Team 3 Capstone Project

Team Soc em Up Tier 3 BY ANGEL C MORRIS

This capstone project demonstrates the Soc'em Up team's cybersecurity expertise through advanced penetration testing and in-depth Wireshark analysis, simulating real-world attacks to identify vulnerabilities and strengthen network defenses.

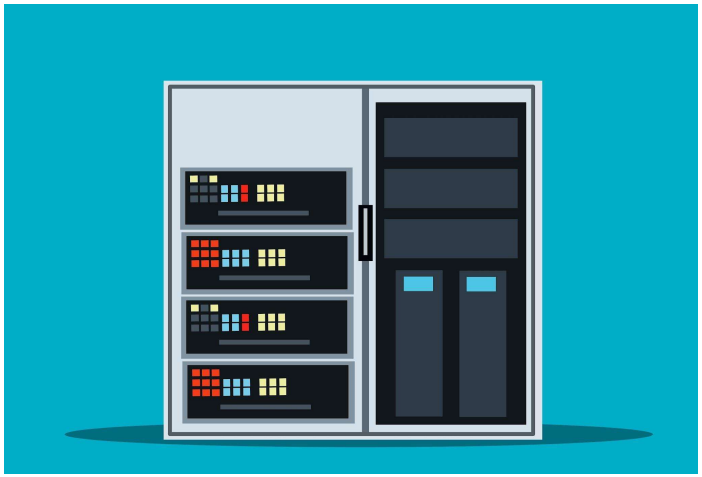
Through this project, the team applied rigorous ethical hacking techniques to assess system resilience, followed by detailed packet-level examination using Wireshark to trace attack vectors and understand network behavior under duress. The findings provide critical insights for improving security postures and incident response strategies.

Tech Solutions Inc.
Incident Analysis Report

We identified and validated the Metasploit framework and the relevant exploit module targeting the Kali test environment. We verified through brute force the username and through wordlists a password. Our work focused on reconnaissance, exploit selection, and confirming exploit viability. At this point, we established the attack surface and prepared the execution pathway. We will now hand off to our teammate, who will demonstrate the full remote code execution process and post-exploitation results.

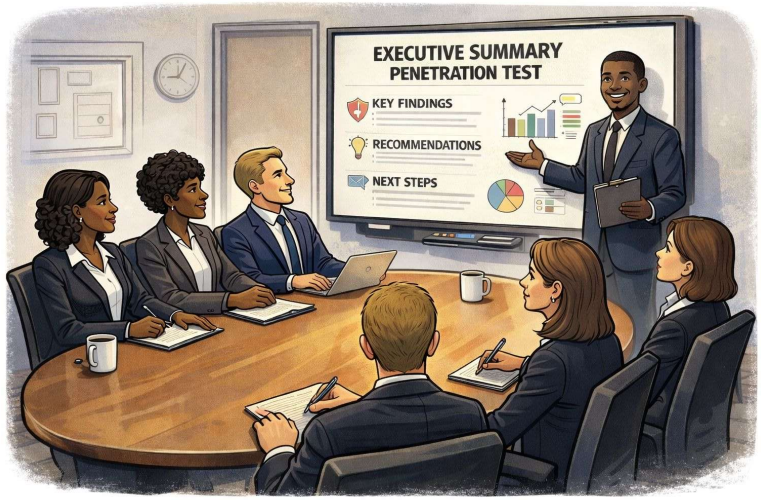
Task #1001 - Penetration Testing Introduction

- Penetration Testing Context.
  - Tech Solutions Inc.,
- Pentest topics discussed:
  - Executive Summary, Scope, Key Phases of the Penetration Test, Report Findings, and Conclusion.



Task #1001 - Executive Summary

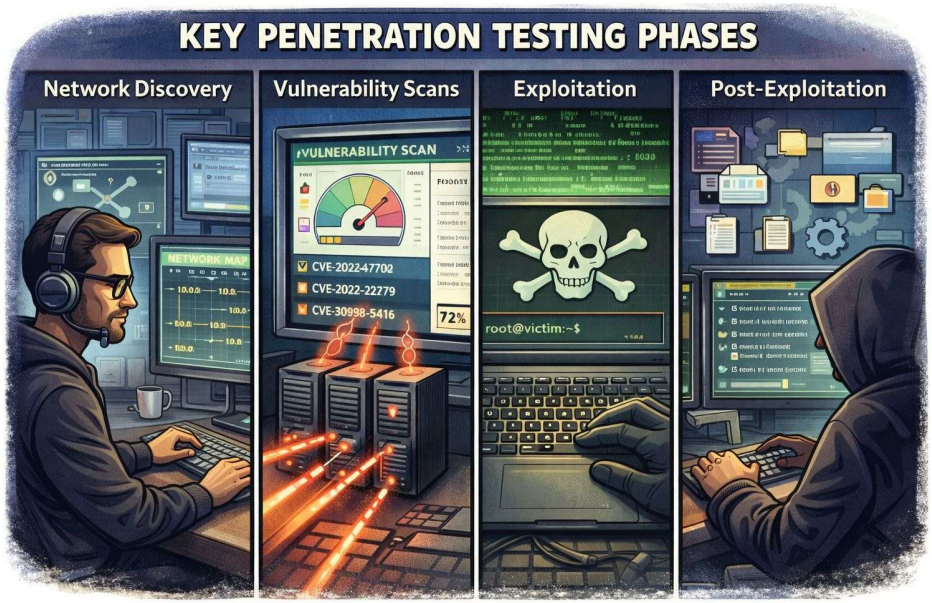
- Multiple vulnerabilities scanned
- Specific Pentest findings: Server configuration information leaks, username leaks, file directory listings, unauthorized privilege escalation, publicly available files, outdated software.
- Penetration testing Tools.
- Network discovery, vulnerability scanning, exploitation, post-exploitation analysis.
- Server Security Posture Summary: High-Risk
- Recommended Mitigations



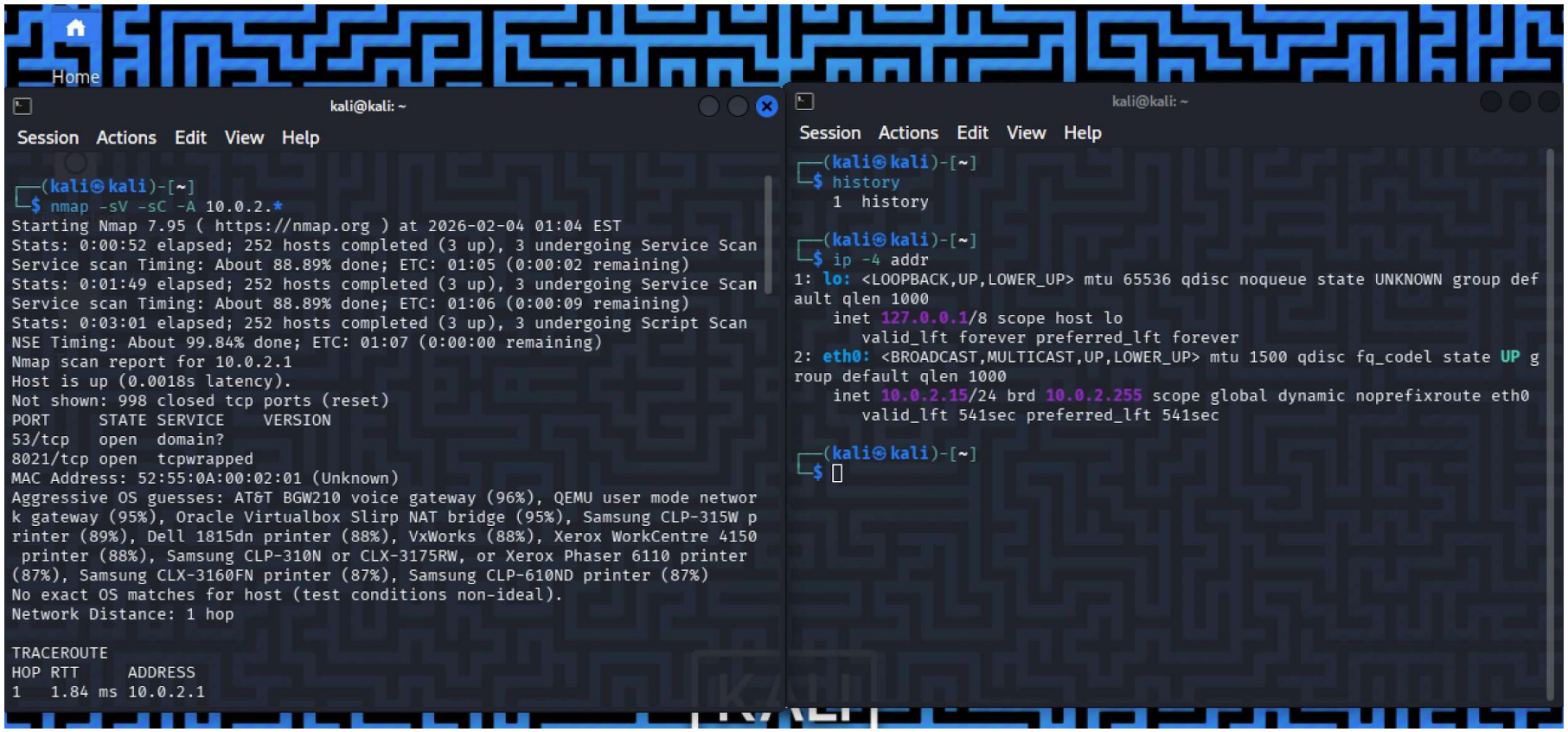
Task #1001 - Scope

- In-Scope Assets
  - Virtual disk image of the business server, NAT network
- Out of Scope Assets
  - Real company servers and real network
- Methodology
  - **Tools Used:** Virtual Box, Virtual Box NAT Network, Kali linux VM, vul01 vm, Nmap, enum4linux, Linux ping command, Metasploit, GoBusters, Linux Secure Shell command, DIRB, WPScan, FireFox, John the Ripper, and various internet resources.
  - **NAT Network IP:** 10.0.2.0/24
  - **NAT Network DHCP:** 10.0.2.1
  - **NAT Network Router:** 10.0.2.2
  - **Kali VM:** 10.0.2.15
  - **VUL01 VM:** 10.0.2.3

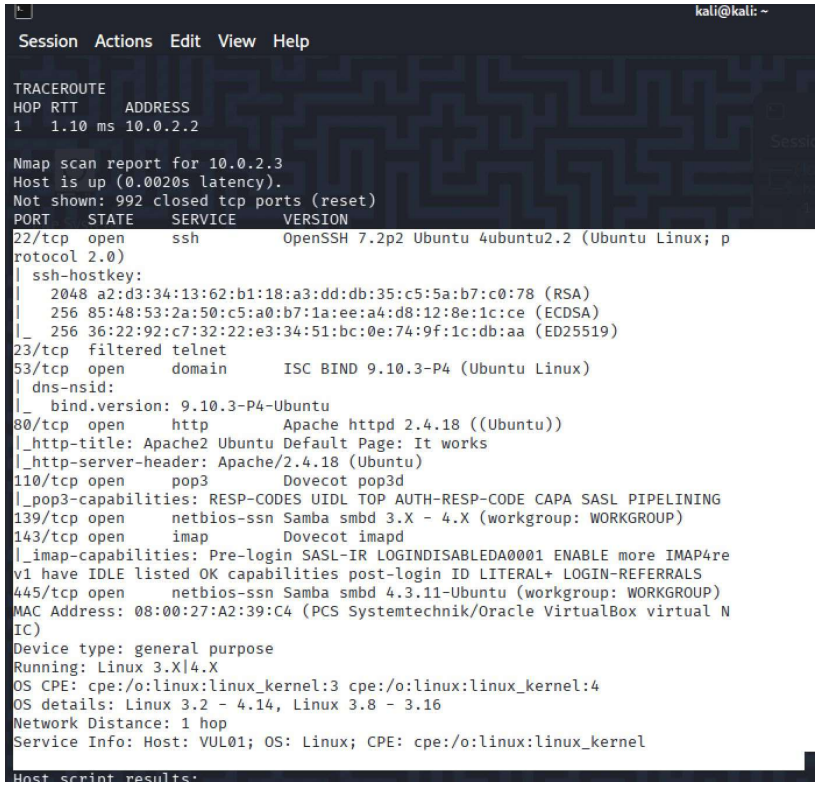
Key Penetration Testing Phases:
Network Discovery, Vulnerability Scans, Exploitation, Post-Exploitation



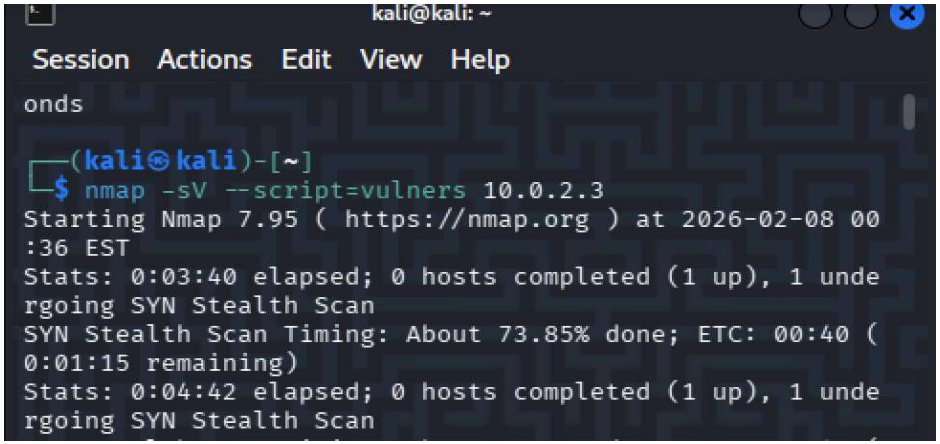
Task #1001 - Network Discovery and NAT Network

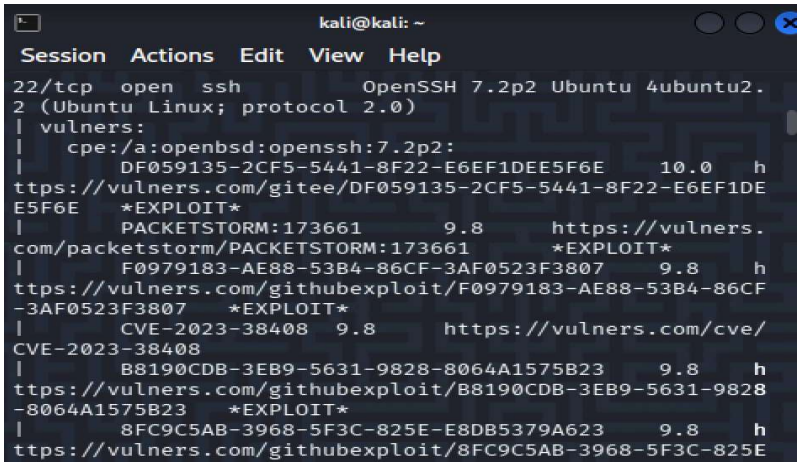


Task #1001 - Nmap Scan



Task #1001 - Vulnerability Scan Overview



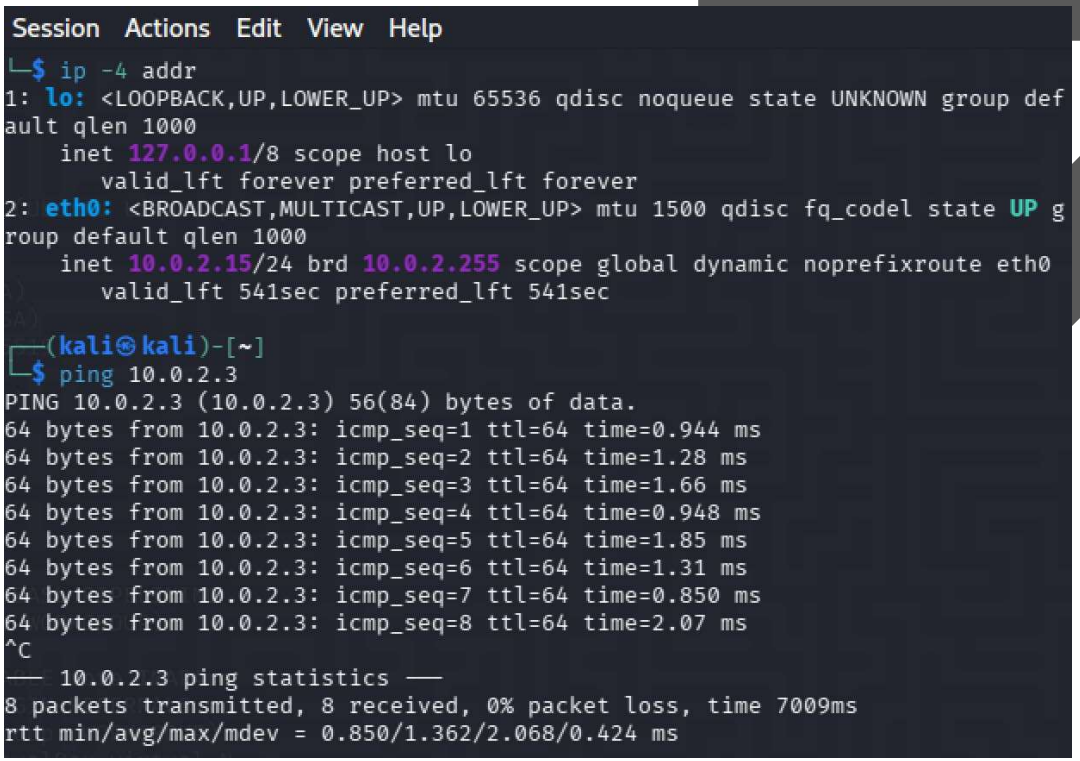


General Overview

Top Three CVEs

- “Terrapin” and Buffer Overflow (CVE-2023-38408 / 2023-48795)
- Apache HTTPD Module RCE (CVE-2021-44790)
- Apache Path Traversal & File Disclosure (CVE-2021-40438)
- Patches

