

# Vulnerability Assessment Report: scanme.nmap.org

## 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: 2026-01-31 05:02:03 (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: 2026-01-31 05:02:31 (GMT0) (28 seconds)
-----
+ 1 host(s) tested
```

## 3. Crawled Website Endpoints

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

## 4. Vulnerabilities Detected

- Missing Security Headers

## 5. Vulnerability Intelligence (CVE Mapping)

### Vulnerabilities in OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13

- CVE-1999-0661: A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) u...
- CVE-2000-0525: OpenSSH does not properly drop privileges when the UseLogin option is enabled, which allows local users to execute arbitrary commands by providing the...
- CVE-2000-0535: OpenSSL 0.9.4 and OpenSSH for FreeBSD do not properly check for the existence of the /dev/random or /dev/urandom devices, which are absent on FreeBSD ...
- CVE-2000-1169: OpenSSH SSH client before 2.3.0 does not properly disable X11 or agent forwarding, which could allow a malicious SSH server to gain access to the X11 ...
- CVE-2001-1459: OpenSSH 2.9 and earlier does not initiate a Pluggable Authentication Module (PAM) session if commands are executed with no pty, which allows local use...

### Vulnerabilities in Apache httpd 2.4.7

- 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...

### Vulnerabilities in Apache 2.4.7

- CVE-2012-2378: Apache CXF 2.4.5 through 2.4.7, 2.5.1 through 2.5.3, and 2.6.x before 2.6.1, does not properly enforce child policies of a WS-SecurityPolicy 1.1 Suppo...
- 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...
- 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...
- 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...

## 6. Attack Possibilities & Mitigation

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

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