PENETRATION TEST REPORT

Generated by KaliPenter

vardhaman.org
22/11/2025, 04:37 PM

---

1. Executive Summary

A penetration test was conducted to identify security deficiencies. The passive reconnaissance scan of vardhaman.org reveals several areas of potential concern. The WHOIS record shows the domain is using Cloudflare for DNS, which provides some inherent protection. TheHarvester scan was hampered by missing API keys, limiting its effectiveness, but it did find a substantial number of subdomains. The subfinder tool confirmed many of these subdomains. Amass timed out. Several subdomains appear to be related to control panels (cpanel, cpcalendars, cpcontacts), which, if not properly secured, could present a significant attack surface. Several exceptions and errors occurred during the Harvester scan, pointing to possible misconfiguration or service availability issues. The active reconnaissance scan reveals several open ports on vardhaman.org that could present potential security vulnerabilities. Specifically, the presence of FTP (port 21), PPTP (port 1723), RTSP (port 554), and HTTP/HTTPS on alternate ports (8080, 8443) requires further investigation. DNSRecon and WhatWeb provided no output, suggesting either the services are protected or the tools failed to gather information. The open ports mentioned should be checked for service versions and known vulnerabilities. The 'filtered' ports could indicate the presence of a firewall or other network security device, so they are not a concern in terms of open port vulnerabilities.

2. Scan Overview

Scan ID	**Duration**
scan-11	14m 32s
Total Findings	**Phases Completed**
13	2

3. Critical Findings

Exposed cPanel Subdomains

HIGH

The discovery of subdomains like cpanel.vardhaman.org, cpcalendars.vardhaman.org, cpcontacts.vardhaman.org, and webmail.vardhaman.org is a serious concern. These are commonly targeted by attackers to gain unauthorized access to server management interfaces, potentially leading to full server compromise. Presence of `webmaila.vardhaman.org` also warrants further investigation.

`Tool: Unknown Tool`

Multiple IPs and Services Pointing to Cloudflare

INFO

Many subdomains resolve to Cloudflare IPs. While Cloudflare provides DDoS protection and CDN services, misconfiguration can expose origin servers. The multiple IPv4 and IPv6 addresses associated with several subdomains should be further investigated. Also the presence of `go.domains.live.com` and `md2-westus.cloudapp.net` might indicate services running on external cloud infrastructure.

`Tool: Unknown Tool`

TheHarvester Missing API Keys

LOW

TheHarvester scan was significantly limited due to numerous missing API keys. This restricts the tool's ability to gather comprehensive information. Several scan engines failed due to the missing API keys.

`Tool: Unknown Tool`

TheHarvester Exceptions and Errors

MEDIUM

TheHarvester encountered several exceptions and errors during its scan, including file not found errors and API request failures. This indicates potential problems with the tool's configuration, dependencies, or the availability of external services.

`Tool: Unknown Tool`

Subdomain Enumeration Reveals Internal Structure

MEDIUM

The enumeration of subdomains reveals potentially sensitive information about the organization's internal structure, including departments (cse, ece, csd), learning platforms (nptel, onlineexam), and other services. This information can be used by attackers to tailor their attacks and increase the likelihood of success.

`Tool: Unknown Tool`

`localhost.vardhaman.org` Points to Loopback Address

INFO

The subdomain `localhost.vardhaman.org` is resolving to `127.0.0.1`. This entry in the DNS configuration is highly unusual and very likely a misconfiguration. Attackers might abuse this situation.

Tool: Unknown Tool

WHOIS Data Shows Domain Lock Enabled

INFO

The WHOIS data indicates that the domain has 'clientTransferProhibited' status. This is a positive security measure, preventing unauthorized domain transfers.

Tool: Unknown Tool

Amass scan timeout

LOW

Amass scan timed out, indicating a possible infrastructure or network issue

Tool: Unknown Tool

Unencrypted FTP Service

HIGH

The FTP service (port 21) is open. If not properly configured with TLS (FTPS) or SFTP, data transmitted over FTP is unencrypted and susceptible to eavesdropping. Credentials transmitted in the clear can be intercepted and reused.

Tool: Unknown Tool

PPTP VPN Service

CRITICAL

The PPTP (Point-to-Point Tunneling Protocol) VPN service (port 1723) is open. PPTP is a deprecated VPN protocol with known and widely exploited security vulnerabilities. Its encryption is weak and easily crackable, making it highly susceptible to man-in-the-middle attacks and data breaches.

Tool: Unknown Tool

Real Time Streaming Protocol Vulnerability

MEDIUM

The RTSP service (port 554) is open. This could be for video streaming, surveillance systems, or other media-related services. RTSP itself may have vulnerabilities that allow unauthorized access, denial of service, or even remote code execution, especially in older implementations or those with default credentials.

Tool: Unknown Tool

HTTP Proxy on Non-Standard Port

MEDIUM

HTTP service is running on port 8080 which is commonly used for proxy servers. Misconfigured or insecure proxies can be exploited to bypass security controls, launch internal attacks, or exfiltrate data. It is important to verify the purpose of this port and implement appropriate security measures.

`Tool: Unknown Tool`

HTTPS on Non-Standard Port

MEDIUM

HTTPS service is running on port 8443. While using HTTPS is generally secure, operating it on a non-standard port can be a sign of misconfiguration or an attempt to obscure the service. Ensure the SSL/TLS configuration is valid and up-to-date (ciphers, protocols). In some situations, clients or firewalls might not correctly handle HTTPS on non-standard ports.

`Tool: Unknown Tool`

4. Mitigation Strategies

1. Exposed cPanel Subdomains:

No mitigation provided.

2. Multiple IPs and Services Pointing to Cloudflare:

No mitigation provided.

3. TheHarvester Missing API Keys:

No mitigation provided.

4. TheHarvester Exceptions and Errors:

No mitigation provided.

5. Subdomain Enumeration Reveals Internal Structure:

No mitigation provided.

6. `localhost.vardhaman.org` Points to Loopback Address:

No mitigation provided.

7. WHOIS Data Shows Domain Lock Enabled:

No mitigation provided.

8. Amass scan timeout:

No mitigation provided.

9. Unencrypted FTP Service:

No mitigation provided.

10. PPTP VPN Service:

No mitigation provided.

11. Real Time Streaming Protocol Vulnerability:

No mitigation provided.

12. HTTP Proxy on Non-Standard Port:

No mitigation provided.

13. HTTPS on Non-Standard Port:

No mitigation provided.