Network Traffic Analysis using Wireshark

Subject: Network Traffic Analysis using Wireshark

Incident ID: IR-2025-1218-005

PREPARED BY:

Vignesh K.

SOC Analyst / Security Researcher

CERTIFICATIONS: Google Cybersecurity Professional

REPORT DATE: December 18, 2025

1. Project Overview and Goal

- **Overview:**This project demonstrates SOC-style network traffic analysis using Wireshark and Nmap to detect reconnaissance, brute-force attempts, and service misconfigurations.
- **Goal:** The purpose is to identify open ports, detect suspicious DNS/HTTP activity, and evaluate the risk of credential compromise.
- **Scenario:** Analysis was conducted on a local LAN environment where a Kali Linux attacker machine interacted with a target Linux server (192.168.31.110).

2. Technical Environment and Tools

The technical components and tools used for this assessment are detailed below.

Component	Description	Detail
Target System	The victim server.	Linux Host (IP: 192.168.31.110)
Attacker System	The scanner machine.	Kali Linux.
Primary Tools	Analysis & Scanning.	Wireshark and Nmap 7.95.
Network	Environment.	Local LAN.

3. Attack/Analysis Simulation

A multi-stage analysis approach was utilized to identify malicious network behavior:

3.1 Scenario 1 – Port Scanning

- Detected multiple SYN packets sent to sequential ports from a single source. Technique: TCP SYN scan (MITRE T1046).

3.2 Scenario 2 – SSH Brute Force

- Identified repeated SSH login attempts via multiple TCP connections to port 22 from the same IP (MITRE T1110)

3.3 Scenario 3 – DNS/HTTP Traffic

- Observed repeated DNS queries resulting in NXDOMAIN responses and unencrypted cleartext HTTP traffic (MITRE T1071)

4. Key Findings and SOC Outcome

The assessment revealed critical exposures that increase the risk of a successful breach

CRITICAL: SMB Misconfiguration (Port 445)

- **Detection:** Nmap script reported "Message signing enabled but not required"
- **Risk:**High-impact vulnerability allowing SMB Relay Attacks (MITM)

High: Credential Compromise Risk (Port 21 & 22)

- **Detection:** Presence of repeated SSH attempts and vsftpd 3.0.5 activity.
- **Risk:** Potential for brute-force success and credential theft over unencrypted FTP.

Medium: Information Disclosure (Port 80)

- **Detection:** `Exposed server banner: Apache/2.4.65 (Debian).`
- **Risk:** Attackers can use specific version numbers to find matching CVEs.

5. Security Recommendations (Next Steps)

Based on the traffic analysis, the following remediation measures are required:

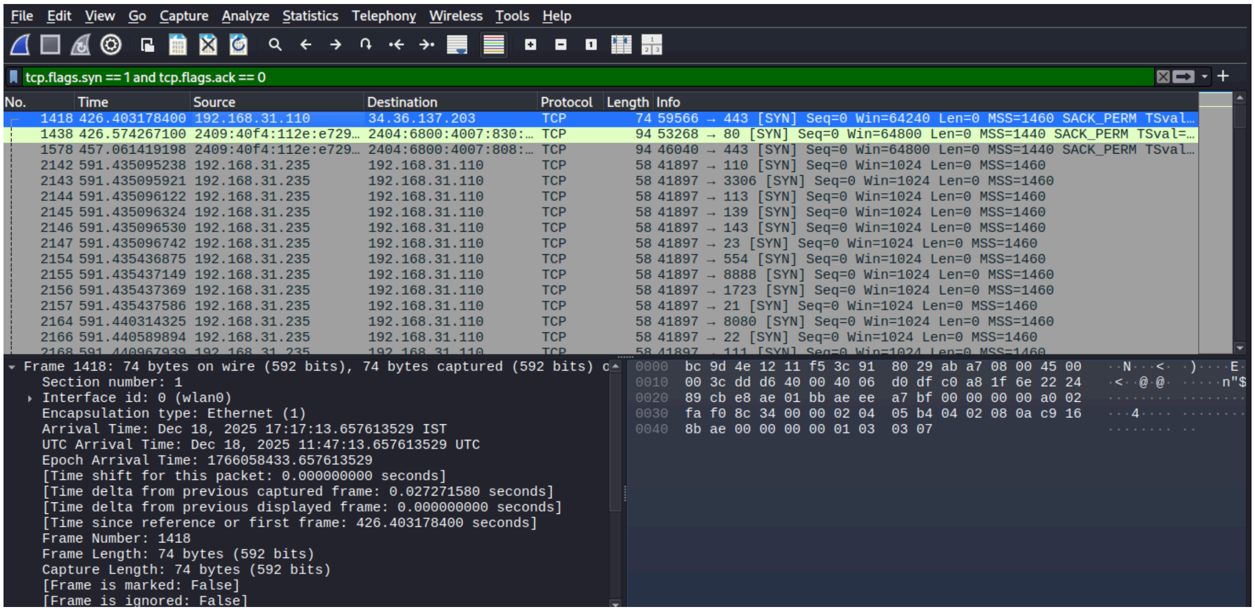
- **CRITICAL: Enforce SMB Signing:** Configure the Samba server to set server signing to mandatory to block relay attacks.
- **HIGH: Secure Protocol Hardening:** Immediately disable FTP (Port 21) and enforce the use of SFTP; enable IDS/IPS to block scanning IPs.
- **MEDIUM: Service Hardening:** Hide version banners in Apache and SSH configurations to prevent casual reconnaissance.
- **MEDIUM: Network Monitoring:** Monitor for DNS anomalies and enforce HTTPS to prevent data exposure.

