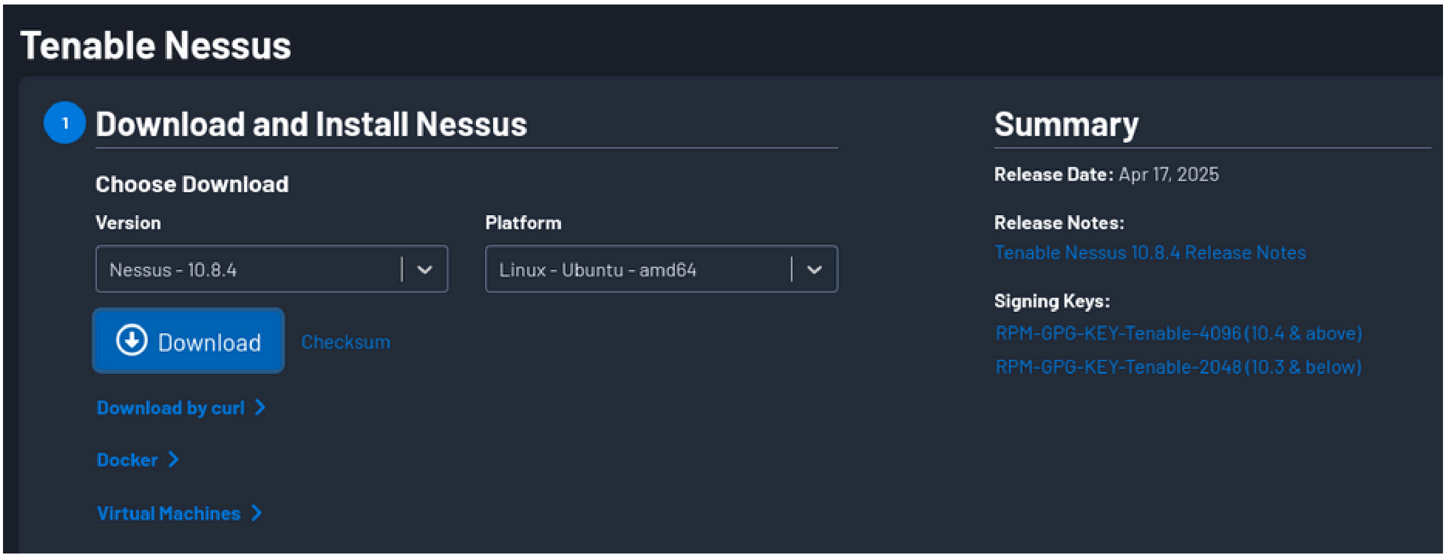
ELEVATE LABS CYBER SECURITY INTERNSHIP

Task-3:

