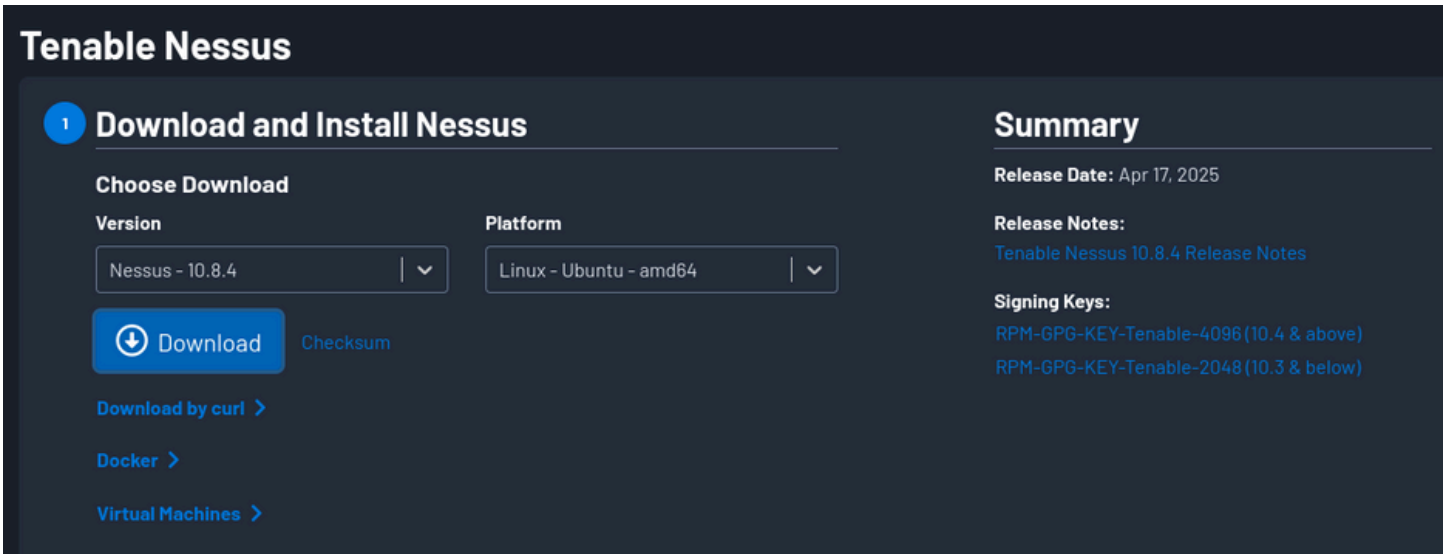
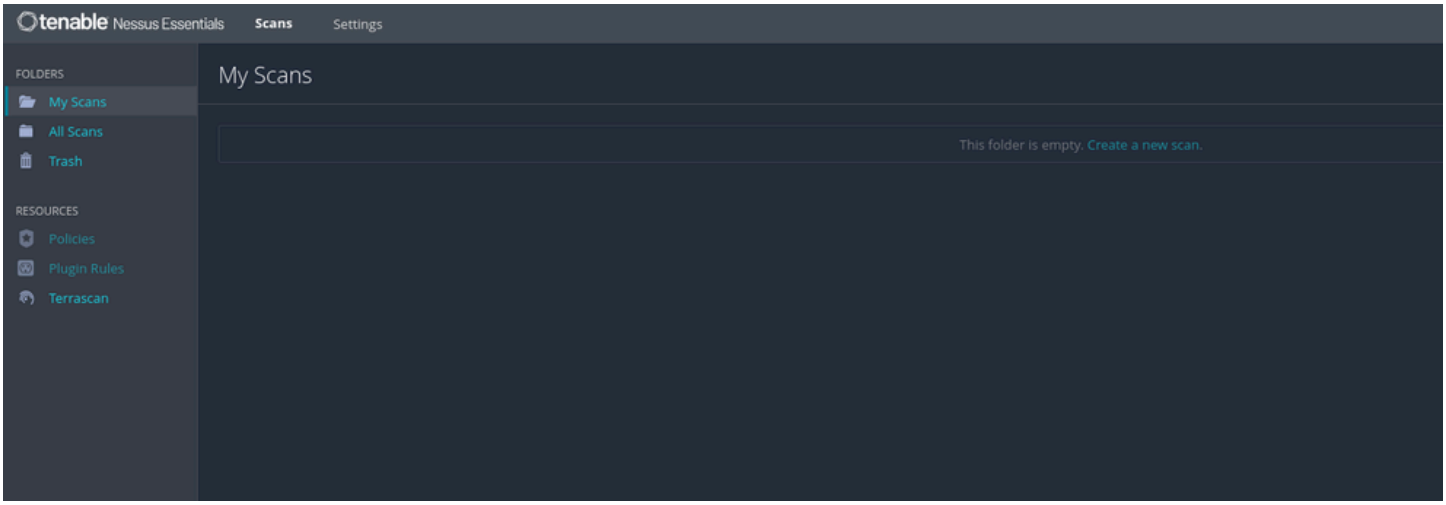
ELEVATE LABS CYBER SECURITY INTERNSHIP

