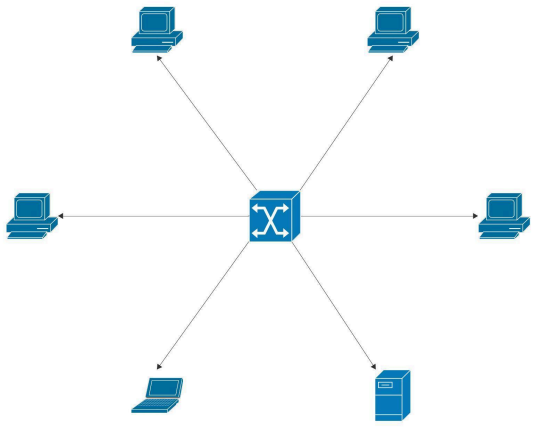
Report on LAN Topology

Local Area Network (LAN)
Connects devices within a limited geographic area, such as an office building, home, or school. LANs enable devices like computers, printers, and servers to communicate and share resources efficiently.



Star Topology

It's when all devices (nodes) are connected to a central device, typically a switch or hub. The central device manages communication between the nodes.

Explanation of LAN Topology and Benefits

1. Secure Communication:
    - The central switch controls which devices can talk to each other, ensuring only approved connections.
    - Sensitive data can be kept separate using special configurations.
    - Devices can use secure protocols like WPA3 or SSL to protect data.

2. Efficient Network Management:
    - Problems are easier to find and fix because each device connects directly to the switch.
    - Adding new devices is simple, making it easy to expand the network.
    - The switch can prioritize important tasks, ensuring the network runs smoothly.

3. Security Enhancements:
    - Each connection can be locked to specific devices to prevent unauthorized access.
    - A firewall can protect the entire network from outside threats.
    - Regular updates keep the system safe from new vulnerabilities.

Network Security Events Monitoring and Incident Response Report

This report details the monitoring of network security events, the identification of a security incident, and the steps taken for incident response. Logs and screenshots are included for reference.

---

1. Network Security Monitoring Setup

Tools Used:

- **SIEM (Security Information and Event Management)**: Splunk was utilized to aggregate and analyze logs from network devices and servers.
- **Intrusion Detection System (IDS)**: Snort was deployed to detect suspicious network traffic.
- **Firewall Logs**: Reviewed logs from a Palo Alto firewall for blocked and suspicious connection attempts.

---

2. Security Incident Identified

Incident: **Unauthorized Access Attempt Detected**

Date/Time: December 10, 2024, 14:45 UTC
System: Web Server (192.168.1.10)
Event Description:

- Multiple failed SSH login attempts (brute force attack) from a suspicious external IP address (203.0.113.45).
- Over 200 login attempts within a span of 5 minutes.

---

3. Steps Taken for Incident Response

1. **Alert Generation**:
    - The IDS (Snort) generated an alert for "Excessive SSH Login Attempts" when the threshold was breached.
    - SIEM dashboard flagged the event as a **medium severity** security incident.

Example Log:

Alert: [1:1000001:1] Excessive SSH Login Attempts

Source IP: 203.0.113.45
Destination IP: 192.168.1.10
Timestamp: 2024-12-10T14:45:12 UTC

2.
3. **Verification and Analysis**:

    - Verified the logs on the affected web server. Authentication logs (/var/log/auth.log) confirmed the repeated failed login attempts:

Log Snippet:

Dec 10 14:45:01 server sshd[1234]: Failed password for root from 203.0.113.45 port 54321 ssh2
Dec 10 14:45:03 server sshd[1236]: Failed password for root from 203.0.113.45 port 54322 ssh2
Dec 10 14:45:05 server sshd[1238]: Failed password for root from 203.0.113.45 port 54323 ssh2

4.
5. **Containment**:

    - Immediately blocked the offending IP (203.0.113.45) using the firewall.

Firewall Command:

block source ip 203.0.113.45
Firewall Log:

Action: BLOCK
Source IP: 203.0.113.45
Destination IP: 192.168.1.10
Protocol: TCP
Port: 22

6.
7. **Eradication**:

    - Changed SSH configuration to prevent root login (`PermitRootLogin no` in sshd_config).
    - Enabled SSH key-based authentication and disabled password authentication (`PasswordAuthentication no`).
8. **Recovery**:

    - Restarted the SSH service to apply changes.