1.Install Nessus Essentials

Downloaded the file through nessus website



Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.8.4

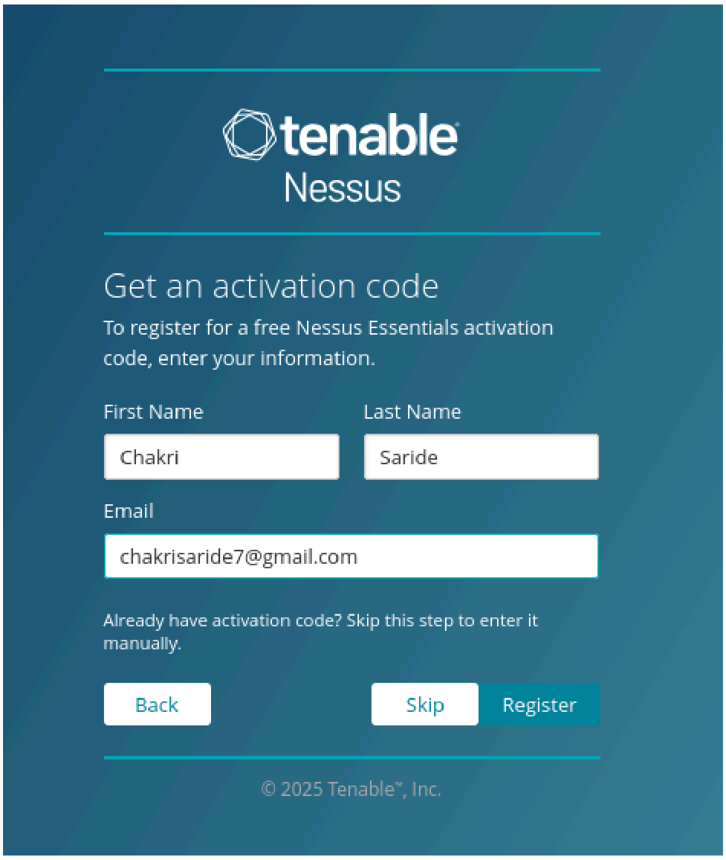
Platform: Linux - Ubuntu - amd64

Summary

Release Date: Apr 17, 2025

Release Notes:
Tenable Nessus 10.8.4 Release Notes

Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)



tenable Nessus

Get an activation code

To register for a free Nessus Essentials activation code, enter your information.

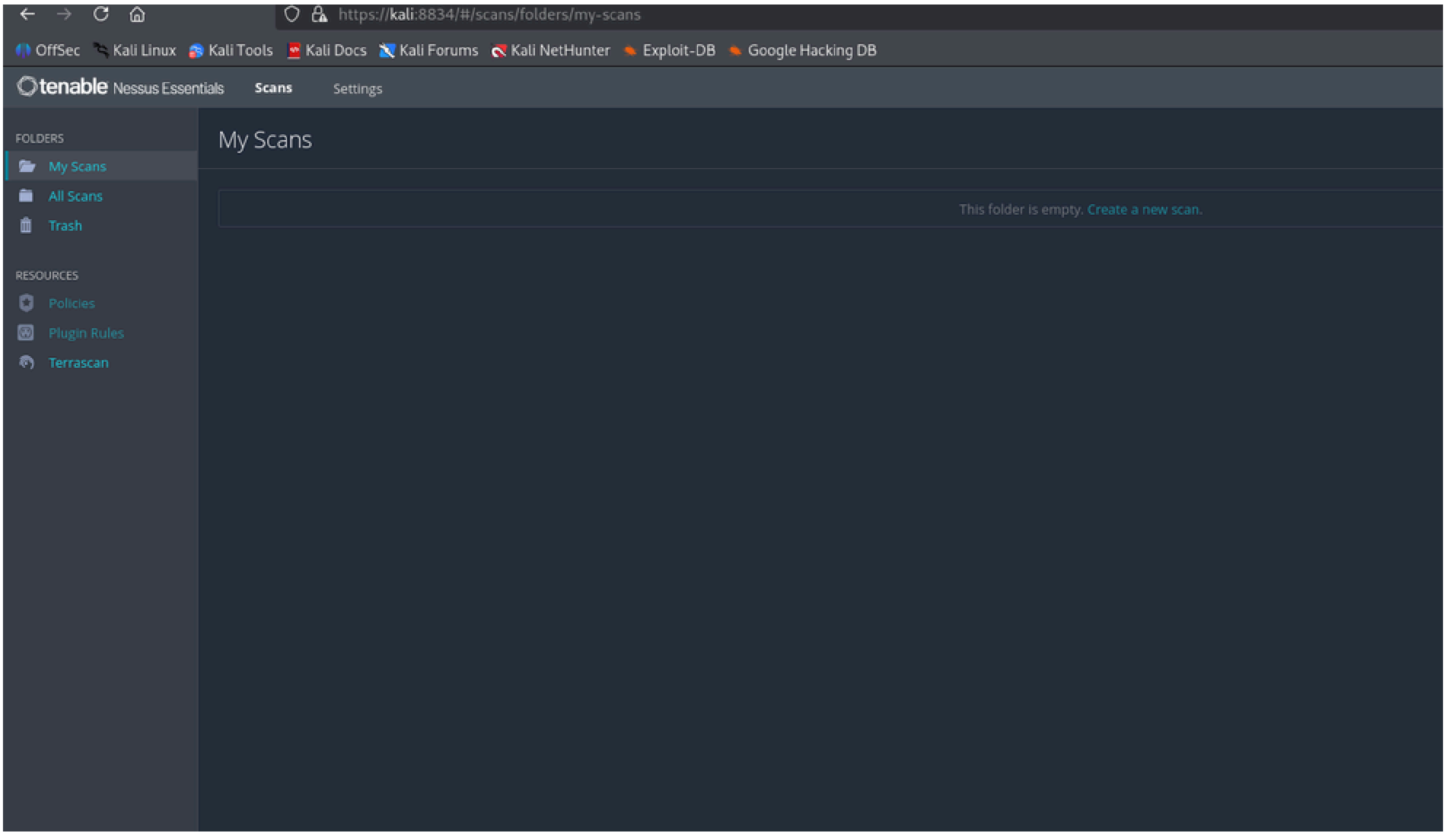
First Name: Chakri

Last Name: Saride

Email: chakrisaride7@gmail.com

Already have activation code? Skip this step to enter it manually.

