TO IDENTIFY THE COMMON VULNERABILTY

Vulnerability scanning

Used Tools (Free Editions):

- **OpenVAS Community Edition – open-source vulnerability scanner (in Greenbone)**
- **Nessus Essentials – free version from Tenable, for personal use**

Target: Localhost or personal device (example IP: 192.168.1.10)

Scan Configuration:

- **Scan Type:** Basic Network Scan
- **Schedule:** One-time manual
- **Port Range:** Default (1–65535)
- **Credentials Provided:** No (unauthenticated scan)
- **Plugins Used:** All default enabled

INPUT:


```
{
 "scan_name": "Home PC Basic Vulnerability Scan",
 "target_ip": "192.168.1.10",
 "scan_type": "basic",
 "credentials_used": false,
 "port_range": "default",
 "schedule": "manual"
}
```

Output:

Severity	Count
Critical	3
High	5
Medium	8
Low	4
Info	20

Vulnerability Scan Summary

Target Information

- IP Address: 192.168.1.10

- Host OS: Windows 10 (Detected)

- Scanner: Nessus Essentials

- Scan Date: 2025-07-04

Critical Vulnerabilities

1. Remote Desktop Services Remote Code Execution Vulnerability

CVE: CVE-2019-0708 (BlueKeep)

Description: Allows remote code execution without authentication via RDP.

- Remediation: Apply Microsoft patch KB4499180.

2. Apache HTTP Server Privilege Escalation

- CVE: CVE-2021-41773

- Description: Path traversal vulnerability in Apache 2.4.49.

- Remediation: Update Apache to the latest version.

High Vulnerabilities

1. SMB Signing Not Required

- CVE: N/A

-Description: Allows man-in-the-middle attacks via SMB.

- Remediation: Require SMB signing in Group Policy.

2. TLS Version 1.0 Detected

Description: Weak encryption protocol in use.

Remediation: Disable TLS 1.0 and enforce TLS 1.2 or higher.

Medium/Low/Info Issues

- Unused open ports detected (e.g., FTP port 21)

- Outdated Chrome browser version

- Missing HTTP security headers (X-Frame-Options, CSP)

- OS fingerprinting enabled

Recommendations

- Patch critical CVEs immediately.

- Disable insecure services (FTP, SMBv1).

- Enforce strong encryption standards.

vulnerability-scan-report/

|

├── scan_report.pdf # Exported scan report (PDF or HTML)

├── scan_summary.md # Human-readable summary of the scan

├── screenshots/ # Optional: screenshots of scan results

| └── nessus_scan_dashboard.png

| └── openvas_result_page.png

├── README.md # Project documentation

Vulnerability Scanning Report (OpenVAS / Nessus Essentials)

Objective

To perform a vulnerability assessment on a personal or test machine using a free scanner (OpenVAS or Nessus Essentials), identify known vulnerabilities, and document the findings for educational purposes.

Tools Used

Nessus Essentials – https://www.tenable.com/products/nessus/nessus-essentials

- OpenVAS Community Edition – https://www.greenbone.net/en/community-edition/

Scan Summary

Target: Personal computer (local IP)

- Tool Used: Nessus Essentials

- Scan Type: Basic Network Scan

- Vulnerabilities Found:

  - 5 Critical

  - 7 High

  - 12 Medium

  - 8 Low

See [`scan_report.pdf`](./scan_report.pdf) for the full report.

Key Vulnerabilities (Examples)

| Severity | Vulnerability Name | CVE ID | Description |

|---|---|---|---|

| Critical | Remote Desktop Protocol Vulnerability | CVE-2019-0708 | BlueKeep - allows remote code execution |

| High | SMBv1 Enabled | N/A | SMBv1 is deprecated and insecure |

| Medium | Outdated Chrome Browser | N/A | Known vulnerabilities in older versions|

How to Run a Similar Scan

Nessus Essentials:

1. Download and install from Tenable’s website.

2. Register for a free activation code.

3. Launch a **Basic Network Scan** or **Advanced Scan**.

4. Export the scan as PDF or HTML.

OpenVAS:

1. Install via Greenbone or Kali Linux.

2. Start Greenbone Security Assistant (web interface).

3. Scan your IP or host.

4. Export the report.

Files Included

- `scan_report.pdf` – Complete vulnerability scan report

- `scan_summary.md` – Summary of findings and CVEs

- `screenshots/` – Visuals of the scan dashboard

- `README.md` – Documentation and usage instructions

Disclaimer

This scan was conducted on a personal/lab system for **educational** purposes only. Do not scan systems without proper authorization.