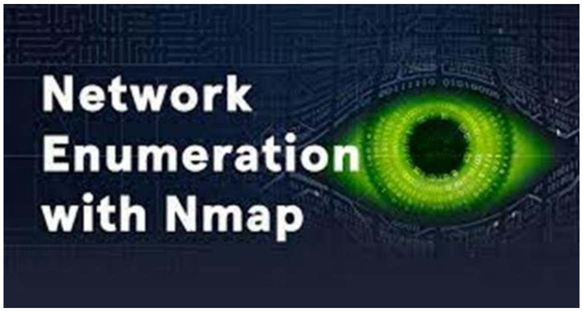
Activity 3
Network Scanning Simulation and Analysis



Using various virtual machines, be able to perform “Network Scanning and Enumeration” for possible target virtualized machines in the network. Also conduct a thorough analysis of a captured network traffic.

Activity Resources

Virtual Machines: Kali Linux, Ubuntu, Metasploitable
Network Traffic Capture: [Activity3]NetCapture_Scenario
Tools: Nmap or ZenMap, Wireshark

Disclaimer: Activity is for educational purpose only! Misuse or targeting other services outside the controlled or virtual environment is punishable by law and the University. The University and the Instructor has no liability on misuse of the tools used in this exercise.

Activity Procedure(s)

Task 1 – Network Scanning and Enumeration Simulation

In your workstation, open/run Oracle VirtualBox Manager and configure virtual machines (Kali Linux, Ubuntu and Metasploitable) network adapter using the following configurations:

Adapter No. 1 Network Configurations

- Enable Network Adapter: YES (checked)
- Attached to: Host-Only Adapter
- Name: Virtual Host-Only Ethernet Adapter (note: choose network that is DHCP server enabled)
- Promiscuous Mode (Advanced): Deny
- Reset MAC Address (press the refresh button)

Run/Start virtual machine simultaneously (make sure all virtual machines are loaded and running). In your Kali Linux virtual machine, run Wireshark and start to capture network packet. Next, be able to perform network scanning and enumeration technique (**nmap -T4 -A -v target-network-range**) using Nmap or ZenMap tool (refer to your course manual as a reference guide). Finally, observe and analyze the captured network traffic in Wireshark.

Task 2 –Network Traffic Examination and Analysis

Open Wireshark and load the network capture file ([Activity3]NetCapture_Scenario). Perform the necessary network investigation of the captured network traffic using various examination techniques (filtering, statistics analysis, and expert information analysis).

Submission Note (Individual Activity)

Use file name convention (LASTNAME_CTAINASL_SECTION_TERM_AY_Activity3.pdf).
Submit/upload Softcopy (PDF file) in MS Teams
Submit a PRINTED activity rubric.

ACTIVITY DOCUMENTATION

Group Name CTRL + Z Wednesday, April 23, 2025

Members Surname, First Name MI. (Alphabetical)

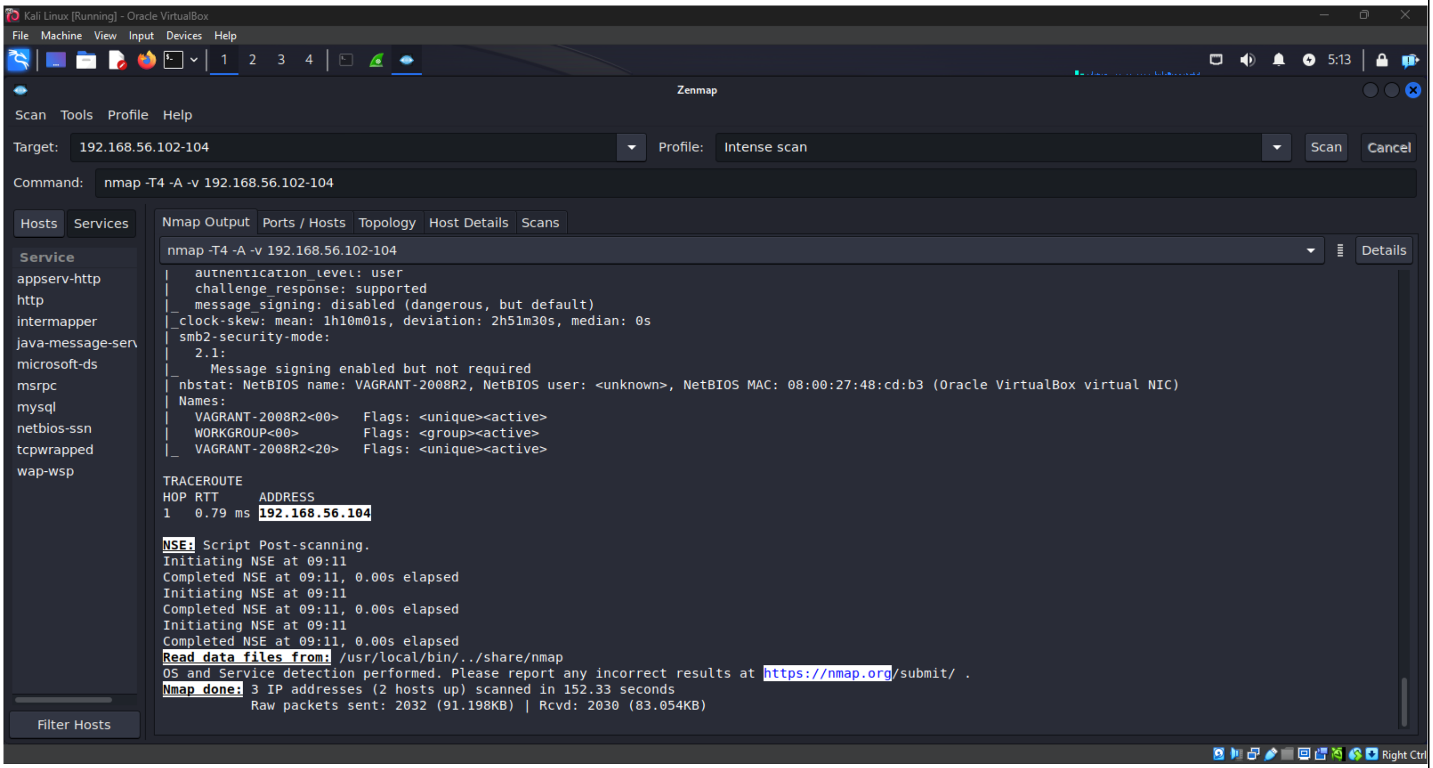
1. Cano, Kaide M.
2. Cuenca, Cyrah Sophia Angella T.
3. Dionela, Terrence A.
4. Umengan, Darwin F.
5. ______

Instruction(s): Provide the appropriate screenshot/screen capture of your workstation.

Network Scanning and Enumeration Simulation

Nmap/ZenMap Report

Display here the result of the Nmap/ZenMap report.



