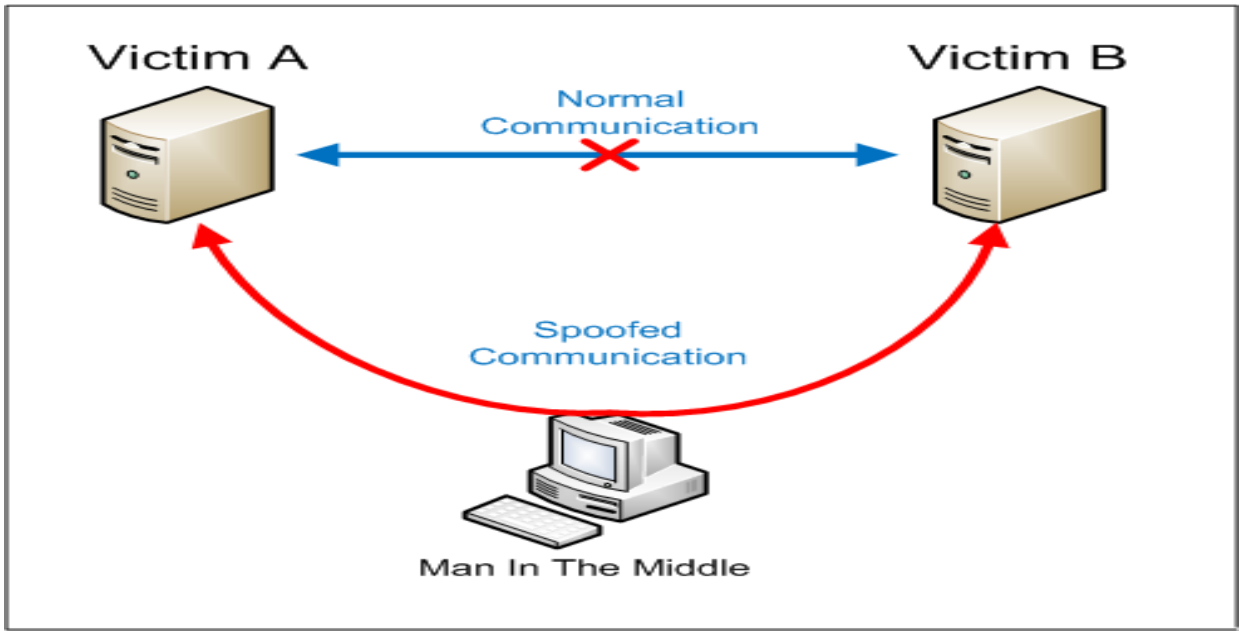
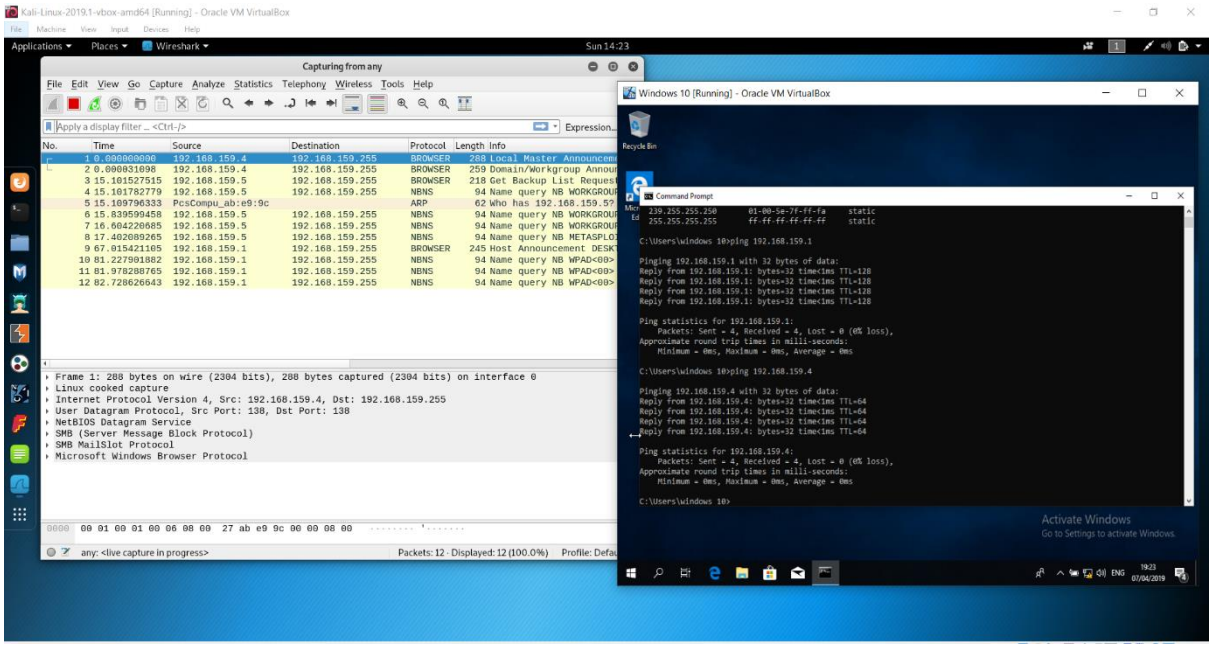
A man in the middle attack is when the attacker place itself in the middle of communications between two devices. In order to accomplish this, the attacker can launch the attack from a device that belongs to the network or can gain illegal access to the network.

Once the attacker has access to the network will then sit in the middle. To do so the attacker will trick the target device and other device (default gateway or any other device in the network) by making them to send traffic through the attacker's device and not directly between them.



There are different ways to do so: ARP spoofing, DHCP spoofing, NDP poisoning (IPv6) and others. Also, there are a number of tools that make it "easy" to perform this kind of attack: Ettercap, Cain and Abel, MIMF (Man in the middle framework), Evilgrade and many others. For the purpose of this assignment we will be using Ettercap since is preinstalled in Kali Linux and we will be performing the MITM attack using ARP poisoning (ARP spoofing). Ettercap can be used from the command line or using its graphical user interface.

The following are screen shots of the process of performing the man in the middle attack.



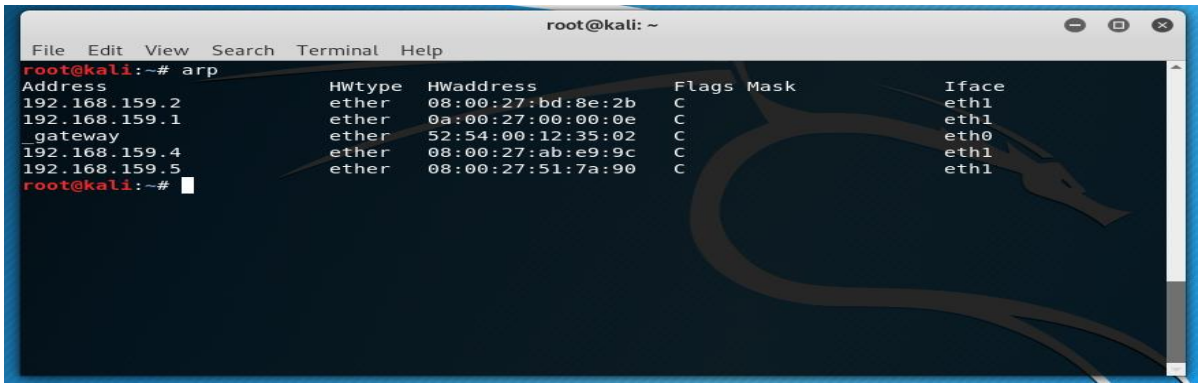
img 1

In image we can see the result of doing ping from the Windows10 machine to metaspoitable (192.168.159.4) and the host machine (192.168.159.1) which acts as the gateway. Note that even if the pings are successful, when we run Wireshark on the Kali machine, we can see the traffic like ARP and NBNS (NetBios Name Service) since we are in the same network, but we cannot see detailed information regarding this traffic. ***NOTE:*** find more about NBNS here: https://wiki.wireshark.org/NetBIOS/NBNS.

