

EXTION INFOTEC PROJECT 1

NETWORK

VULNERABILITY

ASSESSMENTS

MYCHARLA MADHAVKUMAR

13/08/2024

Table of Contents

1. Introduction

- Purpose of the Network Vulnerability Assessment
- Overview of the Project Objectives

2. Preparation Phase

- Defining Scope and Objectives
- Obtaining Permissions and Authorizations
- Setting Up Scanning Tools

3. Vulnerability Scanning

- Conducting External Network Scans
- Performing Internal Network Scans

4. Risk Assessment

- Using CVSS for Vulnerability Scoring
- Prioritizing Risks Based on Severity

5. Mitigation Strategy

- Developing Mitigation Recommendations
- Implementing Security Patches and Updates

6. Documentation and Reporting

- Generating Detailed Vulnerability Reports
- Creating Executive Summaries for Stakeholders

7. Implementation and Verification

- Applying Recommended Changes
- Verifying Effectiveness of Mitigations

8. Conclusion

- Summary of Key Findings and Actions
- Importance of Regular Vulnerability Assessments

Project Overview:

The project aims to conduct a comprehensive assessment of the network infrastructure of [SREEPAADA DEGREE COLLEGE] to identify and mitigate potential vulnerabilities. The assessment will encompass both internal and external network components to ensure a thorough evaluation.

Project Objectives:

1. **Identify Vulnerabilities:** Conduct a thorough scan and analysis of the network to identify potential vulnerabilities.
2. **Assess Risk Levels:** Evaluate the severity and potential impact of identified vulnerabilities on the network.
3. **Recommend Mitigation Strategies:** Propose effective strategies and countermeasures to mitigate identified vulnerabilities.
4. **Enhance Security Posture:** Improve overall network security by implementing recommended changes and best practices.

Project Scope:

1. **Network Components:** Assess all critical network components including routers, switches, firewalls, servers, and endpoints.
2. **Network Protocols:** Evaluate vulnerabilities related to TCP/IP protocols, DNS, DHCP, etc.
3. **External Assessment:** Perform external scans to identify vulnerabilities accessible from outside the organization's network.
4. **Internal Assessment:** Conduct internal scans to identify vulnerabilities within the organization's internal network.
5. **Wireless Network:** Assess vulnerabilities related to Wi-Fi networks and access points.
6. **Web Applications:** Scan web applications hosted on the network for security vulnerabilities.

Project Methodology:

1. Preparation:

- Define scope and objectives.
- Obtain necessary permissions and approvals.
- Set up scanning tools and resources.

2. Vulnerability Scanning:

- Conduct external and internal network scans using appropriate vulnerability scanning tools (e.g., Nessus, OpenVAS, and Nmap).
- Analyze scan results to identify vulnerabilities.

3. Risk Assessment:

- Prioritize identified vulnerabilities based on severity (e.g., CVSS scores).
- Assess potential impact on network security and operations.

4. Mitigation Strategy:

- Develop a plan to address identified vulnerabilities.
- Prioritize mitigation efforts based on risk assessment.

5. Implementation:

- Implement recommended changes and security patches.
- Verify effectiveness of mitigation measures.

6. Documentation and Reporting:

- Compile assessment findings into a comprehensive report.
- Create an executive summary and presentation for stakeholders.

Resources Required:

- **Vulnerability Scanning Tools:** Nessus, OpenVAS, Nmap, Wapplazyer.
- **Documentation Tools:** Microsoft Office Suite, reporting templates.
- **Communication Tools:** Email, Mobiles, WhatsApp.

Personally Used Tools in this Project:

- **Nessus:** A comprehensive vulnerability scanning tool that can identify a wide range of vulnerabilities across the network infrastructure.
- **Nexpose Community:** An open-source vulnerability-scanning tool developed by Rapid7 that can automatically detect new devices and evaluate vulnerabilities.
- **Nikto:** An open-source web server scanner that can check for outdated server versions and scan for potentially dangerous files and programs.
- **Wireshark:** A powerful network protocol analyzer that can capture and analyze network traffic to identify security issues.
- **Aircrack:** A tool focused on Wi-Fi security that can be used for network auditing and retrieving lost encryption keys.
- **Nmap:** A network reconnaissance tool that can be used to identify active hosts, open ports, and running services on the target network.
- **Maltego:** A vulnerability assessment tool that can prioritize scanning, detect vulnerabilities, and generate comprehensive reports.

