

Kayla Hodge
Threat Protection & Testing
Professor Bardowell
CYB4381-O | C202605-01
May 30, 2026
4.5 - Lab Assignment: Lab 6

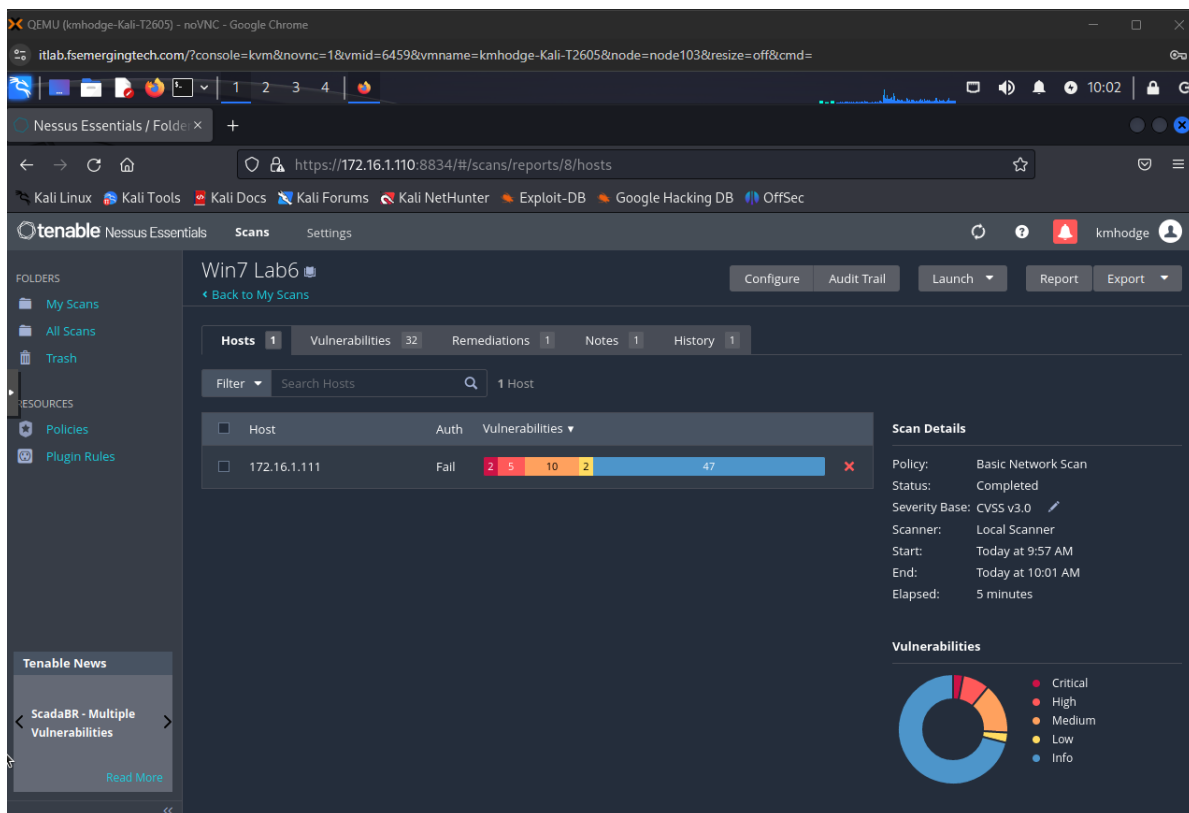
Lab 6:

Validation Scanning with Nessus

Initial Scan Results

The initial Nessus scan of the Windows 7 system identified 66 findings, including 2 critical, 5 high, 10 medium, 2 low, and 47 informational vulnerabilities.

