PENETRATION TEST REPORT

Generated by KaliPenter

vardhaman.org
23/11/2025, 11:27 PM

---

1. Executive Summary

A penetration test was conducted to identify security deficiencies. A passive reconnaissance scan of vardhaman.org revealed 33 unique subdomains. The scan did not resolve any hosts or identify any live services. Several subdomains present potential security concerns, including those related to login portals, webmail, cPanel access, and potentially outdated applications. Further investigation is required to confirm the existence and severity of these vulnerabilities. The active reconnaissance scan of vardhaman.org reveals several potential security concerns. The Nmap scan identifies multiple open ports, including FTP (21), PPTP (1723), and HTTP/HTTPS proxies (8080/8443), which could be exploited if not properly secured. The DNS reconnaissance indicates the domain uses Cloudflare and Microsoft Outlook for email, and provides version information for the DNS servers. The WhatWeb scan failed to execute properly. Further investigation is needed to assess the actual risk associated with these findings.

2. Scan Overview

Scan ID	Duration
scan-21	14m 32s
Total Findings	**Phases Completed**
11	2

3. Critical Findings

Exposed cPanel Subdomain

MEDIUM

The subdomain 'cpanel.vardhaman.org' is exposed. If accessible, this could allow unauthorized access to server management functionalities, potentially leading to complete compromise of the server.

Tool: Passive Recon

Webmail Access Point

MEDIUM

The subdomain 'webmail.vardhaman.org' and 'mail.vardhaman.org' are exposed. If vulnerable, this could allow unauthorized access to email accounts, potentially leading to data breaches and phishing attacks.

Tool: Passive Recon

Login Portal Exposure

MEDIUM

The subdomain 'login.vardhaman.org' is exposed. This could be a target for credential stuffing and brute-force attacks if not properly secured.

Tool: Passive Recon

Potential Outdated Application (rice2016.vardhaman.org)

LOW

The subdomain 'rice2016.vardhaman.org' suggests a potentially outdated application or website. Outdated applications are often vulnerable to known security exploits.

Tool: Passive Recon

Exposed Webdisk

LOW

The subdomain 'webdisk.vardhaman.org' is exposed. If accessible without proper authentication, this could lead to unauthorized file access and data leakage.

Tool: Passive Recon

Localhost Subdomain

INFO

The subdomain 'localhost.vardhaman.org' is likely a misconfiguration or internal development subdomain that should not be publicly accessible.

Tool: Passive Recon

Open FTP Port (21)

MEDIUM

The FTP port is open, which could allow anonymous or unauthorized access to the server's file system if not properly configured. FTP transmits data in cleartext, making it vulnerable to eavesdropping.

Tool: Active Recon

Open PPTP Port (1723)

HIGH

The PPTP port is open. PPTP is an outdated and insecure VPN protocol with known vulnerabilities. It is susceptible to various attacks, including man-in-the-middle attacks and password cracking.

`Tool: Active Recon`

Open HTTP/HTTPS Proxy Ports (8080/8443)

MEDIUM

HTTP/HTTPS proxy ports are open. If these proxies are misconfigured or unauthenticated, they could be abused for malicious purposes, such as bypassing security controls, conducting denial-of-service attacks, or accessing internal resources.

`Tool: Active Recon`

DNS Server Version Disclosure

INFO

The DNS reconnaissance revealed the version of the BIND DNS servers being used. While not a direct vulnerability, this information can be used by attackers to identify known vulnerabilities in specific versions of BIND.

`Tool: Active Recon`

WhatWeb Scan Failure

LOW

The WhatWeb scan failed to execute due to a missing dependency. This prevents the identification of technologies used on the target, potentially missing vulnerabilities.

`Tool: Active Recon`

4. Mitigation Strategies

1. Exposed cPanel Subdomain:

Restrict access to the cPanel interface to authorized IP addresses only. Implement strong authentication mechanisms, including multi-factor authentication. Ensure cPanel is running the latest stable version with all security patches applied.

2. Webmail Access Point:

Ensure the webmail application is running the latest stable version with all security patches applied. Implement strong authentication mechanisms, including multi-factor authentication. Regularly audit email accounts for suspicious activity.

3. Login Portal Exposure:

Implement strong password policies and account lockout mechanisms. Enable multi-factor authentication. Monitor login attempts for suspicious activity. Ensure the login portal is protected against common web application vulnerabilities such as SQL injection and cross-site scripting (XSS).

4. Potential Outdated Application (rice2016.vardhaman.org):

Investigate the purpose of the 'rice2016.vardhaman.org' subdomain. If the application is no longer needed, remove it. If it is still required, update it to the latest version and apply all security patches. Conduct a vulnerability assessment to identify any potential security flaws.

5. Exposed Webdisk:

Ensure the webdisk application is running the latest stable version with all security patches applied. Implement strong authentication mechanisms. Regularly audit file access logs for suspicious activity.

6. Localhost Subdomain:

Remove the 'localhost.vardhaman.org' subdomain from public DNS records. Investigate the purpose of this subdomain and ensure it is not exposing any sensitive information.

7. Open FTP Port (21):

Disable FTP if not required. If FTP is necessary, configure it to require strong authentication, use TLS (FTPS), and restrict access to specific users and directories. Consider using SFTP instead.

8. Open PPTP Port (1723):

Disable PPTP and migrate to a more secure VPN protocol such as OpenVPN, IPsec, or WireGuard.

9. Open HTTP/HTTPS Proxy Ports (8080/8443):

Ensure that the proxies are properly configured with strong authentication and access controls. Regularly monitor proxy logs for suspicious activity. If the proxies are not required, disable them.

10. DNS Server Version Disclosure:

Keep the BIND DNS servers up to date with the latest security patches. Consider hiding the version information in the DNS server configuration.

11. WhatWeb Scan Failure:

Investigate and resolve the WhatWeb error by installing the missing dependency (/usr/bin/lib/messages). Re-run the scan after fixing the issue.