PENETRATION TEST REPORT

Generated by KaliPenter

sophie.sarral.io
22/11/2025, 10:57 PM

---

1. Executive Summary

A penetration test was conducted to identify security deficiencies. The passive reconnaissance scan for sophie.sarral.io reveals a number of issues, primarily related to misconfiguration of the scanning tools. TheHarvester experienced numerous API key errors, significantly limiting its effectiveness. WHOIS queries also failed initially. While amass and subfinder completed, their output is empty, suggesting potential configuration issues or that no data was found. Overall, the results are inconclusive due to these tool setup problems, highlighting a need to correct API key configurations and troubleshoot the individual tools for proper functionality before performing further analysis. The active reconnaissance scan of sophie.sarral.io reveals several potential security vulnerabilities. Open FTP (port 21) and PPTP (port 1723) services are inherently insecure and should be disabled or replaced. The presence of an open MySQL database (port 3306) without appropriate security measures is also a major concern. The absence of WhatWeb and DNSRecon results limits the scope of findings but also reduces the number of false positives. The closed HTTPS port (443) is not necessarily a vulnerability but something to investigate as it could cause downgrade attacks. The open RTSP port might pose a security risk depending on its configuration.

2. Scan Overview

Scan ID	Duration
scan-16	14m 32s
Total Findings	**Phases Completed**
12	2

3. Critical Findings

WHOIS Query Failure LOW

The WHOIS query initially failed with a 'Malformed request' error. This could be due to throttling or an incorrect request format. While WHOIS data may not directly expose critical vulnerabilities, it can provide useful information about the target organization.

`Tool: Passive Recon`

Missing API Keys in theHarvester

MEDIUM

TheHarvester is missing API keys for numerous data sources including BeVigil, Bufferoverun, Censys, CriminalIP, Dehashed, DNSDumpster, FullHunt, Github, Hunter, HunterHow, Intelx, Netlas, Onyph, PentestTools, ProjectDiscovery, RocketReach, SecurityTrail, Shodan, Tomba, Venacus, Virustotal, and WhoisXML. This severely limits the tool's ability to gather information.

`Tool: Passive Recon`

BuiltWith API Error

LOW

The BuiltWith search failed with an error indicating an unexpected content type (text/json instead of expected JSON) and a KEY value of 'None'. This suggests the API key for BuiltWith is either missing or incorrectly configured.

`Tool: Passive Recon`

SecurityScorecard API Error

LOW

The SecurityScorecard search failed due to a missing API key and an exception occurred. The exception suggests a potential issue with the tool's code when attempting to integrate SecurityScorecard.

`Tool: Passive Recon`

Threatminer API Error

LOW

The RapidDNS (Threatminer) search failed with a 500 error indicating an unexpected content type (text/html instead of expected JSON).

`Tool: Passive Recon`

Missing API Endpoints Wordlist

INFO

TheHarvester could not find the API endpoints wordlist. This limits the ability to discover potential API endpoints.

`Tool: Passive Recon`

HaveIBeenPwned API Error

INFO

The HaveIBeenPwned search failed with error: Cannot serialize non-str key None

`Tool: Passive Recon`

Insecure FTP Service

HIGH

The FTP service (port 21) is running without encryption, transmitting credentials and data in plaintext. This makes it vulnerable to eavesdropping and credential theft.

`Tool: Active Recon`

Insecure PPTP Service

CRITICAL

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

`Tool: Active Recon`

Open MySQL Database with potential default credentials

CRITICAL

The MySQL database service (port 3306) is exposed. Without proper authentication and access controls, this could allow unauthorized access to sensitive data. Default credentials may also be in use.

`Tool: Active Recon`

Open RTSP Service

MEDIUM

The RTSP (Real Time Streaming Protocol) service (port 554) is exposed. Vulnerabilities in the RTSP implementation could allow for remote code execution or denial-of-service attacks.

`Tool: Active Recon`

Closed HTTPS Port

MEDIUM

HTTPS (port 443) is closed. Clients may be subject to downgrade attacks, where the attacker forces the client to use unencrypted HTTP instead of HTTPS.

`Tool: Active Recon`

4. Mitigation Strategies

1. WHOIS Query Failure:

Verify the WHOIS query format and ensure the tool is not being throttled. Implement proper error handling to retry queries if needed.

2. Missing API Keys in theHarvester:

Obtain and configure the necessary API keys for each data source in TheHarvester's configuration file (api-keys.yaml). Ensure the keys are valid and properly formatted.

3. BuiltWith API Error:

Verify the BuiltWith API key is correctly configured and that the endpoint is responding with the expected JSON content type. If the key is configured, ensure the BuiltWith API itself is functioning correctly and returning the expected responses.

4. SecurityScorecard API Error:

Provide a valid API key for SecurityScorecard. Investigate the exception ('SearchSecurityScorecard' object has no attribute 'get_ips') in the tool's source code and fix the integration issue to ensure proper functionality with the SecurityScorecard API.

5. Threatminer API Error:

Verify if the Threatminer API endpoint is functioning correctly and returning the expected JSON response. Check for any updates or changes to the Threatminer API that might require adjustments in the tool's code.

6. Missing API Endpoints Wordlist:

Ensure the API endpoints wordlist is present in the specified directory. If it is missing, restore it from the tool's installation files or create a new one.

7. HaveIBeenPwned API Error:

This error suggests a potential bug in how the tool handles null or empty input for HaveIBeenPwned API. Inspect the tool's code and ensure a proper input format, or handle potential null values.

8. Insecure FTP Service:

Disable the FTP service. If file transfer is required, implement SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure), which provide encryption and authentication.

9. Insecure PPTP Service:

Disable the PPTP service immediately. Migrate to a more secure VPN protocol, such as OpenVPN, WireGuard, or IPsec, which offer stronger encryption and authentication mechanisms.

10. Open MySQL Database with potential default credentials:

Restrict access to the MySQL database server to only authorized IP addresses. Change the default root password and create strong, unique passwords for all database users. Consider using firewall rules to limit access to port 3306. Ensure proper authentication is in place. Regularly audit MySQL user

accounts and permissions.

11. Open RTSP Service:

Restrict access to the RTSP service to only authorized IP addresses. Ensure the RTSP server is running the latest version with all security patches applied. Consider disabling the service if it is not essential. Implement authentication and authorization mechanisms for RTSP streams.

12. Closed HTTPS Port:

Investigate why HTTPS is closed. If HTTPS is intended, ensure the service is running and accessible on port 443. Configure the web server to redirect all HTTP traffic to HTTPS (port 443). Implement HSTS (HTTP Strict Transport Security) to prevent downgrade attacks.