

PENETRATION TEST REPORT

Generated by KaliPenter

sophie.sarral.io
22/11/2025, 09:57 PM

1. Executive Summary

A penetration test was conducted to identify security deficiencies. The passive reconnaissance scan against sophie.sarral.io yielded limited usable results due to numerous API key errors in theHarvester and issues with other tools. The WHOIS query failed. theHarvester encountered several problems, including missing API keys for numerous services, decoding errors, captcha issues, and file not found errors. Consequently, it failed to identify any emails, IPs, or other information. Subfinder and Amass returned no output in this data. The overall effectiveness of this passive reconnaissance was severely hampered by these errors, leaving significant gaps in the information gathered. It's imperative to resolve the API key issues and investigate the tool errors to obtain a more complete and accurate picture of the target's attack surface. The active reconnaissance scan of sophie.sarral.io (20.124.91.118) reveals several open ports indicating potential vulnerabilities. Specifically, the presence of FTP (21), RTSP (554), PPTP (1723), and MySQL (3306) services warrants further investigation. The lack of HTTPS being open is also something of note. Further enumeration and vulnerability scanning should be conducted on these services to assess the associated risks and implement appropriate security measures.

2. Scan Overview

Scan ID	Duration
scan-12	14m 32s
Total Findings	Phases Completed
14	2

3. Critical Findings

WHOIS Query Failure

INFO

The WHOIS query returned 'Malformed request.'. This prevents gathering basic domain registration information, which can be helpful in identifying the registrant and related entities.

Tool: Unknown Tool

Missing API Keys in theHarvester

INFO

theHarvester is missing API keys for a large number of services (bevigil, bufferoverun, Censys, criminalip, Dehashed, DNSDumpster, fullhunt, Github, Hunter, hunterhow, Intelx, netlas, onyphe, PentestTools, ProjectDiscovery, RocketReach, Securitytrail, Shodan, Tomba, Venacus, virustotal, whoisxml, zoomeye). This significantly reduces the tool's ability to gather information from external sources.

Tool: Unknown Tool

BuiltWith API Error

INFO

theHarvester encountered an error when querying the BuiltWith API (200, message='Attempt to decode JSON with unexpected mimetype: text/json; charset=utf-8'). This prevents gathering information about the technologies used on the target website.

Tool: Unknown Tool

Bing Search Error

INFO

theHarvester encountered an error when querying Bing (400, message: Can not decode content-encoding: br). This prevents gathering information from Bing search results.

Tool: Unknown Tool

HavelBeenPwned Error

INFO

theHarvester encountered an error when querying HavelBeenPwned (Cannot serialize non-str key None). This prevents gathering information about potential data breaches associated with the domain.

Tool: Unknown Tool

Sitedossier Captcha

INFO

theHarvester's Sitedossier module triggered a captcha, preventing data collection. This indicates potential rate limiting or bot detection by Sitedossier.

Tool: Unknown Tool

ThreatMiner and URLScan.io API Errors

INFO

theHarvester encountered errors when querying ThreatMiner (500, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8') and URLScan.io (429, message='Attempt to decode JSON with unexpected mimetype: text/html'). The Threatminer error indicates a server error or incorrect response format, while the URLScan.io error suggests a rate limit being hit.

Tool: Unknown Tool

Missing API Endpoint Wordlist

LOW

theHarvester couldn't find the API endpoint wordlist (/usr/lib/python3/dist-packages/theHarvester/data/wordlists/api_endpoints.txt) which impacted the API endpoint scanning functionality. This limits the discovery of potential API endpoints.

Tool: Unknown Tool

SecurityScorecard API Error

INFO

theHarvester encountered errors when querying the SecurityScorecard API, likely due to a missing API key and an attribute error ('SearchSecurityScorecard' object has no attribute 'get_ips').

Tool: Unknown Tool

Unencrypted FTP Service

HIGH

The FTP service is running on port 21 without encryption. This allows for the transmission of usernames, passwords, and data in plaintext, making it vulnerable to eavesdropping and credential theft. Attackers can easily capture sensitive information using packet sniffers.

Tool: Unknown Tool

PPTP VPN Vulnerability

CRITICAL

The Point-to-Point Tunneling Protocol (PPTP) VPN service is running on port 1723. PPTP has known and well-documented security vulnerabilities, including vulnerabilities to MS-CHAPv1/v2 authentication which can be easily cracked and vulnerabilities to man-in-the-middle attacks. It's considered obsolete and insecure.

Tool: Unknown Tool

RTSP Service

MEDIUM

The Real-Time Streaming Protocol (RTSP) service is running on port 554. RTSP servers may have vulnerabilities that can be exploited to gain unauthorized access or cause denial-of-service conditions. Default configurations and outdated versions are common attack vectors.

Tool: Unknown Tool

Open MySQL Service

MEDIUM

The MySQL database service is running on port 3306. If not properly secured, it can be vulnerable to unauthorized access, data breaches, and SQL injection attacks. Weak passwords, default configurations, and publicly accessible interfaces are common issues. Without WhatWeb information, we cannot know whether there is a front-end to this server, so the severity should be kept at medium.

Tool: Unknown Tool

HTTP Service Enabled Without HTTPS

LOW

The web server is running on port 80 (HTTP) without a corresponding HTTPS service running. This means that any data transmitted between the client and the server, including sensitive information, is sent in plaintext and can be intercepted by attackers.

Tool: Unknown Tool

4. Mitigation Strategies

1. WHOIS Query Failure:

No mitigation provided.

2. Missing API Keys in theHarvester:

No mitigation provided.

3. BuiltWith API Error:

No mitigation provided.

4. Bing Search Error:

No mitigation provided.

5. HaveIBeenPwned Error:

No mitigation provided.

6. Sitedossier Captcha:

No mitigation provided.

7. ThreatMiner and URLScan.io API Errors:

No mitigation provided.

8. Missing API Endpoint Wordlist:

No mitigation provided.

9. SecurityScorecard API Error:

No mitigation provided.

10. Unencrypted FTP Service:

No mitigation provided.

11. PPTP VPN Vulnerability:

No mitigation provided.

12. RTSP Service:

No mitigation provided.

13. Open MySQL Service:

No mitigation provided.

14. HTTP Service Enabled Without HTTPS:

No mitigation provided.