VULNERABILITY ANALYSIS

Hints/Mini Guide:

1.Install OpenVAS or Nessus Essentials.

2.Set up scan target as your local machine IP or localhost.

3.Start a full vulnerability scan.

4.Wait for the scan to complete (may take 30-60 mins).

5.Review the report for vulnerabilities and severity.

6.Research simple fixes or mitigations for found vulnerabilities.

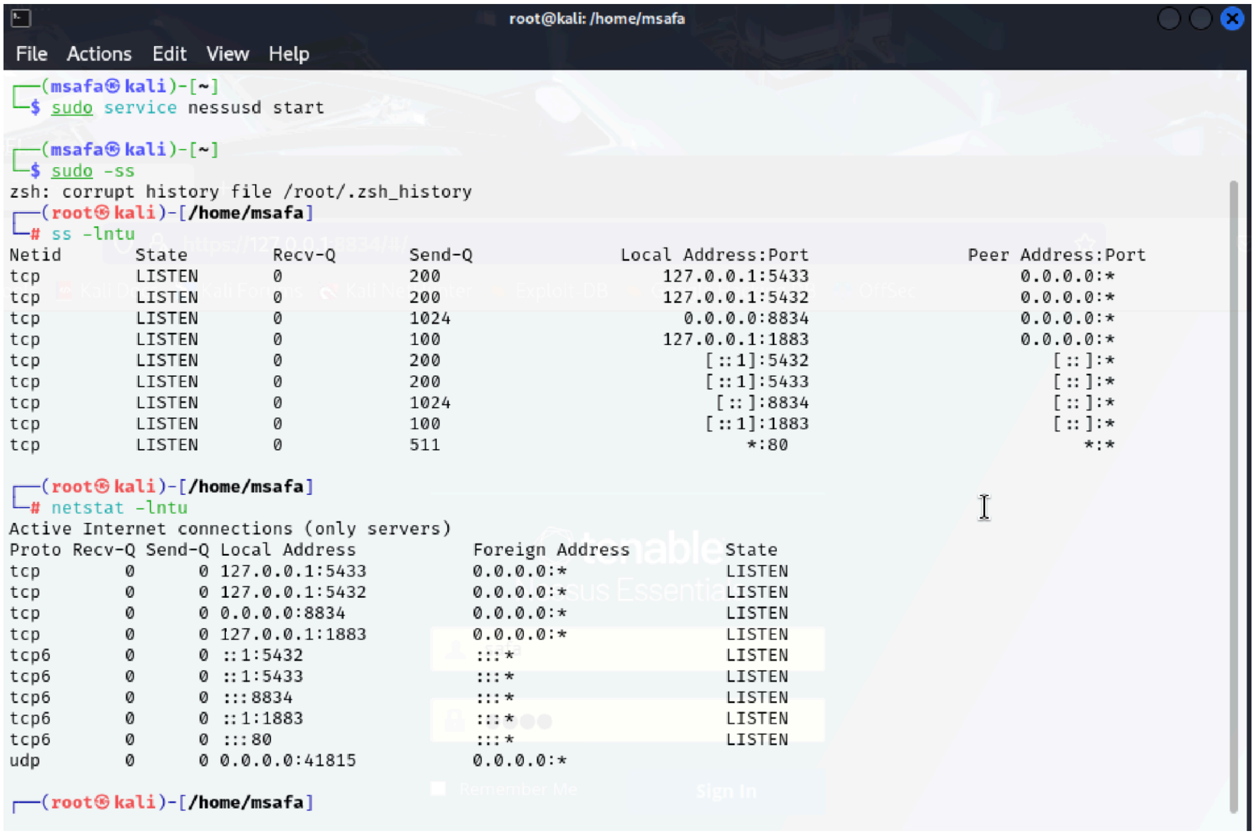
7.Document the most critical vulnerabilities.

8.Take screenshots of the scan results.

Outcome: Introductory vulnerability assessment experience and understanding of common PC risks

ANSWERS

- Nessus Essential is already installed .



```
┌──(msafa㉿kali)-[~]
└─$ sudo service nessusd start

┌──(msafa㉿kali)-[~]
└─$ sudo -ss
zsh: corrupt history file /root/.zsh_history
┌──(root㉿kali)-[/home/msafa]
└─# ss -lntu
Netid        State        Recv-Q       Send-Q               Local Address:Port               Peer Address:Port
tcp          LISTEN       0            200                      127.0.0.1:5433                    0.0.0.0:*
tcp          LISTEN       0            200                      127.0.0.1:5432                    0.0.0.0:*
tcp          LISTEN       0            1024                       0.0.0.0:8834                    0.0.0.0:*
tcp          LISTEN       0            100                      127.0.0.1:1883                    0.0.0.0:*
tcp          LISTEN       0            200                          [::1]:5432                       [::]:*
tcp          LISTEN       0            200                          [::1]:5433                       [::]:*
tcp          LISTEN       0            1024                          [::]:8834                       [::]:*
tcp          LISTEN       0            100                          [::1]:1883                       [::]:*
tcp          LISTEN       0            511                               *:80                           *:*

┌──(root㉿kali)-[/home/msafa]
└─# netstat -lntu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:5433          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8834            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:1883          0.0.0.0:*               LISTEN
tcp6       0      0 ::1:5432                :::*                    LISTEN
tcp6       0      0 ::1:5433                :::*                    LISTEN
tcp6       0      0 :::8834                 :::*                    LISTEN
tcp6       0      0 ::1:1883                :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
udp        0      0 0.0.0.0:41815           0.0.0.0:*

┌──(root㉿kali)-[/home/msafa]
```

