ASSIGNMENT 2

Network Security

Soheil Shirvani 3720505

Security Victim Machine: TCPDump Commands:

1) # ifconfig

```
ubuntu@ubuntu-vic:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:42:00:6f
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe42:6f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:732 (732.0 B)  TX bytes:8561 (8.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:64 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:4960 (4.9 KB)  TX bytes:4960 (4.9 KB)
```

2) sudo tcpdump -i eth0

```
ubuntu@ubuntu-vic:~$ sudo tcpdump -i eth0
[sudo] password for ubuntu:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
09:31:52.793774 IP ubuntu.mdns > 224.0.0.251.mdns: 0 [2q] PTR (QM)? _ipps._tcp.l
cal. PTR (QM)? _ipp._tcp.local. (45)
09:31:54.623794 IP6 fe80::a00:27ff:fe42:6f.mdns > ff02::fb.mdns: 0 [2q] PTR (QM)
 _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
09:32:23.398680 ARP, Request who-has kali tell ubuntu, length 28
09:32:23.399574 ARP, Reply kali is-at 08:00:27:a1:b6:e6 (oui Unknown), length 46
09:32:23.399587 IP ubuntu > kali: ICMP echo request, id 2537, seq 1, length 64
09:32:23.400365 IP kali > ubuntu: ICMP echo reply, id 2537, seq 1, length 64
09:32:24.400636 IP ubuntu > kali: ICMP echo request, id 2537, seq 2, length 64
09:32:24.401602 IP kali > ubuntu: ICMP echo reply, id 2537, seq 2, length 64
09:32:25.402235 IP ubuntu > kali: ICMP echo request, id 2537, seq 3, length 64
09:32:25.403102 IP kali > ubuntu: ICMP echo reply, id 2537, seq 3, length 64
09:32:26.417841 IP ubuntu > kali: ICMP echo request, id 2537, seq 4, length 64
09:32:26.418636 IP kali > ubuntu: ICMP echo reply, id 2537, seq 4, length 64
09:32:28.629172 ARP, Request who-has ubuntu tell kali, length 46
09:32:28.629187 ARP, Reply ubuntu is-at 08:00:27:42:00:6f (oui Unknown), length
28
```

```
ubuntu@ubuntu-vic:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.71 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.992 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.893 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.819 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3019ms
rtt min/avg/max/mdev = 0.819/1.104/1.712/0.356 ms
```

3) sudo tcpdump -I eth0 -X

```
ubuntu@ubuntu-vic:~$ sudo tcpdump -i eth0 -X
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
09:37:59.202215 IP ubuntu > kali: ICMP echo request, id 2542, seq 1, length 64
        0x0000:  4500 0054 d0f8 4000 4001 e65b c0a8 0103  E..T..@.@..[....
        0x0010:  c0a8 0101 0800 9f31 09ee 0001 b794 f661  .......1.......a
        0x0020:  0000 0000 df15 0300 0000 0000 1011 1213  ................
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............ !"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
09:37:59.202441 IP kali > ubuntu: ICMP echo reply, id 2542, seq 1, length 64
        0x0000:  4500 0054 c199 0000 4001 35bb c0a8 0101  E..T....@.5.....
        0x0010:  c0a8 0103 0000 a731 09ee 0001 b794 f661  .......1.......a
        0x0020:  0000 0000 df15 0300 0000 0000 1011 1213  ................
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............ !"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
09:38:00.201228 IP ubuntu > kali: ICMP echo request, id 2542, seq 2, length 64
        0x0000:  4500 0054 d124 4000 4001 e62f c0a8 0103  E..T.$@.@../....
        0x0010:  c0a8 0101 0800 8334 09ee 0002 b894 f661  .......4.......a
        0x0020:  0000 0000 fa11 0300 0000 0000 1011 1213  ................
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............ !"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

4) sudo tcpdump host 192.169.1.3

```
ubuntu@ubuntu-vic:~$ sudo tcpdump host 192.168.1.3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
09:44:27.760108 IP ubuntu > kali: ICMP echo request, id 2564, seq 1, length 64
09:44:27.760940 IP kali > ubuntu: ICMP echo reply, id 2564, seq 1, length 64
09:44:28.761820 IP ubuntu > kali: ICMP echo request, id 2564, seq 2, length 64
09:44:28.762776 IP kali > ubuntu: ICMP echo reply, id 2564, seq 2, length 64
09:44:29.762231 IP ubuntu > kali: ICMP echo request, id 2564, seq 3, length 64
09:44:29.763223 IP kali > ubuntu: ICMP echo reply, id 2564, seq 3, length 64
09:44:30.763475 IP ubuntu > kali: ICMP echo request, id 2564, seq 4, length 64
09:44:30.764307 IP kali > ubuntu: ICMP echo reply, id 2564, seq 4, length 64
09:44:32.845524 ARP, Request who-has ubuntu tell kali, length 46
09:44:32.845539 ARP, Reply ubuntu is-at 08:00:27:42:00:6f (oui Unknown), length
28
```

5) sudo tcpdump -i eth0 src 192.168.1.3

```
ubuntu@ubuntu-vic:~$ sudo tcpdump -i eth0 src 192.168.1.3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
09:49:37.340672 IP ubuntu > kali: ICMP echo request, id 2570, seq 1, length 64
09:49:38.342439 IP ubuntu > kali: ICMP echo request, id 2570, seq 2, length 64
09:49:39.343870 IP ubuntu > kali: ICMP echo request, id 2570, seq 3, length 64
09:49:40.345537 IP ubuntu > kali: ICMP echo request, id 2570, seq 4, length 64
```

6) sudo tcpdump -i eth0 dst 192.168.1.3

```
ubuntu@ubuntu-vic:~$ sudo tcpdump -i eth0 dst 192.168.1.3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
09:52:20.751284 IP kali > ubuntu: ICMP echo request, id 2508, seq 1, length 64
09:52:21.751798 IP kali > ubuntu: ICMP echo request, id 2508, seq 2, length 64
09:52:22.752966 IP kali > ubuntu: ICMP echo request, id 2508, seq 3, length 64
09:52:23.787120 IP kali > ubuntu: ICMP echo request, id 2508, seq 4, length 64
09:52:24.788756 IP kali > ubuntu: ICMP echo request, id 2508, seq 5, length 64
09:52:25.762814 ARP, Reply kali is-at 08:00:27:a1:b6:e6 (oui Unknown), length 46
09:52:25.929977 ARP, Request who-has ubuntu tell kali, length 46
```

7) sudo tcpdump -i eth0 port 443