	Critical	High	Medium	Low	Informational
Count	2	5	10	2	47

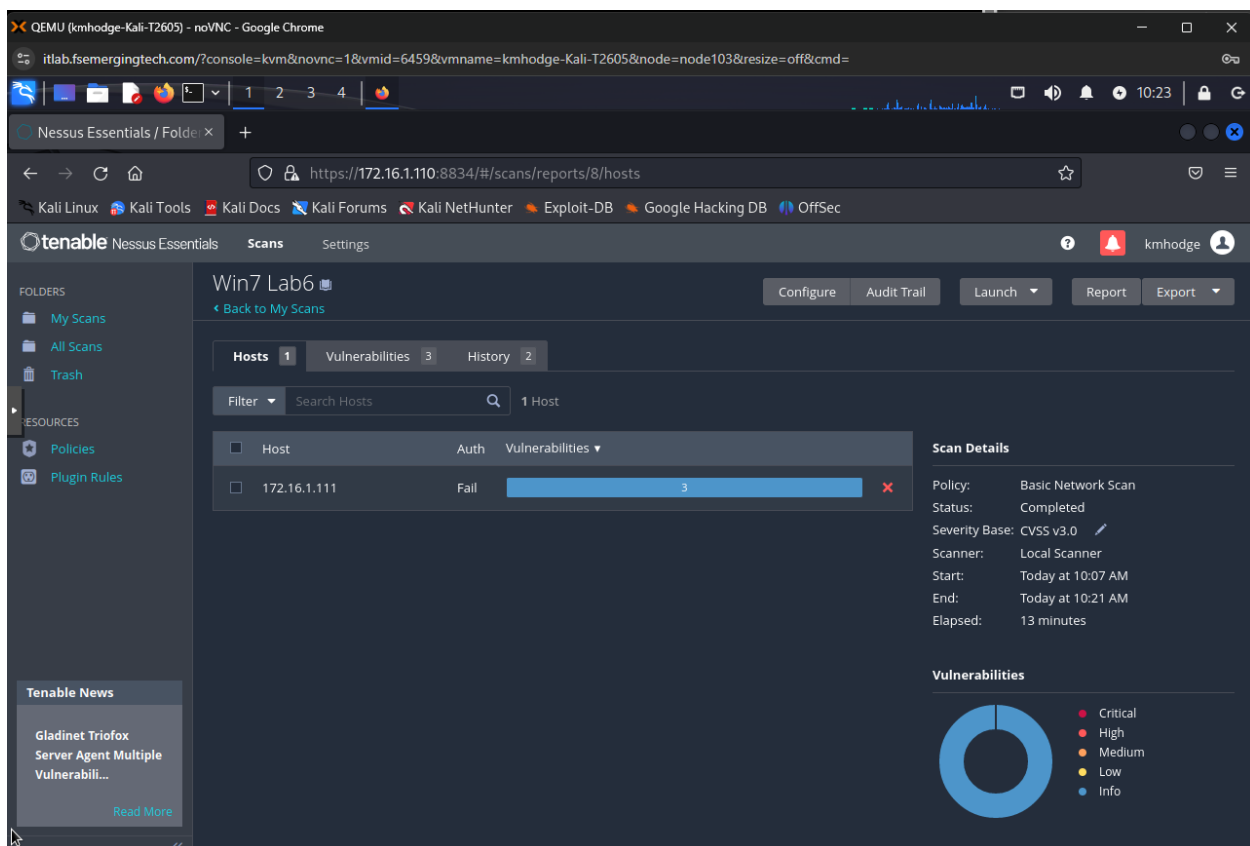


Nessus scan before the firewall.

Any difference in the scan and the scan results? If so, explain.

Yes. After enabling Windows Firewall on Windows 7, the number of detected vulnerabilities decreased significantly. The initial scan identified 66 findings, including critical, high, medium, low, and informational vulnerabilities. After enabling the firewall, Nessus reported only 3 informational findings.

Enabling Windows Firewall blocked many of the ports and services that Nessus used to identify vulnerabilities on the system. As a result, the scanner could no longer access many of the previously exposed services. This significantly reduced the attack surface and prevented Nessus from detecting many of the vulnerabilities identified during the initial scan.



Scan 2 for Windows 7.

Are the SMB vulnerabilities still present after the scan?

No. The SMB-related vulnerabilities were no longer detected after Windows Firewall was enabled. The second Nessus scan reported only three informational findings and no critical, high, medium, or low vulnerabilities. After creating the firewall rule to block SMB ports 445 and 139 and running a third scan, the results were unchanged, with only three informational findings. This indicates that enabling Windows Firewall had already prevented Nessus from detecting the SMB vulnerabilities before the SMB-specific rule was added.

The screenshot displays the Nessus Essentials web interface in a browser window. The URL bar shows the connection to the Nessus server. The interface includes a sidebar with navigation options like 'My Scans', 'All Scans', and 'Trash'. The main content area shows the results of a scan titled 'Win7 Lab6'. A table lists the scanned hosts, with one host (172.16.1.111) showing a 'Fail' status and 3 vulnerabilities. To the right, 'Scan Details' provide information about the scan policy, status, severity base, scanner, and duration. Below the scan details, a 'Vulnerabilities' section features a donut chart showing the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The chart indicates that all detected vulnerabilities are of 'Info' severity.