Purpose of the Network Vulnerability Assessment:

The main Aim of Network Vulnerability test has to identify the vulnerabilities in network and Websites Using the Above tools.

Target Network:	<i>Sreepaada Degree College</i>
Website URL:	https://sreepaadadegreecollege.org/
Registration on:	2022-05-12
Expires on:	2025-05-12
<u>Name Servers</u>	
ns1.dns-parking.com	162.159.24.201
ns2.dns-parking.com	162.159.25.42
IPV4:	93.127.208.87
IPV6:	2a02:4780:11:1594:0:6ab:174e:6

Geolocation data from IP2Location

Product: DB6, 2024-7-1




IP ADDRESS: 93.127.208.87



ISP: IPFFM - Internet Provider Frankfurt GmbH



COUNTRY: India 



ORGANIZATION: Not available



REGION: Maharashtra



LATITUDE: 19.0760



CITY: Mumbai



LONGITUDE: 72.8774

[Incorrect location? Contact IP2Location](#)



[view map](#)

USAGE OF THE TOOLS IN THIS PROJECT

1. NMAP (Port Scanner):-

I Performed Nmap for port scanning on this website, there some open ports

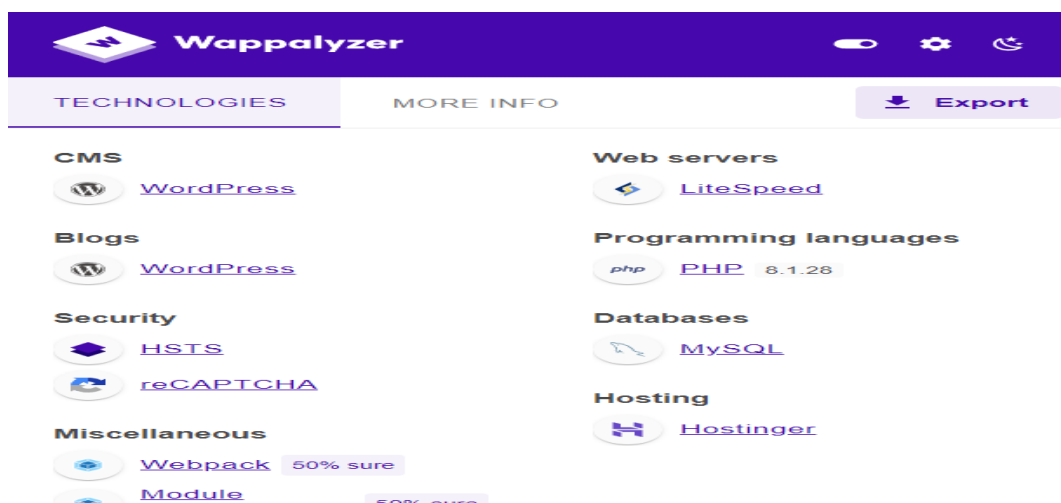
- 21/Tcp ftp
- 80/Tcp http
- 443/tcp https
- 3306/tcp MySQL

```
(kali㉿kali)-[~]
└─$ nmap 93.127.208.87
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-13 05:55 EDT
Nmap scan report for 93.127.208.87
Host is up (0.040s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
```