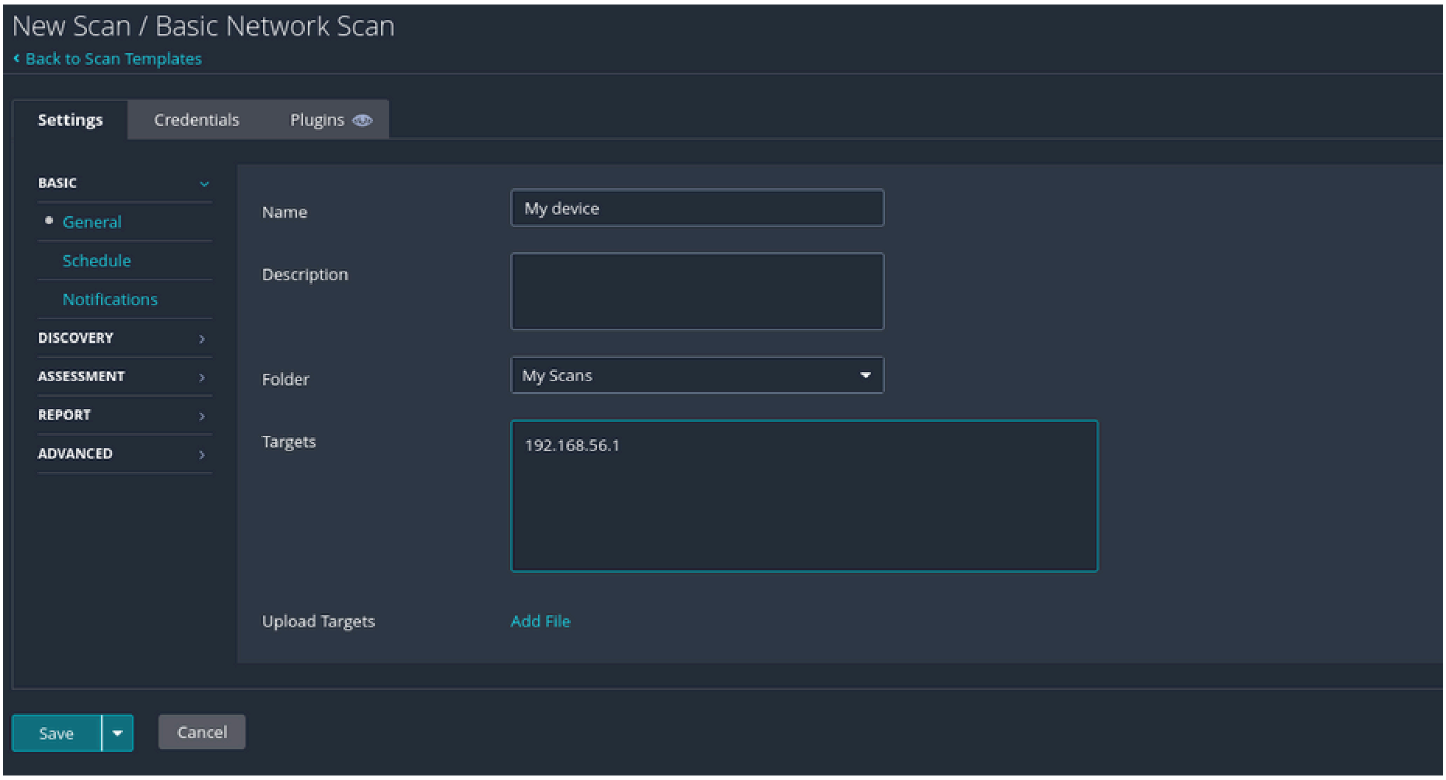
© 2025 Tenable™, Inc.



