Host-Only Network Traffic Analysis Report

SOC Simulation Lab

Name: Sanjeev Kushwaha
Role: SOC Analyst (Lab Simulation)
Date: 21.feb.2026

Tools Used

- Wireshark
- Kali Linux
- Ubuntu
- VMware

Key Findings

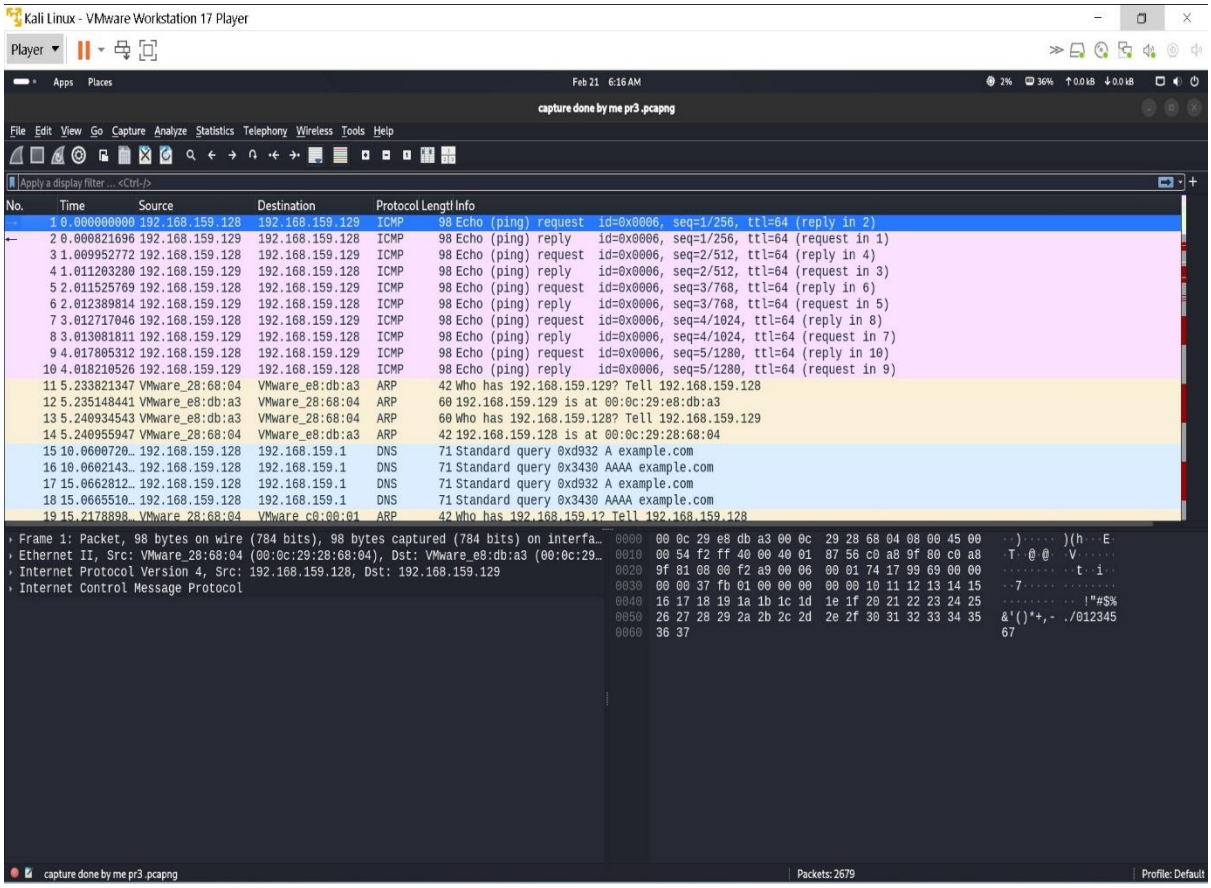
- High volume SYN packets indicating scanning
- Repeated DNS queries
- SSH connection attempt detected
- ARP-based host discovery

1. Executive Summary

This report documents network traffic analysis performed in a controlled host-only lab environment. The objective was to analyze reconnaissance and enumeration activities using Wireshark and identify suspicious indicators consistent with early-stage attack behavior.