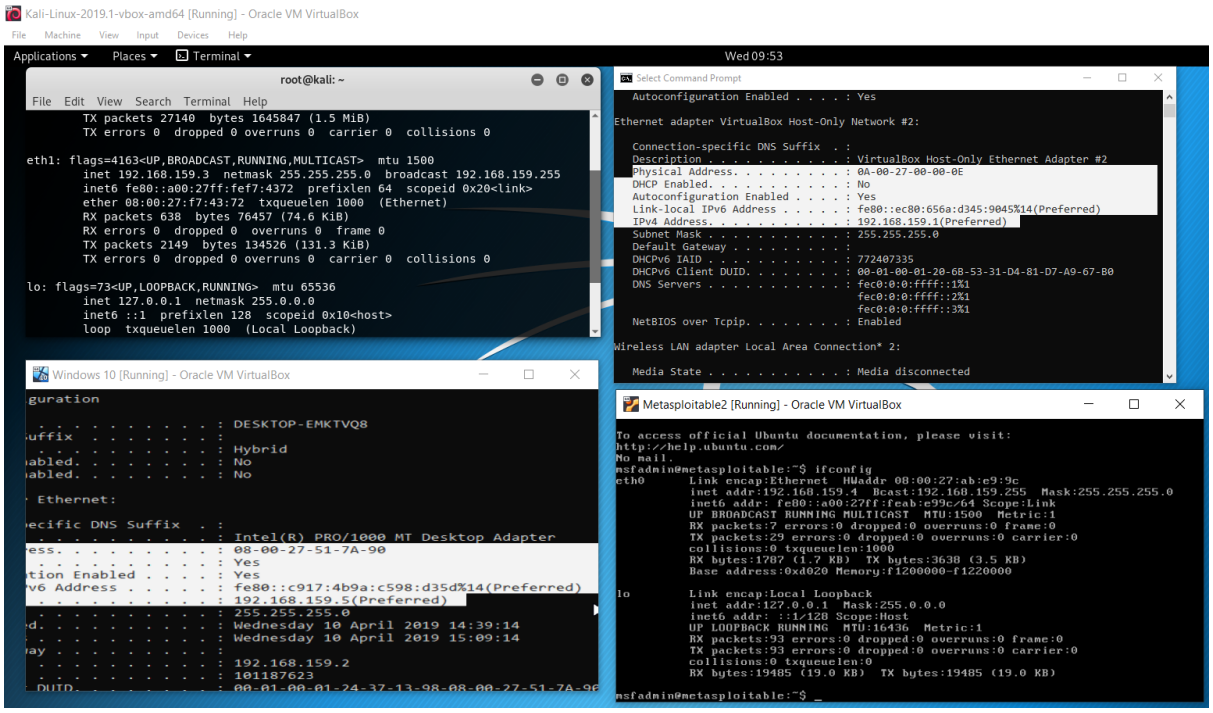
Performing the attack.

First, we need to identify the target for the attack, this can be done by scanning the network. For this end we can use the terminal in the kali machine with commands such as:

- arp
- netdiscover -i (interface we want to scan) -r (the network we want to scan)
  i.e. netdiscover -i eth1 -r 192.168.159.0
- nmap -sn (-sn refers to the network we want to scan) / cider notation for the subnet mask
  i.e. nmap -sn 192.168.159.0/24



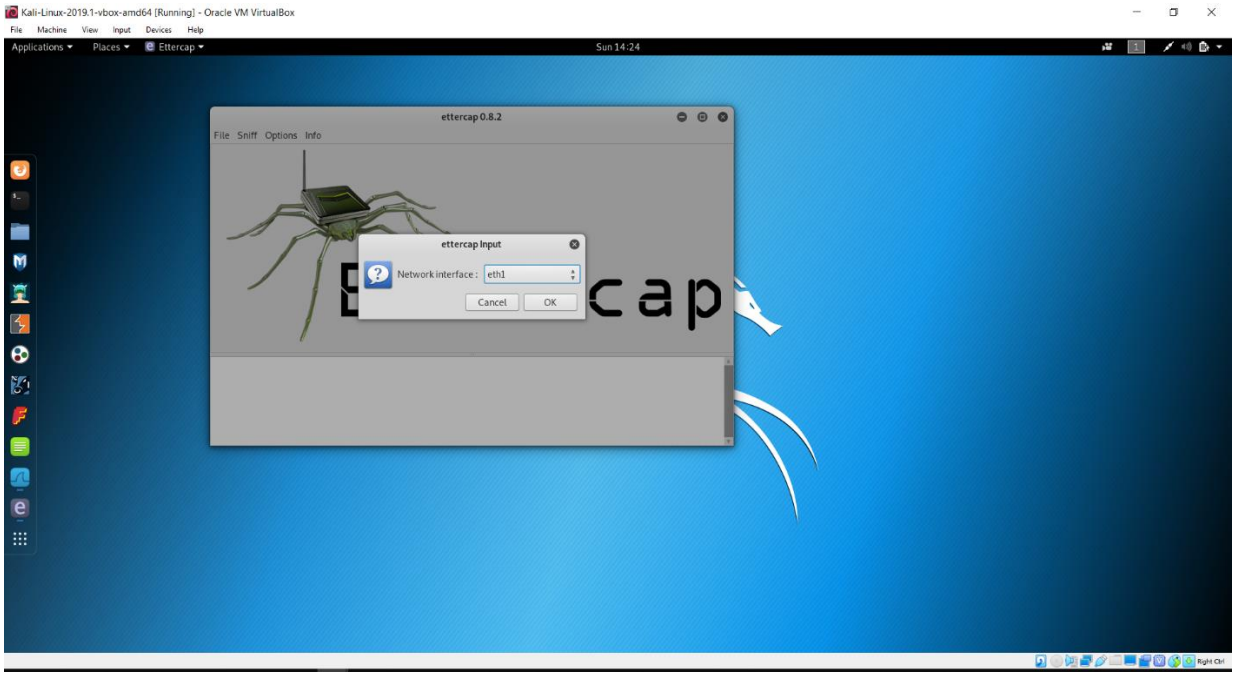
img 2



img 3

In (img 2) we can see the result of executing the arp command in the Kali VM, this shows the arp table that contains the MAC address and the IP address associated to it for all devices that have been communicating in the subnet and we can confirm this by executing the commands (ipconfig /all) in Windows and (ifconfig) in Linux (img 3).

