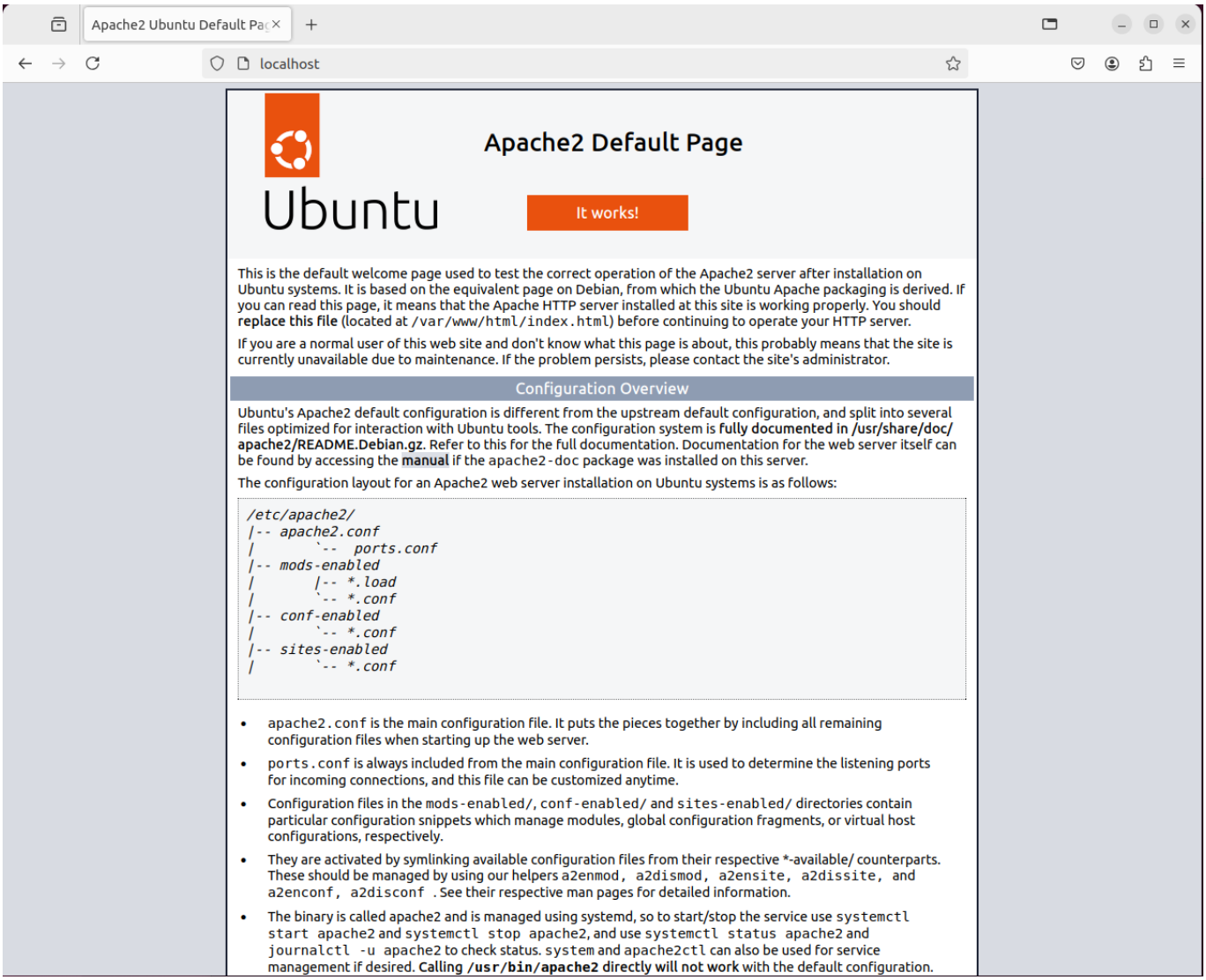
Activity: Recon and Defense (Network Security I)

```
Attacker IP (Thanat Wongsamut 6432067021): 10.144.0.3
Target IP: 10.144.0.101
VM IP: 10.144.0.100
```

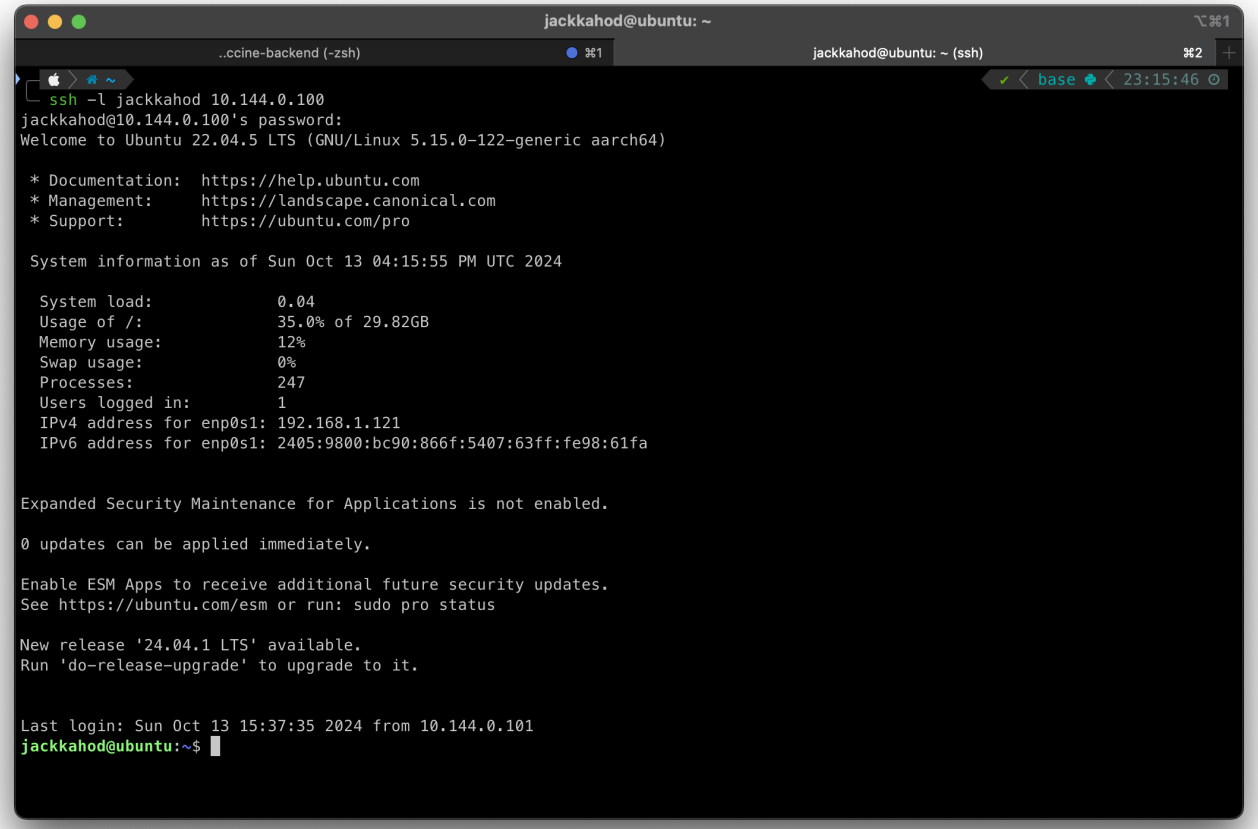
Part I: Prepare your target

Test 1: Use a browser in your target VM to visit the web server on the target VM.

