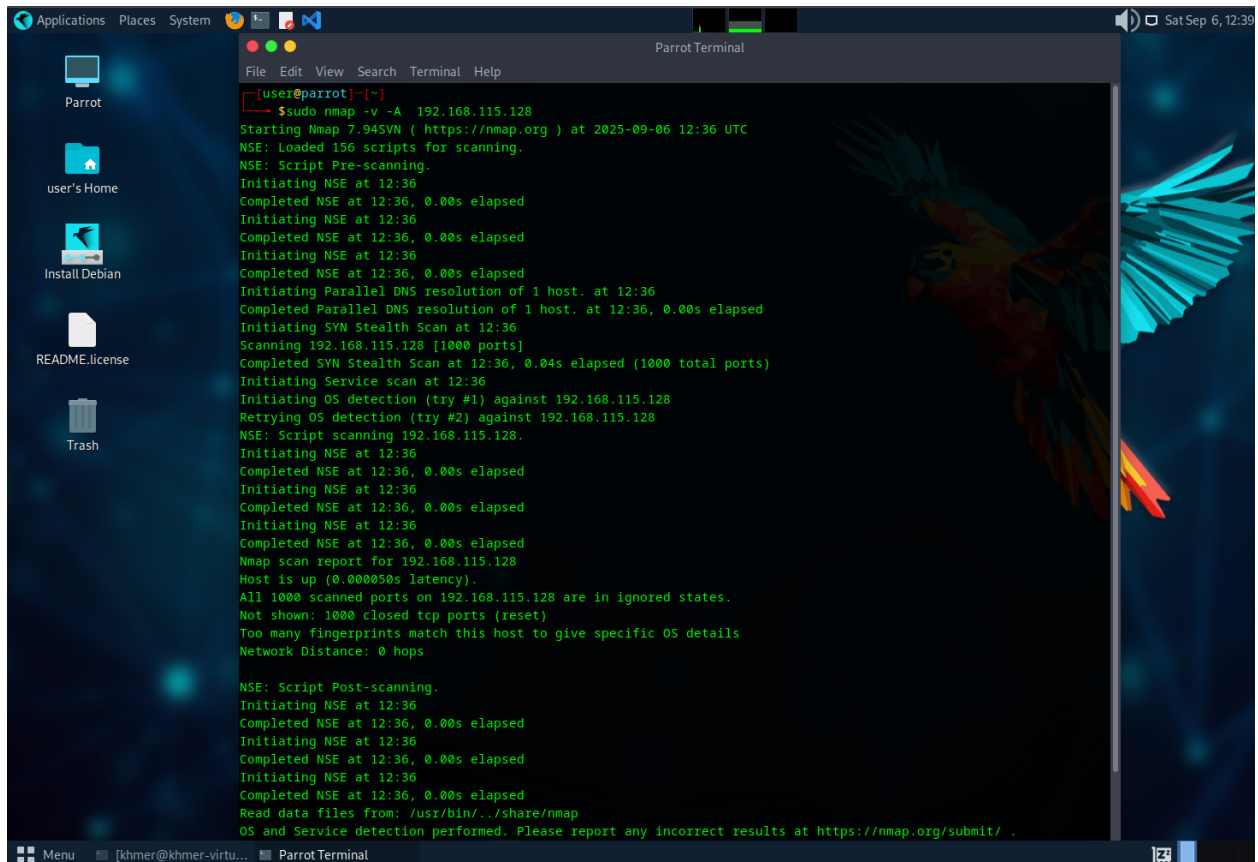


### Act 3

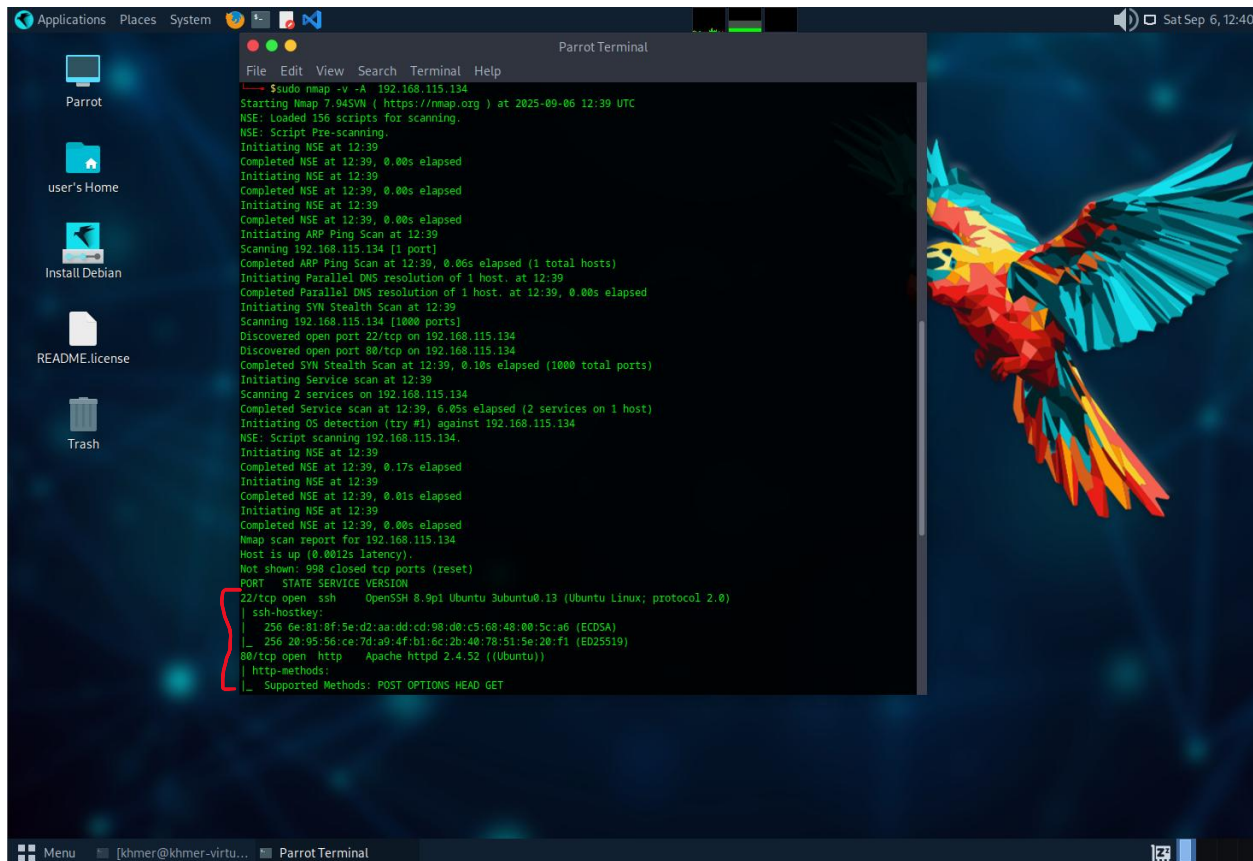
Q1. Notice the open ports on all 3 devices (the attacker notebook, the target notebook, and the target Linux VM). Does anything look suspicious, i.e., some ports that you are not aware of that are open on the VM or on your notebooks?

ANS

Attacker: *all ports closed.*

The image shows a Parrot OS desktop environment. On the left, there is a sidebar with icons for 'Parrot', 'user's Home', 'Install Debian', 'README.license', and 'Trash'. The main area is a dark-themed desktop with a parrot wallpaper. A 'Parrot Terminal' window is open in the center, displaying the output of an nmap scan. The terminal output shows that all 1000 scanned ports on the target host (192.168.115.128) are in ignored states, with no open ports detected. The scan was performed at 2025-09-06 12:36 UTC. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The desktop has a top bar with 'Applications', 'Places', 'System', and a clock showing 'Sat Sep 6, 12:39'.

Target VM: Open ports: 22/tcp (SSH) and 80/tcp (Apache). Running Linux



```
PORT use STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: Expanded Security Maintenance for Applications is not enabled.
|   256 6e:81:8f:5e:d2:aa:dd:cd:98:d0:c5:68:48:00:5c:a6 (ECDSA)
|_  256 20:95:56:ce:7d:a9:4f:b1:6c:2b:40:78:51:5e:20:f1 (ED25519)
80/tcp open  http     Apache httpd 2.4.52 ((Ubuntu))
| http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 00:0C:29:85:F1:3A (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Uptime guess: 49.584 days (since Fri Jul 18 23:55:51 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Target notebook: port 139, 445, 135 opened (These are Windows services (SMB, RPC, etc.).)