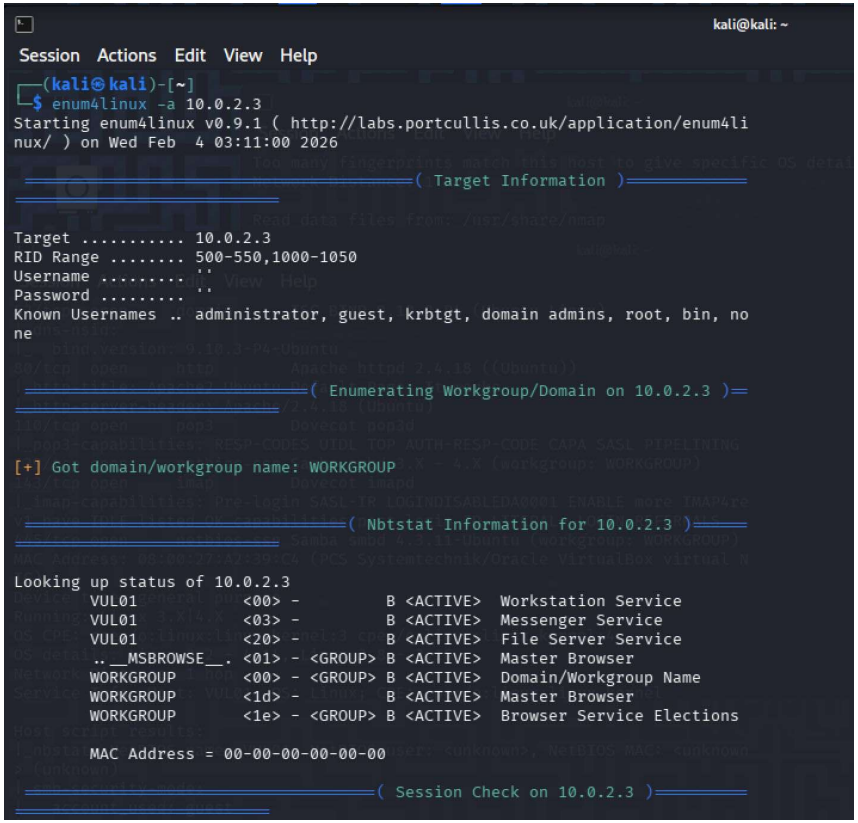
Ping 10.0.2.3

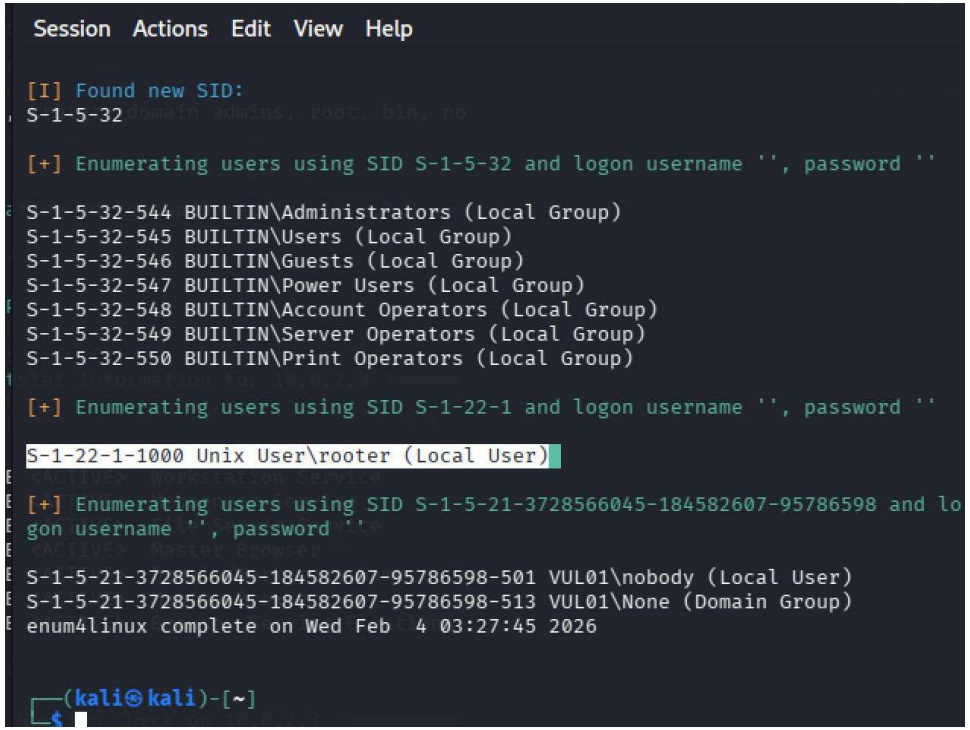


Task #1001 - Exploitation

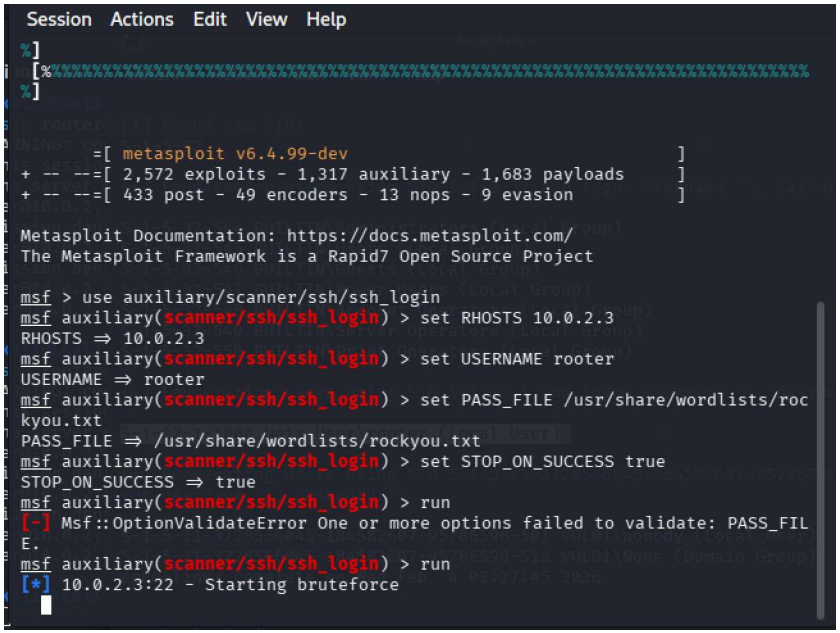
- Varied paths on the team after recon
- Brute Force
- Vulnerability Focused
- Find usernames
- SMB Enum4linux tool