```
ubuntu@ubuntu-vic:~$ sudo tcpdump -i eth0 port 443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
10:00:24.935191 IP ubuntu.52948 > kali.https: Flags [S], seq 1251560256, win 292
00, options [mss 1460,sackOK,TS val 483204 ecr 0,nop,wscale 7], length 0
10:00:24.935964 IP kali.https > ubuntu.52948: Flags [R.], seq 0, ack 1251560257,
 win 0, length 0
10:00:38.178684 IP ubuntu.52950 > kali.https: Flags [S], seq 461567147, win 2920
0, options [mss 1460,sackOK,TS val 486514 ecr 0,nop,wscale 7], length 0
10:00:38.179062 IP kali.https > ubuntu.52950: Flags [R.], seq 0, ack 461567148,
win 0, length 0
ubuntu@ubuntu-vic:~$ wget 192.168.1.1:443
--2022-01-30 10:00:24--  http://192.168.1.1:443/
Connecting to 192.168.1.1:443... failed: Connection refused.
ubuntu@ubuntu-vic:~$ wget 192.168.1.1:443
--2022-01-30 10:00:38--  http://192.168.1.1:443/
Connecting to 192.168.1.1:443... failed: Connection refused.
```

8) sudo tcpdump -i eth0 src port 443

```
ubuntu@ubuntu-vic:~$ sudo tcpdump -i eth0 src port 443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
10:04:05.094713 IP kali.https > ubuntu.52952: Flags [R.], seq 0, ack 3744980645,
 win 0, length 0
10:04:11.735860 IP kali.https > ubuntu.52954: Flags [R.], seq 0, ack 3976464896,
 win 0, length 0
10:04:26.974771 IP ubuntu.https > kali.37276: Flags [R.], seq 0, ack 3004139910,
 win 0, length 0
10:04:29.693931 IP ubuntu.https > kali.37278: Flags [R.], seq 0, ack 2580197558,
 win 0, length 0
```

9) sudo tcpdump -i eth0 src port 443

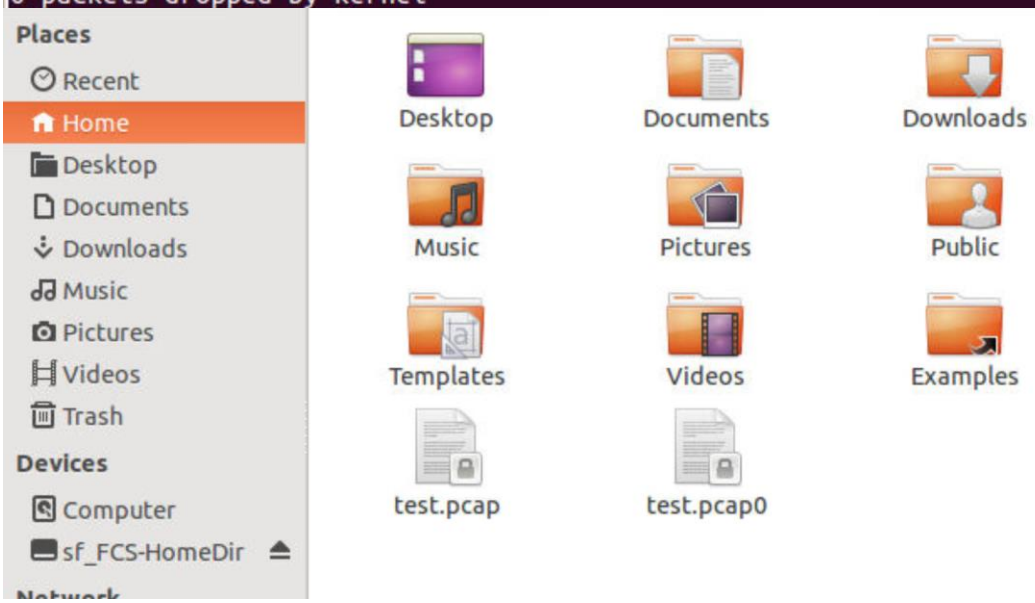
```
ubuntu@ubuntu-vic:~$ wget 192.168.1.1:80
--2022-01-30 10:08:44--  http://192.168.1.1/
Connecting to 192.168.1.1:80... failed: Connection refused.
ubuntu@ubuntu-vic:~$ wget 192.168.1.1:100
--2022-01-30 10:08:48--  http://192.168.1.1:100/
Connecting to 192.168.1.1:100... failed: Connection refused.
ubuntu@ubuntu-vic:~$ wget 192.168.1.1:420
--2022-01-30 10:08:56--  http://192.168.1.1:420/
Connecting to 192.168.1.1:420... failed: Connection refused.
ubuntu@ubuntu-vic:~$ sudo tcpdump -i eth0 portrange 1-443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
10:08:44.697616 IP ubuntu.35940 > kali.http: Flags [S], seq 415683589, win 29200
, options [mss 1460,sackOK,TS val 608145 ecr 0,nop,wscale 7], length 0
10:08:44.698459 IP kali.http > ubuntu.35940: Flags [R.], seq 0, ack 415683590, w
in 0, length 0
10:08:48.528904 IP ubuntu.41476 > kali.100: Flags [S], seq 2042454914, win 29200
, options [mss 1460,sackOK,TS val 609102 ecr 0,nop,wscale 7], length 0
10:08:48.529892 IP kali.100 > ubuntu.41476: Flags [R.], seq 0, ack 2042454915, w
in 0, length 0
10:08:56.417476 IP ubuntu.51134 > kali.420: Flags [S], seq 2914736415, win 29200
, options [mss 1460,sackOK,TS val 611073 ecr 0,nop,wscale 7], length 0
10:08:56.418246 IP kali.420 > ubuntu.51134: Flags [R.], seq 0, ack 2914736416, w
in 0, length 0
```

10) sudo tcpdump -i eth0 -w test.pcap

