

Vulnerability Management Using Nessus Scanner

- Installed and configured Nessus Essentials to perform credentialed scans against windows 10 hosts
- Implemented Vulnerability Management on sandbox networks:
Discover, Prioritize, Assess, Report, Remediate, Verify

The screenshot shows the Nessus web interface for a scan report titled 'windows 10 single host'. The interface includes a sidebar with navigation options like Folders, Resources, and Tenable News. The main content area displays a table of vulnerabilities with columns for Severity, CVSS, VPR, Name, Family, and Count. A 'Scan Details' panel on the right provides information about the scan policy, status, severity base, scanner, start/end times, and elapsed time. A 'Vulnerabilities' donut chart is also present.

Sev	CVSS	VPR	Name	Family	Count
MEDIUM	5.3		SMB Signing not required	Misc.	1
INFO	SMB (Multiple Issues)	Windows	6
INFO			DCE Services Enumeration	Windows	8
INFO			Nessus SYN scanner	Port scanners	3
INFO			Asset Attribute: Fully Qualified Domain Name (FQDN)	General	1
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	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			Nessus Scan information	Settings	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 2:06 PM
End: Today at 2:16 PM
Elapsed: 10 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

The screenshot shows the Nessus web interface for a scan report titled 'windows 10 single host'. The interface includes a sidebar with navigation options like Folders, Resources, and Tenable News. The main content area displays a table of scan histories with columns for Start Time, Last Modified, and Status. A 'Scan Details' panel on the right provides information about the scan policy, status, severity base, scanner, start/end times, and elapsed time. A 'Vulnerabilities' donut chart is also present.

Start Time	Last Modified	Status
Completed Today at 11:11 AM	Today at 11:21 AM	✓ Completed
Today at 11:02 AM	Today at 11:07 AM	✓ Completed
Today at 10:47 AM	Today at 10:51 AM	✓ Completed

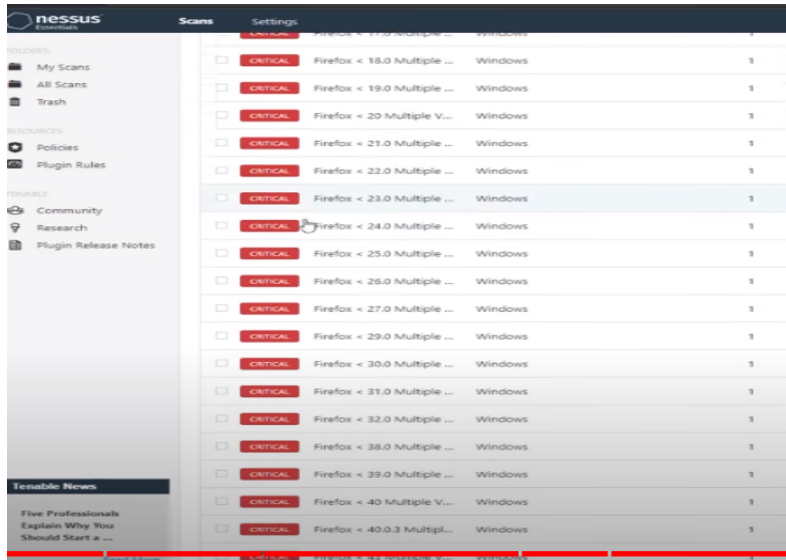
Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:15 AM
End: Today at 11:21 AM
Elapsed: 6 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

- Conducted vulnerability assessment with nessus scanner, remediated vulnerabilities after receiving results



- Introduced remediation process to deal with vulnerabilities stemming from windows updates as well as third party software. In this scenario, I continued to run windows updates and update older version firefox that was downloaded to host.

