CYBER SECURITY INTERNSHIP

Task-3

Vulnerability Scan

Information

Name: K. Vamsi

Institution: Kalasalingam Academy of Research and Education

Internship Role: Cybersecurity Intern

Submission Date: 07/08/2025

1. Introduction

The purpose of this report is to assess and identify vulnerabilities in the target system using an automated vulnerability scanning tool. In this assessment, a comprehensive scan was conducted on a local machine using Nessus Essentials. The goal was to detect misconfigurations, outdated software, open ports, and known security flaws that could be exploited by malicious actors. Vulnerability scanning is a critical step in strengthening the security posture of any system. By identifying these security gaps early, organizations can take timely action to patch vulnerabilities, reduce attack surfaces, and ensure compliance with security best practices.

2. Tools and Environment

Tools	***Description***
Nessus	Automated vulnerability scanner.
xsltproc	Converts .nessus XML output to readable .html format

3. Methodology

- This vulnerability assessment was conducted using **Nessus Essentials**, targeting the local machine (localhost) to identify potential security weaknesses. The following steps were taken during the assessment process
- Installed and configured **Nessus Essentials** on a Kali Linux machine.
- Registered Nessus and allowed it to complete the plugin update.
- Set the scan target as 127.0.0.1 (localhost), representing the local system environment.

Scan Type

- Selected **Basic Network Scan** to perform a comprehensive vulnerability assessment.
- Configured scan settings and started the scan process.
- The scan was executed and took approximately 80 minutes to complete.
- Nessus probed open ports, services, OS details, and software versions to identify known vulnerabilities.

System scan

Hosts	Auth	Vulnerabilities
192.168.0.121	Fail	Critical – 11 High – 7 Medium – 27 Low – 9
192.168.0.122	Pass	Critical – 4 High – 1 Medium – 0 Low – 0
192.168.0.1	Fail	Critical – 3 High – 0 Medium – 10 Low – 4

192.168.0.117	Fail	Critical – 0 High – 2 Medium – 0 Low – 0
192.168.0.103	Fail	0
192.168.0.105	Fail	Low - 1
192.168.0.108	Fail	Low -1
192.168.0.110	Fail	Low -1

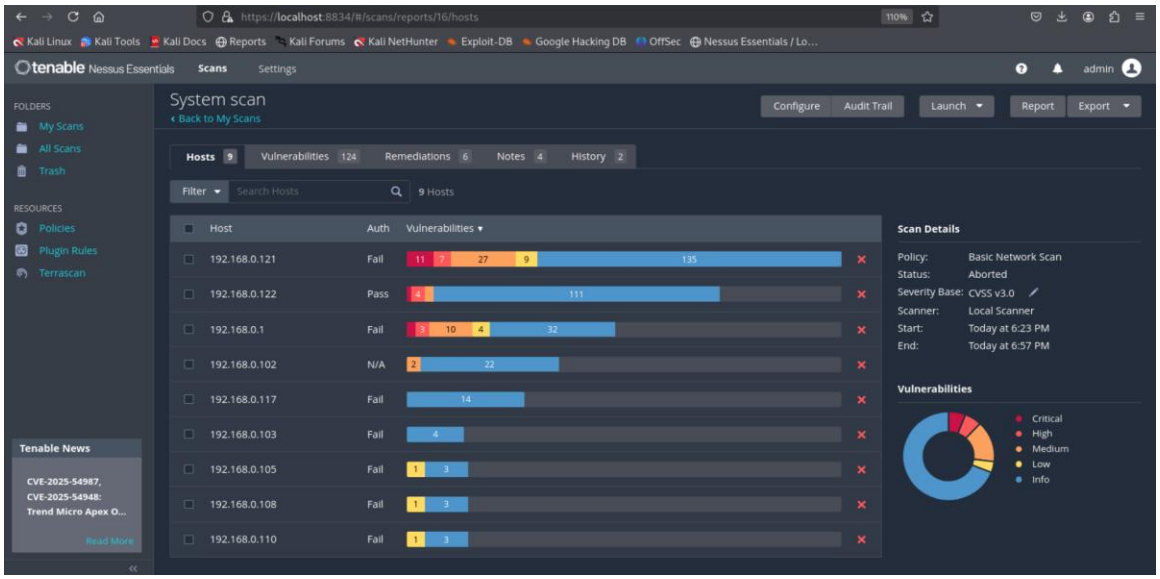
- **121 vulnerabilities** were identified across various system components.
- These vulnerabilities were categorized by severity based on above CVSS scores
  - **Critical**: 18
  - **High**: 10
  - **Medium**: 37
  - **Low/Info**: 121

IP address

I scanned the subnet 192.168.0.0/24 to detect live hosts and identify open ports and running services. The following IP addresses were identified as active 10 hosts

- 192.168.0.1 - network device
- 192.168.0.103 – **Windows**
- 192.168.0.105 – network device
- 192.168.0.108 - network device
- 192.168.0.110 - network device
- 192.168.0.117 - network device
- 192.168.0.121 - **Metasploitable2**
- 192.168.0.122 – **Kali linux**

- For testing purposes, a deliberately vulnerable machine (**Metasploitable2**) was included in the network at IP 192.168.0.121. This allowed realistic identification of common vulnerabilities.
- A vulnerability assessment was conducted using the **Nessus** scanner (Essentials/Free version). Nessus was used to scan the identified IPs for known vulnerabilities based on CVEs, misconfigurations, and outdated software.