```
ubuntu@ubuntu-vic:~$ sudo tcpdump -i eth0 -w test.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
```

11) sudo tcpdump -i eth0 -W 2 -C 10 -w test.pcap

```
ubuntu@ubuntu-vic:~$ sudo tcpdump -i eth0 -W 2 -C 10 -w  test.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
^C16 packets captured
16 packets received by filter
0 packets dropped by kernel
```



12) sudo tcpdump -r test.pcap0

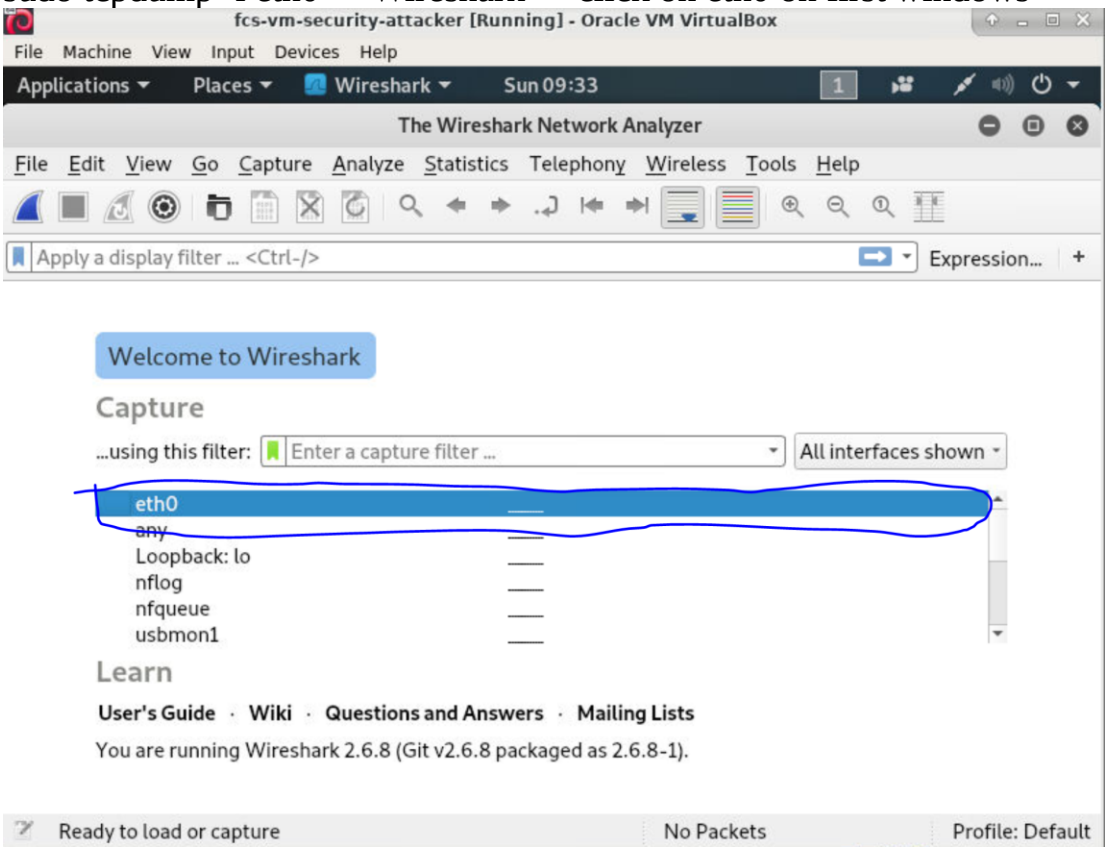
```
ubuntu@ubuntu-vic:~$ sudo tcpdump -r test.pcap0
reading from file test.pcap0, link-type EN10MB (Ethernet)
10:22:47.371475 IP ubuntu.52076 > kali.140: Flags [S], seq 566498725, win 29200,
 options [mss 1460,sackOK,TS val 818812 ecr 0,nop,wscale 7], length 0
10:22:47.372350 IP kali.140 > ubuntu.52076: Flags [R.], seq 0, ack 566498726, wi
n 0, length 0
10:22:47.373409 IP ubuntu.57844 > kali.200: Flags [S], seq 978124257, win 29200,
 options [mss 1460,sackOK,TS val 818814 ecr 0,nop,wscale 7], length 0
10:22:47.374131 IP kali.200 > ubuntu.57844: Flags [R.], seq 0, ack 978124258, wi
n 0, length 0
10:22:52.371221 ARP, Request who-has kali tell ubuntu, length 28
10:22:52.372226 ARP, Reply kali is-at 08:00:27:a1:b6:e6 (oui Unknown), length 46
10:22:52.612092 ARP, Request who-has ubuntu tell kali, length 46
10:22:52.612109 ARP, Reply ubuntu is-at 08:00:27:42:00:6f (oui Unknown), length
