Elevate_Labs_Task_3

Rudra Srilakshmi

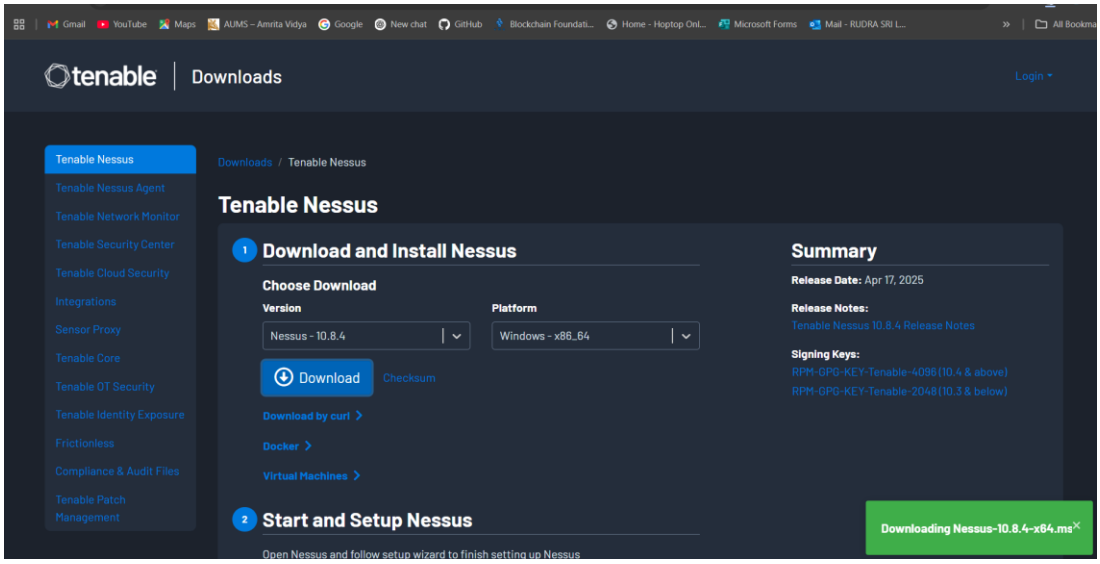
Task 3 : Perform a Basic Vulnerability Scan on Your PC

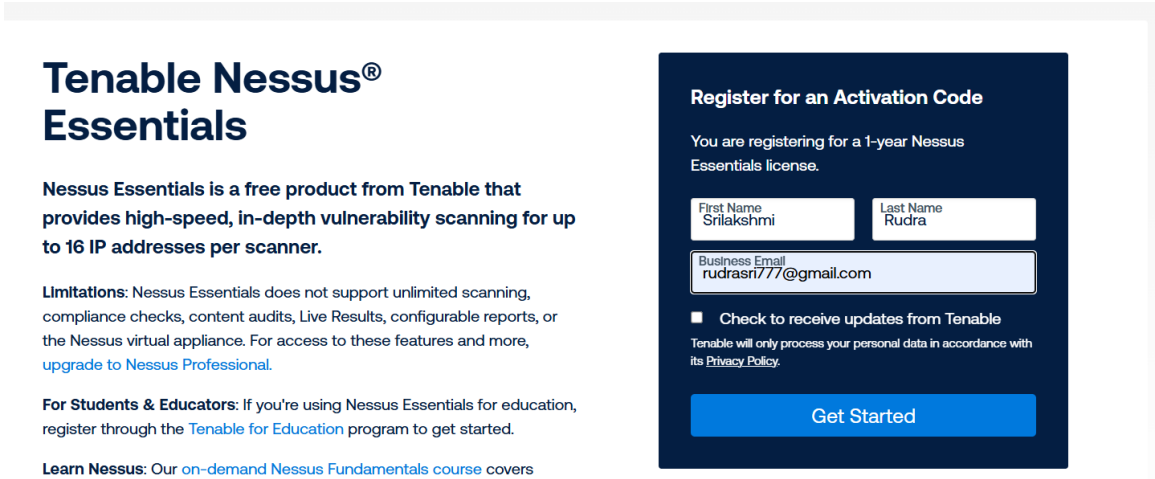
Tools Used:

Nessus Essentials by Tenable (free version)

Target: Local machine IP (identified using ip a)

1.Install OpenVAS or Nessus Essentials.