Host	Auth	Vulnerabilities
172.16.1.111	Fail	3

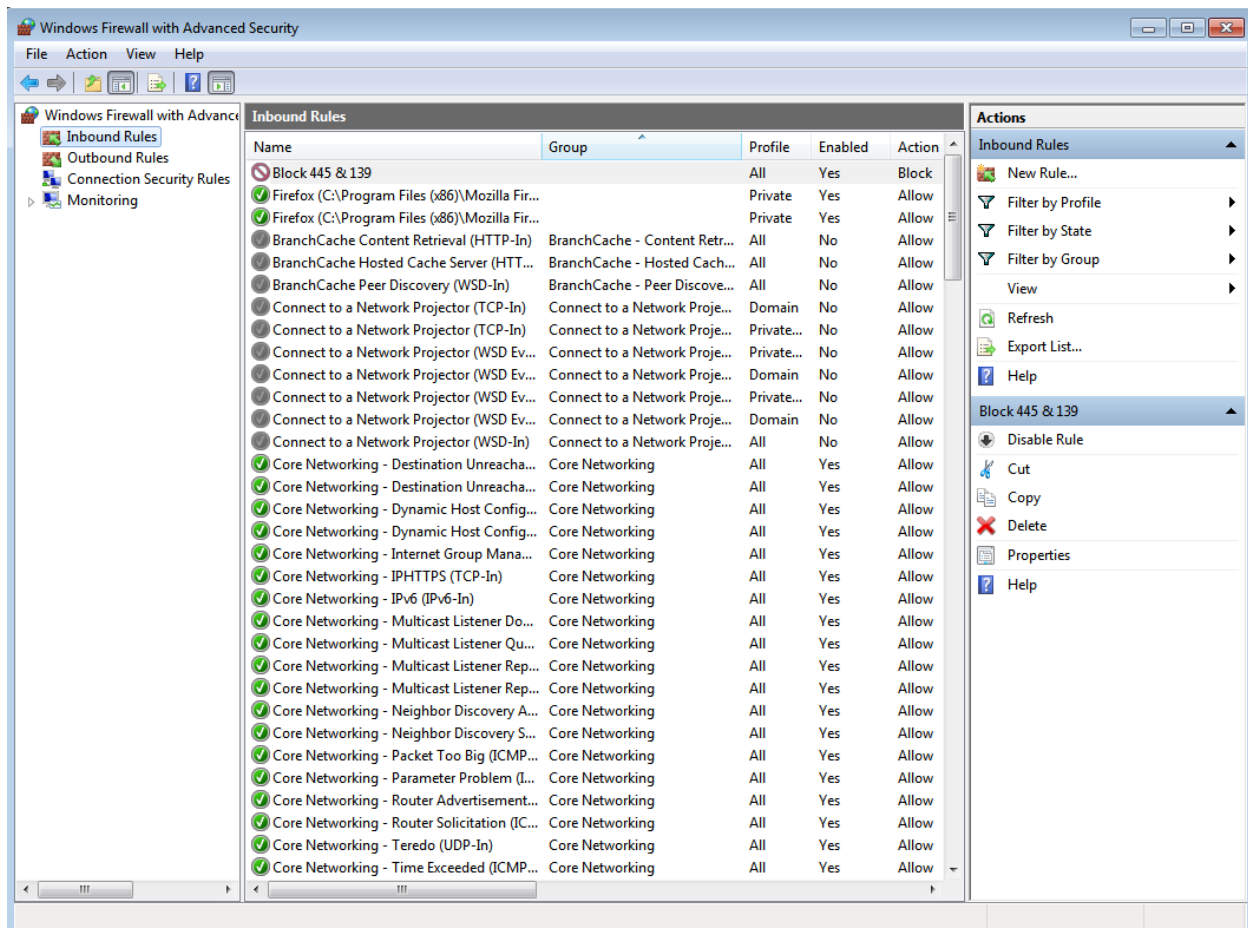
Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 10:07 AM
- End: Today at 10:21 AM
- Elapsed: 13 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Firewall is activated in Windows 7.



A firewall rule was created.

What other ports could you block to remediate the vulnerability findings from the Nessus scan?

No additional ports were identified from the remaining Nessus findings after Windows Firewall was enabled and SMB ports 445 and 139 were blocked. The final scan reported only three informational findings categorized as Misc., General, and Settings. All remaining findings listed the port as N/A, indicating that no specific network service or port was associated with the findings. Because no additional vulnerable ports were identified, no further firewall rules were created, and no additional validation scans were required.

The screenshot shows the Nessus Essentials web interface in a browser window. The URL is `https://172.16.1.110:8834/#/scans/reports/8/hosts/2/vulnerabilities/19506`. The interface includes a sidebar with navigation options like 'My Scans', 'All Scans', 'Trash', 'Policies', and 'Plugin Rules'. The main content area displays a list of findings, including informational items about the Nessus Engine. Below this, there is an 'Output' section with a table of scan results.

Port	Hosts
N/A	172.16.1.111

All remaining scan results list N/A under the port.