Penetration Test Report

Target: vardhaman.org

Scan ID	10
Date	2025-11-22 16:15
Status	Completed
Confidentiality	CONFIDENTIAL

Executive Summary

Passive Recon Phase: The passive reconnaissance scan of vardhaman.org revealed potential infrastructure and application security weaknesses. While theHarvester failed to fully execute due to missing API keys, WHOIS data and subdomain enumeration provided useful information. The primary concerns are related to exposed control panel interfaces (cPanel, webmail, webdisk), potential subdomain takeover candidates, reliance on a single registrar, and the use of Cloudflare's nameservers (implying potential for misconfiguration or bypass). Further investigation is needed to confirm the severity and exploitability of these findings.

Active Recon Phase: The active reconnaissance scan of vardhaman.org reveals several open ports that potentially expose the system to security risks. Specifically, open ports for FTP, PPTP, and RTSP are concerning due to known vulnerabilities. Further investigation is required to determine the specific services running and their configurations to fully assess the risk and implement appropriate mitigation strategies. The HTTP/HTTPS ports should be further examined for web application vulnerabilities. The lack of WhatWeb and DNSRecon data hinders a more thorough assessment.

Detailed Findings

Findings from Passive Recon

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Findings from Active Recon

Name	FTP (Port 21) - Potential Unauthenticated Access/Data Exposure
Severity	Medium
Description	The FTP service is running on port 21. If configured with anonymous access or weak credentials
Mitigation	No mitigation provided

Name	PPTP (Port 1723) - Inherent Security Weaknesses
Severity	High
Description	PPTP (Point-to-Point Tunneling Protocol) is an outdated VPN protocol with known and well-docu
Mitigation	No mitigation provided

Name	RTSP (Port 554) - Potential Media Server Vulnerabilities
Severity	Medium
Description	RTSP (Real Time Streaming Protocol) is used for streaming media. Vulnerabilities in the RTSP s
Mitigation	No mitigation provided

Name	HTTP/HTTPS (Ports 80/443) - Web Application Vulnerabilities
Severity	High
Description	Open HTTP (port 80) and HTTPS (port 443) ports indicate a web server is running. This implies
Mitigation	No mitigation provided

Name	HTTP-Proxy (Port 8080) - Potential Proxy Misconfiguration/Abuse
Severity	Medium
Description	The open HTTP-Proxy port (8080) suggests the presence of a proxy server. A misconfigured or
Mitigation	No mitigation provided

Appendix: Technical Data

The following section contains raw output from the scanning tools.

Raw Output: Passive Recon

{"whois": "Domain Name: vardhaman.org\nRegistry Domain ID: REDACTED\nRegistrar WHOIS Server: http://whois.publicdomainregistry.com\nRegistrar URL: http://www.publicdomainregistry.com\nUpdated Date: 2025-01-30T12:46:14Z\nCreation Date: 2008-04-24T13:24:44Z\nRegistry Expiry Date: 2034-04-24T13:24:44Z\nRegistrar: PDR Ltd. d/b/a PublicDomainRegistry.com\nRegistrar IANA ID: 303\nRegistrar Abuse Contact Email: abuse@publicdomainregistry.com\nRegistrar Abuse Contact Phone: +1.2013775952\nDomain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited\nName Server: owen.ns.cloudflare.com\nName Server: riya.ns.cloudflare.com\nDNSSEC: unsigned\nURL of the ICANN Whois Inaccuracy Complaint Form: https://icann.org/wicf/\n>>> Last update of WHOIS database: 2025-11-22T10:38:13Z <<<\n\nFor more information on Whois status codes, please visit https://icann.org/epp\n\nTerms of Use: Access to Public Interest Registry WHOIS information is provided to assist persons in determining the contents of a domain name registration record in the Public Interest Registry registry database. The data in this record is provided by Public Interest Registry for informational purposes only, and Public Interest Registry does not guarantee its accuracy. This service is intended only for query-based access. You agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator, a Registrar, or Identity Digital except as reasonably necessary to register domain names or modify existing registrations. All rights reserved. Public Interest Registry reserves the right to modify these terms at any time.
... [Output Truncated]

Raw Output: Active Recon

{"nmap_fast": "Starting Nmap 7.95 (https://nmap.org) at 2025-11-22 05:45 EST\nNmap scan report for vardhaman.org (172.67.157.215)\nHost is up (0.27s latency).\nOther addresses for vardhaman.org (not scanned): 2606:4700:3032::ac43:9dd7 2606:4700:3037::6815:8cb 104.21.8.203\nNot shown: 94 filtered tcp ports (no-response)\nPORT STATE SERVICE\n21/tcp open ftp\n80/tcp open http\n443/tcp open https\n554/tcp open rtsp\n1723/tcp open pptp\n8080/tcp open http-proxy\n\nNmap done: 1 IP address (1 host up) scanned in 7.64 seconds", "whatweb": "", "dnsrecon": ""}