My Scans

This folder is empty. Create a new scan.

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



New Scan / Basic Network Scan

Name: My device

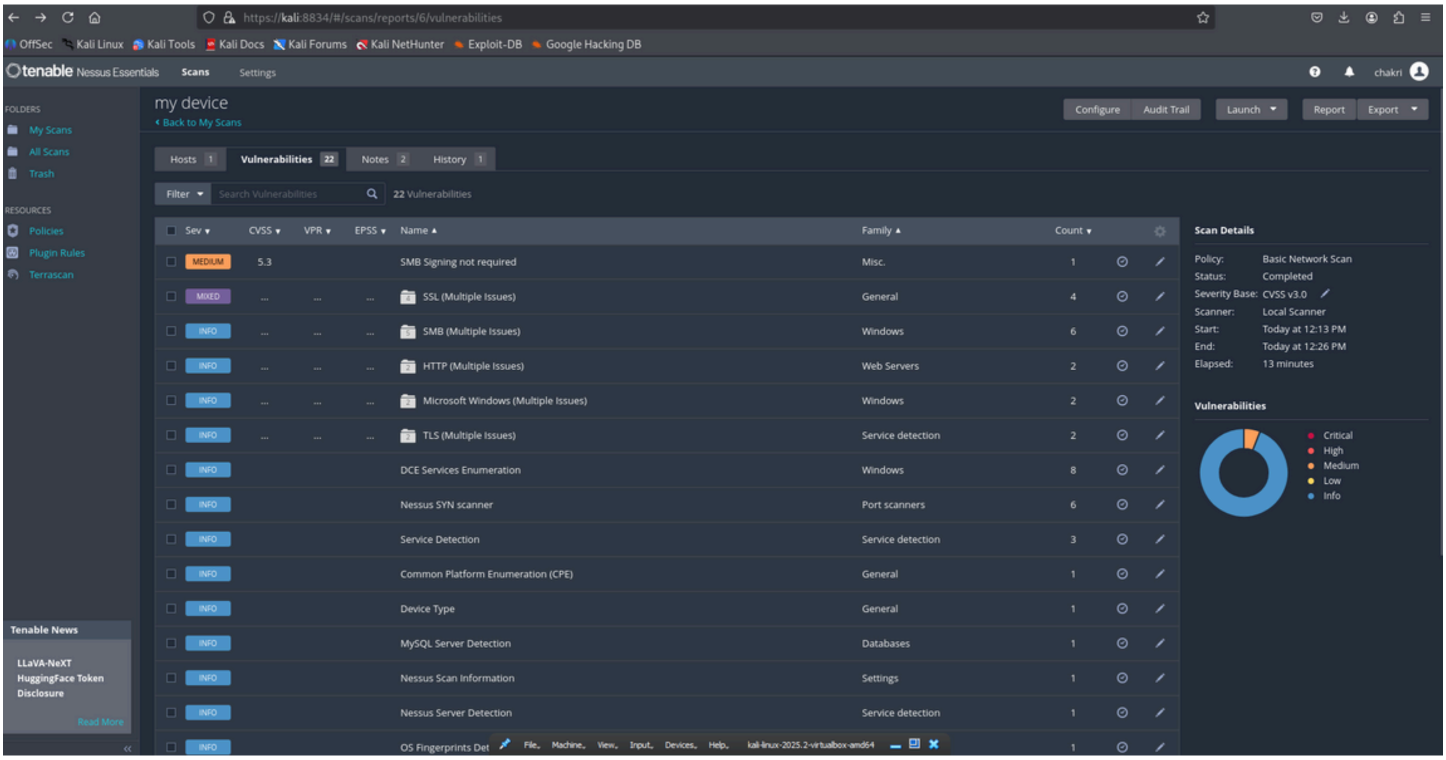
Description:

Folder: My Scans

Targets: 192.168.56.1

3.Start a full vulnerability scan and

4.Wait for scan to complete.