28
10:23:03.042864 IP ubuntu > kali: ICMP echo request, id 3318, seq 1, length 64
10:23:03.043616 IP kali > ubuntu: ICMP echo reply, id 3318, seq 1, length 64
10:23:04.044602 IP ubuntu > kali: ICMP echo request, id 3318, seq 2, length 64
10:23:04.045478 IP kali > ubuntu: ICMP echo reply, id 3318, seq 2, length 64
10:23:05.044970 IP ubuntu > kali: ICMP echo request, id 3318, seq 3, length 64
10:23:05.045785 IP kali > ubuntu: ICMP echo reply, id 3318, seq 3, length 64
10:23:06.046008 IP ubuntu > kali: ICMP echo request, id 3318, seq 4, length 64
10:23:06.046970 IP kali > ubuntu: ICMP echo reply, id 3318, seq 4, length 64
```

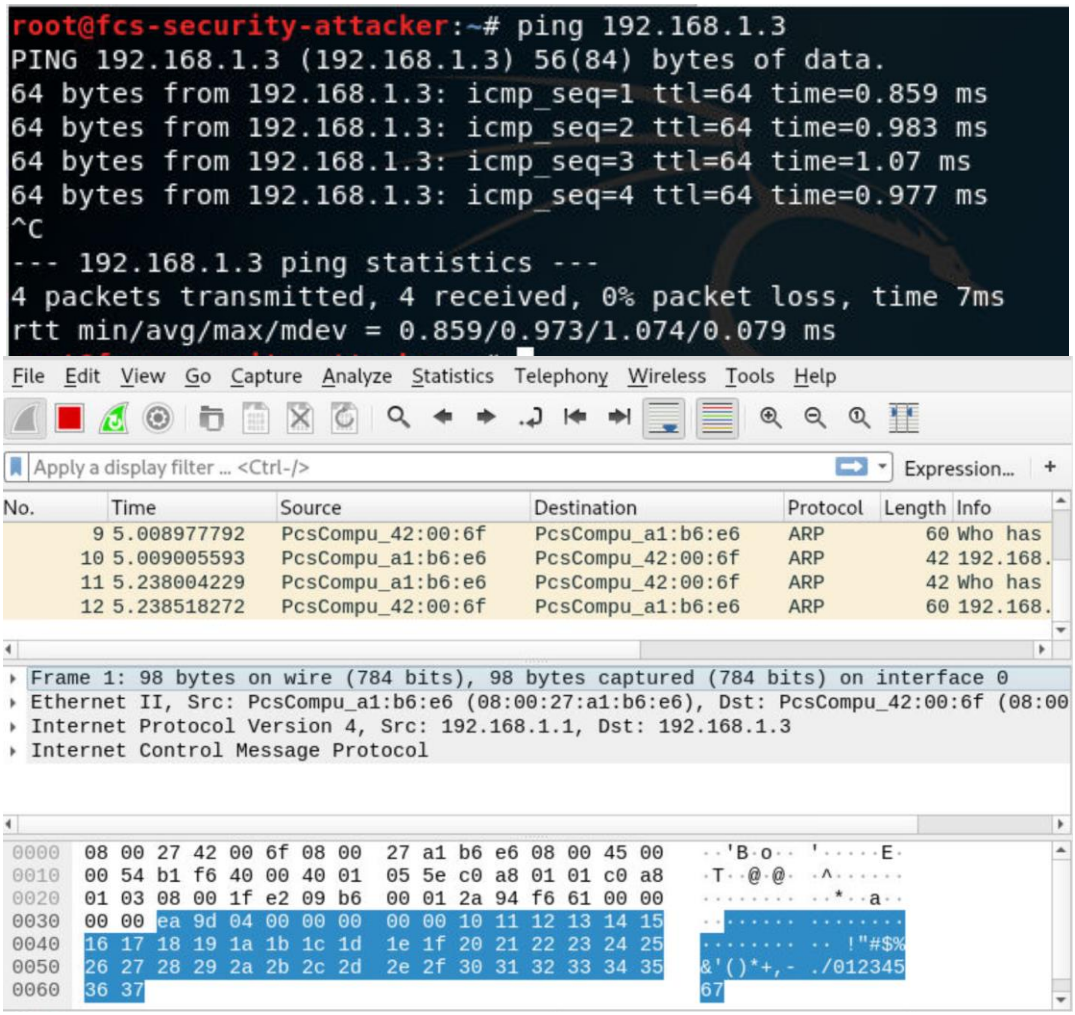
Security Attacker Machine: WireShark Commands:

1) # ifconfig

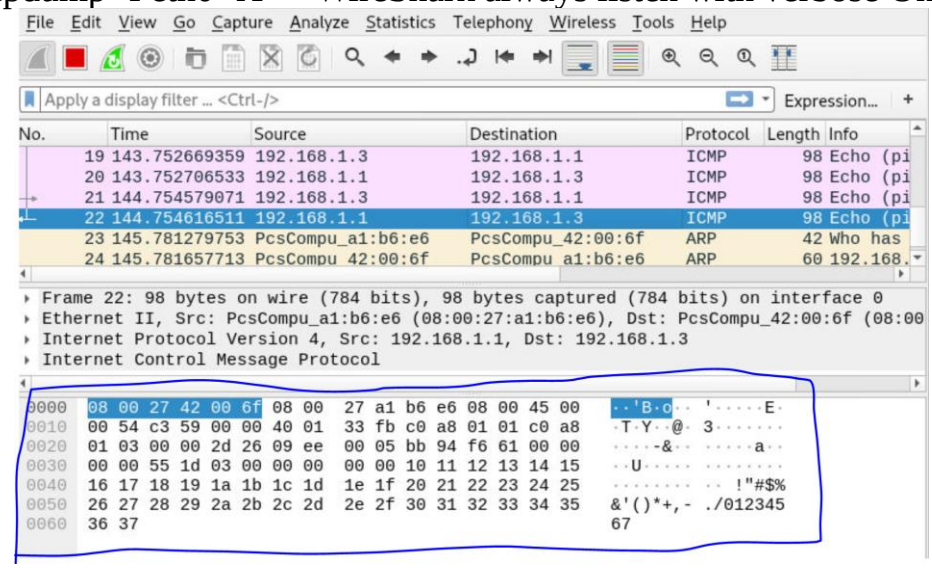
```
root@fcs-security-attacker:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.1  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fea1:b6e6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a1:b6:e6  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 1544 (1.5 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 12  bytes 720 (720.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 720 (720.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2) sudo tcpdump -i eth0 -> Wireshark -> click on eth0 on first windows