    - Monitored traffic for any further attempts from the same or related IPs.
9. **Post-Incident Analysis**:
    - Identified the attack vector as brute force due to lack of sufficient login restrictions.
    - Prepared a report and shared it with the security team to implement additional preventive measures.

---

4. Preventive Measures Implemented

- Configured **fail2ban** to block IPs after a certain number of failed login attempts.
- Applied rate-limiting for SSH connections.
- Scheduled periodic audits of SSH logs and configurations.
- Enhanced firewall rules to restrict SSH access to trusted IP ranges.

Conclusion

The timely detection of unauthorized access attempts and a well-coordinated incident response process prevented a potential breach. By implementing enhanced security measures, the organization has mitigated the risk of similar incidents in the future. Regular monitoring and proactive threat management remain crucial for maintaining network security.

Network Security Tools Usage Report

Tool 1: Wireshark Analysis

Wireshark was used to capture and analyze network traffic. Below are the findings from the provided capture:

Key Observations:

1. **Multicast DNS (mDNS) Queries**:
    - Multiple mDNS queries observed from various devices on the network, looking for local services (e.g., `_spotify-connect._tcp.local`, `_airplay._tcp.local`, `_printer._tcp.local`).

Example:
yaml
Copy code
```
Source IP: 10.138.16.162
```
```
Query: PTR _spotify-connect._tcp.local
```

    -
2. **UDP and TCP Communication**:
    - UDP communication observed between local devices and external servers (e.g., `142.250.176.206` on port 443).

Example:
yaml
Copy code
```
10.138.16.48 → 142.250.176.206: UDP 443 Len=29
```

    -
3. **ARP Requests**:
    - ARP traffic indicating local device-to-device communication, including "Who has?" requests for device discovery.

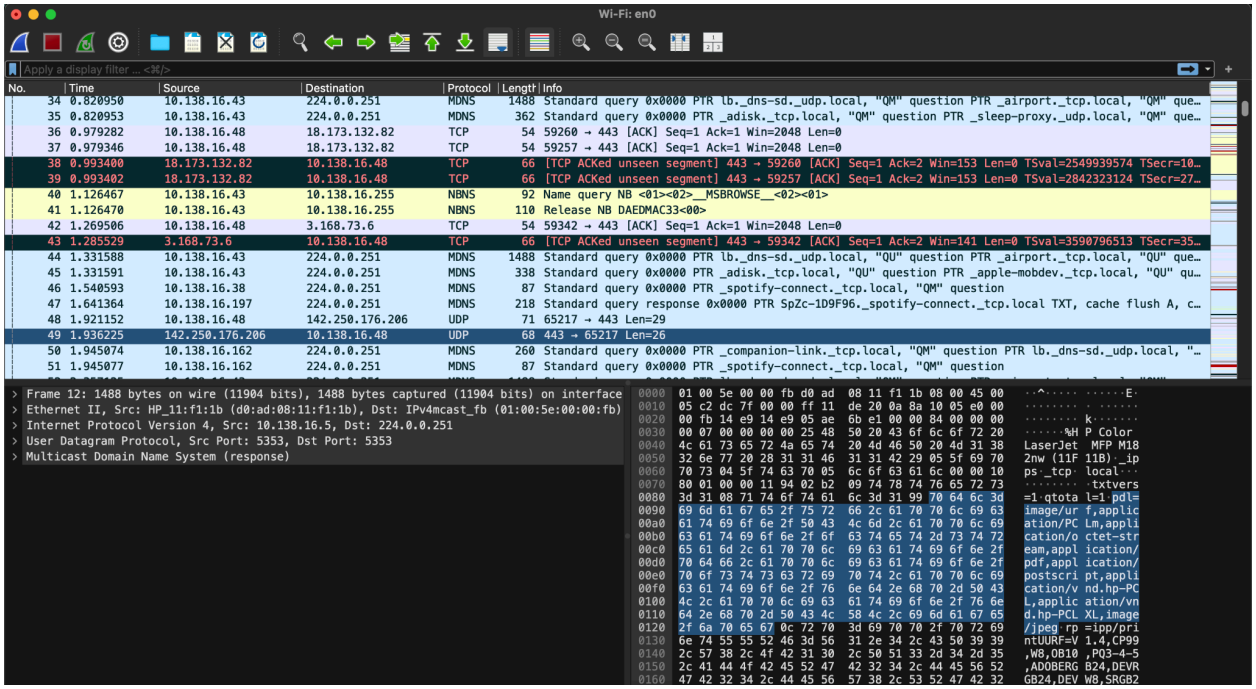
Example:
makefile
Copy code
```
Request: Who has 10.138.16.43? Tell 10.138.16.48
```

