# Network Scan Report

Date: 25th March 2024

Scanner: Nmap

## Executive Summary:

The network scan was conducted to assess the security posture and identify potential vulnerabilities within the network infrastructure. The scan revealed several findings which are detailed below.

## 1. Network Topology:

```
Nmap scan report for 192.168.1.64
MAC Address: 8E:3F:C6:3E:9B:35 (Unknown)

Nmap scan report for 192.168.1.65
MAC Address: 72:CA:94:7D:9C:B6 (Unknown)

Nmap scan report for 192.168.1.67
MAC Address: 04:C8:07:12:EB:0A (Xiaomi Communications)

Nmap scan report for 192.168.1.70
PORT     STATE SERVICE
443/tcp  open  https
3306/tcp open  mysql
9090/tcp open  zeus-admin
MAC Address: 06:EF:76:F3:D6:29 (Unknown)

Nmap scan report for dsldevice.lan (192.168.1.254)
PORT    STATE    SERVICE
22/tcp  filtered ssh
23/tcp  filtered telnet
80/tcp  filtered http
443/tcp filtered https
MAC Address: 88:B3:62:59:43:A0 (Nokia Shanghai Bell)

Nmap scan report for 192.168.1.75


Nmap done: 256 IP addresses (6 hosts up) scanned in 55.78 seconds
```

## 2. Host Discovery:

Total Hosts Discovered: 5
Active Hosts: 192.168.1.64, 192.168.1.65,192.168.1.67, 192.168.1.70, 192.168.1.254, 192.168.1.75
Inactive Hosts: None

## 3. Open Ports:

The following ports were found to be open across the network:

```
   Host 192.168.1.70:
      PORT     STATE SERVICE
      443/tcp  open  https
```

```
    3306/tcp open  mysql
    5353/udp open  zeroconf
    9090/tcp open  zeus-admin
  Host 192.168.1.254:
    2/tcp   filtered ssh
    23/tcp  filtered telnet
    80/tcp  filtered http
    443/tcp filtered https
```

4. Services Running:

Based on the open ports, the following services were identified:

```
  Host 192.168.1.70:
    https
    mysql
    zeroconf
    zeus-admin
```

5. Operating Systems Detected:

```
  Host 192.168.1.70:Device type: general purpose
      Running (JUST GUESSING): Microsoft Windows 11|2022|10 (91%), FreeBSD 6.X (86%)
      OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:freebsd:freebsd:6.2
cpe:/o:microsoft:windows_server_2022
      cpe:/o:microsoft:windows_10
      Aggressive OS guesses: Microsoft Windows 11 21H2 (91%), FreeBSD 6.2-RELEASE (86%),
Microsoft
      Windows Server 2022 (85%), Microsoft Windows 10 (85%)
      No exact OS matches for host (test conditions non-ideal).
```

6. Vulnerability Assessment:

https(443):

Weak SSL/TLS configurations: If improperly configured, SSL/TLS can be vulnerable to attacks like Man-in-the-   Middle (MITM) or protocol downgrade attacks.

Vulnerabilities in web server software: This could allow attackers to exploit known vulnerabilities in the web server software.

MySQL (3306):

Weak authentication: Using weak or default passwords can lead to unauthorized access.

SQL injection: Improper input validation can lead to SQL injection attacks, allowing attackers to execute arbitrary SQL queries.

Zeroconf (5353):

DNS spoofing: Due to its use for service discovery, it can be vulnerable to DNS spoofing attacks if not properly secured.

Information leakage: Since Zeroconf is used for service discovery, information about network services may be exposed.

Zeus-admin (9090):

Default credentials: If default credentials are not changed, attackers can easily gain unauthorized access.

Vulnerabilities in Zeus-admin software: Like any other software, Zeus-admin may have vulnerabilities that could be exploited.

7. Recommendations:

Ensure proper SSL/TLS configurations, use certificates from trusted authorities, keep web server software up to date, and implement security headers.

Use strong, unique passwords, implement proper input validation to prevent SQL injection, regularly update MySQL server software, and restrict access to necessary users.

Secure DNS configurations, use DNSSEC where possible, and limit unnecessary exposure of Zeroconf services.

Change default credentials, restrict access to necessary users, regularly update Zeus-admin software, and monitor for suspicious activities.

Conclusion:

The network scan has revealed vulnerabilities in open ports and running services, including weak SSL/TLS configurations for HTTPS, potential SQL injection risks for MySQL, and susceptibility to DNS spoofing for Zeroconf. To enhance security, immediate actions such as updating software, implementing strong authentication measures, and securing DNS configurations are recommended. Addressing these vulnerabilities will bolster the network's defenses and ensure a more robust security posture.