- sudo service nessusd start this command will start the nessus vulnerability scanning tool and the service started on local port 8834 - you can navigate to the website by using the url - 127.0.0.1://8834

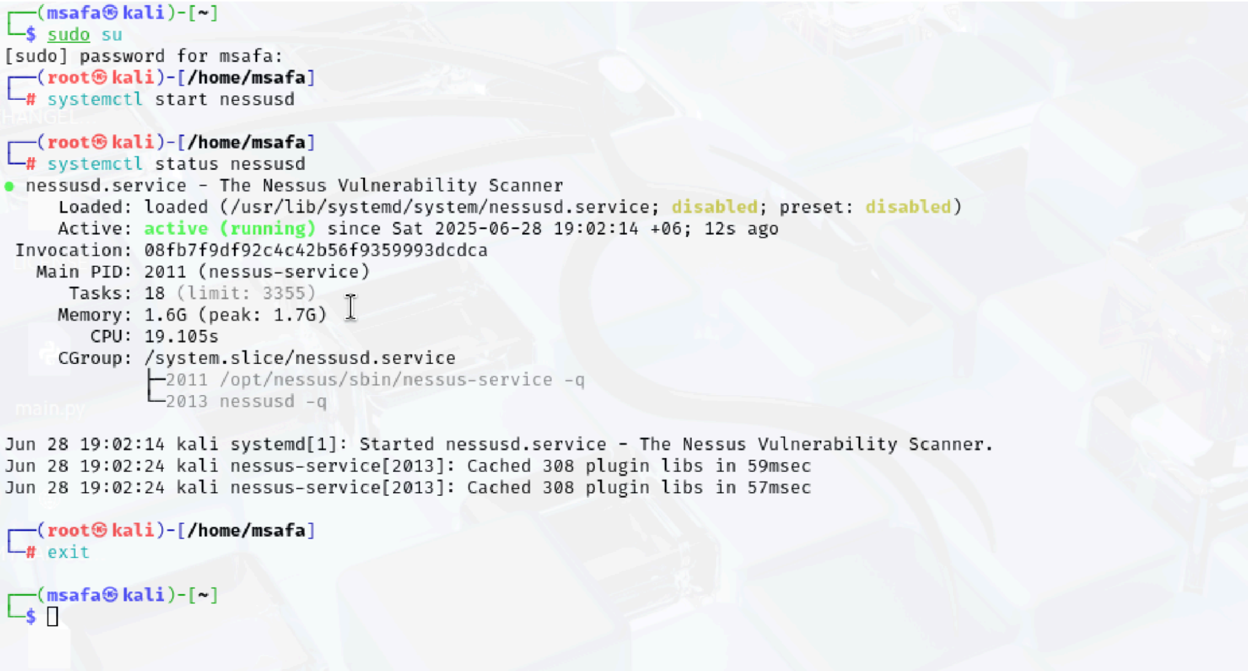
- Check the default port is open - use the command - ss -lntu   or netstat -lntu

- Another method to start and check the status of nessus using ‘systemctl’ command which is system and service manager