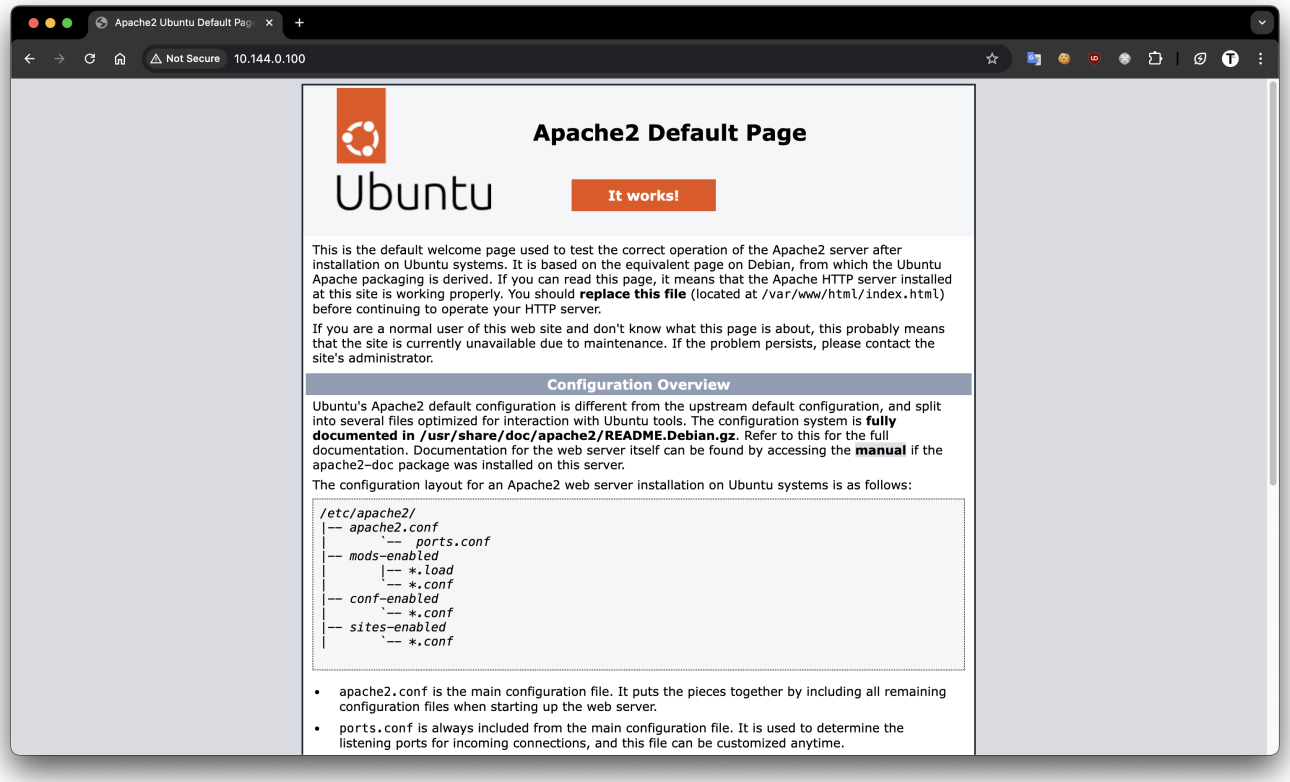


Test 2: Use a browser in your target notebook (notebook 1) to visit the web server on the VM. If you cannot reach the web server, modify your VM network settings in VirtualBox to "Bridge". Google for how to modify the setting if you cannot find it in VirtualBox.

Test 3: Test that the ssh server on your VM is available by running ssh from the target notebook. Mac users may use Terminal. Windows users need to use putty, cygwin, CMDer, WSL, etc.

