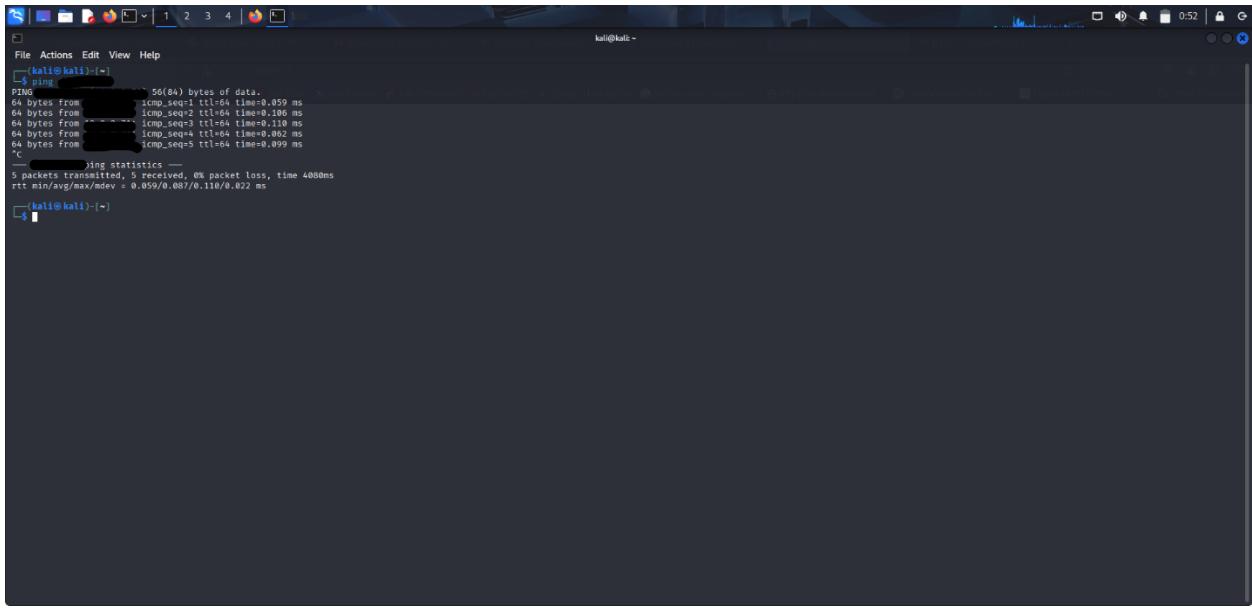


## Tools Used

- Nmap sV, sS, O, p
- NIST
- Nessus

### 1. Pinged target to make sure it had running hosts.



```
kali㉿kali:~$ ping [REDACTED]
PING [REDACTED] (192.168.1.1) 56(84) bytes of data.
64 bytes from [REDACTED]: icmp_seq=1 ttl=64 time=0.059 ms
64 bytes from [REDACTED]: icmp_seq=2 ttl=64 time=0.106 ms
64 bytes from [REDACTED]: icmp_seq=3 ttl=64 time=0.110 ms
64 bytes from [REDACTED]: icmp_seq=4 ttl=64 time=0.062 ms
64 bytes from [REDACTED]: icmp_seq=5 ttl=64 time=0.099 ms
...
      --- [REDACTED] ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4080ms
rtt min/avg/max/mdev = 0.059/0.067/0.110/0.022 ms
kali㉿kali:~$
```

### 2. Utilized Nmap to identify active host, open ports, service versions, and operating systems of the network.

-nmap -sV (Service version detection) -sS (SYN scan) -O (OS detection) -p (Full port scan)