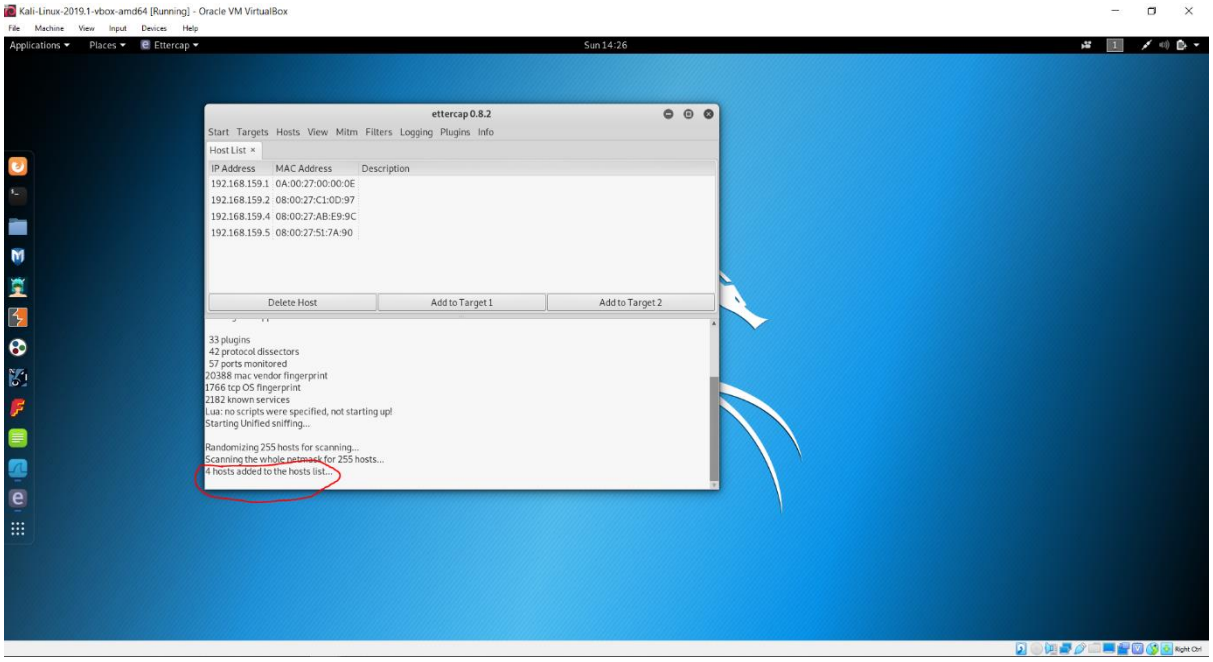
However, Ettercap will scan the network for us when using the GUI.



img 4

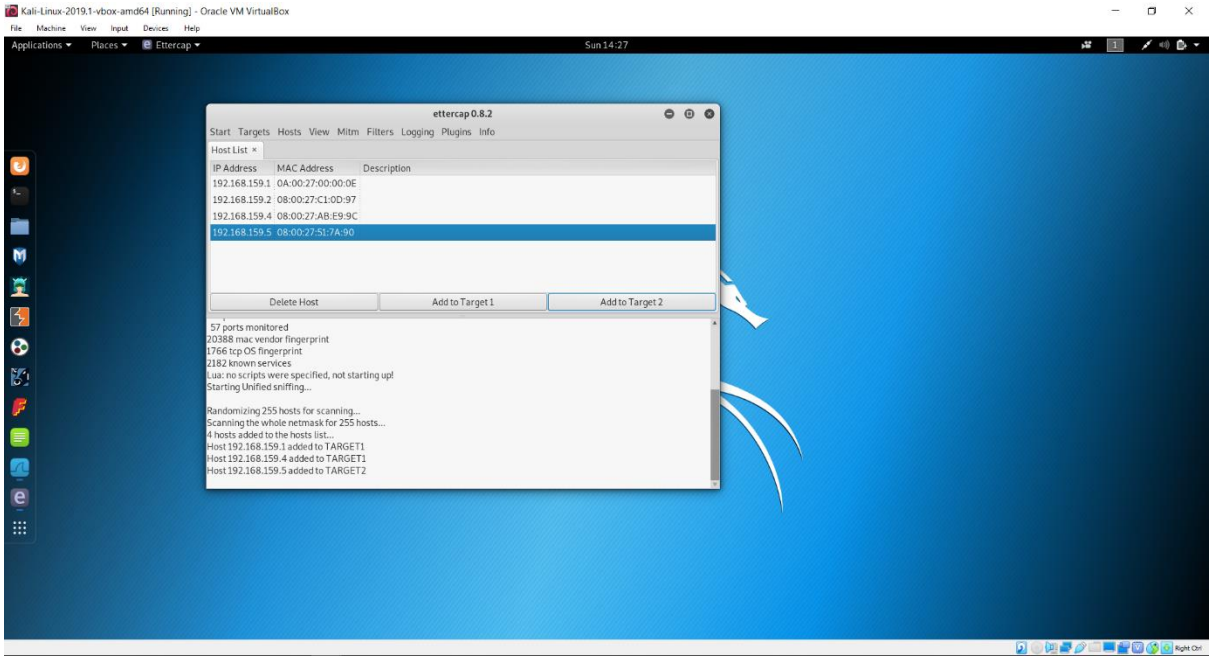

Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Ettercap
Sun 14:25
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Hosts list Ctrl+H
Enable IPv6 scan
Scan for hosts Ctrl+S
Load from file...
Save to file...
Ettercap
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...
33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

img 5


Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Ettercap
Sun 14:26
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List
IP Address MAC Address Description
192.168.159.1 0A:00:27:00:00:0E
192.168.159.2 08:00:27:C1:0D:97
192.168.159.4 08:00:27:AB:E9:9C
192.168.159.5 08:00:27:51:7A:90
Delete Host
Add to Target 1
Add to Target 2
33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...

img 6

After starting Ettercap we have to choose the interface we want to scan or sniff (img 4) and then we can scan for hosts in that interface (img 5), then we can clicking on hosts list to see all host identified on that interface, Ettercap shows all IP addresess and their maping to MAC addresses (img 6), notice that the result matches the result shown by the arp command in img 3. In this case we are using the interface ethernet 1 (eth1), if you are using wifi you will select something like wlan0 or any other interface that applys.