```
[user@parrot]~[~]
$ sudo nmap -v -A 10.116.54.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-06 12:48 UTC
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:48
Completed NSE at 12:48, 0.00s elapsed
Initiating NSE at 12:48
Completed NSE at 12:48, 0.00s elapsed
Initiating NSE at 12:48
Completed NSE at 12:48, 0.00s elapsed
Initiating Ping Scan at 12:48
Scanning 10.116.54.200 [4 ports]
Completed Ping Scan at 12:48, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:48
Completed Parallel DNS resolution of 1 host. at 12:48, 0.00s elapsed
Initiating SYN Stealth Scan at 12:48
Scanning 10.116.54.200 [1000 ports]
Discovered open port 139/tcp on 10.116.54.200
Discovered open port 445/tcp on 10.116.54.200
Discovered open port 135/tcp on 10.116.54.200
Discovered open port 902/tcp on 10.116.54.200
Increasing send delay for 10.116.54.200 from 0 to 5 due to 11 out of 32 dropped probes since last increase.
Discovered open port 912/tcp on 10.116.54.200
Increasing send delay for 10.116.54.200 from 5 to 10 due to 91 out of 302 dropped probes since last increase.
Increasing send delay for 10.116.54.200 from 10 to 20 due to 58 out of 193 dropped probes since last increase.
Increasing send delay for 10.116.54.200 from 20 to 40 due to max_successful_tryno increase to 4
Increasing send delay for 10.116.54.200 from 40 to 80 due to max_successful_tryno increase to 5
Increasing send delay for 10.116.54.200 from 80 to 160 due to max_successful_tryno increase to 6
```

Q2. Look at the information provided by nmap about your OS's on all 3 devices. Is the information correct? Why is it or why is it not correct?

**ANS** Yes. The information is correct. Nmap can guess the information of the target from the target's response and using Nmap's database (Nmap has a **database** of known OS fingerprints. Each entry in this database contains the characteristic responses of a particular OS. Nmap compares the observed responses from the target against this database.)

Q3. What do you think about the information you can get using nmap? Scary?

**ANS**

- nmap can reveal: Which ports are open, Which services are running, Software versions, Sometimes even the OS type.
- Yes, attacker can identify possible attack points from the information.

Q4. Look at the access.log file for the web server in your Linux VM. What IP addresses do you see accessing the web server? Which devices do these IP addresses belong to?

**ANS** 192.168.115.134 is target notebook VM, 192.168.115.128 is attacker notebook.

Q5. Find the nmap scan in the web server log. Copy the lines from the log file that were created because of the nmap scan.

ANS

```
khmer@khmer-virtual-machine:/var/log/apache2$ cat access.log
```

```
192.168.115.134 - - [06/Sep/2025:19:13:26 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0"
```

```
192.168.115.134 - - [06/Sep/2025:19:13:26 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://192.168.115.134/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0"
```

```
192.168.115.134 - - [06/Sep/2025:19:13:26 +0700] "GET /favicon.ico HTTP/1.1" 404 493 "http://192.168.115.134/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0"
```

```
192.168.115.134 - - [06/Sep/2025:19:15:31 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0"
```

```
192.168.115.134 - - [06/Sep/2025:19:15:31 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://192.168.115.134/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0"
```

```
192.168.115.128 - - [06/Sep/2025:19:32:31 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"
```

```
192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

```
192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

```
192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

```
192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"
```

```
192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

```
192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

```
192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

```
192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /nmaplowercheck1757161953 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /evox/about HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "PYOW / HTTP/1.1" 501 500 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /HMAP1 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /favicon.ico HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET / HTTP/1.1" 200 10926 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:39:42 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /nmaplowercheck1757162383 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /HMAP1 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"



192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "SZTO / HTTP/1.1" 501 500 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /evox/about HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /favicon.ico HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET / HTTP/1.1" 200 10926 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:48:05 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /nmaplowercheck1757162886 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /evox/about HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "KBCU / HTTP/1.1" 501 500 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /favicon.ico HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /HNAP1 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET / HTTP/1.1" 200 10926 "-" "-"

192.168.115.128 - - [06/Sep/2025:20:56:34 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /nmaplowercheck1757166995 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "PEEZ / HTTP/1.1" 501 500 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /HMAP1 HTTP/1.1" 404 457 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /evox/about HTTP/1.1" 404 457 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /favicon.ico HTTP/1.1" 404 457 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0  
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET / HTTP/1.1" 200 10926 "-" "-"

Result of `iptables -L`

root@khmer-virtual-machine:~# `iptables -L`

Chain INPUT (policy ACCEPT)

target	prot	opt	source	destination
--------	------	-----	--------	-------------

Chain FORWARD (policy ACCEPT)

target	prot	opt	source	destination
--------	------	-----	--------	-------------

Chain OUTPUT (policy ACCEPT)

target	prot	opt	source	destination
--------	------	-----	--------	-------------

Q6. After you successfully install your iptable rule(s), how do the reported results from your new nmap scan compare to your previous scan before using iptables?

Look to see if OS detection, port open results, etc. have changed. Something(s) have definitely changed.

**ANS** found only port 80 and OS(but just guessing) look at the arrows.

```
File Edit View Search Terminal Help
root@khmer@parrot:~# $sudo nmap -v -A 192.168.115.134
Starting Nmap 7.95.0 ( https://nmap.org ) at 2025-09-06 15:02 UTC
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating ARP Ping Scan at 15:02
Completed ARP Ping Scan at 15:02, 0.00s elapsed (1 total hosts)
Initiating Parallel OS resolution of 1 host: at 15:02
Completed Parallel OS resolution of 1 host: at 15:02, 0.00s elapsed
Initiating OS Scan: Scan at 15:02
Scanning 192.168.115.134 [1000 ports]
Discovered open port 80/tcp on 192.168.115.134
Completed OS Scan: Scan at 15:02, 4.71s elapsed (1000 total ports)
Initiating Service scan at 15:02
Scanning 1 service on 192.168.115.134
Completed Service scan at 15:02, 0.00s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.115.134
Retrying OS detection (try #2) against 192.168.115.134
NSE: Script scanning 192.168.115.134.
Initiating NSE at 15:02
Completed NSE at 15:02, 5.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Nmap scan report for 192.168.115.134
Host is up (0.001s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache/2.4.52 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_ http-title: Apache/2.4.52 ((Ubuntu))
|_ http-headers: Apache/2.4.52 ((Ubuntu))
MAC Address: 08:0C:29:05:F1:3A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose/pc
Running (JUST GUESSING): Linux 4.x|5.x|2.6.x|3.x (99%), Synology DiskStation Manager 5.X (89%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/o:synology:diskstation_manager:5.2
Aggressive OS guesses: Linux 4.15 - 5.8 (99%), Linux 5.0 - 5.4 (99%), Linux 5.0 - 5.5 (99%), Linux 5.4 (87%), Linux 2.6.32 (87%), Linux 3.10 (87%), Linux 3.10 - 4.11 (87%), Linux 3.2 - 4.9 (87%), Linux 3.4 - 3.10 (87%), Linux 5.1 (87%)
No host OS matches for host (test conditions non-ideal)
Uptime guess: 49.638 days (since Fri Jul 18 23:55:50 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)

```

Q7. Notice that nmap can still figure out you have Apache httpd running. Look at the access.log file for the web server in your Linux VM. Are the logs the same as in Part II?

**ANS** nmap can still figure out. No the logs are not the same as in PartII.

```
192.168.115.128 - - [06/Sep/2025:22:02:43 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /nmaplowercheck1757170967 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /HNAP1 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "SGWI / HTTP/1.1" 501 500 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /favicon.ico HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /evox/about HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:48 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:48 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:48 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:52 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:22:02:52 +0700] "GET / HTTP/1.1" 200 10926 "-" "-"

Q8. Explain whether or not you could prevent nmap from reaching the web server while still allowing legitimate clients to get service. Will a firewall be sufficient for this? Or do you need some other device? Please think critically about this.

ANS

You can't fully prevent Nmap from reaching an open web server while still allowing legitimate clients. A basic firewall isn't enough for this task.

A firewall like **iptables** works at a low level, filtering traffic based on port and protocol. The rule to allow web traffic on port 80 opens a path for anyone. Since Nmap's reconnaissance probes use the same protocol as a regular web browser, the firewall lets them through.

To block Nmap's specific probing behavior, you need a more advanced security tool, like a **Web Application Firewall (WAF)**. A WAF inspects the actual content of the HTTP requests, allowing it to detect and block suspicious patterns and methods that a standard browser wouldn't use.

Q9. What are your firewall rules? Run iptables -L on your VM and enter the output here.

ANS

```
root@khmer-virtual-machine:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination           ctstate RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere               anywhere              tcp dpt:http
ACCEPT     tcp  --  10.116.54.200          anywhere              tcp dpt:ssh
ACCEPT     all  --  anywhere               anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@khmer-virtual-machine:~#
```