

FreshScanSentry

Detailed Findings Report & Fix Guide

Target: scanme.nmap.org

Scan type: network

Scanned: 10/12/2026, 2:10:34 PM

Report generated: 10/12/2026, 2:15:49 PM

SAMPLE REPORT

A real Basic Scan of scanme.nmap.org, a server the Nmap project runs so anyone can test scanners against it. Your report shows the same detail for your own systems.

Summary

Exposure grade: B 2 medium-risk issues and no high-risk ones.

This scan found Medium-risk issues worth addressing soon. None are immediately critical, but they meaningfully increase your exposure.

Findings: 0 High, 2 Medium, 2 Low, 4 Informational (8 total).

Findings & Remediation

Medium - Outdated OpenSSH 6.6.1p1 with known vulnerabilities (port 22)

scanme.nmap.org

OpenSSH 6.6.1p1 matches 58 published vulnerabilities (CVEs) for its version, the most severe rated 10.0 out of 10. Nmap also lists 98 public exploits (ready-made attack code) for this version. This is based on the version number the server reports. Linux distributions often patch security fixes without changing that number, so some of these may already be fixed. Check that the system is receiving its security updates.

How to fix this: Update OpenSSH to the latest supported release (or install your operating system's security updates), then re-scan to confirm. If a hosting provider manages this server, ask them which version you're running.

Medium - Outdated Apache httpd 2.4.7 with known vulnerabilities (port 80)

scanme.nmap.org

Apache httpd 2.4.7 matches 127 published vulnerabilities (CVEs) for its version, the most severe rated 10.0 out of 10. Nmap also lists 61 public exploits (ready-made attack code) for this version. This is based on the version number the server reports, which usually means the software is out of date.

How to fix this: Update Apache httpd to the latest supported release (or install your operating system's security updates), then re-scan to confirm. If a hosting provider manages this server, ask them which version you're running.

Low - Open port 22 (ssh)

scanme.nmap.org

SSH exposure is normal but should be key-based and rate-limited.

How to fix this: Use key-based authentication instead of passwords, disable root login, and consider rate-limiting login attempts to reduce automated brute-force noise.

Low - Open port 80 (http)

scanme.nmap.org

Unencrypted HTTP; consider redirecting to HTTPS.

How to fix this: Redirect all HTTP traffic to HTTPS and obtain a valid TLS certificate (e.g. via Let's Encrypt) if you haven't already.

Informational - Forms that may lack CSRF protection (port 80)

scanme.nmap.org

Nmap found 2 forms (nst-head-search, nst-foot-search) without an obvious anti-CSRF token on <http://scanme.nmap.org:80/>. This is often a false alarm for simple forms like site search, which don't change anything. It matters for forms that log in, save data or make payments.

How to fix this: For any form that changes data or account state, add a CSRF token (most web frameworks have

this built in) and set cookies with SameSite=Lax or Strict. Search-only forms can be left as they are.

Informational - Web server reveals its software version (port 80)

scanme.nmap.org

The web server announces itself as "Apache/2.4.7 (Ubuntu)". Showing the exact software and version makes it easier for attackers to match the server to known vulnerabilities.

How to fix this: Hide version details in the server banner (Apache: "ServerTokens Prod" and "ServerSignature Off"; nginx: "server_tokens off"), and keep the software updated.

Informational - Interesting paths found on the web server (port 80)

scanme.nmap.org

Nmap found these paths worth reviewing: /images/: directory listing is turned on. Directory listings and admin or backup paths can reveal files you didn't mean to publish.

How to fix this: Turn off directory listing (Apache: "Options -Indexes"; nginx: "autoindex off"), and remove or password-protect anything that shouldn't be public.

Informational - Open port 9929 (nping-echo)

scanme.nmap.org

Open port found; verify it should be reachable.

How to fix this: Confirm this port is intentionally exposed to the network it was scanned from. If it doesn't need to be public, close it at the firewall to reduce your attack surface.