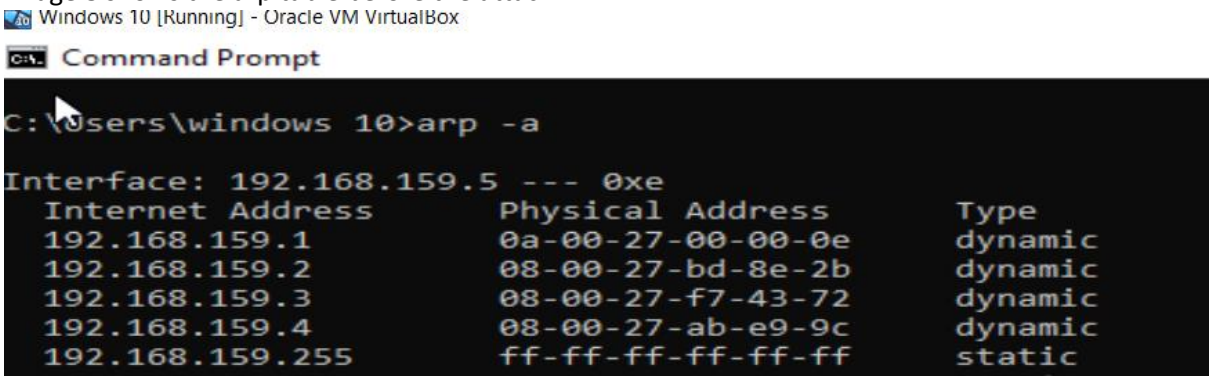


img 7

Now we can add the target or targets to groups (img 7), basically we are telling Ettercap that we want to be in the middle of group 1 (host pc, metaspotable2) and group 2 (Windows Vm) and then we can start the attack.

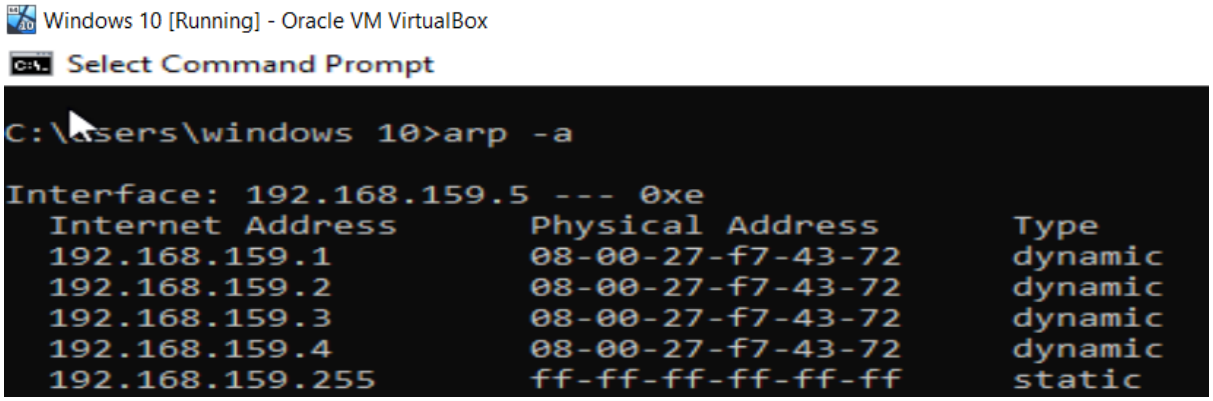
We can si the result of the attack issuing the command arp -a in the windows VM, the target.

Image 8 shows the arp table before the attack



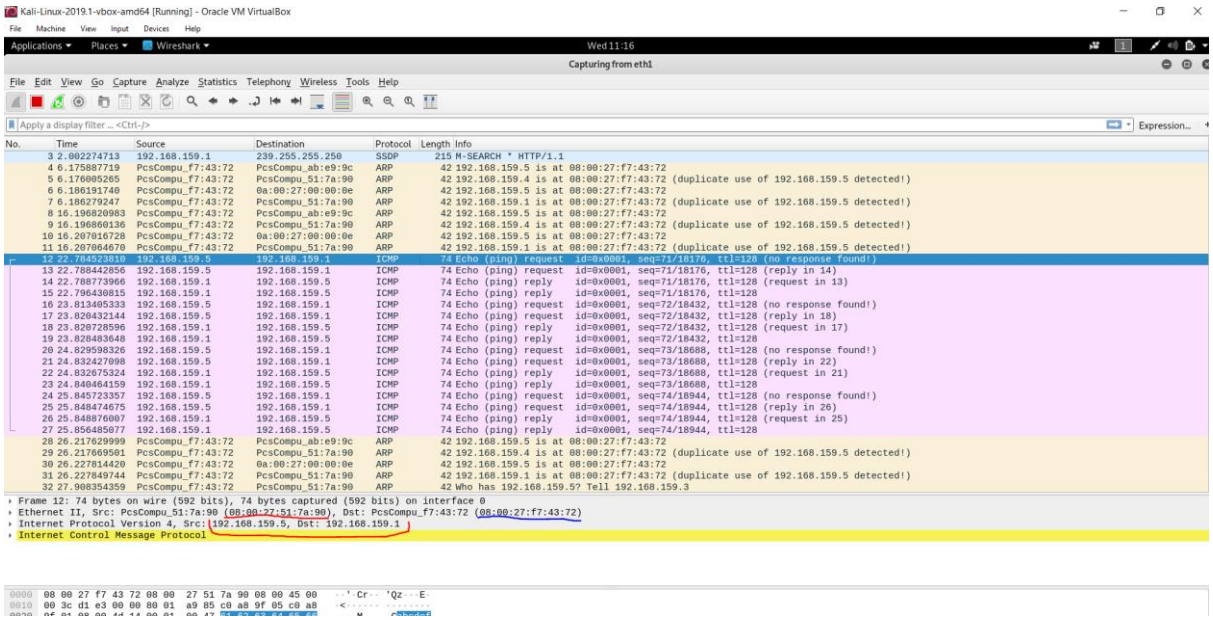
img 8

Image 9 shows the arp table after the attack is lauched.

