Vulnerability Assessment Report: scanme.nmap.org

SECURITY SCORE: 5/100

OVERALL RISK LEVEL: CRITICAL

1. Network Scan Results (Nmap)

Port	Service	Version	State
22	tcpwrapped		open
25	smtp		filtered
80	http	2.4.7	open
135	msrpc		filtered
139	netbios-ssn		filtered
179	bgp		filtered
445	microsoft-ds		filtered
1030	iad1		filtered
9929	nping-echo		open
31337	tcpwrapped		open

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: 2026-02-22 14:44:15 (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: 2026-02-22 14:44:45 (GMT0) (30 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

[nikto stderr]
+ ERROR: Host maximum execution time of 180 seconds reached
```

3. Crawled Website Endpoints

- http://scanme.nmap.org/
- http://scanme.nmap.org/#menu

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

4. Vulnerability Intelligence (CVE Mapping)

Note: Findings categorized by severity.
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...
Modern Vulnerabilities in Apache httpd 2.4.7
- [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...
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

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