

Elevate_Labs_Task_3

Rudra Srilakshmi

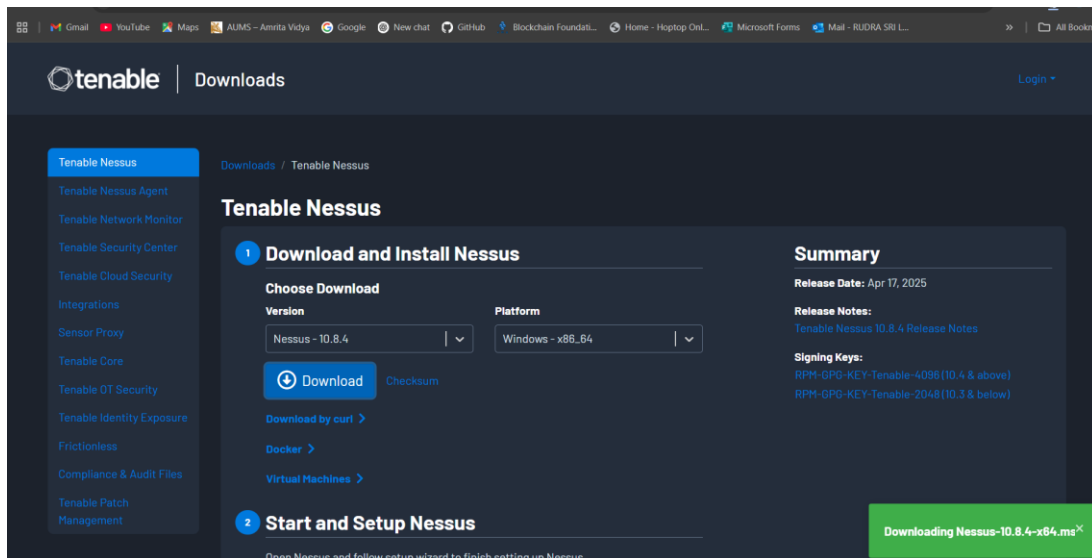
Task 3 : Perform a Basic Vulnerability Scan on Your PC

Tools Used:

Nessus Essentials by Tenable (free version)

Target: Local machine IP (identified using ip a)

1.Install OpenVAS or Nessus Essentials.



Tenable Nessus® Essentials

Nessus Essentials is a free product from Tenable that provides high-speed, in-depth vulnerability scanning for up to 16 IP addresses per scanner.

Limitations: Nessus Essentials does not support unlimited scanning, compliance checks, content audits, Live Results, configurable reports, or the Nessus virtual appliance. For access to these features and more, upgrade to [Nessus Professional](#).

For Students & Educators: If you're using Nessus Essentials for education, register through the [Tenable for Education](#) program to get started.

Learn Nessus: Our [on-demand Nessus Fundamentals course](#) covers

Register for an Activation Code

You are registering for a 1-year Nessus Essentials license.

First Name
Srilakshmi

Last Name
Rudra

Business Email
rudrasri777@gmail.com

☒ Check to receive updates from Tenable

Tenable will only process your personal data in accordance with its [Privacy Policy](#).

Get Started

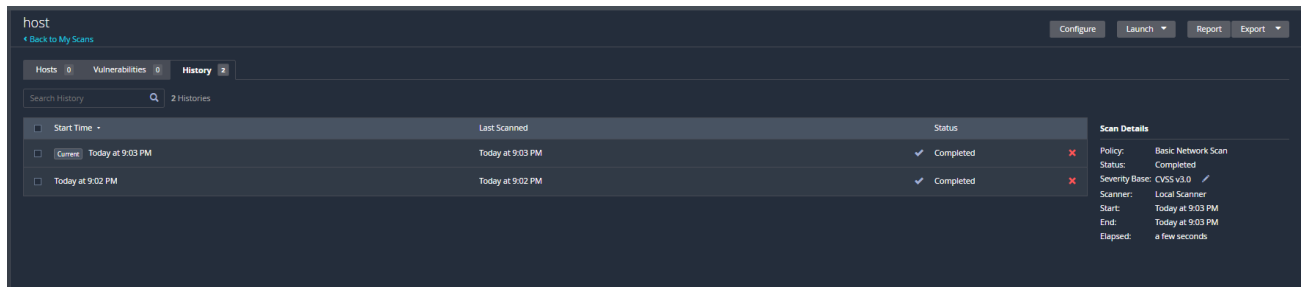
2.Set up scan target as your local machine IP or localhost.