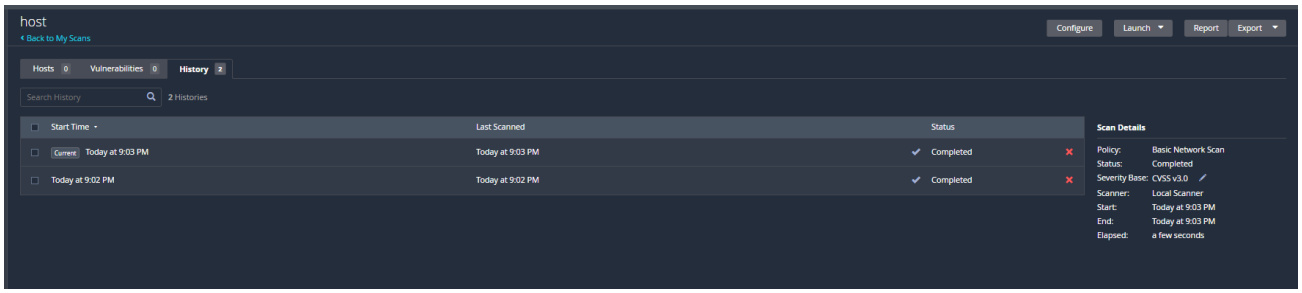


2.Set up scan target as your local machine IP or localhost.

Used this command - "*ip a",* to get the local IP of my system: 172.21.108.213

As, shown in the screenshot below tried a Host Discovery scan with this IP, but Nessus showed:
"No results found. Go back and scan a different set of targets."

So I used the loopback address 127.0.0.1 (localhost) instead to scan the machine locally.

