PENETRATION TEST REPORT

Generated by KaliPenter

sophie.sarral.io
23/11/2025, 10:17 PM

---

1. Executive Summary

A penetration test was conducted to identify security deficiencies. The passive reconnaissance scan of sarral.io revealed limited directly exploitable vulnerabilities. The WHOIS data shows domain privacy is enabled, obscuring registrant information. TheHarvester found no IPs, emails, people, or hosts associated with the target subdomain sophie.sarral.io. Amass encountered errors related to missing parser model files, indicating a potential configuration issue with the tool itself rather than a vulnerability in the target. Subfinder returned no results. Overall, the passive reconnaissance phase yielded minimal actionable intelligence, suggesting a relatively small attack surface or effective information security practices. The active reconnaissance scan of sophie.sarral.io reveals several potential vulnerabilities. Open FTP, SSH, HTTP, RTSP, and MySQL ports are identified, along with PPTP which is considered insecure. The WhatWeb scan failed, preventing technology fingerprinting. DNS reconnaissance only found an A record and no SRV records, and DNSSEC is not configured. The open ports present the most immediate risk, particularly FTP, PPTP and MySQL if not properly secured.

2. Scan Overview

Scan ID	Duration
scan-19	14m 32s
Total Findings	**Phases Completed**
12	2

3. Critical Findings

WHOIS Privacy Enabled

INFO

WHOIS privacy is enabled, which hides the registrant's contact information. While this protects the owner's privacy, it can hinder legitimate security research and incident response efforts.

Tool: Passive Recon

Amass Parser Model File Error

LOW

Amass reported errors indicating missing parser model files. This suggests a configuration issue with the Amass tool itself, potentially preventing it from fully discovering subdomains and other assets.

Tool: Passive Recon

DNSSEC Unsigned

INFO

The domain's DNS records are not signed with DNSSEC. This makes the domain potentially vulnerable to DNS spoofing and cache poisoning attacks.

Tool: Passive Recon

Open FTP Port (21)

MEDIUM

The FTP port is open, potentially allowing anonymous access or brute-force attacks to gain unauthorized access to the server's file system. FTP transmits credentials in plaintext.

Tool: Active Recon

Open SSH Port (22)

MEDIUM

The SSH port is open, which is standard for remote administration. However, it is a common target for brute-force attacks and vulnerability exploitation.

Tool: Active Recon

Open HTTP Port (80)

LOW

The HTTP port is open, indicating a web server is running. Without HTTPS redirection, sensitive data may be transmitted in plaintext.

Tool: Active Recon

Open RTSP Port (554)

MEDIUM

The RTSP port is open, suggesting a streaming media server is running. Vulnerabilities in the RTSP server could allow unauthorized access or denial-of-service attacks.

Tool: Active Recon

Open PPTP Port (1723)

HIGH

The PPTP port is open. PPTP is an outdated and insecure VPN protocol with known vulnerabilities. It should not be used.

Tool: Active Recon

Open MySQL Port (3306)

HIGH

The MySQL port is open, potentially allowing unauthorized access to the database if not properly secured. Direct access to the database server from the internet is generally discouraged.

Tool: Active Recon

Missing HTTPS (Port 443 Closed)

MEDIUM

Port 443 is closed, indicating HTTPS is not enabled. This means that sensitive data transmitted over HTTP is vulnerable to eavesdropping.

Tool: Active Recon

WhatWeb Scan Failure

LOW

The WhatWeb scan failed due to a missing library. This prevents the identification of technologies used on the target, hindering vulnerability assessment.

Tool: Active Recon

Missing DNSSEC

LOW

DNSSEC is not configured for the domain. This makes the domain vulnerable to DNS spoofing and cache poisoning attacks.

Tool: Active Recon

4. Mitigation Strategies

1. WHOIS Privacy Enabled:

No direct mitigation is needed from the target's perspective. However, consider the implications for transparency and potential legal requirements for disclosing contact information.

2. Amass Parser Model File Error:

Ensure Amass is correctly configured with all necessary dependencies and data files. Reinstall or update Amass and its dependencies if necessary. This is an issue with the scanning tool, not the target.

3. DNSSEC Unsigned:

Implement DNSSEC to digitally sign DNS records, ensuring their authenticity and integrity. This helps prevent attackers from manipulating DNS responses.

4. Open FTP Port (21):

Disable FTP if not required. If required, configure FTP to use explicit TLS/SSL (FTPS) and enforce strong authentication.

5. Open SSH Port (22):

Ensure SSH is configured with strong passwords or, preferably, key-based authentication. Consider using port knocking or limiting access to specific IP addresses. Keep SSH software updated.

6. Open HTTP Port (80):

Implement HTTPS and redirect all HTTP traffic to HTTPS. Ensure the web server is properly configured and patched against known vulnerabilities.

7. Open RTSP Port (554):

Disable RTSP if not required. If required, ensure the RTSP server is up-to-date with the latest security patches and properly configured with authentication.

8. Open PPTP Port (1723):

Disable PPTP and migrate to a more secure VPN protocol such as OpenVPN, IPSec, or WireGuard.

9. Open MySQL Port (3306):

Restrict access to the MySQL port to only authorized IP addresses or internal networks. Ensure strong authentication is used and the MySQL server is up-to-date with the latest security patches. Consider using a firewall to protect the database server.

10. Missing HTTPS (Port 443 Closed):

Enable HTTPS on the web server by installing an SSL/TLS certificate and configuring the server to listen on port 443. Redirect all HTTP traffic to HTTPS.

11. WhatWeb Scan Failure:

Investigate and resolve the WhatWeb error by installing the missing library or troubleshooting the tool's configuration. Re-run the scan after fixing the issue.

12. Missing DNSSEC:

Implement DNSSEC to digitally sign DNS records and ensure their authenticity.