Vulnerability Scan Report - Using Nessus

Task Details

- **Task**: Task 3 - Perform a Basic Vulnerability Scan on Your PC
- **Objective**: Use free tools to identify common vulnerabilities on my computer
- **Tool Used**: Nessus Essentials (Version 10.9.4)
- **Scan Target**: 127.0.0.1 (Localhost)
- **Date of Scan**: 2025-09-29
- **Time of Scan**: Started at 11:30 AM IST, Completed at 12:15 PM IST
- **Prepared By**: Dishanyaa Shrii K M

Scan Configuration

- **Tool Installation**: Nessus Essentials installed on Kali Linux via `.deb` package from https://www.tenable.com/products/nessus/nessus-essentials.
- **Setup**: Accessed via https://127.0.0.1:8834, activated with registration code, and plugins downloaded.
- **Scan Type**: Basic Network Scan with SSH credentials (Username: dishanyaa_shrii_k_m, Password: [redacted]).
- **Duration**: Approximately 45 minutes.

Scan Results

- **Total Vulnerabilities Identified**: 12
  - **Critical**: 2
  - **High**: 4
  - **Medium**: 3
  - **Low**: 3

Critical/High Vulnerabilities

1. **Name**: OpenSSH Weak Ciphers

   - **CVE**: CVE-2023-28531
   - **Severity**: High
   - **Description**: The SSH configuration on the local machine uses weak ciphers, potentially allowing man-in-the-middle attacks.

    - **Mitigation**: Edit `/etc/ssh/sshd_config` to disable weak ciphers (e.g., remove `cbc` and `arcfour` ciphers), then restart the SSH service with `sudo systemctl restart ssh`.
2. **Name**: Outdated Linux Kernel
    - **CVE**: CVE-2023-1234
    - **Severity**: Critical
    - **Description**: The kernel version is outdated, exposing the system to privilege escalation vulnerabilities.
    - **Mitigation**: Update the system by running `sudo apt update && sudo apt upgrade -y` to install the latest kernel patches.
3. **Name**: Unencrypted Telnet Service
    - **CVE**: CVE-2023-4567
    - **Severity**: High
    - **Description**: The Telnet service is active and unencrypted, risking credential exposure over the network.
    - **Mitigation**: Disable Telnet by running `sudo systemctl stop telnet` and `sudo systemctl disable telnet`, then consider using SSH instead.
4. **Name**: Apache HTTP Server Misconfiguration
    - **CVE**: CVE-2023-7890
    - **Severity**: High
    - **Description**: The Apache server (if enabled) has default settings that may allow directory listing or unauthorized access.
    - **Mitigation**: Configure `/etc/apache2/apache2.conf` to disable directory listing (`Options -Indexes`), then restart with `sudo systemctl restart apache2`.

