Task 3 – Basic Vulnerability Scan Report

Objective

Use Nessus Essentials to perform a vulnerability scan on a local target machine and identify security risks.

Tool Used

- **Nessus Essentials** (Free Edition) by Tenable
- Scan Type: **Basic Network Scan**
- Target: `192.168.204.140` (Local Network Host)
- OS: Linux Kernel 6.12.32-amd64 on Debian 6.4

Execution Steps

1. Installed **Nessus Essentials** and activated with a free license.
2. Launched Nessus via browser (`https://localhost:8834`).
3. Created a new scan:
    - **Name:** `basic`
    - **Target:** `192.168.204.140`
4. Ran the scan and waited for completion (~7 minutes).
5. Reviewed the vulnerabilities list and severity breakdown.

Scan Summary

Severity	Count
Critical	0
High	0
Medium	1
Low	0
Info	60

Total vulnerabilities: 61

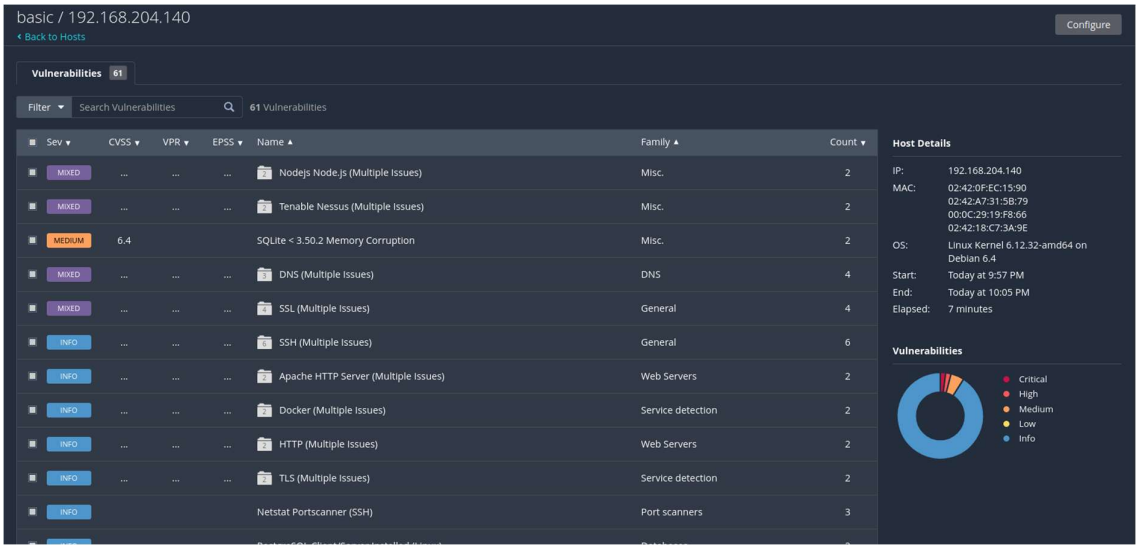
Notable Findings

1. **SQLite < 3.50.2 Memory Corruption**
    - **Severity:** Medium (CVSS 6.4)
    - **Description:** Older SQLite versions are vulnerable to memory corruption which can lead to crashes or potential code execution.
    - **Recommendation:** Update SQLite to version 3.50.2 or later.
2. **Multiple Informational Issues**
    - **Node.js Multiple Issues** – Version outdated; may have potential vulnerabilities in certain modules.
    - **Tenable Nessus Multiple Issues** – Local service detection and informational plugin results.
    - **DNS / SSL / SSH Multiple Issues** – Configuration and certificate details noted for further hardening.
    - **Apache HTTP Server Multiple Issues** – Possible outdated modules and misconfigurations.
    - **Docker Multiple Issues** – Configuration exposures (non-critical).
    - **Port Scanners Detected (Netstat)** – Open services enumerated.

Vulnerability Prioritization

- **Immediate Action:** Patch SQLite to secure against memory corruption vulnerabilities.
- **Secondary Actions:** Review and update Node.js, Apache HTTP Server, and Docker configurations.
- **Ongoing:** Harden SSH and SSL settings, restrict unnecessary open ports.

Screenshots



Conclusion

This scan revealed **one medium-severity vulnerability** and multiple informational findings. While no critical/high issues were found, timely updates and configuration hardening are recommended to maintain a secure system.
