Vulnerability Assessment Report: scanme.nmap.org

SECURITY SCORE: 42/100

OVERALL RISK LEVEL: HIGH

1. Network Scan Results (Nmap)

Port	State	Service	Version	Evidence
22	OPEN	ssh	6.6.1p1 Ubuntu 2ubuntu2.13	None
25	FILTERED	smtp		None
80	OPEN	http	2.4.7	**http-title:** Go ahead and ScanMe!...
135	FILTERED	msrpc		None
139	FILTERED	netbios-ssn		None
179	FILTERED	bgp		None
445	FILTERED	microsoft-ds		None
9929	OPEN	nping-echo		None
31337	OPEN	tcpwrapped		None

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 45.33.32.156
+ Target Hostname: scanme.nmap.org
+ Target Port: 80
+ Start Time: 2026-02-24 16:26:36 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ 26 items checked: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2026-02-24 16:27:07 (GMT0) (31 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 600 seconds reached
```

3. Crawled & Fuzzed Endpoints

- http://scanme.nmap.org/shared/css/nst.css?v=2
- http://scanme.nmap.org/
- http://scanme.nmap.org/shared/css/nst-foot.css?v=2

- http://scanme.nmap.org/site.css
- http://scanme.nmap.org
- http://scanme.nmap.org/images/sitelogo.png
- http://scanme.nmap.org/shared/images/tiny-eyeicon.png
- http://scanme.nmap.org/shared/images/nst-icons.svg

4. Vulnerability Intelligence (CVE Mapping)

Version-Associated CVEs (Unverified Exploit) in Apache httpd 2.4.7

- [POTENTIAL] CVE-2021-44224: a crafted uri sent to httpd configured as a forward proxy (proxyrequests on) can cause a crash (null pointer d...
- [POTENTIAL] CVE-2025-66200: mod_userdir+suexec bypass via allowoverride fileinfo vulnerability in apache http server. users with access to...

Legacy Vulnerability Intelligence

- ■■ NOTICE: Filtered 1 legacy vulnerabilities.

5. Attack Possibilities & Mitigation

[CRITICAL] Attack: Blind SQL Injection (HTML Form at /search/)
Evidence: Payload forced server to sleep for 3.39 seconds.
Mitigation: Use prepared statements.

[LOW] Attack: Missing Anti-Clickjacking Protection
Mitigation: Implement DENY or SAMEORIGIN X-Frame-Options.

[NOTE] Attack: Missing Content-Security-Policy (CSP)
Mitigation: Implement a strict CSP header.