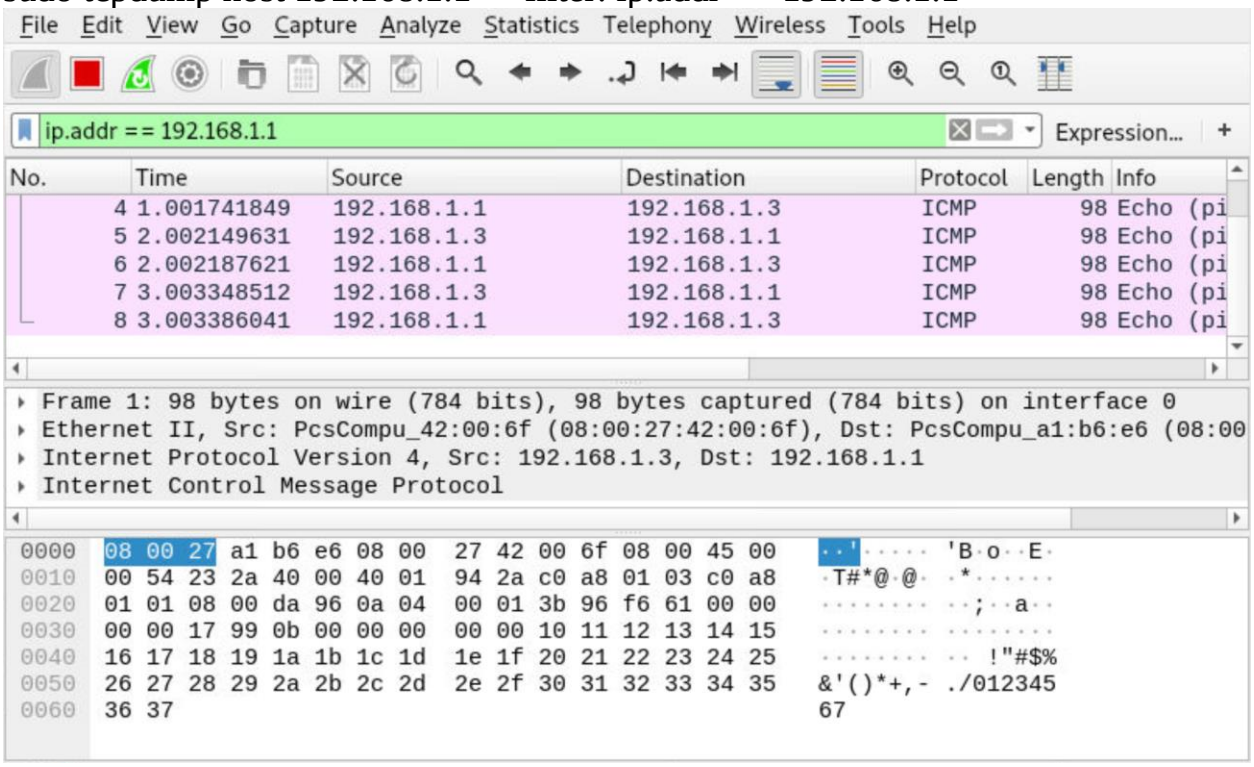




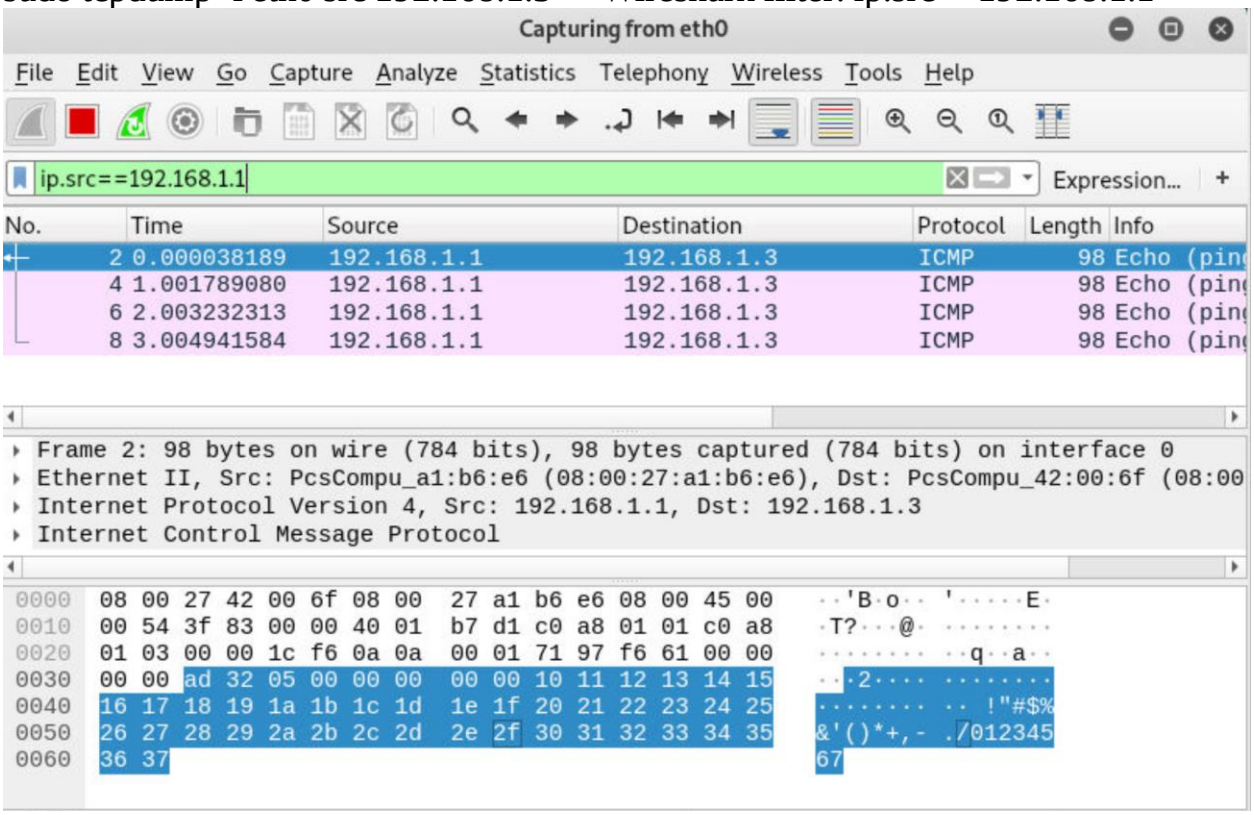
3) sudo tcpdump -I eth0 -X -> WireShark always listen with verbose On



