

# Penetration Testing Report

Prepared By: Tarun M

Date: 10/08/2025

## 1. Executive Summary

A penetration test was conducted against scanme.nmap.org (45.33.32.156) to identify open ports, running services, and potential vulnerabilities. The assessment revealed outdated services and unnecessary open ports. Remediation steps have been recommended to improve security posture.

## 2. Scope of Work

Target Host: scanme.nmap.org (45.33.32.156) Date of Testing: 10/08/2025 Testing Methodology: External reconnaissance and service enumeration Tools Used: Nmap, WhatWeb, Nikto, Gobuster, Searchsploit

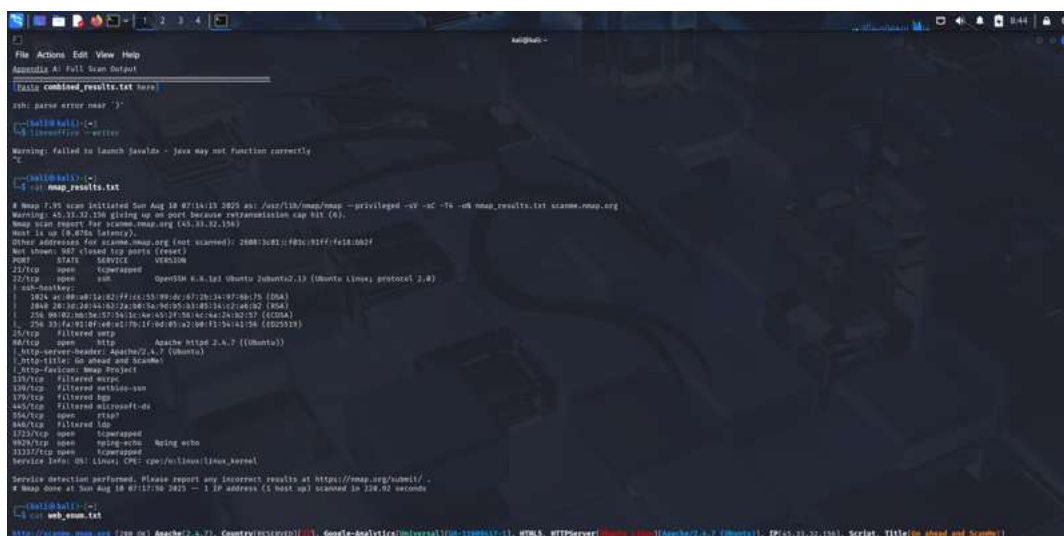
## 3. Findings Summary

| Port  | State | Service    | Version/Notes                                 |
|-------|-------|------------|---|
| 22    | Open  | SSH        | OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (outdated) |
| 80    | Open  | HTTP       | Apache httpd 2.4.7 ((Ubuntu)) – outdated      |
| 1723  | Open  | tcpwrapped | Service responded but details hidden          |
| 9929  | Open  | nping-echo | Nmap testing service                          |
| 31337 | Open  | tcpwrapped | Service responded but details hidden          |

## 4. Detailed Methodology

### Step 1 – Nmap Service & Port Scan

Nmap was used to identify open ports, running services, and their versions. Command used: nmap -sV -sC -T4 scanme.nmap.org



```
File Actions Edit View Help
Amendable A: Full Scan Output
[Full combined_results.txt here]
ysh: parse error near `)'
--(nmap@kali)~$-
$ nmap -sV -sC -T4 scanme.nmap.org
Nmap 7.95 scan initiated Sun Aug 10 07:13:13 2025 as: /usr/bin/nmap --privileged -sV -sC -T4 -oN nmap_results.txt scanme.nmap.org
scanning: 45.33.32.156 giving up on port because retransmission cap hit (6).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0000s latency).
Other addresses for scanme.nmap.org (not scanned): 2000:3::81::f8b:91ff:fe1d:0a2f
Not shown: 655 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh             OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http            Apache httpd 2.4.7 ((Ubuntu))
1723/tcp  open  tcpwrapped
9929/tcp  open  nping-echo      Nmap testing service
31337/tcp open  tcpwrapped
Service detection performed. Please report any incorrect results at https://nmap.org/nodebug/
# Nmap done at Sun Aug 10 07:17:38 2025 -- 1 IP address (1 host up) scanned in 210.50 seconds
--(nmap@kali)~$-
$ cat nmap_results.txt
Nmap (2.4.7), Country[RESERVED][9], Google-Analytica[Universal][00-13806417-1], HTML5, HTTPServer[Apache/2.4.7 (Ubuntu)], IP[45.33.32.156], Script, Title[on ahead and Scanme]
```

Results indicated multiple open ports including SSH (OpenSSH 6.6.1p1) and HTTP (Apache 2.4.7), both outdated. Some ports were filtered, indicating firewall rules in place.