6. Conclusion

- This assessment successfully validated practical SOC skills in identifying reconnaissance and service vulnerabilities.
- While individual risks like banner exposure are modest, the combination of brute-force attempts and SMB misconfigurations represents a high risk to the environment. Immediate hardening is recommended to secure the attack surface.

7. Evidence (Screenshots)

7.1 WireShark Basic Scan



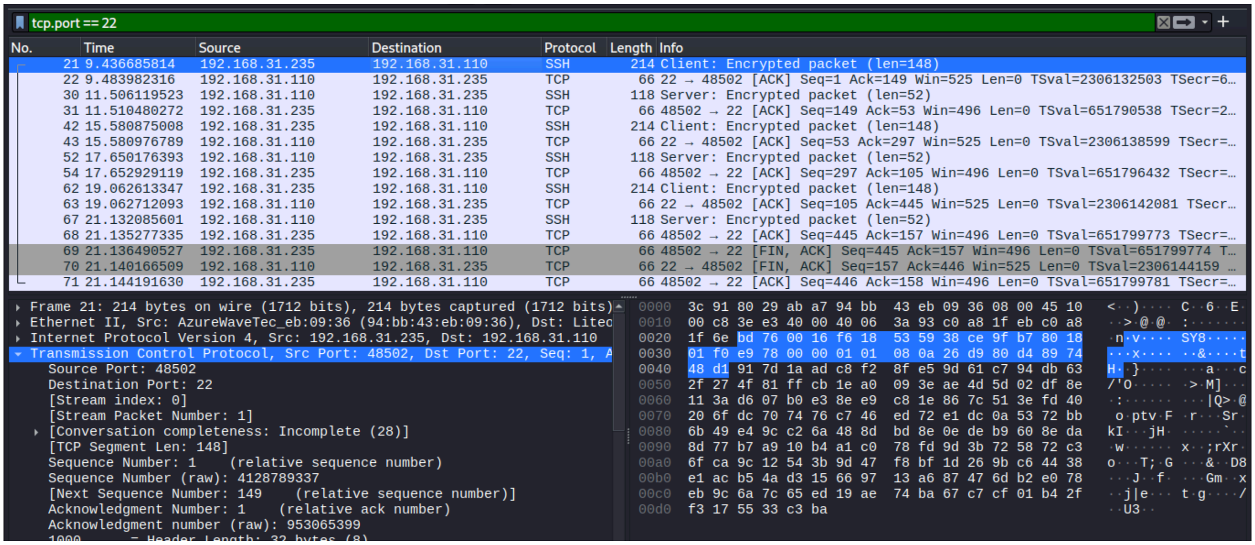
```
tcp.flags.syn == 1 and tcp.flags.ack == 0
```

```
No.  Time           Source                Destination           Protocol Length Info
1418 426.403178400 192.168.31.110        34.36.137.203         TCP      74 59566 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval…
1438 426.574267100 2409:40f4:112e:e729… 2404:6800:4007:830:… TCP      94 53268 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=…
1578 457.061419198 2409:40f4:112e:e729… 2404:6800:4007:808:… TCP      94 46040 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval…
2142 591.435095238 192.168.31.235        192.168.31.110        TCP      58 41897 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2143 591.435095921 192.168.31.235        192.168.31.110        TCP      58 41897 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2144 591.435096122 192.168.31.235        192.168.31.110        TCP      58 41897 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2145 591.435096324 192.168.31.235        192.168.31.110        TCP      58 41897 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2146 591.435096530 192.168.31.235        192.168.31.110        TCP      58 41897 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2147 591.435096742 192.168.31.235        192.168.31.110        TCP      58 41897 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2154 591.435436875 192.168.31.235        192.168.31.110        TCP      58 41897 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2155 591.435437149 192.168.31.235        192.168.31.110        TCP      58 41897 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2156 591.435437369 192.168.31.235        192.168.31.110        TCP      58 41897 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2157 591.435437586 192.168.31.235        192.168.31.110        TCP      58 41897 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2164 591.440314325 192.168.31.235        192.168.31.110        TCP      58 41897 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2166 591.440589894 192.168.31.235        192.168.31.110        TCP      58 41897 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2168 591.440967939 192.168.31.235        192.168.31.110        TCP      58 41897 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
▾ Frame 1418: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) o
    Section number: 1
  ▸ Interface id: 0 (wlan0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec 18, 2025 17:17:13.657613529 IST
    UTC Arrival Time: Dec 18, 2025 11:47:13.657613529 UTC
    Epoch Arrival Time: 1766058433.657613529
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.027271580 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 426.403178400 seconds]
    Frame Number: 1418
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
```

```
0000  bc 9d 4e 12 11 f5 3c 91  80 29 ab a7 08 00 45 00   ··N···<· ·)····E·
0010  00 3c dd d6 40 00 40 06  d0 df c0 a8 1f 6e 22 24   ·<··@·@· ·····n"$
0020  89 cb e8 ae 01 bb ae ee  a7 bf 00 00 00 00 a0 02   ········ ········
0030  fa f0 8c 34 00 00 02 04  05 b4 04 02 08 0a c9 16   ···4···· ········
0040  8b ae 00 00 00 00 01 03  03 07                     ········ ··
```