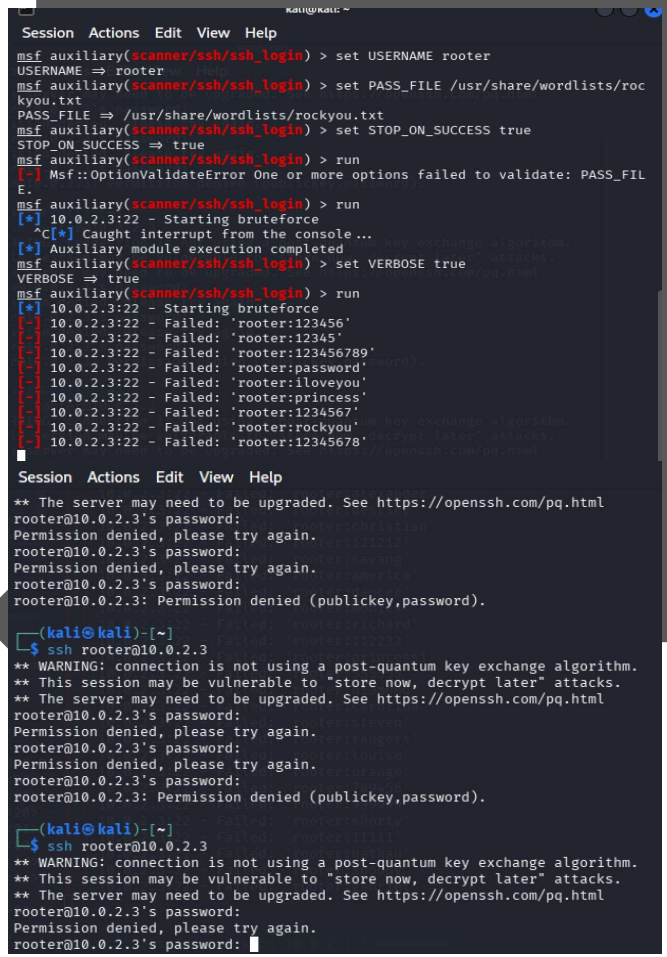
Task #1001 - Enum4linux



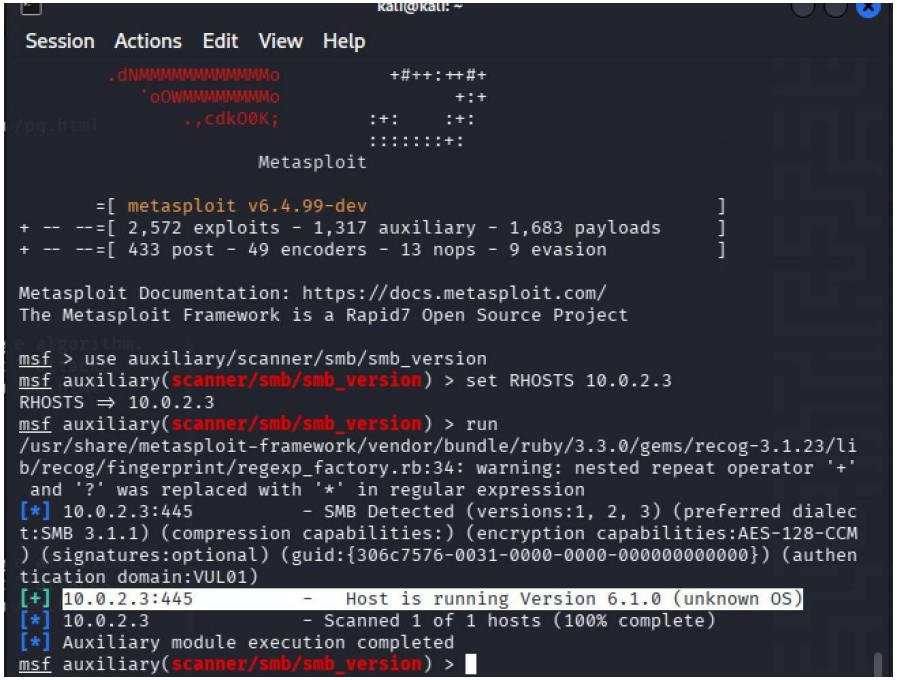


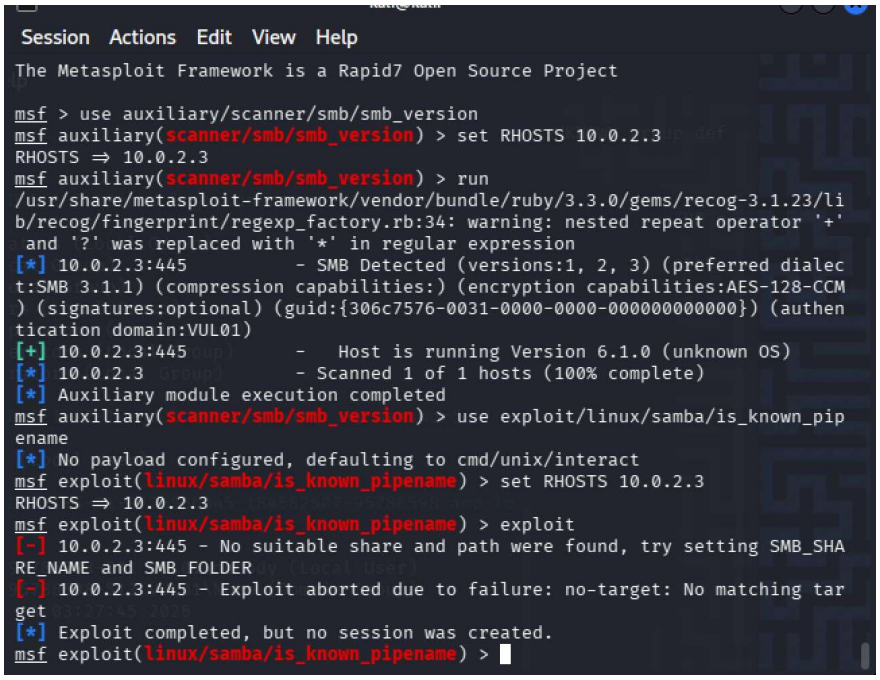
Task #1001 - Metasploit



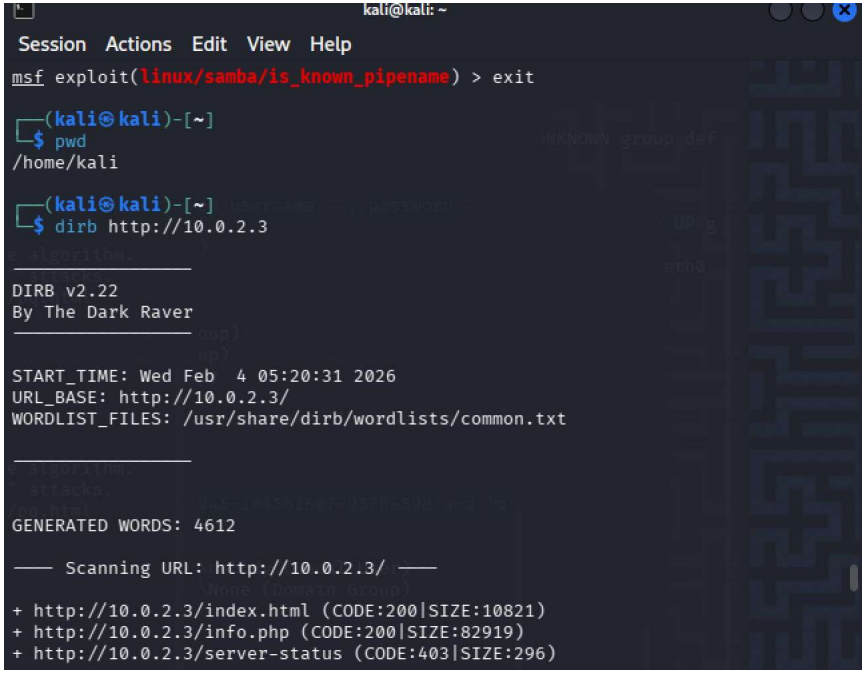


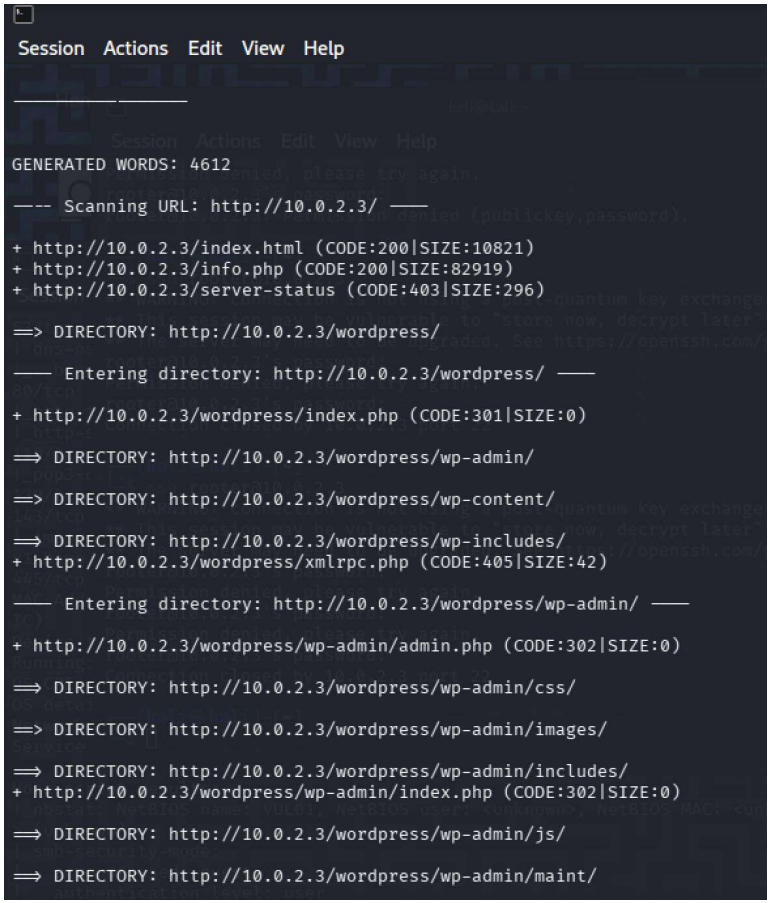
Task #1001 - SambaCry





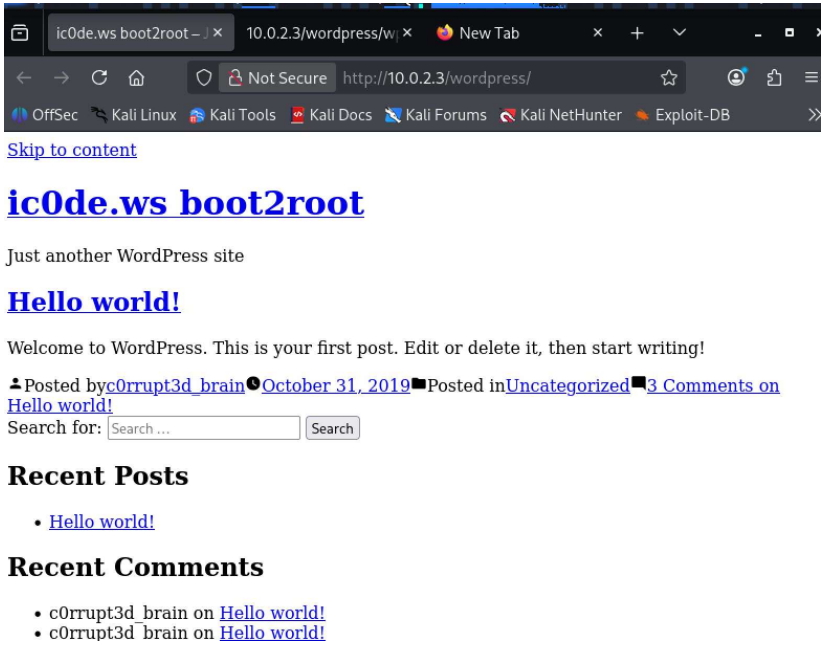
Task #1001 - Port 80 WordPress



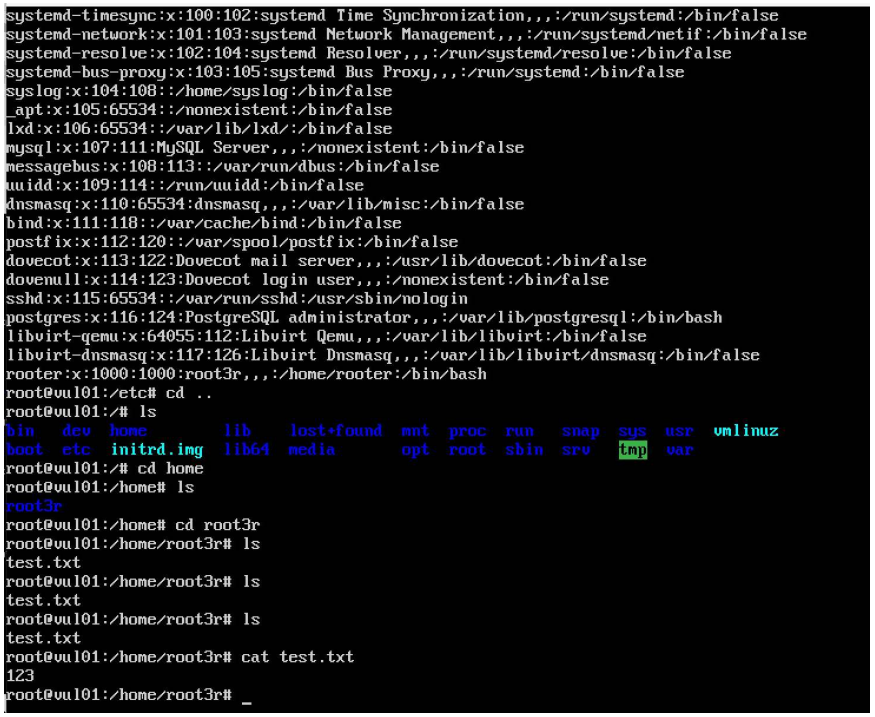


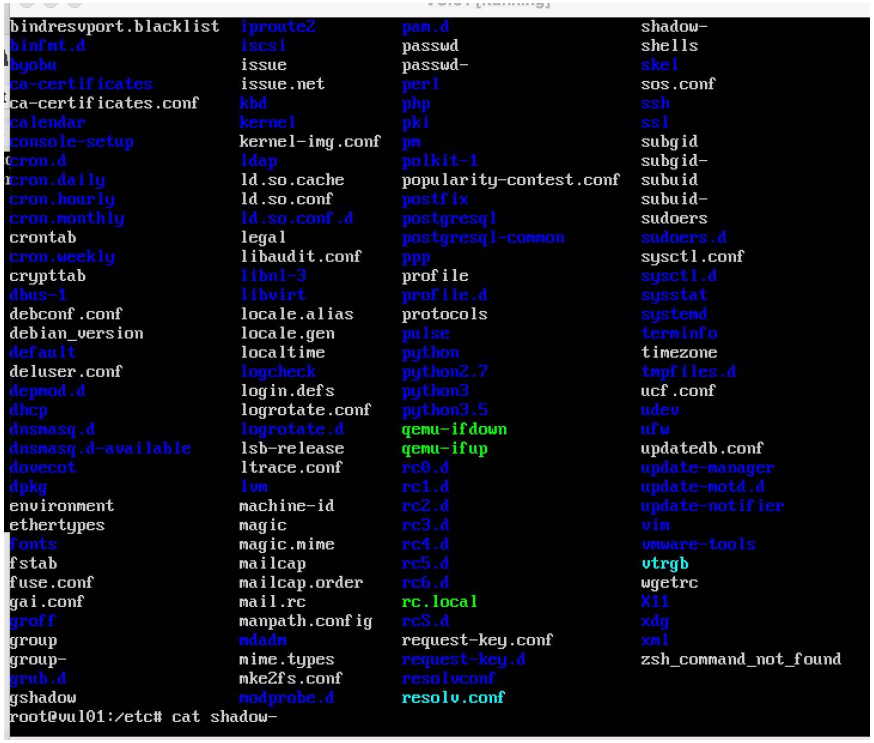
Task #1001 - WordPress Page

- VM running slow
- File directories
- Finding root

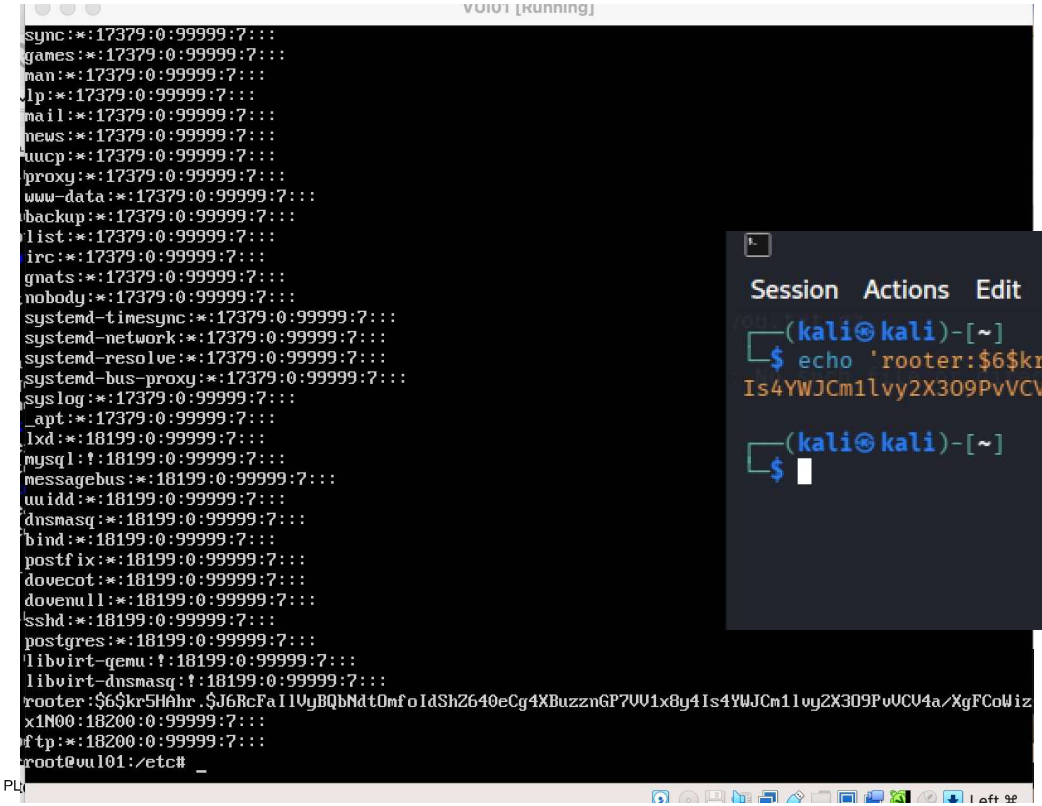


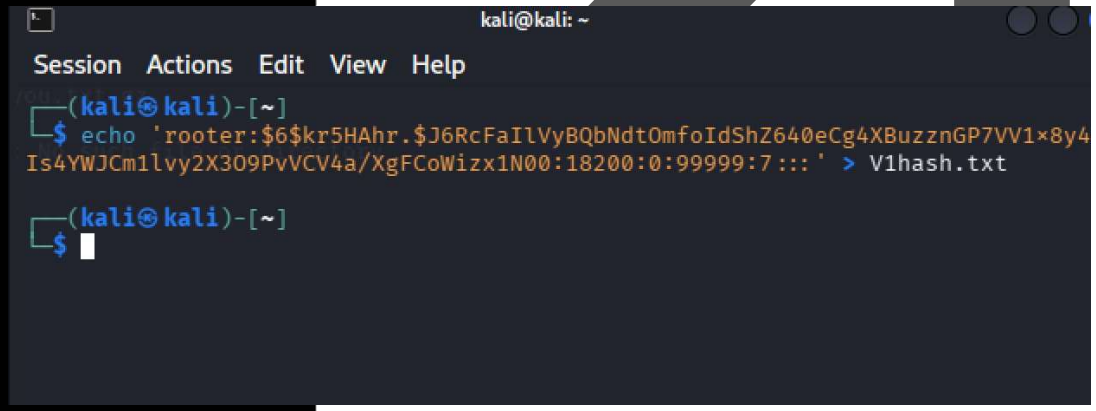
Task #1001 - Root Login/SSH Attempt



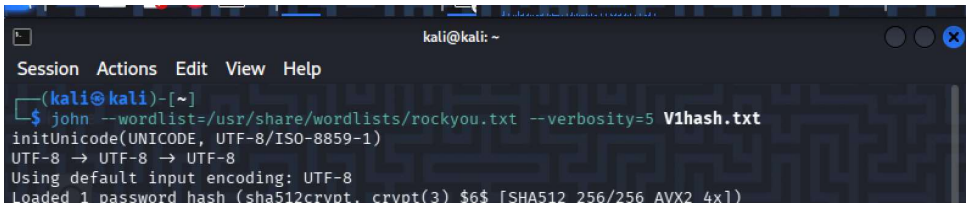


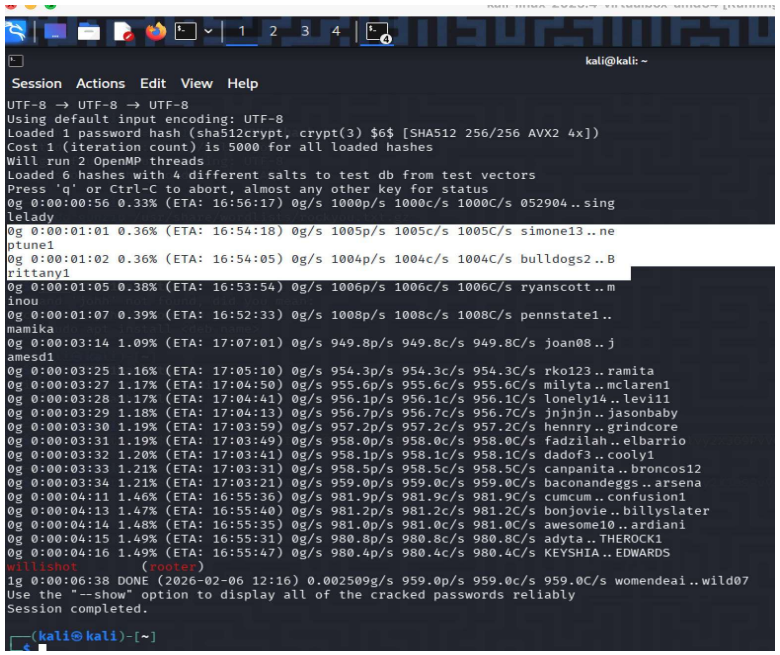
Task #1001 - Password Hash for “Rooter”

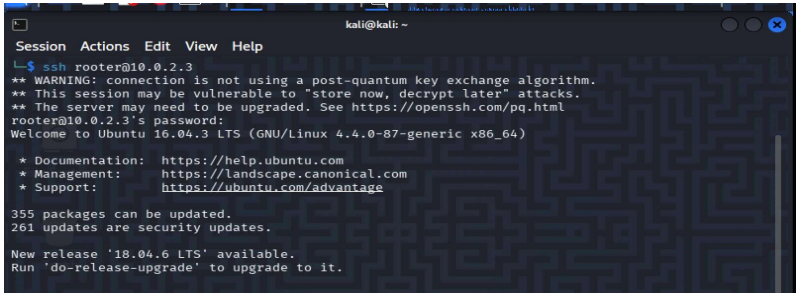


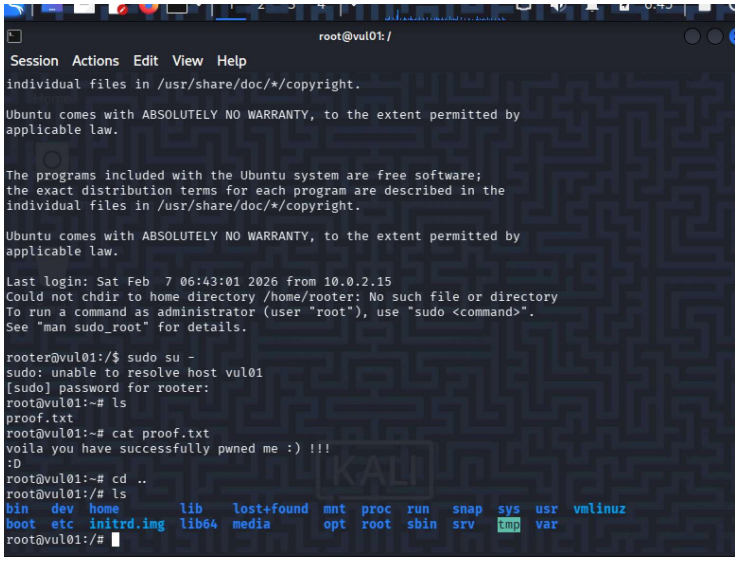


Task #1001 - Password Hash Cracking



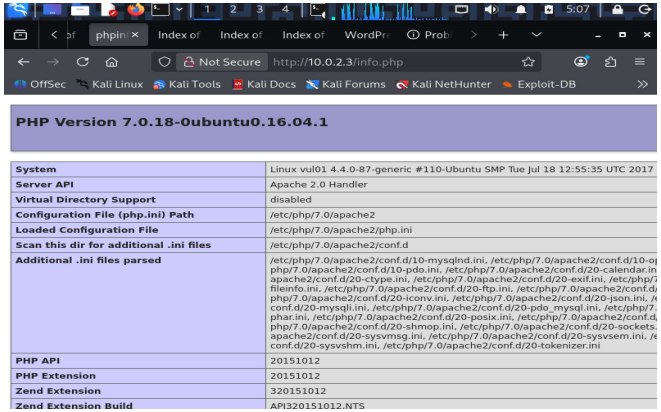


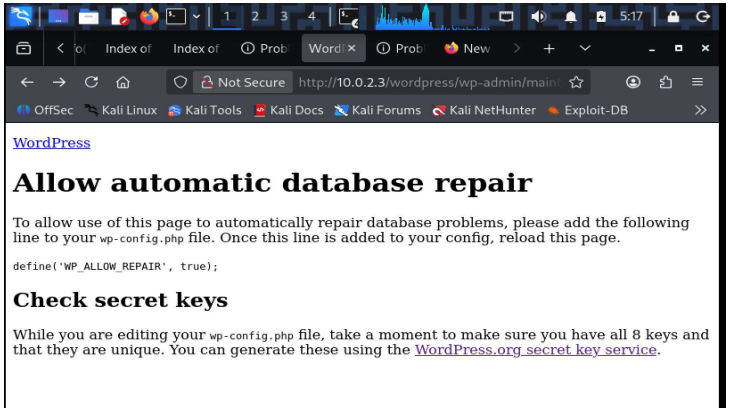


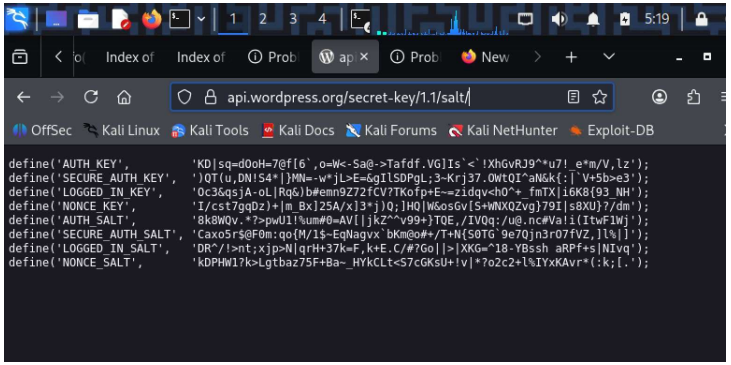


Task #1001 - Recommended Mitigations

- Implement use of “Least privileges”
- Update OpenSSH,
- Update the Apache version to 2.4.52 or higher
- Harden the security of server through configurations
- Patch all other vulnerabilities
- Implement a patch management program.
- Remove configuration info from the public facing internet:







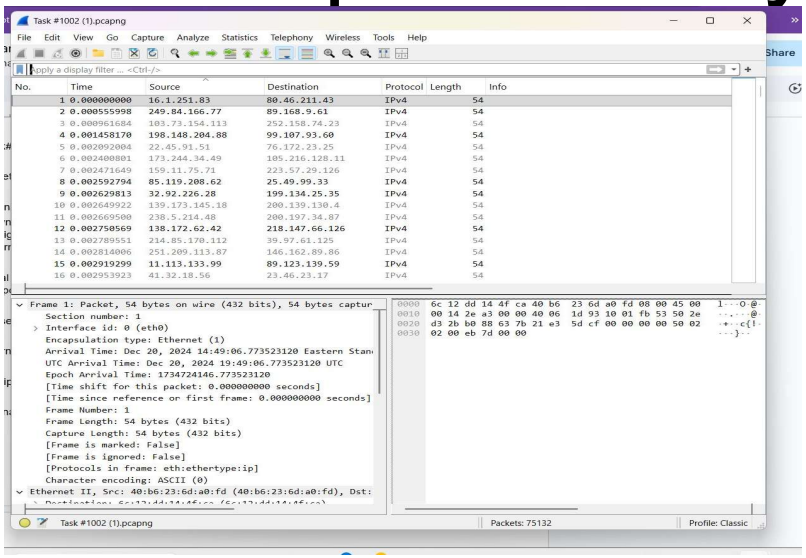
Task #1002 - Wireshark Capture Analysis

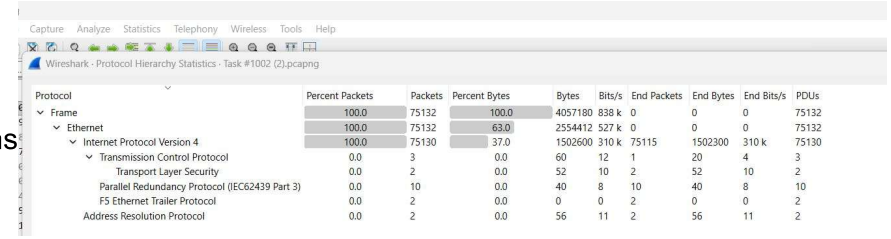
Analysis Overview

- Examined packet capture for anomalies and malicious indicators
- Identified unusual TLS handshake behavior
- Observed repeated failed connections and suspicious endpoint patterns
- Traffic suggested early-stage reconnaissance or C2 beaconing

Key Findings

- Multiple TLS Client Hello packets with no server responses
- Repeated SYN attempts to external IPs
- Asymmetric traffic patterns indicating possible scanning
- Endpoint analysis showed unusual outbound connections





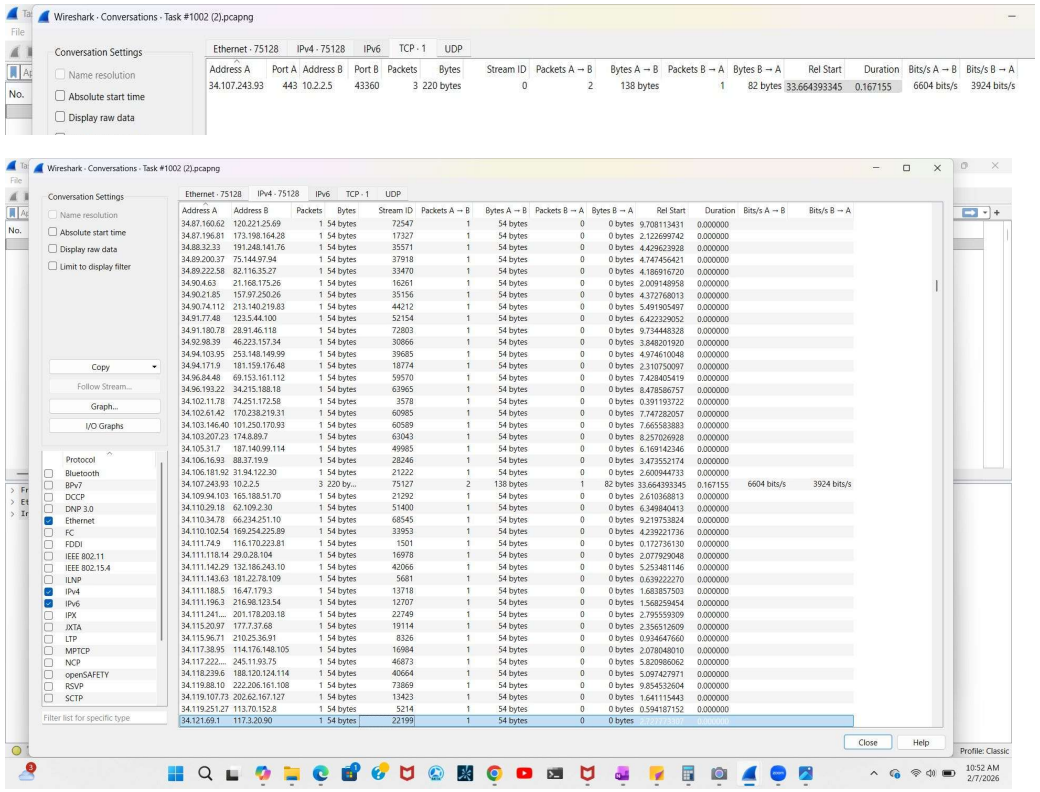
Task #1002 - Wireshark Capture Analysis cont…

Mitigations

- Enforce outbound firewall rules
- Implement TLS inspection where appropriate
- Enable IDS/IPS signatures for anomalous TLS behavior
- Monitor for repeated failed connection attempts

Recommendations Moving Forward

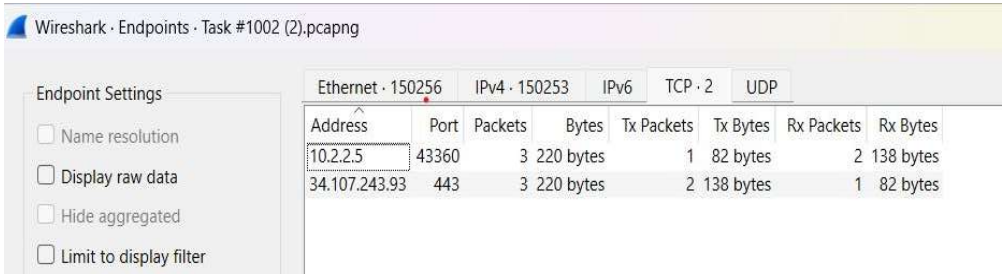
- Conduct host-based malware scan
- Review outbound traffic baselines
- Implement stricter egress filtering
- Deploy continuous monitoring for TLS anomalies



Task #1002 - Wireshark Capture Analysis cont…

Endpoint Analysis (Critical Evidence)

Endpoint statistics revealed a 3-packet TLS session between an internal host and a Google Cloud server. Although initially suspicious due to its minimal size, the traffic pattern, directionality, and byte distribution aligned with benign telemetry rather than malicious communication.



- Extremely small TLS exchange
- No payload transfer
- Directionality consistent with a failed or lightweight handshake
- Matches cloud-hosted telemetry patterns, not C2 behavior

Packet-Level Inspection

- Frame 1 showed a normal **SYN/ACK** from 93.184.216.34 → 10.0.2.15.
- TCP options (MSS, SACK, timestamps) were valid.
- No malformed fields or suspicious flags.
- No evidence of:
- SYN floods
- Beaconing
- Payload-bearing malicious packets

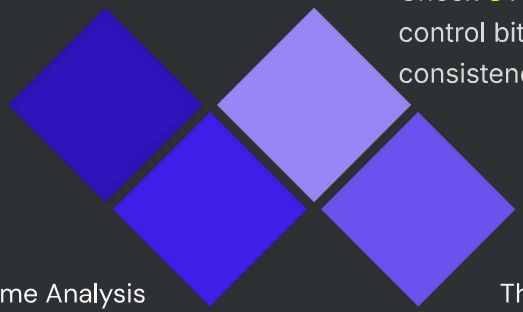
Packet-Level Inspection Results

TCP Validation

Confirm sequence, options, and window values.

Flag Verification

Check SYN/ACK and control bit consistency.



Frame Analysis

Inspect Ethernet/IP headers for anomalies.

Threat Assessment

Evaluate indicators and classify risk.

Detailed examination confirmed normal network behavior with no malicious indicators.

Frame 1 Analysis

Normal **SYN/ACK** from 93.184.216.34 → 10.0.2.15 with valid TCP options (MSS, SACK, timestamps).

No Evidence Found

- SYN floods
- Beaconing activity
- Payload-bearing malicious packets
- Malformed fields or suspicious flags

Task #1002 - Wireshark Capture Analysis cont…

Documenting Findings and Recommendations

The findings confirmed that the traffic was benign, with no indicators of compromise. Recommendations focus on strengthening monitoring practices, improving visibility into outbound TLS connections, and maintaining DNS and traffic baselines to support future investigations.

Summarized Findings

- Traffic was predominantly normal IPv4 communication.
- The 3-packet TLS session was legitimate cloud telemetry.
- No indicators of:
  - C2 communication
  - Scanning
  - Exfiltration
  - ARP spoofing
- No malicious payloads detected.

Task #1003 - Wireshark Capture Analysis

Analysis Overview

- Investigated capture containing suspicious scanning behavior
- Identified repeated SYN packets and port-scanning patterns
- Observed abnormal traffic volume from a single internal host

Key Findings

- SYN flood-like behavior targeting multiple ports
- No corresponding ACKs, indicating reconnaissance
- Internal host identified as the scanning source
- Traffic consistent with horizontal scanning

Suspicious Encrypted Outbound Communication

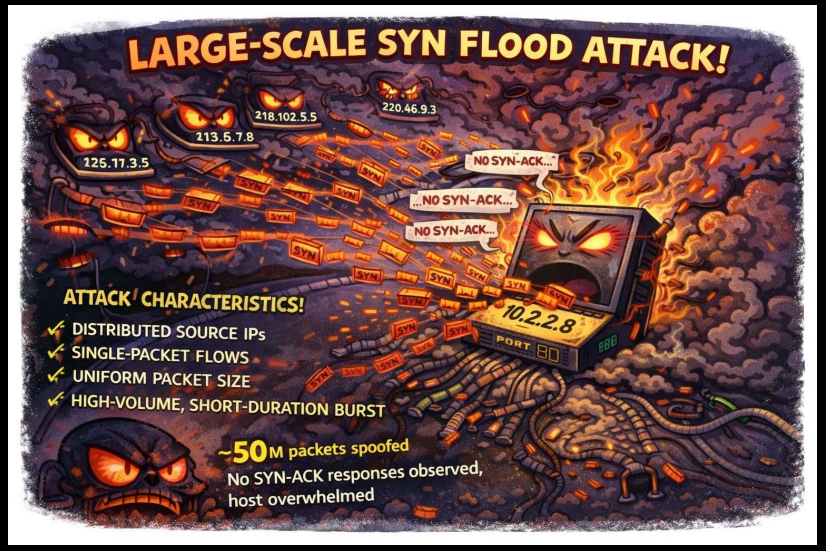
- Internal hosts **10.2.2.5** and **10.2.2.8** initiated **long-duration TLSv1.3 sessions**.
- Sessions involved **large encrypted payloads** sent to external cloud-hosted IPs.
- Behavior is consistent with:
    - Data exfiltration
    - Command-and-control (C2) communication
    - Malware beaconing

Large-Scale SYN Flood Attack

- Host **10.2.2.8** received **hundreds of thousands of spoofed SYN packets** on port 80.
- No SYN-ACK responses were observed, confirming the host was overwhelmed.
- Attack characteristics:Distributed source IPs,Single-packet flows,Uniform packet size,High-volume, short-duration burst

Task #1003 - Wireshark Capture Analysis cont…

The capture revealed two major categories of malicious activity: suspicious long-duration encrypted outbound communication from internal hosts, and a massive SYN flood attack targeting 10.2.2.8. Together, these behaviors indicate a coordinated, multi-stage intrusion involving compromise, potential data exfiltration, and deliberate service disruption.



Task #1003 (2).pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

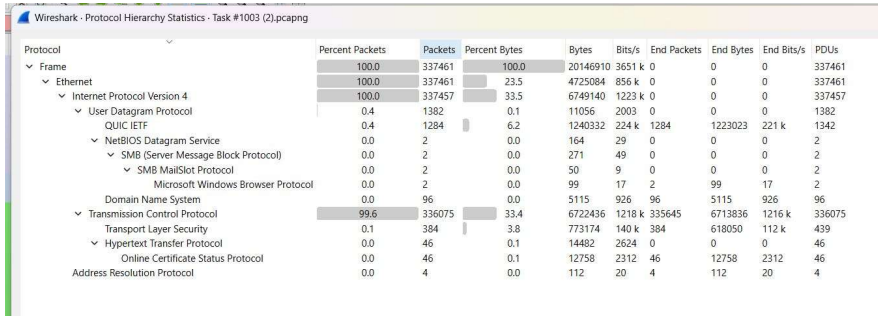
Apply a display filter ... <Ctrl-/>

	Time	Source	Destination	Protocol	Lengtl	Info
122	14.617295241	130.19.249.201	10.2.2.8	TCP	54	2989 → 80 [SYN] Seq=0 Win=512 Len=0
123	14.617302306	255.1.164.227	10.2.2.8	TCP	54	2990 → 80 [SYN] Seq=0 Win=512 Len=0
124	14.617309716	224.197.234.40	10.2.2.8	TCP	54	2991 → 80 [SYN] Seq=0 Win=512 Len=0
125	14.617316694	56.74.96.105	10.2.2.8	TCP	54	2992 → 80 [SYN] Seq=0 Win=512 Len=0
126	14.617323292	189.66.31.198	10.2.2.8	TCP	54	2993 → 80 [SYN] Seq=0 Win=512 Len=0
127	14.617331302	28.245.155.136	10.2.2.8	TCP	54	2994 → 80 [SYN] Seq=0 Win=512 Len=0
128	14.617367303	237.55.89.136	10.2.2.8	TCP	54	2995 → 80 [SYN] Seq=0 Win=512 Len=0
129	14.617377326	155.9.110.245	10.2.2.8	TCP	54	2996 → 80 [SYN] Seq=0 Win=512 Len=0
130	14.617385037	60.135.121.204	10.2.2.8	TCP	54	2997 → 80 [SYN] Seq=0 Win=512 Len=0
131	14.617526137	155.183.24.195	10.2.2.8	TCP	54	2998 → 80 [SYN] Seq=0 Win=512 Len=0
132	14.617546040	222.232.245.255	10.2.2.8	TCP	54	2999 → 80 [SYN] Seq=0 Win=512 Len=0
133	14.617588648	66.112.187.181	10.2.2.8	TCP	54	3000 → 80 [SYN] Seq=0 Win=512 Len=0
134	14.617600926	245.219.160.136	10.2.2.8	TCP	54	3001 → 80 [SYN] Seq=0 Win=512 Len=0
135	14.617613128	60.130.222.150	10.2.2.8	TCP	54	3002 → 80 [SYN] Seq=0 Win=512 Len=0
136	14.617657836	119.164.26.24	10.2.2.8	TCP	54	3003 → 80 [SYN] Seq=0 Win=512 Len=0
137	14.617668332	104.93.155.97	10.2.2.8	TCP	54	3004 → 80 [SYN] Seq=0 Win=512 Len=0
138	14.617727443	192.125.19.106	10.2.2.8	TCP	54	3005 → 80 [SYN] Seq=0 Win=512 Len=0
139	14.617745837	238.183.164.75	10.2.2.8	TCP	54	3006 → 80 [SYN] Seq=0 Win=512 Len=0
140	14.617784740	157.195.204.198	10.2.2.8	TCP	54	3007 → 80 [SYN] Seq=0 Win=512 Len=0