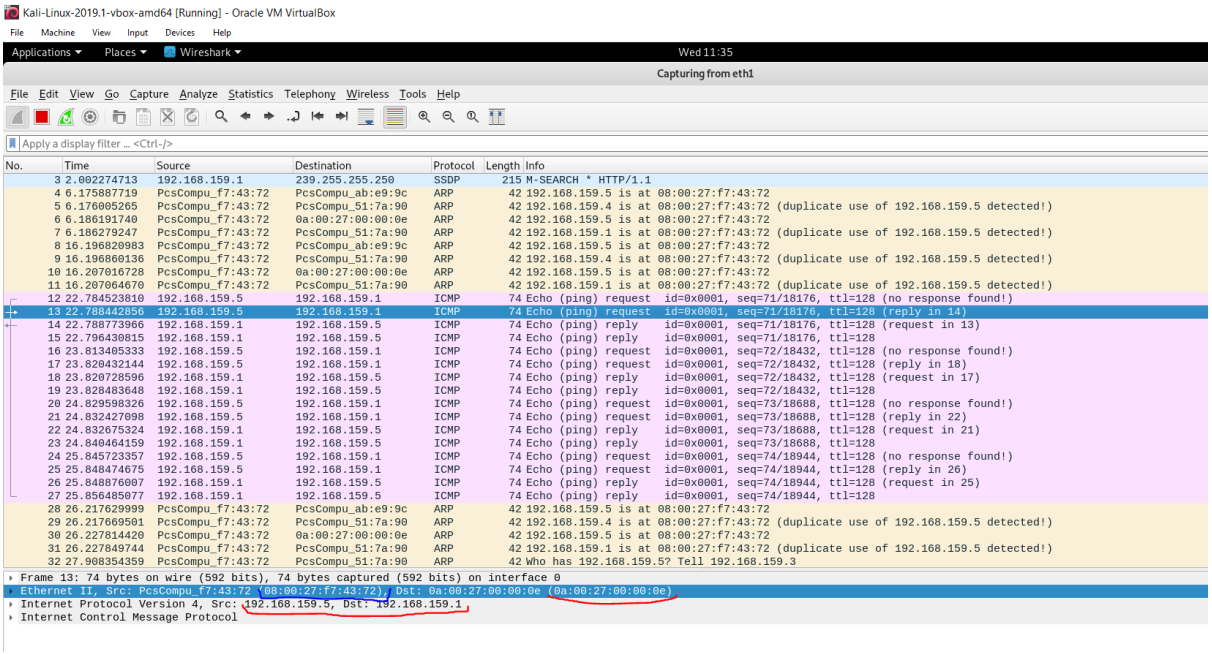


img 9

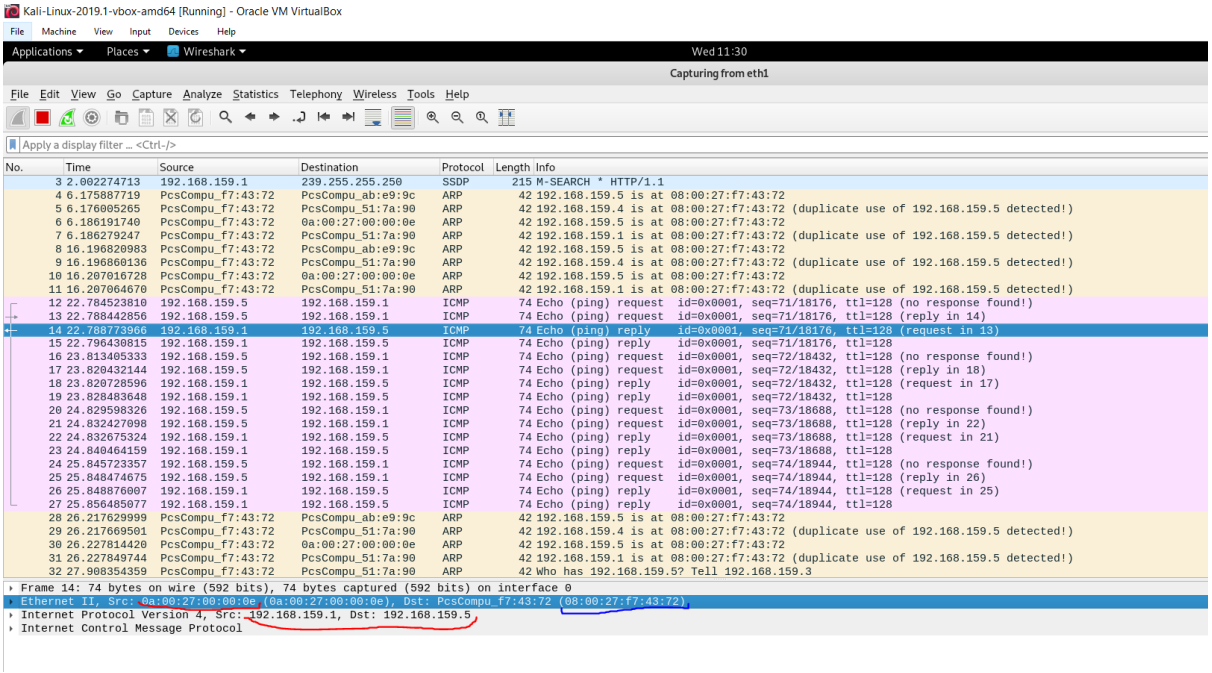
Notice how all Ip addresses are mapped to the same MAC address, which is the MAC of the attacker, the Kali VM. We can see this in more detail using Wireshark. The next image shows a ping from the Windows VM to the host machine.



