Host Scanned	127.0.0.1
Vulnerabilities Detected	
Apache HTTP Server Expect Header Information-Disclosure (CVE-2021-41773)	Medium risk, CVSS 5.8
ISC BIND Assertion Failure in buffer.c (CVE-2016-2776)	High risk, CVSS 7.5
Default Credentials on SSH Server	High risk, CVSS 7.3
SOCKS Proxy Detection (Transparent)	Medium risk, CVSS 5.0
PHP Unsupported Version Detection	Medium risk, CVSS 4.3
SSL/TLS: Vulnerable Cipher Suites for HTTPS	Medium risk, CVSS 4.0
HTTP Security Headers Missing	Low risk, CVSS 2.6
OS End of Life Detection	Low risk, CVSS 2.3

Recommendations
Patch Apache HTTP Server to fix CVE-2021-41773.
Update BIND to the latest secure version.
Remove or change default SSH credentials immediately.
Disable or secure SOCKS proxy service if not required.
Upgrade PHP to a supported version.
Reconfigure SSL/TLS to use strong cipher suites only.
Implement standard HTTP security headers (CSP, HSTS, X-Frame-Options).
Migrate to a supported operating system version.