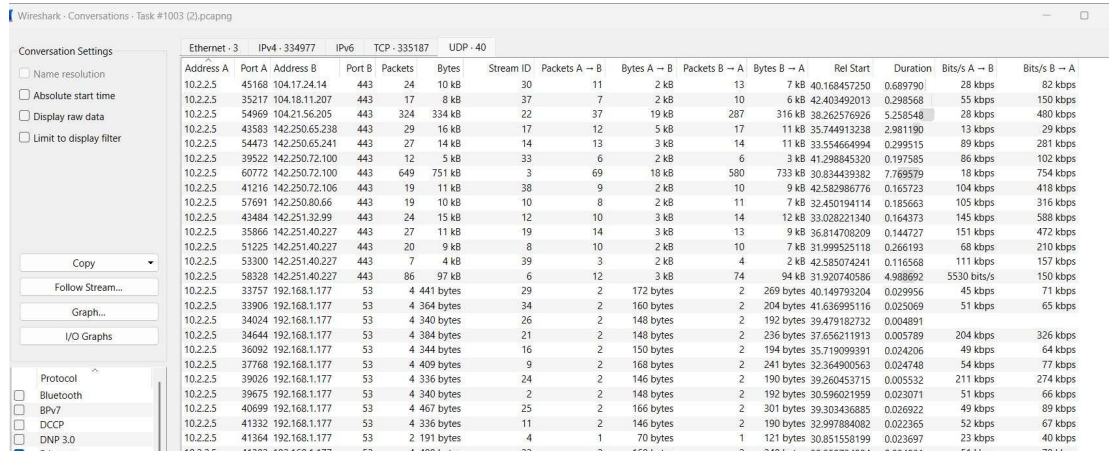
```
Frame 3: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
    Section number: 1
  > Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec 20, 2024 15:19:10.517584110 Eastern Standard Time
    UTC Arrival Time: Dec 20, 2024 20:19:10.517584110 UTC
    Epoch Arrival Time: 1734725950.517584110
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 9.003414 milliseconds]
    [Time delta from previous displayed frame: 9.003414 milliseconds]
    [Time since reference or first frame: 31.809251 milliseconds]
    Frame Number: 3
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
```

```
0000  52 54 00 12
0010  00 3c 5c 4e
0020  a5 11 e3 0e
0030  fa f0 d3 6a
0040  33 28 00 00
```

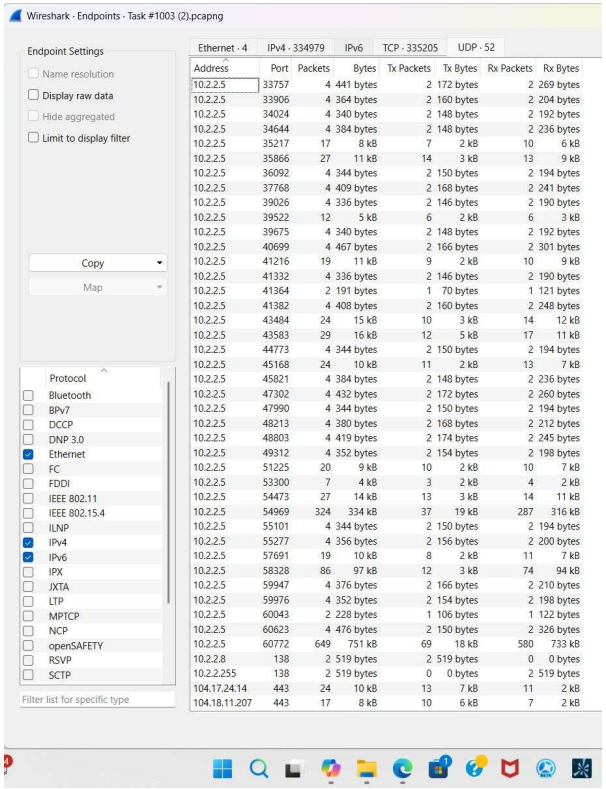
Task #1003 - Wireshark Capture Analysis cont…



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	337461	100.0	20146910	3651 k	0	0	0	337461
Ethernet	100.0	337461	23.5	4725084	856 k	0	0	0	337461
Internet Protocol Version 4	100.0	337457	33.5	6749140	1223 k	0	0	0	337457
User Datagram Protocol	0.4	1382	0.1	11056	2003	0	0	0	1382
QUIC IETF	0.4	1284	6.2	1240332	224 k	1284	1223023	221 k	1342
NetBIOS Datagram Service	0.0	2	0.0	164	29	0	0	0	2
SMB (Server Message Block Protocol)	0.0	2	0.0	271	49	0	0	0	2
SMB MailSlot Protocol	0.0	2	0.0	50	9	0	0	0	2
Microsoft Windows Browser Protocol	0.0	2	0.0	99	17	2	99	17	2
Domain Name System	0.0	96	0.0	5115	926	96	5115	926	96
Transmission Control Protocol	99.6	336075	33.4	6722436	1218 k	335645	6713836	1216 k	336075
Transport Layer Security	0.1	384	3.8	773174	140 k	384	618050	112 k	439
Hypertext Transfer Protocol	0.0	46	0.1	14482	2624	0	0	0	46
Online Certificate Status Protocol	0.0	46	0.1	12758	2312	46	12758	2312	46
Address Resolution Protocol	0.0	4	0.0	112	20	4	112	20	4



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.2.2.5	45168	104.17.24.14	443	24	10 kB	30	11	2 kB	13	7 kB	40.168457250	0.689790	28 kbps	82 kbps
10.2.2.5	35217	104.18.11.207	443	17	8 kB	37	7	2 kB	10	6 kB	42.403492013	0.298568	55 kbps	150 kbps
10.2.2.5	54969	104.21.56.205	443	324	334 kB	22	37	19 kB	287	316 kB	38.262576926	5.258548	28 kbps	480 kbps
10.2.2.5	43583	142.250.65.238	443	29	16 kB	17	12	5 kB	17	11 kB	35.744913238	2.981190	13 kbps	29 kbps
10.2.2.5	54473	142.250.65.241	443	27	14 kB	14	13	3 kB	14	11 kB	33.554664994	0.299515	89 kbps	281 kbps
10.2.2.5	39522	142.250.72.100	443	12	5 kB	33	6	2 kB	6	3 kB	41.298845320	0.197585	86 kbps	102 kbps
10.2.2.5	60772	142.250.72.100	443	649	751 kB	3	69	18 kB	580	733 kB	30.834439382	7.769579	18 kbps	754 kbps
10.2.2.5	41216	142.250.72.106	443	19	11 kB	38	9	2 kB	10	9 kB	42.582986776	0.165723	104 kbps	418 kbps
10.2.2.5	57691	142.250.80.66	443	19	10 kB	10	8	2 kB	11	7 kB	32.450194114	0.185663	105 kbps	316 kbps
10.2.2.5	43484	142.251.32.99	443	24	15 kB	12	10	3 kB	14	12 kB	33.028221340	0.164373	145 kbps	588 kbps
10.2.2.5	35866	142.251.40.227	443	27	11 kB	19	14	3 kB	13	9 kB	36.814708209	0.144727	151 kbps	472 kbps
10.2.2.5	51225	142.251.40.227	443	20	9 kB	8	10	2 kB	10	7 kB	31.999525118	0.266193	68 kbps	210 kbps
10.2.2.5	53300	142.251.40.227	443	7	4 kB	39	3	2 kB	4	2 kB	42.585074241	0.116568	111 kbps	157 kbps
10.2.2.5	58328	142.251.40.227	443	86	97 kB	6	12	3 kB	74	94 kB	31.920740586	4.988692	5530 bits/s	150 kbps
10.2.2.5	33757	192.168.1.177	53	4	441 bytes	29	2	172 bytes	2	269 bytes	40.149793204	0.029956	45 kbps	71 kbps
10.2.2.5	33906	192.168.1.177	53	4	364 bytes	34	2	160 bytes	2	204 bytes	41.636995116	0.025069	51 kbps	65 kbps
10.2.2.5	34024	192.168.1.177	53	4	340 bytes	26	2	148 bytes	2	192 bytes	39.479182732	0.004891		
10.2.2.5	34644	192.168.1.177	53	4	384 bytes	21	2	148 bytes	2	236 bytes	37.656211913	0.005789	204 kbps	326 kbps
10.2.2.5	36092	192.168.1.177	53	4	344 bytes	16	2	150 bytes	2	194 bytes	35.719099391	0.024206	49 kbps	64 kbps
10.2.2.5	37768	192.168.1.177	53	4	409 bytes	9	2	168 bytes	2	241 bytes	32.364900563	0.024748	54 kbps	77 kbps
10.2.2.5	39026	192.168.1.177	53	4	336 bytes	24	2	146 bytes	2	190 bytes	39.260453715	0.005532	211 kbps	274 kbps
10.2.2.5	39675	192.168.1.177	53	4	340 bytes	2	2	148 bytes	2	192 bytes	30.596021959	0.023071	51 kbps	66 kbps
10.2.2.5	40699	192.168.1.177	53	4	467 bytes	25	2	166 bytes	2	301 bytes	39.303436885	0.026922	49 kbps	89 kbps
10.2.2.5	41332	192.168.1.177	53	4	336 bytes	11	2	146 bytes	2	190 bytes	32.997884082	0.022365	52 kbps	67 kbps
10.2.2.5	41364	192.168.1.177	53	2	191 bytes	4	1	70 bytes	1	121 bytes	30.851558199	0.023697	23 kbps	40 kbps



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.2.2.5	33757	4	441 bytes	2	172 bytes	2	269 bytes
10.2.2.5	33906	4	364 bytes	2	160 bytes	2	204 bytes
10.2.2.5	34024	4	340 bytes	2	148 bytes	2	192 bytes
10.2.2.5	34644	4	384 bytes	2	148 bytes	2	236 bytes
10.2.2.5	35217	17	8 kB	7	2 kB	10	6 kB
10.2.2.5	35866	27	11 kB	14	3 kB	13	9 kB
10.2.2.5	36092	4	344 bytes	2	150 bytes	2	194 bytes
10.2.2.5	37768	4	409 bytes	2	168 bytes	2	241 bytes
10.2.2.5	39026	4	336 bytes	2	146 bytes	2	190 bytes
10.2.2.5	39522	12	5 kB	6	2 kB	6	3 kB
10.2.2.5	39675	4	340 bytes	2	148 bytes	2	192 bytes
10.2.2.5	40699	4	467 bytes	2	166 bytes	2	301 bytes
10.2.2.5	41216	19	11 kB	9	2 kB	10	9 kB
10.2.2.5	41332	4	336 bytes	2	146 bytes	2	190 bytes
10.2.2.5	41364	2	191 bytes	1	70 bytes	1	121 bytes
10.2.2.5	41382	4	408 bytes	2	160 bytes	2	248 bytes
10.2.2.5	43484	24	15 kB	10	3 kB	14	12 kB
10.2.2.5	43583	29	16 kB	12	5 kB	17	11 kB
10.2.2.5	44773	4	344 bytes	2	150 bytes	2	194 bytes
10.2.2.5	45168	24	10 kB	11	2 kB	13	7 kB
10.2.2.5	45821	4	384 bytes	2	148 bytes	2	236 bytes
10.2.2.5	47302	4	432 bytes	2	172 bytes	2	260 bytes
10.2.2.5	47990	4	344 bytes	2	150 bytes	2	194 bytes
10.2.2.5	48213	4	380 bytes	2	168 bytes	2	212 bytes
10.2.2.5	48803	4	419 bytes	2	174 bytes	2	245 bytes
10.2.2.5	49312	4	352 bytes	2	154 bytes	2	198 bytes
10.2.2.5	51225	20	9 kB	10	2 kB	10	7 kB
10.2.2.5	53300	7	4 kB	3	2 kB	4	2 kB
10.2.2.5	54473	27	14 kB	13	3 kB	14	11 kB
10.2.2.5	54969	324	334 kB	37	19 kB	287	316 kB
10.2.2.5	55101	4	344 bytes	2	150 bytes	2	194 bytes
10.2.2.5	55277	4	356 bytes	2	156 bytes	2	200 bytes
10.2.2.5	57691	19	10 kB	8	2 kB	11	7 kB
10.2.2.5	58328	86	97 kB	12	3 kB	74	94 kB
10.2.2.5	59947	4	376 bytes	2	166 bytes	2	210 bytes
10.2.2.5	59976	4	352 bytes	2	154 bytes	2	198 bytes
10.2.2.5	60043	2	228 bytes	1	106 bytes	1	122 bytes
10.2.2.5	60623	4	476 bytes	2	150 bytes	2	326 bytes
10.2.2.5	60772	649	751 kB	69	18 kB	580	733 kB
10.2.2.8	138	2	519 bytes	2	519 bytes	0	0 bytes
10.2.2.255	138	2	519 bytes	0	0 bytes	2	519 bytes
104.17.24.14	443	24	10 kB	13	7 kB	11	2 kB
104.18.11.207	443	17	8 kB	10	6 kB	7	2 kB

Task #1003 - Wireshark Capture Analysis cont…

Controls and Mitigation Recommendations

To prevent similar multi-stage attacks, the organization must strengthen both inbound and outbound controls, improve monitoring visibility, and deploy protections against denial-of-service attacks and encrypted malicious communication.

- **SYN Flood Mitigation**
  - Enable SYN cookies
  - Apply rate limiting
  - Filter spoofed IP ranges at the firewall
- **Outbound Traffic Controls**
  - Implement strict egress filtering
  - Monitor for abnormal TLS patterns
  - Deploy TLS inspection where appropriate
- **Detection & Monitoring**
  - Deploy IDS/IPS to detect C2 and DoS activity
  - Enable detailed logging across internal hosts
  - Monitor for long-duration encrypted sessions
- **Hardening Measures**
  - Patch vulnerable systems
  - Segment internal networks
  - Limit lateral movement opportunities

Key Takeaways

- Internal hosts were likely compromised before the DoS attack.
- Encrypted outbound traffic suggests possible exfiltration or C2 activity.
- SYN flood attack indicates deliberate service disruption.
- Implementing recommended controls will significantly improve network resilience.