2. Wappalzyer (Technologies used in this Website):-

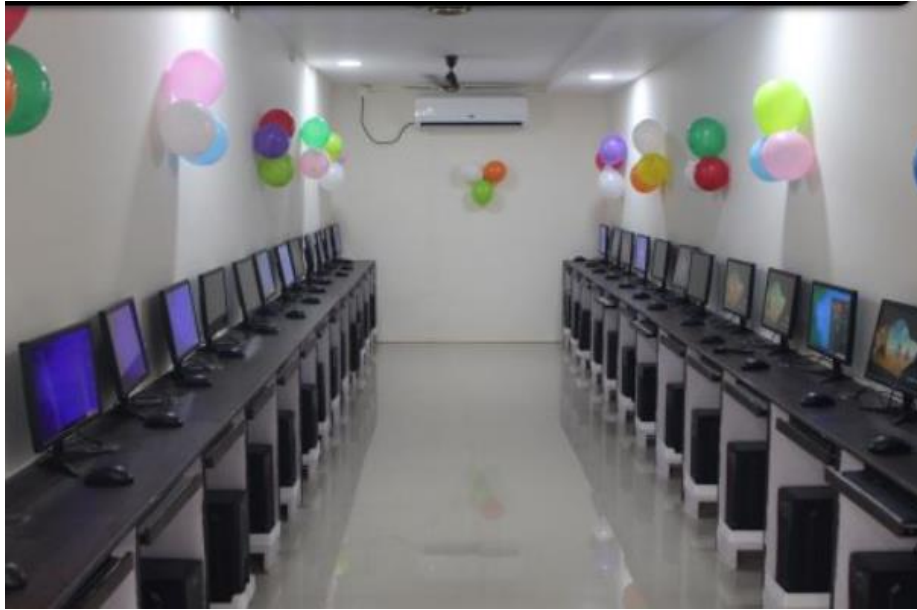
Using this tool to know what are technologies are used to build this website and any vulnerabilities/bugs available in this technologies (Outdated software's) are used.



3. Maltego (Vulnerability analysis tool for Website):-

Maltego is tool is mainly used for deep report about Website, which is Dns address, Document snapshots, domains, any data is leaked in web like PDFs, Sub Domains, Email ids, Phone Numbers ...etc.

Leaked Snaps:



<https://web.archive.org/web/20240705135007/https://sreepaadadegreecollege.org/admin/uploads/slides/52689.jpeg> - : Link

We fixed some bugs and updated domain team about this issue in this website

4. **Aircrack:-**

A tool focused on Wi-Fi security that can be used for network auditing and retrieving lost encryption keys.

Using a tool I will be find in wireless connection security vulnerability they maintain username & Password is Default like Admin & admin.

- I will Update the Username and Password
- Password Encryption Become stronger
- Apply Mac Filtration
- Ip Scanning And Device Identification
- Ip Camera Device Authentication check.

5. **Wireshark:**

A powerful network protocol analyser that can capture and analyse network traffic to identify security issues.

- Packet sniffing
- Packet Capturing
- Username and Password Capturing(Sniff)
- Traffic analyser

6. **Nexpose Community:**

An open-source vulnerability-scanning tool developed by Rapid7 that can automatically detect new devices and evaluate vulnerabilities.

This Tool Generally Check for Hardware Vulnerability and Operating system Bugs or Outdated software's, drivers about the device.

I check this Organization Everything will be fine and not detect any hardware vulnerability and change Router will be Change for Greater Hardware Support for Wireless Internet.

Conclusion:

In conclusion, penetration testing plays a crucial role in strengthening an organization's security posture. By simulating real-world attacks, pentesting helps identify vulnerabilities before malicious actors can exploit them, allowing for timely remediation. This proactive approach not only enhances the security of systems and data but also builds resilience against potential breaches.

Effective penetration testing involves a thorough assessment of an organization's IT infrastructure, applications, and network configurations. The insights gained from these tests provide valuable feedback for improving security policies, practices, and technologies. Regular pentesting, combined with continuous monitoring and updates, ensures that security measures evolve alongside emerging threats.

Ultimately, the benefits of penetration testing extend beyond merely addressing weaknesses; they foster a culture of security awareness and preparedness within the organization. By prioritizing and investing in pentesting, organizations can better safeguard their assets, protect sensitive information, and maintain trust with clients and stakeholders.

-----END-----