Act 3 : NetworkSecurity

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?
VM :

```
ak1ra@Achiras-MacBook-Air ~ % nmap -T4 -A -v 192.168.1.122
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-08 12:22 +0700
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
Initiating Ping Scan at 12:22
Scanning 192.168.1.122 [2 ports]
Completed Ping Scan at 12:22, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:22
Completed Parallel DNS resolution of 1 host. at 12:22, 0.50s elapsed
Initiating Connect Scan at 12:22
Scanning 192.168.1.122 [1000 ports]
Discovered open port 80/tcp on 192.168.1.122
Discovered open port 22/tcp on 192.168.1.122
Completed Connect Scan at 12:22, 1.59s elapsed (1000 total ports)
Initiating Service scan at 12:22
Scanning 2 services on 192.168.1.122
Completed Service scan at 12:22, 6.05s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.1.122.
Initiating NSE at 12:22
Completed NSE at 12:22, 0.44s elapsed
Initiating NSE at 12:22
Completed NSE at 12:22, 0.04s elapsed
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
Nmap scan report for 192.168.1.122
Host is up (0.017s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 17:d1:a1:f1:9d:88:92:7e:f1:67:65:7d:46:eb:f4:7f (ECDSA)
|_  256 b9:a3:d8:84:a9:44:19:71:0d:70:a6:74:78:bf:c2:34 (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
Read data files from: /opt/homebrew/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.76 seconds
ak1ra@Achiras-MacBook-Air ~ %
```

Not thing look suspicious, port 22 and 80 setting by us

Target Notebook :

```
ak1ra@Achiras-MacBook-Air ~ % nmap -T4 -A -v 192.168.1.100
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-08 12:31 +0700
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:31
Completed NSE at 12:31, 0.00s elapsed
Initiating NSE at 12:31
Completed NSE at 12:31, 0.00s elapsed
Initiating NSE at 12:31
Completed NSE at 12:31, 0.00s elapsed
Initiating Ping Scan at 12:31
Scanning 192.168.1.100 [2 ports]
Completed Ping Scan at 12:31, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:31
Completed Parallel DNS resolution of 1 host. at 12:31, 0.50s elapsed
Initiating Connect Scan at 12:31
Scanning 192.168.1.100 [1000 ports]
Discovered open port 445/tcp on 192.168.1.100
Discovered open port 80/tcp on 192.168.1.100
Discovered open port 135/tcp on 192.168.1.100
Discovered open port 139/tcp on 192.168.1.100
Completed Connect Scan at 12:31, 1.05s elapsed (1000 total ports)
Initiating Service scan at 12:31
Scanning 4 services on 192.168.1.100
Completed Service scan at 12:32, 6.24s elapsed (4 services on 1 host)
NSE: Script scanning 192.168.1.100.
Initiating NSE at 12:32
Completed NSE at 12:32, 5.09s elapsed
Initiating NSE at 12:32
Completed NSE at 12:32, 0.03s elapsed
Initiating NSE at 12:32
Completed NSE at 12:32, 0.00s elapsed
Nmap scan report for 192.168.1.100
Host is up (0.0061s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE       VERSION
80/tcp  open  http          nginx 1.29.0
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.29.0
|_http-title: Welcome to nginx!
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 1s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: LUCASS, NetBIOS user: <unknown>, NetBIOS MAC: 08:6a:c5:8e:dd:07 (Intel Corporate)
| Names:
|   LUCASS<20>           Flags: <unique><active>
|   LUCASS<00>           Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>
```