Task #1004 - Wireshark Capture Analysis

Percentage of total Packets found by Protocol:

IPv6: 83.6% of traffic : Internet Control Message Protocol (ICMP)

IPv4: 16.4% of traffic :

UDP(16.1%)

→Quick UDP internet Connections Protocol (QUIC IETF) 16.0%

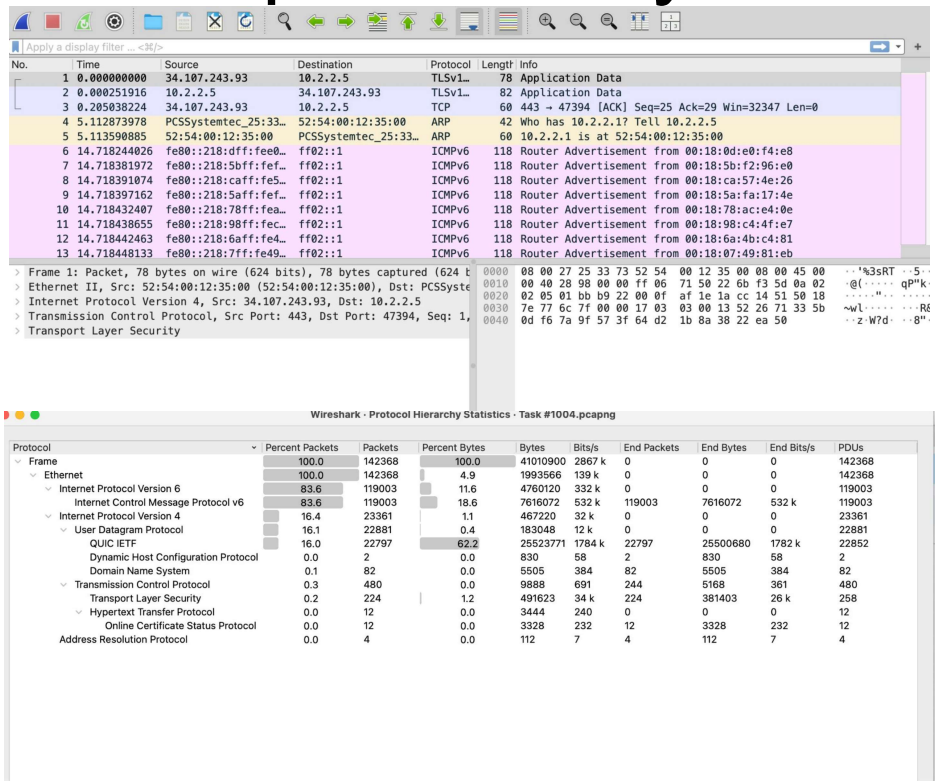
→Domain Name System (DNS) 0.1% TCP(0.3%)

→Transport Layer Security (TLS) 0.2%

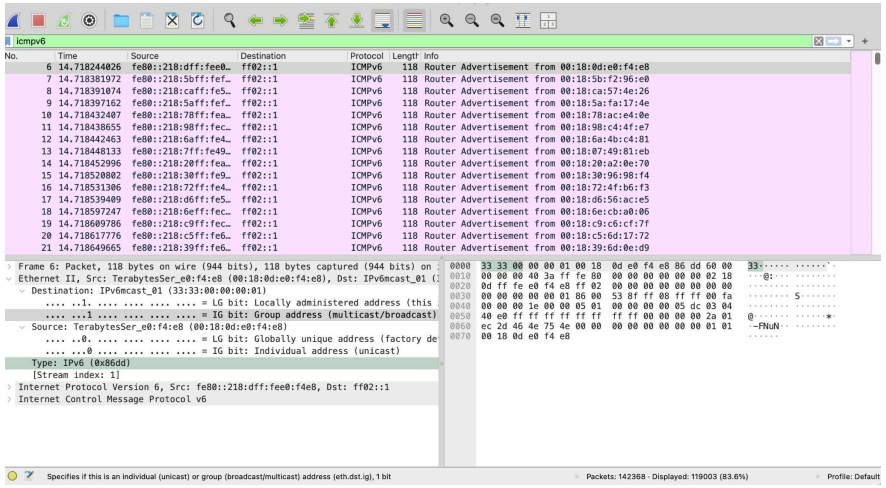
→ Hyper Text Transfer Protocol (HTTP) Address Resolution Protocol (ARP) <0.1%

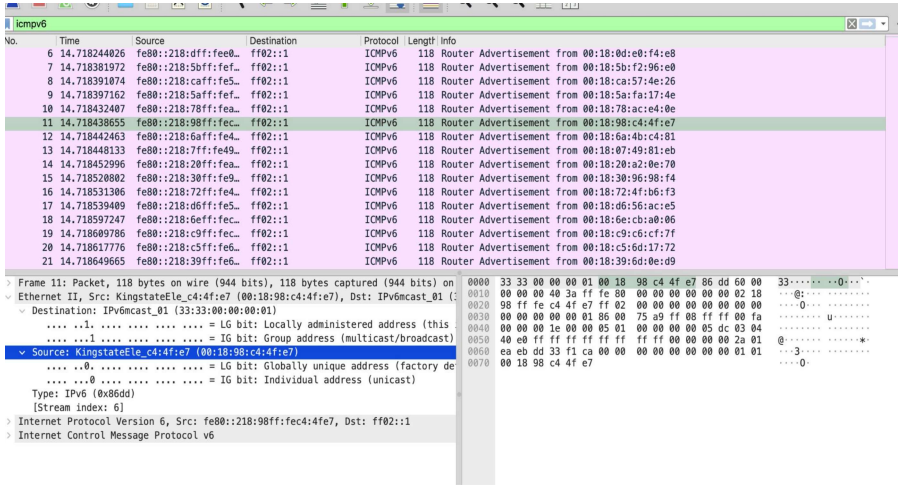
Largest Data Amounts by Protocol:

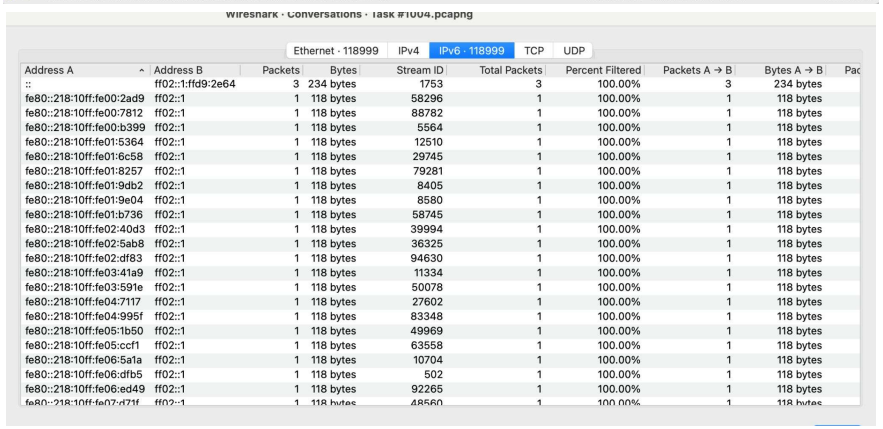
ICMP: 18.6% QUIC IETF: 62%

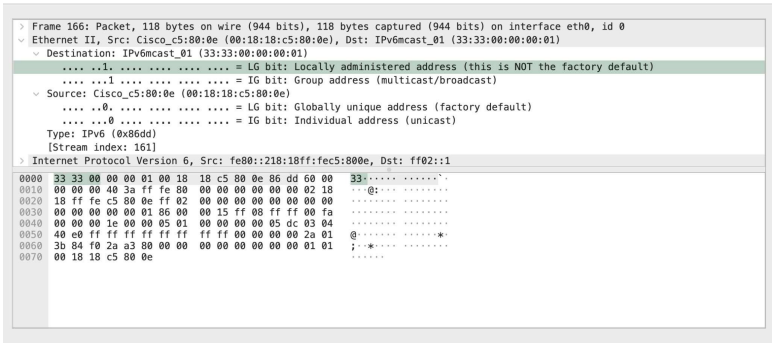


Task #1004 - ICMP Investigation





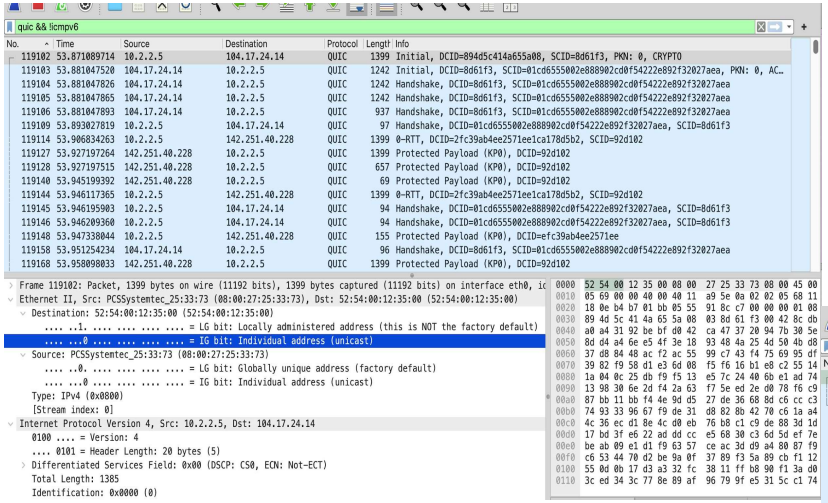


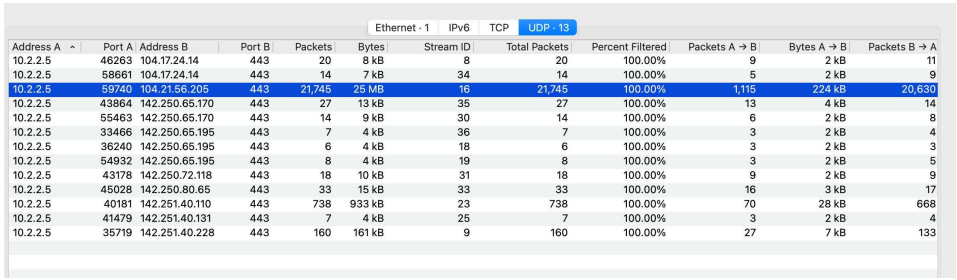


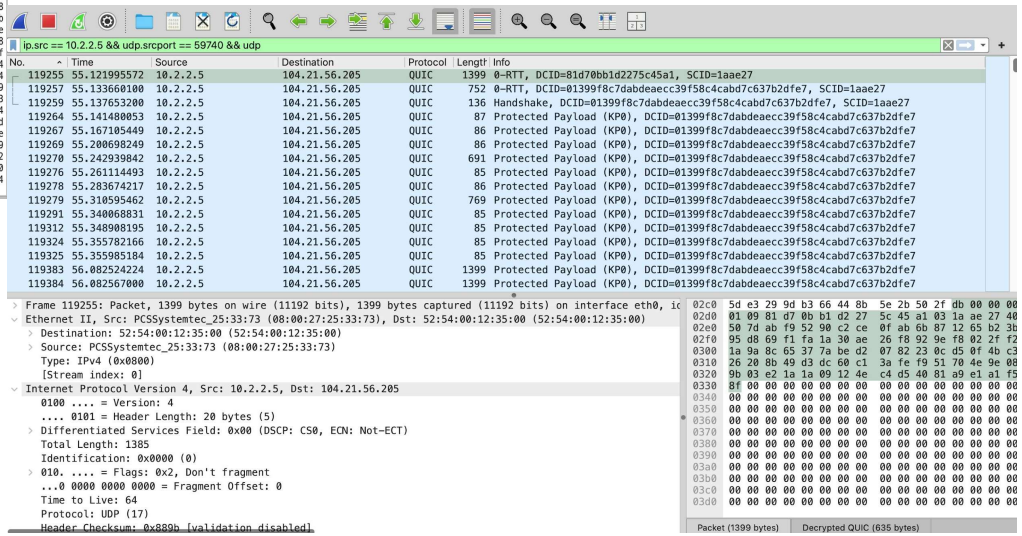
Task #1004 - ICMP Findings

- Nature of the attack?
- Router Advertisements to ff02::1
- Spoofing
- RA Flood
- Suspected Devic Source: PCSsystemtec…(10.2.2.5)
- Distraction?

Task #1004 - QUIC Investigation

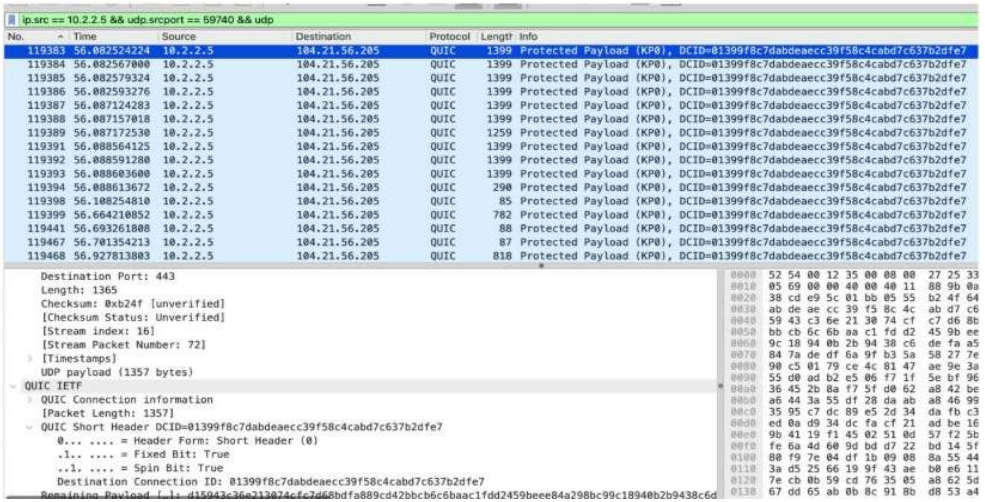




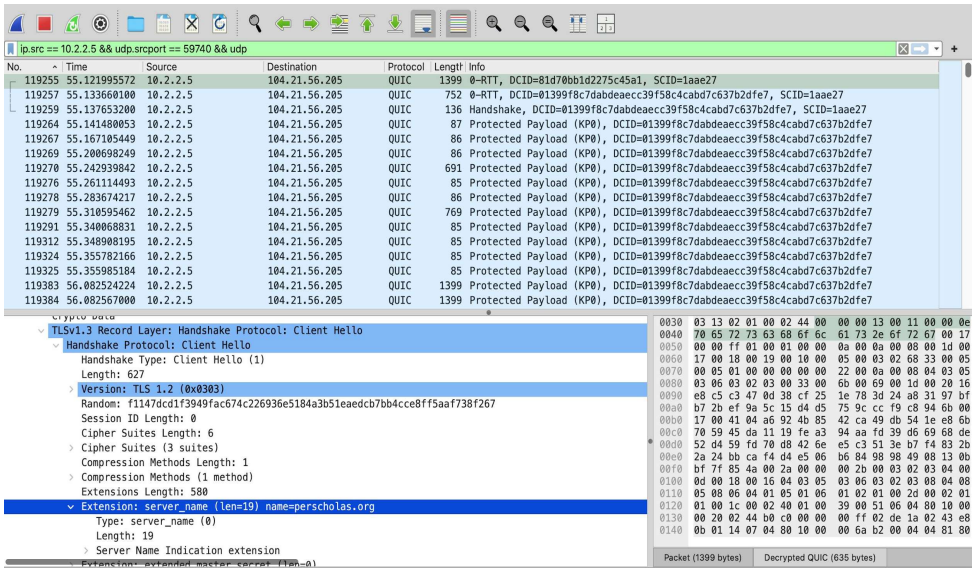


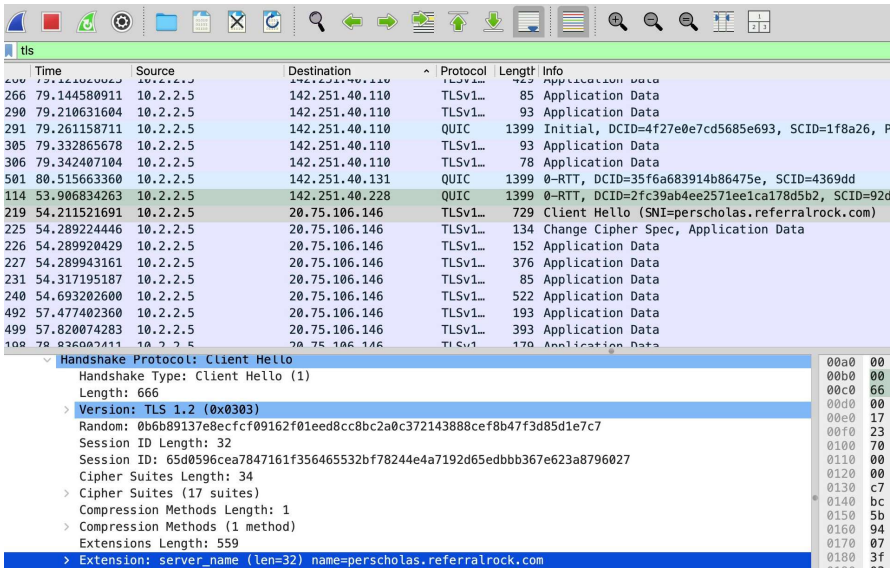
Task #1004 - QUIC Findings

- Multiple packets sizes of 1399 bytes from source IP 10.2.2.5:59740 (PCSSystemtec..) to destination IP address 104.21.56.205:443 (CloudFlare IP)
- Raw data exfiltration?
- You can see the encrypted payload (TLS 1.3) in the QUIC Short Header below:



Task #1004 - Interesting findings





Task #1004 - Summary/Mitigations

- The ICMP indicates an RA Flood DOS attack
- The QUIC traffic indicates a possible data exfiltration
- Exfiltration Mitigations:
  - Isolate the 10.2.2.5 machine, remove it from the network, and image the disk. Next, find what service is using port 59470 on the machine. Look for signs of persistence by checking important folders where malware hides, startup folders, and browser extensions. Lastly, update the firewall rules.
- RA flood Mitigations:
  - RA guard on the switch.
  - Port security with MAC limiting.
  - Disabling unused ports

Task 5 Wireshark Investigation Methodology

01

Baseline Inspection

Initial packet capture review to identify anomalies

02

Protocol Filtering

Systematic isolation of DNS, QUIC, and Layer-2 traffic

03

Temporal Analysis

I/O graph correlation to pinpoint attack timing

04

Deep Packet Inspection

Examination of packet contents for attack signatures

05

Hypothesis Testing

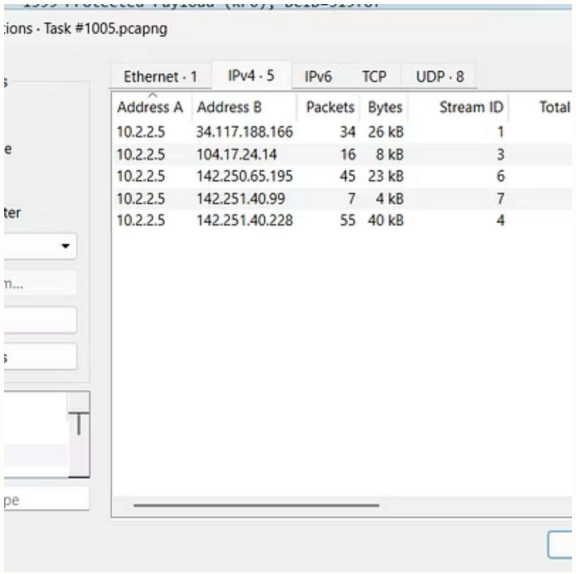
Validation of attack attribution and impact

