

Vulnerability Management Lab Using Nessus

Overview

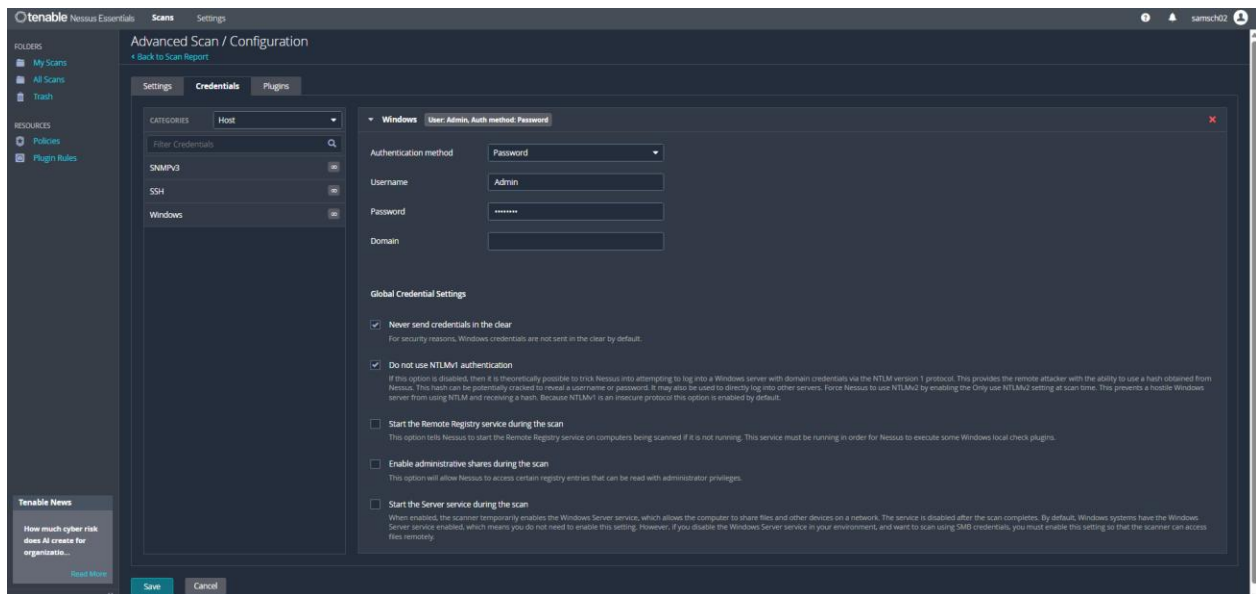
Performed a vulnerability assessment of two Windows 11 endpoints using Tenable Nessus to practice vulnerability scanning, risk identification, and remediation planning.

Step 1: Endpoint Preparation

Configured two Windows 11 endpoints for credentialed vulnerability scanning.

Prepared the systems by:

- Enabling authenticated scanning access
- Configuring administrative credentials
- Verifying network connectivity between the scanner and target devices