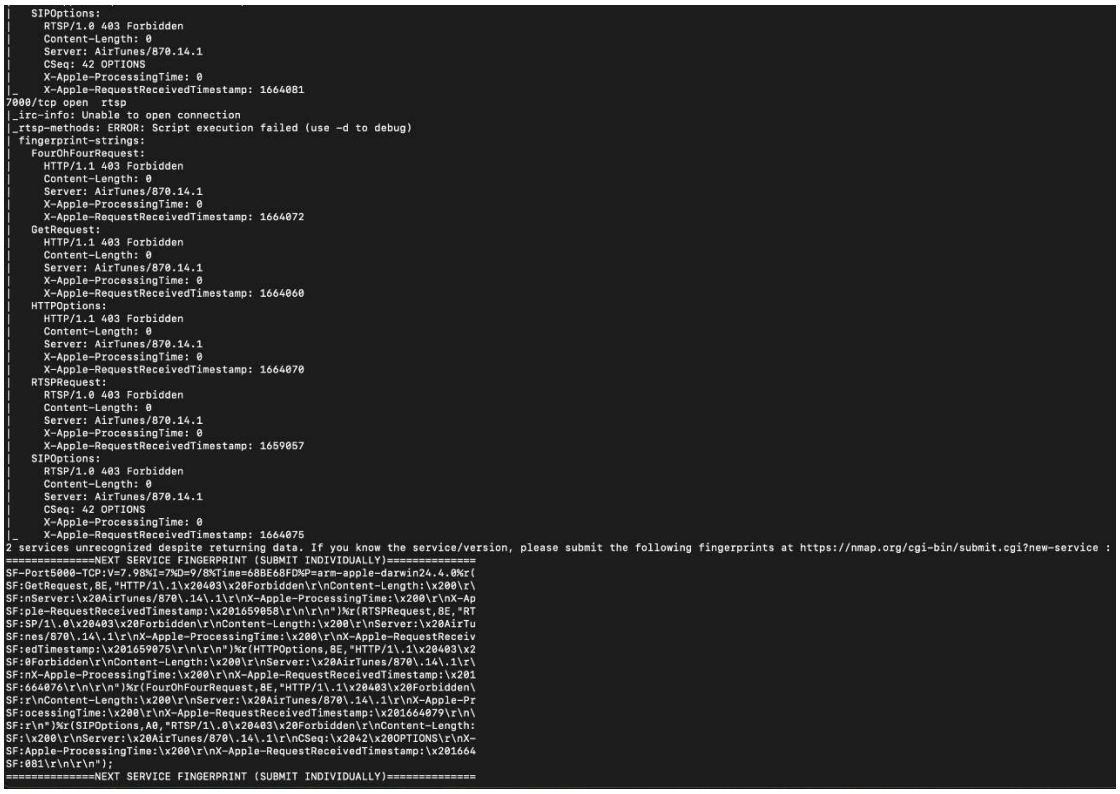
```
| smb2-time:
|   date: 2025-09-08T05:32:03
|_  start_date: N/A

NSE: Script Post-scanning.
Initiating NSE at 12:32
Completed NSE at 12:32, 0.00s elapsed
Initiating NSE at 12:32
Completed NSE at 12:32, 0.00s elapsed
Initiating NSE at 12:32
Completed NSE at 12:32, 0.00s elapsed
Read data files from: /opt/homebrew/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
ak1ra@Achiras-MacBook-Air ~ %
```

Only port 80 is suspicious because I open nginx, other like 445,135,139 is default of window

