EXTION INFOTEC PROJECT 2

WEBSITE VULNERABILITY ASSESSMENTS

MYCHARLA MADHAVKUMAR

27/08/2024

**Table of Contents**

# Introduction

* + Purpose of the Website Vulnerability Assessment
  + Overview of the Project Objectives

# Preparation Phase

* + Defining Scope and Objectives
  + Obtaining Permissions and Authorizations
  + Setting Up Scanning Tools

# Vulnerability Scanning

* + Conducting External Network Scans

# Risk Assessment

* + Using CVSS for Vulnerability Scoring
  + Prioritizing Risks Based on Severity

# Mitigation Strategy

* + Developing Mitigation Recommendations
  + Implementing Security Patches and Updates

# Documentation and Reporting

* + Generating Detailed Vulnerability Reports
  + Creating Executive Summaries for Stakeholders

# Implementation and Verification

* + Applying Recommended Changes
  + Verifying Effectiveness of Mitigations

# Conclusion

* + Summary of Key Findings and Actions
  + Importance of Regular Vulnerability Assessments

**Project Overview:**

The project aims to conduct a comprehensive assessment of the infrastructure of [**RIVAN SMART**] to identify and mitigate potential vulnerabilities. The assessment will external Website 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. **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, The harvest).
   * Analyze scan results to identify vulnerabilities.
3. **Risk Assessment:**
   * Prioritize identified vulnerabilities based on severity.
   * 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, Penetration Tools
* **Information Gathering:** Google Dorks, Metadata, Reverse image.
* **Documentation Tools:** Microsoft Office Suite, reporting templates.
* **Communication Tools:** Email, Mobiles, WhatsApp.

**Personally Used Tools in this Project:**

### 1. **Censys Web Scanner**

* A search engine that scans and indexes internet-connected devices, helping cybersecurity professionals identify vulnerabilities and monitor networks.

### 2. **The Harvester**

* An OSINT tool used to gather emails, subdomains, and IPs from various public sources during the reconnaissance phase of penetration testing.

### 3. **Pen Tools**

* A collective term for tools used in penetration testing to assess the security of systems by simulating attacks and finding vulnerabilities.

### 4. **Napalm FTP Server**

* A lightweight FTP server often used in penetration testing labs for serving files or interacting with FTP clients in a controlled environment.

### 5. **Meta Data**

* Data that provides information about other data, often extracted from files to gather additional intelligence during penetration testing or forensic analysis.

### 6. **Tor Browser**

* A browser that enables anonymous internet browsing by routing traffic through the Tor network, helping users protect their privacy and evade tracking.

### 7. **Parrot & Kali Linux Operating Systems**

* Security-focused Linux distributions preloaded with tools for penetration testing, digital forensics, and security research.

### 8. **Windows 2019 Server**

* A server operating system by Microsoft used for managing enterprise applications, services, and networks, often tested in security assessments.

### 9. **WordPress Scanner**

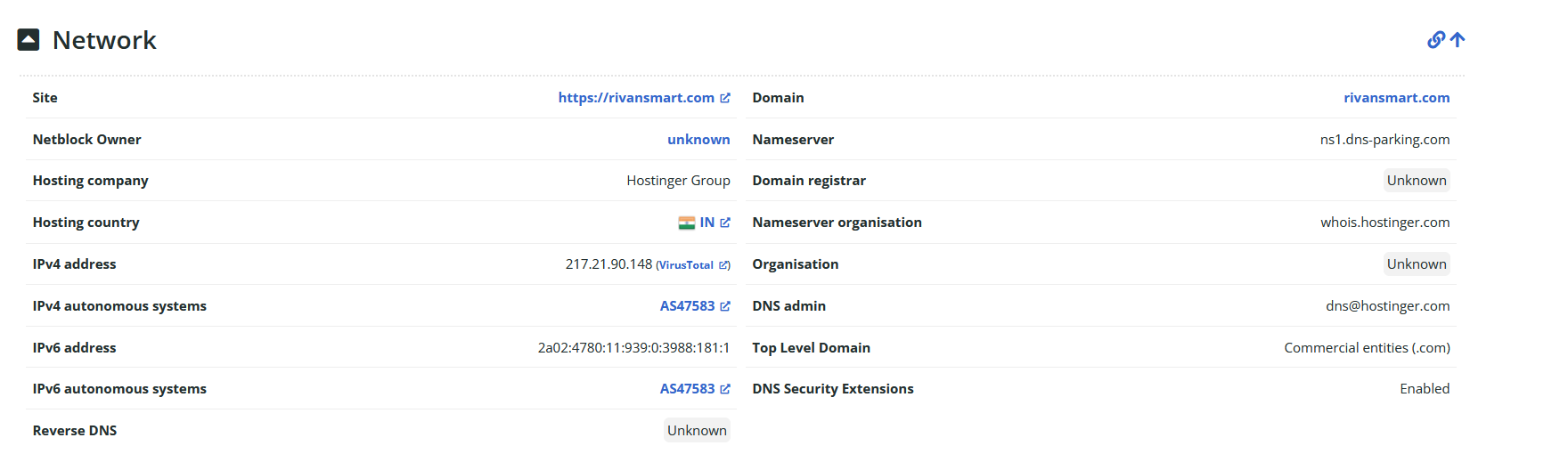
* A tool that scans WordPress websites for vulnerabilities, outdated plugins, and security weaknesses to help protect against potential attacks.