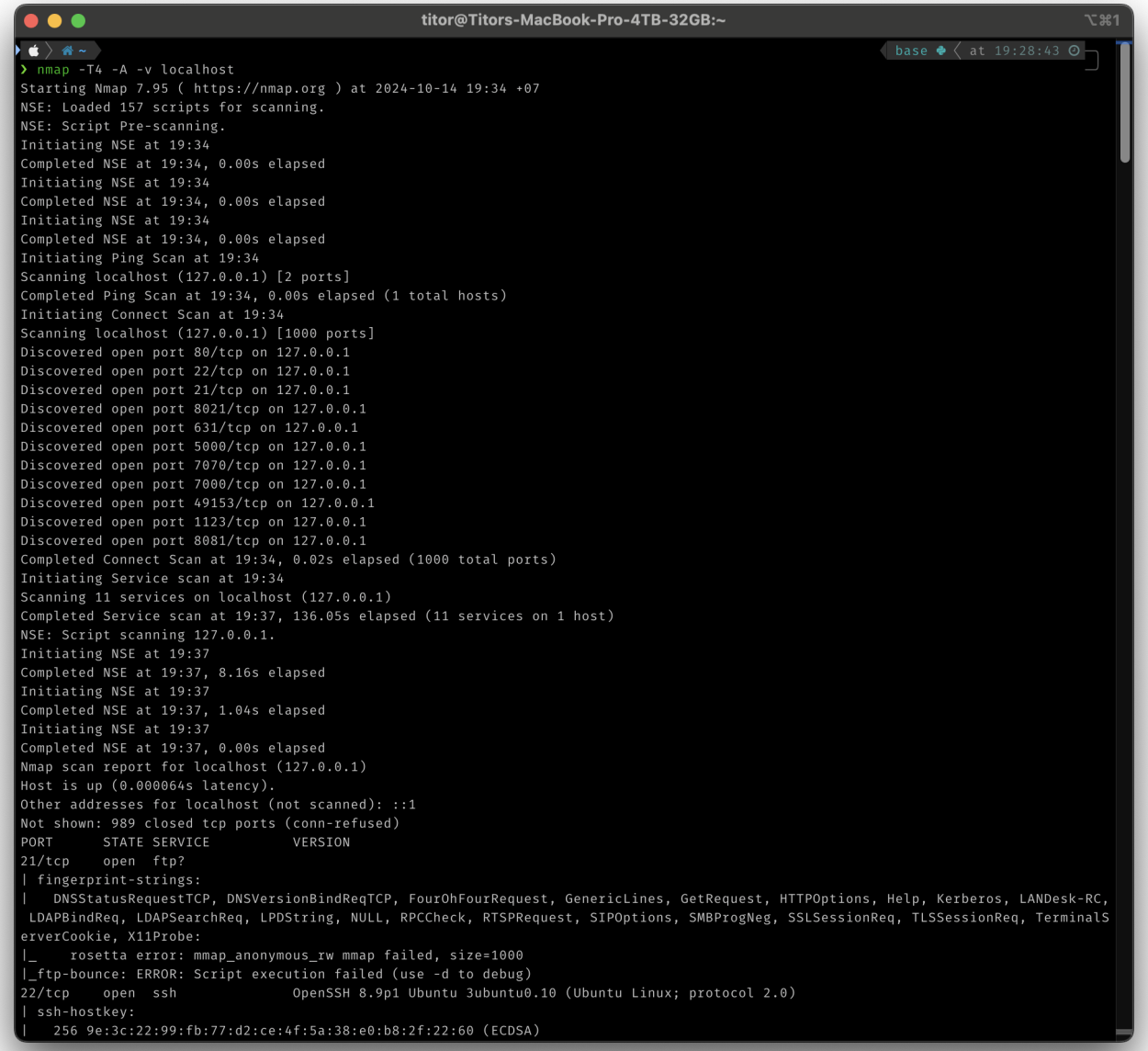


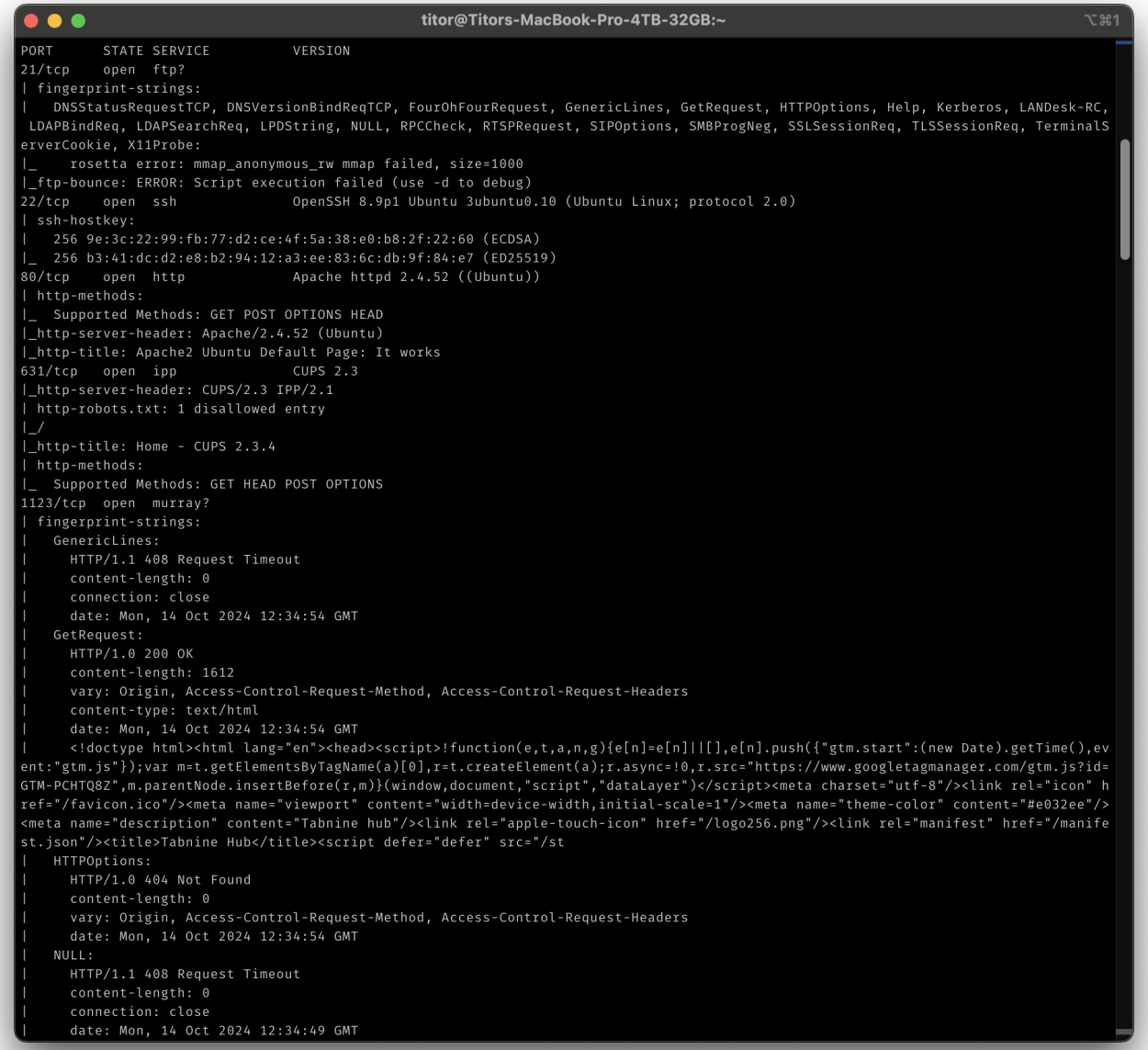
Test 4: Test that the attacker can access the web server on your VM. Use a browser in your attacker notebook (notebook 2) to visit the web server on the VM.