Task-3:

1. Install Nessus Essentials

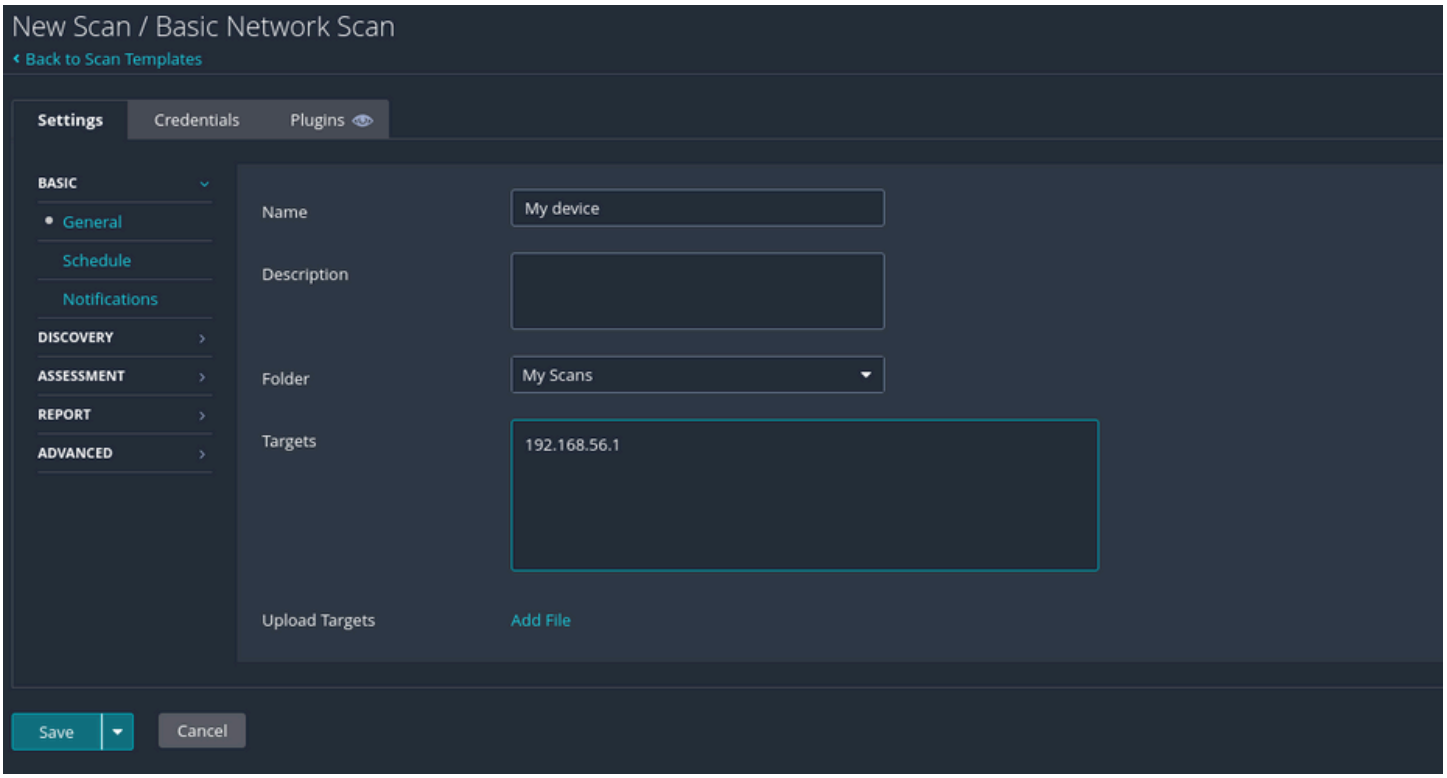
Successfully downloaded and installed **Nessus Essentials** from the official Tenable website.