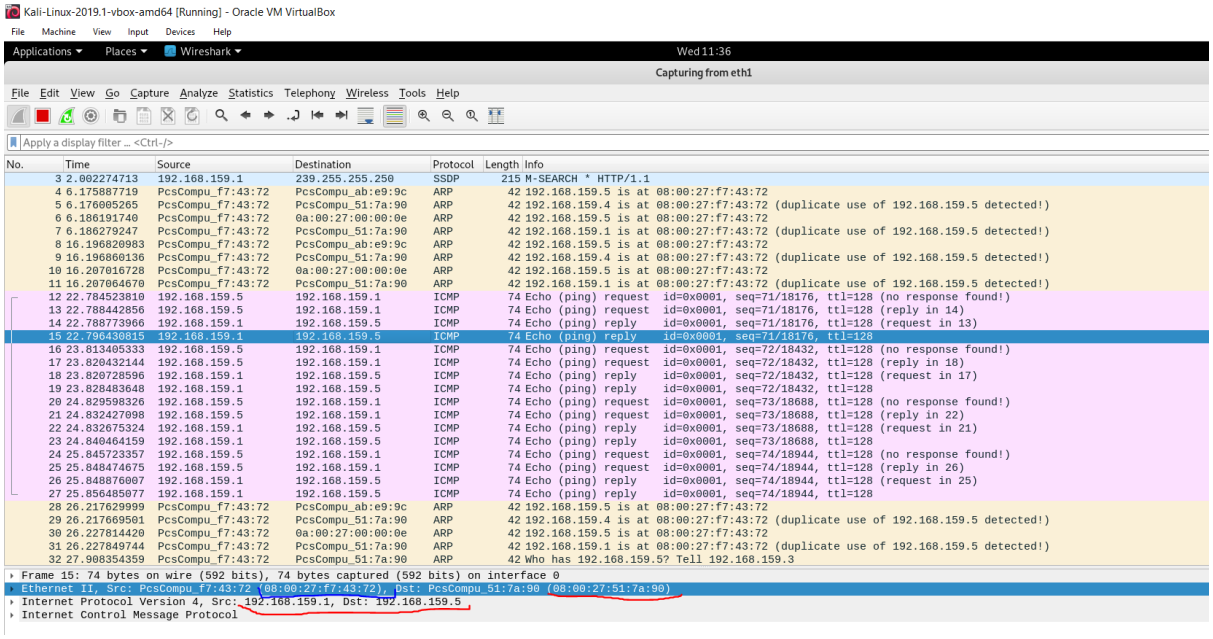
img 10


Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Wireshark Wed 11:35
Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
3 2.002274713 192.168.159.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
4 6.175887719 PcsCompu_f7:43:72 PcsCompu_ab:e9:9c ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
5 6.176005265 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.4 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
6 6.186191740 PcsCompu_f7:43:72 0a:00:27:00:00:0e ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
7 6.186279247 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.1 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
8 16.196820983 PcsCompu_f7:43:72 PcsCompu_ab:e9:9c ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
9 16.196860136 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.4 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
10 16.207016728 PcsCompu_f7:43:72 0a:00:27:00:00:0e ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
11 16.207064670 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.1 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
12 22.784523810 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (no response found!)
13 22.788442856 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 14)
14 22.788773966 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=71/18176, ttl=128 (request in 13)
15 22.796430815 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=71/18176, ttl=128
16 23.813405333 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (no response found!)
17 23.820432144 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (reply in 18)
18 23.820728596 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=72/18432, ttl=128 (request in 17)
19 23.828483648 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=72/18432, ttl=128
20 24.829598326 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (no response found!)
21 24.832427098 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (reply in 22)
22 24.832675324 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=73/18688, ttl=128 (request in 21)
23 24.840464159 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=73/18688, ttl=128
24 25.845723357 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (no response found!)
25 25.848474675 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (reply in 26)
26 25.848876007 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=74/18944, ttl=128 (request in 25)
27 25.856485077 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=74/18944, ttl=128
28 26.217629999 PcsCompu_f7:43:72 PcsCompu_ab:e9:9c ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
29 26.217669501 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.4 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
30 26.227814420 PcsCompu_f7:43:72 0a:00:27:00:00:0e ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
31 26.227849744 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.1 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
32 27.908354359 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 Who has 192.168.159.5? Tell 192.168.159.3
Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: PcsCompu_f7:43:72 (08:00:27:f7:43:72), Dst: 0a:00:27:00:00:0e (0a:00:27:00:00:0e)
Internet Protocol Version 4, Src: 192.168.159.5, Dst: 192.168.159.1
Internet Control Message Protocol

img 11


Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Wireshark Wed 11:30
Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
3 2.002274713 192.168.159.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
4 6.175887719 PcsCompu_f7:43:72 PcsCompu_ab:e9:9c ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
5 6.176005265 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.4 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
6 6.186191740 PcsCompu_f7:43:72 0a:00:27:00:00:0e ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
7 6.186279247 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.1 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
8 16.196820983 PcsCompu_f7:43:72 PcsCompu_ab:e9:9c ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
9 16.196860136 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.4 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
10 16.207016728 PcsCompu_f7:43:72 0a:00:27:00:00:0e ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
11 16.207064670 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.1 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
12 22.784523810 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (no response found!)
13 22.788442856 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 14)
14 22.788773966 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=71/18176, ttl=128 (request in 13)
15 22.796430815 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=71/18176, ttl=128
16 23.813405333 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (no response found!)
17 23.820432144 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (reply in 18)
18 23.820728596 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=72/18432, ttl=128 (request in 17)
19 23.828483648 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=72/18432, ttl=128
20 24.829598326 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (no response found!)
21 24.832427098 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (reply in 22)
22 24.832675324 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=73/18688, ttl=128 (request in 21)
23 24.840464159 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=73/18688, ttl=128
24 25.845723357 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (no response found!)
25 25.848474675 192.168.159.5 192.168.159.1 ICMP 74 Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (reply in 26)
26 25.848876007 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=74/18944, ttl=128 (request in 25)
27 25.856485077 192.168.159.1 192.168.159.5 ICMP 74 Echo (ping) reply id=0x0001, seq=74/18944, ttl=128
28 26.217629999 PcsCompu_f7:43:72 PcsCompu_ab:e9:9c ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
29 26.217669501 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.4 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
30 26.227814420 PcsCompu_f7:43:72 0a:00:27:00:00:0e ARP 42 192.168.159.5 is at 08:00:27:f7:43:72
31 26.227849744 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 192.168.159.1 is at 08:00:27:f7:43:72 (duplicate use of 192.168.159.5 detected!)
32 27.908354359 PcsCompu_f7:43:72 PcsCompu_51:7a:90 ARP 42 Who has 192.168.159.5? Tell 192.168.159.3
Frame 14: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 0a:00:27:00:00:0e (0a:00:27:00:00:0e), Dst: PcsCompu_f7:43:72 (08:00:27:f7:43:72)
Internet Protocol Version 4, Src: 192.168.159.1, Dst: 192.168.159.5
Internet Control Message Protocol

