

Lab 2: Vulnerability Scanner

Task 1: Nessus Essentials Setup

No deliverable for this task.

Task 2: Unauthenticated Scan

The screenshot shows the Tenable Nessus Essentials web interface. The main content area displays the results of an 'Unauthenticated Scan'. The interface includes a sidebar with navigation options like Summary, Console, and Folders. The main content area displays a table of hosts with their authentication status and vulnerability counts. A 'Scan Details' panel on the right provides information about the scan policy, status, and duration. A 'Vulnerabilities' donut chart is also visible.

Host	Auth	Vulnerabilities
192.168.1.106	Pass	35
192.168.1.105	Fail	6
192.168.1.1	Fail	5

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 1:29 PM
- End: Today at 1:46 PM
- Elapsed: 17 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Kayla Hodge
CTI4001-O | C202512-02
Network Security and Software
Lab 2: Vulnerability Scanner
November 28, 2025

The screenshot shows the Tenable Nessus Essentials interface. The main window displays the results of an "Unauthenticated Scan / 192.168.1.106". The "Vulnerabilities" section shows 48 vulnerabilities. The table lists the severity, CVSS score, VPR, EPSS, Family, and Count for each vulnerability. The "Host" column shows the IP address 192.168.1.106. The "Host Details" section on the right provides information about the host, including the operating system (Rocky Linux release 8.8 (Green Obsidian)), kernel (4.18.0-477.13.1.el8_8.x86_64), and the scan date and time (Today at 1:29 PM). The "Host Details" section also includes a "Download" link for the host details.

Sev	CVSS	VPR	EPSS	Family	Count
MIXED	...	...	...	Rocky Linux Local Security Checks	60
MIXED	...	...	...	General	4
MIXED	...	...	...	Misc	2
MIXED	...	...	...	Misc	5
INFO	...	...	...	General	9
INFO	...	...	...	General	3
INFO	...	...	...	Web Servers	2
INFO	...	...	...	Service detection	2
INFO	...	...	...	Service detection	2

The screenshot shows the Tenable Nessus Essentials interface. The main window displays the results of an "Unauthenticated Scan / 192.168.1.105". The "Vulnerabilities" section shows 21 vulnerabilities. The table lists the severity, CVSS score, VPR, EPSS, Family, and Count for each vulnerability. The "Host" column shows the IP address 192.168.1.105. The "Host Details" section on the right provides information about the host, including the operating system (Microsoft Windows Server 2019), kernel (4.18.0-477.13.1.el8_8.x86_64), and the scan date and time (Today at 1:29 PM). The "Host Details" section also includes a "Download" link for the host details.

Sev	CVSS	VPR	EPSS	Family	Count
MIXED	...	...	...	General	7
MIXED	5.3	...	...	Misc	1
MIXED	...	...	...	Service detection	4
MIXED	...	...	...	Misc	2
LOW	2.1	2.2	0.0037	DMB (Multiple Issues)	1
INFO	...	...	...	Windows	6
INFO	...	...	...	General	2
INFO	...	...	...	Windows	9
INFO	...	...	...	Port scanners	4

node101 - Proxmox Virtual Environment

Virtual Lab Virtual Environment 8.3.2

Tasks Cluster log

Start Time	End Time	Node
Nov 26 14:04:30		node1
Nov 26 13:54:54		node1
Nov 26 13:54:12	Nov 26 13:54:44	node103
Nov 26 13:30:31	Nov 26 13:54:05	node103
Nov 26 13:30:29	Nov 26 13:30:31	node103

Virtual Machines:

- 3046 (kmhodge-Firewall-2512)
- 3047 (kmhodge-Kali-2512)
- 3048 (kmhodge-Win10-2512)
- 3049 (kmhodge-Nessus-2512)

Virtual Machine Details:

Virtual Machine: 3047 (kmhodge-Kali-2512)

