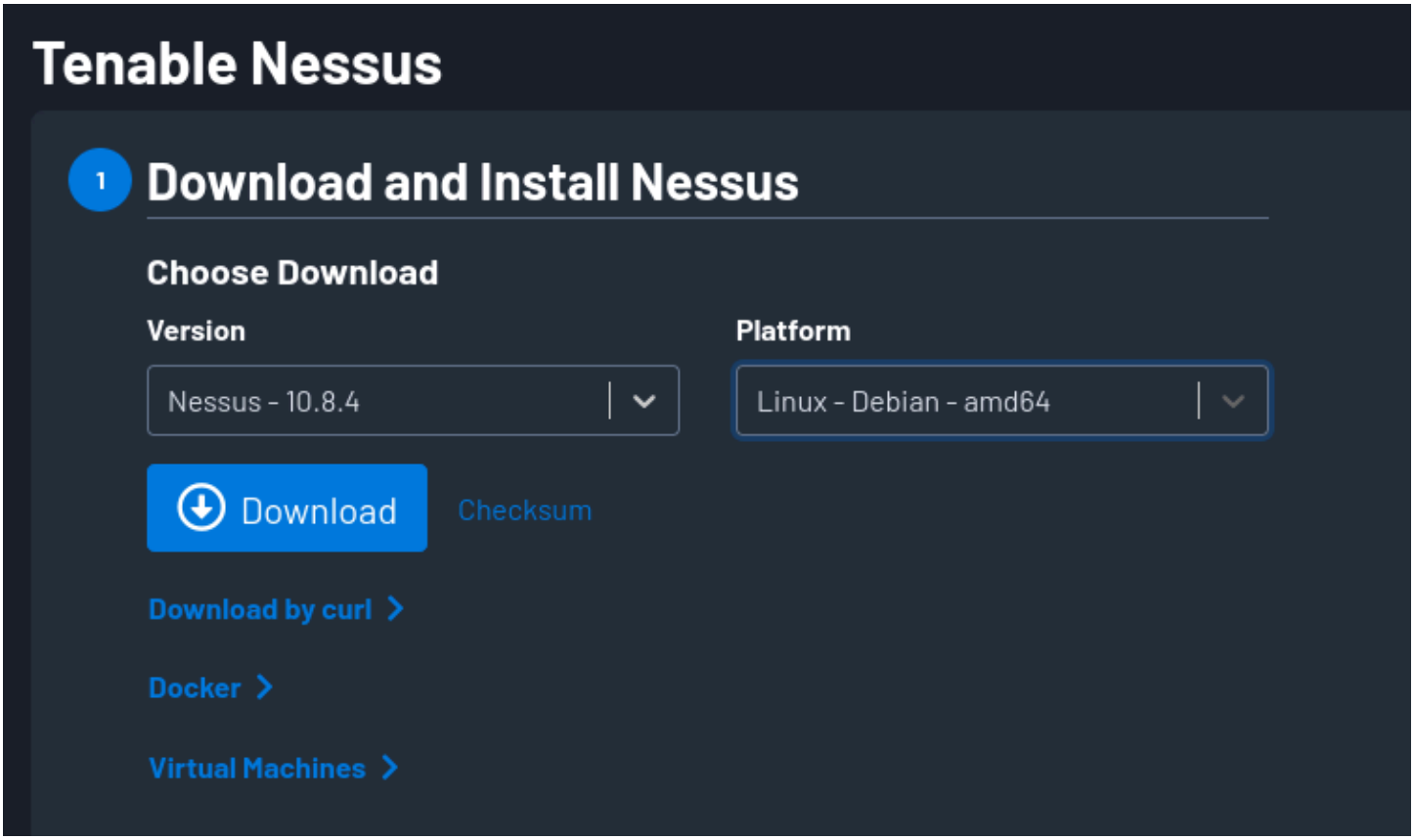
ELEVATE LABS CYBER SECURITY INTERNSHIP

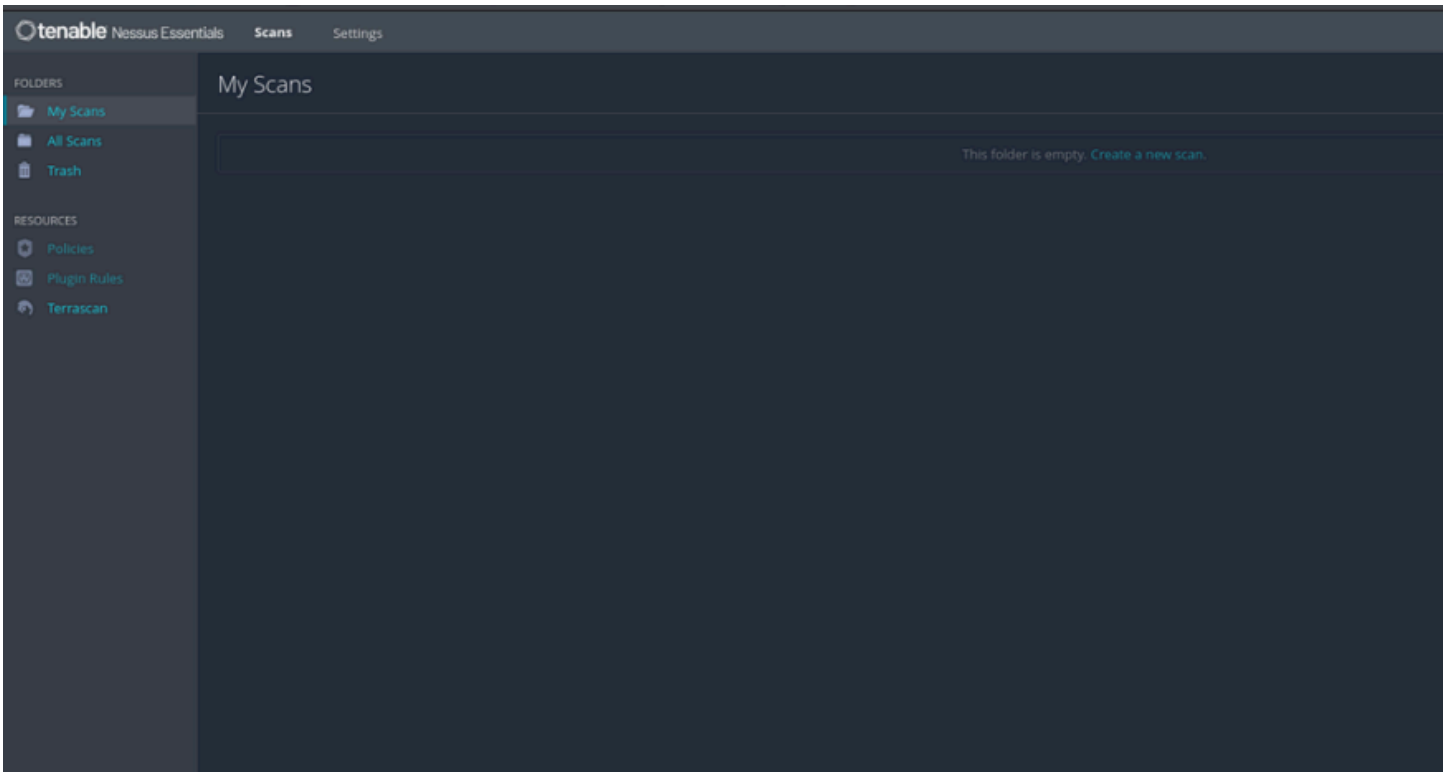
Task-3:

1)

I have done this using nessus tool
i have downloaded the debian version of the nessus application as i am using kali linux

