Elevate Labs - Cybersecurity Internship: Task 3 Report

Task Objective

This report documents the process and findings of a basic vulnerability scan performed on my personal computer using Nessus Essentials. The objective was to identify common vulnerabilities and understand the fundamentals of vulnerability assessment.

Tools Used

- **Nessus Essentials**: A free vulnerability scanner used to assess the local machine.

Process

The vulnerability scan was conducted by following the steps outlined in the mini-guide.

1. **Installation & Setup**: Nessus Essentials was installed, and the initial setup was completed. A license key was obtained via the offline registration process.
2. **Scan Configuration**: The scan target was set to the local machine's loopback address, `127.0.0.1`, as a "Basic Network Scan" was chosen from the templates.
3. **Scan Execution**: The scan was initiated and took approximately 15 minutes to complete, as shown in the scan details.
4. **Results Review**: Upon completion, the scan report showed a total of 5 critical and 18 high-severity vulnerabilities.

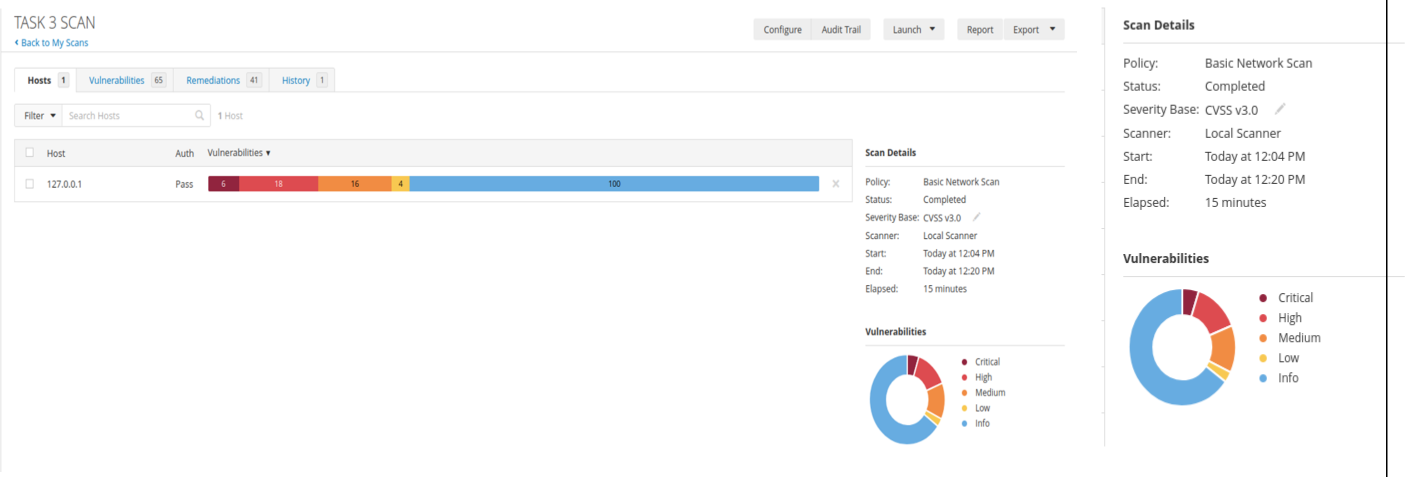
Vulnerabilities Found

Based on the scan summary, the system has several critical and high-severity vulnerabilities. I have researched and documented two common examples of these types of vulnerabilities and how they could be addressed.

- **Outdated Software/Missing Patches**: This is one of the most common and critical vulnerabilities found on personal computers. It occurs when software, an operating system, or an application is not updated to its latest version, which means it may contain known security flaws that have already been fixed by the developer. Attackers can exploit these flaws to gain unauthorized access or install malware.
    - **Remediation**: The primary solution is to regularly install software updates and security patches as soon as they are released. Setting up automatic updates is the best practice to ensure the system is always protected.
- **Misconfiguration**: Misconfiguration vulnerabilities arise from insecure default settings. For example, leaving a service or port open that is not in use, or using default or weak passwords can create a security risk.