Fig(1): Scanning Results

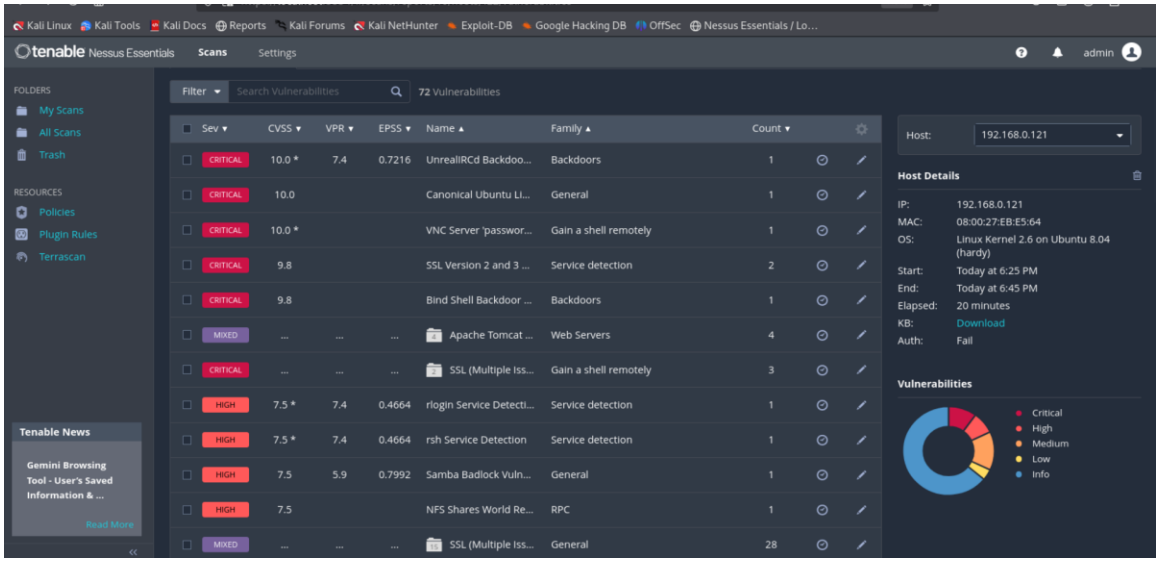


Fig (2): Severity and CVSS

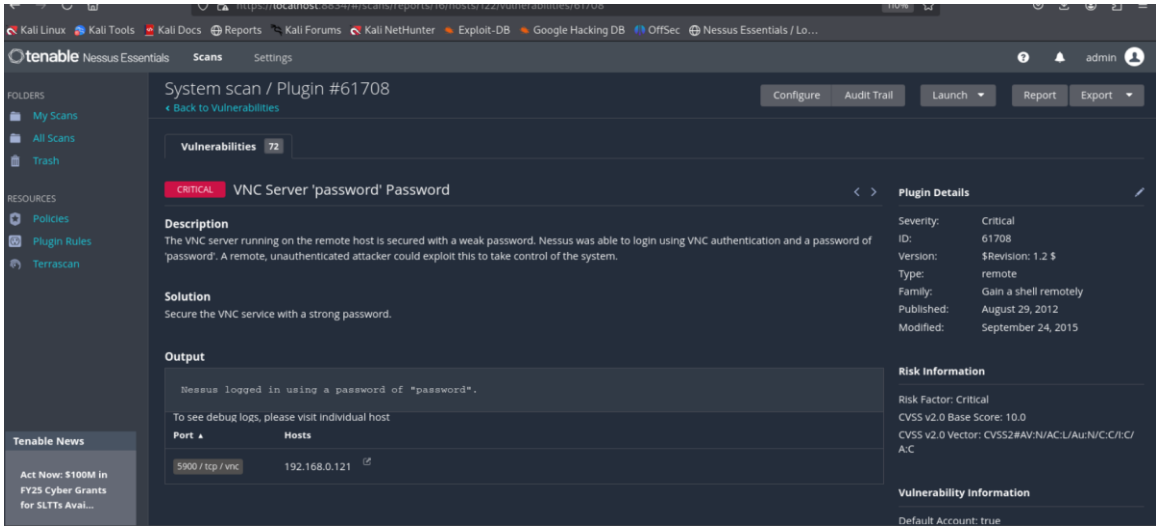


Fig (3): VNC Vulnerabilities

Mitigation Steps: Set a Strong VNC Password

- Login to the Metasploitable 2 machine.
- Run the following command: vncpasswd
- Enter a **new strong password** (minimum 8-12 characters, avoid dictionary words).
- Restart the VNC server:
- vncserver -kill :1
- vncserver :1
- You may replace :1 with your correct display number.

```
          RX packets:145 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14805 (14.4 KB)  TX bytes:7498 (7.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25617 (25.0 KB)  TX bytes:25617 (25.0 KB)

msfadmin@metasploitable:~$ vncpassswd
-bash: vncpassswd: command not found
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$
```

Fig (4): apply the changes

Remediation

TOP 5 critical Vulnerabilities in my findings

1. **UnrealIRCd Backdoor Detection**
   ➤ **Remediation:** Remove UnrealIRCd and install the latest official version from the trusted source.

2. **Canonical Ubuntu Linux SEoL (8.04.x)**
   ➤ **Remediation:** Upgrade to a supported Ubuntu version (e.g., 20.04 or later).

3. **VNC Server 'password' Password**
   ➤ **Remediation:** Set a strong VNC password (avoid default/common passwords like "password").

4. **SSL Version 2 and 3 Protocol Detection**
   ➤ **Remediation:** Disable SSLv2 and SSLv3 in all services and enforce TLS 1.2+.

5. **Bind Shell Backdoor Detection**
   ➤ **Remediation:** Kill the bind shell process and perform a full malware cleanup or reinstall the OS.