Operating System: Kali Linux

IP Address: 192.168.1.1

Virtual Machine Tools: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec

Nessus Essentials / Scans

Unauthenticated Scan / 192.168.1.1

Vulnerabilities: 27

Filter: Search Vulnerabilities

Sev	CVSS	VPR	EPSS	Family	Count	Host
CRITICAL	10.0			General	1	192.168.1.1
MEDIUM	5.8			Misc.	1	192.168.1.1
MEDIUM				Web Servers	7	192.168.1.1
MEDIUM				General	6	192.168.1.1
LOW	2.1 *	2.2	0.0037	General	1	192.168.1.1
INFO				DNS	3	192.168.1.1
INFO				Service detection	2	192.168.1.1
INFO				Port scanners	3	192.168.1.1
INFO				Service detection	3	192.168.1.1

Host Details:

Host: 192.168.1.1

OS: OPNsense.localdomain

SAC: BC24:11:46:8B:AA

IS: FreeBSD 13.1-RELEASE-p7 (amd64)

Start: Today at 1:29 PM

End: Today at 1:46 PM

Lapsed: 17 minutes

IP: Download

Auth: Fail

Vulnerabilities:

Legend: Critical (Red), High (Orange), Medium (Yellow), Low (Green), Info (Blue)

Status: OK

Task 3: Authenticated Scan

The screenshot displays the Tenable Nessus Essentials web interface. The main panel shows the 'Authenticated Scan' results for host 192.168.1.105. The scan status is 'Fail' with a severity of '5'. The scan details indicate it was a 'Basic Network Scan' completed by a 'Local Scanner' on November 28, 2025, at 1:55 PM, taking 5 minutes. A donut chart shows the distribution of vulnerabilities: Critical (1), High (1), Medium (1), Low (1), and Info (1).

Host	Auth	Vulnerabilities
192.168.1.105	Fail	5

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 1:55 PM
- End: Today at 2:00 PM
- Elapsed: 5 minutes

Vulnerabilities

- 1 Critical
- 1 High
- 1 Medium
- 1 Low
- 1 Info

The screenshot displays the Tenable Nessus Essentials web interface, showing a detailed view of the vulnerabilities for host 192.168.1.105. The main panel shows the 'Authenticated Scan / 192.168.1.105' results. The scan status is 'Fail' with a severity of '5'. The scan details indicate it was a 'Basic Network Scan' completed by a 'Local Scanner' on November 28, 2025, at 1:55 PM, taking 5 minutes. A donut chart shows the distribution of vulnerabilities: Critical (1), High (1), Medium (1), Low (1), and Info (1).

Sev	CVSS	VPR	EPSS	Family	Count
INFO	...	...	...	Windows	10
INFO	...	...	...	Windows	9
MIXED	...	...	...	General	7
MIXED	...	...	...	Service detection	4
INFO	...	...	...	Port scanners	4
MIXED	...	...	...	Windows	2
MIXED	...	...	...	Misc.	2
INFO	...	...	...	General	2
MEDIUM	5.3	...	...	Misc.	1

Host Details

- 192.168.1.105
- SAC: BC24:11-AE-E9CB
- IS: Microsoft Windows Server 2019
- Start: Today at 1:55 PM
- End: Today at 2:00 PM
- Elapsed: 5 minutes
- Status: Download
- Auth: Fail

Vulnerabilities

- 1 Critical
- 1 High
- 1 Medium
- 1 Low
- 1 Info

Lab 2 Write Up

Was there a difference in the results between the unauthenticated and authenticated scans on your Windows 10 VM?

Yes, there was a noticeable difference between the unauthenticated and authenticated scans on the Windows 10 VM. The unauthenticated scan identified several vulnerabilities, but the results were limited because Nessus could only see what was externally exposed or discoverable without credentials. Once the authenticated scan was run, Nessus gained deeper access into the system and was able to pull far more detailed information. This included additional Windows-specific findings, missing patches, misconfigurations, and services that aren't visible from the outside. Overall, the authenticated scan produced a more complete and accurate picture of the system's security posture.

Why might there be a difference between the two scans?

The difference exists because authenticated and unauthenticated scans operate at two completely different levels of visibility. An unauthenticated scan analyzes the system from the perspective of an outsider with no login access, so it can only detect surface-level weaknesses, such as open ports, banner information, and publicly accessible vulnerabilities. Authenticated scans, however, use valid system credentials to log in and inspect the host from the inside. This lets Nessus check installed software versions, patch levels, configuration settings, registry keys, and local security policies. Because of this deeper access, authenticated scans consistently reveal more vulnerabilities and provide far more reliable results for remediation planning.