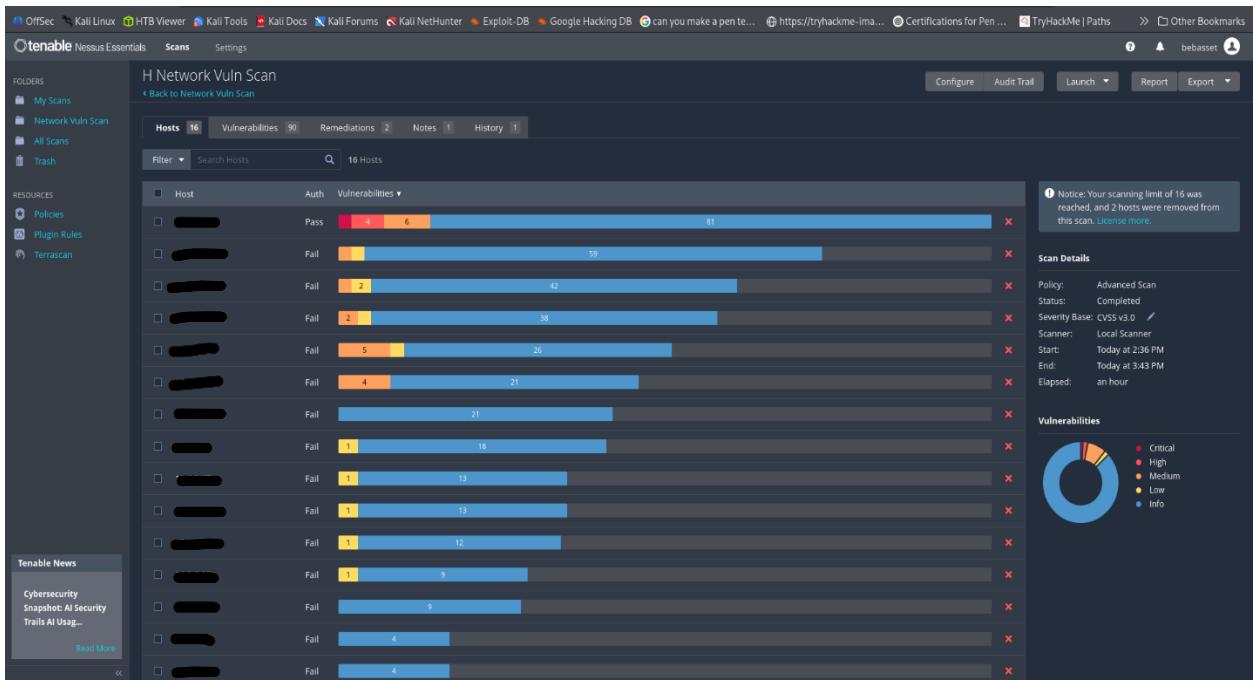
```
(kali㉿kali)-[~]
└─$ sudo nmap -sV -sS -O -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 23:06 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 11.76% done; ETC: 23:06 (0:00:08 remaining)
Stats: 0:02:09 elapsed; 16 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 79.80% done; ETC: 23:09 (0:00:32 remaining)
Stats: 0:03:48 elapsed; 16 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.52% done; ETC: 23:10 (0:00:44 remaining)
Stats: 0:04:47 elapsed; 16 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.82% done; ETC: 23:12 (0:00:47 remaining)
Stats: 0:05:46 elapsed; 16 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 88.10% done; ETC: 23:12 (0:00:46 remaining)
Stats: 0:06:38 elapsed; 16 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.07% done; ETC: 23:13 (0:00:43 remaining)
Stats: 0:08:34 elapsed; 16 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.77% done; ETC: 23:15 (0:00:28 remaining)
Stats: 0:08:35 elapsed; 16 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.81% done; ETC: 23:15 (0:00:28 remaining)
Stats: 0:09:23 elapsed; 16 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.65% done; ETC: 23:16 (0:00:19 remaining)
Stats: 0:10:57 elapsed; 16 hosts completed (4 up), 4 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 23:17 (0:00:16 remaining)
Stats: 0:10:57 elapsed; 16 hosts completed (4 up), 4 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 23:17 (0:00:16 remaining)
Stats: 0:11:05 elapsed; 16 hosts completed (4 up), 4 undergoing Service Scan
Service scan Timing: About 41.67% done; ETC: 23:17 (0:00:22 remaining)
Nmap scan report for
Host is up (0.0067s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    filtered ssh
23/tcp    filtered telnet
53/tcp    open  domain      dnsmasq 2.83
80/tcp    open  http        Xfinity Broadband Router Server
111/tcp   filtered rpcbind
443/tcp   open  ssl/https   Xfinity Broadband Router Server
1883/tcp  open  mosquito version 1.6.9
5969/tcp  filtered acmsofa
7547/tcp  filtered cwmp
8080/tcp  filtered http-proxy
```

### 3. Nessus Setup

- Sudo systemctl start nessusd.service
- Sudo systemctl status nessusd (In order to check if scanner is running)

```
(kali㉿kali)-[~/Downloads]
└─$ /bin/systemctl start nessusd.service
(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Sun 2025-08-03 21:40:54 EDT; 6min ago
     Invocation: ac1d4518a974c2ab01cc9081870cb5
   Main PID: 262085 (nessus-service)
      Tasks: 1 (limit: 2397)
        Memory: 193.4M (peak: 198.1M)
        CPU: 1min 50.347s
       CGroup: /system.slice/nessusd.service
           └─262085 /opt/nessus/sbin/nessus-service -q
Aug 03 21:40:54 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Aug 03 21:40:54 kali nessus-service[262085]: nessus-service [262085][INFO] : Nessus 19.13.2 [build 20017] Started
(kali㉿kali)-[~/Downloads]
└─$
```

4. Utilized Nessus to specify vulnerabilities and vulnerability details of network.



5. Utilized NIST (National Institute of Standards and Technology)/NVD (National Vulnerability Database) to specify the vulnerability details.

