

Forum:[Hack Forums](#)

Thread: [what are good scanners beside nmap?](#)

L3ANDRINK3R - August 17, 2025, 1:53 pm

i've been using nmap for.. well forever so i was wondering is there anything better? cuz i know nmap doesnt show ALL vulnerabilities considering it relies on on scripts and user input. so if you guys can tell me more scanners that would be quite lovely.

DramaKing - August 17, 2025, 2:17 pm

(Aug 17, 2025 01:53 PM)L3ANDRINK3R Wrote: [\[CITE\]](#) i've been using nmap for.. well forever so i was wondering is there anything better? cuz i know nmap doesnt show ALL vulnerabilities considering it relies on on scripts and user input. so if you guys can tell me more scanners that would be quite lovely.

There are other good scanners, but none as good as nmap, and I think that the developers of MegaPing, masscan, etc., gave up long ago. You won't find scripting engines with any of those.

???????????? - August 17, 2025, 11:14 pm

(Aug 17, 2025 01:53 PM)L3ANDRINK3R Wrote: [\[CITE\]](#) i've been using nmap for.. well forever so i was wondering is there anything better? cuz i know nmap doesnt show ALL vulnerabilities considering it relies on on scripts and user input. so if you guys can tell me more scanners that would be quite lovely.

Nmap is excellent for discovery and quick checks, but it's not a full vulnerability scanner. If you want deeper results, tools like OpenVAS/Greenbone (free, CVE-focused), Nessus or Nexpose (enterprise-grade with massive vuln databases), and lightweight speed demons like Masscan or RustScan can complement it. For web-specific issues, Nikto or OWASP ZAP are better fits. Many people use nmap for recon, then feed results into these dedicated scanners for full vulnerability coverage.

pwningtheunpwned - September 9, 2025, 2:16 pm

Nmap is inescapable, amazing scripting engine, anything you want it to be. For speed, I've been using Rustscan with --scripts none and --ulimit 5000 to get all open ports then scan all those ports with Nmap with the -sV, -sC, -O (you can exclude it, those suffice) and the specified ports as sudo to ensure maximal stealth with -sS is extremely good.

Don't expect exploitation from recon. Recon leads to exploitation. Not only that but scripts can directly check for such without consulting the Metasploit console and even exploit them in rare cases