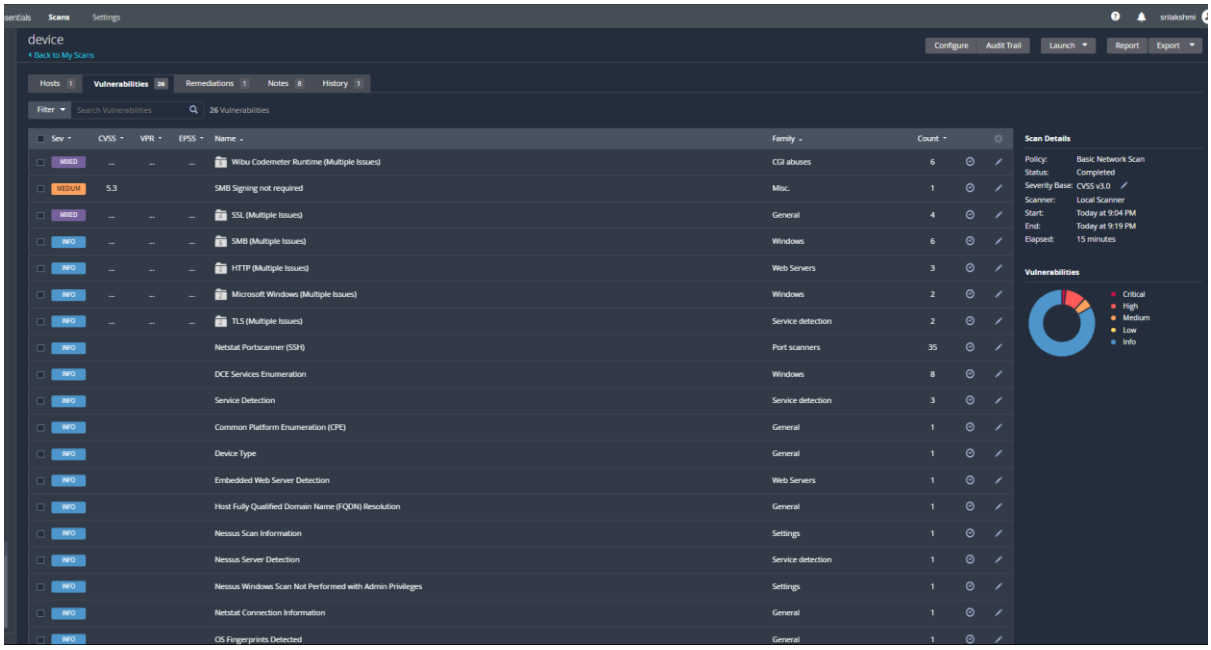


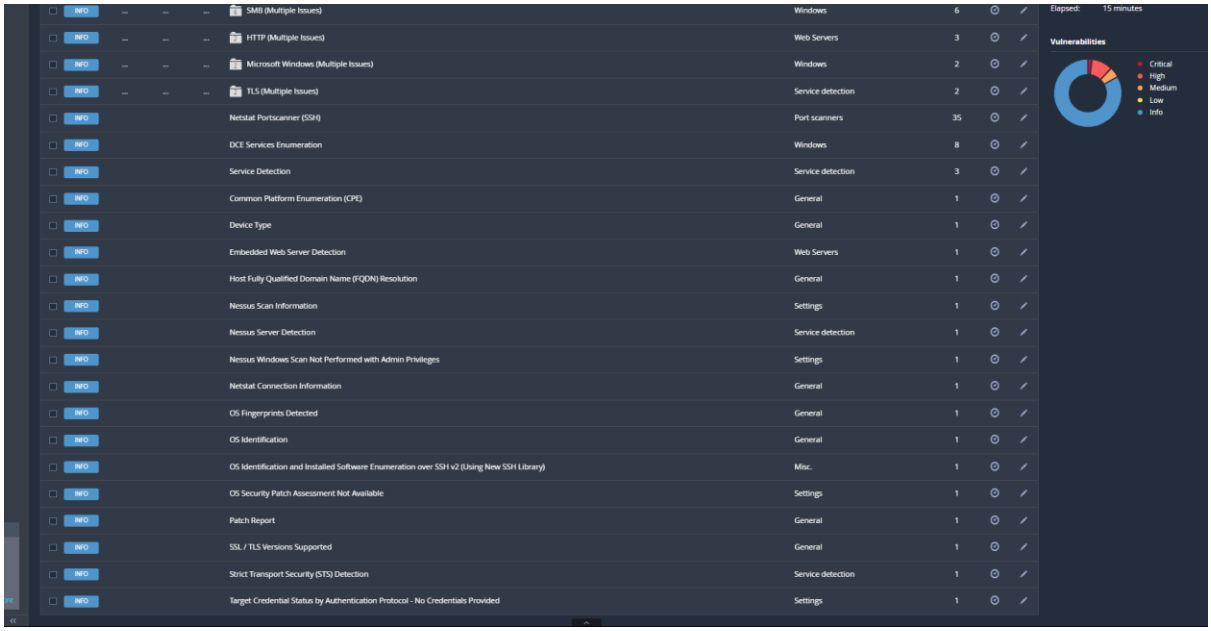
3.Start a full vulnerability scan.

Created a Basic Network Scan named *"device"* with the target: 127.0.0.1

Scan launched using Local Scanner

4.Wait for scan to complete





5.Review the report for vulnerabilities and severity.

The Nessus Essentials vulnerability scan on my local machine detected a total of 26 vulnerabilities. These were categorized based on severity, which included 1 vulnerability of mixed severity , 1 vulnerability marked as medium severity, and over 20 vulnerabilities classified as informational.

6.Research simple fixes or mitigations for found vulnerabilities.

Some important vulnerabilities found and researched:

Vulnerability	Description	Suggested Fix
SMB Signing not required (Medium)	Allows man-in-the-middle attacks on SMB communication	Enable SMB signing in Windows Group Policy
Wibu Codemeter Runtime (Multiple Issues)	CGI-related security issues from outdated runtime	Uninstall or update Wibu Codemeter if unused
Netstat Portscanner (SSH)	System exposes SSH port info, useful to attackers	Restrict external access or disable if not needed
TLS (Multiple Issues)	Deprecated or weak TLS versions detected	Disable old TLS versions and update configurations
SSL/TLS Versions Supported	Shows all SSL/TLS versions supported by the host	Harden SSL config to support only TLS 1.2/1.3
OS Identification / Fingerprints Detected	System info leaked to scanners	Restrict ICMP/ping and apply firewall rules

7.Document the most critical vulnerabilities.

- SMB Signing Not Required – Medium risk; enables MITM attacks
- Codemeter Runtime Multiple Issues – Mixed severity; known vulnerabilities
- TLS/SSL Support Disclosure – Informs attacker of weak points
- Netstat Port Scanner – SSH open info exposed
- Nessus Windows Scan Not Performed with Admin Privileges – May limit full scan, recommend running as admin
- OS Enumeration / Fingerprinting – Can help attacker craft OS-specific exploits

8.Take screenshots of the scan results.

Attached screenshots from Nessus GUI showing scan summary, vulnerability list.