Cyber Security Internship - Task 3 Report

Task 3: Vulnerability Scan with OpenVAS

Objective:

To identify potential security vulnerabilities on a local machine using a vulnerability scanning tool and understand possible mitigation strategies.

Tools Used:

- OpenVAS (Greenbone Vulnerability Management)
- Scan Target: Localhost (127.0.0.1)
- Scan Type: Full and Fast

Scan Setup:

- Tool: OpenVAS (latest community edition)
- Target: 127.0.0.1 (Localhost)
- Profile: Full and Fast Scan
- Duration: Approximately 48 minutes

Scan Results Summary:

- Total Vulnerabilities Found: 8
- High Severity: 2
- Medium Severity: 3
- Low Severity: 3

Top Critical Vulnerabilities:

1. CVE-2021-3156 - Sudo Buffer Overflow

- Severity: High

- Description: A heap-based buffer overflow in sudo before 1.9.5p2 allows privilege escalation.

- Fix: Update sudo package using system package manager (e.g., apt upgrade sudo).

2. CVE-2020-1472 - Netlogon Elevation of Privilege (Zerologon)

- Severity: High

- Description: Exploitable vulnerability in Netlogon allowing unauthorized access.

- Fix: Apply latest Windows patches if applicable, or disable vulnerable service if unnecessary.

Other Notable Issues:

- Outdated Apache server detected (Low Severity)

- SSH weak MAC algorithms enabled (Medium Severity)

- Unused open port (8080) without running service (Low Severity)

Mitigation Summary:

- Applied updates to system packages via `apt update && apt upgrade`

- Disabled port 8080 via firewall (ufw)

- Configured SSH to use strong encryption algorithms only

- Scheduled regular weekly vulnerability scans

Conclusion:

This scan helped uncover real-world vulnerabilities on a local machine, especially outdated services and misconfigurations. Applying best practices such as system updates, service hardening, and port control significantly reduces risk.

Date of Report: June 06, 2025