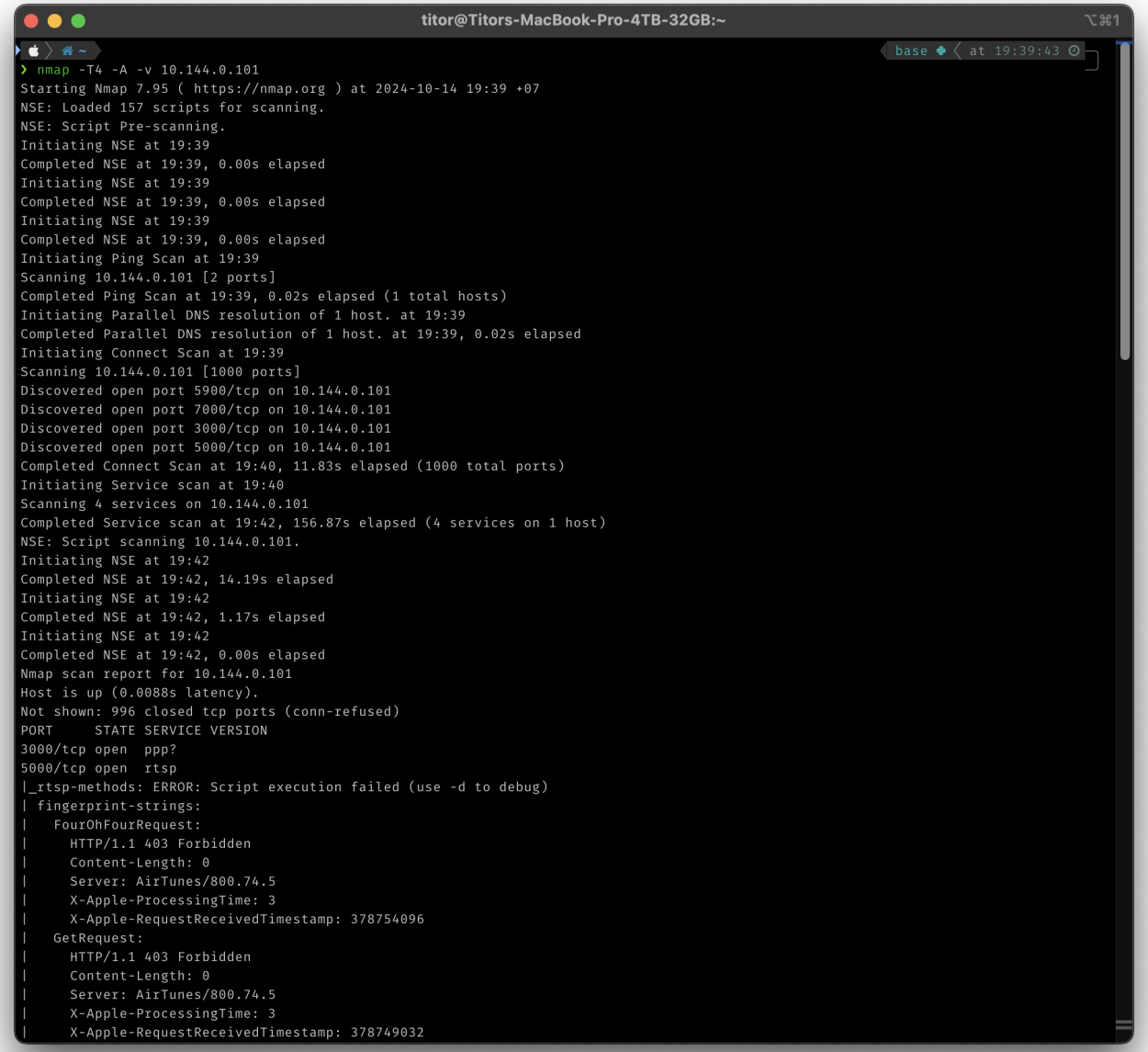
Part II. Reconnaissance

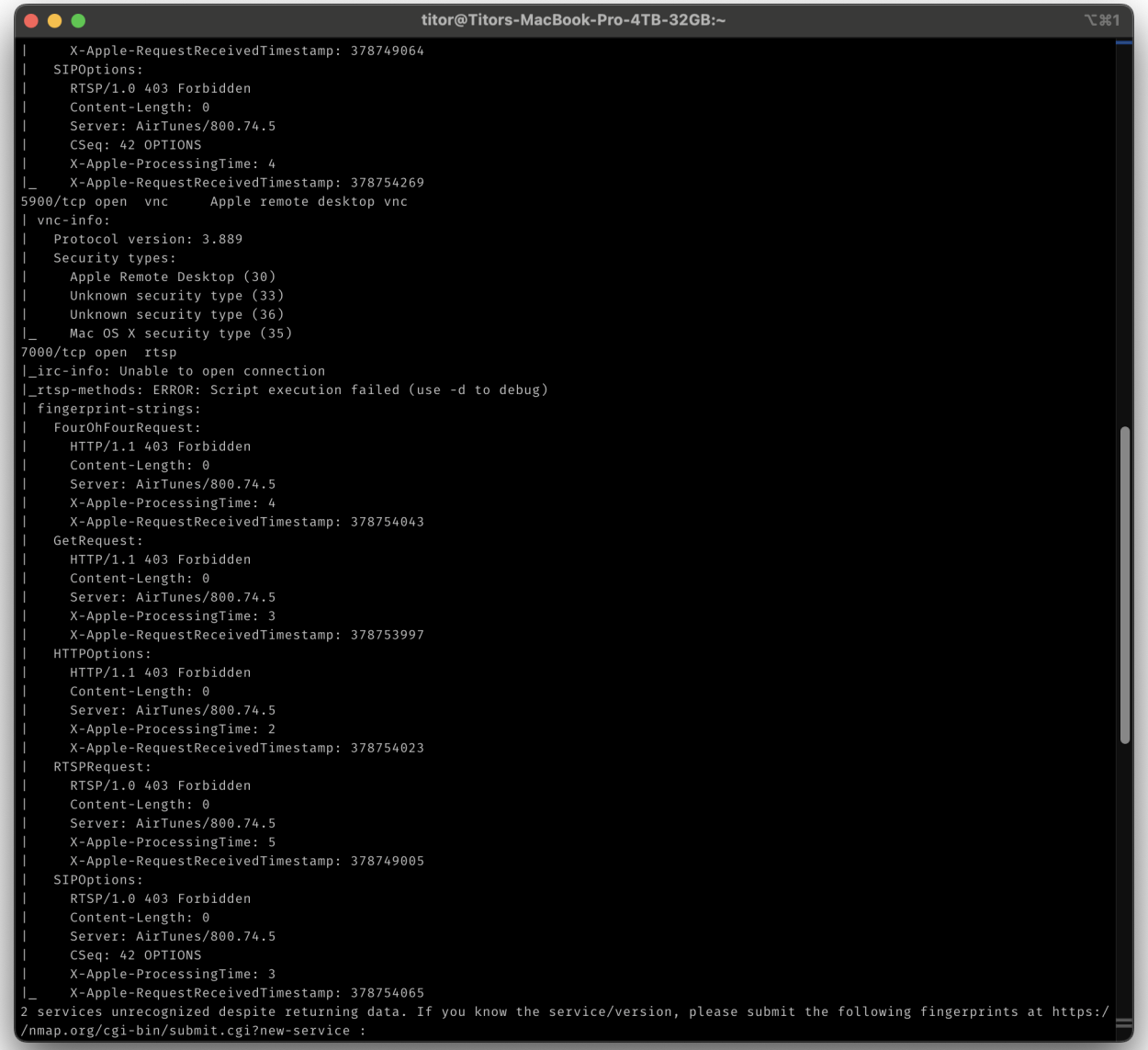
Run nmap from the attacker notebook against itself (localhost).




titor@Titors-MacBook-Pro-4TB-32GB:~
⌥⌘1
PORT   STATE SERVICE   VERSION
21/tcp   open ftp?
| fingerprint-strings:
| DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LANDesk-RC,
 LDAPBindReq, LDAPSearchReq, LPDString, NULL, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalS
erverCookie, X11Probe:
|_   rosetta error: mmap_anonymous_rw mmap failed, size=1000
|_ftp-bounce: ERROR: Script execution failed (use -d to debug)
22/tcp   open ssh   OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 9e:3c:22:99:fb:77:d2:ce:4f:5a:38:e0:b8:2f:22:60 (ECDSA)
|_ 256 b3:41:dc:d2:e8:b2:94:12:a3:ee:83:6c:db:9f:84:e7 (ED25519)
80/tcp   open http   Apache httpd 2.4.52 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
631/tcp   open ipp   CUPS 2.3
|_http-server-header: CUPS/2.3 IPP/2.1
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 2.3.4
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
1123/tcp open murray?
| fingerprint-strings:
| GenericLines:
| HTTP/1.1 408 Request Timeout
| content-length: 0
| connection: close
| date: Mon, 14 Oct 2024 12:34:54 GMT
| GetRequest:
| HTTP/1.0 200 OK
| content-length: 1612
| vary: Origin, Access-Control-Request-Method, Access-Control-Request-Headers
| content-type: text/html
| date: Mon, 14 Oct 2024 12:34:54 GMT
| <!doctype html><html lang="en"><head><script>!function(e,t,a,n,g){e[n]=e[n]||[],e[n].push({"gtm.start":(new Date).getTime(),ev
ent:"gtm.js"});var m=t.getElementsByTagName(a)[0],r=t.createElement(a);r.async=!0,r.src="https://www.googletagmanager.com/gtm.js?id=
GTM-PCHTQ8Z",m.parentNode.insertBefore(r,m)}(window,document,"script","dataLayer")</script><meta charset="utf-8"/><link rel="icon" h
ref="/favicon.ico"/><meta name="viewport" content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#e032ee"/>
<meta name="description" content="Tabnine hub"/><link rel="apple-touch-icon" href="/logo256.png"/><link rel="manifest" href="/manife
st.json"/><title>Tabnine Hub</title><script defer="defer" src="/st
| HTTPOptions:
| HTTP/1.0 404 Not Found
| content-length: 0
| vary: Origin, Access-Control-Request-Method, Access-Control-Request-Headers
| date: Mon, 14 Oct 2024 12:34:54 GMT
| NULL:
| HTTP/1.1 408 Request Timeout
| content-length: 0
| connection: close
| date: Mon, 14 Oct 2024 12:34:49 GMT