2. Lab Environment

- Attacker Machine: Kali Linux – 192.168.159.128
- Target Machine: Ubuntu – 192.168.159.129
- Network Type: Host-Only
- Total Packets Captured: ~2679
- Analysis Tool: Wireshark



3. Attack Simulation Evidence

```
┌──(cs㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    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 00:0c:29:28:68:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.159.128/24 brd 192.168.159.255 scope global dynamic noprefixroute eth0
       valid_lft 1405sec preferred_lft 1405sec
    inet6 fe80::20c:29ff:fe28:6804/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
ubantu24@ubantu24:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:e8:db:a3 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.159.129/24 metric 100 brd 192.168.159.255 scope global dynamic
ens33
       valid_lft 1588sec preferred_lft 1588sec
    inet6 fe80::20c:29ff:fee8:dba3/64 scope link
       valid_lft forever preferred_lft forever
ubantu24@ubantu24:~$ _
```

```
┌──(cs㉿kali)-[~]
└─$ ping 192.168.159.129
PING 192.168.159.129 (192.168.159.129) 56(84) bytes of data.
64 bytes from 192.168.159.129: icmp_seq=1 ttl=64 time=0.832 ms
64 bytes from 192.168.159.129: icmp_seq=2 ttl=64 time=1.59 ms
64 bytes from 192.168.159.129: icmp_seq=3 ttl=64 time=1.57 ms
64 bytes from 192.168.159.129: icmp_seq=4 ttl=64 time=0.762 ms
64 bytes from 192.168.159.129: icmp_seq=5 ttl=64 time=0.744 ms
64 bytes from 192.168.159.129: icmp_seq=6 ttl=64 time=1.20 ms
^C
--- 192.168.159.129 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5019ms
rtt min/avg/max/mdev = 0.744/1.114/1.585/0.359 ms
```

```
ubantu24@ubantu24:~$ ping 192.168.159.128
PING 192.168.159.128 (192.168.159.128) 56(84) bytes of data.
64 bytes from 192.168.159.128: icmp_seq=1 ttl=64 time=1.21 ms
64 bytes from 192.168.159.128: icmp_seq=2 ttl=64 time=1.15 ms
64 bytes from 192.168.159.128: icmp_seq=3 ttl=64 time=1.09 ms
64 bytes from 192.168.159.128: icmp_seq=4 ttl=64 time=1.20 ms
64 bytes from 192.168.159.128: icmp_seq=5 ttl=64 time=1.24 ms
^C
--- 192.168.159.128 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.094/1.177/1.243/0.051 ms
ubantu24@ubantu24:~$
```

Fig. controlled Lab setup kali as attacker, ubuntu as victim

3.1: nmap -sS 192.168.159.129

```
┌──(cs㉿kali)-[~]
└─$ nmap -sS 192.168.159.129
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-20 11:35 EST
Nmap scan report for 192.168.159.129
Host is up (0.00063s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:E8:DB:A3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds

┌──(cs㉿kali)-[~]
└─$
```