Target: 192.168.56.102-104

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.56.102-104

Service
- appserv-http
- http
- intermapper
- java-message-serv
- microsoft-ds
- msrpc
- mysql
- netbios-ssn
- tcpwrapped
- wap-wsp

nmap -T4 -A -v 192.168.56.102-104

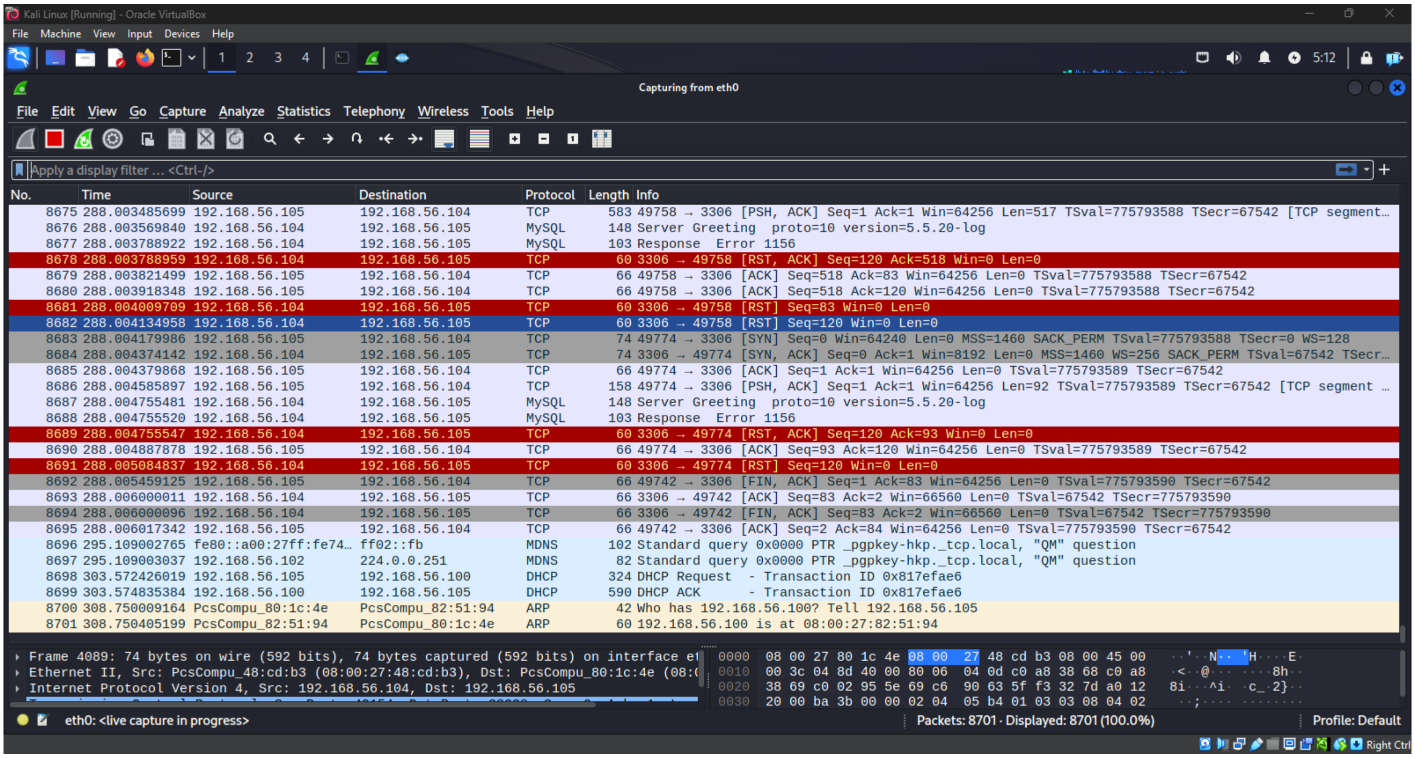
```
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h10m01s, deviation: 2h51m30s, median: 0s
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:48:cd:b3 (Oracle VirtualBox virtual NIC)
| Names:
|   VAGRANT-2008R2<00>   Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  VAGRANT-2008R2<20>   Flags: <unique><active>

TRACEROUTE
HOP RTT     ADDRESS
1   0.79 ms 192.168.56.104

NSE: Script Post-scanning.
Initiating NSE at 09:11
Completed NSE at 09:11, 0.00s elapsed
Initiating NSE at 09:11
Completed NSE at 09:11, 0.00s elapsed
Initiating NSE at 09:11
Completed NSE at 09:11, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 3 IP addresses (2 hosts up) scanned in 152.33 seconds
           Raw packets sent: 2032 (91.198KB) | Rcvd: 2030 (83.054KB)
```

Wireshark Report

Display here the result of the captured network traffic using Wireshark.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
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
8675 288.003485699 192.168.56.105         192.168.56.104  TCP      583 49758 → 3306 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=517 TSval=775793588 TSecr=67542 [TCP segment…
8676 288.003569840 192.168.56.104         192.168.56.105  MySQL    148 Server Greeting  proto=10 version=5.5.20-log
8677 288.003788922 192.168.56.104         192.168.56.105  MySQL    103 Response  Error 1156
8678 288.003788959 192.168.56.104         192.168.56.105  TCP       60 3306 → 49758 [RST, ACK] Seq=120 Ack=518 Win=0 Len=0
8679 288.003821499 192.168.56.105         192.168.56.104  TCP       66 49758 → 3306 [ACK] Seq=518 Ack=83 Win=64256 Len=0 TSval=775793588 TSecr=67542
8680 288.003918348 192.168.56.105         192.168.56.104  TCP       66 49758 → 3306 [ACK] Seq=518 Ack=120 Win=64256 Len=0 TSval=775793588 TSecr=67542
8681 288.004009709 192.168.56.104         192.168.56.105  TCP       60 3306 → 49758 [RST] Seq=83 Win=0 Len=0
8682 288.004134958 192.168.56.104         192.168.56.105  TCP       60 3306 → 49758 [RST] Seq=120 Win=0 Len=0
8683 288.004179986 192.168.56.105         192.168.56.104  TCP       74 49774 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=775793588 TSecr=0 WS=128
8684 288.004374142 192.168.56.104         192.168.56.105  TCP       74 3306 → 49774 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=67542 TSecr…
8685 288.004379868 192.168.56.105         192.168.56.104  TCP       66 49774 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=775793589 TSecr=67542
8686 288.004585897 192.168.56.105         192.168.56.104  TCP      158 49774 → 3306 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=92 TSval=775793589 TSecr=67542 [TCP segment …
8687 288.004755481 192.168.56.104         192.168.56.105  MySQL    148 Server Greeting  proto=10 version=5.5.20-log
8688 288.004755520 192.168.56.104         192.168.56.105  MySQL    103 Response  Error 1156
8689 288.004755547 192.168.56.104         192.168.56.105  TCP       60 3306 → 49774 [RST, ACK] Seq=120 Ack=93 Win=0 Len=0
8690 288.004887878 192.168.56.105         192.168.56.104  TCP       66 49774 → 3306 [ACK] Seq=93 Ack=120 Win=64256 Len=0 TSval=775793589 TSecr=67542
8691 288.005084837 192.168.56.104         192.168.56.105  TCP       60 3306 → 49774 [RST] Seq=120 Win=0 Len=0
8692 288.005459125 192.168.56.105         192.168.56.104  TCP       66 49742 → 3306 [FIN, ACK] Seq=1 Ack=83 Win=64256 Len=0 TSval=775793590 TSecr=67542
8693 288.006000011 192.168.56.104         192.168.56.105  TCP       66 3306 → 49742 [ACK] Seq=83 Ack=2 Win=66560 Len=0 TSval=67542 TSecr=775793590
8694 288.006000096 192.168.56.104         192.168.56.105  TCP       66 3306 → 49742 [FIN, ACK] Seq=83 Ack=2 Win=66560 Len=0 TSval=67542 TSecr=775793590
8695 288.006017342 192.168.56.105         192.168.56.104  TCP       66 49742 → 3306 [ACK] Seq=2 Ack=84 Win=64256 Len=0 TSval=775793590 TSecr=67542
8696 295.109002765 fe80::a00:27ff:fe74…  ff02::fb        MDNS     102 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
8697 295.109003037 192.168.56.102         224.0.0.251     MDNS      82 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
8698 303.572426019 192.168.56.105         192.168.56.100  DHCP     324 DHCP Request  - Transaction ID 0x817efae6
8699 303.574835384 192.168.56.100         192.168.56.105  DHCP     590 DHCP ACK      - Transaction ID 0x817efae6
8700 308.750009164 PcsCompu_80:1c:4e      PcsCompu_82:51:94 ARP      42 Who has 192.168.56.100? Tell 192.168.56.105
8701 308.750405199 PcsCompu_82:51:94      PcsCompu_80:1c:4e ARP      60 192.168.56.100 is at 08:00:27:82:51:94
```