img 12

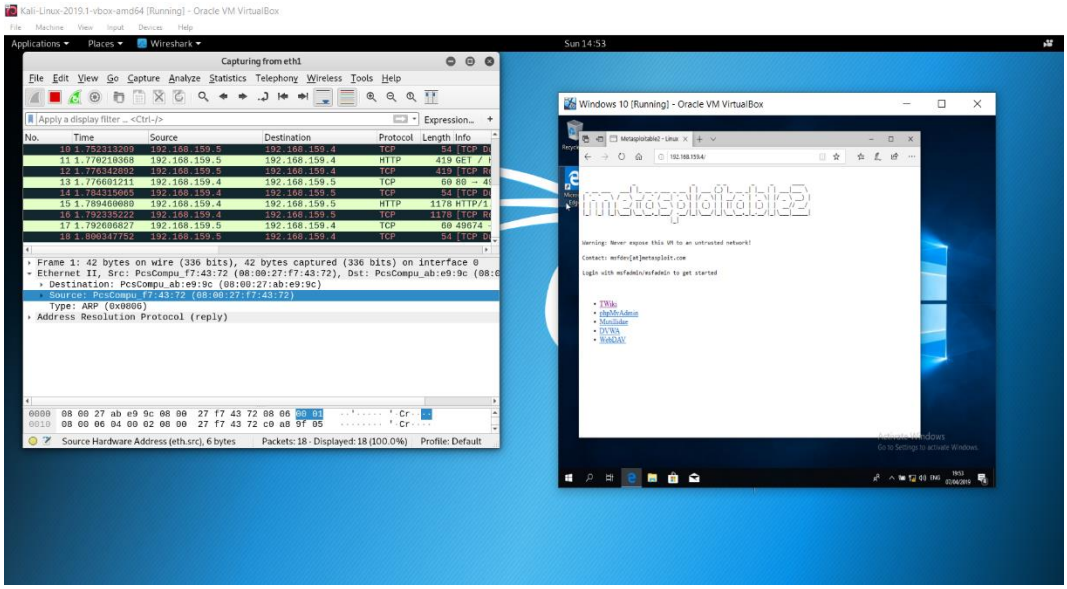


img 13

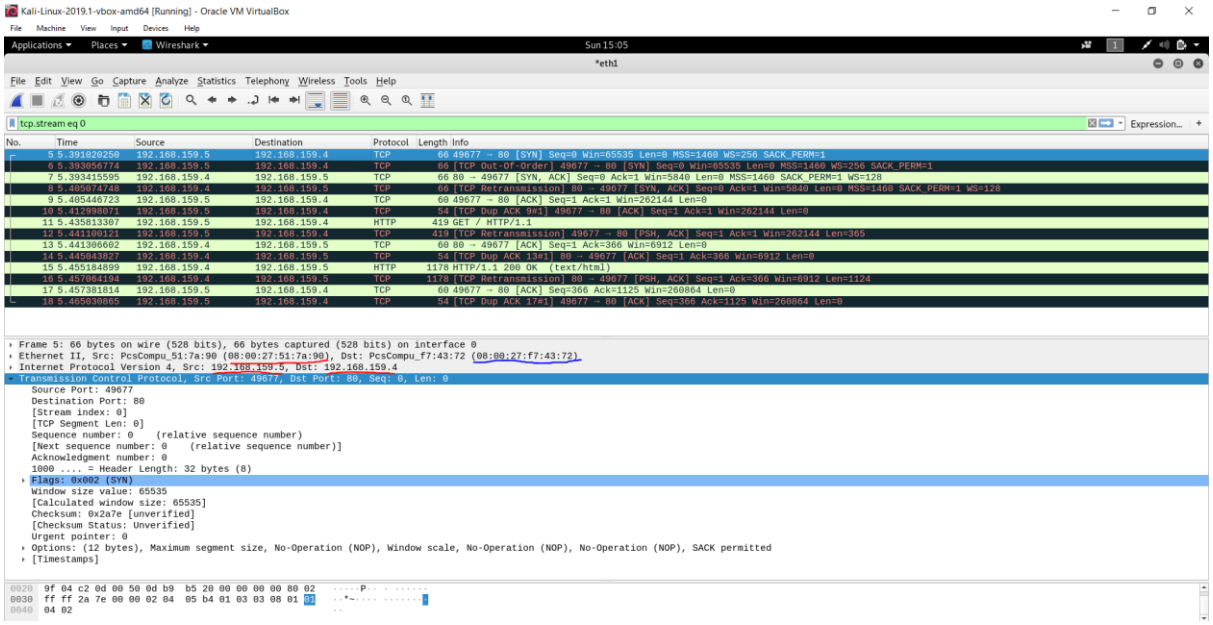
In image 10 and 11 we can see the ICMP request from the windows VM to the host machine. Notice how the traffic is being redirect trough the kali machine, the layer 3 information remains the same (source and destinarion) but layer 2 information changes, in img11 you can see the traffic going from the windows VM to Kali VM and then from Kali VM to host machine. See img 3 to check the addresses.

In images 12 and 13 we can see how the ICMP response is also sent through the Kali machine. So we have perfomr a ma in the middle attack, all traffic between these machines will be seen by the Kali machine, also in the case that the hoist machi act as a default gateway we could see web traffic.

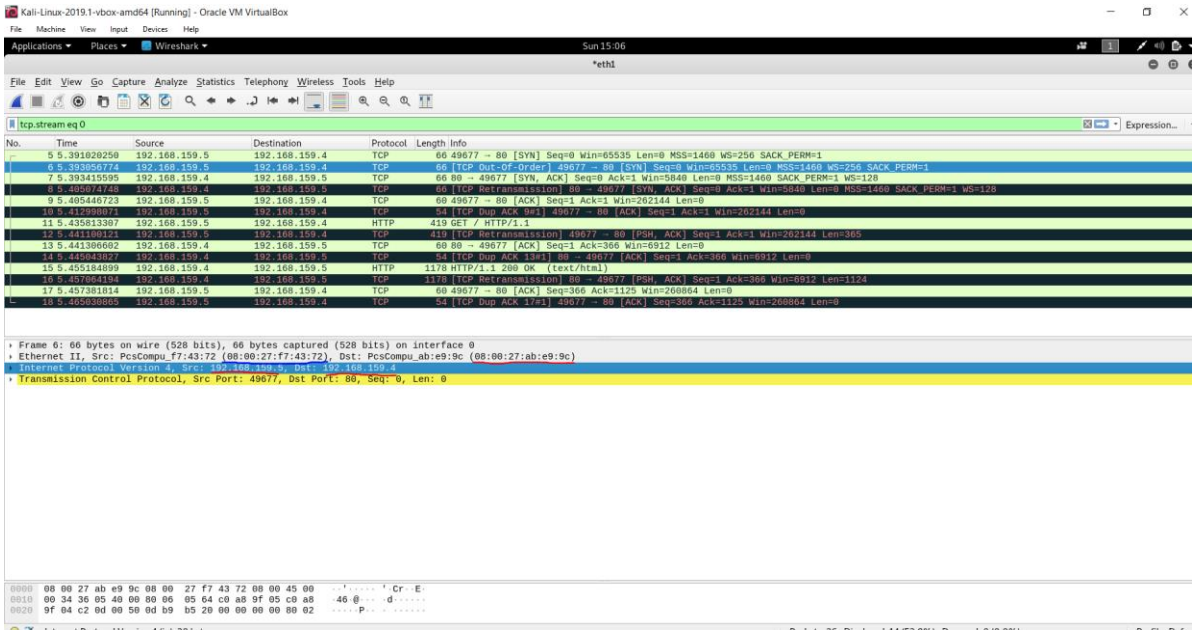
Given that we are also in the middle of the windows VM and the metaspoitable machine we can sniff the traffic and see what is going on between those two.