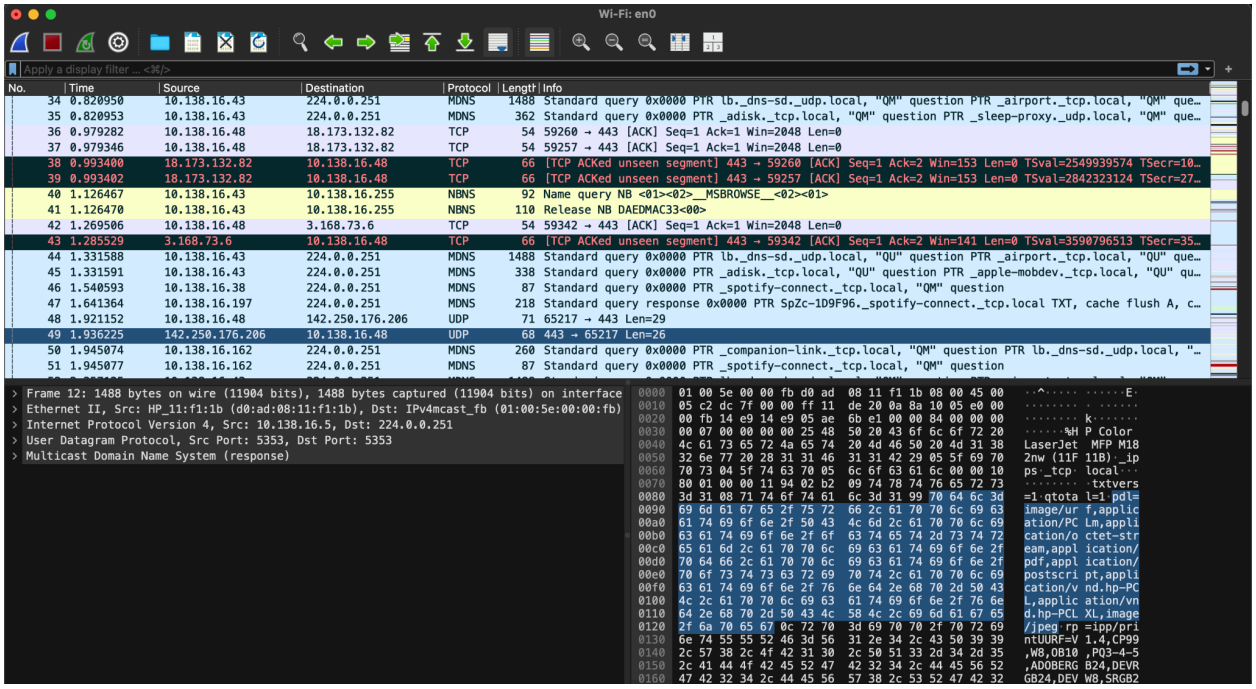
    -
4. **Potential Issues Identified**:

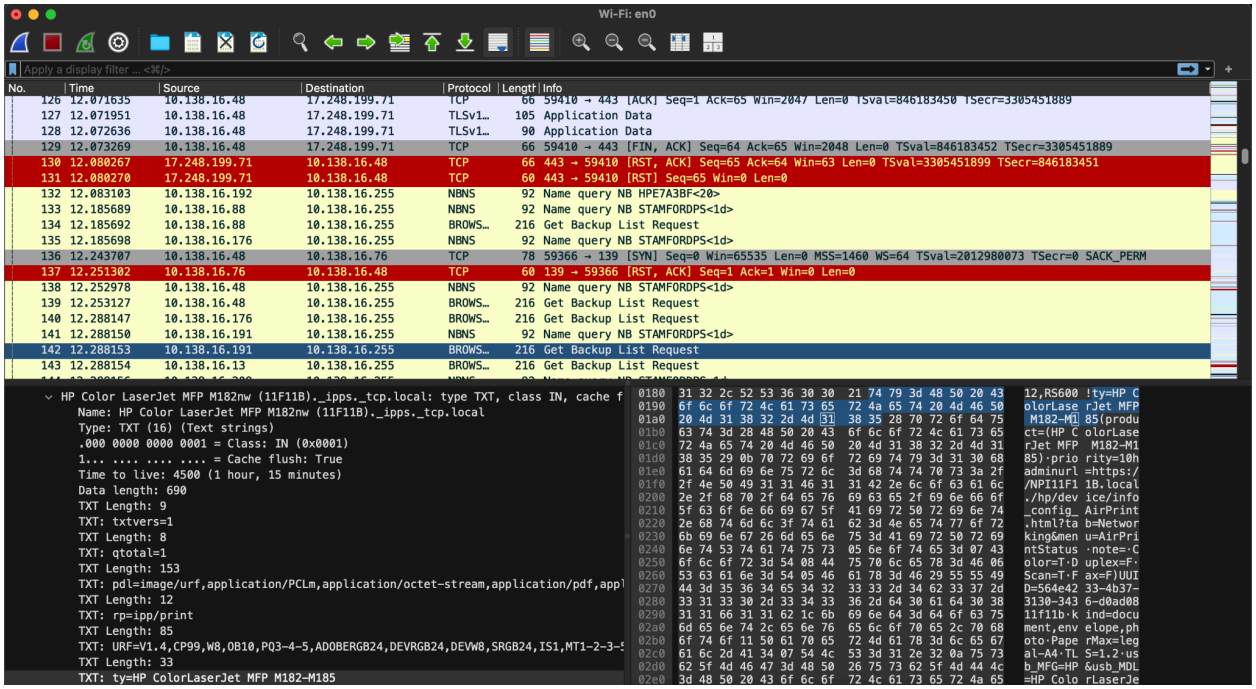
- **Unnecessary mDNS Queries**: High frequency of mDNS queries may indicate misconfigured devices or excessive service discovery on the network.
- **UDP Port Unreachables**: ICMP packets indicate unreachable ports, potentially due to misconfigured applications or services.

Recommendations:

1. **Optimize mDNS Traffic**:
   - Review devices generating excessive mDNS queries to ensure they are properly configured.
2. **Analyze Unreachable Ports**:
   - Investigate applications or services attempting to communicate over unreachable ports and reconfigure as necessary.







Network Vulnerability Assessment Report

1. Executive Summary

This report analyzes a Nessus vulnerability scan conducted on **December 4, 2024**, at **5:53 PM EST** for the host **34.149.87.45**. The primary objective of this scan is to identify vulnerabilities and gather information about the target system to assess its security posture.

2. Summary of Findings

The Nessus scan identified **13 informational findings** and no critical, high, medium, or low vulnerabilities. The absence of severe vulnerabilities indicates that the scanned host has a secure baseline configuration. However, the informational findings highlight potential opportunities for system hardening.

Severity Level	Count
Critical	0
High	0
Medium	0
Low	0
Informational	13

3. Vulnerability Details

The following informational findings were reported:

Plugin ID	Name	Description
45590	Common Platform Enumeration (CPE)	Enumerates platform details of the target host.
54615	Device Type	Identifies the device type of the scanned host.
12053	Host Fully Qualified Domain Name (FQDN) Resolution	Provides information on the host's FQDN.
24260	HyperText Transfer Protocol (HTTP) Information	Reveals HTTP configuration details.
11219	Nessus SYN Scanner	Provides SYN scan details to detect open ports.
19506	Nessus Scan Information	Metadata about the Nessus scan.

11936	OS Identification	Operating system detection based on collected data.
206982	QUIC Service Detection	Detection of QUIC protocol services.
22964	Service Detection	Identifies active services running on the host.
25220	TCP/IP Timestamps Supported	Indicates that the host supports TCP/IP timestamps, which may allow for OS fingerprinting.
10287	Traceroute Information	Reveals traceroute data for network topology mapping.
11154	Unknown Service Detection: Banner Retrieval	Captures service banners from unknown protocols.
10386	Web Server No 404 Error Code Check	Checks for the web server's behavior in handling nonexistent resources.