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."

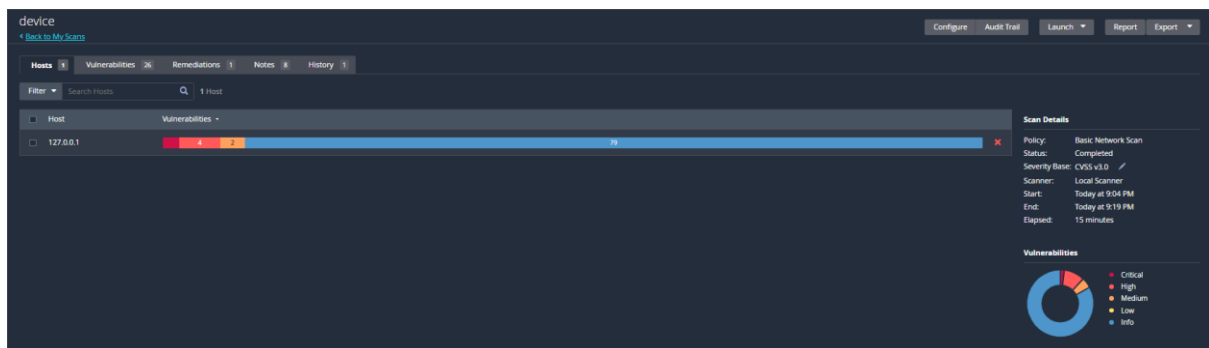
So I used the loopback address 127.0.0.1 (localhost) instead to scan the machine locally.



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

The screenshot shows the Nessus Essentials interface with the 'device' scan results. The table lists 26 vulnerabilities, categorized by severity (Info, Medium, Mixed). The 'Scan Details' panel on the right shows the scan was completed by 'Local Scanner' at 9:04 PM. A 'Vulnerabilities' donut chart shows the distribution: 1 Critical, 1 High, 1 Medium, 20 Low, and 3 Info.

Sev	CVSS	VPR	EPSS	Name	Family	Count
Mixed				Wibu CodeMeter Runtime (Multiple Issues)	CG abuses	6
Medium	5.3			SMB Signing not required	Misc.	1
Info				SSL (Multiple Issues)	General	4
Info				SMB (Multiple Issues)	Windows	6
Info				HTTP (Multiple Issues)	Web Servers	3
Info				Microsoft Windows (Multiple Issues)	Windows	2
Info				TLS (Multiple Issues)	Service detection	2
Info				Nessus PortScanner (SSH)	Port scanners	35
Info				DCE Services Enumeration	Windows	8
Info				Service Detection	Service detection	3
Info				Common Platform Enumeration (CPE)	General	1
Info				Device Type	General	1
Info				Embedded Web Server Detection	Web Servers	1
Info				Host Fully Qualified Domain Name (FQDN) Resolution	General	1
Info				Nessus Scan Information	Settings	1
Info				Nessus Server Detection	Service detection	1
Info				Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
Info				Nessus Connection Information	General	1
Info				OS Fingerprints Detected	General	1

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 9:04 PM
- End: Today at 9:19 PM
- Elapsed: 15 minutes

Vulnerabilities

- 1 Critical
- 1 High
- 1 Medium
- 20 Low
- 3 Info

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.