3.2: ssh fakeuser@192.168.159.129

```
┌──(cs㉿kali)-[~]
└─$ ssh fakeuser@192.168.159.129
fakeuser@192.168.159.129's password:
Permission denied, please try again.
fakeuser@192.168.159.129's password:
Permission denied, please try again.
fakeuser@192.168.159.129's password:
fakeuser@192.168.159.129: Permission denied (publickey,password).
```

```
575482 320.562128664 VMware_28:68:04  VMware_c0:00:01  ARP   42 Who has 192.168.159.1? Te
575483 320.562712087 VMware_c0:00:01  VMware_28:68:04  ARP   60 192.168.159.1 is at 00:50
575484 325.399662392 192.168.159.128  192.168.159.1    DNS   81 Standard query 0x8a0f A 1
575485 325.400114621 192.168.159.128  192.168.159.1    DNS   81 Standard query 0x310a AAA
575486 330.405901608 192.168.159.128  192.168.159.1    DNS   81 Standard query 0x8a0f A 1
575487 330.406494206 192.168.159.128  192.168.159.1    DNS   81 Standard query 0x310a AAA
575488 335.410204674 192.168.159.128  192.168.159.1    DNS   93 Standard query 0x522d A 1
575489 335.411444878 192.168.159.128  192.168.159.1    DNS   93 Standard query 0x3d2b AAA
575490 340.416915539 192.168.159.128  192.168.159.1    DNS   93 Standard query 0x522d A 1
575491 340.418056616 192.168.159.128  192.168.159.1    DNS   93 Standard query 0x3d2b AAA
575492 345.424862360 192.168.159.128  192.168.159.1    DNS   81 Standard query 0x29f4 A 2
575493 345.425290846 192.168.159.128  192.168.159.1    DNS   81 Standard query 0x39f3 AAA
575494 345.649729476 VMware_28:68:04  VMware_c0:00:01  ARP   42 Who has 192.168.159.1? Te
575495 345.650451 VMware_c0:00:01  VMware_28:68:04  ARP   60 192.168.159.1 is at 00:50
> Frame 1: Packet, 93 bytes on wire (744 bits), 93 by  0000  00 50 56 c0 00 01 00 0c  29 28 68 04 08 00 45
```

3.3: curl http://192.169.159.129:8000

```
┌──(cs㉿kali)-[~]
└─$ curl http://192.168.159.129:8000
<!DOCTYPE HTML>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a></li>
<li><a href=".bash_logout">.bash_logout</a></li>
<li><a href=".bashrc">.bashrc</a></li>
<li><a href=".cache/">.cache/</a></li>
<li><a href=".config/">.config/</a></li>
<li><a href=".dmrc">.dmrc</a></li>
<li><a href=".local/">.local/</a></li>
<li><a href=".profile">.profile</a></li>
<li><a href=".ssh/">.ssh/</a></li>
<li><a href=".sudo_as_admin_successful">.sudo_as_admin_successful</a></li>
<li><a href=".xsession">.xsession</a></li>
<li><a href="Desktop/">Desktop/</a></li>
<li><a href="Document/">Document/</a></li>
<li><a href="Downloads/">Downloads/</a></li>
</ul>
<hr>
</body>
</html>
```

