PENETRATION TEST REPORT

Generated by KaliPenter

sophie.sarral.io
23/11/2025, 09:57 PM

---

1. Executive Summary

A penetration test was conducted to identify security deficiencies. The passive reconnaissance scan of sophie.sarral.io encountered issues with WHOIS, theHarvester, Subfinder, and Amass. WHOIS returned a malformed request, theHarvester reported an invalid source and lack of Google support, Subfinder returned no results, and Amass failed to load parser model files. The Amass output also shows a large number of progress bars, indicating a potentially lengthy or stalled process. These issues suggest problems with tool configuration, dependencies, or the target's information availability. Further investigation is needed to resolve these errors and obtain useful reconnaissance data. The active reconnaissance scan of sophie.sarral.io reveals several potential vulnerabilities. Open ports for FTP, SSH, HTTP, RTSP, PPTP, and MySQL services are exposed. The WhatWeb scan failed, preventing technology fingerprinting. DNS reconnaissance successfully resolved the A record but failed to find SRV records and encountered an error related to DNSSEC. The open ports and lack of HTTPS are the most concerning findings.

2. Scan Overview

Scan ID	Duration
scan-18	14m 32s
Total Findings	**Phases Completed**
13	2

3. Critical Findings

WHOIS Malformed Request LOW

The WHOIS query returned a 'Malformed request' error, indicating a problem with the query itself or the WHOIS server's ability to process it. This prevents gathering domain registration information.

`Tool: Passive Recon`

theHarvester Invalid Source and Google Engine Issue

LOW

theHarvester reported an 'Invalid source' error and indicates that the Google engine is not supported. This limits the tool's ability to discover email addresses, subdomains, and other information from various sources.

`Tool: Passive Recon`

Subfinder No Results

INFO

Subfinder returned no results, indicating that it was unable to find any subdomains for the target domain using its configured sources.

`Tool: Passive Recon`

Amass Parser Model File Not Found

MEDIUM

Amass failed to load the parser model file, preventing it from properly parsing and analyzing address information. This could impact the accuracy and completeness of its subdomain enumeration results.

`Tool: Passive Recon`

Amass Stalled Process

MEDIUM

The Amass output shows numerous progress bars that do not seem to be advancing, suggesting a potential stall or performance issue. This could prevent the tool from completing its subdomain enumeration process.

`Tool: Passive Recon`

Unencrypted FTP Service

HIGH

The FTP service (port 21) is open and likely unencrypted. This allows for the transmission of usernames, passwords, and data in cleartext, making it vulnerable to eavesdropping and credential theft.

`Tool: Active Recon`

Exposed SSH Service

MEDIUM

The SSH service (port 22) is open. While SSH is generally secure, it is a common target for brute-force attacks and vulnerability exploitation. Default configurations and weak passwords can lead to unauthorized access.

Tool: Active Recon

Unencrypted HTTP Service

HIGH

The HTTP service (port 80) is open, but HTTPS (port 443) is closed. This means that all communication with the web server is unencrypted, making it vulnerable to eavesdropping and man-in-the-middle attacks. Sensitive data, such as login credentials and personal information, can be intercepted.

Tool: Active Recon

Open RTSP Service

MEDIUM

The RTSP service (port 554) is open. RTSP is often used for streaming media and can be vulnerable to various attacks, including denial-of-service and buffer overflows. The specific risk depends on the RTSP server software and its configuration.

Tool: Active Recon

Open PPTP Service

CRITICAL

The PPTP service (port 1723) is open. PPTP is an outdated and insecure VPN protocol with known vulnerabilities. It is highly susceptible to eavesdropping and man-in-the-middle attacks.

Tool: Active Recon

Exposed MySQL Service

HIGH

The MySQL service (port 3306) is open. This allows potential attackers to attempt to connect to the database server. If the database server is not properly secured, it could lead to unauthorized access to sensitive data.

Tool: Active Recon

WhatWeb Scan Failure

LOW

The WhatWeb scan failed due to a missing dependency. This prevents the identification of technologies used on the target system, which could aid in identifying specific vulnerabilities.

Tool: Active Recon

Missing DNSSEC

INFO

The DNS reconnaissance reported that there was no answer for the DNSSEC query. DNSSEC helps prevent DNS spoofing and cache poisoning attacks.

```
Tool: Active Recon
```

4. Mitigation Strategies

1. WHOIS Malformed Request:

Verify the WHOIS query syntax and ensure the WHOIS server is functioning correctly. Try a different WHOIS server or tool. If the issue persists, the target domain may have WHOIS privacy enabled, or the WHOIS server may be experiencing temporary issues.

2. theHarvester Invalid Source and Google Engine Issue:

Review theHarvester's configuration file (proxies.yaml) and command-line arguments to ensure valid sources are specified. Investigate why the Google engine is not supported and consider alternative search engines or sources. Ensure the API keys are valid and properly configured.

3. Subfinder No Results:

Verify Subfinder's configuration and ensure it has access to valid API keys for its data sources. Consider using other subdomain enumeration tools to compare results. The target domain may have limited publicly available subdomain information.

4. Amass Parser Model File Not Found:

Ensure that the libpostal library and its associated data files are correctly installed and configured. Verify that the 'LIBPOSTAL_DATA_PATH' environment variable is set to the correct directory containing the parser model files. Reinstall libpostal if necessary.

5. Amass Stalled Process:

Monitor Amass's resource usage (CPU, memory, network) to identify any bottlenecks. Increase the tool's verbosity to get more detailed output and diagnose the issue. Consider running Amass with fewer threads or a smaller scope to improve performance. Check for network connectivity issues that may be preventing Amass from accessing its data sources.

6. Unencrypted FTP Service:

Disable the FTP service if not required. If required, enable and enforce FTPS (FTP over SSL/TLS) or SFTP (SSH File Transfer Protocol) to encrypt all communications.

7. Exposed SSH Service:

Ensure SSH is configured securely with strong passwords or key-based authentication. Implement rate limiting and intrusion detection/prevention systems to mitigate brute-force attacks. Keep SSH software

up to date with the latest security patches. Consider using port knocking or changing the default port to reduce attack surface.

8. Unencrypted HTTP Service:

Enable HTTPS by obtaining and installing an SSL/TLS certificate. Redirect all HTTP traffic to HTTPS to ensure all communication is encrypted. Enforce HSTS (HTTP Strict Transport Security) to prevent browsers from connecting over HTTP.

9. Open RTSP Service:

Disable the RTSP service if not required. If required, ensure the RTSP server software is up to date with the latest security patches. Implement access controls to restrict access to authorized users only. Consider using a firewall to limit access to the RTSP port.

10. Open PPTP Service:

Disable the PPTP service immediately. Migrate to a more secure VPN protocol, such as OpenVPN, IPSec, or WireGuard.

11. Exposed MySQL Service:

Ensure the MySQL service is not directly exposed to the internet. If remote access is required, use a VPN or SSH tunnel. Implement strong authentication and access controls. Keep MySQL software up to date with the latest security patches. Consider using a firewall to restrict access to the MySQL port.

12. WhatWeb Scan Failure:

Investigate and resolve the WhatWeb dependency issue. Ensure all necessary libraries and dependencies are installed correctly. Re-run the WhatWeb scan after resolving the issue.

13. Missing DNSSEC:

Implement DNSSEC to ensure the integrity and authenticity of DNS records.