Attacker Notebook :

```
ak1ra@Achiras-MacBook-Air ~ % nmap -T4 -A -v localhost
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-08 12:26 +0700
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:26
Completed NSE at 12:26, 0.00s elapsed
Initiating NSE at 12:26
Completed NSE at 12:26, 0.00s elapsed
Initiating NSE at 12:26
Completed NSE at 12:26, 0.00s elapsed
Initiating Ping Scan at 12:26
Scanning localhost (127.0.0.1) [2 ports]
Completed Ping Scan at 12:26, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 12:26
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 5000/tcp on 127.0.0.1
Discovered open port 7000/tcp on 127.0.0.1
Completed Connect Scan at 12:26, 0.01s elapsed (1000 total ports)
Initiating Service scan at 12:26
Scanning 2 services on localhost (127.0.0.1)
Completed Service scan at 12:26, 18.53s elapsed (2 services on 1 host)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 12:26
Completed NSE at 12:26, 8.02s elapsed
Initiating NSE at 12:26
Completed NSE at 12:26, 0.00s elapsed
Initiating NSE at 12:26
Completed NSE at 12:26, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000016s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
5000/tcp open  rtsp
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/870.14.1
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 1664079
|   GetRequest:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/870.14.1
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 1659058
|   HTTPOptions:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/870.14.1
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 1664076
|   RTSPRequest:
|     RTSP/1.0 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/870.14.1
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 1659075
```



```
|   SIPOptions:
|     RTSP/1.0 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/870.14.1
|     CSeq: 42 OPTIONS
|     X-Apple-ProcessingTime: 0
|_    X-Apple-RequestReceivedTimestamp: 1664081
7000/tcp open  rtsp
|_irc-info: Unable to open connection
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/870.14.1
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 1664072
|   GetRequest:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/870.14.1
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 1664060
|   HTTPOptions:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/870.14.1
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 1664070
|   RTSPRequest:
|     RTSP/1.0 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/870.14.1
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 1659057
|   SIPOptions:
|     RTSP/1.0 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/870.14.1
|     CSeq: 42 OPTIONS
|     X-Apple-ProcessingTime: 0
|_    X-Apple-RequestReceivedTimestamp: 1664075
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5000-TCP:V=7.98%I=7%D=9/8%Time=68BE68FD%P=arm-apple-darwin24.4.0%r(
SF:GetRequest,8E,"HTTP/1\.1\x20403\x20Forbidden\r\nContent-Length:\x200\r\
SF:nServer:\x20AirTunes/870\.14\.1\r\nX-Apple-ProcessingTime:\x200\r\nX-Ap
SF:ple-RequestReceivedTimestamp:\x201659058\r\n\r\n")%r(RTSPRequest,8E,"RT
SF:SP/1\.0\x20403\x20Forbidden\r\nContent-Length:\x200\r\nServer:\x20AirTu
SF:nes/870\.14\.1\r\nX-Apple-ProcessingTime:\x200\r\nX-Apple-RequestReceiv
SF:edTimestamp:\x201659075\r\n\r\n")%r(HTTPOptions,8E,"HTTP/1\.1\x20403\x2
SF:0Forbidden\r\nContent-Length:\x200\r\nServer:\x20AirTunes/870\.14\.1\r\
SF:nX-Apple-ProcessingTime:\x200\r\nX-Apple-RequestReceivedTimestamp:\x201
SF:664076\r\n\r\n")%r(FourOhFourRequest,8E,"HTTP/1\.1\x20403\x20Forbidden\
SF:r\nContent-Length:\x200\r\nServer:\x20AirTunes/870\.14\.1\r\nX-Apple-Pr
SF:ocessingTime:\x200\r\nX-Apple-RequestReceivedTimestamp:\x201664079\r\n\
SF:r\n")%r(SIPOptions,A0,"RTSP/1\.0\x20403\x20Forbidden\r\nContent-Length:
SF:\x200\r\nServer:\x20AirTunes/870\.14\.1\r\nCSeq:\x2042\x20OPTIONS\r\nX-
SF:Apple-ProcessingTime:\x200\r\nX-Apple-RequestReceivedTimestamp:\x201664
SF:081\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
```

```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port7000-TCP:V=7.98%I=7%D=9/8%Time=68BE6901%P=arm-apple-darwin24.4.0%r(
SF:RTSPRequest,8E,"RTSP/1\.0\x20403\x20Forbidden\r\nContent-Length:\x200\r
SF:\nServer:\x20AirTunes/870\.14\.1\r\nX-Apple-ProcessingTime:\x200\r\nX-A
SF:pple-RequestReceivedTimestamp:\x201659057\r\n\r\n")%r(GetRequest,8E,"HT
SF:TP/1\.1\x20403\x20Forbidden\r\nContent-Length:\x200\r\nServer:\x20AirTu
SF:nes/870\.14\.1\r\nX-Apple-ProcessingTime:\x200\r\nX-Apple-RequestReceiv
SF:edTimestamp:\x201664060\r\n\r\n")%r(HTTPOptions,8E,"HTTP/1\.1\x20403\x2
SF:0Forbidden\r\nContent-Length:\x200\r\nServer:\x20AirTunes/870\.14\.1\r\
SF:nX-Apple-ProcessingTime:\x200\r\nX-Apple-RequestReceivedTimestamp:\x201
SF:664070\r\n\r\n")%r(FourOhFourRequest,8E,"HTTP/1\.1\x20403\x20Forbidden\
SF:r\nContent-Length:\x200\r\nServer:\x20AirTunes/870\.14\.1\r\nX-Apple-Pr
SF:ocessingTime:\x200\r\nX-Apple-RequestReceivedTimestamp:\x201664072\r\n\
SF:r\n")%r(SIPOptions,A0,"RTSP/1\.0\x20403\x20Forbidden\r\nContent-Length:
SF:\x200\r\nServer:\x20AirTunes/870\.14\.1\r\nCSeq:\x2042\x20OPTIONS\r\nX-
SF:Apple-ProcessingTime:\x200\r\nX-Apple-RequestReceivedTimestamp:\x201664
SF:075\r\n\r\n");

NSE: Script Post-scanning.
Initiating NSE at 12:26
Completed NSE at 12:26, 0.00s elapsed
Initiating NSE at 12:26
Completed NSE at 12:26, 0.00s elapsed
Initiating NSE at 12:26
Completed NSE at 12:26, 0.00s elapsed
Read data files from: /opt/homebrew/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.68 seconds
ak1ra@Achiras-MacBook-Air ~ %
```

