

PENETRATION TEST REPORT

Generated by KaliPenter

sophie.sarral.io
22/11/2025, 10:40 PM

1. Executive Summary

A penetration test was conducted to identify security deficiencies. The passive reconnaissance scan against sophie.sarral.io revealed several issues primarily related to the configuration of theHarvester tool. Numerous API keys are missing, which significantly limits the tool's ability to gather comprehensive information. The WHOIS request failed initially, but the tool did not retry the request later. Furthermore, theHarvester encountered multiple errors while searching various online services, indicating potential rate limiting or API issues. No direct vulnerabilities against the target domain were identified, only issues in the scanner setup. The other tools (subfinder, amass) returned no results. Overall, the scan was largely unsuccessful due to configuration problems with the tools used. The active reconnaissance scan of sophie.sarral.io (20.124.91.118) reveals several potentially vulnerable services. Open ports include FTP (21), SSH (22), HTTP (80), RTSP (554), PPTP (1723), and MySQL (3306). The absence of WhatWeb output limits technology fingerprinting. DNSRecon also returned no data which might suggest DNS information is either not exposed or is being effectively protected. The presence of PPTP and MySQL, along with FTP could pose significant risks.

2. Scan Overview

Scan ID	Duration
scan-15	14m 32s
Total Findings	Phases Completed
14	2

3. Critical Findings

Missing API Keys for theHarvester	MEDIUM
-----------------------------------	--------

TheHarvester is missing API keys for numerous data sources, including Bevigil, Bufferoverrun, Censys, CriminalIP, Dehashed, DNSDumpster, FullHunt, Github, Hunter, Hunterhow, Intelx, Netlas, Onyph, PentestTools, ProjectDiscovery, RocketReach, Securitytrail, Shodan, Tomba, Venacus, VirusTotal, WhoisXML, and Zoomeye. This prevents the tool from effectively gathering information from these sources.

Tool: Passive Recon

WHOIS Request Failure

LOW

The initial WHOIS request returned 'Malformed request.' This may indicate issues with the WHOIS server or the tool's request format. A successful WHOIS query can provide valuable information about the domain's registration details.

Tool: Passive Recon

BuiltWith API Error

LOW

The BuiltWith search resulted in an error indicating an unexpected mimetype ('text/json; charset=utf-8') being returned. This might indicate an issue with the BuiltWith API or incorrect handling of the response by theHarvester, potentially because no API key was set.

Tool: Passive Recon

HavelBeenPwned API Error

LOW

The HavelBeenPwned search returned an error, 'Cannot serialize non-str key None'. This error suggests a problem in how the search query is being constructed with Null values.

Tool: Passive Recon

SecurityScorecard API Error

LOW

The SecurityScorecard search failed because of missing API keys and 'SearchSecurityScorecard' object has no attribute 'get_ips'. This could be a code problem that needs more deep investigation and maybe a code update.

Tool: Passive Recon

Sitedossier CAPTCHA

INFO

Sitedossier module triggered a CAPTCHA indicating rate limiting. This prevents information gathering from this source.

Tool: Passive Recon

Threatminer API Error

LOW

Subdomaincenter search resulted in an error 500 with an unexpected mimetype ('text/html; charset=utf-8'), suggesting an API issue or incorrect response handling.

Tool: Passive Recon

Urlscan.io API Rate Limit

INFO

The subdomainfinder99 tool hit a rate limit (error 429) on the urlscan.io API. This prevents information gathering from this source.

Tool: Passive Recon

Missing API Endpoint Wordlist

INFO

TheHarvester is unable to locate API endpoint wordlist '/usr/lib/python3/dist-packages/theHarvester/data/wordlists/api_endpoints.txt'. This could result in fewer endpoints being scanned.

Tool: Passive Recon

Unencrypted FTP Service

HIGH

The FTP service (port 21) is running unencrypted. This allows for sensitive information like usernames, passwords, and transmitted data to be intercepted in transit.

Tool: Active Recon

PPTP VPN Service

CRITICAL

The PPTP (Point-to-Point Tunneling Protocol) VPN service (port 1723) is known to have significant security vulnerabilities and is considered obsolete. It's susceptible to various attacks, including man-in-the-middle attacks and cryptographic weaknesses.

Tool: Active Recon

Exposed MySQL Service

MEDIUM

The MySQL database service (port 3306) is open and accessible. Without proper access controls, authentication, and security hardening, it could be vulnerable to unauthorized access, data breaches, and SQL injection attacks.

Tool: Active Recon

Unencrypted HTTP Service

LOW

The HTTP service (port 80) is running unencrypted. All communication is sent in plain text, so user data may be exposed.

Tool: Active Recon

RTSP service exposed

MEDIUM

The RTSP service (port 554) is exposed, which commonly deals with media streaming. This may indicate open and easily accessible camera systems or media servers, and its security depends on its specific implementation. Vulnerabilities in the RTSP service itself or the underlying media server could be exploited.

Tool: Active Recon

4. Mitigation Strategies

1. Missing API Keys for theHarvester:

Populate the `/etc/theHarvester/api-keys.yaml` file with the correct API keys for each data source.

2. WHOIS Request Failure:

Investigate the reason for the malformed request. Retry the WHOIS query using a different tool or manually. Ensure correct formatting of the WHOIS query.

3. BuiltWith API Error:

Provide BuiltWith API key (if available), verify that theHarvester is correctly parsing the BuiltWith API response. Check the BuiltWith API status for any ongoing issues.

4. HavelBeenPwned API Error:

Debug the HavelBeenPwned module of theHarvester to identify where the null value is originating from and fix the module's parameter validation.

5. SecurityScorecard API Error:

Provide valid SecurityScorecard API key and debug the tool to find the source of this error. Potentially report an issue/bug report to the tool owner.

6. Sitedossier CAPTCHA:

Change the IP address used for scanning, manually solve the CAPTCHA, or wait before rerunning the Sitedossier module. Consider implementing a proxy list for theHarvester.

7. Threatminer API Error:

Verify that theHarvester is correctly parsing the Threatminer API response. Check the Threatminer API status for any ongoing issues.

8. Urlscan.io API Rate Limit:

Implement proper rate limiting in theHarvester or use a proxy to distribute requests and avoid hitting the rate limit. Obtain a urlscan.io API key (if available) to increase the rate limit.

9. Missing API Endpoint Wordlist:

Ensure the existence of this wordlist on the filesystem or manually create if missing. If this is a new installation of theHarvester consider reinstalling the tool to ensure no other crucial files are missing.

10. Unencrypted FTP Service:

Disable the FTP service if it is not required. If FTP is necessary, switch to a secure alternative like SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure) which encrypts the data stream. Enforce strong password policies.

11. PPTP VPN Service:

Immediately disable the PPTP service. Migrate to a more secure VPN protocol such as OpenVPN, WireGuard, or IPsec. Ensure any new VPN implementation includes multi-factor authentication.

12. Exposed MySQL Service:

Restrict access to the MySQL service to only authorized IP addresses. Implement strong authentication, including strong passwords and consider using multi-factor authentication. Regularly apply security patches and updates to the MySQL server. Consider using a firewall to protect the database server.

13. Unencrypted HTTP Service:

Redirect all traffic to HTTPS. Implement HSTS (HTTP Strict Transport Security) to prevent browsers from connecting to the site over HTTP.

14. RTSP service exposed:

Assess if the RTSP service is necessary. If it is, ensure it's properly secured with authentication and access controls. Check for known vulnerabilities in the specific RTSP implementation and the media server being used, and apply any available patches or updates. Consider placing the RTSP service behind a firewall and limiting access to authorized IP addresses only.