

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

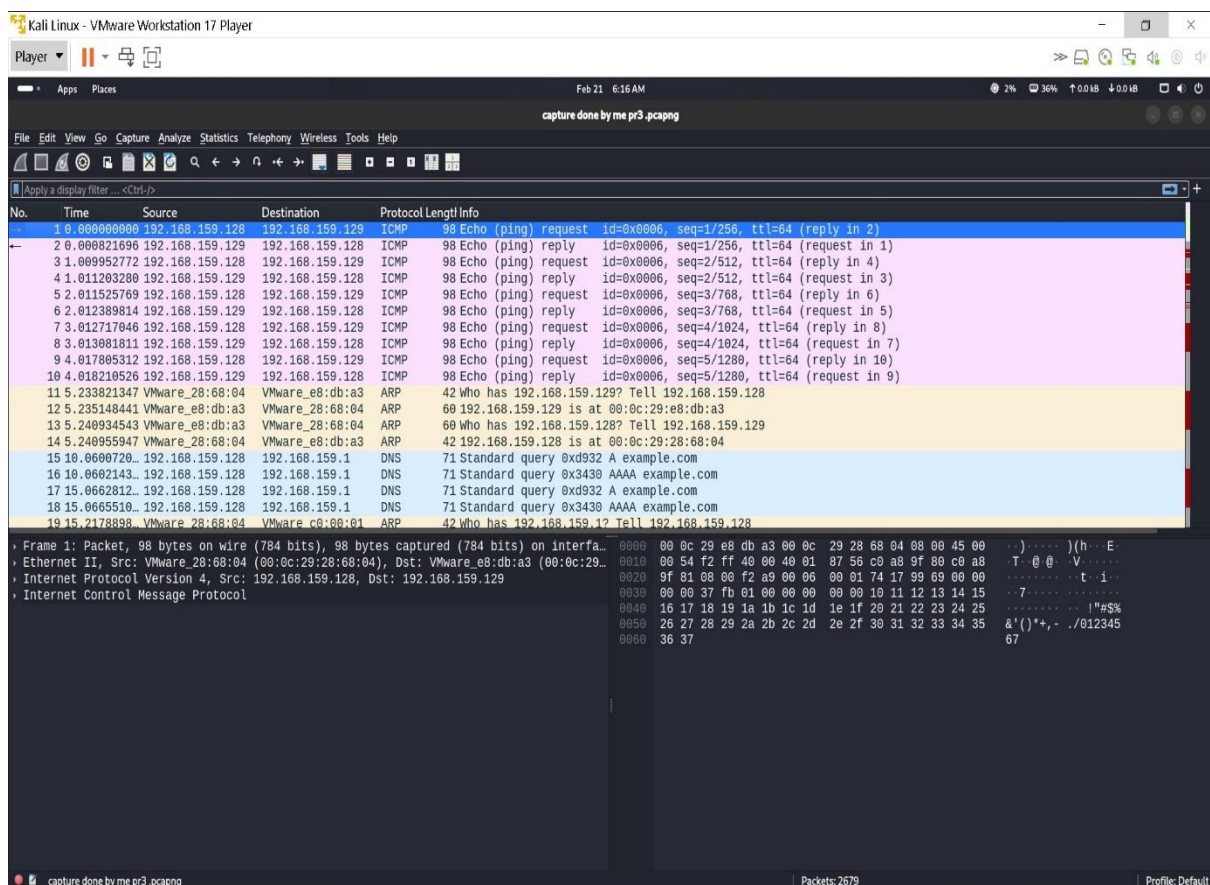
- High volume SYN packets indicating scanning
- Repeated DNS queries
- SSH connection attempt detected
- ARP-based host discovery

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
```

```
ubuntu24@ubuntu24:~$ 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group 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
ubuntu24@ubuntu24:~$ _
```

```
(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

ubuntu24@ubuntu24:~$ 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
ubuntu24@ubuntu24:~$
```

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).
```

3.3: curl http://192.168.159.129:8000

```
(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>
```

