Vulnerability Assessment Report – Day 3 Internship Task

Project: Basic Vulnerability Scan Using Nessus Essentials

Prepared by: ***Putta Honna***

Operating System: Windows 11, kali Linux

1. Objective

The objective of this task is to perform a vulnerability assessment on my local machine using **Nessus Essentials**, identify security weaknesses, analyze their severity, and document recommended fixes.

2. Tools Used

- **Nessus Essentials**
- Operating System: *Windows/Linux*

3. Methodology

The following steps were performed:

1. Installed Nessus Essentials and completed product activation.
2. Configured a **Basic Network Scan** targeting the local machine IP.
3. Launched a full vulnerability scan.
4. Waited for the scan to complete approx. 30–60 minutes
5. Analyzed the scan report generated by Nessus.
6. Researched fixes for identified vulnerabilities.
7. Documented critical and high-severity vulnerabilities.
8. Captured screenshots of scan configuration and results.

4. Scan Findings Summary

Severity Level	Number of Vulnerabilities
Critical	----------
High	----------
Medium	CVE-1999-0524
Low	----------
Info	----------

5. Vulnerability 1 – Outdated Software Version

Severity: High
CVE ID: CVE-1999-0524 Vulnerability
Description:

CVE-1999-0524 refers to a vulnerability where **ICMP (Internet Control Message Protocol)** information, such as **netmask** and **timestamp**, is accessible from arbitrary hosts. This exposure can lead to potential misuse of sensitive network information, such as aiding attackers in reconnaissance or exploiting time-based attacks.

Key Details

- **Description**: The vulnerability arises when a system allows ICMP messages, specifically types 13 and 14 (timestamp request and reply) and types 17 and 18 (netmask request and reply), to be processed without proper access controls.
- **Impact**: Unauthorized actors can gather sensitive network details, such as the system's time or subnet mask, which could be leveraged for further attacks, including random number generator exploits seeded with the system time.
- **Severity**: The CVSS 2.0 base score is **2.1 (Low)**, indicating limited direct impact but potential for misuse in specific scenarios.

Affected Systems

This vulnerability affects multiple operating systems, including:

- Linux Kernel
- Microsoft Windows
- Apple macOS
- Cisco IOS
- Oracle Solaris
- HP-UX, IBM AIX, and others.

Mitigation

To mitigate this vulnerability:

1. **Restrict ICMP Traffic**: Configure firewalls to block or limit ICMP requests, especially timestamp and netmask-related messages.
2. **System Hardening**: Disable unnecessary ICMP responses in the system's network configuration.
3. **Vendor Patches**: Apply any available patches or updates from the operating system or device vendor.

Recommended Fix:
Enable secure configurations recommendion The vulnerability **CVE-1999-0524** is an **Information Leak/Disclosure** due to a system responding to **ICMP Timestamp Request** (type 13) and/or **ICMP Netmask Request** packets.

An attacker can use this response to gain information about the target system's time or network configuration.

The general recommendation to fix or mitigate this vulnerability is to **filter out the ICMP Timestamp Request and Reply messages** on affected hosts or network devices.

