Comprehensive Reconnaissance Report

Professional Security Assessment

Target	Generated
127.0.0.1	2025-09-01 14:11:18

Executive Summary

Services Detected

5

Open Ports

0

Vulnerabilities

0

Risk Assessment

High Risk Services

2

Medium Risk Services

1

Low Risk Services

2

Network Scan Results

TCP Fast Scan

No TCP fast scan data available

TCP Full Scan

No TCP full scan data available

UDP Fast Scan

No UDP fast scan data available

Service Analysis

22

Port/Protocol: ssh
Port: 22
Version: 10.0p2

Vulnerabilities Detected

ExploitDB CVEs:

none

Metasploit CVEs:

none

Target: 127.0.0.1

Port: 22

Server: OpenSSH

Version: 10.0p2

Auth Methods:

Exploitdb Mods: none

Exploitdb Cves: none

Msf Mods: none

Msf Cves: none

Http

Port/Protocol: 8000/tcp
Port: 8000

Target: 127.0.0.1

Os Fingerprint: Linux 2.6.32, Linux 5.0 - 6.2

Http Banner: unknown

Https Banner: unknown

Vulnerable Endpoints:

- **Sql Injection:**
- **Xss:**
- **Lfi:**
- **File Upload:**

Technologies:

- **Web Server:**
- **Programming Language:**
- **Framework:**
- **Cms:**
- **Database:**
- **Javascript:**
- **Other:**

Wordpress Findings:

- **Version:** unknown
- **Plugins:**
- **Themes:**
- **Vulnerabilities:**

Joomla Findings:

- **Version:** unknown
- **Components:**
- **Vulnerabilities:**

Sqlmap Findings:

- **Injectable Parameters:**

Ssh

Port/Protocol: 22/tcp
Port: 22
Version: 10.0p2

Vulnerabilities Detected

ExploitDB CVEs:

none

Metasploit CVEs:

none

Target: 127.0.0.1

Port: 22

Server: OpenSSH

Version: 10.0p2

Auth Methods:

Exploitdb Mods: none

Exploitdb Cves: none

Msf Mods: none

Msf Cves: none

Postgresql

Port/Protocol: 5432/tcp
Port: 5432

Target: 127.0.0.1

Nmap Postgresql Banner: Starting Nmap 7.95 (https://nmap.org) at 2025-09-01 13:41 +01 Nmap scan report for localhost (127.0.0.1) Host is up (0.000081s latency). PORT STATE SERVICE VERSION 5432/tcp open postgresql PostgreSQL DB 9.6.0 or later Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 7.12 seconds

Raw Postgresql Banner: [!] No banner — PostgreSQL requires proper handshake.

Msf Exploit Found: yes

Msf Exploit Mods: exploit/linux/http/acronis_cyber_infra_cve_2023_45249, exploit/linux/http/appsmith_rce_cve_2024_55964, exploit/linux/http/beyondtrust_pra_rs_unauth_rce, exploit/linux/postgres/postgres_payload, exploit/multi/http/manage_engine_dc_pmp_sqli, exploit/multi/http/rudder_server_sqli_rce, exploit/multi/postgres/postgres_copy_from_program_cmd_exec, exploit/multi/postgres/postgres_createlang, exploit/windows/misc/manageengine_eventlog_analyzer_rce, exploit/windows/postgres/postgres_payload

Msf Exploit Cves: CVE-2007-3280, CVE-2014-3996, CVE-2015-7387, CVE-2019-9193, CVE-2023-30625, CVE-2023-45249, CVE-2024-12356, CVE-2024-55963, CVE-2024-55964, CVE-2025-1094

Port: 5432

Http-Proxy

Port/Protocol: 8080/tcp
Port: 8080

Target: 127.0.0.1

Vulnerability Summary

22 (ssh)

VULNERABILITY TYPE	DETAILS
ExploitDB CVEs	none
Metasploit CVEs	none

Ssh (22/tcp)

VULNERABILITY TYPE	DETAILS
ExploitDB CVEs	none
Metasploit CVEs	none

No known vulnerabilities detected in scanned services.

Report Generated: 2025-09-01 14:11:18

Target: 127.0.0.1