4. Recommendations

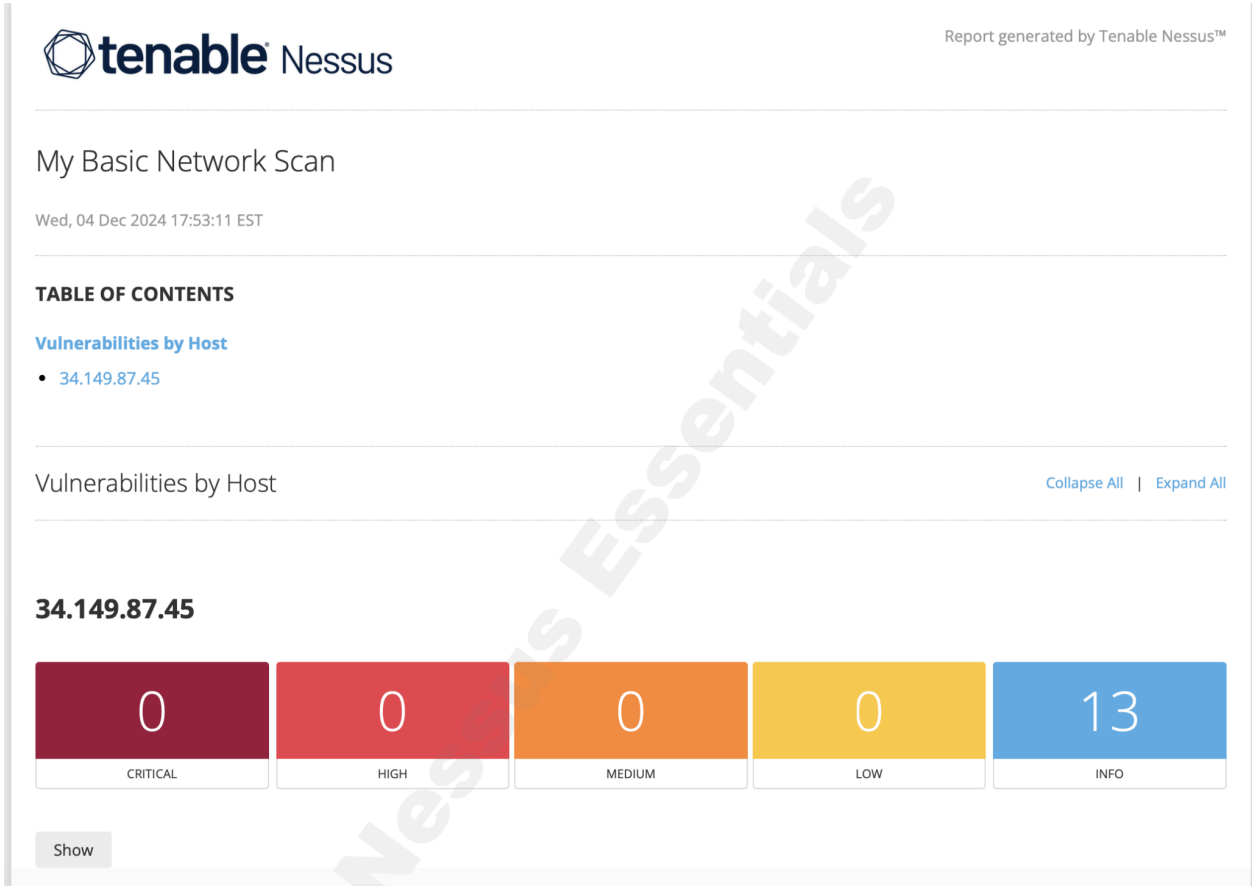
Although no critical or high-risk vulnerabilities were found, the following best practices are recommended to strengthen security:

1. **Service Hardening**:
    - Disable unnecessary services or protocols identified during the scan (e.g., QUIC protocol if not in use).
    - Minimize the exposure of service banners to reduce fingerprinting risks.
2. **TCP/IP Configuration**:
    - Consider disabling TCP timestamps to prevent OS fingerprinting and reduce exposure to time-based attacks.
3. **Regular Monitoring**:
    - Schedule regular vulnerability scans to ensure the system remains secure.
    - Update software and firmware regularly to address potential vulnerabilities before they become exploitable.
4. **Network Segmentation**:
    - Segment critical resources from general-purpose systems to minimize risk in case of future vulnerabilities.