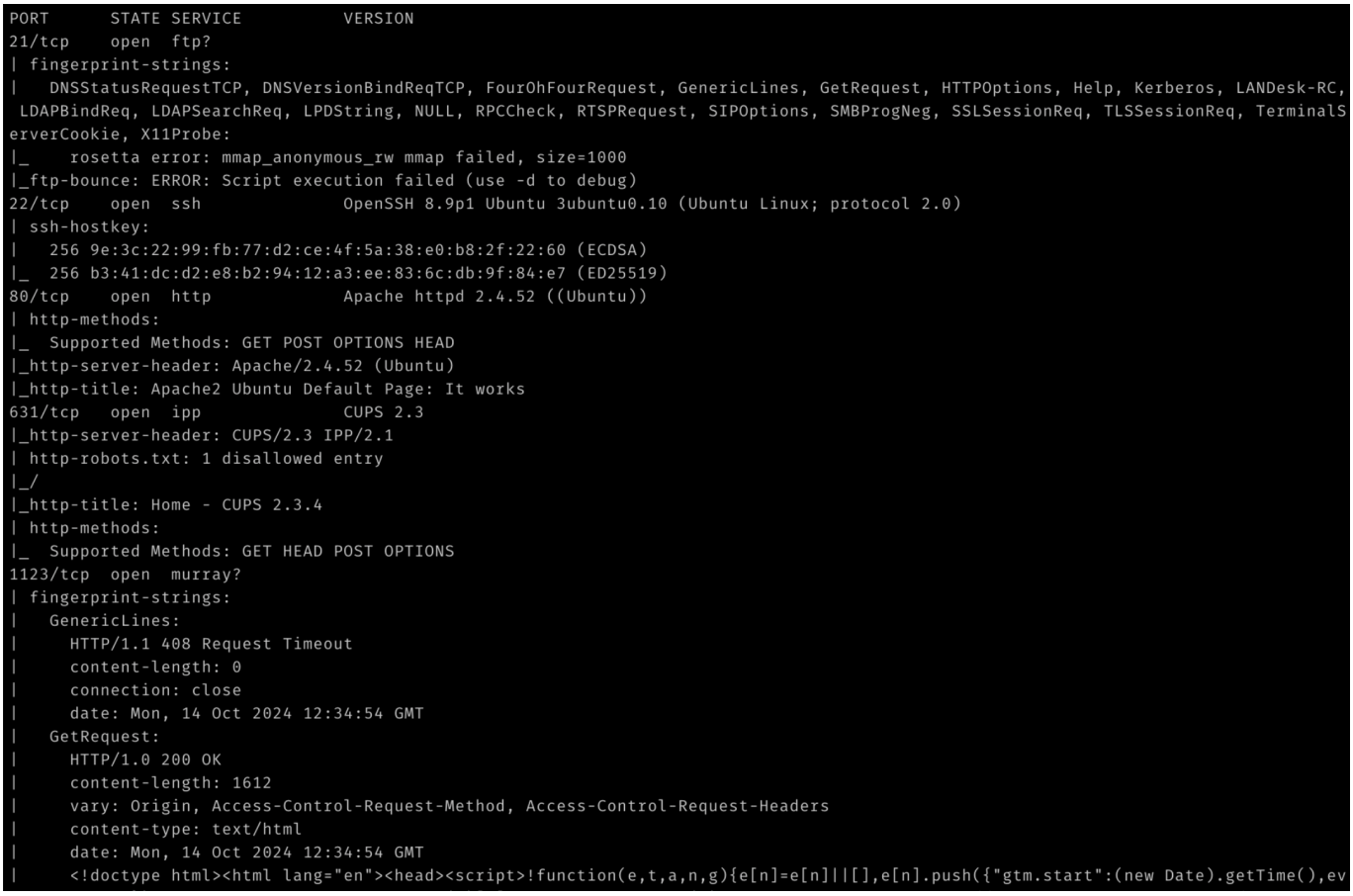
Run nmap from the attacker notebook against the target notebook (not the VM, but the host).




titor@Titors-MacBook-Pro-4TB-32GB:~
⌥⌘1
| X-Apple-RequestReceivedTimestamp: 378749064
| SIPOptions:
| RTSP/1.0 403 Forbidden
| Content-Length: 0
| Server: AirTunes/800.74.5
| CSeq: 42 OPTIONS
| X-Apple-ProcessingTime: 4
|_   X-Apple-RequestReceivedTimestamp: 378754269
5900/tcp open vnc   Apple remote desktop vnc
| vnc-info:
| Protocol version: 3.889
| Security types:
| Apple Remote Desktop (30)
| Unknown security type (33)
| Unknown security type (36)
|_   Mac OS X security type (35)
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/800.74.5
| X-Apple-ProcessingTime: 4
| X-Apple-RequestReceivedTimestamp: 378754043
| GetRequest:
| HTTP/1.1 403 Forbidden
| Content-Length: 0
| Server: AirTunes/800.74.5
| X-Apple-ProcessingTime: 3
| X-Apple-RequestReceivedTimestamp: 378753997
| HTTPOptions:
| HTTP/1.1 403 Forbidden
| Content-Length: 0
| Server: AirTunes/800.74.5
| X-Apple-ProcessingTime: 2
| X-Apple-RequestReceivedTimestamp: 378754023
| RTSPRequest:
| RTSP/1.0 403 Forbidden
| Content-Length: 0
| Server: AirTunes/800.74.5
| X-Apple-ProcessingTime: 5
| X-Apple-RequestReceivedTimestamp: 378749005
| SIPOptions:
| RTSP/1.0 403 Forbidden
| Content-Length: 0
| Server: AirTunes/800.74.5
| CSeq: 42 OPTIONS
| X-Apple-ProcessingTime: 3
|_   X-Apple-RequestReceivedTimestamp: 378754065
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 :

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?