22 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not required	Misc.	1
MIXED	...	...	...	SSL (Multiple Issues)	General	4
INFO	...	...	...	SMB (Multiple Issues)	Windows	6
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	2
INFO	...	...	...	Microsoft Windows (Multiple Issues)	Windows	2
INFO	...	...	...	TLS (Multiple Issues)	Service detection	2
INFO				DCE Services Enumeration	Windows	8
INFO				Nessus SYN scanner	Port scanners	6
INFO				Service Detection	Service detection	3
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				MySQL Server Detection	Databases	1
INFO				Nessus Scan Information	Settings	1
INFO				Nessus Server Detection	Service detection	1
INFO				OS Fingerprints Det		1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:13 PM
End: Today at 12:26 PM
Elapsed: 13 minutes

Vulnerabilities

● Critical
● High
● Medium
● Low
● Info

5.Review the report for vulnerabilities and severity.

Name	Notes
SSL (Multiple Issues)	Likely includes weak ciphers, self-signed certs, deprecated SSL versions. If so, it’s worth reviewing your SSL/TLS configuration.
SMB (Multiple Issues)	Could indicate open ports, SMBv1 usage, or banner grabbing. Review for legacy protocol usage.
HTTP (Multiple Issues)	Might include missing security headers (e.g., CSP, HSTS), verbose banners, etc. Helps attackers fingerprint services.
Microsoft Windows (Multiple Issues)	May include info about OS version, build, and services. Useful for attackers to identify potential exploits.
TLS (Multiple Issues)	Could include support for deprecated versions like TLS 1.0/1.1. Should only support TLS 1.2/1.3.
DCE Services Enumeration	Indicates exposure of RPC services. May be used for lateral movement or service abuse in Windows environments.
Nessus SYN scanner	Internal to the scan, no risk.
Service Detection	Lists open ports and services; useful for mapping your attack surface.
Common Platform Enumeration (CPE)	Identifies software based on responses; good for inventory.
MySQL Server Detection	Confirms a MySQL instance is exposed – if it’s public-facing, that’s a risk.
OS Fingerprinting / Identification	Reveals OS and version; helpful to attackers but not a direct vulnerability.
Nessus Scan Information / Server	Meta info from the scanner – no action

Nessus Scan Information / Server Detection	Meta info from the scanner — no action required.

6.Research simple fixes or mitigations for found vulnerabilities.

1. SMB Signing Not Required

- **Severity**: Medium (CVSS 5.3)
- **Risk**: Allows Man-in-the-Middle (MitM) attacks over SMB.
- **Fix**:
  - Enable SMB signing via Group Policy:
    - Microsoft network client/server: Digitally sign communications (always)
  - Restart system after applying.

2. SSL / TLS (Multiple Issues)

- **Severity**: Informational (may include weak ciphers, SSLv3, self-signed certs).
- **Fix**:
  - Disable SSLv2/3, TLS 1.0/1.1.
  - Use only TLS 1.2/1.3 with strong ciphers (AES-GCM, SHA256).
  - Ensure valid certificates from a trusted CA.

3. SMB (Multiple Issues)

- **Fix**:
  - Disable SMBv1:
    ```
    Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
    ```
  - Ensure SMB signing is enforced.
  - Block port 445 externally.

4. HTTP (Multiple Issues)

- **Fix**:
  - Add security headers (CSP, X-XSS-Protection, etc.).
  - Remove banner/version info.
  - Use HTTPS and redirect HTTP traffic.

5. DCE Services Enumeration

- **Fix**:
  - Block RPC ports (135, 139, 445) via firewall.
  - Disable unnecessary services like Remote Registry.
  - Use host-based firewall rules.

6. MySQL Server Detection

- **Fix**:
  - Bind MySQL to localhost (bind-address = 127.0.0.1).
  - Use strong passwords; disable remote root login.

7.Document the most critical vulnerabilities

The most critical vulnerability found in the scan is “SMB Signing Not Required.” This means that while SMB signing is supported on the system, it is not enforced. SMB (Server Message Block) is a protocol used in Windows systems for file sharing, printer access, and other network services. When signing is not required, an attacker on the same network can intercept and alter the communication between systems, leading to Man-in-the-Middle (MitM) attacks. This allows them to steal credentials, hijack sessions, or inject malicious data into the traffic.

To fix this issue, we plan to enforce SMB signing on all systems. This can be done by enabling two settings in the Group Policy Editor: “Microsoft network client: Digitally sign communications (always)” and “Microsoft network server: Digitally sign communications (always).” Once these are enabled and the systems are restarted, all SMB traffic will be cryptographically signed, preventing tampering or impersonation. This change will significantly reduce the risk of SMB-based attacks in our environment.