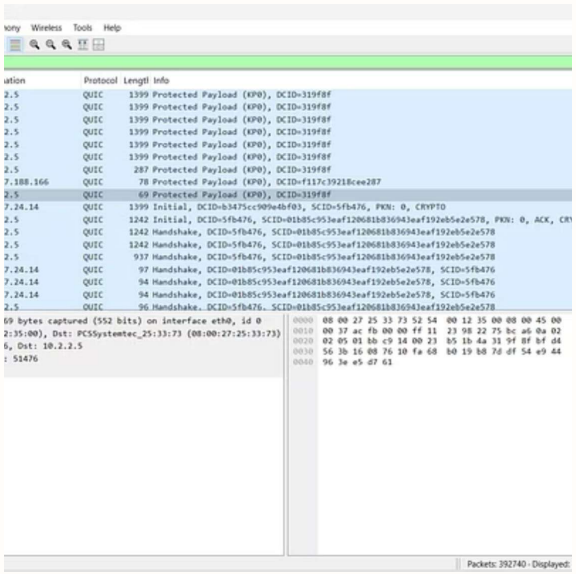
06

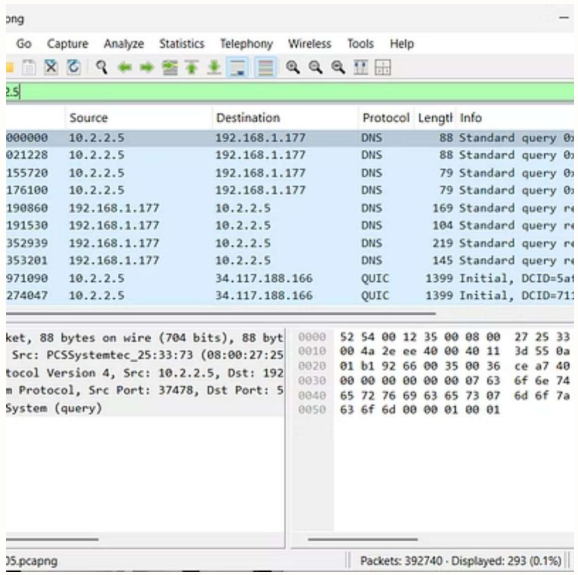
Mitigation Planning

Development of defensive recommendations

Protocol Analysis: DNS, QUIC, and IPv4 Traffic Patterns

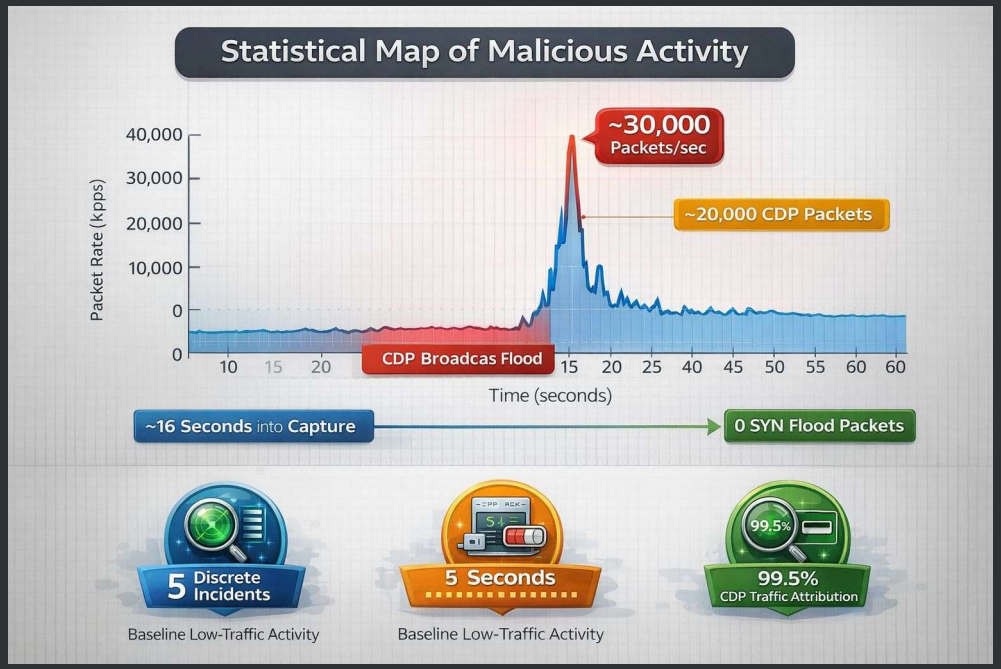


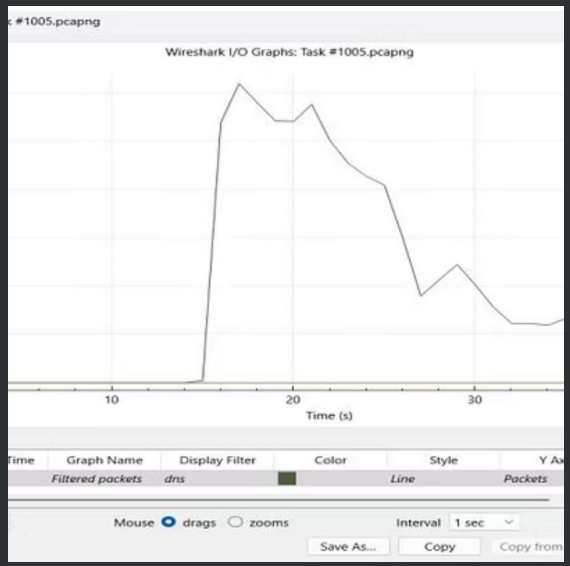




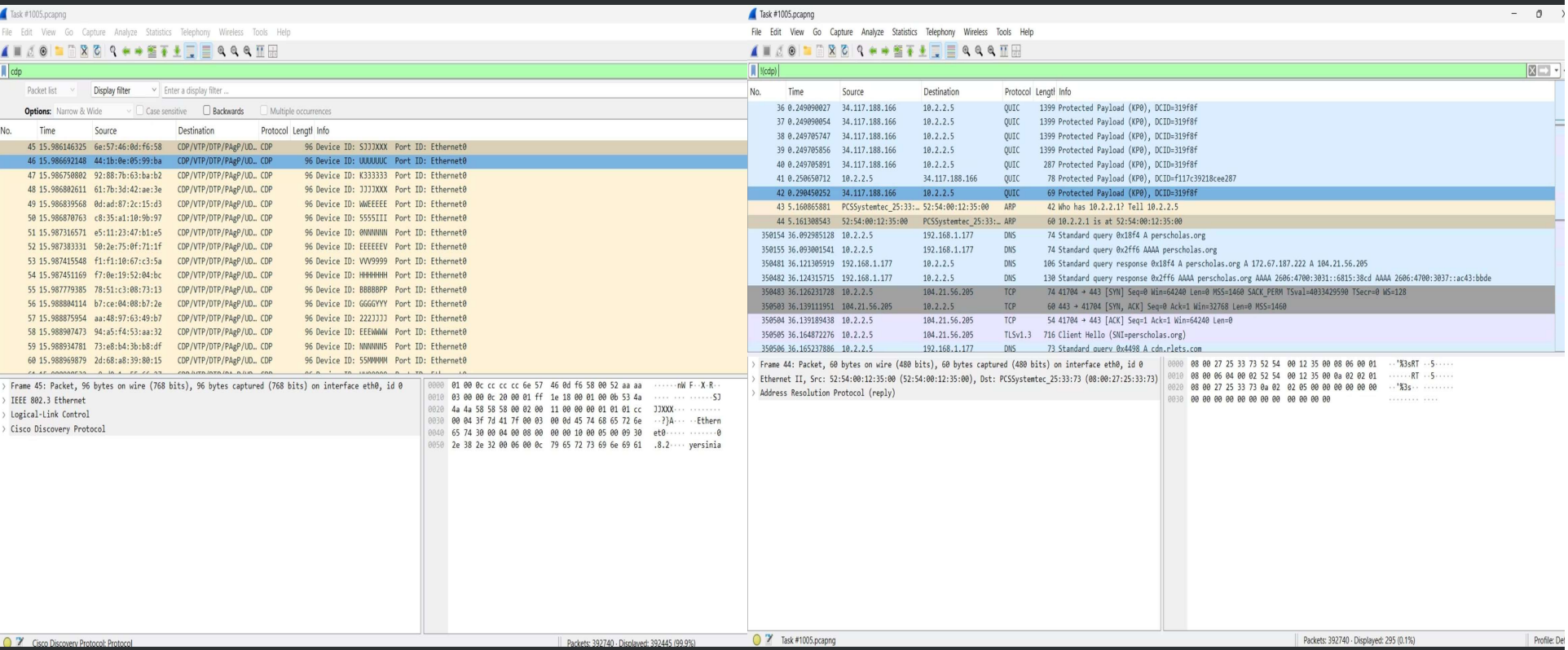
These Wireshark captures illustrate the protocol filtering analysis performed to isolate DNS, QUIC, and IPv4 traffic. By systematically examining these protocols, we confirmed that the network anomaly was not related to common attack vectors involving these layers, thereby narrowing down the scope of the investigation.

Wireshark Evidence





I/O graphs and protocol filtering confirmed the CDP flood pattern, with temporal correlation showing the attack concentrated at the 15-16 second mark.



CDP Protocol Analysis - Detailed View

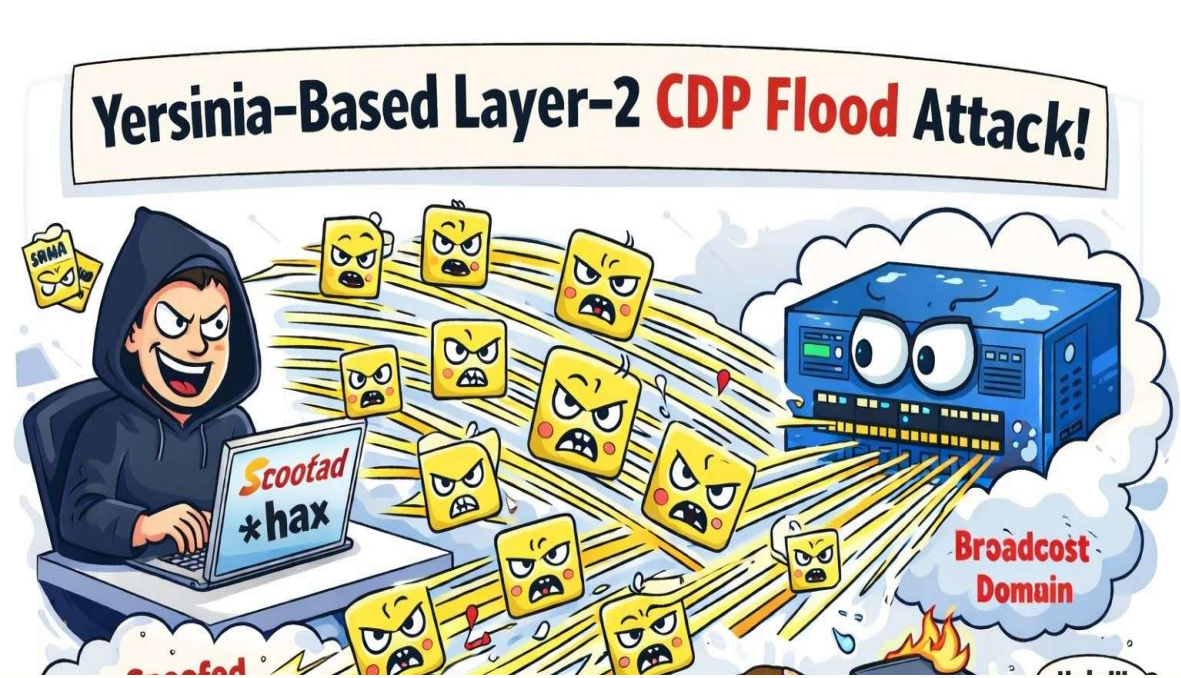
Simple CDP filter confirming the high volume of invalid CDP advertisements that contributed to the broadcast storm during the attack.

Packet Capture Timeline - Attack Sequence

This Wireshark view shows clustered CDP packets aligning with the attack timeline, confirming broadcast storm activity.

⚠ ATTACK IDENTIFIED

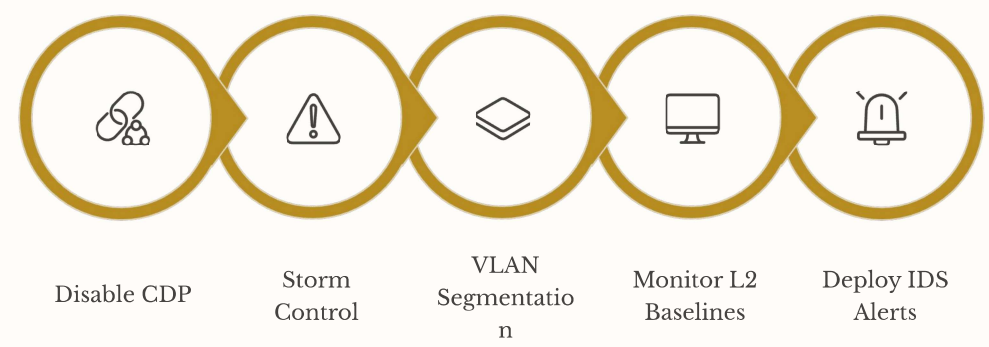
Attack Attribution: Yersinia Framework



Yersinia Framework

A specialized Layer-2 attack tool designed to exploit network protocols including CDP, STP, and DHCP through packet injection and spoofing techniques.

Mitigation Recommendations



A comprehensive defense-in-depth approach combining protocol hardening, network segmentation, and continuous monitoring.

Immediate Actions

Traffic Controls

Enable broadcast storm control thresholds

Network Segmentation

Monitoring

Deploy IDS signatures for Layer-2 anomalies

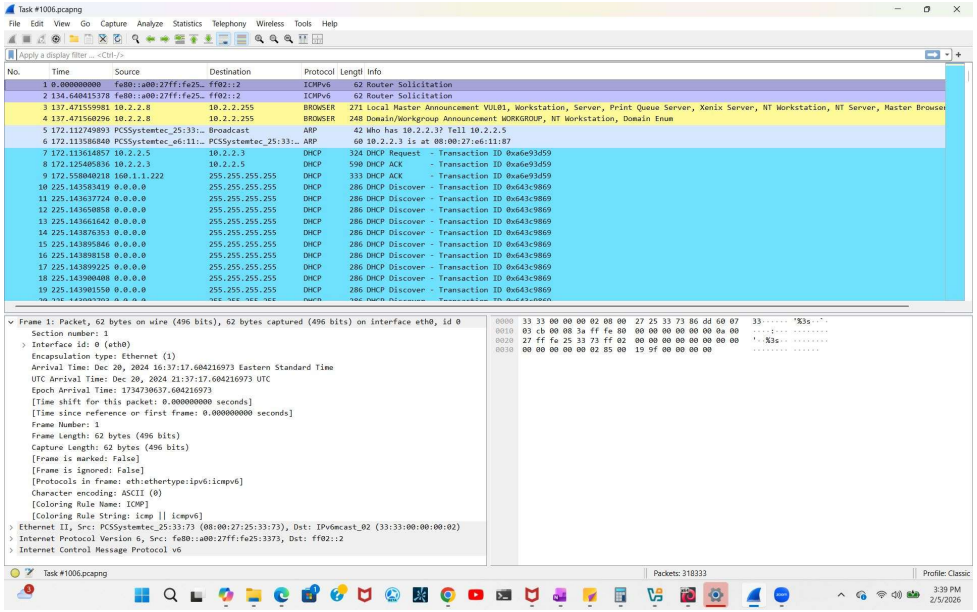
Task #1006 - Wireshark Capture Analysis

Analysis Overview

- Analyzed capture dominated by DHCP traffic
- Identified repeated DHCP Discover packets
- Observed broadcast storm consistent with DHCP starvation

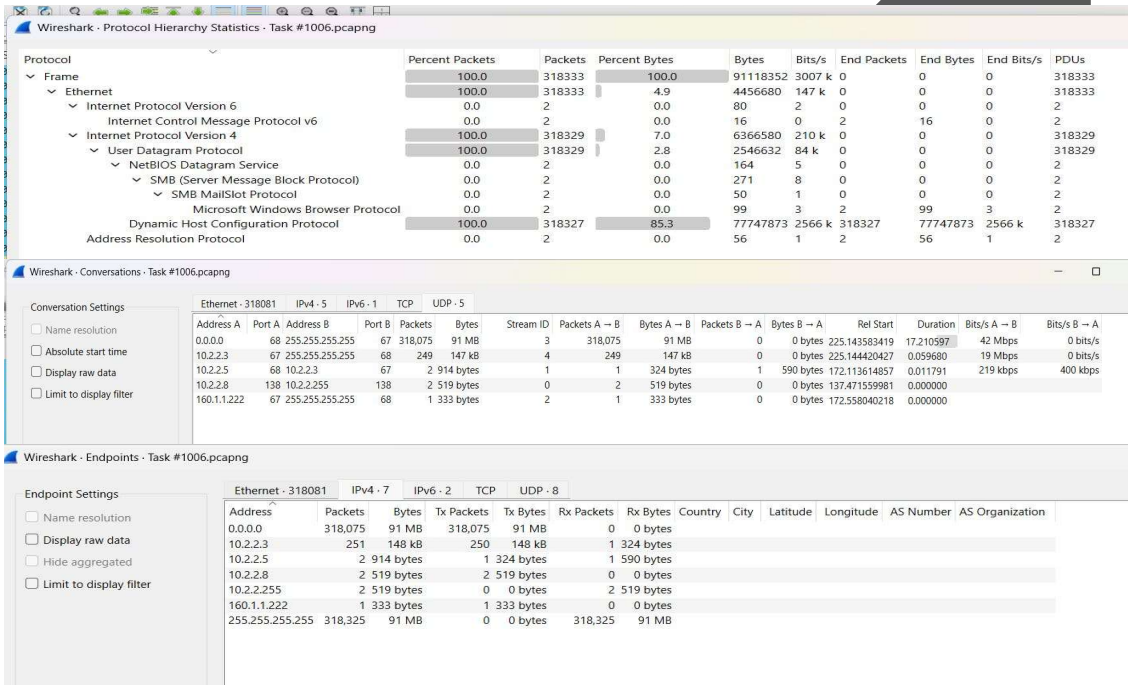
Key Findings

- 318,327 DHCP packets (99.998% of capture)
- All Discover packets used same transaction ID
- 0.0.0.0 → 255.255.255.255 flood at 42 Mbps
- Legitimate DHCP server unable to respond
- Windows Browser and ICMPv6 traffic minima



Task #1006 - Wireshark Capture Analysis cont…

The analysis revealed that the network traffic was overwhelmingly dominated by DHCP Discover broadcasts, totaling more than 318,000 packets with no corresponding DHCP Offer or ACK responses. This behavior is characteristic of a DHCP Starvation Attack, a denial-of-service technique used to exhaust DHCP server resources. Additional anomalies included repeated ARP probes, ICMPv6 router solicitations, and numerous one-packet Ethernet conversations, suggesting spoofed MAC activity.