7.2 SSH Scan



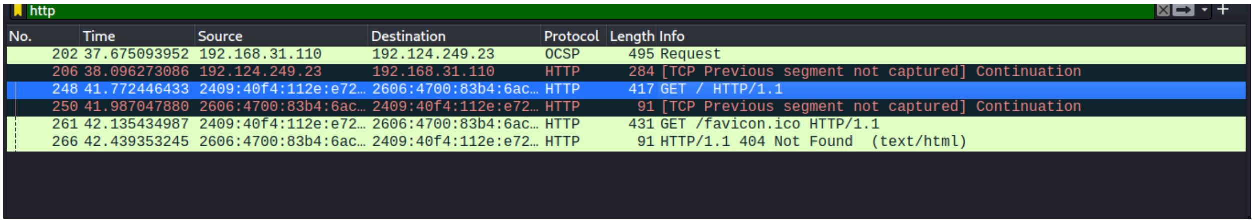
```
tcp.port == 22
```

```
No. Time          Source           Destination      Protocol Length Info
 21 9.436685814   192.168.31.235   192.168.31.110   SSH      214 Client: Encrypted packet (len=148)
 22 9.483982316   192.168.31.110   192.168.31.235   TCP       66 22 → 48502 [ACK] Seq=1 Ack=149 Win=525 Len=0 TSval=2306132503 TSecr=6…
 30 11.506119523  192.168.31.110   192.168.31.235   SSH      118 Server: Encrypted packet (len=52)
 31 11.510480272  192.168.31.235   192.168.31.110   TCP       66 48502 → 22 [ACK] Seq=149 Ack=53 Win=496 Len=0 TSval=651790538 TSecr=2…
 42 15.580875008  192.168.31.235   192.168.31.110   SSH      214 Client: Encrypted packet (len=148)
 43 15.580976789  192.168.31.110   192.168.31.235   TCP       66 22 → 48502 [ACK] Seq=53 Ack=297 Win=525 Len=0 TSval=2306138599 TSecr=…
 52 17.650176393  192.168.31.110   192.168.31.235   SSH      118 Server: Encrypted packet (len=52)
 54 17.652929119  192.168.31.235   192.168.31.110   TCP       66 48502 → 22 [ACK] Seq=297 Ack=105 Win=496 Len=0 TSval=651796432 TSecr=…
 62 19.062613347  192.168.31.235   192.168.31.110   SSH      214 Client: Encrypted packet (len=148)
 63 19.062712093  192.168.31.110   192.168.31.235   TCP       66 22 → 48502 [ACK] Seq=105 Ack=445 Win=525 Len=0 TSval=2306142081 TSecr…
 67 21.132085601  192.168.31.110   192.168.31.235   SSH      118 Server: Encrypted packet (len=52)
 68 21.135277335  192.168.31.235   192.168.31.110   TCP       66 48502 → 22 [ACK] Seq=445 Ack=157 Win=496 Len=0 TSval=651799773 TSecr=…
 69 21.136490527  192.168.31.235   192.168.31.110   TCP       66 48502 → 22 [FIN, ACK] Seq=445 Ack=157 Win=496 Len=0 TSval=651799774 T…
 70 21.140166509  192.168.31.110   192.168.31.235   TCP       66 22 → 48502 [FIN, ACK] Seq=157 Ack=446 Win=525 Len=0 TSval=2306144159 …