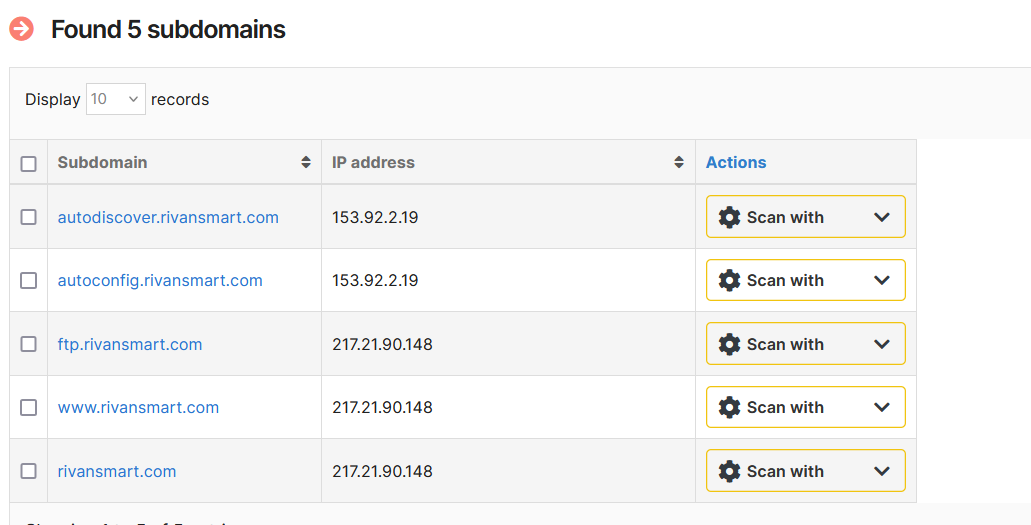
# Purpose of the Network Vulnerability Assessment:

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

Target Network: Rivan Smart Pvt Limited

Website URL: https://rivansmart.com/



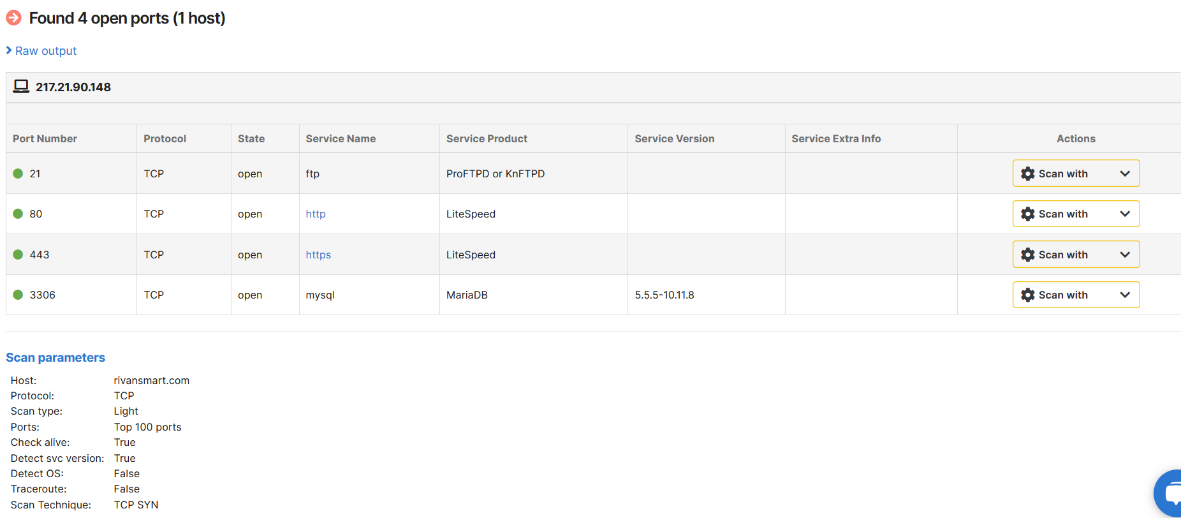


**USAGE OF THE TOOLS IN THIS PROJECT**

1. **(Port Scanner):-**

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

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



1. **The Harvester (Email info about Websites):-**

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.



