Vulnerability Assessment Report: scanme.nmap.org

SECURITY SCORE: 45/100

OVERALL RISK LEVEL: HIGH

1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
22	ssh	6.6.1p1 Ubuntu 2ubuntu2.13	None
25	smtp		None
80	http	2.4.7	**http-title:** Go ahead and ScanMe!...
135	msrpc		None
139	netbios-ssn		None
179	bgp		None
445	microsoft-ds		None
999	garcon		None
1029	ms-lsa		None
1062	veracity		None
1175	dossier		None
1236	bvcontrol		None
2008	conf		None
2160	apc-2160		None
2383	ms-olap4		None
3001	nessus		None
3333	dec-notes		None
3546			None
5051	ida-agent		None
5080	onscreen		None
5225	hp-server		None
5907	dsd		None
9200	wap-wsp		None
9929	nping-echo		None
10621			None
14442			None

31337	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: 2026-02-23 16:51:46 (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: 2026-02-23 16:52:17 (GMT0) (31 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

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

3. Crawled Website Endpoints

- http://scanme.nmap.org/#menu
- [FORM] http://scanme.nmap.org/search/
- http://scanme.nmap.org/

4. Vulnerability Intelligence (CVE Mapping)

Modern Vulnerabilities in Apache httpd 2.4.7
- [CRITICAL 9.8] CVE-2016-6814: When an application with unsupported Codehaus versions of Groovy from 1.7.0 to 2.4.3, Apache Groovy 2.4.4 to 2.4.7 on classpath uses standard Java ser...
- [HIGH 8.2] CVE-2021-44224: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixin...
- [MEDIUM 5.4] CVE-2025-66200: mod_userdir+suexec bypass via AllowOverride FileInfo vulnerability in Apache HTTP Server. Users with access to use the RequestHeader directive in htac...

Modern Vulnerabilities in Apache 2.4.7
- [CRITICAL 9.8] CVE-2016-6814: When an application with unsupported Codehaus versions of Groovy from 1.7.0 to 2.4.3, Apache Groovy 2.4.4 to 2.4.7 on classpath uses standard Java ser...
- [HIGH 8.2] CVE-2021-44224: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixin...
- [MEDIUM 5.4] CVE-2025-66200: mod_userdir+suexec bypass via AllowOverride FileInfo vulnerability in Apache HTTP Server. Users with access to use the RequestHeader directive in htac...

Legacy Vulnerability Intelligence
- ■■ NOTICE: Our engine identified 2 additional legacy vulnerabilities (pre-2016) associated with these services. These have been filtered to prioritize current threats.

5. Attack Possibilities & Mitigation

[LOW] Attack: Clickjacking / Cross-Site Scripting (XSS)
Mitigation: Implement X-Frame-Options and Content-Security-Policy headers.