 71 21.144191630  192.168.31.235   192.168.31.110   TCP       66 48502 → 22 [ACK] Seq=446 Ack=158 Win=496 Len=0 TSval=651799781 TSecr=…
```

```
▸ Frame 21: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
▸ Ethernet II, Src: AzureWaveTec_eb:09:36 (94:bb:43:eb:09:36), Dst: Litec
▸ Internet Protocol Version 4, Src: 192.168.31.235, Dst: 192.168.31.110
▾ Transmission Control Protocol, Src Port: 48502, Dst Port: 22, Seq: 1, A
    Source Port: 48502
    Destination Port: 22
    [Stream index: 0]
    [Stream Packet Number: 1]
  ▸ [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 148]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4128789337
    [Next Sequence Number: 149    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 953065399
    1000 .... = Header Length: 32 bytes (8)
```

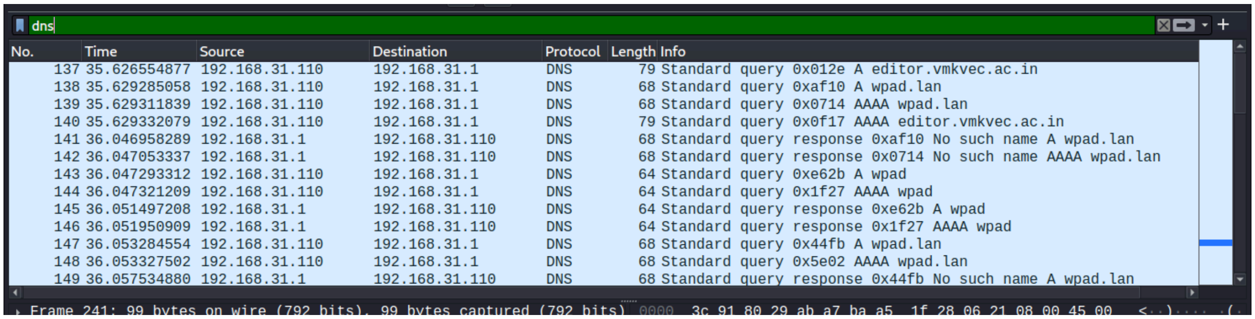
```
0000  3c 91 80 29 ab a7 94 bb  43 eb 09 36 08 00 45 10   <··)···· C··6··E·
0010  00 c8 3e e3 40 00 40 06  3a 93 c0 a8 1f eb c0 a8   ··>·@·@· :·······
0020  1f 6e bd 76 00 16 f6 18  53 59 38 ce 9f b7 80 18   ·n·v···· SY8·····
0030  01 f0 e9 78 00 00 01 01  08 0a 26 d9 80 d4 89 74   ···x···· ··&····t
0040  48 d1 91 7d 1a ad c8 f2  8f e5 9d 61 c7 94 db 63   H··}···· ···a···c
0050  2f 27 4f 81 ff cb 1e a0  09 3e ae 4d 5d 02 df 8e   /'O····· ·>·M]···
0060  11 3a d6 07 b0 e3 8e e9  c8 1e 86 7c 51 3e fd 40   ·:······ ···|Q>·@
0070  20 6f dc 70 74 76 c7 46  ed 72 e1 dc 0a 53 72 bb    o·ptv·F ·r···Sr·
0080  6b 49 e4 9c c2 6a 48 8d  bd 8e 0e de b9 60 8e da   kI···jH· ·····`··
0090  8d 77 b7 a9 10 b4 a1 c0  78 fd 9d 3b 72 58 72 c3   ·w······ x··;rXr·
00a0  6f ca 9c 12 54 3b 9d 47  f8 bf 1d 26 9b c6 44 38   o···T;·G ···&··D8
00b0  e1 ac b5 4a d3 15 66 97  13 a6 87 47 6d b2 e0 78   ···J··f· ···Gm··x
00c0  eb 9c 6a 7c 65 ed 19 ae  74 ba 67 c7 cf 01 b4 2f   ··j|e··· t·g····/
00d0  f3 17 55 33 c3 ba                                  ··U3··
```