## Vulnerabilities Found

- Found 90 Vulnerabilities
- 1 Critical Level Vulnerability
- 4 High Level Vulnerabilities
- 19 Medium Level Vulnerabilities
- 10 Low Level Vulnerabilities

### CVE (Common Vulnerability Exposure):

- CVE-2007-6750

### Vulnerability Type:

- Local File Inclusion (LFI)

### Vulnerability:

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause DOS(Denial of service) (Daemon Outage) via partial HTTP requests, as demonstrated by Slowlaris related to the lack of the mod\_req timeout module in versions before 2.2.15.

#### **CVE (Common Vulnerability Exposure):**

- CVE-2005-3299

#### **Vulnerability Type:**

- Local File Inclusion (LFI)

#### **Vulnerability:**

- Includes a PHP file inclusion vulnerability in core file (grab\_globals.lib.php)
- Can expose sensitive files (e.g./etc/password) that attackers can get to RCE (Remote Control Execution)

#### **CVE (Common Vulnerability Exposure):**

- CVE-2024-21892
- CVE-2024-22019
- CVE-2024-21965
- CVE-2024-22017
- CVE-2023-46809
- CVE-2024-21891
- CVE-2024-21890

#### **Vulnerability Type:**

- Node.js Multiple Vulnerabilities

#### **Vulnerability:**

- These vulnerabilities affect various modules within Node.js and may lead to denial of service, memory corruption, or security bypass

- Impact depends on context but could allow attackers to crash or manipulate Node.js services.

#### **Fix:**

- **Upgrade to Node.js version 18.19.1 / 20.11.1 / 21.6.2 or later.**

---

#### **CVE (Common Vulnerability Exposure):**

- CVE-2024-27980
- CVE-2024-22020
- CVE-2024-36137
- CVE-2024-22018
- CVE-2024-37372

#### **Vulnerability Type:**

- Node.js Vulnerabilities
- Vulnerability:
- These CVEs involve insecure module handling and potential bypass of security restrictions in Node.js environments.
- Can lead to Remote Code Execution or elevated privileges.

#### **Fix:**

- **Upgrade to Node.js version 18.20.4 / 20.15.1 / 22.4.1 or later.**

---

#### **CVE (Common Vulnerability Exposure):**

- CVE-2024-27983
- CVE-2024-27982
- Vulnerability Type:
- Node.js Memory & Input Validation Issues
- Vulnerability:
- Potential memory exposure or corruption through improperly validated input.

**-Fix:**

- **Upgrade to Node.js version 18.20.1 / 20.12.1 / 21.7.2 or later.**

---

**CVE (Common Vulnerability Exposure):**

- CVE-2025-23085
- CVE-2025-23083
- CVE-2025-23084

**Vulnerability Type:**

- Node.js Security Bypass & Denial of Service Vulnerability:
- Exploitable flaws that allow attackers to disrupt service availability or bypass security checks.

**Fix:**

- **Upgrade to Node.js version 18.20.6 / 20.18.2 / 22.13.1 / 23.6.1 or later.**

---

**CVE (Common Vulnerability Exposure):**

- CVE-2025-27210
- CVE-2025-27209

Vulnerability Type:

- Node.js Input Validation / Memory Safety Issue

**Vulnerability:**

- Could lead to application crashes or unexpected behavior in production.

Fix:

- Upgrade to Node.js version 20.19.4 / 22.17.1 / 24.4.1 or later.

---

**CVE (Common Vulnerability Exposure):**

- CVE-2025-23165
- CVE-2025-23166

- CVE-2025-23167

**Vulnerability Type:**

- Node.js Path Traversal & Code Injection Vulnerability:
  - May allow unauthorized file access or execution of arbitrary commands.

**Fix:**

- **Upgrade to Node.js version 20.19.2 / 22.15.1 / 23.11.1 / 24.0.2 or later.**

---

## SSL Certificate Cannot Be Trusted

**Vulnerability Type:**

- SSL Misconfiguration Vulnerability:
  - The service is using a self-signed or expired certificate, which cannot be trusted by browsers or clients.

**Fix:**

- **Purchase or generate a proper SSL certificate from a trusted certificate authority (CA).**

---

## CVE (Common Vulnerability Exposure):

- CVE-2025-29087

- CVE-2025-3277

**Vulnerability Type:**

- SQLite Use-After-Free / Memory Corruption Vulnerability:
  - May lead to memory corruption or undefined behavior when parsing malformed SQL.

**Fix:**

- **Upgrade to SQLite version 3.49.1 or later.**

---

### **CVE (Common Vulnerability Exposure):**

- SQLite < 3.50.2 Memory Corruption  
Vulnerability Type:
- Heap-based Memory Corruption  
Vulnerability:
- Older versions of SQLite are vulnerable to memory corruption which can be triggered via crafted SQL inputs.

### **Fix:**

- **Upgrade to SQLite version 3.50.2 or later.**