

Rapport de Scan de Vulnérabilités

Cible : 127.0.0.1 | Généré le : 11/07/2026 10:19 | Outil : Automated Vulnerability Scanner v1.0

Résumé : 6 port(s) ouvert(s) détecté(s) — Critical: 1 High: 2 Medium: 2 Low: 1

Port	Service / Bannière	Risque	CVSS	Constat
21	220 ProFTPD 1.3.5 Server ready.	High	7.5	Unencrypted FTP service exposed
22	SSH-2.0-OpenSSH_7.4	Low	3.1	SSH service exposed - verify version is current
23	Telnet service ready	Critical	9.8	Telnet service exposed (cleartext credentials)
80	HTTP/1.1 200 OK Server: Apache/2.4.29 (Ubuntu)	Medium	5.3	Web server banner discloses version information
3306	5.5.5-10.1.38-MariaDB	High	8.2	Database service reachable from network
8080	HTTP/1.1 200 OK Server: Jetty/9.4.z	Medium	5.0	Secondary web service on non-standard port

Recommandations de remédiation

- Port 21 (High)** : Disable FTP or migrate to SFTP/FTPS with strong authentication.
- Port 22 (Low)** : Keep OpenSSH patched; disable password auth in favor of keys.
- Port 23 (Critical)** : Disable Telnet immediately; use SSH for remote administration.
- Port 80 (Medium)** : Suppress server version disclosure (ServerTokens/ServerSignature).
- Port 3306 (High)** : Restrict MySQL/MariaDB to localhost or a private VLAN; enforce TLS.
- Port 8080 (Medium)** : Confirm this service is intended to be internet-facing; patch regularly.