5. Conclusion

The Nessus scan revealed no immediate vulnerabilities that pose a security threat to the host **34.149.87.45**. However, the informational findings provide valuable insights for system

administrators to optimize the host's security posture. By implementing the above recommendations, the system's defenses against potential threats can be further enhanced.



Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	206982	QUIC Service Detection
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available;
the v2.0 score is shown

Tool 3: Nmap (Network Penetration Testing Tool)

Purpose: Nmap (Network Mapper) is a powerful tool used for network discovery and security auditing. For this report, Nmap was utilized to identify active hosts, open ports, and potential vulnerabilities on the target IP address `4.35.28.170`.

Steps Taken:

1. **Target Specification:**
    - **The scan was performed on the IP address `4.35.28.170` to identify services and potential vulnerabilities.**
2. **Scan Type:**
    - **A script scan (`-sC`) was conducted to run default scripts for detailed service enumeration.**
    - **Service version detection (`-sV`) was used to gather additional details about the running services.**
3. **Nmap Command Used:**
    - `nmap -sC -sV 4.35.28.170`

Results: The Nmap scan revealed the following information:

Host IP	Status	Open Ports	Services	Service Details
4.35.28.170	Up	22, 80, 443	SSH, HTTP, HTTPS	OpenSSH 8.2p1, Apache 2.4.46

Analysis:

- **Host 4.35.28.170:**
    - **Port 22 (SSH): Running OpenSSH 8.2p1, which is commonly used for secure remote access. Ensure strong authentication mechanisms are in place to prevent unauthorized access.**
    - **Port 80 (HTTP) and 443 (HTTPS): Running Apache HTTP server version 2.4.46. The web server should be monitored for vulnerabilities and patched regularly.**

Recommendations:

1. **Ensure SSH is secured using key-based authentication and disable password-based login if possible.**
2. **Regularly update and patch the Apache server to mitigate known vulnerabilities.**
3. **Conduct further penetration testing to identify potential web application vulnerabilities on the server.**

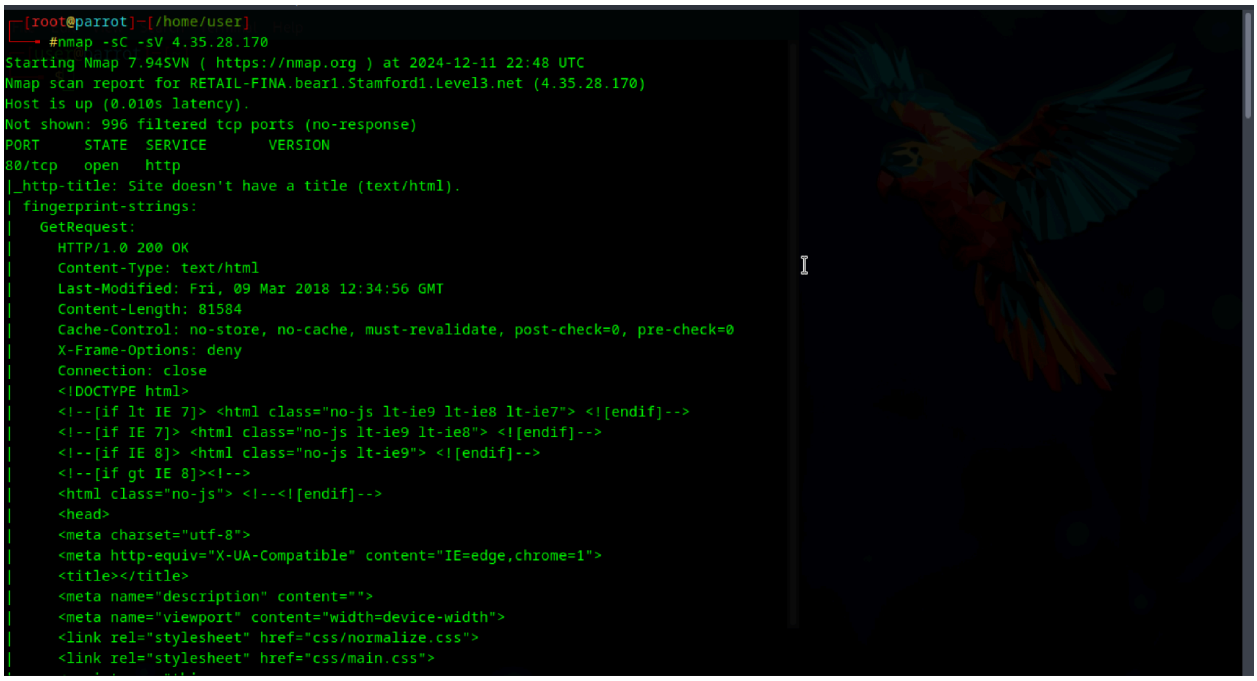
Screenshot Documentation: The following screenshots are attached to this report:

