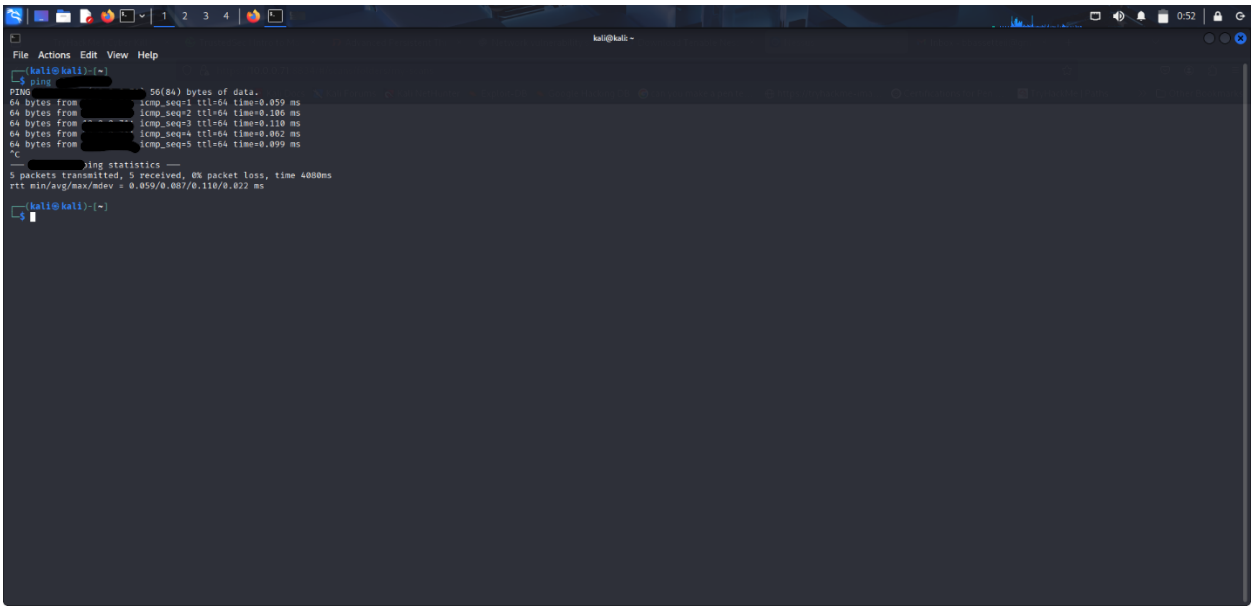
Tools Used

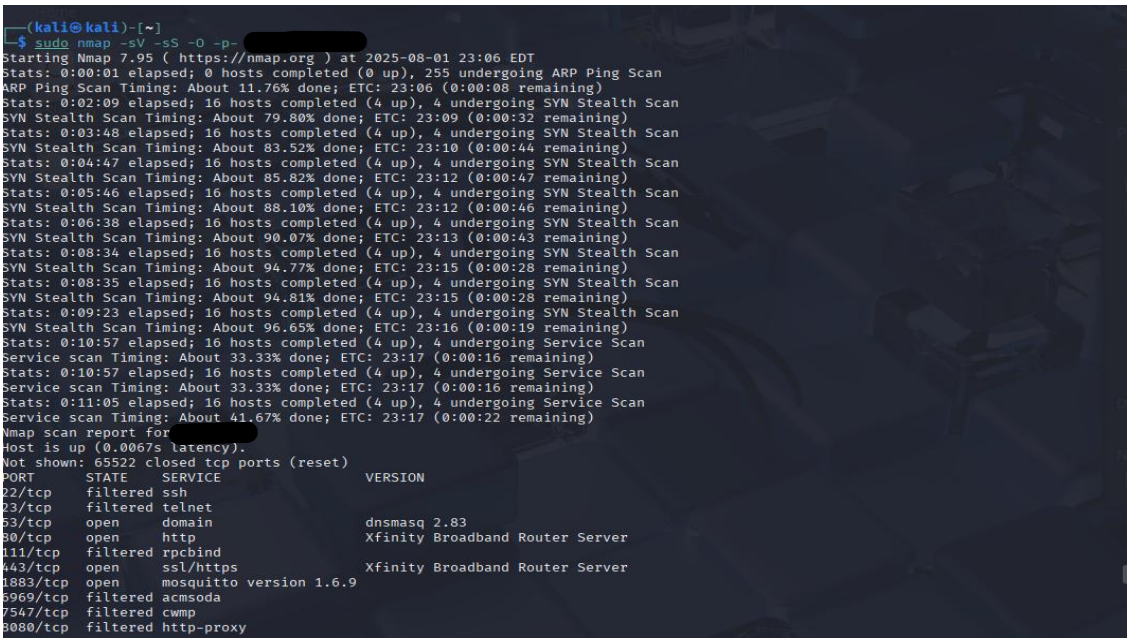
- Nmap sV, sS, O, p
- NIST
- Nessus

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



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)



3. Nessus Setup

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

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 Server1.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 Issu

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.**