6. updating features:-

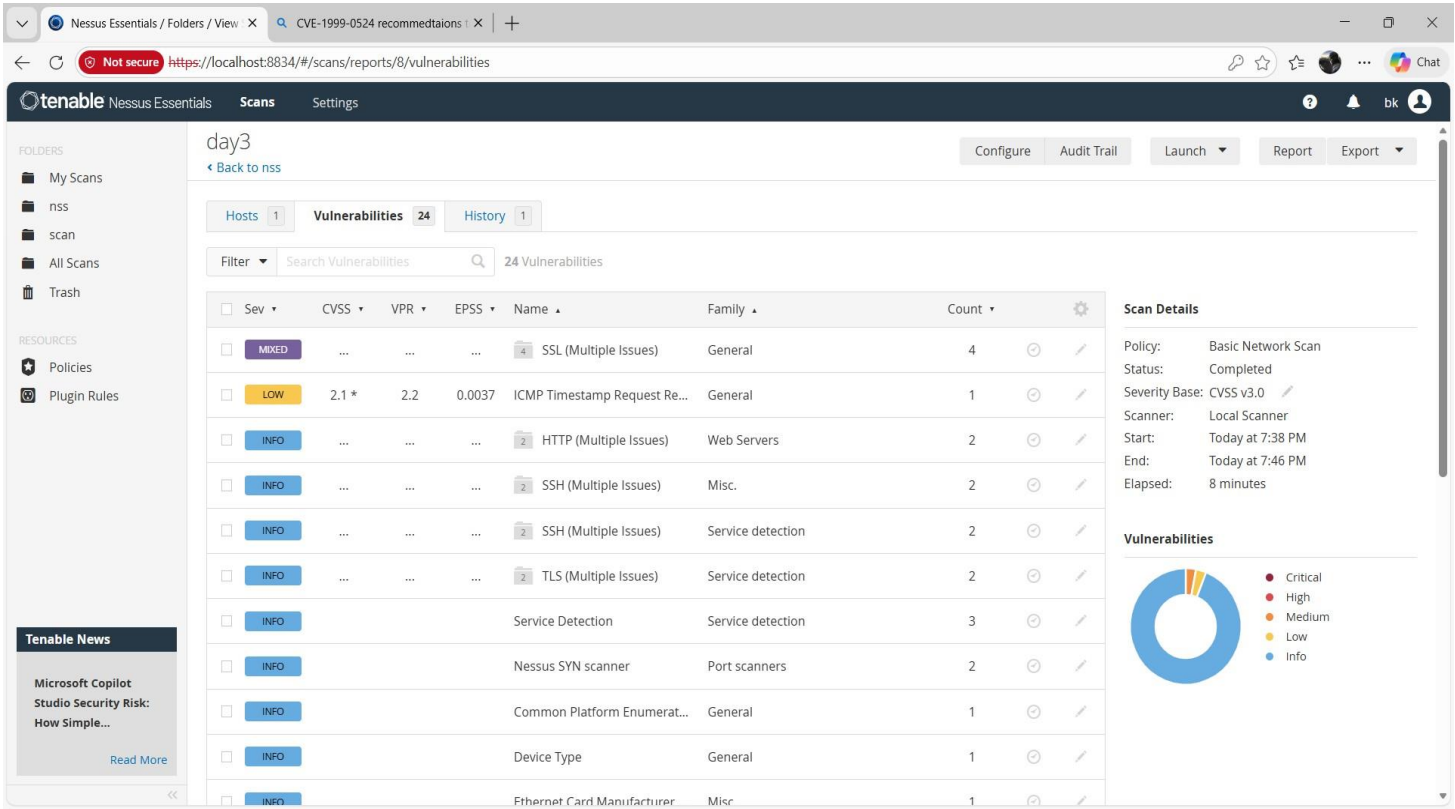
To improve system security:

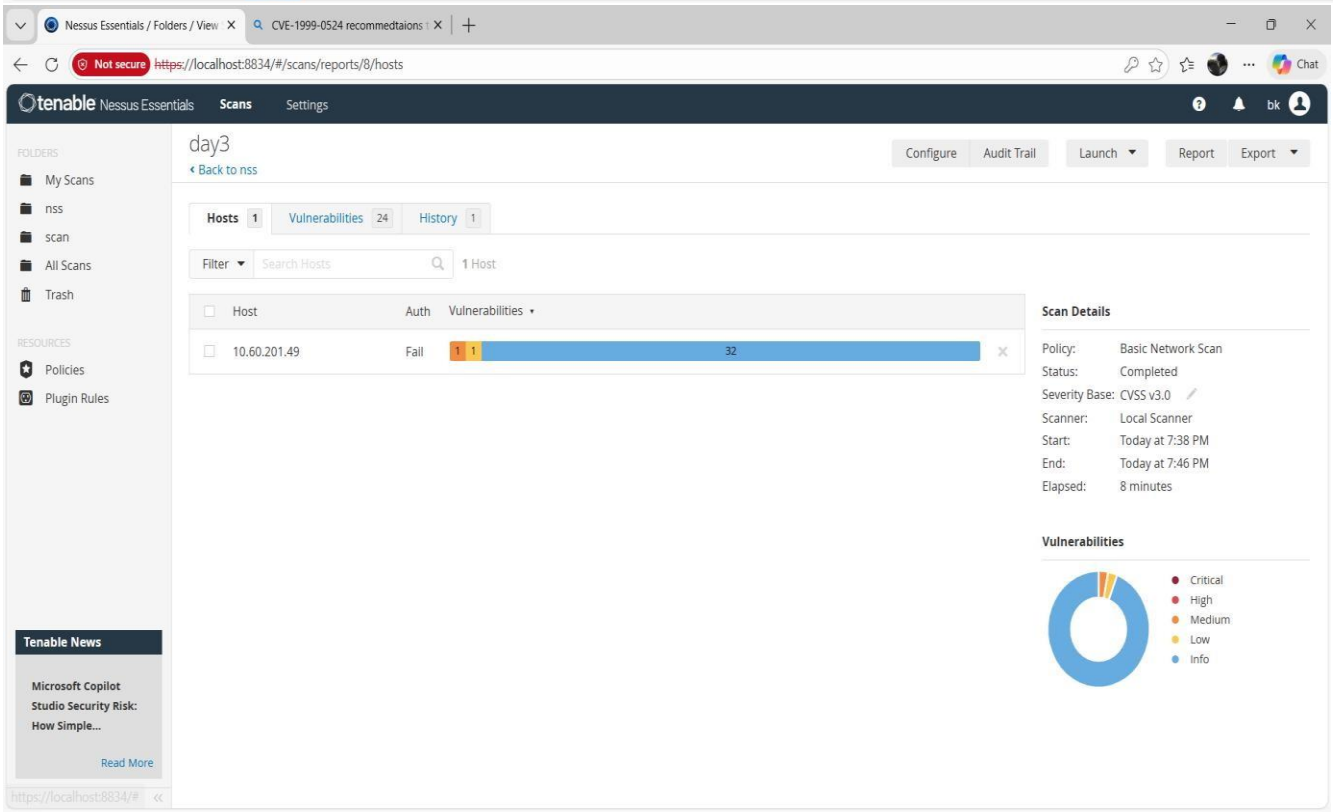
- Regularly update OS and installed applications.
- Disable or uninstall unused services.
- Enable firewall and restrict unnecessary ports.
- Follow vendor configuration guidelines.
- Re-run vulnerability scans monthly.

7. Screenshots:-

Ip addd:-- 10.60.201.49

- Final vulnerability results

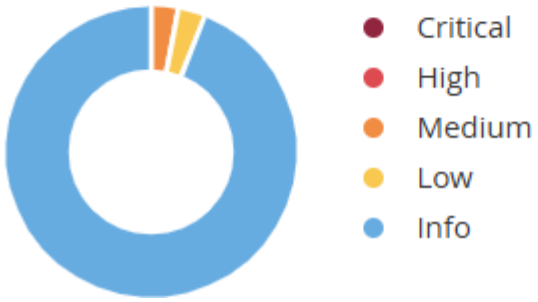




Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 7:38 PM
End:	Today at 7:46 PM
Elapsed:	8 minutes

Vulnerabilities



-
-
- **8. Conclusion**

The Nessus Essentials scan successfully identified multiple vulnerabilities on the local machine. By applying the recommended fixes, the overall security posture of the system can be significantly improved. This task enhanced my understanding of vulnerability scanning, remediation techniques, and basic security assessment workflow.