```
› Frame 4089: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface et
› Ethernet II, Src: PcsCompu_48:cd:b3 (08:00:27:48:cd:b3), Dst: PcsCompu_80:1c:4e (08:(
› Internet Protocol Version 4, Src: 192.168.56.104, Dst: 192.168.56.105

0000  08 00 27 80 1c 4e 08 00  27 48 cd b3 08 00 45 00   ··'··N·· 'H····E·
0010  00 3c 04 8d 40 00 80 06  04 0d c0 a8 38 68 c0 a8   ·<··@··· ····8h··
0020  38 69 c0 02 95 5e 69 c6  90 63 5f f3 32 7d a0 12   8i···^i· ·c_·2}··
0030  20 00 ba 3b 00 00 02 04  05 b4 01 03 03 08 04 02    ··;···· ········
```

eth0: <live capture in progress>
Packets: 8701 · Displayed: 8701 (100.0%)
Profile: Default
Right Ctrl

Q1. What is/are the IP Address of the target machine(s) in the network? [Hint: Except machines in ignored states]

[Answer Format: IP Address, …, IP Address]
Answer: 192.168.56.105

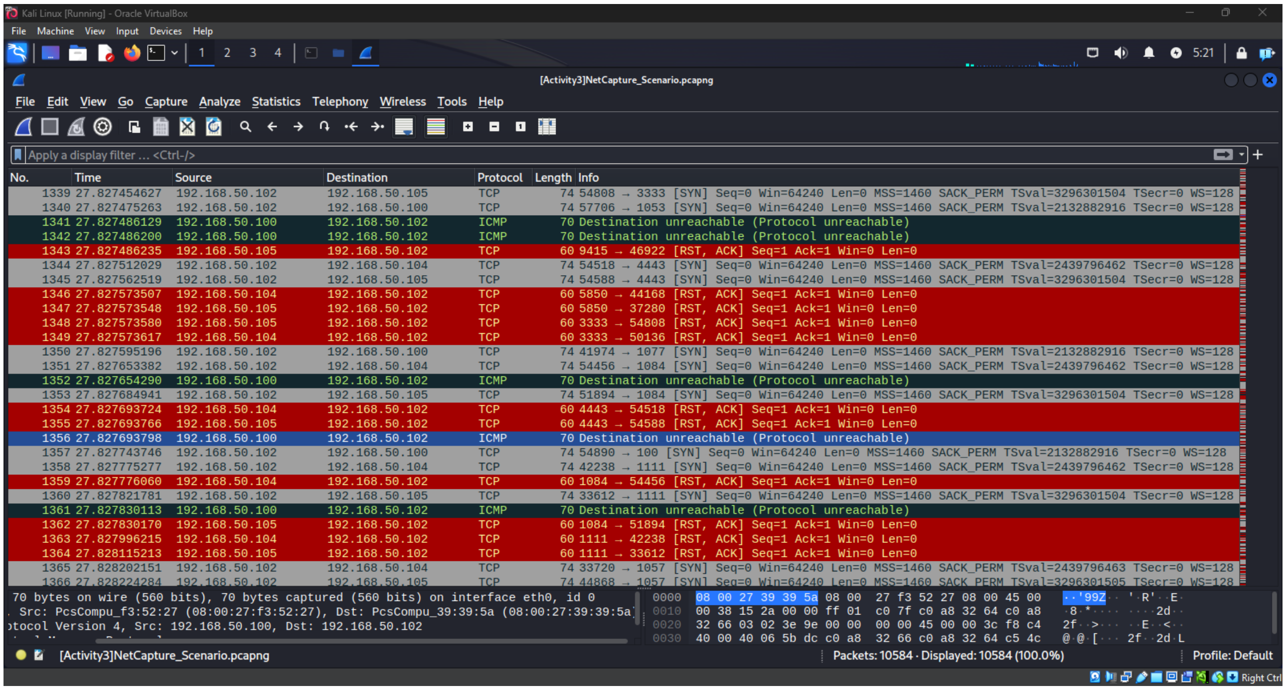
Q2. What is/are the scanned available OPEN Ports of the target machine(s)? Identify which port is related to hosting web services (bold, italic). [Hint: Except machines in ignored states]

[Answer Format: IP Address: List Ports, …, IP Address: List Ports]
Answer: 192.168.56.104: 80/TCP, 135/TCP, 139/TCP, 445/TCP, 3000/TCP, 3306/TCP, 3989/TCP, 4848/TCP, 7676/TCP, 8080/TCP, 8181/TCP, 8383/TCP, 9200/TCP, 49152/TCP, 49153/TCP, 49154/TCP

Network Traffic Examination and Analysis

Wireshark Capture

Display here the Wireshark capture file.



Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
5:21
[Activity3]NetCapture_Scenario.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Right Ctrl

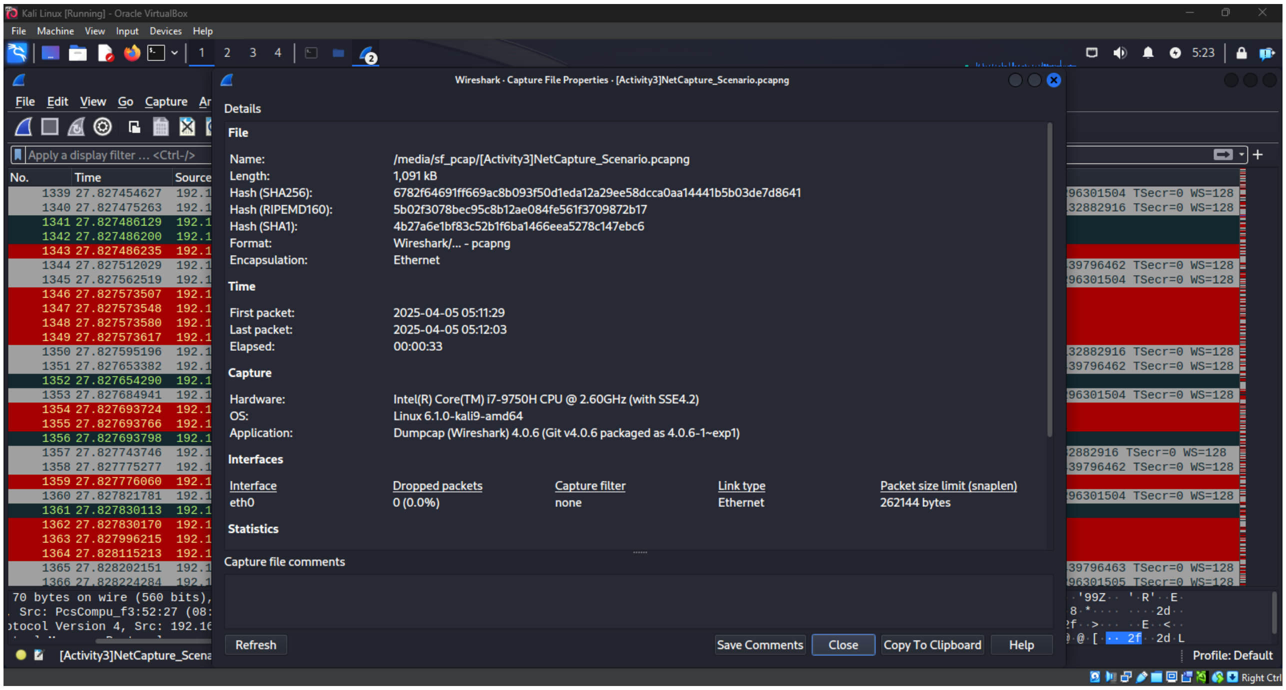
```
No.   Time        Source          Destination     Protocol Length Info
 1339 27.827454627 192.168.50.102 192.168.50.105  TCP      74 54808 → 3333 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3296301504 TSecr=0 WS=128
 1340 27.827475263 192.168.50.102 192.168.50.100  TCP      74 57706 → 1053 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2132882916 TSecr=0 WS=128
 1341 27.827486129 192.168.50.100 192.168.50.102  ICMP     70 Destination unreachable (Protocol unreachable)
 1342 27.827486200 192.168.50.100 192.168.50.102  ICMP     70 Destination unreachable (Protocol unreachable)
 1343 27.827486235 192.168.50.105 192.168.50.102  TCP      60 9415 → 46922 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1344 27.827512029 192.168.50.102 192.168.50.104  TCP      74 54518 → 4443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2439796462 TSecr=0 WS=128
 1345 27.827562519 192.168.50.102 192.168.50.105  TCP      74 54588 → 4443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3296301504 TSecr=0 WS=128
 1346 27.827573507 192.168.50.104 192.168.50.102  TCP      60 5850 → 44168 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1347 27.827573548 192.168.50.105 192.168.50.102  TCP      60 5850 → 37280 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1348 27.827573580 192.168.50.105 192.168.50.102  TCP      60 3333 → 54808 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1349 27.827573617 192.168.50.104 192.168.50.102  TCP      60 3333 → 50136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1350 27.827595196 192.168.50.102 192.168.50.100  TCP      74 41974 → 1077 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2132882916 TSecr=0 WS=128
 1351 27.827653382 192.168.50.102 192.168.50.104  TCP      74 54456 → 1084 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2439796462 TSecr=0 WS=128
 1352 27.827654290 192.168.50.100 192.168.50.102  ICMP     70 Destination unreachable (Protocol unreachable)
 1353 27.827684941 192.168.50.102 192.168.50.105  TCP      74 51894 → 1084 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3296301504 TSecr=0 WS=128
 1354 27.827693724 192.168.50.104 192.168.50.102  TCP      60 4443 → 54518 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1355 27.827693766 192.168.50.105 192.168.50.102  TCP      60 4443 → 54588 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1356 27.827693798 192.168.50.100 192.168.50.102  ICMP     70 Destination unreachable (Protocol unreachable)
 1357 27.827743746 192.168.50.102 192.168.50.100  TCP      74 54890 → 100 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2132882916 TSecr=0 WS=128
 1358 27.827775277 192.168.50.102 192.168.50.104  TCP      74 42238 → 1111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2439796462 TSecr=0 WS=128
 1359 27.827776060 192.168.50.104 192.168.50.102  TCP      60 1084 → 54456 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1360 27.827821781 192.168.50.102 192.168.50.105  TCP      74 33612 → 1111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3296301504 TSecr=0 WS=128
 1361 27.827830113 192.168.50.100 192.168.50.102  ICMP     70 Destination unreachable (Protocol unreachable)
 1362 27.827830170 192.168.50.105 192.168.50.102  TCP      60 1084 → 51894 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1363 27.827996215 192.168.50.104 192.168.50.102  TCP      60 1111 → 42238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1364 27.828115213 192.168.50.105 192.168.50.102  TCP      60 1111 → 33612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1365 27.828202151 192.168.50.102 192.168.50.104  TCP      74 33720 → 1057 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2439796463 TSecr=0 WS=128
 1366 27.828224284 192.168.50.102 192.168.50.105  TCP      74 44868 → 1057 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3296301505 TSecr=0 WS=128
```