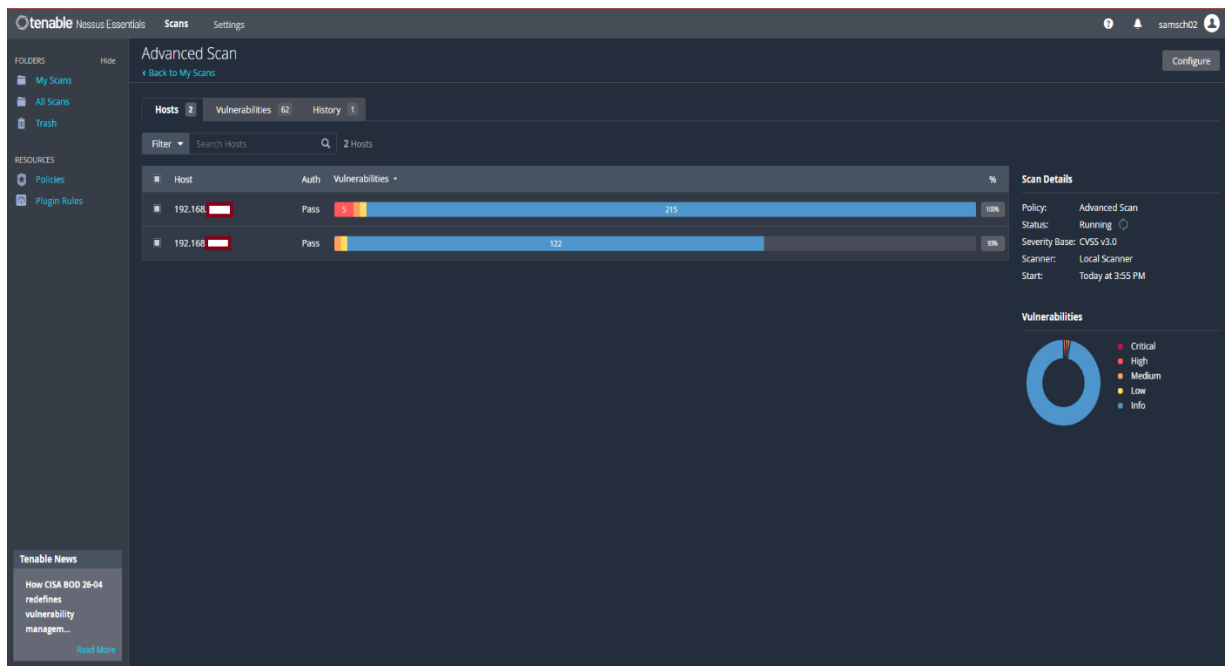


Step 2: Credentialed Nessus Scan

Created and executed an advanced credentialed scan using Nessus.

The scan evaluated:

- Operating system configuration
- Installed software
- Missing security updates
- Vulnerability exposure
- System settings



Step 3: Vulnerability Review & Analysis

Reviewed scan results to identify security findings and prioritize potential risks.

Analyzed:

- Severity ratings
- Affected systems
- Vulnerability details
- Recommended remediation steps

The screenshot shows the Tenable Nessus Essentials interface for an Advanced Scan of host 192.168.3.183. The main panel displays a table of 59 vulnerabilities. The table columns include Severity (Sev), CVSS, VPR, EPSS, Name, Family, and Count. The vulnerabilities are sorted by severity, with High (8.8) and Medium (6.5) issues at the top. The host details sidebar on the right shows the host's IP, DNS, MAC, OS (Microsoft Windows 11 Pro Build 22H2), and scan statistics. A vulnerability severity distribution chart is also visible.

Sev	CVSS	VPR	EPSS	Name	Family	Count
HIGH	8.8			WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)	Windows : Microsoft Bulletins	1
HIGH	7.5			Microsoft ASP.NET Core DoS (March 2026)	Windows : Microsoft Bulletins	1
MEDIUM	6.5			Microsoft .NET Core (Multiple Issues)	Windows	5
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
LOW	2.1			ICMP Timestamp Request Remote Date Disclosure	General	1
INFO				Microsoft Windows (Multiple Issues)	Windows	95
INFO				SMB (Multiple Issues)	Windows	18
INFO				Microsoft Office (Multiple Issues)	Windows	3
INFO				Windows (Multiple Issues)	Windows	3
INFO				Google Chrome (Multiple Issues)	Windows	2
INFO				Microsoft (Multiple Issues)	Windows	2
INFO				Microsoft Edge (Multiple Issues)	Windows	2
INFO				Microsoft Internet Explorer (Multiple Issues)	Windows	2
INFO				Microsoft Windows (Multiple Issues)	Windows : User management	2

The screenshot shows the Tenable Nessus Essentials interface for an Advanced Scan of host 192.168.3.184. The main panel displays a table of 22 vulnerabilities. The table columns include Severity (Sev), CVSS, VPR, EPSS, Name, Family, and Count. The vulnerabilities are sorted by severity, with Medium (5.3) and Low (2.1) issues at the top. The host details sidebar on the right shows the host's IP, DNS, MAC, OS (Microsoft Windows 11 Pro Build 22H2), and scan statistics. A vulnerability severity distribution chart is also visible.

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not required	Misc.	1
LOW	2.1	2.9	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO				Microsoft Windows (Multiple Issues)	Windows	57
INFO				SMB (Multiple Issues)	Windows	7
INFO				Nessus PortScanner (WMI)	Port scanners	33
INFO				DCE Services Enumeration	Windows	9
INFO				Service Detection	Service detection	2
INFO				Additional DNS Hostnames	General	1
INFO				Device Hostname	General	1
INFO				Ethernet Card Manufacturer Detection	Misc.	1
INFO				Ethernet MAC Addresses	General	1
INFO				Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO				Intel Active Management Technology (AMT) detection	Windows	1
INFO				Intel CPUID detection	Service detection	1
INFO				IP Assignment Method Detection	General	1
INFO				mDNS Detection (Local Network)	Service detection	1
INFO				Microsoft Internet Explorer Version Detection	Windows	1

Step 4: Remediation & Security Improvements

Reviewed recommended actions to improve endpoint security.

Focused on:

- Reducing vulnerabilities
 - Improving system configurations
 - Understanding patch and security management processes
-

Project Outcome

Successfully completed a credentialed vulnerability assessment against Windows 11 endpoints using Nessus. This project provided hands-on experience with vulnerability management processes, security scanning, risk assessment, and interpreting security findings.