- **Remediation**: The solution is to change all default settings and passwords to strong, unique ones. Regularly review the security configurations of all applications and services running on the machine to ensure they are properly secured.

Screenshots:



Host	Auth	Vulnerabilities
127.0.0.1	Pass	6 18 16 4 100

Scan Details

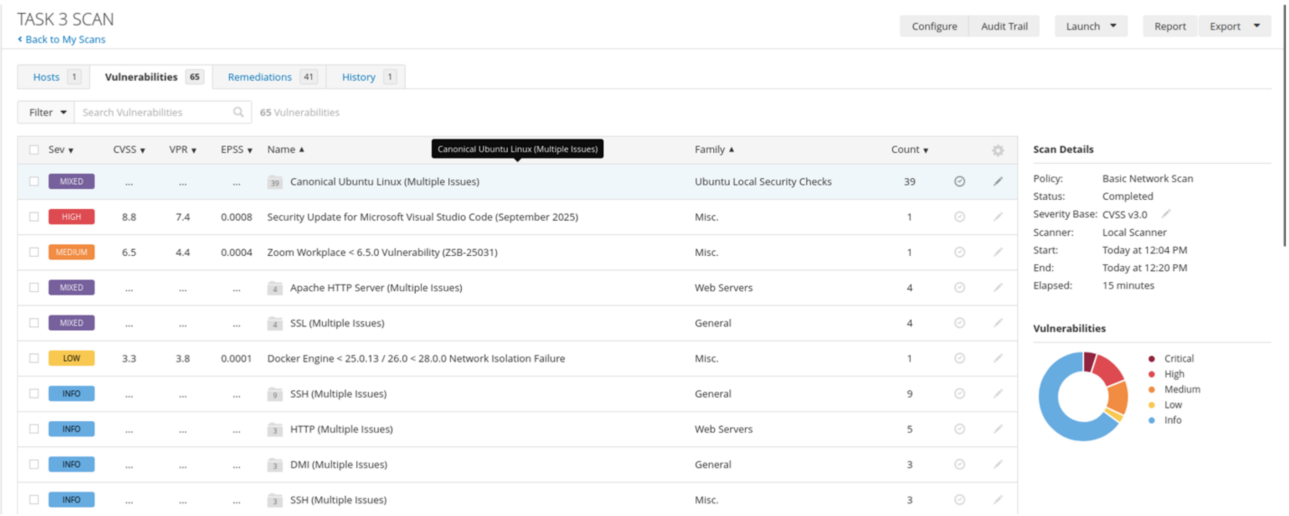
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:04 PM
End: Today at 12:20 PM
Elapsed: 15 minutes

Vulnerabilities

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:04 PM
End: Today at 12:20 PM
Elapsed: 15 minutes

Vulnerabilities



Sev	CVSS	VPR	EPSS	Name	Family	Count
MIXED	...	...	...	39 Canonical Ubuntu Linux (Multiple Issues)	Ubuntu Local Security Checks	39
HIGH	8.8	7.4	0.0008	Security Update for Microsoft Visual Studio Code (September 2025)	Misc.	1
MEDIUM	6.5	4.4	0.0004	Zoom Workplace < 6.5.0 Vulnerability (ZSB-25031)	Misc.	1
MIXED	...	...	...	4 Apache HTTP Server (Multiple Issues)	Web Servers	4
MIXED	...	...	...	4 SSL (Multiple Issues)	General	4
LOW	3.3	3.8	0.0001	Docker Engine < 25.0.13 / 26.0 < 28.0.0 Network Isolation Failure	Misc.	1
INFO	...	...	...	9 SSH (Multiple Issues)	General	9
INFO	...	...	...	3 HTTP (Multiple Issues)	Web Servers	5
INFO	...	...	...	3 DMI (Multiple Issues)	General	3
INFO	...	...	...	3 SSH (Multiple Issues)	Misc.	3

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:04 PM
End: Today at 12:20 PM
Elapsed: 15 minutes

Vulnerabilities