```
70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface eth0, id 0
. Src: PcsCompu_f3:52:27 (08:00:27:f3:52:27), Dst: PcsCompu_39:39:5a (08:00:27:39:39:5a
otocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.102
```

```
0000  08 00 27 39 39 5a 08 00  27 f3 52 27 08 00 45 00   ··'99Z·· '·R'··E·
0010  00 38 15 2a 00 00 ff 01  c0 7f c0 a8 32 64 c0 a8   ·8·*···· ····2d··
0020  32 66 03 02 3e 9e 00 00  00 00 45 00 00 3c f8 c4   2f··>··· ··E··<··
0030  40 00 40 06 5b dc c0 a8  32 66 c0 a8 32 64 c5 4c   @·@·[··· 2f··2d·L
```

[Activity3]NetCapture_Scenario.pcapng | Packets: 10584 · Displayed: 10584 (100.0%) | Profile: Default

Display here the Wireshark capture file properties information.



Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
5:23
Wireshark · Capture File Properties · [Activity3]NetCapture_Scenario.pcapng
Refresh
Save Comments
Close
Copy To Clipboard
Help
Profile: Default
Right Ctrl

Details

File

Name: /media/sf_pcap/[Activity3]NetCapture_Scenario.pcapng
Length: 1,091 kB
Hash (SHA256): 6782f64691ff669ac8b093f50d1eda12a29ee58dcca0aa14441b5b03de7d8641
Hash (RIPEMD160): 5b02f3078bec95c8b12ae084fe561f3709872b17
Hash (SHA1): 4b27a6e1bf83c52b1f6ba1466eea5278c147ebc6
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2025-04-05 05:11:29
Last packet: 2025-04-05 05:12:03
Elapsed: 00:00:33

Capture

Hardware: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (with SSE4.2)
OS: Linux 6.1.0-kali9-amd64
Application: Dumpcap (Wireshark) 4.0.6 (Git v4.0.6 packaged as 4.0.6-1~exp1)

Interfaces

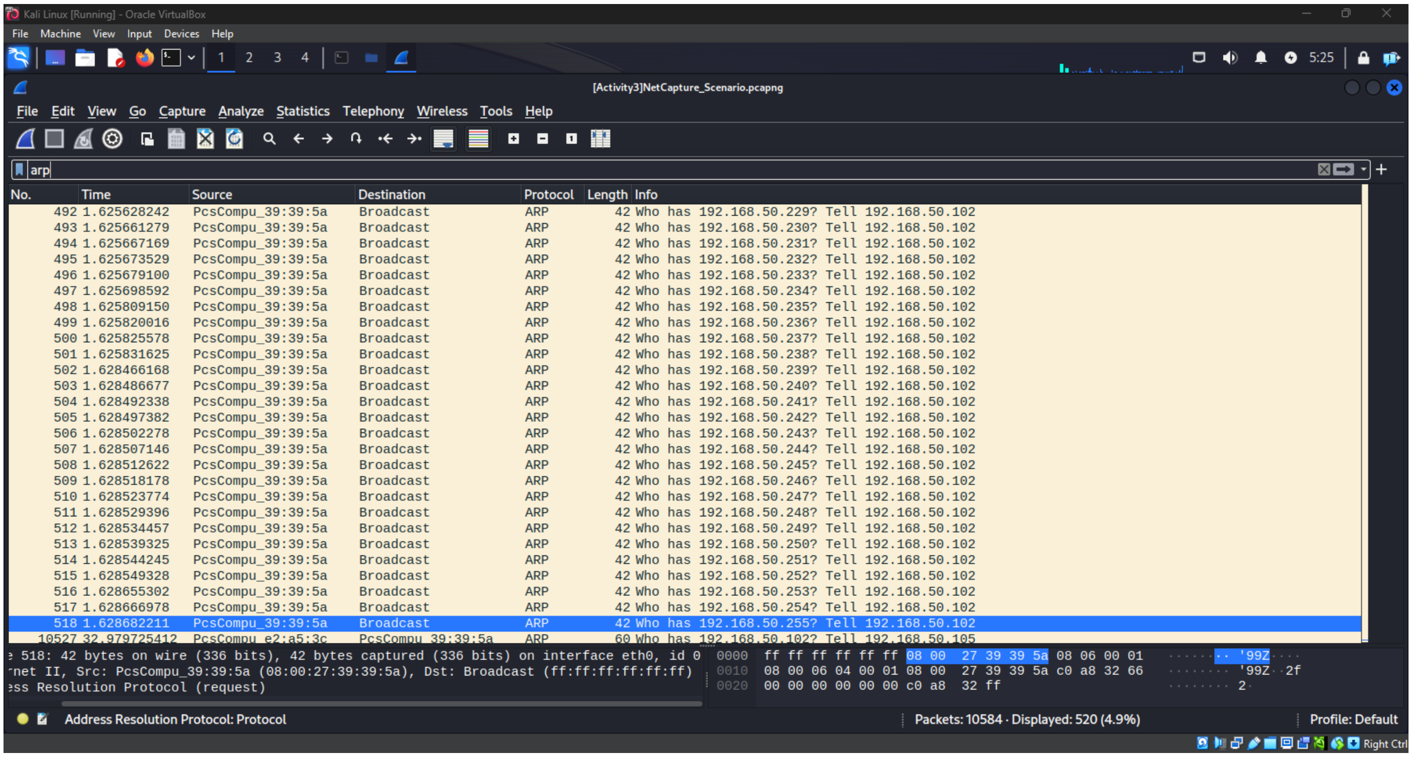
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
eth0	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Capture file comments

Wireshark Filtering

Display here the result of the Wireshark capture using filter command **ARP**.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
5:25
[Activity3]NetCapture_Scenario.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Right Ctrl