- sudo systemctl start nessusd

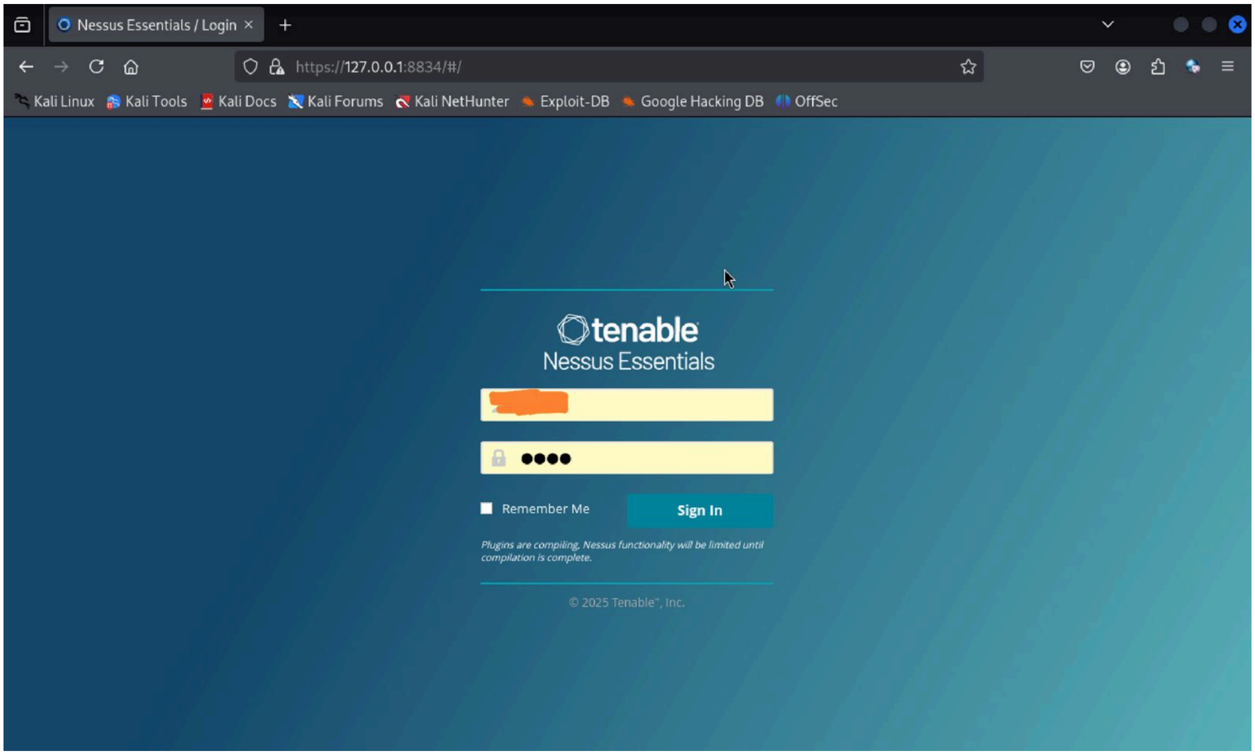
- sudo systemctl status nessusd

The below image shows it : -



```
┌──(msafa㉿kali)-[~]
└─$ sudo su
[sudo] password for msafa:
┌──(root㉿kali)-[/home/msafa]
└─# systemctl start nessusd

┌──(root㉿kali)-[/home/msafa]
└─# systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Sat 2025-06-28 19:02:14 +06; 12s ago
 Invocation: 08fb7f9df92c4c42b56f9359993dcdca
   Main PID: 2011 (nessus-service)
      Tasks: 18 (limit: 3355)
     Memory: 1.6G (peak: 1.7G)
        CPU: 19.105s
     CGroup: /system.slice/nessusd.service
             ├─2011 /opt/nessus/sbin/nessus-service -q
             └─2013 nessusd -q

Jun 28 19:02:14 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Jun 28 19:02:24 kali nessus-service[2013]: Cached 308 plugin libs in 59msec
Jun 28 19:02:24 kali nessus-service[2013]: Cached 308 plugin libs in 57msec

┌──(root㉿kali)-[/home/msafa]
└─# exit

┌──(msafa㉿kali)-[~]
└─$ ▯
```

- Go to the web interface of the nessus - http://127.0.0.1:8834



[redacted]

●●●●

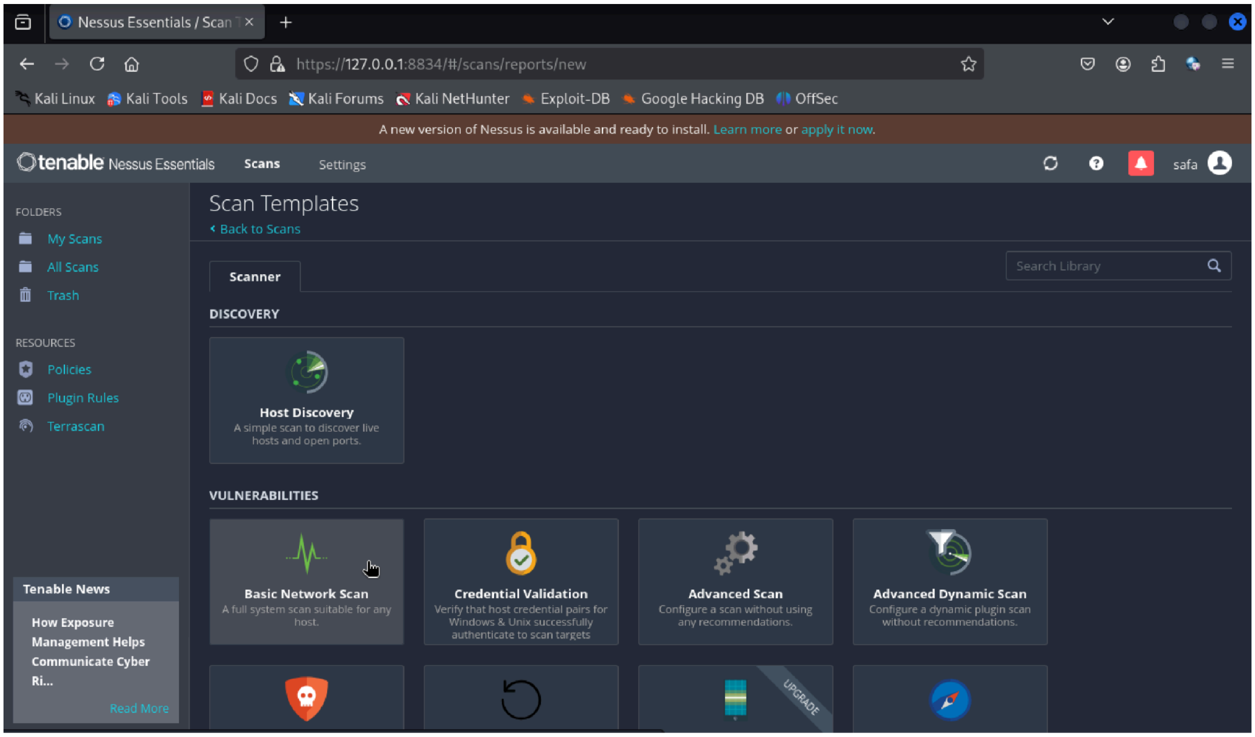
Plugins are compiling. Nessus functionality will be limited until compilation is complete.

