PENETRATION TEST REPORT

Generated by KaliPenter

sophie.sarral.io
23/11/2025, 11:03 PM

1. Executive Summary

A penetration test was conducted to identify security deficiencies. The passive reconnaissance scan for sophie.sarral.io yielded no subdomains. Several tools (Findomain, Assetfinder, dnsx) were not installed, limiting the effectiveness of the scan. The absence of resolved hosts and live services further indicates a lack of discovered information. This could be due to a well-configured target or limitations in the scanning environment. The active reconnaissance scan of sophie.sarral.io reveals several potential vulnerabilities. Open FTP, SSH, HTTP, RTSP, PPTP, and MySQL ports are exposed. The WhatWeb scan failed due to a missing library. DNS reconnaissance was successful in identifying the A record but failed to find SRV records and encountered an error with DNSSEC. The open ports represent potential attack vectors, and the failed WhatWeb scan hinders technology identification.

2. Scan Overview

Scan ID	Duration
scan-20	14m 32s
Total Findings	**Phases Completed**
11	2

3. Critical Findings

Missing Reconnaissance Tools

LOW

Several key reconnaissance tools (Findomain, Assetfinder, dnsx) are not installed, significantly limiting the scope and effectiveness of the passive enumeration. This prevents the discovery of potential subdomains and associated vulnerabilities.

Tool: Passive Recon

Limited Subdomain Enumeration

INFO

The scan found no subdomains. This could indicate a small attack surface or effective subdomain hiding techniques. However, the lack of installed tools makes it difficult to draw definitive conclusions.

`Tool: Passive Recon`

Tool not installed - Resolved Hosts

INFO

The 'resolved_hosts' field indicates that the tool responsible for resolving hosts is not installed. This prevents the identification of IP addresses associated with the target domain and any discovered subdomains.

`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 system. FTP transmits data in cleartext, including credentials, making it vulnerable to eavesdropping.

`Tool: Active Recon`

Open SSH Port (22)

MEDIUM

The SSH port is open, which could be targeted by brute-force attacks or exploits targeting SSH vulnerabilities. While SSH is generally secure, misconfigurations or outdated versions can introduce risks.

`Tool: Active Recon`

Open HTTP Port (80)

LOW

The HTTP port is open, potentially allowing unencrypted communication. If sensitive data is transmitted over HTTP, it is vulnerable to interception.

`Tool: Active Recon`

Open RTSP Port (554)

MEDIUM

The RTSP (Real Time Streaming Protocol) port is open, potentially allowing unauthorized access to video streams or exploitation of RTSP vulnerabilities. This is especially concerning if the server is not properly secured.

`Tool: Active Recon`

Open PPTP Port (1723)

HIGH

The PPTP (Point-to-Point Tunneling Protocol) 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 the database is not properly secured, it could be vulnerable to SQL injection attacks or brute-force attacks on the MySQL user accounts.

`Tool: Active Recon`

WhatWeb Scan Failure

LOW

The WhatWeb scan failed due to a missing library, preventing the identification of technologies used on the target. This limits the ability to identify specific vulnerabilities associated with those technologies.

`Tool: Active Recon`

Missing DNSSEC

INFO

The DNS reconnaissance reported an error when querying for DNSSEC records. DNSSEC helps prevent DNS spoofing and cache poisoning attacks.

`Tool: Active Recon`

4. Mitigation Strategies

1. Missing Reconnaissance Tools:

Install the missing tools (Findomain, Assetfinder, dnsx) to enhance the reconnaissance capabilities. Ensure they are properly configured and updated regularly.

2. Limited Subdomain Enumeration:

Investigate alternative subdomain enumeration techniques, including using online passive DNS databases and certificate transparency logs. Consider using a more comprehensive toolset after installing the missing dependencies.

3. Tool not installed - Resolved Hosts:

Identify and install the necessary tool for resolving hosts. Ensure it is properly configured and integrated into the reconnaissance workflow.

4. Open FTP Port (21):

Disable FTP if not required. If required, configure FTP to use secure protocols like SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure). Enforce strong authentication and access controls.

5. Open SSH Port (22):

Ensure SSH is running the latest version with all security patches applied. Implement strong password policies or, preferably, use SSH key-based authentication. Consider using port knocking or limiting SSH access to specific IP addresses.

6. Open HTTP Port (80):

Redirect all HTTP traffic to HTTPS (port 443) to ensure encrypted communication. Implement HSTS (HTTP Strict Transport Security) to enforce HTTPS usage.

7. Open RTSP Port (554):

Disable RTSP if not required. If required, implement strong authentication and access controls. Ensure the RTSP server is running the latest version with all security patches applied. Consider using a firewall to restrict access to authorized IP addresses.

8. Open PPTP Port (1723):

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

9. Open MySQL Port (3306):

Ensure the MySQL server 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 updated with the latest security patches.

10. WhatWeb Scan Failure:

Install the missing library (`/usr/bin/lib/messages`) or reinstall WhatWeb to ensure all dependencies are met. Verify the WhatWeb installation and configuration.

11. Missing DNSSEC:

Implement DNSSEC for the domain sophie.sarral.io to enhance DNS security.