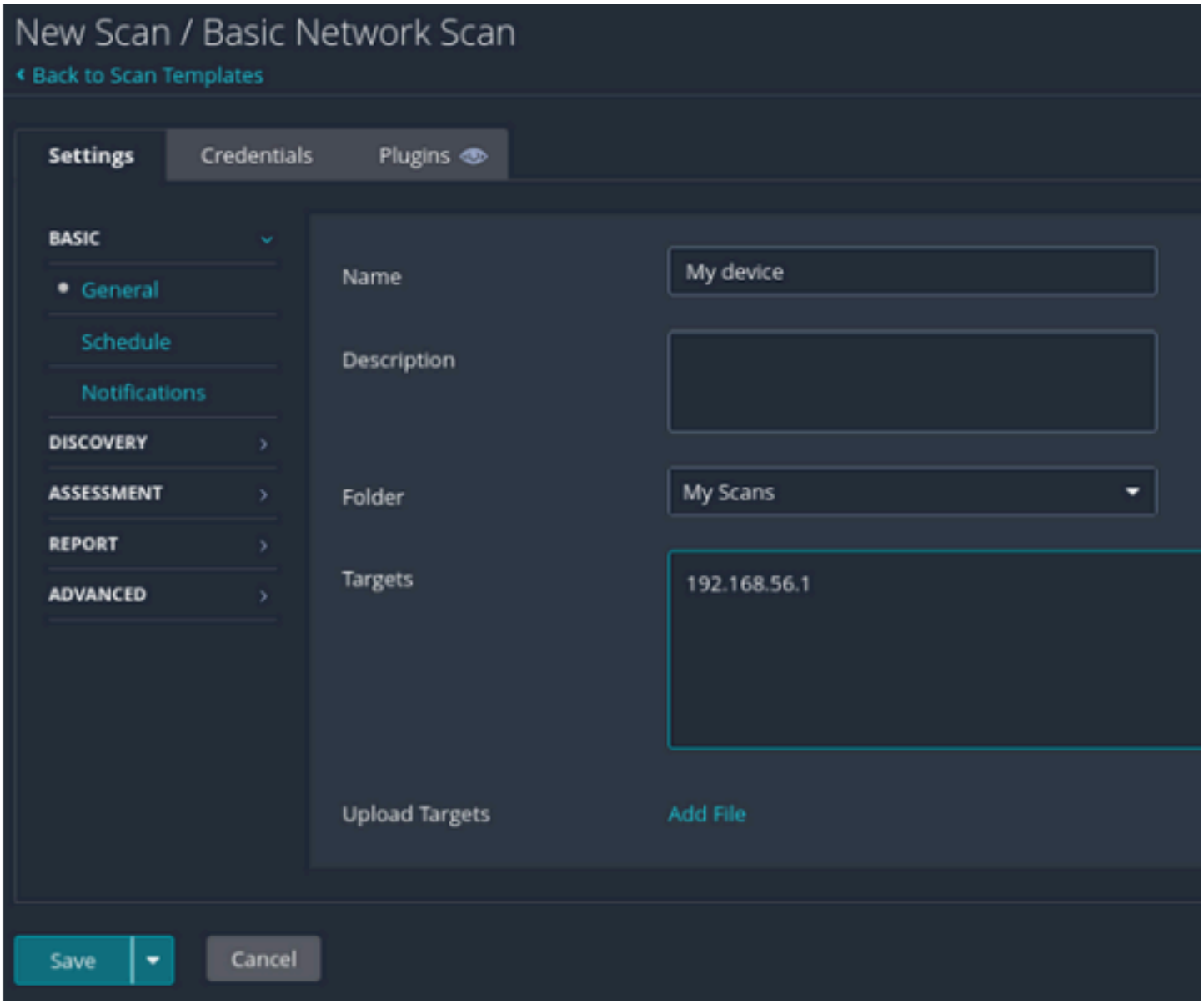


After logging in and now we can see the interface



2)