© 2025 Tenable™, Inc.

-

Now we are on the tenable - Nessus Essentials - Vulnerability Scanner
Go to new scan
Select basic Network scan

-



A new version of Nessus is available and ready to install. Learn more or apply it now.

Host Discovery – A simple scan to discover live hosts and open ports.

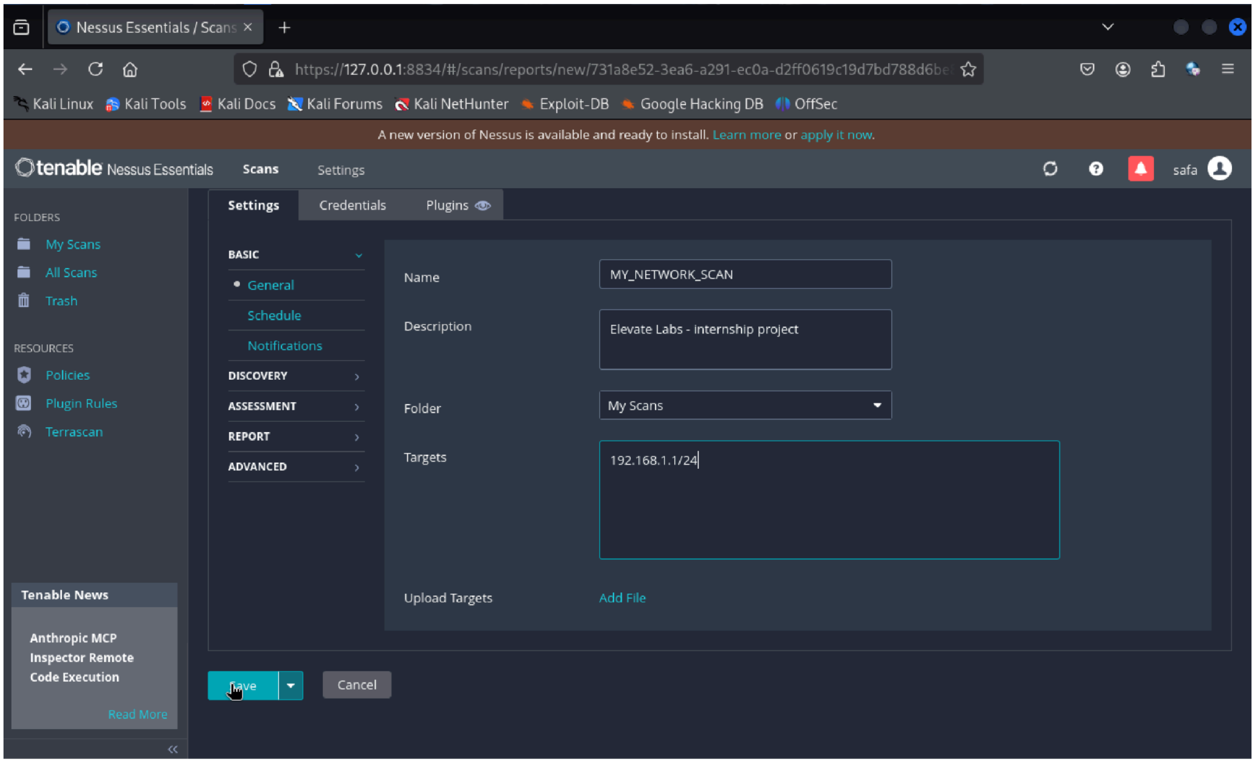
Basic Network Scan – A full system scan suitable for any host.

Credential Validation – Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets

Advanced Scan – Configure a scan without using any recommendations.

Advanced Dynamic Scan – Configure a dynamic plugin scan without recommendations.