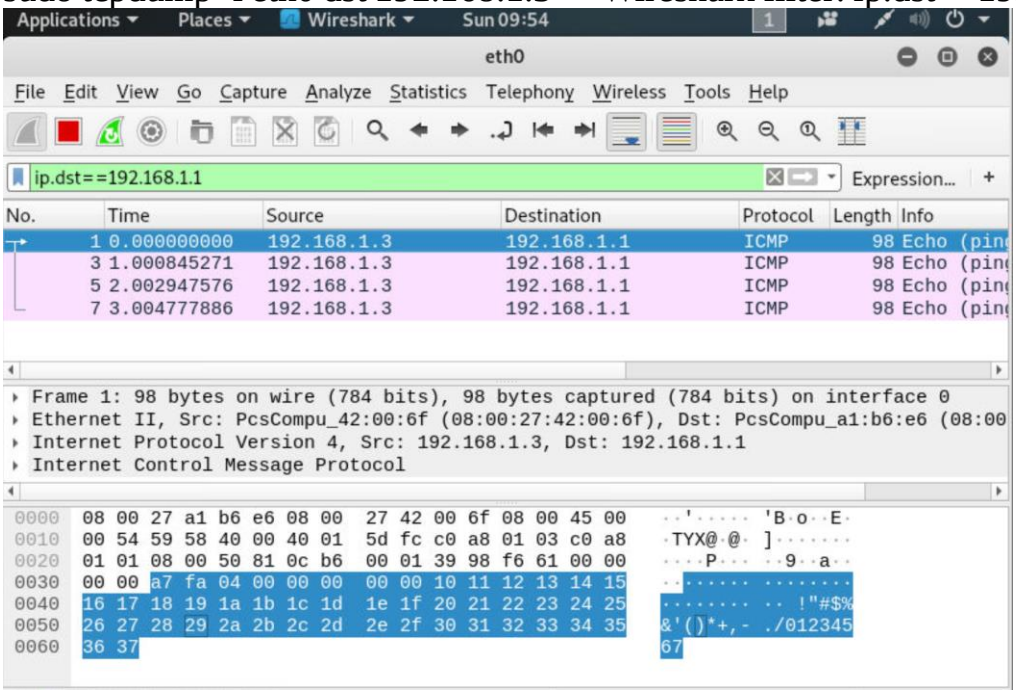
4) sudo tcpdump host 192.168.1.1 -> filter: ip.addr == 192.168.1.1



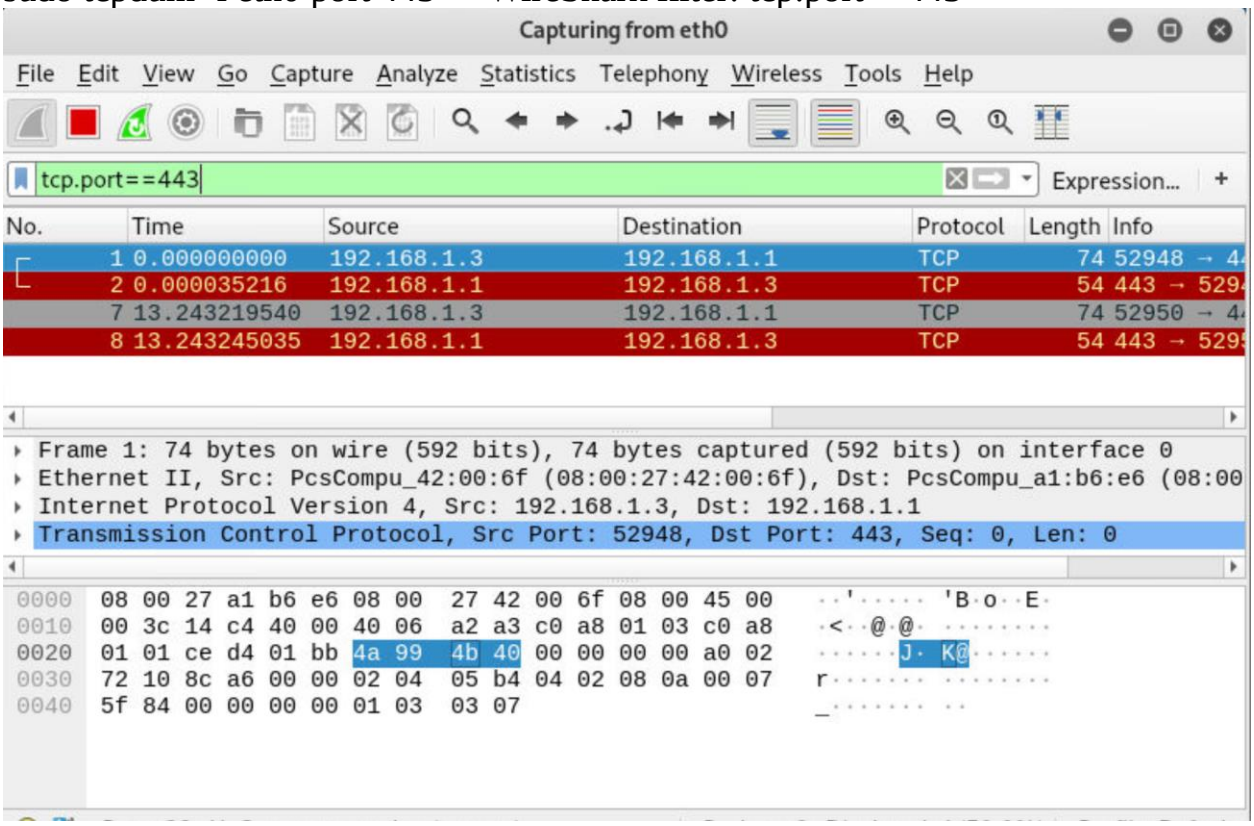
5) sudo tcpdump -i eth0 src 192.168.1.3 -> Wireshark filter: ip.src==192.168.1.1