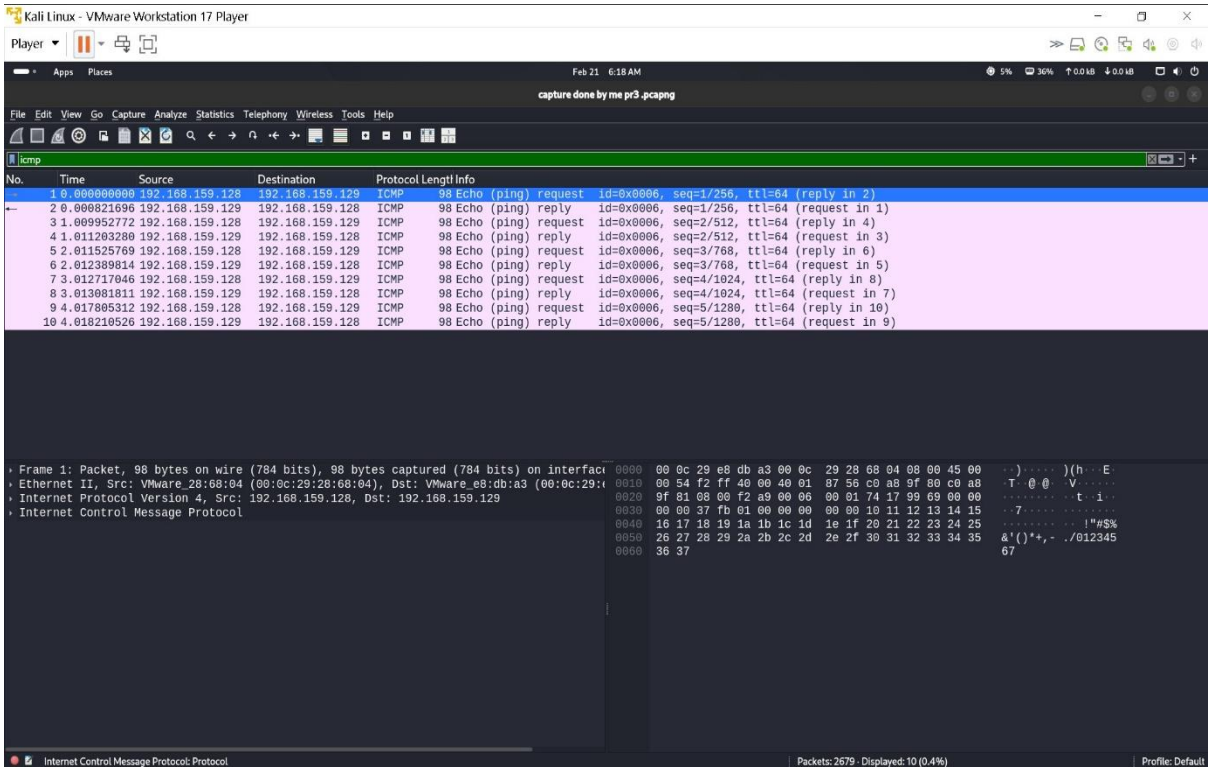
3.3.1: created http server using python

```
ubantu24@ubantu24:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.159.128 - - [20/Feb/2026 16:59:30] "GET / HTTP/1.1" 200 -
192.168.159.128 - - [20/Feb/2026 17:00:02] "GET / HTTP/1.1" 200 -
192.168.159.128 - - [20/Feb/2026 17:00:03] "GET / HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
ubantu24@ubantu24:~$ _
```

4. Traffic Analysis Findings

4.1 ICMP Activity (Ping Analysis)

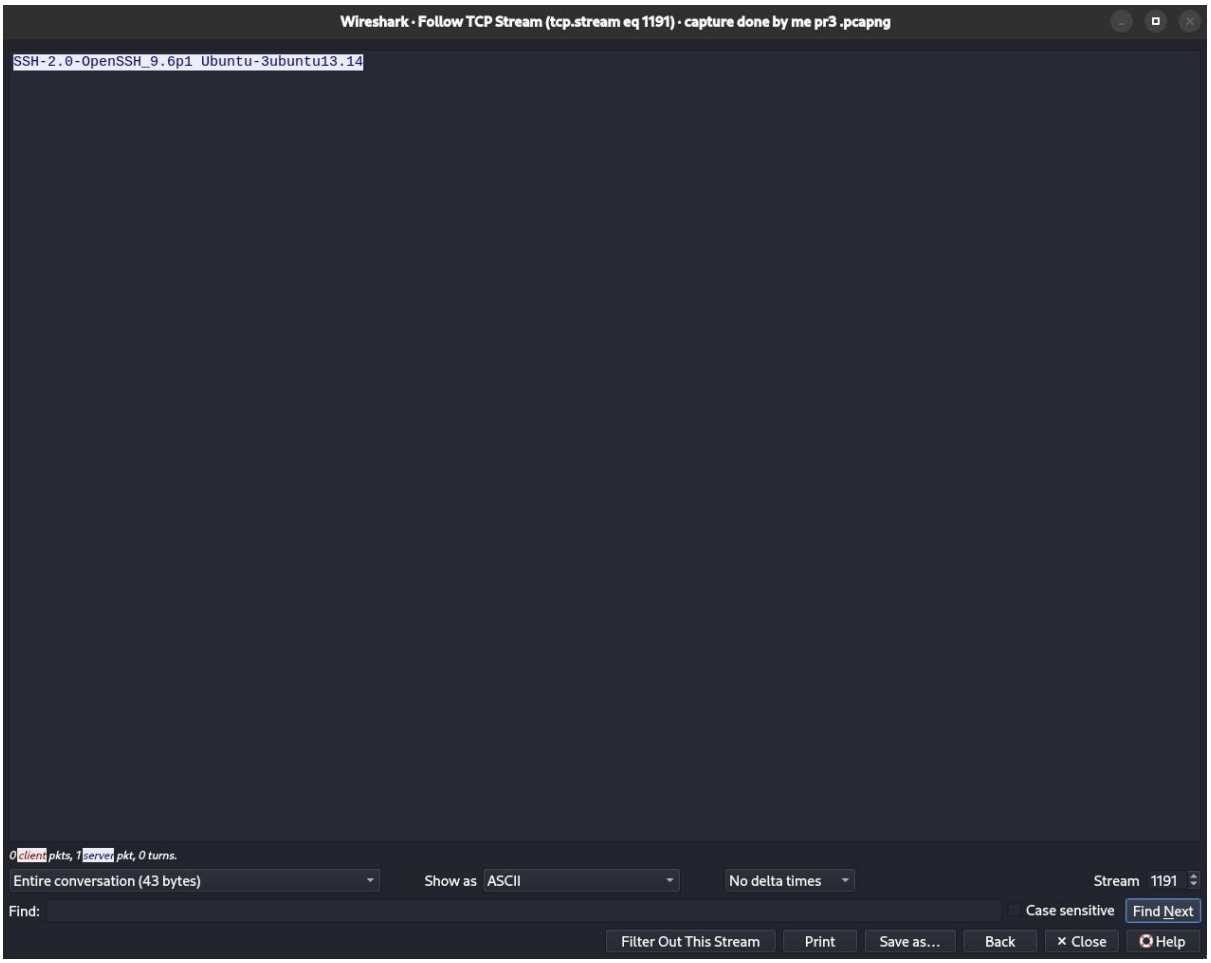
ICMP echo requests and replies were observed between attacker and target. Some unsuccessful pings were detected, indicating host discovery attempts.



Filter Used: icmp

4.2: SSH Connection Attempt

SSH connection attempt observed from 192.168.159.128 to 192.168.159.129. TCP handshake behavior indicates authentication attempt using fake user credentials.

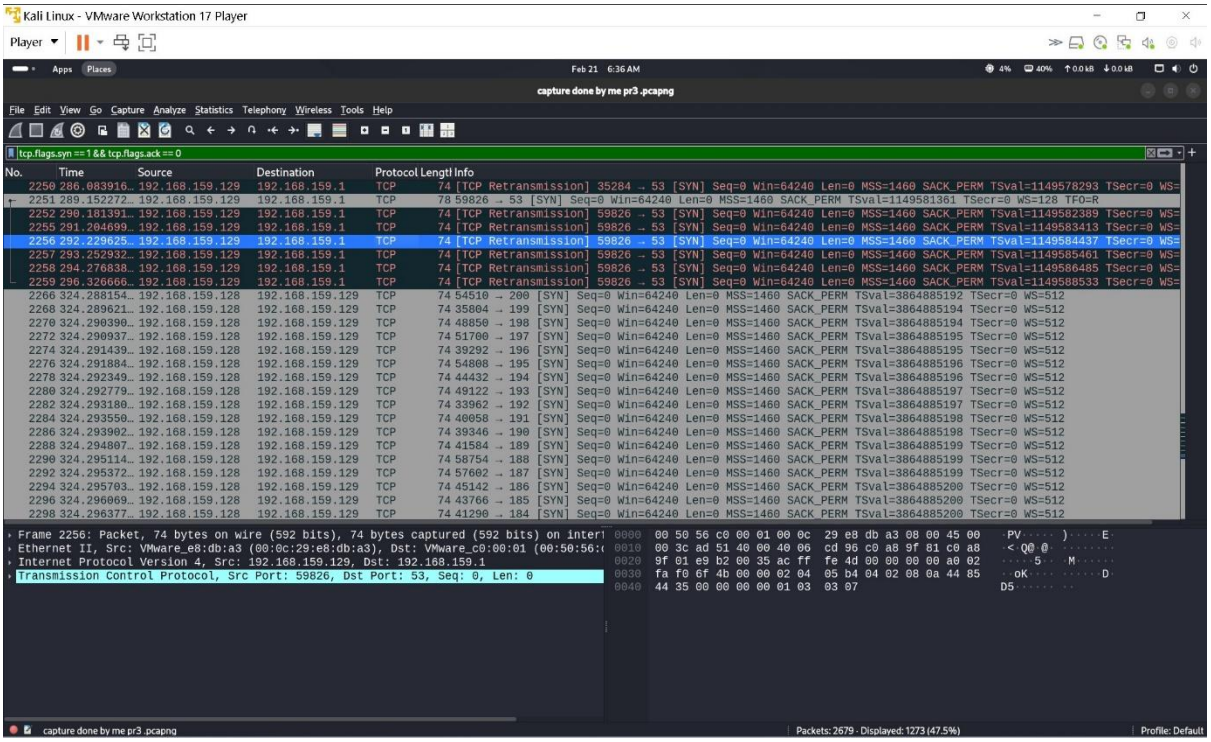


Filter:

tcp.port == 22

4.2 SYN Scan / Port Scanning Activity

Multiple TCP SYN packets sent without completing full handshake indicate port scanning behavior consistent with reconnaissance activity.

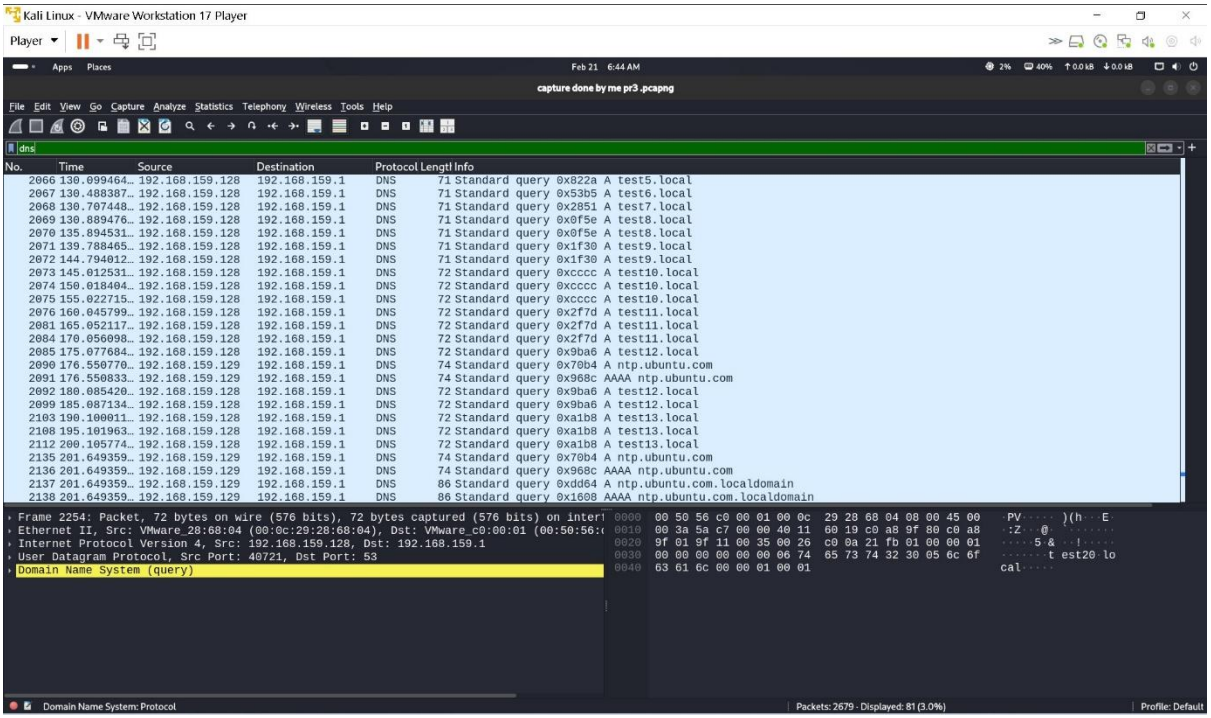


Filter:

tcp.flags.syn == 1 && tcp.flags.ack == 0

4.3 DNS Enumeration

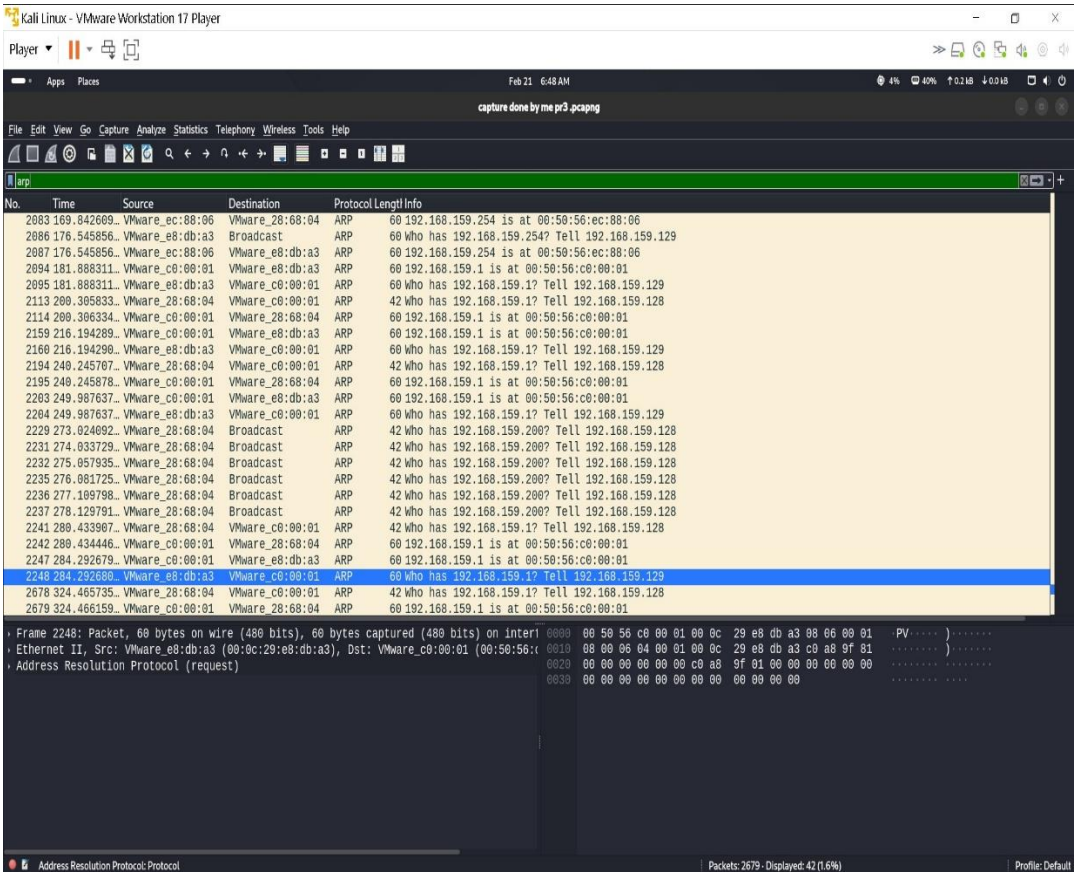
Repeated DNS queries for test*.local domains were observed, suggesting enumeration attempts.