Give every essential details - Targets and Name of the scan



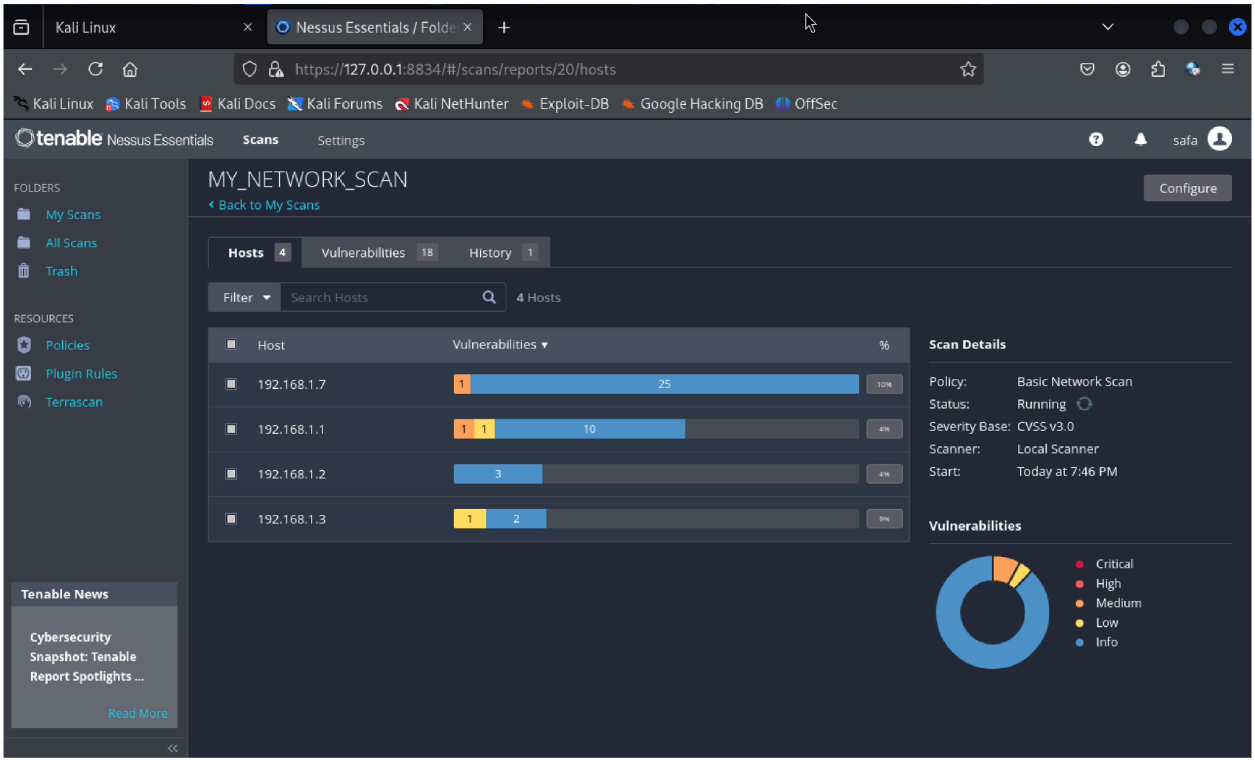
A new version of Nessus is available and ready to install. Learn more or apply it now.