```
arp
```

```
No.    Time          Source               Destination          Protocol Length Info
  492 1.625628242   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.229? Tell 192.168.50.102
  493 1.625661279   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.230? Tell 192.168.50.102
  494 1.625667169   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.231? Tell 192.168.50.102
  495 1.625673529   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.232? Tell 192.168.50.102
  496 1.625679100   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.233? Tell 192.168.50.102
  497 1.625698592   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.234? Tell 192.168.50.102
  498 1.625809150   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.235? Tell 192.168.50.102
  499 1.625820016   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.236? Tell 192.168.50.102
  500 1.625825578   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.237? Tell 192.168.50.102
  501 1.625831625   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.238? Tell 192.168.50.102
  502 1.628466168   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.239? Tell 192.168.50.102
  503 1.628486677   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.240? Tell 192.168.50.102
  504 1.628492338   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.241? Tell 192.168.50.102
  505 1.628497382   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.242? Tell 192.168.50.102
  506 1.628502278   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.243? Tell 192.168.50.102
  507 1.628507146   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.244? Tell 192.168.50.102
  508 1.628512622   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.245? Tell 192.168.50.102
  509 1.628518178   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.246? Tell 192.168.50.102
  510 1.628523774   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.247? Tell 192.168.50.102
  511 1.628529396   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.248? Tell 192.168.50.102
  512 1.628534457   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.249? Tell 192.168.50.102
  513 1.628539325   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.250? Tell 192.168.50.102
  514 1.628544245   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.251? Tell 192.168.50.102
  515 1.628549328   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.252? Tell 192.168.50.102
  516 1.628655302   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.253? Tell 192.168.50.102
  517 1.628666978   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.254? Tell 192.168.50.102
  518 1.628682211   PcsCompu_39:39:5a    Broadcast            ARP        42 Who has 192.168.50.255? Tell 192.168.50.102
10527 32.979725412  PcsCompu_e2:a5:3c    PcsCompu_39:39:5a    ARP        60 Who has 192.168.50.102? Tell 192.168.50.105
```

```
e 518: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
rnet II, Src: PcsCompu_39:39:5a (08:00:27:39:39:5a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
ess Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 08 00  27 39 39 5a 08 06 00 01   ········ '99Z····
0010  08 00 06 04 00 01 08 00  27 39 39 5a c0 a8 32 66   ········ '99Z··2f
0020  00 00 00 00 00 00 c0 a8  32 ff                     ········ 2·
```

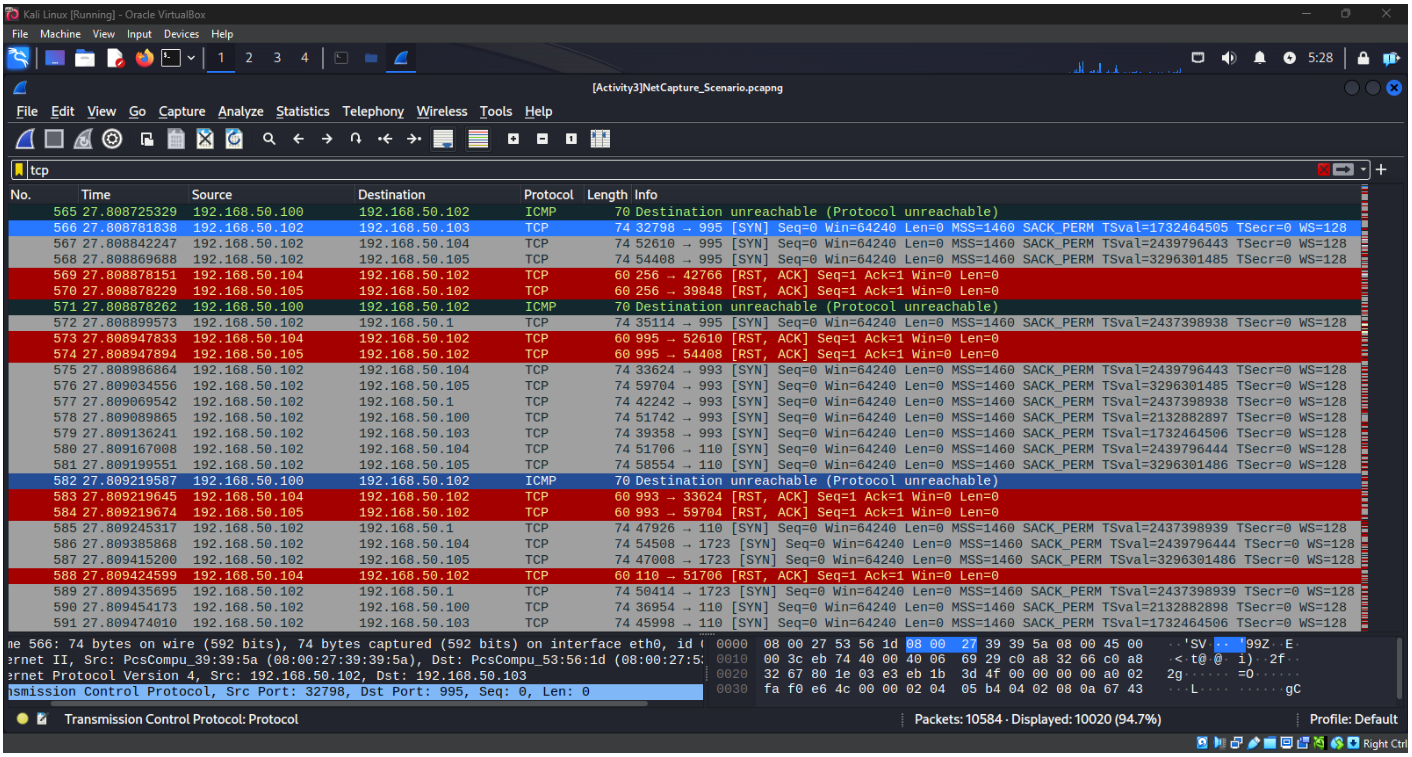
Address Resolution Protocol: Protocol | Packets: 10584 · Displayed: 520 (4.9%) | Profile: Default

Observation and Findings: What does the filter result suggests? Explain!

The filter shows repeated ARP requesrtts with no replies, which means one computer is trying and failing to find another device on the network. This could mean the other device is offlice, disconnected, or there is a network issue.

Wireshark Filtering

Display here the result of the Wireshark capture using filter command for **TCP Connect() Scan**.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
5:28
[Activity3]NetCapture_Scenario.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Right Ctrl

tcp