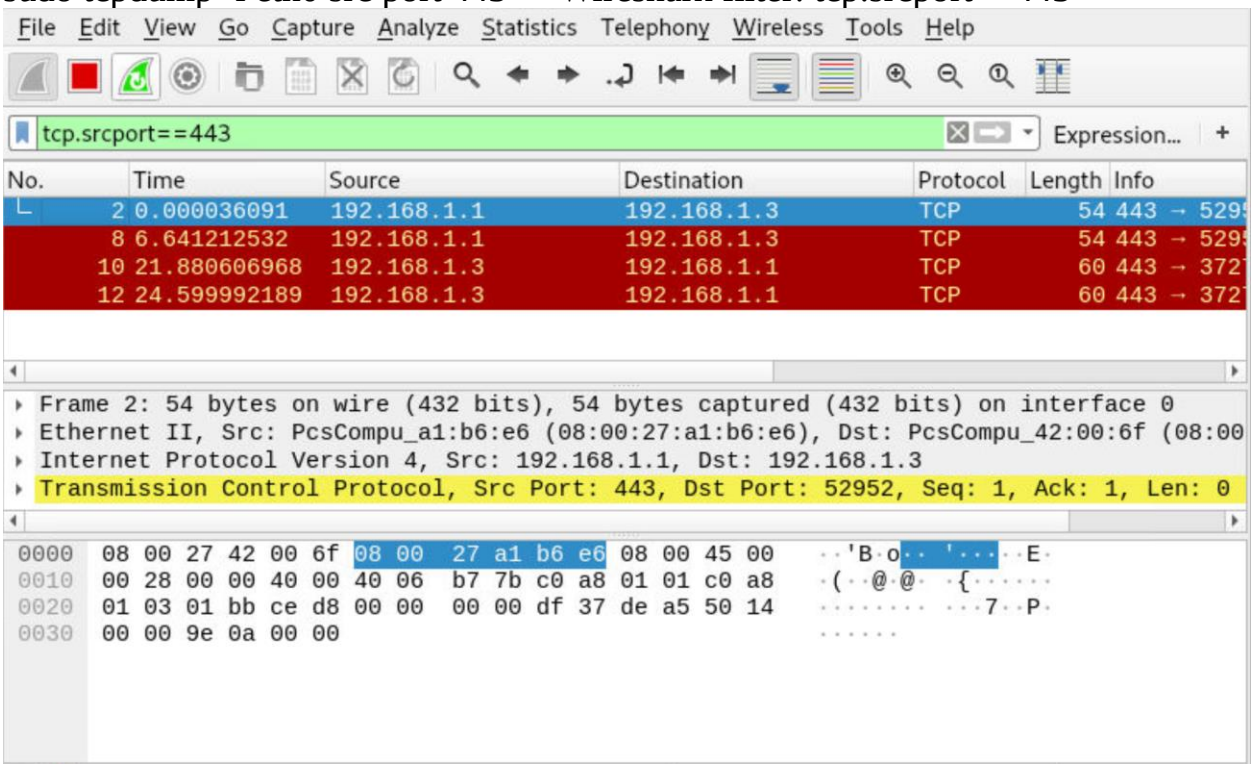
6) sudo tcpdump -i eth0 dst 192.168.1.3 -> Wireshark filter: ip.dst==192.168.1.1