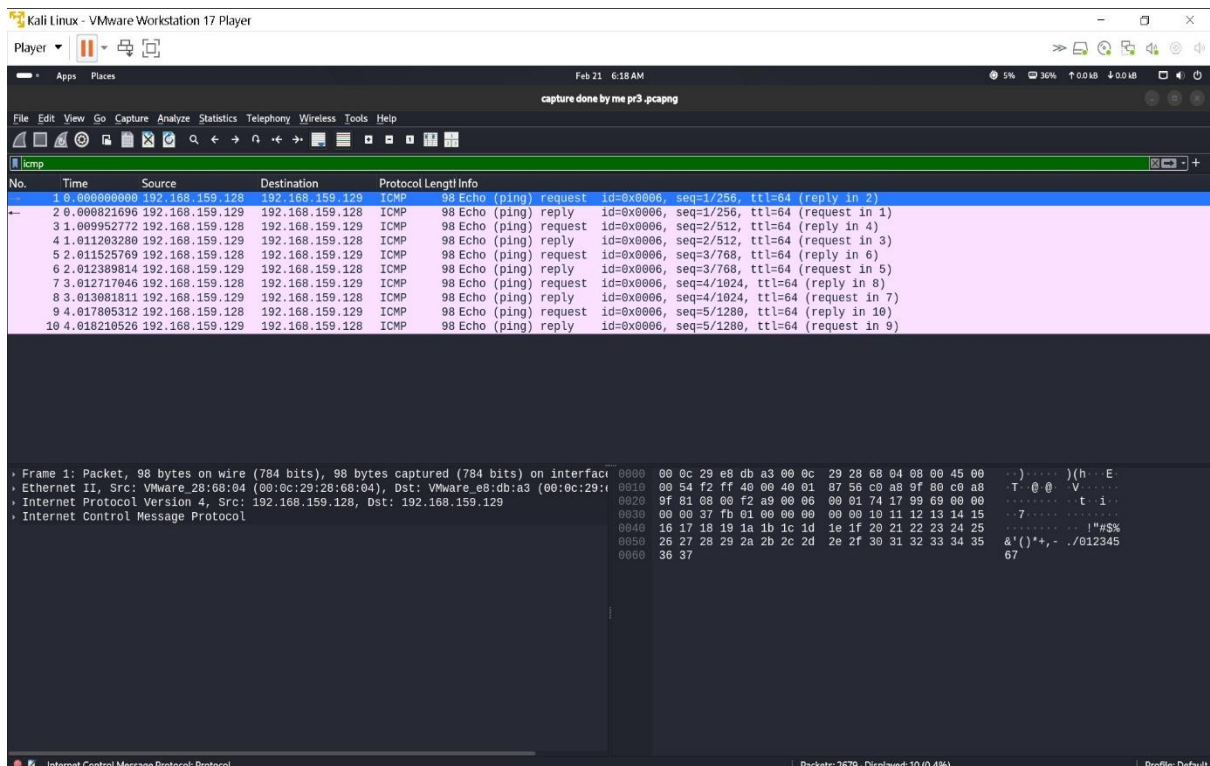
3.3.1: created http server using python

```
ubuntu24@ubuntu24:~$ 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.
ubuntu24@ubuntu24:~$ _
```

4. Traffic Analysis Findings

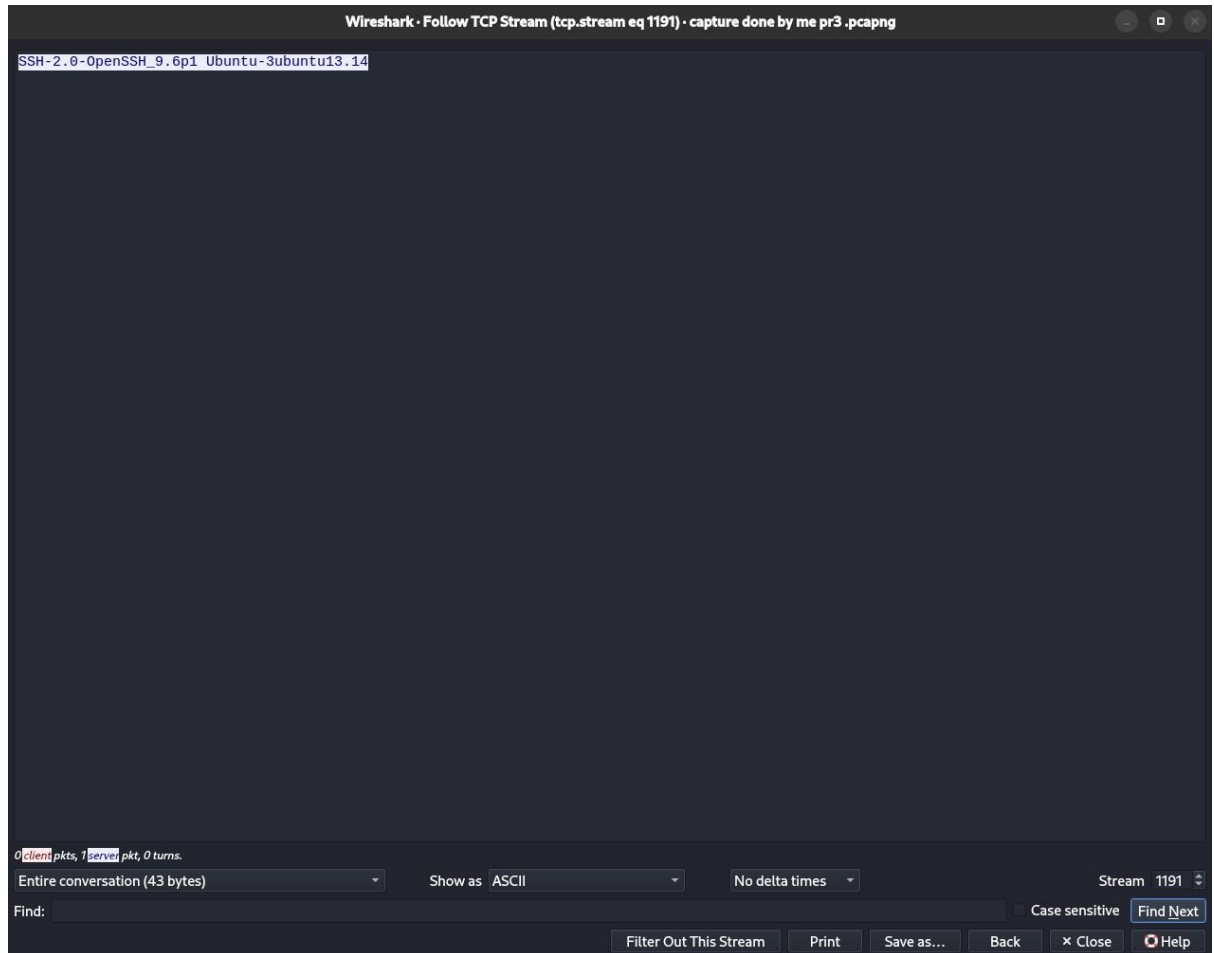
4.1 ICMP Activity (Ping Analysis)

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.

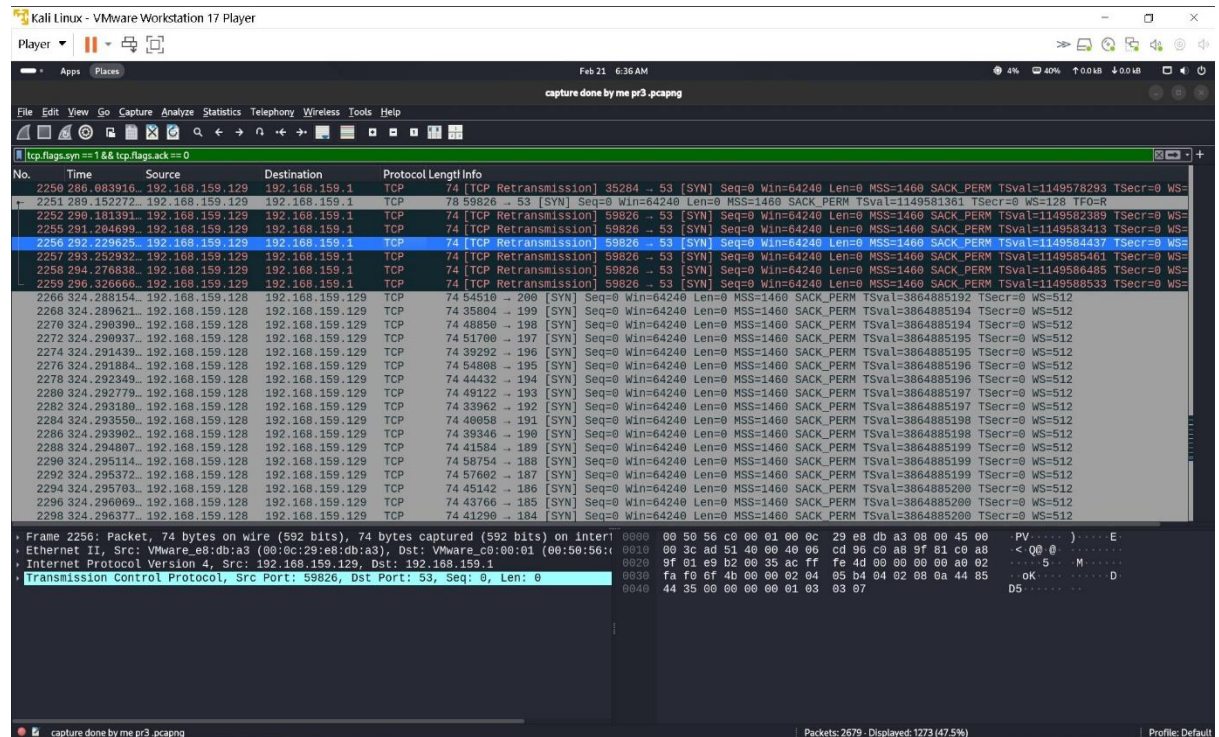


Filter:

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.

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of DNS queries, all originating from 192.168.159.128 and destined for 192.168.159.1. The queries are for various test domains (test5.local through test13.local) and ntp.ubuntu.com. The bottom pane shows a detailed view of a selected packet (No. 2138), which is a DNS query for ntp.ubuntu.com. The packet details show it is a Standard query, type AAAA, and the destination port is 53. The packet bytes pane shows the raw data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
2066	130.099464	192.168.159.128	192.168.159.1	DNS	71	Standard query 0x822a A test5.local
2067	130.488387	192.168.159.128	192.168.159.1	DNS	71	Standard query 0x53b5 A test6.local
2068	130.707448	192.168.159.128	192.168.159.1	DNS	71	Standard query 0x2851 A test7.local
2069	130.889476	192.168.159.128	192.168.159.1	DNS	71	Standard query 0x8f5e A test8.local
2070	135.894531	192.168.159.128	192.168.159.1	DNS	71	Standard query 0x0f5e A test8.local
2071	139.788465	192.168.159.128	192.168.159.1	DNS	71	Standard query 0x1f30 A test9.local
2072	144.794812	192.168.159.128	192.168.159.1	DNS	71	Standard query 0x1f30 A test9.local
2073	145.012531	192.168.159.128	192.168.159.1	DNS	72	Standard query 0xc000 A test10.local
2074	150.018404	192.168.159.128	192.168.159.1	DNS	72	Standard query 0xc000 A test10.local
2075	155.022715	192.168.159.128	192.168.159.1	DNS	72	Standard query 0xc000 A test10.local
2076	160.045799	192.168.159.128	192.168.159.1	DNS	72	Standard query 0x2f7d A test11.local
2081	165.052117	192.168.159.128	192.168.159.1	DNS	72	Standard query 0x2f7d A test11.local
2084	170.056098	192.168.159.128	192.168.159.1	DNS	72	Standard query 0x2f7d A test11.local
2085	175.077684	192.168.159.128	192.168.159.1	DNS	72	Standard query 0x9ba6 A test12.local
2090	176.550770	192.168.159.128	192.168.159.1	DNS	74	Standard query 0x70b4 A ntp.ubuntu.com
2091	176.550833	192.168.159.128	192.168.159.1	DNS	74	Standard query 0x960c AAAA ntp.ubuntu.com
2092	180.085420	192.168.159.128	192.168.159.1	DNS	72	Standard query 0x9ba6 A test12.local
2099	185.087134	192.168.159.128	192.168.159.1	DNS	72	Standard query 0x9ba6 A test12.local
2103	190.100011	192.168.159.128	192.168.159.1	DNS	72	Standard query 0xa1b8 A test13.local
2108	195.101963	192.168.159.128	192.168.159.1	DNS	72	Standard query 0xa1b8 A test13.local
2112	200.105774	192.168.159.128	192.168.159.1	DNS	72	Standard query 0xa1b8 A test13.local
2135	201.649359	192.168.159.128	192.168.159.1	DNS	74	Standard query 0x70b4 A ntp.ubuntu.com
2136	201.649359	192.168.159.128	192.168.159.1	DNS	74	Standard query 0x960c AAAA ntp.ubuntu.com
2137	201.649359	192.168.159.128	192.168.159.1	DNS	86	Standard query 0xd6d4 A ntp.ubuntu.com.localdomain
2138	201.649359	192.168.159.128	192.168.159.1	DNS	86	Standard query 0x1608 AAAA ntp.ubuntu.com.localdomain

Frame 2254: Packet, 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface
Ethernet II, Src: VMware_28:68:04 (00:0c:29:28:68:04), Dst: VMware_c0:00:01 (00:50:56:00:00:01)
Internet Protocol Version 4, Src: 192.168.159.128, Dst: 192.168.159.1
User Datagram Protocol, Src Port: 40721, Dst Port: 53
Domain Name System (query)

Filter: Dns

4.4 ARP Discovery

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

The image shows a Wireshark packet capture window titled "capture done by me pr3 pc3.png". The filter bar at the top is set to "arp". The packet list on the left shows 42 packets, with the last three (2248, 2678, and 2679) selected. The packet details pane on the right shows the selected packet (2248) as an ARP request from VMware_e8:db:a3 to VMware_c0:00:01. The packet bytes pane at the bottom shows the raw data of the ARP request.

No.	Time	Source	Destination	Protocol	Length	Info
2083	169.842609...	VMware_ec:88:06	VMware_28:68:04	ARP	60	192.168.159.254 is at 00:50:56:ec:88:06
2086	176.545856...	VMware_e8:db:a3	Broadcast	ARP	60	Who has 192.168.159.254? Tell 192.168.159.129
2087	176.545856...	VMware_ec:88:06	VMware_e8:db:a3	ARP	60	192.168.159.254 is at 00:50:56:ec:88:06
2094	181.888311...	VMware_c0:00:01	VMware_e8:db:a3	ARP	60	192.168.159.1 is at 00:50:56:c0:00:01
2095	181.888311...	VMware_e8:db:a3	VMware_c0:00:01	ARP	60	Who has 192.168.159.1? Tell 192.168.159.129
2113	200.305833...	VMware_28:68:04	VMware_c0:00:01	ARP	42	Who has 192.168.159.1? Tell 192.168.159.128
2114	200.305833...	VMware_c0:00:01	VMware_28:68:04	ARP	60	192.168.159.1 is at 00:50:56:c0:00:01
2159	216.194289...	VMware_c0:00:01	VMware_e8:db:a3	ARP	60	192.168.159.1 is at 00:50:56:c0:00:01
2160	216.194289...	VMware_e8:db:a3	VMware_c0:00:01	ARP	60	Who has 192.168.159.1? Tell 192.168.159.129
2194	240.245707...	VMware_28:68:04	VMware_c0:00:01	ARP	42	Who has 192.168.159.1? Tell 192.168.159.128
2195	240.245707...	VMware_c0:00:01	VMware_28:68:04	ARP	60	192.168.159.1 is at 00:50:56:c0:00:01
2203	249.987637...	VMware_c0:00:01	VMware_e8:db:a3	ARP	60	192.168.159.1 is at 00:50:56:c0:00:01
2204	249.987637...	VMware_e8:db:a3	VMware_c0:00:01	ARP	60	Who has 192.168.159.1? Tell 192.168.159.129
2229	273.024092...	VMware_28:68:04	Broadcast	ARP	42	Who has 192.168.159.200? Tell 192.168.159.128
2231	274.033729...	VMware_28:68:04	Broadcast	ARP	42	Who has 192.168.159.200? Tell 192.168.159.128
2232	275.057935...	VMware_28:68:04	Broadcast	ARP	42	Who has 192.168.159.200? Tell 192.168.159.128
2235	276.081725...	VMware_28:68:04	Broadcast	ARP	42	Who has 192.168.159.200? Tell 192.168.159.128
2236	277.109798...	VMware_28:68:04	Broadcast	ARP	42	Who has 192.168.159.200? Tell 192.168.159.128
2237	278.129791...	VMware_28:68:04	Broadcast	ARP	42	Who has 192.168.159.200? Tell 192.168.159.128
2241	280.433907...	VMware_28:68:04	VMware_c0:00:01	ARP	42	Who has 192.168.159.1? Tell 192.168.159.128
2242	280.434446...	VMware_c0:00:01	VMware_28:68:04	ARP	60	192.168.159.1 is at 00:50:56:c0:00:01
2247	284.292679...	VMware_c0:00:01	VMware_e8:db:a3	ARP	60	192.168.159.1 is at 00:50:56:c0:00:01
2248	284.292688...	VMware_e8:db:a3	VMware_c0:00:01	ARP	60	Who has 192.168.159.1? Tell 192.168.159.129
2678	324.465735...	VMware_28:68:04	VMware_c0:00:01	ARP	42	Who has 192.168.159.1? Tell 192.168.159.128
2679	324.466159...	VMware_c0:00:01	VMware_28:68:04	ARP	60	192.168.159.1 is at 00:50:56:c0:00:01