1. **Google Dorks (Some Info Leaked in Web):-**

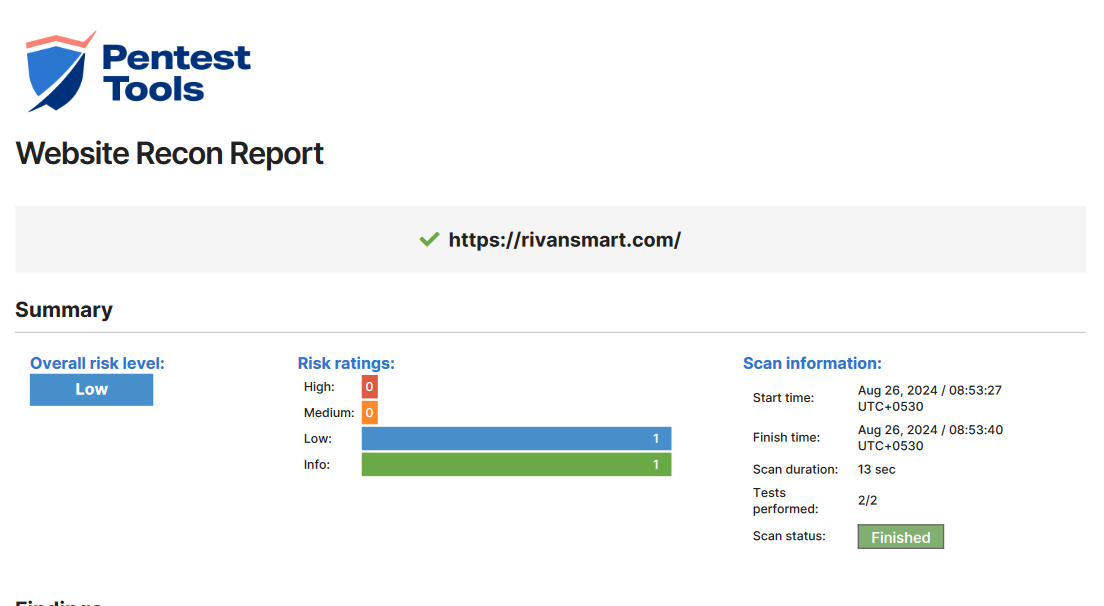
Google Dorks is mainly used for deep report about Website, which is Dns address, Document snapshots, domains, any data is leaked in web like PDFs, Sub Domains, Email ids, Phone Numbers …etc.

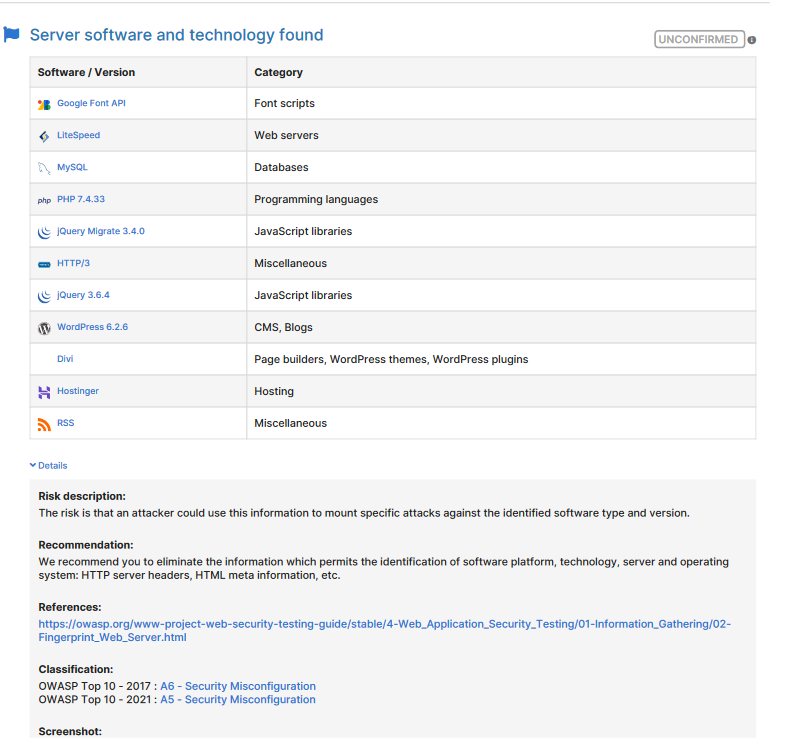
**Leaked Pdfs:**

****

****

1. **Scanning Reports:**

****

** .**

**Web scanning Reports:**

* <https://drive.google.com/file/d/1a0XLz1sqfPabvT5TXXU1oEK0kqKm6paj/view?usp=sharing>
* <https://drive.google.com/file/d/1AfflFMUpEhfsEL9cuthvrzwYnuvilHfJ/view?usp=sharing>
* <https://drive.google.com/file/d/1qTHbnQWBxrjJ-mdezoR2rk2e7IJ55GPw/view?usp=sharing>
* <https://drive.google.com/file/d/1kKRH22gOR1oTmN2rs4jvXOq9WZrQFSRr/view?usp=sharing>
* <https://drive.google.com/file/d/1QzMecChP3MmijHc4wVUgsTz87jR1D-LB/view?usp=sharing>

**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