Name: MY_NETWORK_SCAN

Description: Elevate Labs - internship project

Folder: My Scans

Targets: 192.168.1.1/24



https://127.0.0.1:8834/#/scans/reports/20/hosts

MY_NETWORK_SCAN

‹ Back to My Scans

Hosts 4 | Vulnerabilities 18 | History 1

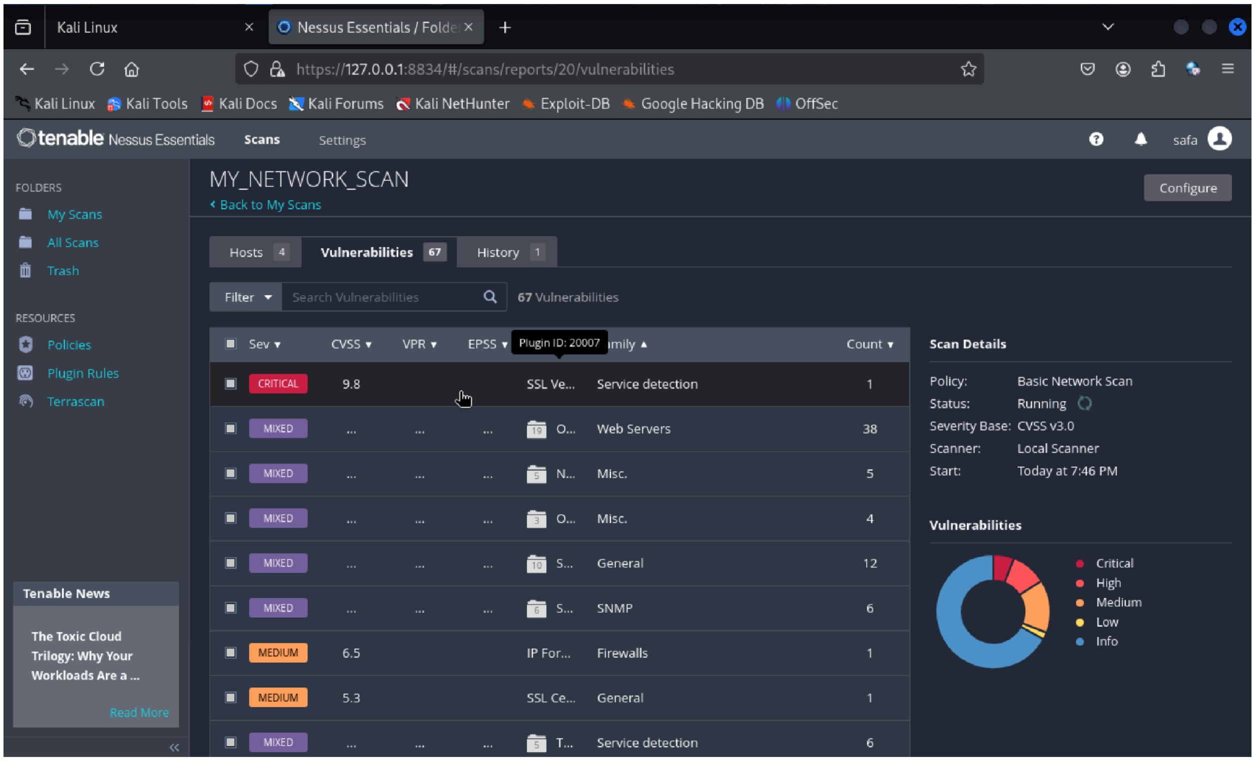
4 Hosts

Host	Vulnerabilities	%
192.168.1.7	1 · 25	10%
192.168.1.1	1 · 1 · 10	4%
192.168.1.2	3	4%
192.168.1.3	1 · 2	9%

Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 7:46 PM

Vulnerabilities



https://127.0.0.1:8834/#/scans/reports/20/vulnerabilities

MY_NETWORK_SCAN

‹ Back to My Scans

Hosts 4 | Vulnerabilities 67 | History 1

67 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	9.8			SSL Ve...	Service detection	1
MIXED	...	...	...	10 O...	Web Servers	38
MIXED	...	...	...	5 N...	Misc.	5
MIXED	...	...	...	3 O...	Misc.	4
MIXED	...	...	...	10 S...	General	12
MIXED	...	...	...	6 S...	SNMP	6
MEDIUM	6.5			IP For...	Firewalls	1
MEDIUM	5.3			SSL Ce...	General	1
MIXED	...	...	...	5 T...	Service detection	6

Plugin ID: 20007

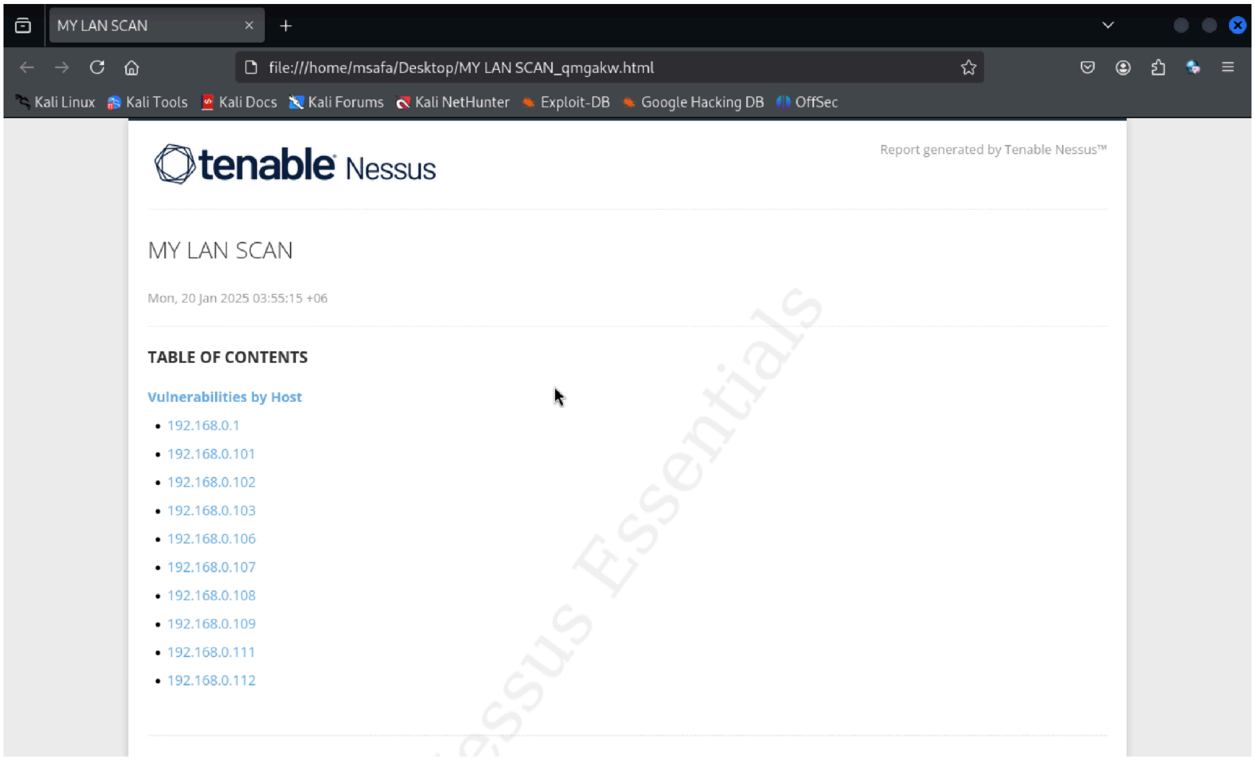
Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 7:46 PM

Vulnerabilities

Automatic vulnerability scanning started and it is showing as much information needed and the description also.

