

# Vulnerability Assessment Report: scanme.nmap.org

## SECURITY SCORE: 98/100

OVERALL RISK LEVEL: LOW

### 1. Network Scan Results (Nmap)

Port	Service	Version	State
22	ssh	6.6.1p1 Ubuntu 2ubuntu2.13	open
25	smtp		filtered
80	http	2.4.7	open
135	msrpc		filtered
139	netbios-ssn		filtered
179	bgp		filtered
445	microsoft-ds		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: 2026-02-23 15:55:06 (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 15:55:33 (GMT0) (27 seconds)
-----
+ 1 host(s) tested
[stderr]
+ ERROR: Host maximum execution time of 86400 seconds reached
```

### 3. Crawled Website Endpoints

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

## **4. Vulnerability Intelligence (CVE Mapping)**

No relevant CVEs identified.

## **5. Attack Possibilities & Mitigation**

**[LOW] Attack:** Clickjacking / Cross-Site Scripting (XSS)

**Mitigation:** Implement X-Frame-Options and Content-Security-Policy headers.