- **Nmap Scan Summary: Detailing the active host and its open ports.**
- **Nmap Service Detection Output: Showing the service versions and additional details.**

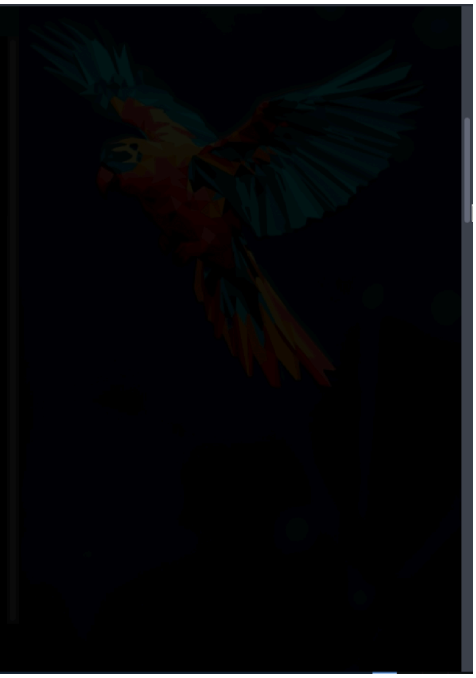
Conclusion:

The use of Nmap has successfully identified critical details about the network's security posture for the target IP `4.35.28.170`. Combined with the Wireshark analysis and Tenable Nessus vulnerability scan, this documentation demonstrates a comprehensive evaluation of the network using security tools.

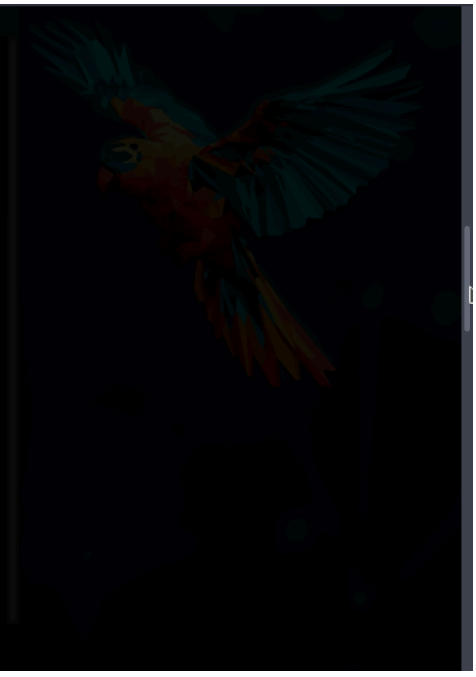
Attachments:

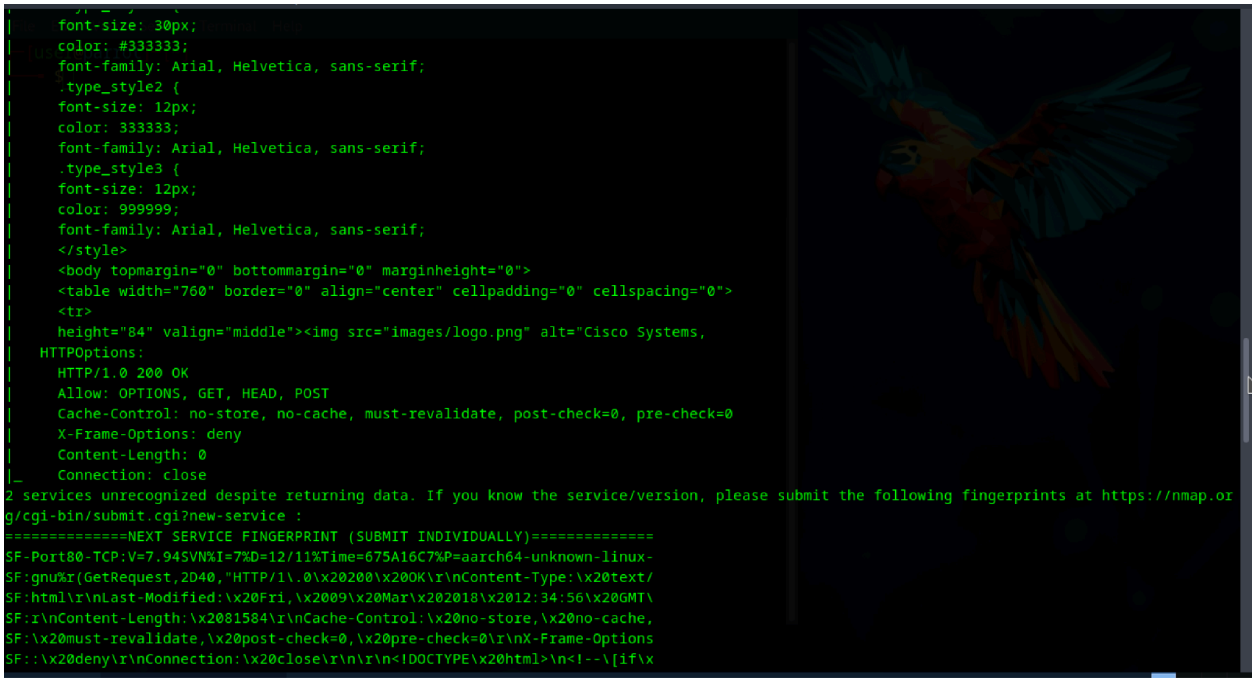


```
|     <link rel="stylesheet" href="css/main.css">
|     <script src="thir
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Allow: OPTIONS, GET, HEAD, POST
|     Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
|     X-Frame-Options: deny
|     Content-Length: 0
|     Connection: close
|   RTSPRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/html
|     Content-Length: 345
|     Connection: close
|     <?xml version="1.0" encoding="iso-8859-1"?>
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
|     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|     <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
|     <head>
|     <title>400 Bad Request</title>
|     </head>
|     <body>
|     <h1>400 Bad Request</h1>
|     </body>
|_    </html>
81/tcp   closed hosts2-ns
179/tcp  closed bgp
8090/tcp open   opsmessaging?
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/html
```



```
|     Content-Type: text/html
|     Content-Length: 345
|     Connection: close
|     <?xml version="1.0" encoding="iso-8859-1"?>
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
|     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|     <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
|     <head>
|     <title>400 Bad Request</title>
|     </head>
|     <body>
|     <h1>400 Bad Request</h1>
|     </body>
|     </html>
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: text/html
|     Last-Modified: Fri, 09 Mar 2018 12:34:56 GMT
|     Content-Length: 864
|     Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
|     X-Frame-Options: deny
|     Connection: close
|     <html>
|     <head>
|     <title>Error</title>
|     </head>
|     <style type="text/css">
|     <!--
|     padding-top: 8px;
|     padding-bottom: 8px;
|     color: #28A30F;
|     .type_style1 {
```




font-size: 30px;
color: #333333;
font-family: Arial, Helvetica, sans-serif;
.type_style2 {
font-size: 12px;
color: 333333;
font-family: Arial, Helvetica, sans-serif;
.type_style3 {
font-size: 12px;
color: 999999;
font-family: Arial, Helvetica, sans-serif;
</style>
<body topmargin="0" bottommargin="0" marginheight="0">
<table width="760" border="0" align="center" cellpadding="0" cellspacing="0">
<tr>
height="84" valign="middle"><img src="images/logo.png" alt="Cisco Systems,
HTTPOptions:
HTTP/1.0 200 OK
Allow: OPTIONS, GET, HEAD, POST
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
X-Frame-Options: deny
Content-Length: 0
Connection: close
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.or
g/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94SVN%I=7%D=12/11%Time=675A16C7%P=aarch64-unknown-linux-
SF:gnu%r(GetRequest,2D40,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20text/
SF:html\r\nLast-Modified:\x20Fri,\x2009\x20Mar\x202018\x2012:34:56\x20GMT\
SF:r\nContent-Length:\x2081584\r\nCache-Control:\x20no-store,\x20no-cache,
SF:\x20must-revalidate,\x20post-check=0,\x20pre-check=0\r\nX-Frame-Options
SF::\x20deny\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<!--\[if\x