Wireshark · Protocol Hierarchy Statistics · Task #1006.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	318333	100.0	91118352	3007 k	0	0	0	318333
Ethernet	100.0	318333	4.9	4456680	147 k	0	0	0	318333
Internet Protocol Version 6	0.0	2	0.0	80	2	0	0	0	2
Internet Control Message Protocol v6	0.0	2	0.0	16	0	2	16	0	2
Internet Protocol Version 4	100.0	318329	7.0	6366580	210 k	0	0	0	318329
User Datagram Protocol	100.0	318329	2.8	2546632	84 k	0	0	0	318329
NetBIOS Datagram Service	0.0	2	0.0	164	5	0	0	0	2
SMB (Server Message Block Protocol)	0.0	2	0.0	271	8	0	0	0	2
SMB MailSlot Protocol	0.0	2	0.0	50	1	0	0	0	2
Microsoft Windows Browser Protocol	0.0	2	0.0	99	3	2	99	3	2
Dynamic Host Configuration Protocol	100.0	318327	85.3	77747873	2566 k	318327	77747873	2566 k	318327
Address Resolution Protocol	0.0	2	0.0	56	1	2	56	1	2

Wireshark · Conversations · Task #1006.pcapng

Conversation Settings: Name resolution; Absolute start time; Display raw data; Limit to display filter

Ethernet · 318081 | IPv4 · 5 | IPv6 · 1 | TCP | UDP · 5

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
0.0.0.0	68	255.255.255.255	67	318,075	91 MB	3	318,075	91 MB	0	0 bytes	225.143583419	17.210597	42 Mbps	0 bits/s
10.2.2.3	67	255.255.255.255	68	249	147 kB	4	249	147 kB	0	0 bytes	225.144420427	0.059680	19 Mbps	0 bits/s
10.2.2.5	68	10.2.2.3	67	2	914 bytes	1	1	324 bytes	1	590 bytes	172.113614857	0.011791	219 kbps	400 kbps
10.2.2.8	138	10.2.2.255	138	2	519 bytes	0	2	519 bytes	0	0 bytes	137.471559981	0.000000		
160.1.1.222	67	255.255.255.255	68	1	333 bytes	2	1	333 bytes	0	0 bytes	172.558040218	0.000000		

Wireshark · Endpoints · Task #1006.pcapng

Endpoint Settings: Name resolution; Display raw data; Hide aggregated; Limit to display filter

Ethernet · 318081 | IPv4 · 7 | IPv6 · 2 | TCP | UDP · 8

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
0.0.0.0	318,075	91 MB	318,075	91 MB	0	0 bytes						
10.2.2.3	251	148 kB	250	148 kB	1	324 bytes						
10.2.2.5	2	914 bytes	1	324 bytes	1	590 bytes						
10.2.2.8	2	519 bytes	2	519 bytes	0	0 bytes						
10.2.2.255	2	519 bytes	0	0 bytes	2	519 bytes						
160.1.1.222	1	333 bytes	1	333 bytes	0	0 bytes						
255.255.255.255	318,325	91 MB	0	0 bytes	318,325	91 MB						

Mitigation Recommendations

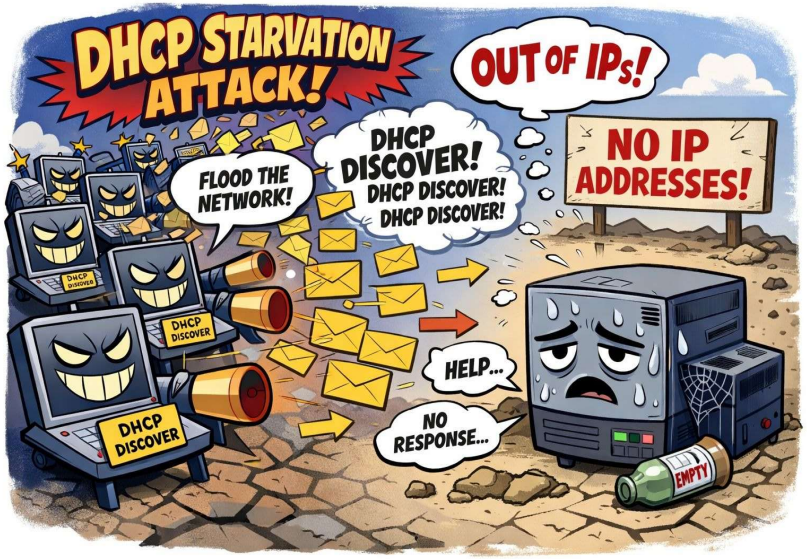
To prevent similar DHCP-based attacks, the network should implement DHCP Snooping, rate limiting, and port-security controls. Additional monitoring and segmentation strategies will help detect and contain broadcast-based denial-of-service attempts.

Key Points

- Enable DHCP Snooping on switches
- Apply rate limiting for DHCP requests per port
- Enforce port security to restrict MAC address counts
- Deploy IDS/IPS with DHCP flood signatures
- Implement broadcast storm control
- Strengthen DHCP server redundancy and segmentation

Conclusion

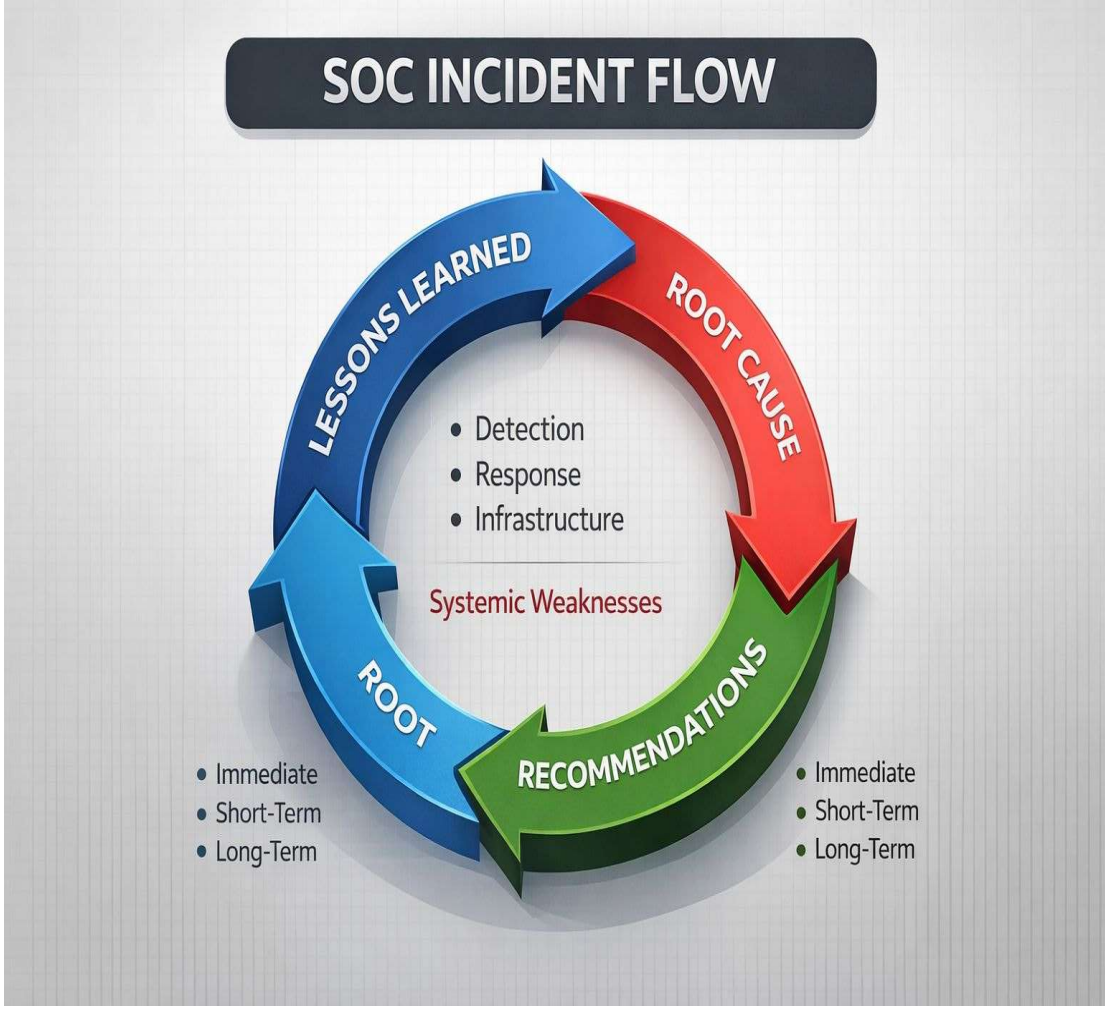
The analysis confirms a DHCP Starvation Attack characterized by excessive DHCP Discover traffic and the absence of DHCP server responses. This attack disrupts network operations by preventing legitimate clients from obtaining IP addresses. Implementing the recommended mitigations will significantly reduce the risk of future DHCP-based disruptions.

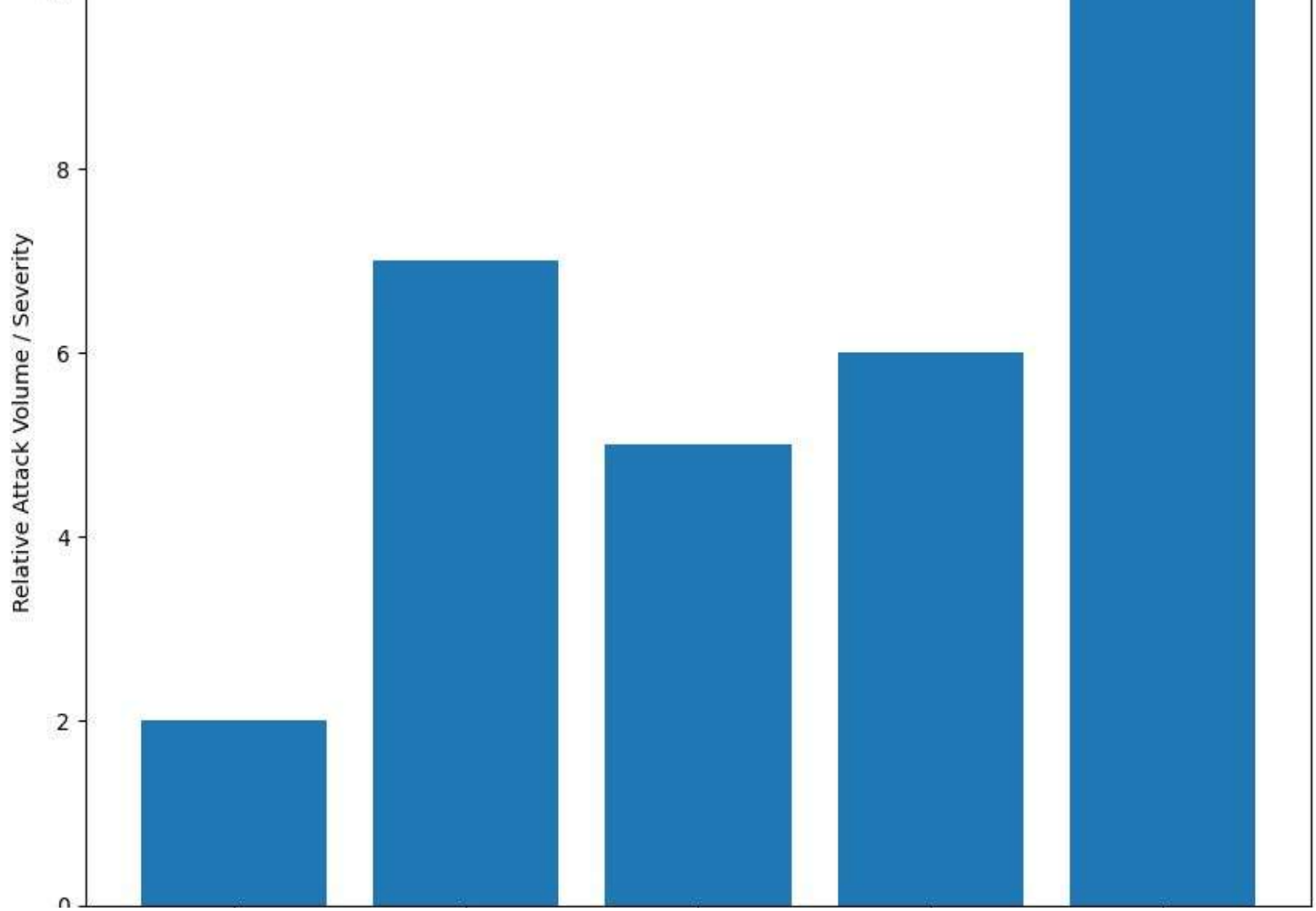


Key Points

- DHCP Starvation Attack confirmed
- Network disruption caused by DHCP exhaustion
- Supporting evidence from protocol hierarchy and conversations
- Mitigations will improve network resilience and stability

Key Lessons Learned





SOC Remediation Det

Task 1002 – TLS Reco
• Enforce outbound fi
• Monitor failed TLS h
• Deploy IDS alerts fo

Task 1003 – SYN Floo
• Enable SYN cookies
• Deploy IDS/IPS for p
• Segment internal h

Task 1004 – ICMP RA
• Rate-limit ICMP rout
• Monitor QUIC large-
• Inspect encrypted e

Task 1005 – CDP Floo
• Disable CDP where
• Enable broadcast st
• Deploy Layer-2 ano

Task 1006 – DHCP Sta
• Enable DHCP snoop
• Apply per-port rate
• Enforce MAC port s

LESSONS LEARNED
SOC’em Up TIER 3 Executive Summary

I conducted a penetration test and completed five Wireshark-based traffic investigations to assess and respond to security events within the Tech Solutions Inc. network environment.

The team strengthened proficiency in analyzing enterprise protocols, including **TLS, DHCP, ARP, IPv4/IPv6, and Layer 2 communications**, to differentiate baseline traffic from anomalous or malicious activity.

Observed threat behaviors included:

- Network reconnaissance and scanning
- Encrypted outbound traffic consistent with potential C2 activity
- Broadcast-based denial-of-service conditions
- DHCP starvation attacks impacting availability

A standardized forensic methodology was applied using **Protocol Hierarchy, Conversations, Endpoints, and packet-level inspection**, resulting in discovery of a failed handshake, multiple incoming floods and an almost 100% DHCP starvation as well as snooping. To improve real-time anomaly detection, accelerate incident analysis, and continuously strengthen defenses based on lessons learned. Tech Solutions can Enhance NIST CSF Detect (DE.AE, DE.CM) and Respond (RS.AN, RS.IM) functions.

THE END
THANK YOU

ANY QUESTIONS?