- We can download the report in various formats like pdf and html . I prefer html.



Report generated by Tenable Nessus™

MY LAN SCAN

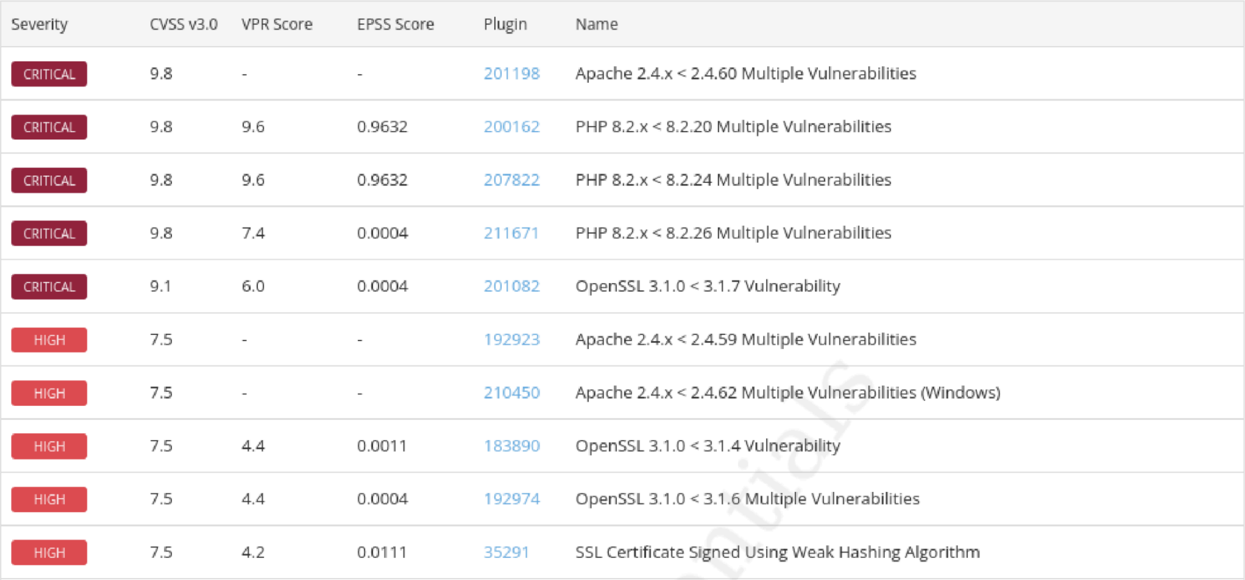
Mon, 20 Jan 2025 03:55:15 +06

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.0.1
- 192.168.0.101
- 192.168.0.102
- 192.168.0.103
- 192.168.0.106
- 192.168.0.107
- 192.168.0.108
- 192.168.0.109
- 192.168.0.111
- 192.168.0.112

You can get every endpoints scanned details by clicking the appropriate IP address



Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
CRITICAL	9.8	-	-	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	200162	PHP 8.2.x < 8.2.20 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	207822	PHP 8.2.x < 8.2.24 Multiple Vulnerabilities
CRITICAL	9.8	7.4	0.0004	211671	PHP 8.2.x < 8.2.26 Multiple Vulnerabilities
CRITICAL	9.1	6.0	0.0004	201082	OpenSSL 3.1.0 < 3.1.7 Vulnerability
HIGH	7.5	-	-	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	-	-	210450	Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)
HIGH	7.5	4.4	0.0011	183890	OpenSSL 3.1.0 < 3.1.4 Vulnerability
HIGH	7.5	4.4	0.0004	192974	OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities
HIGH	7.5	4.2	0.0111	35291	SSL Certificate Signed Using Weak Hashing Algorithm

✅ Core Elements of Nessus Vulnerability Scanning

🔹 1. Discovery / Network Enumeration

- **Purpose**: Identify all live hosts within the target IP range or network.
- **How**: Uses ping sweeps (ICMP), TCP SYN scans, ARP scans (for local network).
- **Output**: Active hosts, open ports, services detected.

🔹 2. Port Scanning

- **Purpose**: Discover which TCP/UDP ports are open on each host.
- **How**: SYN scan, Connect scan, or version-specific scanning.
- **Output**: Open ports → e.g., 80/tcp (HTTP), 443/tcp (HTTPS), 22/tcp (SSH).

🔹 3. Service & Version Detection

- **Purpose**: Identify what services are running on those open ports and their versions.
- **How**: Banner grabbing, protocol handshakes, fingerprinting.
- **Output**: e.g., Apache HTTPD 2.4.41, OpenSSH 8.0

🔹 4. OS Detection

- **Purpose**: Estimate the operating system type and version.
- **How**: Analyzes TTL, TCP/IP stack behavior, service banners.
- **Output**: e.g., Linux Kernel 5.x, Windows Server 2019.