Attacker notebook:



```
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LANDesk-RC,
 LDAPBindReq, LDAPSearchReq, LPDString, NULL, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalS
erverCookie, X11Probe:
|_    rosetta error: mmap_anonymous_rw mmap failed, size=1000
|_ftp-bounce: ERROR: Script execution failed (use -d to debug)
22/tcp    open  ssh              OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 9e:3c:22:99:fb:77:d2:ce:4f:5a:38:e0:b8:2f:22:60 (ECDSA)
|_  256 b3:41:dc:d2:e8:b2:94:12:a3:ee:83:6c:db:9f:84:e7 (ED25519)
80/tcp    open  http             Apache httpd 2.4.52 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
631/tcp   open  ipp              CUPS 2.3
|_http-server-header: CUPS/2.3 IPP/2.1
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 2.3.4
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
1123/tcp  open  murray?
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 408 Request Timeout
|     content-length: 0
|     connection: close
|     date: Mon, 14 Oct 2024 12:34:54 GMT
|   GetRequest:
|     HTTP/1.0 200 OK
|     content-length: 1612
|     vary: Origin, Access-Control-Request-Method, Access-Control-Request-Headers
|     content-type: text/html
|     date: Mon, 14 Oct 2024 12:34:54 GMT
|     <!doctype html><html lang="en"><head><script>!function(e,t,a,n,g){e[n]=e[n]||[],e[n].push({"gtm.start":(new Date).getTime(),ev
```

1. **Port 21 (FTP)**:
    - Risky to have open; potential security issue due to cleartext data transmission and possible configuration issues.
2. **Port 1123 (Murray?)**:
    - Unusual service; identified as "Murray?" with web-like responses indicating "Tabnine Hub." Could be a rogue or misconfigured service.
3. **Other Open Ports (22, 80, 631)**:
    - Standard services (SSH, HTTP, CUPS), but still need securing:
        - **SSH (22)**: Restrict access, use key-based authentication.
        - **HTTP (80)**: Verify necessity of the web server.
        - **IPP/CUPS (631)**: Disable if not used for printing.

Target notebook:

```
PORT     STATE SERVICE VERSION
3000/tcp open  ppp?
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/800.74.5
|     X-Apple-ProcessingTime: 3
|     X-Apple-RequestReceivedTimestamp: 378754096
|   GetRequest:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/800.74.5
|     X-Apple-ProcessingTime: 3
|     X-Apple-RequestReceivedTimestamp: 378749032
```

```
5900/tcp open  vnc     Apple remote desktop vnc
| vnc-info:
|   Protocol version: 3.889
|   Security types:
|     Apple Remote Desktop (30)
|     Unknown security type (33)
|     Unknown security type (36)
|_    Mac OS X security type (35)
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/800.74.5
|     X-Apple-ProcessingTime: 4
|     X-Apple-RequestReceivedTimestamp: 378754043
|   GetRequest:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/800.74.5
|     X-Apple-ProcessingTime: 3
|     X-Apple-RequestReceivedTimestamp: 378753997
|   HTTPOptions:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/800.74.5
|     X-Apple-ProcessingTime: 2
|     X-Apple-RequestReceivedTimestamp: 378754023
|   RTSPRequest:
|     RTSP/1.0 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/800.74.5
|     X-Apple-ProcessingTime: 5
|     X-Apple-RequestReceivedTimestamp: 378749005
|   SIPOptions:
|     RTSP/1.0 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/800.74.5
|     CSeq: 42 OPTIONS
|     X-Apple-ProcessingTime: 3
|_    X-Apple-RequestReceivedTimestamp: 378754065
```

- **Port 5000 and 7000**:
  - Associated with the **AirTunes protocol**, used for wireless music streaming.
- **Port 3000**:
  - Port 3000 is running the project web app
- **Port 5900 (VNC)**:
  - Associated with **Virtual Network Computing (VNC)**, allowing for remote desktop access.

VM:

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 5a:3e:aa:10:0c:a3:ad:51:8b:5e:fa:d9:a5:88:8c:35 (ECDSA)
|_  256 ee:1c:2b:88:c5:0c:16:4c:c3:7e:d9:2f:45:ae:86:1f (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- **Port 22, 80**:
    - Same as Attacker notebook Port (SSH Port and HTTP Port)

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

- **Attacker Notebook**:
    - Nmap provides accurate information about the operating system and the open ports.
- **Target Notebook**:
    - The detected **open port 5900** (VNC) is noted as potentially abnormal. It may appear open but doesn't have an application actively running on it.
    - This could indicate a configuration issue or leftover settings from previous installations. If VNC is not intentionally set up, this may be a vulnerability.
- **Target Linux VM**:
    - The OS information matches expectations, with open ports reflecting typical services (SSH, HTTP).

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

Ans

Using Nmap to gather information about devices on a network can indeed be concerning. The level of detail it provides such as open ports, operating system versions, and service information can expose potential vulnerabilities.

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?

```
jackkahod@ubuntu: ~
jackkahod@ubuntu:~$ cat /var/log/apache2/access.log

127.0.0.1 - - [14/Oct/2024:12:33:28 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0"
127.0.0.1 - - [14/Oct/2024:12:33:28 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0"
127.0.0.1 - - [14/Oct/2024:12:33:28 +0000] "GET /favicon.ico HTTP/1.1" 404 487 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0"
10.144.0.101 - - [14/Oct/2024:12:33:57 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36"
10.144.0.101 - - [14/Oct/2024:12:33:57 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://10.144.0.100/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36"
10.144.0.101 - - [14/Oct/2024:12:33:57 +0000] "GET /favicon.ico HTTP/1.1" 404 490 "http://10.144.0.100/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36"
10.144.0.3 - - [14/Oct/2024:12:34:21 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36"
10.144.0.3 - - [14/Oct/2024:12:34:21 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://10.144.0.100/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36"
10.144.0.101 - - [14/Oct/2024:12:34:48 +0000] "-" 408 0 "-" "-"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /robots.txt HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "PROPFIND / HTTP/1.1" 405 522 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /nmaplowercheck1728909828 HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "PROPFIND / HTTP/1.1" 405 522 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /.git/HEAD HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "POST /sdk HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "MTBA / HTTP/1.1" 501 497 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "PROPFIND / HTTP/1.1" 405 522 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /HNAP1 HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /favicon.ico HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /evox/about HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET / HTTP/1.1" 200 10926 "-" "-"
jackkahod@ubuntu:~$
```

From the **access.log** file for the web server on the Linux VM, the following IP addresses were observed accessing the web server:

- **IP Address**: `127.0.0.1`
    - **Device**: This is the localhost address.
- **IP Address**: `10.144.0.3`
    - **Device**: This IP belongs to the attacker's notebook.

