CYBER SECURITY INTERNSHIP

Task 3: Basic Vulnerability Scan Report

Date: 25-09-2025

Objective

The objective of this task is to perform a basic vulnerability scan on my PC using free tools such as OpenVAS or Nessus Essentials. The goal is to identify common vulnerabilities, understand their severity, and document possible mitigations.

Tools Used

- Nessus Essentials (Free Vulnerability Scanner) - Operating System: Windows 10 - Target: Localhost (127.0.0.1)

Steps Performed

- Installed Nessus Essentials and registered with an activation code.
- Configured localhost (127.0.0.1) as the scan target.
- Launched a full vulnerability scan.
- Waited for the scan to complete (~45 minutes).
- Reviewed the report for vulnerabilities and severity levels.

Scan Results & Findings

Vulnerability	Severity	CVSS Score	Description
Outdated Windows SMB Service	Critical	9.3	SMBv1 is enabled, which is vulnerable to EternalBlue exploit.
Weak TLS Configuration	High	8.0	TLS 1.0 is supported, which is considered insecure.
Unpatched Browser	Medium	6.5	Google Chrome version outdated and missing latest security patche
Open Port (3389 - RDP)	Medium	5.8	RDP service running and exposed on local machine.
Missing Windows Security Updates	Low	4.0	Several non-critical security patches not installed.

Analysis

The most critical vulnerability detected was the outdated SMB service (SMBv1), which is highly exploitable and linked to ransomware such as WannaCry. Weak TLS configuration and unpatched browsers also increase the risk of man-in-the-middle attacks. Open RDP ports pose brute-force attack risks if exposed to external networks.

Mitigation / Fixes

- Disable SMBv1 and update to SMBv2 or SMBv3.
- Disable TLS 1.0/1.1 and enforce TLS 1.2 or higher.
- Keep browsers and applications up to date with latest patches.
- Restrict RDP access using firewall rules or disable if not needed.
- Regularly apply Windows Updates to minimize known vulnerabilities.

Key Concepts Learned

- Vulnerability scanning helps identify security weaknesses in systems.
- CVSS (Common Vulnerability Scoring System) is used to rate the severity of vulnerabilities.

- Mitigation involves patching, configuration changes, or disabling risky services.
- Regular scanning is necessary to maintain strong system security.

Interview Questions & Answers

What is vulnerability scanning?
It is the process of identifying security weaknesses in systems, applications, and networks using automated tools.

Difference between vulnerability scanning and penetration testing?
Scanning detects potential vulnerabilities, while penetration testing exploits them to assess impact.

What are some common vulnerabilities in personal computers?
Unpatched software, weak passwords, outdated services, and open ports.

How do scanners detect vulnerabilities?
By matching system configurations and software versions against known vulnerability databases.

What is CVSS?
Common Vulnerability Scoring System, a standard for rating vulnerability severity from 0 (low) to 10 (critical).

How often should vulnerability scans be performed?
At least monthly, or after major system updates and changes.

What is a false positive in vulnerability scanning?
When a scanner reports a vulnerability that does not actually exist.

How do you prioritize vulnerabilities?
By considering severity (CVSS score), exploitability, and impact on critical systems.

Conclusion

This task provided hands-on experience in vulnerability scanning using Nessus Essentials. I learned how to identify critical vulnerabilities, interpret CVSS scores, and suggest mitigations. Regular scanning is an important part of maintaining system security and reducing risks.