7) sudo tcpdum -i eth0 port 443 -> WireShark filter: tcp.port==443

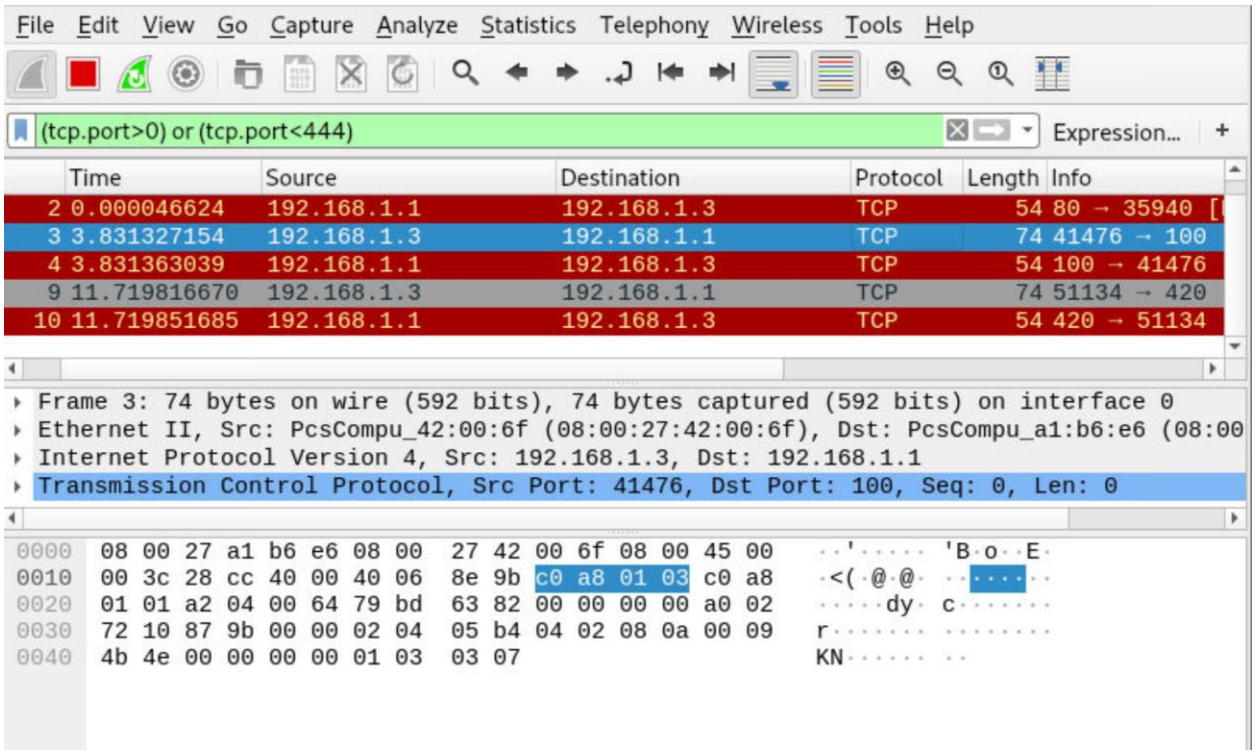


8) sudo tcpdump -i eth0 src port 443 -> Wireshark filter: tcp.srcport==443

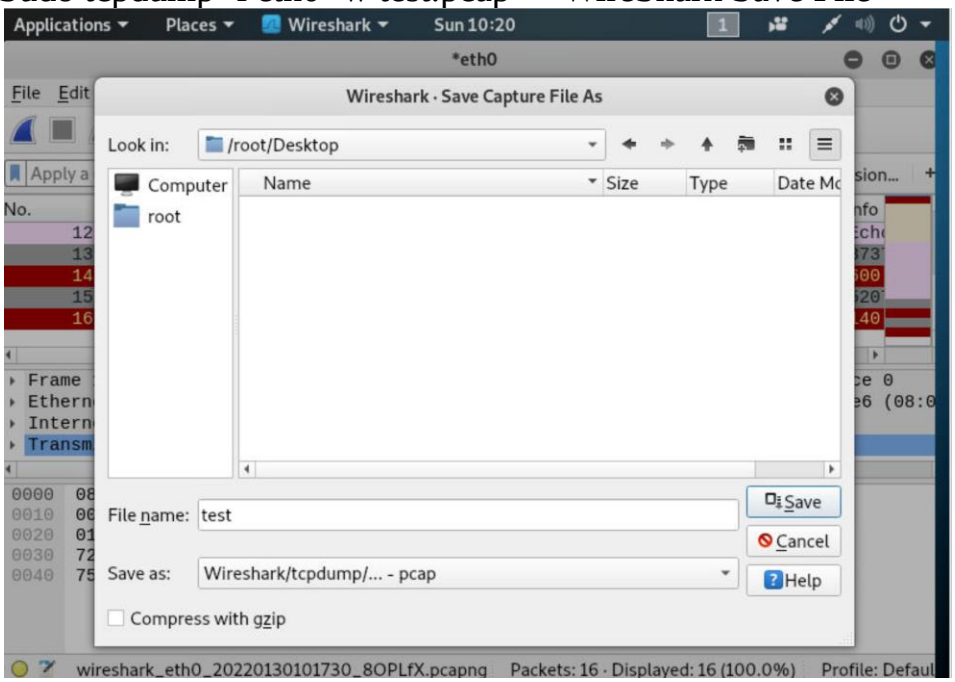


9) sudo tcpdump -i eth0 portrange 1-443

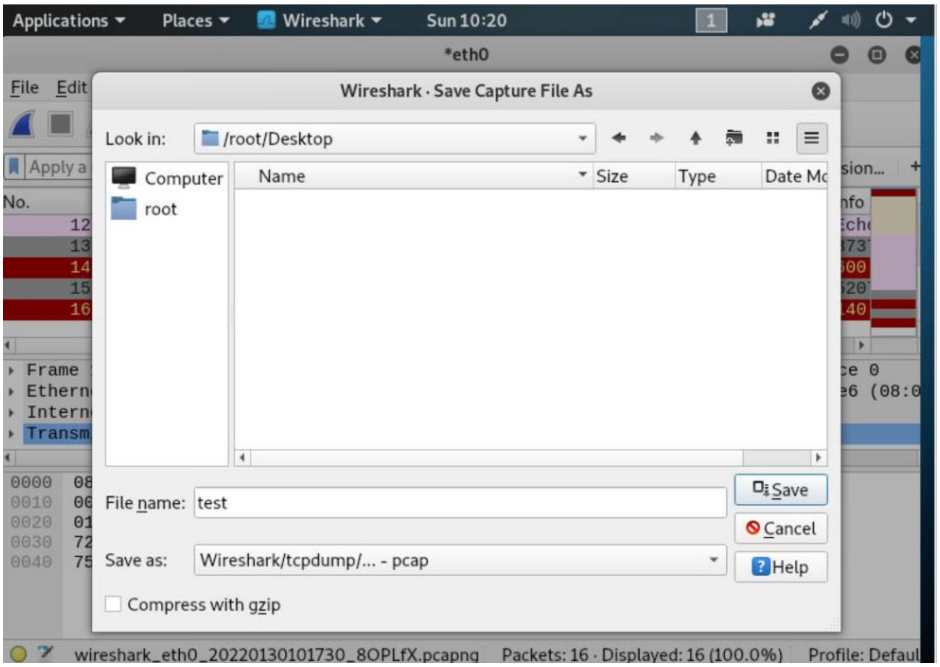
➔ Wireshark filter: (tcp.port > 0) or (tcp.port < 444)



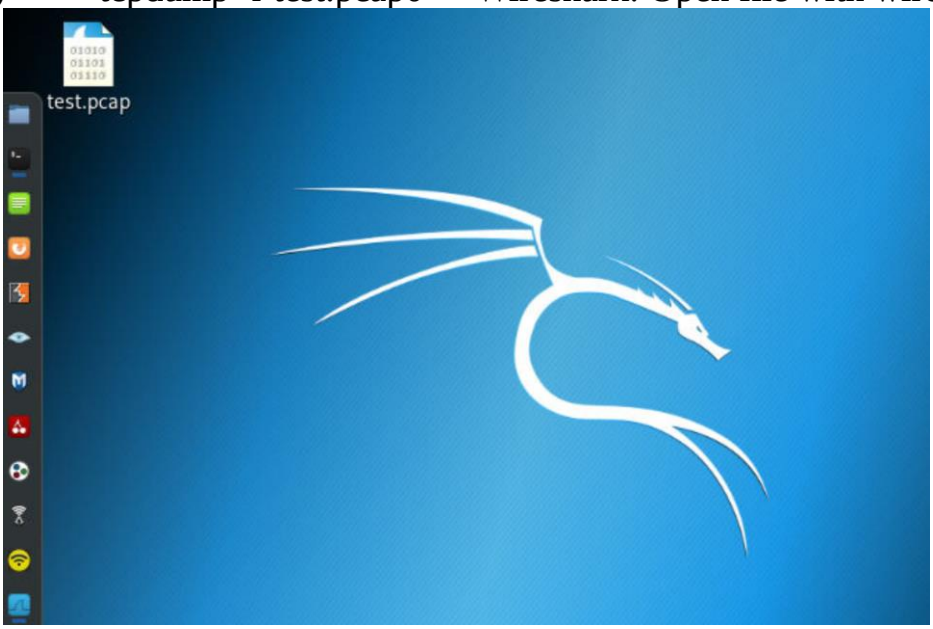
10) Sudo tcpdump -i eth0 -w test.pcap -> WireShark Save File



11) Sudo tcpdump -i eth0 -W 2 -C 10 -w test.pcap
➔ Wireshark save file as (can choose different formats and names)



12) tcpdump -r test.pcap0 -> Wireshark: Open file with wireshark



After Double Clicking on file Wiresharks opens: