# Nmap Scan in Kali Linux

**Scan done on:** http://scanme.nmap.org

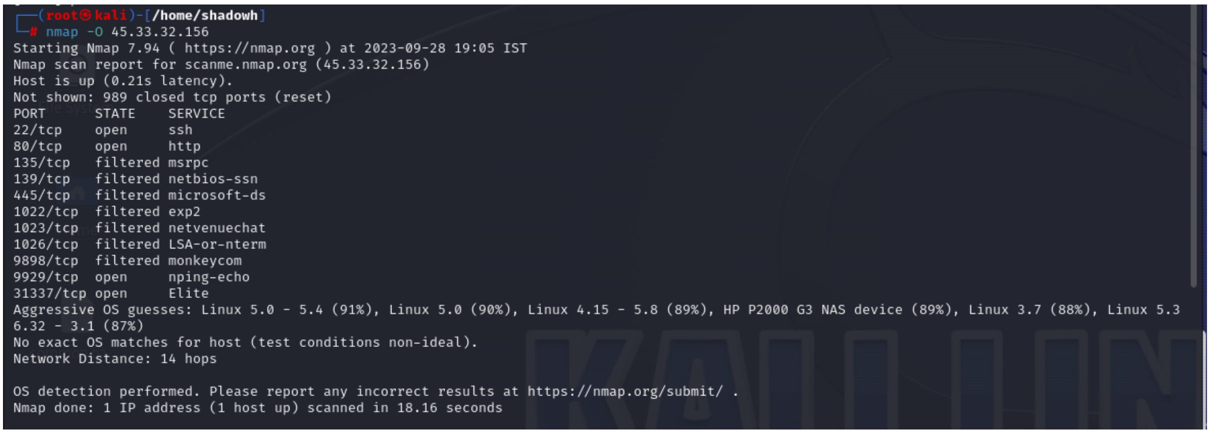
**PROCESS:**

*Step 1:*

First found the IP Address of http://scanme.nmap.org by pinging it.

*Step 2:*

Starting the nmap scan for ports and operating system probability.

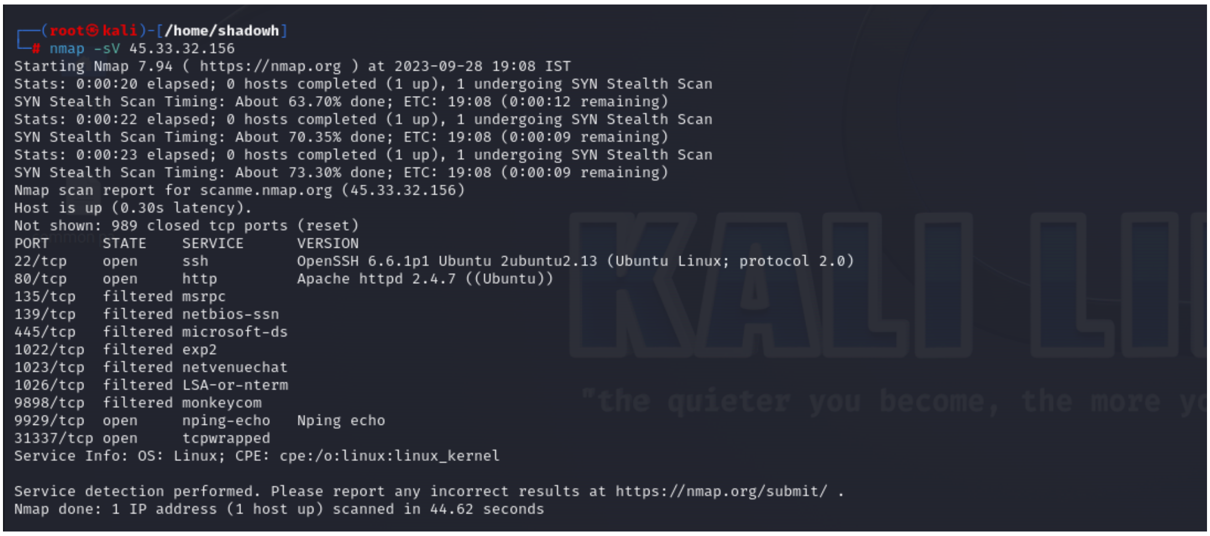


```
┌──(root㉿kali)-[/home/shadowh]
└─# nmap -O 45.33.32.156
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-28 19:05 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1022/tcp  filtered exp2
1023/tcp  filtered netvenuechat
1026/tcp  filtered LSA-or-nterm
9898/tcp  filtered monkeycom
9929/tcp  open     nping-echo
31337/tcp open     Elite
Aggressive OS guesses: Linux 5.0 - 5.4 (91%), Linux 5.0 (90%), Linux 4.15 - 5.8 (89%), HP P2000 G3 NAS device (89%), Linux 3.7 (88%), Linux 5.3
6.32 - 3.1 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 14 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.16 seconds
```

*Step 3:*

Finding the versions with nmap

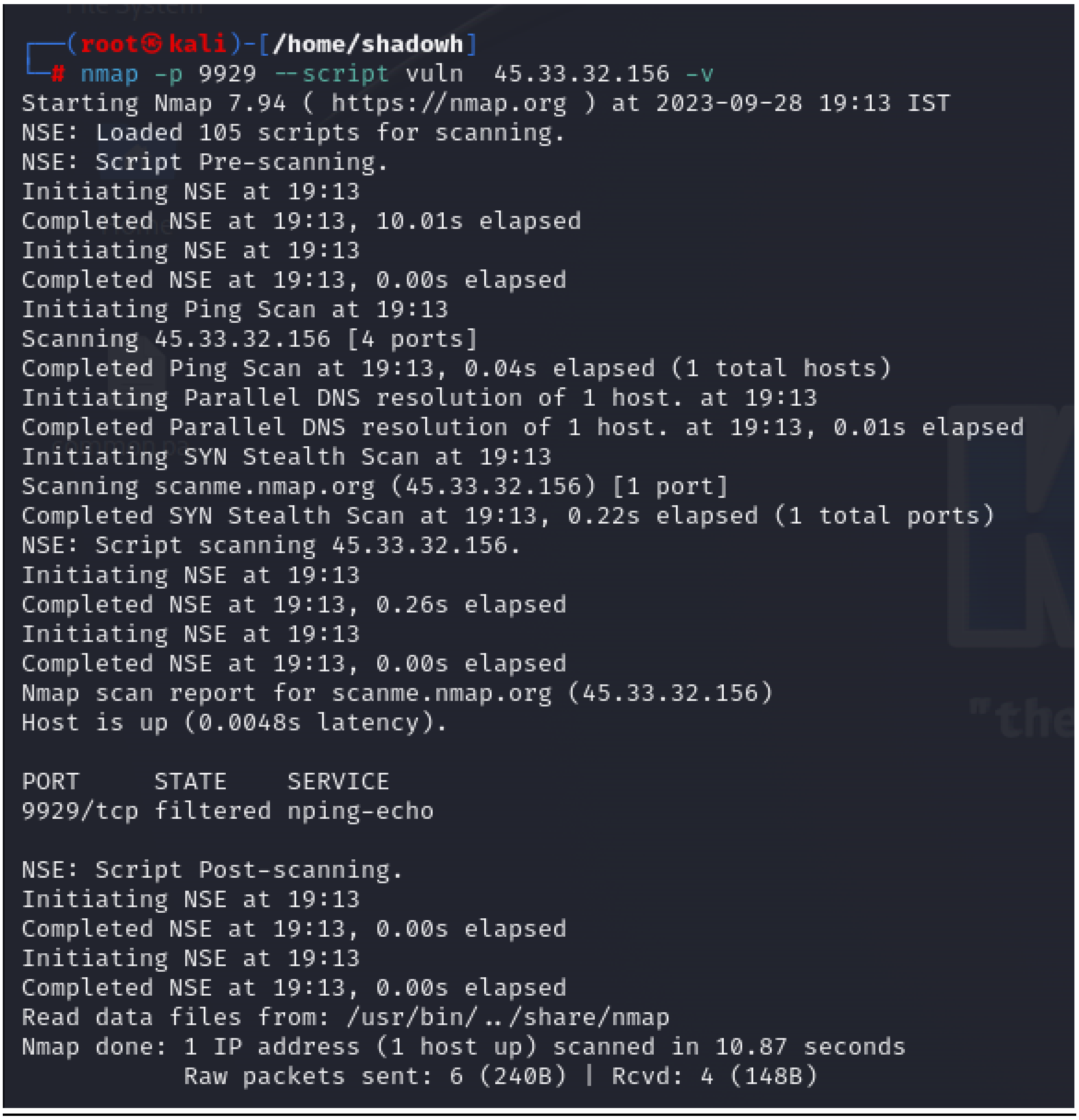


```
┌──(root㉿kali)-[/home/shadowh]
└─# nmap -sV 45.33.32.156
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-28 19:08 IST
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 63.70% done; ETC: 19:08 (0:00:12 remaining)
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 70.35% done; ETC: 19:08 (0:00:09 remaining)
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 73.30% done; ETC: 19:08 (0:00:09 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Not shown: 989 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))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1022/tcp  filtered exp2
1023/tcp  filtered netvenuechat
1026/tcp  filtered LSA-or-nterm
9898/tcp  filtered monkeycom
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.62 seconds
```

*Step 4:*

Searching for vulnerabilities by accessing an open port.



```
┌──(root㉿kali)-[/home/shadowh]
└─# nmap -p 9929 --script vuln  45.33.32.156 -v
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-28 19:13 IST
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:13
Completed NSE at 19:13, 10.01s elapsed
Initiating NSE at 19:13
Completed NSE at 19:13, 0.00s elapsed
Initiating Ping Scan at 19:13
Scanning 45.33.32.156 [4 ports]
Completed Ping Scan at 19:13, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:13
Completed Parallel DNS resolution of 1 host. at 19:13, 0.01s elapsed
Initiating SYN Stealth Scan at 19:13
Scanning scanme.nmap.org (45.33.32.156) [1 port]
Completed SYN Stealth Scan at 19:13, 0.22s elapsed (1 total ports)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 19:13
Completed NSE at 19:13, 0.26s elapsed
Initiating NSE at 19:13
Completed NSE at 19:13, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0048s latency).

PORT     STATE    SERVICE
9929/tcp filtered nping-echo

NSE: Script Post-scanning.
Initiating NSE at 19:13
Completed NSE at 19:13, 0.00s elapsed
Initiating NSE at 19:13
Completed NSE at 19:13, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.87 seconds
           Raw packets sent: 6 (240B) | Rcvd: 4 (148B)
```

**RESULT:**

Thus completed the nmap scan on http://scanme.nmap.org

Found 4 open ports and 7 filtered ports in the scan.

Also found the Operating Systems and their versions.

The nmap scan also performed the scan for vulnerabilities on a particular port and completed various scans on the port.