Nothing suspicious, port 5000 and 7000 is default of macOS

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 : Its only provide two of them both of then are correct, which are

Linux of target VM :

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 17:d1:a1:f1:9d:88:92:7e:f1:67:65:7d:46:eb:f4:7f (ECDSA)
|_  256 b9:a3:d8:84:a9:44:19:71:0d:70:a6:74:78:bf:c2:34 (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Window of target notebook :

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          nginx 1.29.0
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.29.0
|_http-title: Welcome to nginx!
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

The one which is MacOS (attacker notebook) did not show.

Reason : namp using OS fingerprinting by sending specially crafted packet and analyzing how the target respond -> Nmap compares responses against its OS fingerprint database

And Linux VM responded a obvious fingerprint so easy so nmap, while Windows exposed multiple services -> which give much data easily identified as windows. The reason why MacOS did not show it might because it is localhost(which skip lot of step in network -> less data to identify), service not authenticate -> forbidden 403 so cant get response to analyze.

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

Ans : Scary a bit. So its easy for Hacker to identify which port is accessible. And might know our OS which can help hacker to plan how to hack our 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?

```
vboxuser@Ubuntu24:/var/log$ sudo cat apache2/access.log
127.0.0.1 - - [07/Sep/2025:05:42:12 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:141.0) Gecko/20100101 Firefox/141.0"
127.0.0.1 - - [07/Sep/2025:05:42:12 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:141.0) Gecko/20100101 Firefox/
141.0"
127.0.0.1 - - [07/Sep/2025:05:42:12 +0000] "GET /favicon.ico HTTP/1.1" 404 487 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:141.0) Gecko/20100101 Firefox/141.0"
127.0.0.1 - - [07/Sep/2025:05:49:14 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:141.0) Gecko/20100101 Firefox/141.0"
```

```
vboxuser@Ubuntu24:/var/log$ sudo tail -f  apache2/access.log
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "GET /favicon.ico HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "GET / HTTP/1.1" 200 10926 "-" "-"
192.168.1.102 - - [08/Sep/2025:06:16:48 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safa
ri/605.1.15"
192.168.1.102 - - [08/Sep/2025:06:16:51 +0000] "GET / HTTP/1.1" 200 3459 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safa
ri/605.1.15"
192.168.1.100 - - [08/Sep/2025:06:16:59 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/5
37.36 Edg/140.0.0.0"
192.168.1.100 - - [08/Sep/2025:06:17:51 +0000] "-" 408 0 "-" "-"
SSS
```