Scanning my own machine for any vulnerabilities using this tool

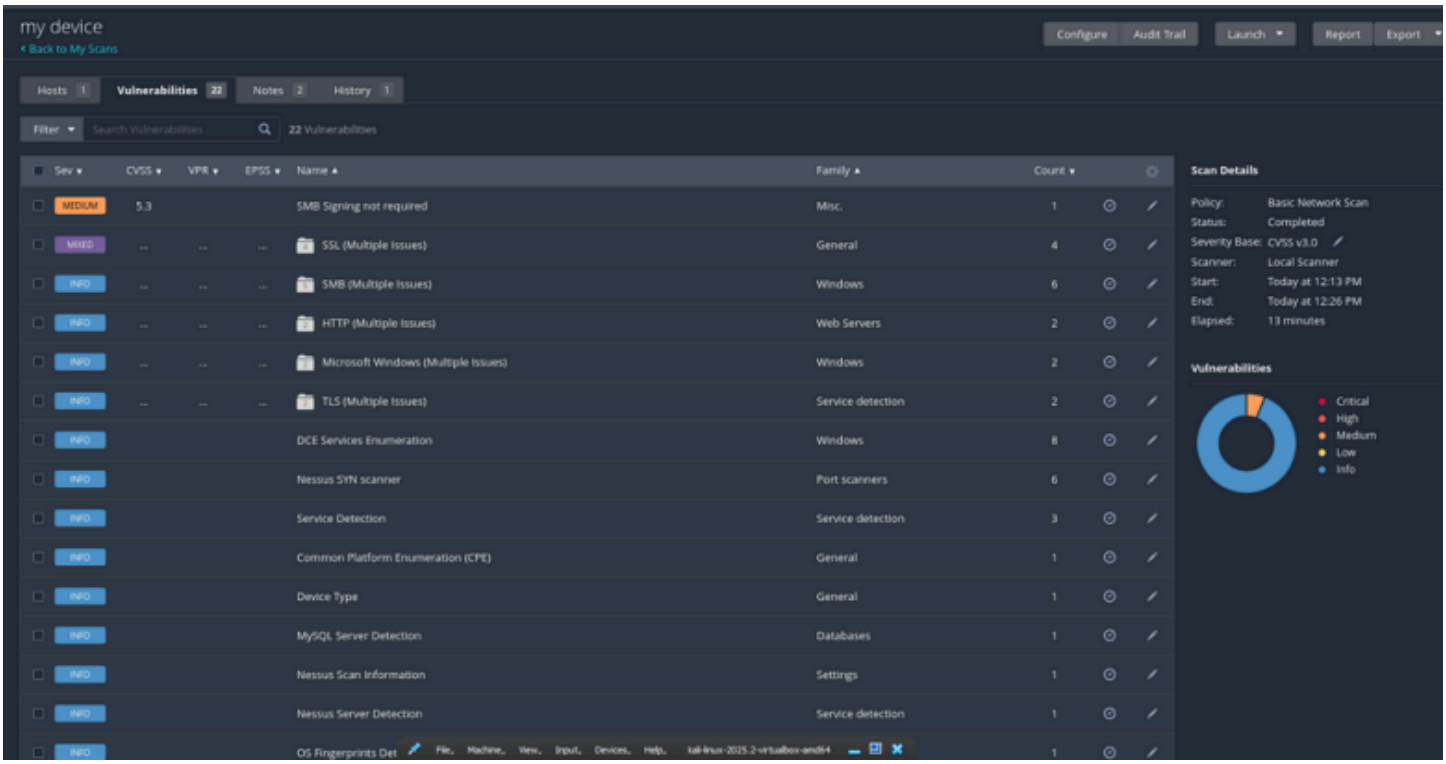


3)

started vulnerability scan and after it completed the application will show the report of the scan of our system

4)

the scan report



on left we can see severity also the name of the vulnerability and information about it

5)

Vulnerability Name	Explanation
SSL (Multiple Issues)	May involve weak ciphers, self-signed certificates, or outdated SSL versions. Review your TLS setup.
SMB (Multiple Issues)	Suggests open SMB ports or use of outdated protocols like SMBv1. Check for legacy configurations.
HTTP (Multiple Issues)	Could include missing security headers or verbose server banners. Increases risk of service probing.
Microsoft Windows (Multiple Issues)	Reveals OS version and services. This information can aid attackers in targeting specific exploits.
TLS (Multiple Issues)	Indicates deprecated TLS versions like 1.0/1.1. Ensure support is limited to TLS 1.2 or 1.3.
DCE Services Enumeration	Shows exposed RPC services. These can be used for lateral movement or exploited in Windows systems.
Service Detection	Lists open ports and their associated services. Useful for understanding the system's exposure.
Common Platform Enumeration (CPE)	Identifies software using banner analysis. Helps maintain software inventory.
MySQL Server Detection	Detects an accessible MySQL instance. If public-facing, it may pose a security risk.
OS Fingerprinting / Identification	Discloses operating system and version details, aiding in attack planning. Not directly exploitable.

6)

Vulnerability Name	Simple Fix or Mitigation
SSL (Multiple Issues)	Disable weak ciphers and insecure SSL versions (SSLv2/3). Use a valid certificate from a trusted CA.
SMB (Multiple Issues)	Disable SMBv1. Allow SMB access only to trusted internal hosts. Close unused SMB ports.
HTTP (Multiple Issues)	Add security headers like HSTS, CSP, and X-Content-Type-Options. Hide or minimize version banners.
Microsoft Windows (Multiple Issues)	Keep Windows updated. Disable unnecessary services and features. Harden system settings using security guides.
TLS (Multiple Issues)	Disable support for TLS 1.0 and 1.1. Enforce TLS 1.2 or 1.3 only. Use strong cipher suites.
DCE Services Enumeration	Restrict access to RPC services using firewalls. Disable unused DCE/RPC services.
Service Detection	Block unused ports using firewall rules. Minimize the number of exposed services.
Common Platform Enumeration (CPE)	Regularly patch and update identified software. Remove unused applications and services.
MySQL Server Detection	Restrict MySQL to localhost unless needed externally. Use strong credentials and disable remote root access.
OS Fingerprinting / Identification	Use firewall rules or packet filtering to limit exposure. Disable ICMP replies if not necessary.

7)

The most critical vulnerability found is **ssl (multiple issues)** this includes problems like using outdated ssl or tls versions such as sslv2 or sslv3 weak cipher suites and self-signed certificates these issues put encrypted network communication at serious risk attackers can take advantage of these flaws to intercept data perform man in the middle(mitm) attacks or impersonate trusted services since ssl or tls is used across web servers databases and many internal tools a weak configuration affects a wide range of systems fixing this should be a priority by allowing only modern tls versions disabling weak ciphers and replacing self-signed certificates with those from a trusted certificate authority