🔹 5. Vulnerability Enumeration

- **Purpose**: Match detected services & OS versions to known vulnerabilities (CVEs).
- **How**: Uses Nessus plugins/rules with CVE databases and vendor advisories.
- **Output**: List of vulnerabilities with severity ratings (Critical, High, Medium, Low).

🔹 6. Risk Rating & CVSS Scoring

- **Purpose**: Prioritize vulnerabilities based on impact and exploitability.

- **How**: CVSS (Common Vulnerability Scoring System) base scores.
- **Output**: e.g., CVE-2021-34527 — CVSS 9.8 (Critical).

🔹 7. Proof of Concept or Exploit Checks (Safe)

- **Purpose**: Some plugins can verify if a vulnerability is real (safe checks).
- **How**: May send non-destructive probes to confirm.
- **Output**: Confirmed vs. potential vulnerabilities.

🔹 8. Reporting

- **Purpose**: Generate detailed reports for remediation.
- **Includes**:
    - Host summaries
    - Vulnerability details with descriptions
    - Risk scores
    - Suggested fixes or references to patches

Review the Report for Vulnerabilities

- Once finished, open the **report** or **task results**
- Look for:
    - **Critical (Red)**
    - **High (Orange)**
    - **Medium (Yellow)**

- Review:
    - CVE IDs
    - Plugin/Family
    - Affected services (e.g., open ports, misconfigurations)

Research Fixes for Found Vulnerabilities

For each major finding:

- Google CVE ID or plugin title
- Common fixes:

- Updating software (e.g., Apache, OpenSSH)
- Disabling unused ports/services
- Applying system patches
- Configuring firewalls properly

Research Simple Fixes or Mitigations

Here's a simplified list of some critical and high vulnerabilities from thescan with practical mitigation suggestions:

Vulnerability	CVE / Plugin	Severity	Fix / Mitigation
Apache 2.4.x < 2.4.60 Multiple Vulnerabilities	Plugin: 201198	Critical	Upgrade Apache to version **2.4.60** or newer using your package manager or from source.
PHP 8.2.x < 8.2.20 / 8.2.24 / 8.2.26	Plugins: 200162, 207822, 211671	Critical	Update PHP to at least **8.2.26** to patch remote code execution and memory corruption issues.
OpenSSL 3.1.0 < 3.1.7 / 3.1.4 / 3.1.6	Plugins: 201082, 183890, 192974	Critical / High	Upgrade OpenSSL to **3.1.7 or latest stable version** to fix memory handling, DoS, and potential leakage issues.
SSL Certificate Signed Using Weak Hashing Algorithm	Plugin: 35291	High	Reissue your SSL certificate using a **stronger hash algorithm (e.g., SHA-256)**.
OpenSSL 3.1.0 < 3.1.5 / 3.1.8	Plugins: 185161, 209154	Medium	Ensure OpenSSL is updated beyond 3.1.8. Use `apt upgrade openssl` or equivalent.

SSL Self-Signed / Cannot Be Trusted / Expired / Wrong Hostname	Plugins: 51192, 57582, 45411, etc.	Medium	Replace self-signed or expired certs with CA-signed ones and ensure hostname matches the cert.
HTTP TRACE / TRACK Methods Allowed	Plugin: 11213	Medium	Disable TRACE / TRACK in Apache by setting `TraceEnable Off` in the config.
SMB Signing Not Required	Plugin: 57608	Medium	Enable SMB signing in Samba config for integrity protection.

Document the Most Critical Vulnerabilities

Here's a professional documentation format for reporting:

📄 Vulnerability Report Summary

1. Apache 2.4.x < 2.4.60 Multiple Vulnerabilities

- **Severity**: Critical (CVSS: 9.8)
- **Plugin ID**: 201198
- **Description**: Remote attackers may exploit memory corruption, privilege escalation, or denial of service flaws in outdated Apache versions.
- **Fix**: Update Apache to **v2.4.60** or higher.

---

2. PHP 8.2.x < 8.2.26 Multiple Vulnerabilities

- **Severity**: Critical (CVSS: 9.8)
- **Plugin IDs**: 200162, 207822, 211671
- **Description**: Multiple RCE and buffer overflow vulnerabilities in outdated PHP version.
- **Fix**: Upgrade to **PHP 8.2.26**.

---

3. OpenSSL 3.1.0 < 3.1.7

- **Severity**: Critical (CVSS: 9.1)
- **Plugin ID**: 201082
- **Description**: Buffer over-read and DoS vulnerabilities due to improper handling of X.509 certificates.
- **Fix**: Upgrade OpenSSL to **3.1.7** or later.

---

4. SSL Certificate Signed Using Weak Hashing Algorithm

- **Severity**: High (CVSS: 7.5)
- **Plugin ID**: 35291
- **Description**: SSL cert is signed with a weak hash like **SHA-1**.
- **Fix**: Use **SHA-256 or better** when generating certs.

---

5. SSL Self-Signed Certificate / Cannot Be Trusted

- **Severity**: Medium
- **Plugin IDs**: 51192, 57582
- **Description**: Certificates are not signed by a trusted CA.
- **Fix**: Purchase or generate certs signed by **Let’s Encrypt** or another trusted CA.