127.0.0.1 : vm localhost

192.168.1.102 : attacker notebook (MacOS)

192.168.1.100 : target notebook (Windows)

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.

```
vboxuser@Ubuntu24:/var/log$ sudo cat apache2/access.log | grep Nmap
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "GET /nmaplowercheck1757308937 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "PROPFIND / HTTP/1.1" 405 523 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "PROPFIND / HTTP/1.1" 405 523 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "GET /robots.txt HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "GET /.git/HEAD HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "POST /sdk HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "GET /evox/about HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "WPVO / HTTP/1.1" 501 498 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "PROPFIND / HTTP/1.1" 405 523 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "GET /HNAP1 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "GET /favicon.ico HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:05:22:19 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

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 :

```
ak1ra@Achiras-MacBook-Air ~ % nmap -T4 -A -v 192.168.1.122
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-08 13:45 +0700
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:45
Completed NSE at 13:45, 0.00s elapsed
Initiating NSE at 13:45
Completed NSE at 13:45, 0.00s elapsed
Initiating NSE at 13:45
Completed NSE at 13:45, 0.00s elapsed
Initiating Ping Scan at 13:45
Scanning 192.168.1.122 [2 ports]
Completed Ping Scan at 13:45, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:45
Completed Parallel DNS resolution of 1 host. at 13:45, 0.50s elapsed
Initiating Connect Scan at 13:45
Scanning 192.168.1.122 [1000 ports]
Discovered open port 80/tcp on 192.168.1.122
Completed Connect Scan at 13:46, 48.37s elapsed (1000 total ports)
Initiating Service scan at 13:46
Scanning 1 service on 192.168.1.122
Completed Service scan at 13:46, 6.03s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.1.122.
Initiating NSE at 13:46
Completed NSE at 13:46, 5.02s elapsed
Initiating NSE at 13:46
Completed NSE at 13:46, 0.04s elapsed
Initiating NSE at 13:46
Completed NSE at 13:46, 0.00s elapsed
Nmap scan report for 192.168.1.122
Host is up (0.0052s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD

NSE: Script Post-scanning.
Initiating NSE at 13:46
Completed NSE at 13:46, 0.00s elapsed
Initiating NSE at 13:46
Completed NSE at 13:46, 0.00s elapsed
Initiating NSE at 13:46
Completed NSE at 13:46, 0.00s elapsed
Read data files from: /opt/homebrew/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.16 seconds
ak1ra@Achiras-MacBook-Air ~ %
```

Port open results changed : port 22/tcp gone as designed

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 : same as part 2

```
vboxuser@Ubuntu24:/var/log$ sudo tail -f  apache2/access.log
sudo: unable to resolve host Ubuntu24: Temporary failure in name resolution
192.168.1.102 - - [08/Sep/2025:06:46:11 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:06:46:11 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:06:46:11 +0000] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:06:46:11 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:06:46:11 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:06:46:11 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:06:46:12 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:06:46:12 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.102 - - [08/Sep/2025:06:46:15 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
192.168.1.102 - - [08/Sep/2025:06:46:16 +0000] "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 : Firewall is not sufficient, cuz it only work on packet-level rules (IP, port, protocol). They cannot tell whether a packet is from a real browser or from nmap.

Solution : use whitelist (for internal or allowed device) combined with Proxy/ CDN so scanner can only scan Proxy or CDN not the real device or server.

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

Ans :

```
vboxuser@Ubuntu24:/var/log$ sudo iptables -L
sudo: unable to resolve host Ubuntu24: Temporary failure in name resolution
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  192.168.1.100        anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

หมายเหตุ : ที่เห็นมี tcp anywhere 2 อัน เพราะผมพิมคำสั่งเหมือนกันสองรอบ มีผลเหมือนกับมีบรรทัดเดียว