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

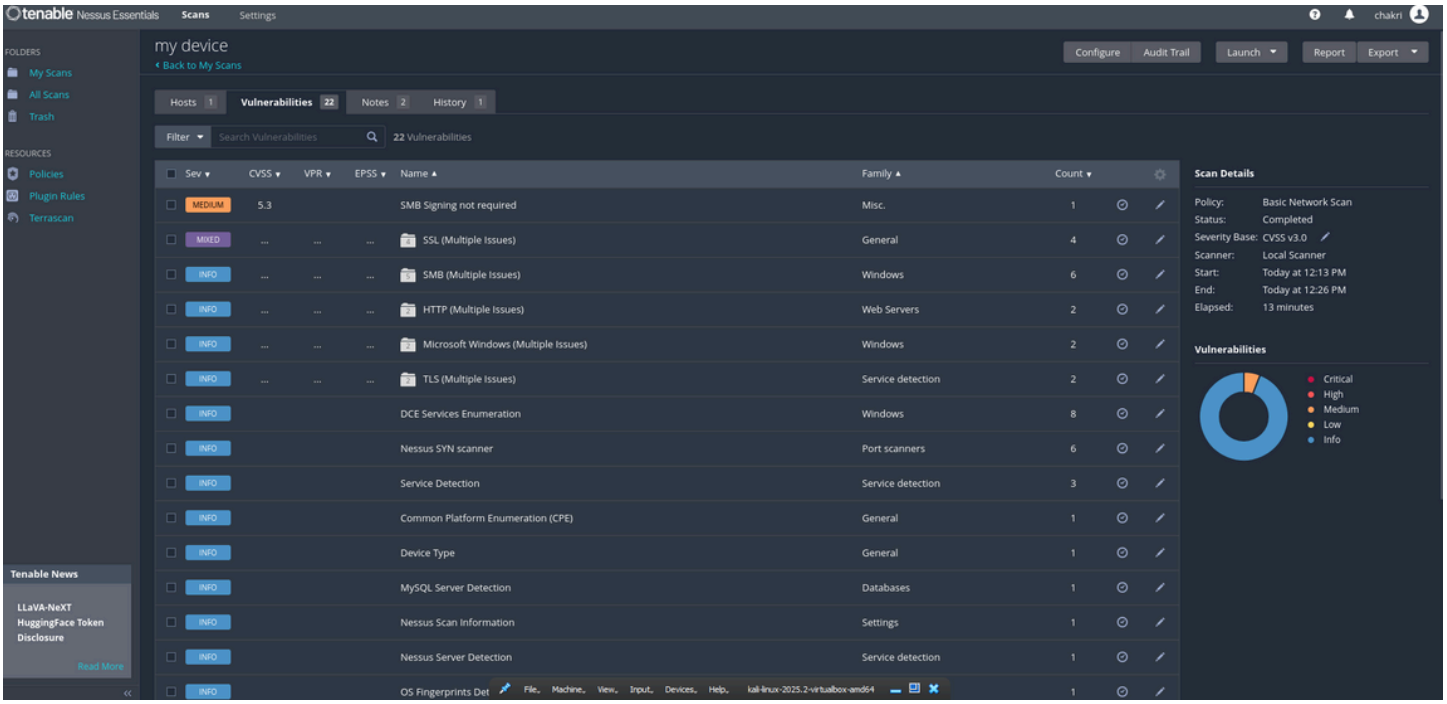
- Configured scan target as the **local machine IP address**.
- Selected **Full Vulnerability Scan** from the scan templates.



3. Start a full vulnerability scan.

4. Wait for scan to complete.

- Initiated the scan and allowed Nessus to complete a full assessment of the system.
- The scan ran successfully and generated a comprehensive report of identified vulnerabilities.



5. Review the report for vulnerabilities and severity.

Name	Description
SSL (Multiple Issues)	SSL/TLS configuration contains deprecated protocols (e.g., SSLv3), self-signed certificates, or weak ciphers. This could compromise encrypted communications.
SMB (Multiple Issues)	Possible use of outdated SMBv1, open ports, or banners revealing system information. These are exploitable via legacy protocols.
HTTP (Multiple Issues)	Missing security headers (like CSP, HSTS) and excessive version/banner information increase susceptibility to reconnaissance and attacks.
Microsoft Windows (Multiple Issues)	Reveals system OS, build, and version — assisting attackers in crafting targeted exploits.
TLS (Multiple Issues)	Supports outdated TLS versions (1.0/1.1). Secure systems should only support TLS 1.2 or 1.3.
DCE Services Enumeration	RPC services are discoverable. May enable lateral movement within a network.
Service Detection	Exposed ports and services mapped. Useful for attacker reconnaissance.
Common Platform Enumeration (CPE)	Software recognized via fingerprinting. Helps in inventorying but also exposes software details.
MySQL Server Detection	Detects exposed MySQL service. If public-facing, it’s a serious risk.
OS Fingerprinting / Identification	Identifies system OS and version — not a direct threat but aids attackers.

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:
    - Client: “Digitally sign communications (always)”
    - 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.
  - Enable only TLS 1.2/1.3 with strong ciphers (AES-GCM, SHA256).
  - Use 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, X-Content-Type-Options, etc.).
  - Redirect HTTP to HTTPS.

5. DCE Services Enumeration

- **Fix**:
  - Block RPC ports (135, 139, 445) using firewalls.
  - Disable unnecessary services like Remote Registry.
  - Enforce local firewall rules.

6. MySQL Server Detection

- **Fix**:
  - Bind MySQL to localhost (bind-address = 127.0.0.1).
  - Disable remote root login and use strong passwords.

7. Document the most critical vulnerabilities

SMB Signing Not Required

Severity: Medium (CVSS 5.3)
Impact: Without enforced signing, SMB communications can be intercepted or altered, exposing the system to **Man-in-the-Middle (MitM)** attacks. This could result in session hijacking, credential theft, or malicious payload injection.

Remediation Plan:

1. Enable SMB signing for both clients and servers:
    - Navigate to **Group Policy Editor**.
    - Configure:
        - Microsoft network client: Digitally sign communications (always)
        - Microsoft network server: Digitally sign communications (always)
2. Apply the changes and **restart** the affected systems.

🛡️ This configuration ensures all SMB traffic is **cryptographically verified**, effectively neutralizing tampering attempts and enhancing the system's resistance to network-based attacks.