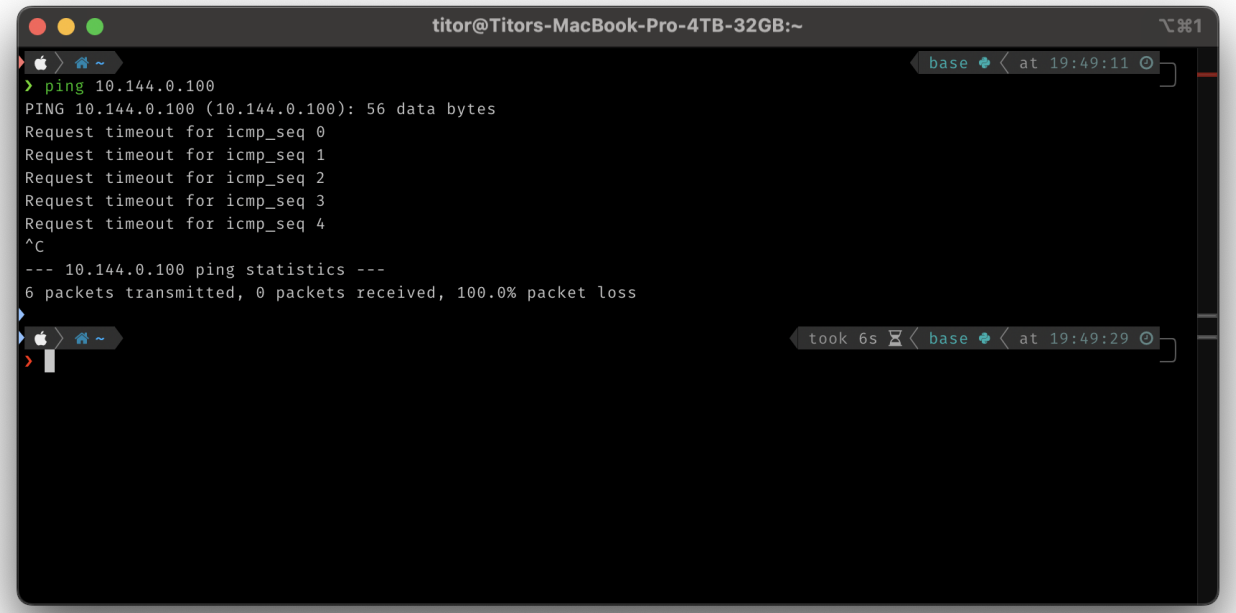
Q5. Find the nmap scan in the web server log. Copy the lines from the log file that were created because of the nmap scan.

```
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /robots.txt HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "PROPFIND / HTTP/1.1" 405 522 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /nmaplowercheck1728909828 HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "PROPFIND / HTTP/1.1" 405 522 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /.git/HEAD HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "POST /sdk HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "MTBA / HTTP/1.1" 501 497 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "PROPFIND / HTTP/1.1" 405 522 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /HNAP1 HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /favicon.ico HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET /evox/about HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
10.144.0.3 - - [14/Oct/2024:12:43:48 +0000] "GET / HTTP/1.1" 200 10926 "-" "-"
```

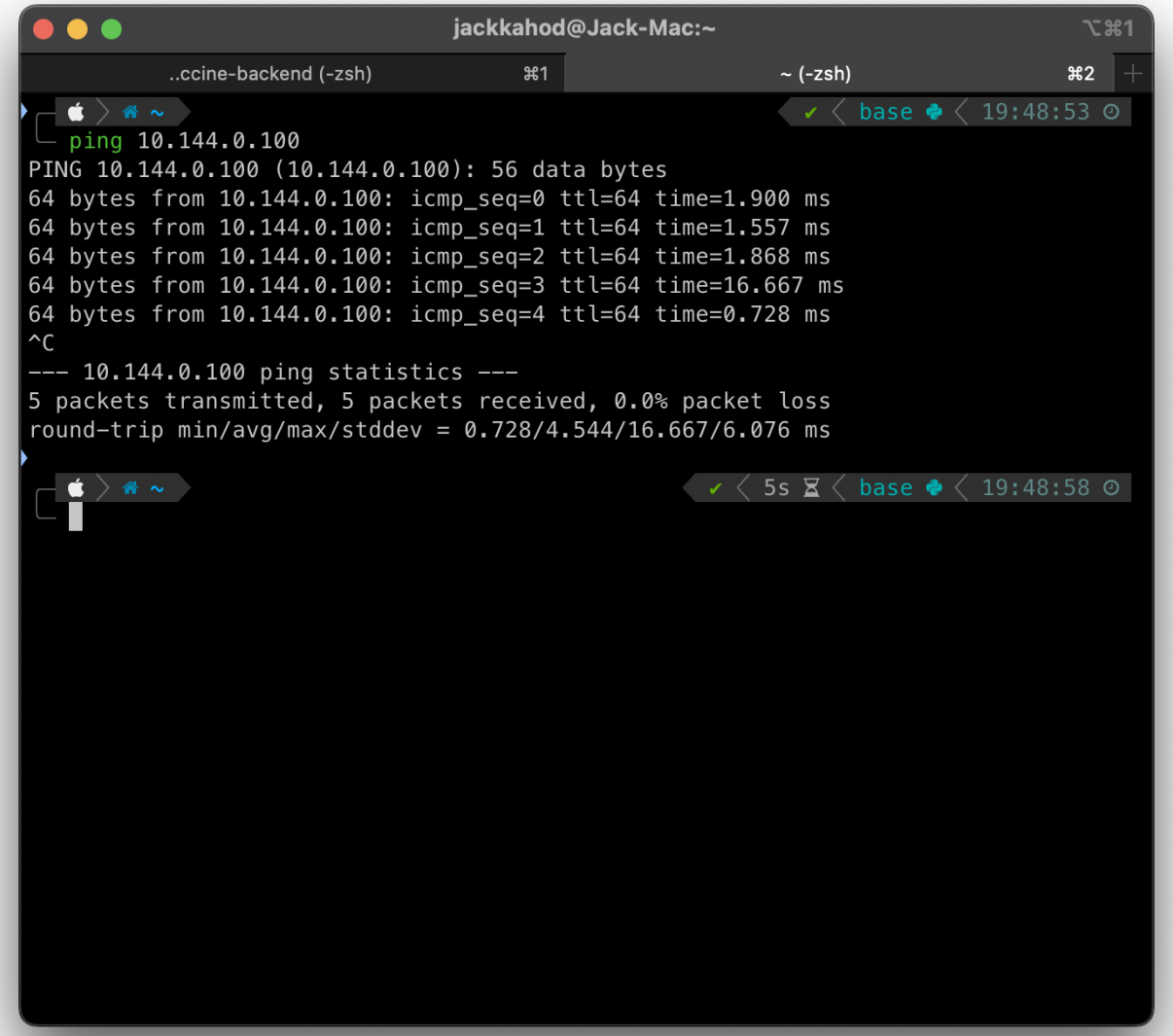
Part III. Defense

Test 1: Ping your VM from your two notebooks. You should not see any responses.

Attacker notebook:



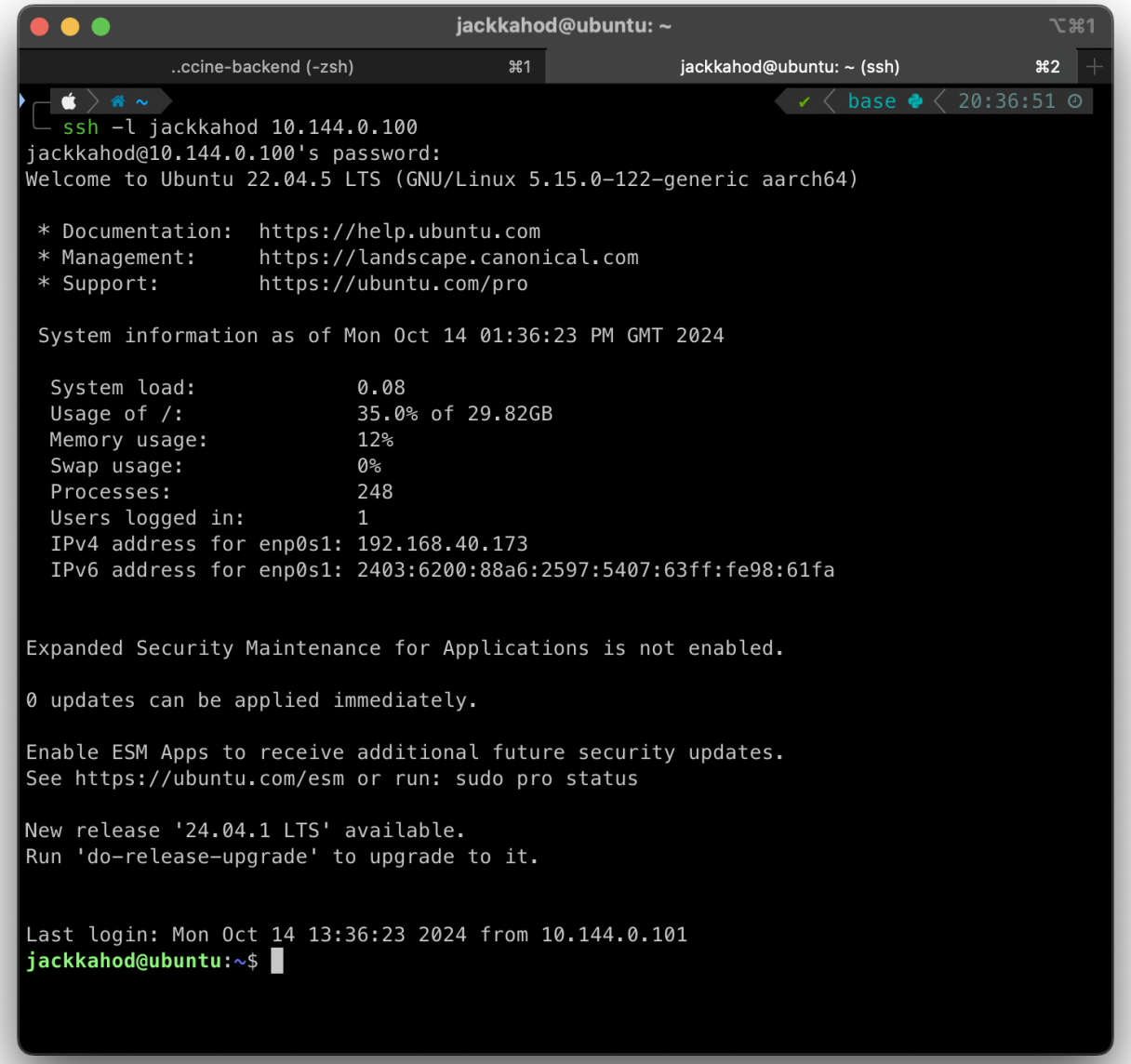
Target notebook:



Test 2: Access the web server on your VM from your browser on your 2 notebooks. You should be able to get the same web page as before.

Yes, still got the same webpage

Test 3: ssh from your target notebook (notebook 1) into the VM. You should be able to get the same results as before.



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

Before Firewall:

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 5a:3e:aa:10:0c:a3:ad:51:8b:5e:fa:d9:a5:88:8c:35 (ECDSA)
|_  256 ee:1c:2b:88:c5:0c:16:4c:c3:7e:d9:2f:45:ae:86:1f (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

After Firewall:

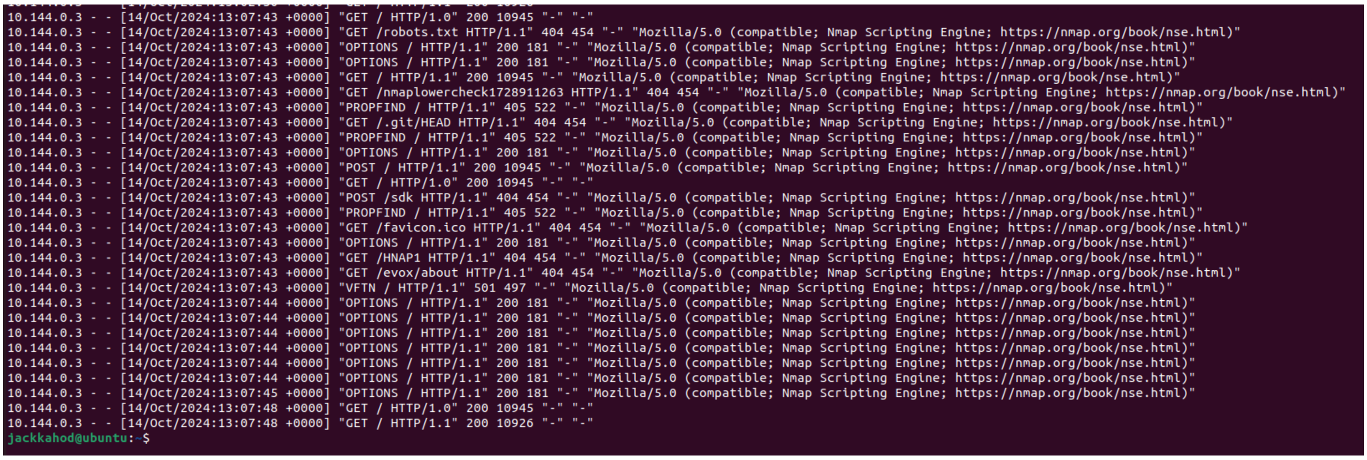
```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD

NSE: Script Post-scanning.
Initiating NSE at 20:07
Completed NSE at 20:07, 0.00s elapsed
Initiating NSE at 20:07
Completed NSE at 20:07, 0.00s elapsed
Initiating NSE at 20:07
Completed NSE at 20:07, 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 63.64 seconds
```

The new Nmap scan results indicated that port 22 (SSH) is no longer visible to the scan, suggesting that the iptables rules effectively blocked access to this port.

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

After running the second Nmap scan, it was observed that Nmap was still able to detect that Apache HTTPD was running on the server.



```
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "GET /robots.txt HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "GET /nmaplowercheck1728911263 HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "PROPFIND / HTTP/1.1" 405 522 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "GET /.git/HEAD HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "PROPFIND / HTTP/1.1" 405 522 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "POST /sdk HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "PROPFIND / HTTP/1.1" 405 522 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "GET /favicon.ico HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "GET /HNAP1 HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "GET /evox/about HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:43 +0000] "VFTN / HTTP/1.1" 501 497 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:44 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:44 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:44 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:44 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:44 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:44 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:45 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.144.0.3 - - [14/Oct/2024:13:07:48 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
10.144.0.3 - - [14/Oct/2024:13:07:48 +0000] "GET / HTTP/1.1" 200 10926 "-" "-"
jackkahod@ubuntu:~$
```

- **Access Log Consistency**: The access logs from the web server remained the same as those recorded in Part II.

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

- **Inability to Fully Restrict Access**: It's impossible to prevent Nmap from accessing the web server while allowing legitimate users. Essential ports must remain open, which Nmap can exploit.
- **Limitations of Firewalls**: A firewall alone is not enough, as it can only control traffic based on rules without discerning intent.
- **Need for Additional Measures**:
    - **Traffic Analysis Tools** can identify and block suspicious patterns.
    - **Whitelisting** limits access to trusted IP addresses, reducing exposure to scans.

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