## Step 2 – Web Vulnerability Scan (Nikto)

Nikto was used to identify web vulnerabilities and outdated software versions. Command used: `nikto -h http://scanme.nmap.org`

```
File Actions Edit View Help
kali@kali:~$ nikto -h http://scanme.nmap.org -u nikto_results.txt
Nikto v2.3.8

+ Multiple IPs Found: 65.32.32.156, 2000:3c01::f80c::91ff:fa18:002f
+ Target IP: 65.32.32.156
+ Target hostname: scanme.nmap.org
+ Target Port: 80
+ Start Time: 2025-08-10 07:24:43 (GMT+4)

+ Server: Apache/2.4.7 (Ubuntu)
+ / The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ / The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis-x-content-type-header/
+ No CSS Directives Found (use '-C all' to force check all possible dirs)
+ /index/ Unknown header 'X-Content-Type-Options' found, with content: list.
+ /index/ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for '/index' were found: index.html. See: http://www.wisec.it/sectos.php?id=4086bdc3b035,6
https://exchange.vforce.lanload.com/vulnerabilities/6275
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.34). Apache 2.2.34 is the EOL for the 2.4 branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS.
+ /images/ Directory indexing found.

kali@kali:~$ nikto -h http://scanme.nmap.org -tuning 1 -u nikto_results.txt
Nikto v2.3.8

+ Multiple IPs Found: 65.32.32.156, 2000:3c01::f80c::91ff:fa18:002f
+ Target IP: 65.32.32.156
+ Target hostname: scanme.nmap.org
+ Target Port: 80
+ Start Time: 2025-08-10 07:25:15 (GMT+4)

+ Server: Apache/2.4.7 (Ubuntu)
+ / The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ / The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis-x-content-type-header/
+ No CSS Directives Found (use '-C all' to force check all possible dirs)
+ /index/ Unknown header 'X-Content-Type-Options' found, with content: list.
+ /index/ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for '/index' were found: index.html. See: http://www.wisec.it/sectos.php?id=4086bdc3b035,6
https://exchange.vforce.lanload.com/vulnerabilities/6275
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.34). Apache 2.2.34 is the EOL for the 2.4 branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS.
+ 2348 requests: 0 error(s) and 0 slow(s) reported on remote host
+ End Time: 2025-08-10 08:11:13 (GMT+4) (379 seconds)

+ 1 host(s) tested

kali@kali:~$
```

Nikto identified outdated Apache version and missing security headers (X-Frame-Options, X-Content-Type-Options). These issues may allow clickjacking or MIME-based attacks.

## Step 3 – Directory Enumeration (Gobuster)

Gobuster was used to discover hidden directories and files. Command used: `gobuster dir -u http://scanme.nmap.org -w /usr/share/wordlists/dirb/common.txt`

```
[*] URL: http://scanme.nmap.org
[*] Method: GET
[*] Threads: 10
[*] Wordlist: /usr/share/dirb/wordlists/common.txt
[*] Negative Status codes: 404
[*] User Agent: gobuster/3.0
[*] Timeout: 10s

Starting gobuster in directory enumeration mode

./hta (Status: 403) [Size: 286]
./htaccess (Status: 403) [Size: 291]
./htpasswd (Status: 403) [Size: 291]
./svn (Status: 301) [Size: 316] --> http://scanme.nmap.org/svn/
./svn/entries (Status: 403) [Size: 294]
./favicon.ico (Status: 403) [Size: 293]
./images (Status: 301) [Size: 318] --> http://scanme.nmap.org/images/
./index (Status: 200) [Size: 6974]
./index.html (Status: 200) [Size: 6974]
./server-status (Status: 403) [Size: 295]
./shared (Status: 301) [Size: 318] --> http://scanme.nmap.org/shared/
Progress: 4014 / 4015 (99.98%)

Finished

kali@kali:~$ curl -I http://scanme.nmap.org/svn/
curl -I http://scanme.nmap.org/shared/

HTTP/1.1 403 Forbidden
Date: Sun, 10 Aug 2025 12:29:42 GMT
Server: Apache/2.4.7 (Ubuntu)
```

Directories such as `/images/`, `/shared/`, and `/svn/` were found but returned 403 Forbidden, indicating restricted access. These could leak data if misconfigured.

## Step 4 – Exploit Search (Searchsploit)

Searchsploit was used to identify public exploits for detected software versions. Commands used: `searchsploit apache 2.4.7` `searchsploit openssh 6.6.1`