```
No.   Time         Source          Destination     Protocol Length Info
  565 27.808725329 192.168.50.100  192.168.50.102  ICMP       70 Destination unreachable (Protocol unreachable)
  566 27.808781838 192.168.50.102  192.168.50.103  TCP        74 32798 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1732464505 TSecr=0 WS=128
  567 27.808842247 192.168.50.102  192.168.50.104  TCP        74 52610 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2439796443 TSecr=0 WS=128
  568 27.808869688 192.168.50.102  192.168.50.105  TCP        74 54408 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3296301485 TSecr=0 WS=128
  569 27.808878151 192.168.50.104  192.168.50.102  TCP        60 256 → 42766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  570 27.808878229 192.168.50.105  192.168.50.102  TCP        60 256 → 39848 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  571 27.808878262 192.168.50.100  192.168.50.102  ICMP       70 Destination unreachable (Protocol unreachable)
  572 27.808899573 192.168.50.102  192.168.50.1    TCP        74 35114 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2437398938 TSecr=0 WS=128
  573 27.808947833 192.168.50.104  192.168.50.102  TCP        60 995 → 52610 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  574 27.808947894 192.168.50.105  192.168.50.102  TCP        60 995 → 54408 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  575 27.808986864 192.168.50.102  192.168.50.104  TCP        74 33624 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2439796443 TSecr=0 WS=128
  576 27.809034556 192.168.50.102  192.168.50.105  TCP        74 59704 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3296301485 TSecr=0 WS=128
  577 27.809069542 192.168.50.102  192.168.50.1    TCP        74 42242 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2437398938 TSecr=0 WS=128
  578 27.809089865 192.168.50.102  192.168.50.100  TCP        74 51742 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2132882897 TSecr=0 WS=128
  579 27.809136241 192.168.50.102  192.168.50.103  TCP        74 39358 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1732464506 TSecr=0 WS=128
  580 27.809167008 192.168.50.102  192.168.50.104  TCP        74 51706 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2439796444 TSecr=0 WS=128
  581 27.809199551 192.168.50.102  192.168.50.105  TCP        74 58554 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3296301486 TSecr=0 WS=128
  582 27.809219587 192.168.50.100  192.168.50.102  ICMP       70 Destination unreachable (Protocol unreachable)
  583 27.809219645 192.168.50.104  192.168.50.102  TCP        60 993 → 33624 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  584 27.809219674 192.168.50.105  192.168.50.102  TCP        60 993 → 59704 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  585 27.809245317 192.168.50.102  192.168.50.1    TCP        74 47926 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2437398939 TSecr=0 WS=128
  586 27.809385868 192.168.50.102  192.168.50.104  TCP        74 54508 → 1723 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2439796444 TSecr=0 WS=128
  587 27.809415200 192.168.50.102  192.168.50.105  TCP        74 47008 → 1723 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3296301486 TSecr=0 WS=128
  588 27.809424599 192.168.50.104  192.168.50.102  TCP        60 110 → 51706 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  589 27.809435695 192.168.50.102  192.168.50.1    TCP        74 50414 → 1723 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2437398939 TSecr=0 WS=128
  590 27.809454173 192.168.50.102  192.168.50.100  TCP        74 36954 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2132882898 TSecr=0 WS=128
  591 27.809474010 192.168.50.102  192.168.50.103  TCP        74 45998 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1732464506 TSecr=0 WS=128
```

```
me 566: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id (
ernet II, Src: PcsCompu_39:39:5a (08:00:27:39:39:5a), Dst: PcsCompu_53:56:1d (08:00:27:5:
ernet Protocol Version 4, Src: 192.168.50.102, Dst: 192.168.50.103
nsmission Control Protocol, Src Port: 32798, Dst Port: 995, Seq: 0, Len: 0
```

```
0000  08 00 27 53 56 1d 08 00  27 39 39 5a 08 00 45 00   ··'SV···'99Z··E·
0010  00 3c eb 74 40 00 40 06  69 29 c0 a8 32 66 c0 a8   ·<·t@·@· i)··2f··
0020  32 67 80 1e 03 e3 eb 1b  3d 4f 00 00 00 00 a0 02   2g······ =O······
0030  fa f0 e6 4c 00 00 02 04  05 b4 04 02 08 0a 67 43   ···L···· ······gC
```

Transmission Control Protocol: Protocol

Packets: 10584 · Displayed: 10020 (94.7%)

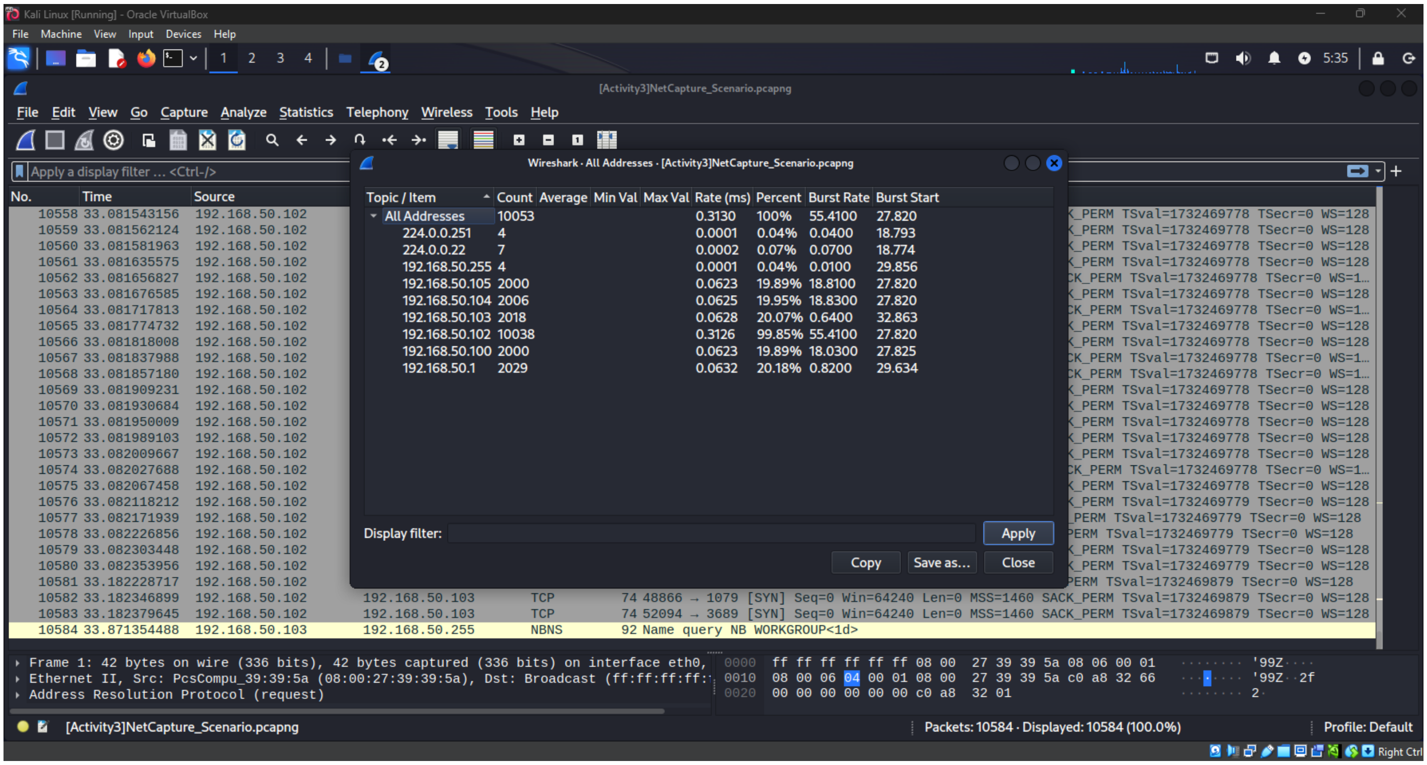
Profile: Default

Observation and Findings: What does the filter result suggests? Explain!

The filter shows the result of a TCP Connect() scan. IT reveals multiple connection attempts (SYN packets) from one device to different ports on another device. Some ports respond with SYN-ACK, which means that the port is open, and others respond with RST, which means that the port is closed. This suggests that a port scaninng activity is happening, likely to find which ports are open the target machine.

Wireshark Statistics (IPv4 Conversations)

Display here the statistics summary report.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
5:35
[Activity3]NetCapture_Scenario.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Wireshark · All Addresses · [Activity3]NetCapture_Scenario.pcapng
Display filter:
Apply
Copy
Save as…
Close
Right Ctrl

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
All Addresses	10053				0.3130	100%	55.4100	27.820
224.0.0.251	4				0.0001	0.04%	0.0400	18.793
224.0.0.22	7				0.0002	0.07%	0.0700	18.774
192.168.50.255	4				0.0001	0.04%	0.0100	29.856
192.168.50.105	2000				0.0623	19.89%	18.8100	27.820
192.168.50.104	2006				0.0625	19.95%	18.8300	27.820
192.168.50.103	2018				0.0628	20.07%	0.6400	32.863
192.168.50.102	10038				0.3126	99.85%	55.4100	27.820
192.168.50.100	2000				0.0623	19.89%	18.0300	27.825
192.168.50.1	2029				0.0632	20.18%	0.8200	29.634

