Penetration Test Report

Target: sophie.sarral.io

Scan ID	9
Date	2025-11-22 15:59
Status	Completed
Confidentiality	CONFIDENTIAL

Executive Summary

Passive Recon Phase: The passive reconnaissance scan of sophie.sarral.io revealed several issues impacting the effectiveness of the scan itself, primarily related to missing API keys and file access problems within the Harvester tool. This significantly limited the amount of information gathered. The WHOIS lookup indicates a malformed request. The results of successful searches are not apparent in the provided output. Overall, the scan provided very little usable information about the target's attack surface, and further investigation with properly configured tools is needed.

Active Recon Phase: The active reconnaissance scan of sophie.sarral.io reveals several open ports that present potential security vulnerabilities. The open FTP (port 21), SSH (port 22), HTTP (port 80), RTSP (port 554), PPTP (port 1723), and MySQL (port 3306) ports, coupled with a closed HTTPS (port 443) port, highlight potential areas of concern. Further investigation is needed to determine the versions of the services running on these ports and to assess the specific risks associated with them. The absence of WhatWeb and dnsrecon data limits the completeness of this initial assessment.

Detailed Findings

Findings from Passive Recon

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Findings from Active Recon

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Name	Unknown
Severity	Unknown
Description	No description
Mitigation	No mitigation provided

Appendix: Technical Data

The following section contains raw output from the scanning tools.

Raw Output: Passive Recon

{"whois": "Malformed request.\n>>> Last update of WHOIS database: 2025-11-22T10:27:32Z <<<\n\nTerms of Use: Access to WHOIS information is provided to assist persons in determining the contents of a domain name registration record in the registry database. The data in this record is provided by Identity Digital or the Registry Operator for informational purposes only, and accuracy is not guaranteed. This service is intended only for query-based access. You agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator, a Registrar, or Identity Digital except as reasonably necessary to register domain names or modify existing registrations. When using the Whois service, please consider the following: The Whois service is not a replacement for standard EPP commands to the SRS service. Whois is not considered authoritative for registered domain objects. The Whois service may be scheduled for downtime during production or OT&E; maintenance periods. Queries to the Whois services are throttled. If too many queries are received from a single IP address within a specified time, the service will begin to reject further queries for a period of time to prevent disruption of Whois service access. Abuse of the Whois system through data mining is mitigated by detecting and limiting bulk query access from single sources. Where applicable, the presence of a [Non-Public Data] tag indicates that such data is not made publicly available due to applicable data privacy laws or requirements. Should you wish to contact the registrant, please refer to the Whois records available through the registrar
... [Output Truncated]

Raw Output: Active Recon

{"nmap_fast": "Starting Nmap 7.95 (https://nmap.org) at 2025-11-22 05:29 EST\nNmap scan report for sophie.sarral.io (20.124.91.118)\nHost is up (0.19s latency).\nNot shown: 92 filtered tcp ports (no-response)\nPORT STATE SERVICE\n21/tcp open ftp\n22/tcp open ssh\n80/tcp open http\n443/tcp closed https\n554/tcp open rtsp\n1723/tcp open pptp\n3000/tcp closed ppp\n3306/tcp open mysql\n\nNmap done: 1 IP address (1 host up) scanned in 5.20 seconds", "whatweb": "", "dnsrecon": ""}