PENETRATION TEST REPORT

Generated by KaliPenter

sophie.sarral.io
22/11/2025, 11:15 PM

1. Executive Summary

A penetration test was conducted to identify security deficiencies. The passive reconnaissance scan of sophie.sarral.io encountered issues with several tools. The WHOIS request failed, theHarvester reported an invalid source and Google engine not supported, and Amass failed to load a parser model file. Subfinder returned no results. The Amass output shows a large number of progress bars, suggesting it attempted many queries, but ultimately failed to parse the results due to the missing model file. These errors indicate potential misconfiguration or dependency issues with the tools themselves, rather than direct vulnerabilities in the target. Further investigation is needed to ensure the tools are correctly configured and functioning before relying on their output. 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 identification. DNS reconnaissance successfully resolved the A record but failed to find SRV records and encountered an error with DNSSEC. The open ports and lack of HTTPS are the most concerning findings.

2. Scan Overview

Scan ID	Duration
scan-17	14m 32s
Total Findings	**Phases Completed**
13	2

3. Critical Findings

WHOIS Request Failure INFO

The WHOIS request returned a 'Malformed request' error, preventing retrieval of domain registration information.

Tool: Passive Recon

theHarvester Invalid Source

INFO

theHarvester reported an 'Invalid source' error. This suggests a configuration issue or an attempt to use an unsupported data source.

Tool: Passive Recon

Amass Parser Model File Not Found

LOW

Amass failed to load the address parser model file, preventing it from properly parsing and analyzing discovered data. This likely indicates a missing dependency or misconfiguration.

Tool: Passive Recon

Subfinder No Results

INFO

Subfinder returned no results. This could indicate a lack of subdomains or an issue with the tool's configuration or data sources.

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's 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, indicating that the website is not enforcing HTTPS. This allows for man-in-the-middle attacks and eavesdropping on sensitive data transmitted over the network.

Tool: Active Recon

Exposed RTSP Service

MEDIUM

The RTSP service (port 554) is open. RTSP is often used for streaming media and can be vulnerable to buffer overflows and other security flaws if not properly secured and updated.

`Tool: Active Recon`

Exposed PPTP Service

CRITICAL

The PPTP service (port 1723) is open. PPTP is an outdated and insecure VPN protocol with known vulnerabilities. It should not be used.

`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 not properly secured, this could lead to data breaches and unauthorized access.

`Tool: Active Recon`

Missing HTTPS Service

MEDIUM

The HTTPS service (port 443) is closed. This means that secure communication is not available, and all traffic is sent in plaintext.

`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, limiting the ability to identify specific vulnerabilities.

`Tool: Active Recon`

DNSSEC Error

INFO

The DNS reconnaissance encountered an error when querying for DNSSEC records. This could indicate a misconfiguration or lack of DNSSEC implementation.

`Tool: Active Recon`

4. Mitigation Strategies

1. WHOIS Request Failure:

Verify the WHOIS server is accessible and the request format is correct. Check for rate limiting or temporary server issues. If the issue persists, consider using an alternative WHOIS service or tool.

2. theHarvester Invalid Source:

Review theHarvester's configuration file (proxies.yaml) and command-line arguments to ensure a valid source is specified. Consider using other supported search engines or data sources.

3. Amass Parser Model File Not Found:

Ensure that the libpostal library and its associated data files are correctly installed and configured. Verify that the AMASS_POSTAL_DATADIR environment variable (if used) points to the correct directory containing the parser model file. Reinstall Amass and its dependencies if necessary.

4. Subfinder No Results:

Verify Subfinder's configuration and data sources. Ensure that the target domain is correctly specified. Consider using other subdomain enumeration tools to compare results.

5. Unencrypted FTP Service:

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

6. 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 updated to patch known vulnerabilities.

7. Unencrypted HTTP Service:

Redirect all HTTP traffic to HTTPS. Obtain and install an SSL/TLS certificate and configure the web server to enforce HTTPS. Implement HSTS (HTTP Strict Transport Security) to prevent browsers from connecting over HTTP.

8. Exposed RTSP Service:

If RTSP is required, ensure it is properly secured with authentication and access controls. Keep the RTSP server software updated to patch known vulnerabilities. If not required, disable the service.

9. Exposed PPTP Service:

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

10. Exposed MySQL Service:

Restrict access to the MySQL service to only authorized IP addresses. Ensure strong authentication is used and that the database server is configured securely. Keep the MySQL server software updated to patch known vulnerabilities.

11. Missing HTTPS Service:

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

12. WhatWeb Scan Failure:

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

13. DNSSEC Error:

Investigate the DNS configuration and ensure that DNSSEC is properly configured if it is intended to be used. If not, this can be ignored.