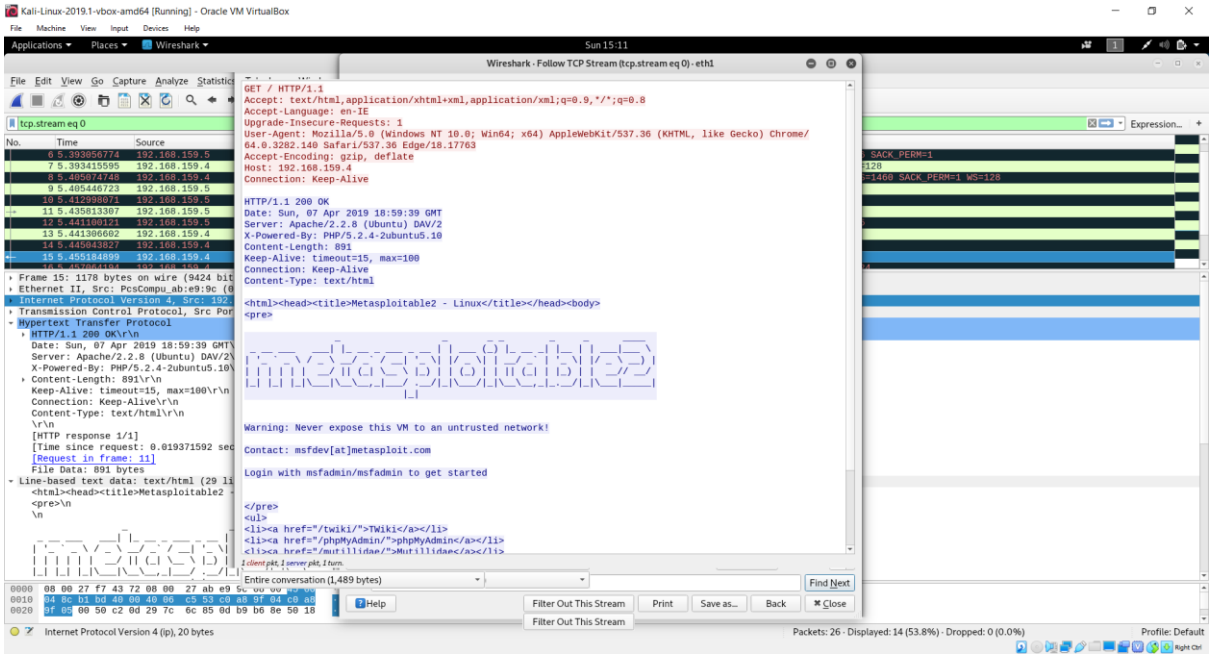
img 14


Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Wireshark Sun 15:05
*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
No. Time Source Destination Protocol Length Info
5 5.391020250 192.168.159.5 192.168.159.4 TCP 66 49677 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
6 5.393056774 192.168.159.5 192.168.159.4 TCP 66 [TCP Out-Of-Order] 49677 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
7 5.393415595 192.168.159.4 192.168.159.5 TCP 66 80 → 49677 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
8 5.405074748 192.168.159.4 192.168.159.5 TCP 66 [TCP Retransmission] 80 → 49677 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
9 5.405446723 192.168.159.5 192.168.159.4 TCP 60 49677 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
10 5.412998071 192.168.159.5 192.168.159.4 TCP 54 [TCP Dup ACK 9#1] 49677 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
11 5.435813307 192.168.159.5 192.168.159.4 HTTP 419 GET / HTTP/1.1
12 5.441100121 192.168.159.5 192.168.159.4 TCP 419 [TCP Retransmission] 49677 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=365
13 5.441306602 192.168.159.4 192.168.159.5 TCP 60 80 → 49677 [ACK] Seq=1 Ack=366 Win=6912 Len=0
14 5.445043027 192.168.159.4 192.168.159.5 TCP 54 [TCP Dup ACK 13#1] 80 → 49677 [ACK] Seq=1 Ack=366 Win=6912 Len=0
15 5.455184899 192.168.159.4 192.168.159.5 HTTP 1178 HTTP/1.1 200 OK (text/html)
16 5.457064194 192.168.159.4 192.168.159.5 TCP 1178 [TCP Retransmission] 80 → 49677 [PSH, ACK] Seq=1 Ack=366 Win=6912 Len=1124
17 5.457381814 192.168.159.5 192.168.159.4 TCP 60 49677 → 80 [ACK] Seq=366 Ack=1125 Win=260864 Len=0
18 5.465030865 192.168.159.5 192.168.159.4 TCP 54 [TCP Dup ACK 17#1] 49677 → 80 [ACK] Seq=366 Ack=1125 Win=260864 Len=0
Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: PcsCompu_51:7a:90 (08:00:27:51:7a:90), Dst: PcsCompu_f7:43:72 (08:00:27:f7:43:72)
Internet Protocol Version 4, Src: 192.168.159.5, Dst: 192.168.159.4
Transmission Control Protocol, Src Port: 49677, Dst Port: 80, Seq: 0, Len: 0
Source Port: 49677
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window size value: 65535
[Calculated window size: 65535]
Checksum: 0x2a7e [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
[Timestamps]
0020 9f 04 c2 0d 00 50 0d b9 b5 20 00 00 00 00 80 02
0030 ff ff 2a 7e 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02

img 15


Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Wireshark Sun 15:06
*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
No. Time Source Destination Protocol Length Info
5 5.391020250 192.168.159.5 192.168.159.4 TCP 66 49677 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
6 5.393056774 192.168.159.5 192.168.159.4 TCP 66 [TCP Out-Of-Order] 49677 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
7 5.393415595 192.168.159.4 192.168.159.5 TCP 66 80 → 49677 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
8 5.405074748 192.168.159.4 192.168.159.5 TCP 66 [TCP Retransmission] 80 → 49677 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
9 5.405446723 192.168.159.5 192.168.159.4 TCP 60 49677 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
10 5.412998071 192.168.159.5 192.168.159.4 TCP 54 [TCP Dup ACK 9#1] 49677 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
11 5.435813307 192.168.159.5 192.168.159.4 HTTP 419 GET / HTTP/1.1
12 5.441100121 192.168.159.5 192.168.159.4 TCP 419 [TCP Retransmission] 49677 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=365
13 5.441306602 192.168.159.4 192.168.159.5 TCP 60 80 → 49677 [ACK] Seq=1 Ack=366 Win=6912 Len=0
14 5.445043027 192.168.159.4 192.168.159.5 TCP 54 [TCP Dup ACK 13#1] 80 → 49677 [ACK] Seq=1 Ack=366 Win=6912 Len=0
15 5.455184899 192.168.159.4 192.168.159.5 HTTP 1178 HTTP/1.1 200 OK (text/html)
16 5.457064194 192.168.159.4 192.168.159.5 TCP 1178 [TCP Retransmission] 80 → 49677 [PSH, ACK] Seq=1 Ack=366 Win=6912 Len=1124
17 5.457381814 192.168.159.5 192.168.159.4 TCP 60 49677 → 80 [ACK] Seq=366 Ack=1125 Win=260864 Len=0
18 5.465030865 192.168.159.5 192.168.159.4 TCP 54 [TCP Dup ACK 17#1] 49677 → 80 [ACK] Seq=366 Ack=1125 Win=260864 Len=0
Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: PcsCompu_f7:43:72 (08:00:27:f7:43:72), Dst: PcsCompu_ab:e9:9c (08:00:27:ab:e9:9c)
Internet Protocol Version 4, Src: 192.168.159.5, Dst: 192.168.159.4
Transmission Control Protocol, Src Port: 49677, Dst Port: 80, Seq: 0, Len: 0
0000 08 00 27 ab e9 9c 08 00 27 f7 43 72 08 00 45 00
0010 00 34 36 05 40 00 80 06 05 64 c0 a8 9f 05 c0 a8
0020 9f 04 c2 0d 00 50 0d b9 b5 20 00 00 00 00 80 02

img 16



img 17

There are some things we can do in order to minimize thye risk of being affected by this kind of attack:

- Avoid connecting to public networks as much as much as you can and if you connect to one then try not to enter any passwords or sensitive data on your device.
- Make sure that the websites you visit use HTTPS (encrypted) and not HTTP (plain text).
- Check your emails senders before clicking on them and avoid any link that looks suspicious even if you who the sender is.
- Beware of pirate content.
- Use tools to protect your system, antivirus, firewalls, etc.
- As a website administrator make sure you implement HSTS (HTTP strict transport security) to avoid protocol downgrade (from HTTPS to HTTP), nake sur to use TLS 1.1 and TLS 1.2.
- As network administrator you can scan your network to search for unsual activities, also you can implement tools as Static ARP if possible or whenever is possible.

As regular users our best line of the defence is to beware of what we do and where we go online, keep your eyes open and stay away from anything that looks suspisious to you and if something is telling you CLICK ME NOW.. please don’t!

References:

"Man in the middle attack using ettercap" University of Trento. Available at: https://securitylab.disi.unitn.it/lib/exe/fetch.php?media=teaching:netsec:2016:g4_-_mitm.pdf

Professor Messer, *Man-in-the-Middle Attacks - CompTIA Security+ SY0-401: 3.2*, YouTube video. Available from: https://www.youtube.com/watch?v=p4pLVN_hVsU

Raphaël Hertzog, Jim O'Gorman, Mati Aharoni. 2017, Kali Linux Revealed, Mastering the Penetration Testing Distribution.

"What is Man-in-the-Middle-Attack?" Comodo Group Inc. Available at: https://securebox.comodo.com/ssl-sniffing/man-in-the-middle-attack/