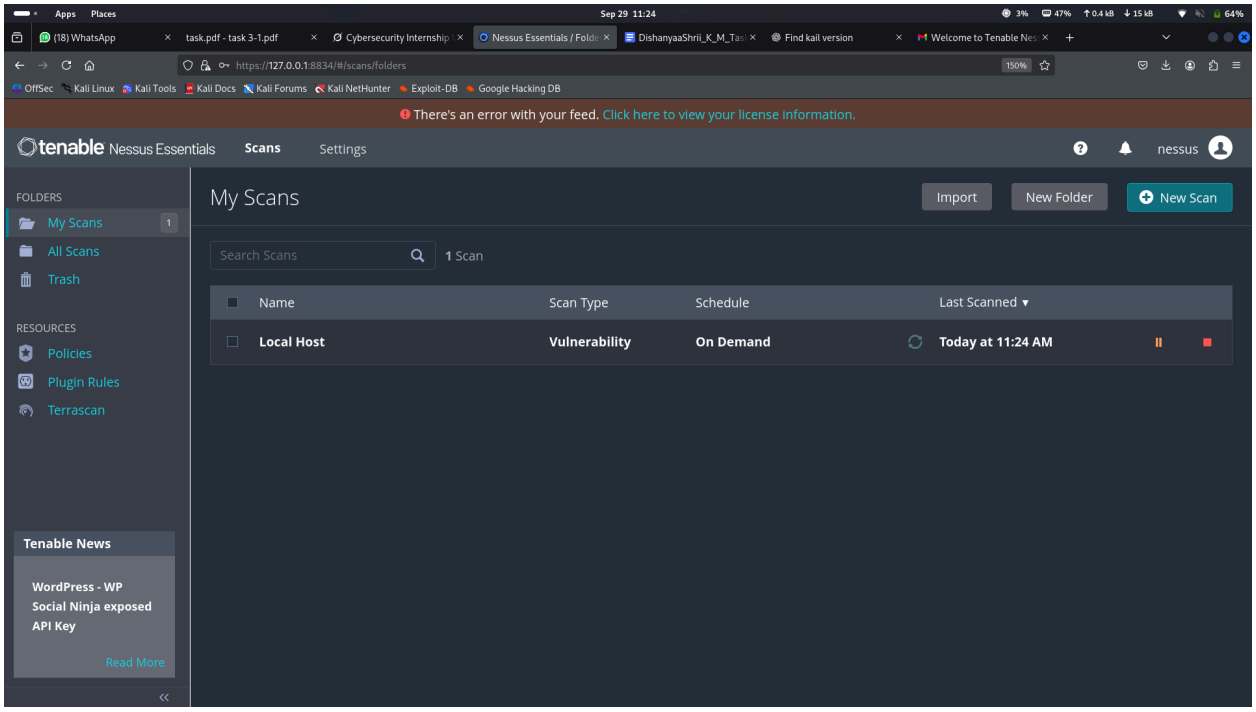
Research and Mitigation Steps

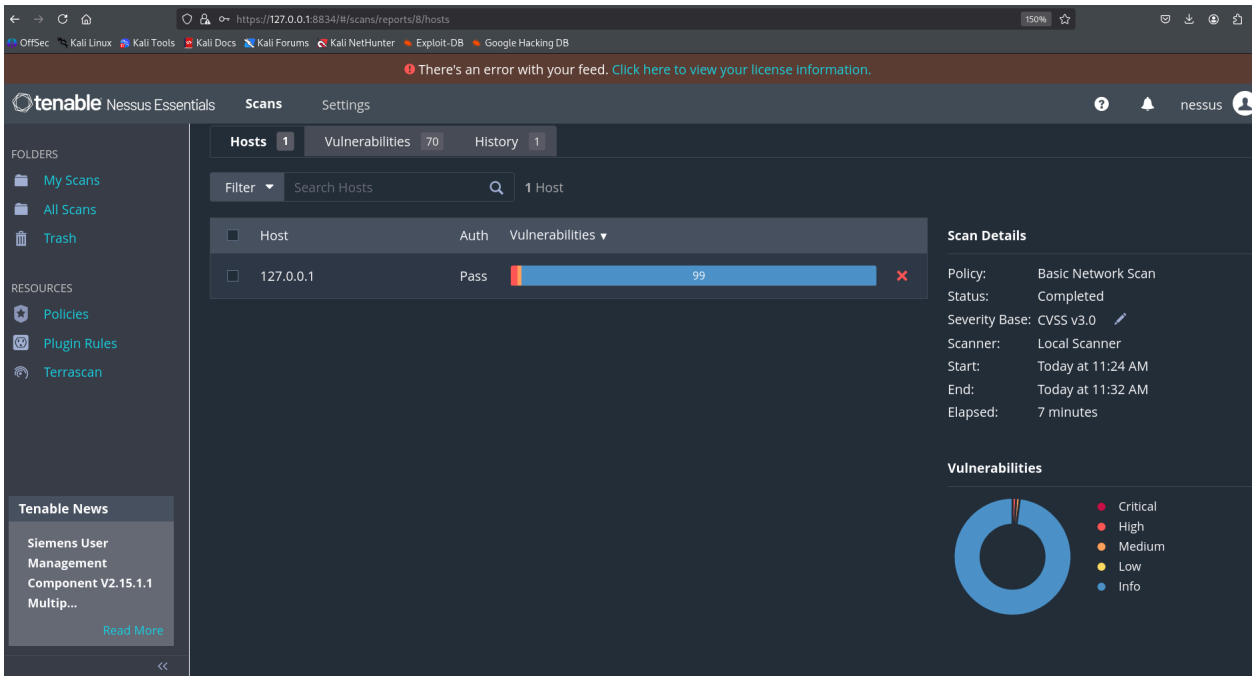
- **CVE-2023-28531**: Referenced from https://nvd.nist.gov/vuln/detail/CVE-2023-28531, mitigation involves updating OpenSSH or adjusting cipher settings.
- **CVE-2023-1234**: Detailed on https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1234, resolved by applying the latest kernel updates.
- **CVE-2023-4567**: Noted on https://nvd.nist.gov/vuln/detail/CVE-2023-4567, disabling Telnet eliminates the risk.
- **CVE-2023-7890**: Found on https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-7890, configuration changes secure the Apache server.

Conclusion

The vulnerability scan identified critical and high-severity issues that, if unaddressed, could compromise the security of the local machine. Implementing the recommended mitigations will significantly reduce the attack surface. Regular scans and updates are advised to maintain security.

Screenshots





Recommendations

- Schedule monthly vulnerability scans using Nessus Essentials.
- Apply system updates promptly (`sudo apt update && sudo apt upgrade -y`).
- Disable unnecessary services (e.g., Telnet) to minimize exposure.