7.3 Http Scan



```
http
No.     Time         Source                Destination           Protocol Length Info
    202 37.675093952 192.168.31.110        192.124.249.23        OCSP      495 Request
    206 38.096273086 192.124.249.23        192.168.31.110        HTTP      284 [TCP Previous segment not captured] Continuation
    248 41.772446433 2409:40f4:112e:e72… 2606:4700:83b4:6ac… HTTP      417 GET / HTTP/1.1
    250 41.987047880 2606:4700:83b4:6ac… 2409:40f4:112e:e72… HTTP       91 [TCP Previous segment not captured] Continuation
    261 42.135434987 2409:40f4:112e:e72… 2606:4700:83b4:6ac… HTTP      431 GET /favicon.ico HTTP/1.1
    266 42.439353245 2606:4700:83b4:6ac… 2409:40f4:112e:e72… HTTP       91 HTTP/1.1 404 Not Found  (text/html)
```

7.4 DNS Scan



```
dns
No.     Time         Source                Destination           Protocol Length Info
    137 35.626554877 192.168.31.110        192.168.31.1          DNS        79 Standard query 0x012e A editor.vmkvec.ac.in
    138 35.629285058 192.168.31.110        192.168.31.1          DNS        68 Standard query 0xaf10 A wpad.lan
    139 35.629311839 192.168.31.110        192.168.31.1          DNS        68 Standard query 0x0714 AAAA wpad.lan
    140 35.629332079 192.168.31.110        192.168.31.1          DNS        79 Standard query 0x0f17 AAAA editor.vmkvec.ac.in
    141 36.046958289 192.168.31.1          192.168.31.110        DNS        68 Standard query response 0xaf10 No such name A wpad.lan
    142 36.047053337 192.168.31.1          192.168.31.110        DNS        68 Standard query response 0x0714 No such name AAAA wpad.lan
    143 36.047293312 192.168.31.110        192.168.31.1          DNS        64 Standard query 0xe62b A wpad
    144 36.047321209 192.168.31.110        192.168.31.1          DNS        64 Standard query 0x1f27 AAAA wpad
    145 36.051497208 192.168.31.1          192.168.31.110        DNS        64 Standard query response 0xe62b A wpad
    146 36.051950909 192.168.31.1          192.168.31.110        DNS        64 Standard query response 0x1f27 AAAA wpad
    147 36.053284554 192.168.31.110        192.168.31.1          DNS        68 Standard query 0x44fb A wpad.lan
    148 36.053327502 192.168.31.110        192.168.31.1          DNS        68 Standard query 0x5e02 AAAA wpad.lan
    149 36.057534880 192.168.31.1          192.168.31.110        DNS        68 Standard query response 0x44fb No such name A wpad.lan
› Frame 241: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)  0000  3c 91 80 29 ab a7 ba a5  1f 28 06 21 08 00 45 00   <··)···· ·(·
```