Elevate Labs – Cyber Security Internship

NAME: Srinivas Atta

Task 3: Perform a Basic Vulnerability Scan on Your PC

By: Ministry of MSME, Govt. of India

Objective

Use free vulnerability scanning tools to identify common security issues and weaknesses on your personal computer, and understand basic risk assessment techniques.

Tools Required

- OpenVAS Community Edition (free vulnerability scanner)
  or
- Nessus Essentials (free for personal use)

Execution Steps / Guide

1. Install Vulnerability Scanner
   - Download and install OpenVAS Community Edition (recommended) or Nessus Essentials from their official websites.
   - Register for a free activation key if required (Nessus Essentials).
2. Set Up the Scan Target
   - Configure the scanner to target your local machine's IP address (`localhost` or its IPv4/IPv6).
   - Temporarily adjust firewall rules if needed for scanning.
3. Run a Full Vulnerability Scan
   - Create a new scan task and select "Full and Fast Scan" or equivalent.
   - Wait for the scan to finish (can take 30–60 minutes).
4. Review Scan Results
   - Open the generated report after completion.
   - Take screenshots of the dashboard, vulnerabilities list, and example vulnerability details.

5. Document and Analyze Key Findings
    - Highlight the most critical vulnerabilities (by severity rating).
    - Research each one's security impact.
6. Plan and Document Remediation
    - Identify fixes like patches, disabling services, or configuration changes.

Findings / Results

- Tool Used: [OpenVAS / Nessus Essentials]
- Target: [localhost / your PC's IP]
- Scan Duration: [e.g., 40 minutes]
- Vulnerabilities Detected: [X total, Y High, Z Medium]

Sample Findings:

1. Outdated OpenSSH – *High risk*, potential remote code execution.
2. Missing Windows/Ubuntu Security Updates – *Medium/High risk*, allows privilege escalation.
3. Open Ports Detected – Unnecessary services (FTP/RDP/SMB) exposed to network.

Evidence: *(Insert screenshots of scan results here)*

Security Analysis

The scan revealed outdated software, missing updates, and unneeded services. These could allow attackers to exploit known vulnerabilities, perform privilege escalation, or gain control of the system.

Recommendations

- Keep OS, software, and dependencies up-to-date.
- Disable unused ports/services.
- Enable automatic updates where possible.
- Run scheduled vulnerability scans monthly.
- Enforce strong authentication policies.

Outcome

- Hands-on experience using vulnerability scanners.
- Learned to assess and prioritize vulnerabilities.

- Understood the role of patching and configuration hardening in system security.

Key Concepts

- Vulnerability scanning
- Risk assessment
- CVSS (Common Vulnerability Scoring System)
- Remediation steps
- Preventive security practices