Filter: Dns

4.4 ARP Discovery

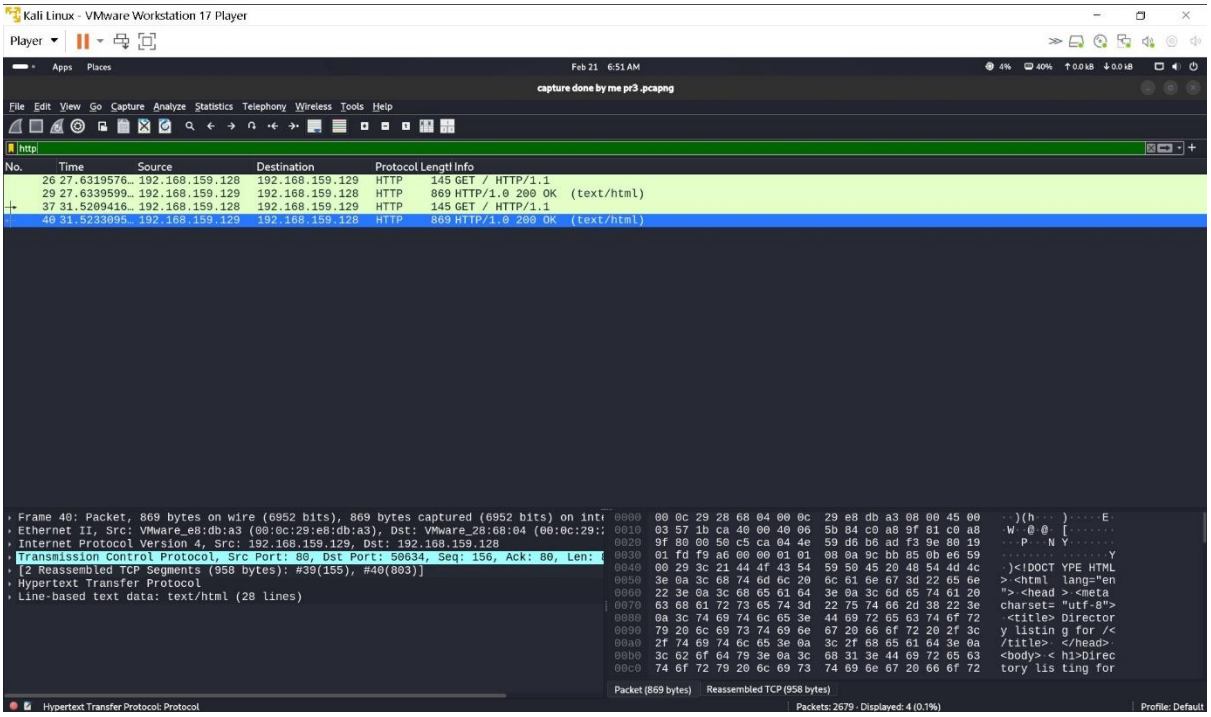
ARP request-response communication confirms local network host discovery attempt.



Filter : arp

4.5 HTTP Request

HTTP GET request observed from attacker to target system using curl, indicating service interaction attempt.



Filter : http

5. Indicators of Compromise (IOC) / Suspicious Behavior

- High volume TCP SYN packets
- Repeated DNS query pattern
- SSH login attempt
- Port scanning behavior
- ARP host discovery

6. Conclusion

Analysis confirms reconnaissance and enumeration activities consistent with pre-attack behavior. No malware payload detected, as activity was conducted in a controlled lab environment for educational purposes.