Frame 2248: Packet, 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on Interface 0
Ethernet II, Src: VMware_e8:db:a3 (00:0c:29:e8:db:a3), Dst: VMware_c0:00:01 (00:50:56:c0:00:01)
Address Resolution Protocol (request)

0000 00 50 56 c0 00 01 00 0c 29 e8 db a3 00 00 01
0019 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0020 00 00 00 00 00 00 c0 a8 9f 01 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Address Resolution Protocol: Protocol

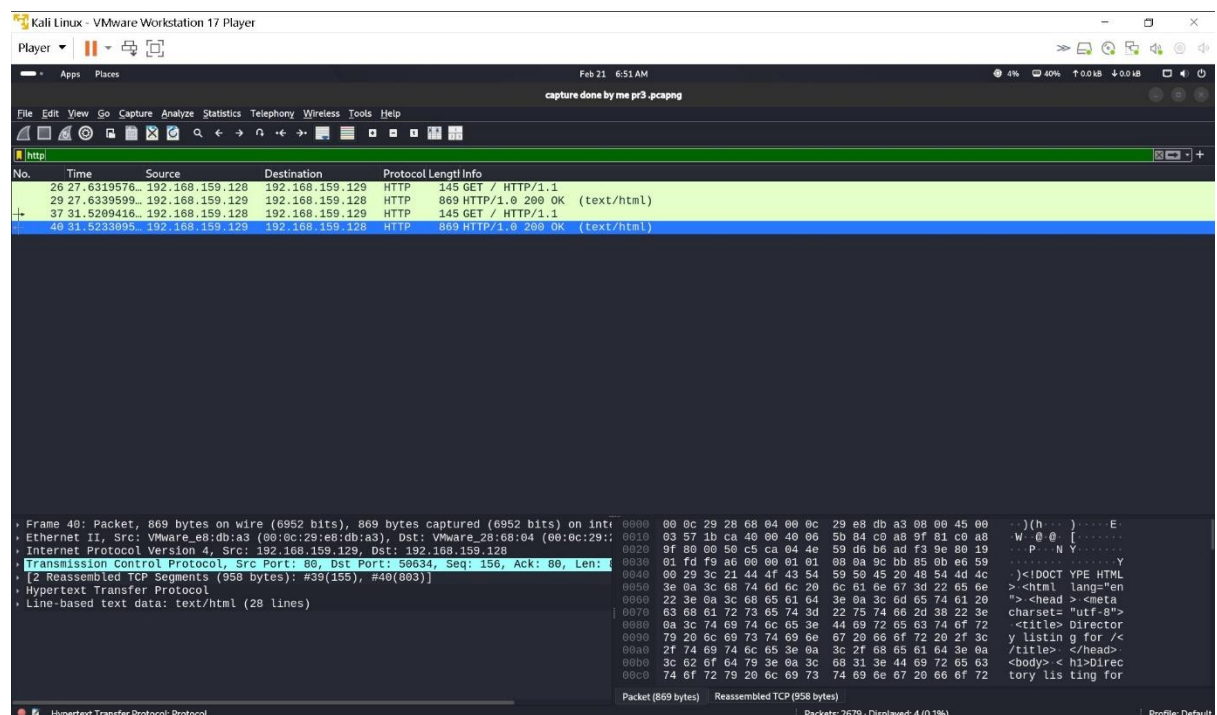
Packets: 2679 - Displayed: 42 (1.6%)

Profile: Default

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.