```
No.   Time         Source
10558 33.081543156 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10559 33.081562124 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10560 33.081581963 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10561 33.081635575 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10562 33.081656827 192.168.50.102          CK_PERM TSval=1732469778 TSecr=0 WS=1…
10563 33.081676585 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10564 33.081717813 192.168.50.102          CK_PERM TSval=1732469778 TSecr=0 WS=1…
10565 33.081774732 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10566 33.081818008 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10567 33.081837988 192.168.50.102          CK_PERM TSval=1732469778 TSecr=0 WS=1…
10568 33.081857180 192.168.50.102          CK_PERM TSval=1732469778 TSecr=0 WS=1…
10569 33.081909231 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10570 33.081930684 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10571 33.081950009 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10572 33.081989103 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10573 33.082009667 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10574 33.082027688 192.168.50.102          CK_PERM TSval=1732469778 TSecr=0 WS=1…
10575 33.082067458 192.168.50.102          K_PERM TSval=1732469778 TSecr=0 WS=128
10576 33.082118212 192.168.50.102          K_PERM TSval=1732469779 TSecr=0 WS=128
10577 33.082171939 192.168.50.102           _PERM TSval=1732469779 TSecr=0 WS=128
10578 33.082226856 192.168.50.102          PERM TSval=1732469779 TSecr=0 WS=128
10579 33.082303448 192.168.50.102          K_PERM TSval=1732469779 TSecr=0 WS=128
10580 33.082353956 192.168.50.102          K_PERM TSval=1732469779 TSecr=0 WS=128
10581 33.182228717 192.168.50.102          PERM TSval=1732469879 TSecr=0 WS=128
10582 33.182346899 192.168.50.102  192.168.50.103  TCP   74 48866 → 1079 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1732469879 TSecr=0 WS=128
10583 33.182379645 192.168.50.102  192.168.50.103  TCP   74 52094 → 3689 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1732469879 TSecr=0 WS=128
10584 33.871354488 192.168.50.103  192.168.50.255  NBNS  92 Name query NB WORKGROUP<1d>
```

```
› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0,
› Ethernet II, Src: PcsCompu_39:39:5a (08:00:27:39:39:5a), Dst: Broadcast (ff:ff:ff:ff:
› Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 08 00  27 39 39 5a 08 06 00 01   ········ '99Z····
0010  08 00 06 04 00 01 08 00  27 39 39 5a c0 a8 32 66   ········ '99Z··2f
0020  00 00 00 00 00 00 c0 a8  32 01                     ········ 2·
```

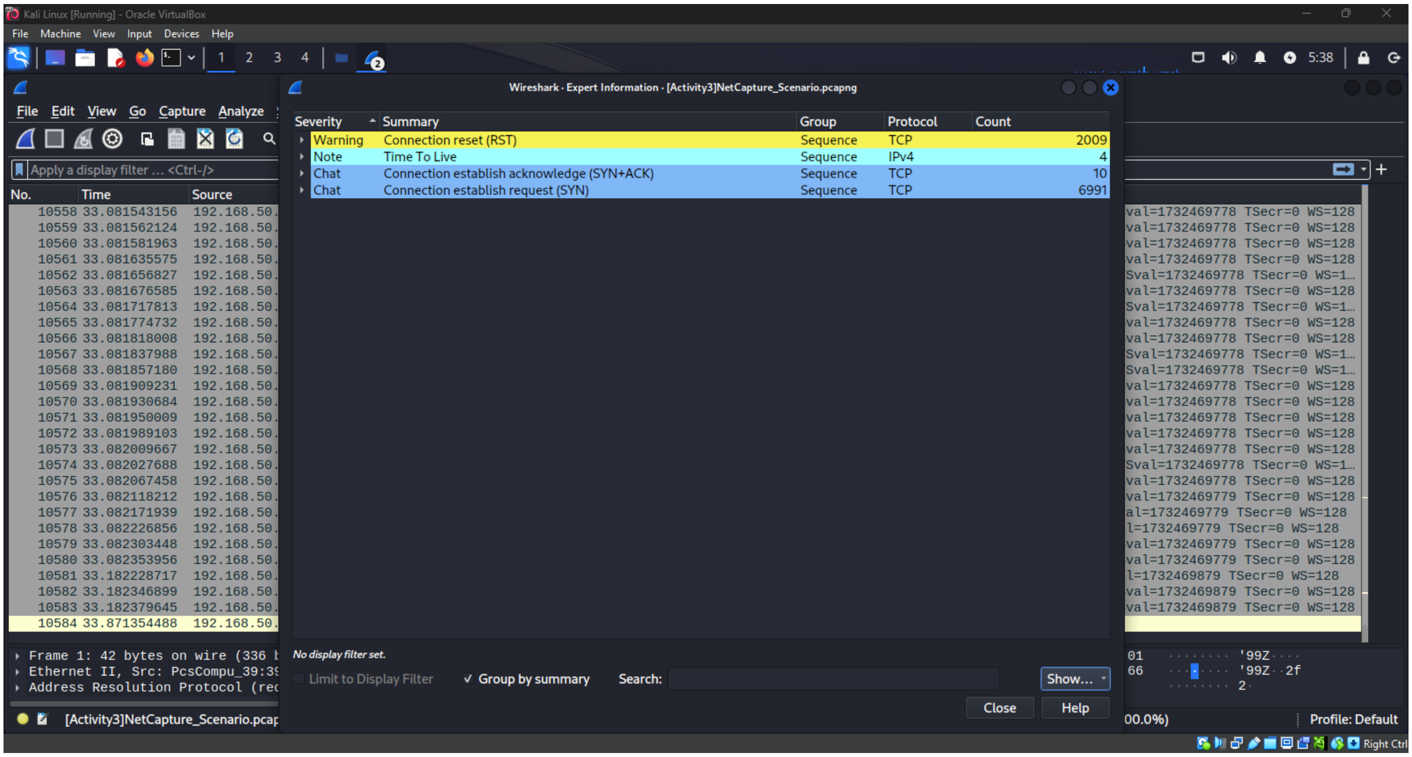
```
[Activity3]NetCapture_Scenario.pcapng    Packets: 10584 · Displayed: 10584 (100.0%)    Profile: Default
```

Observation and Findings: What does the statistics result suggests? Explain!

THe statistics suggest that a device is actively communicating with other devices on the network in a normal way, possibly showing data or using services. The network is not overloaded and does not have a sign of attack or heavy traffic.

Wireshark Expert Information

Display here the Expert Information summary report.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
5:38
File Edit View Go Capture Analyze
Wireshark · Expert Information · [Activity3]NetCapture_Scenario.pcapng
Show...
Close
Help
Right Ctrl

Apply a display filter … <Ctrl-/>

Severity	Summary	Group	Protocol	Count
Warning	Connection reset (RST)	Sequence	TCP	2009
Note	Time To Live	Sequence	IPv4	4
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	10
Chat	Connection establish request (SYN)	Sequence	TCP	6991

No display filter set.

☐ Limit to Display Filter ✓ Group by summary Search:

```
No.   Time         Source
10558 33.081543156 192.168.50.
10559 33.081562124 192.168.50.
10560 33.081581963 192.168.50.
10561 33.081635575 192.168.50.
10562 33.081656827 192.168.50.
10563 33.081676585 192.168.50.
10564 33.081717813 192.168.50.
10565 33.081774732 192.168.50.
10566 33.081818008 192.168.50.
10567 33.081837988 192.168.50.
10568 33.081857180 192.168.50.
10569 33.081909231 192.168.50.
10570 33.081930684 192.168.50.
10571 33.081950009 192.168.50.
10572 33.081989103 192.168.50.
10573 33.082009667 192.168.50.
10574 33.082027688 192.168.50.
10575 33.082067458 192.168.50.
10576 33.082118212 192.168.50.
10577 33.082171939 192.168.50.
10578 33.082226856 192.168.50.
10579 33.082303448 192.168.50.
10580 33.082353956 192.168.50.
10581 33.182228717 192.168.50.
10582 33.182346899 192.168.50.
10583 33.182379645 192.168.50.
10584 33.871354488 192.168.50.
```

```
val=1732469778 TSecr=0 WS=128
val=1732469778 TSecr=0 WS=128
val=1732469778 TSecr=0 WS=128
val=1732469778 TSecr=0 WS=128
Sval=1732469778 TSecr=0 WS=1…
val=1732469778 TSecr=0 WS=128
Sval=1732469778 TSecr=0 WS=1…
val=1732469778 TSecr=0 WS=128
val=1732469778 TSecr=0 WS=128
Sval=1732469778 TSecr=0 WS=1…
Sval=1732469778 TSecr=0 WS=1…
val=1732469778 TSecr=0 WS=128
val=1732469778 TSecr=0 WS=128
val=1732469778 TSecr=0 WS=128
val=1732469778 TSecr=0 WS=128
val=1732469778 TSecr=0 WS=128
Sval=1732469778 TSecr=0 WS=1…
val=1732469778 TSecr=0 WS=128
val=1732469779 TSecr=0 WS=128
al=1732469779 TSecr=0 WS=128
l=1732469779 TSecr=0 WS=128
val=1732469779 TSecr=0 WS=128
val=1732469779 TSecr=0 WS=128
l=1732469879 TSecr=0 WS=128
val=1732469879 TSecr=0 WS=128
val=1732469879 TSecr=0 WS=128
```

```
› Frame 1: 42 bytes on wire (336 b
› Ethernet II, Src: PcsCompu_39:39
› Address Resolution Protocol (req
```

```
01   ·········  '99Z····
66   ···▪·····  '99Z··2f
     ·········  2·
```

[Activity3]NetCapture_Scenario.pcap 00.0%) Profile: Default

Observation and Findings: What does the expert information result suggests? Explain!

The network is functioning and devices are communicating properly. However, the connection reset warning, RST, means that some connections may have been interrupted or closed unexpectedly.

Question and Answer

What is the IP Address of the attacker and the target machine(s) being scanned? [Hint: Except machines in ignored states]

Answer (Attacker's IP Address) : 192.168.50.105

Answer (Target's IP Address) : 192.168.50.102, 192.168.50.104

What ports in the target machine(s) are open? List them down accordingly. *[Answer Format: IP Address: List Ports]*

Answer (Target No.1) : 192.168.56.104: 80/TCP, 135/TCP, 139/TCP, 445/TCP, 3000/TCP, 3306/TCP, 3989/TCP, 4848/TCP, 7676/TCP, 8080/TCP, 8181/TCP, 8383/TCP, 9200/TCP, 49152/TCP, 49153/TCP, 49154/TCP

Answer (Target No.2) : 192.168.50.102

Mitigation and Recommendations

What are the necessary countermeasures to avoid or prevent network scanning and enumeration.

To prevent network scanning and enumeration, implement firewalls, IDS/IPS, and access controls; disable unused services and ping replies; segment the network; enforce strong authentication; keep systems updated; monitor traffic; and use honeypots to detect threats.

ACTIVITY RUBRICS

Group Name CTRL + Z Wednesday, April 23, 2025

Members Surname, First Name MI. (Alphabetical)

1. Cano, Kaide M.
2. Cuenca, Cyrah Sophia Angella T.
3. Dionela, Terrence A.
4. Umengan, Darwin F.
5. ______

Criteria	Activity Rubrics					Points
	Not Attempted (0 points)	**Beginning (1 point)**	**Developing (2 points)**	**Proficient (3 points)**	**Exemplary (4 points)**	
Tool Usage	No attempt to use relevant tool(s).	Incorrect or unsuitable tool(s) selected.	Tool(s) used is/are somewhat suitable but not optimal.	Selected appropriate tool(s) with minor mismatches to the scenario.	Selected the most appropriate tool(s) for the task based on scenario.	
Network Scanning and Enumeration	No attempt to perform Network and Port Discovery.	No effective Network and Port discovery or major inaccuracies in discovered devices/services.	Basic Network and Port discovery with missing or inaccurate identification of devices or services.	Network and Port discovery conducted effectively; minor discrepancies or gaps in discovered devices/services.	Thorough discovery and accurate mapping; includes detailed identification of devices, IP addresses, and open ports.	
Use of Wireshark Filters and Features	No attempt to perform filtering of network traffic data.	Filters not used or configured incorrectly, leading to large irrelevant data.	Basic filters applied; excessive or irrelevant data captured.	Capture filters set up correctly with minor inefficiencies.	Capture filters configured accurately; unnecessary data excluded effectively.	
	No attempt to use Wireshark features.	Wireshark features not used effectively; manual analysis dominates.	Limited use of Wireshark features; investigation hindered by inefficiency.	Basic features used effectively; advanced features used with some errors.	Advanced features used effectively (e.g., filters, color coding, statistics)	
Analysis, Interpretation and Mitigation	No attempt to conduct analysis and interpretation.	Minimal or incorrect analysis; important information overlooked.	Basic analysis performed, but some important findings are missed or misinterpreted.	Results analyzed accurately but with some minor gaps in interpretation.	Detailed and accurate analysis of results; clear identification of open ports, services, and potential vulnerabilities.	
	No attempt to provide recommendations for mitigation.	Incorrect recommendations for mitigation.	Generalized or incomplete recommendations; lacks actionable steps.	Mostly accurate and actionable recommendations with minor omissions.	Accurate and actionable recommendations tailored to the scenario.	
Documentation	No attempt to provide report documentation of findings.	Poor documentation of findings; lacks structure or critical details.	Basic report provided with significant omissions or unclear explanations.	Detailed report provided; minor gaps in methods or findings.	Comprehensive report including methods, findings, and recommendations.	

Total Score and Feedback			**TOTAL POINTS EARNED (20 max points)**	
☐ Exemplary	20	Exemplary work demonstrating mastery of Wireshark features, thorough investigation, analysis, and comprehensive reporting.		
☐ Proficient	16-19	Solid performance with minor gaps in technical skills or documentation.		
☐ Developing	12-15	Basic understanding of Wireshark and investigation concepts; several significant gaps in execution.		
☐ Beginning	8-11	Minimal effort or understanding; critical errors or omissions in the capture, analysis, or reporting.		
☐ Not Attempted	0-7	Indicates failure to perform network investigation and analysis.		

Evaluated by: ______________________ Name of Course Instructor	**Remarks/Comments**