

Activity: Recon and Defense (Network Security I)

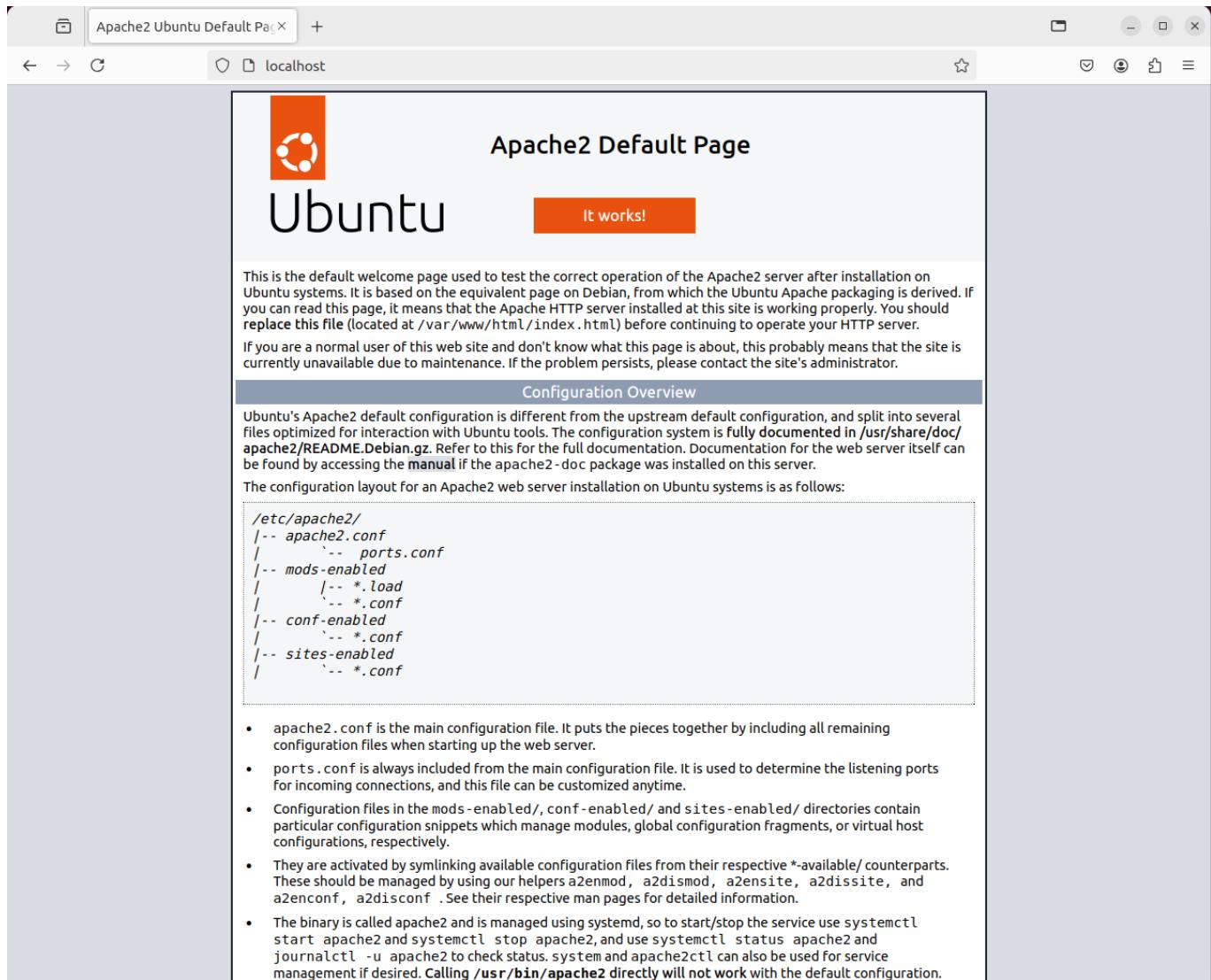
Attacker IP (Thanat Wongsamut 6432067021): 10.144.0.3

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.



The screenshot shows a web browser window with the title "Apache2 Ubuntu Default Page". The address bar shows "localhost". The page content includes the Ubuntu logo, the text "Apache2 Default Page", and a button labeled "It works!". Below this, there is a message about the default welcome page and a "Configuration Overview" section. The configuration overview details the layout of the Apache2 configuration files in /etc/apache2, listing the main configuration file (apache2.conf), ports configuration (ports.conf), and various modules and site configurations in mods-enabled, conf-enabled, and sites-enabled directories. A bulleted list explains the purpose of each type of configuration file.

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.load
|   '-- *.conf
|-- conf-enabled
|   '-- *.conf
|-- sites-enabled
|   '-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2` and is managed using `systemd`, so to start/stop the service use `systemctl start apache2` and `systemctl stop apache2`, and use `systemctl status apache2` and `journalctl -u apache2` to check status. `systemctl` and `apache2ctl` can also be used for service management if desired. Calling `/usr/bin/apache2` directly will not work with the default configuration.

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.

The screenshot shows a web browser window with the URL `10.144.0.100` in the address bar. The page title is "Apache2 Default Page" with the Ubuntu logo. A red button says "It works!". Below the title, there is a message about the default welcome page and instructions to replace the file if needed. A section titled "Configuration Overview" provides details on the configuration layout, listing files like `/etc/apache2/apache2.conf`, `/etc/apache2/mods-enabled/*.load`, `/etc/apache2/conf-enabled/*.conf`, and `/etc/apache2/sites-enabled/*.conf`. A bulleted list at the bottom explains the functions of these files.

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.load
|   '-- *.conf
|-- conf-enabled
|   '-- *.conf
|-- sites-enabled
|   '-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

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.

The screenshot shows a macOS terminal window with two tabs. The active tab, labeled 'jackkahod@ubuntu: ~', displays the output of an SSH session to an Ubuntu 22.04 LTS VM. The session starts with a password prompt and a welcome message. It then provides system information, including load average (0.04), memory usage (12%), swap usage (0%), and process count (247). Network interfaces are listed with their respective IPv4 and IPv6 addresses. A note about ESM Apps is present, followed by a message about a new release ('24.04.1 LTS') available for upgrade. The last login information is shown, and the prompt ends with '\$'. The other tab, labeled 'jackkahod@ubuntu: ~ (ssh)', is visible in the background.

```
ssh -l jackkahod 10.144.0.100
jackkahod@10.144.0.100's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-122-generic aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Sun Oct 13 04:15:55 PM UTC 2024

System load:          0.04
Usage of /:           35.0% of 29.82GB
Memory usage:         12%
Swap usage:           0%
Processes:            247
Users logged in:     1
IPv4 address for enp0s1: 192.168.1.121
IPv6 address for enp0s1: 2405:9800:bc90:866f:5407:63ff:fe98:61fa

Expanded Security Maintenance for Applications is not enabled.

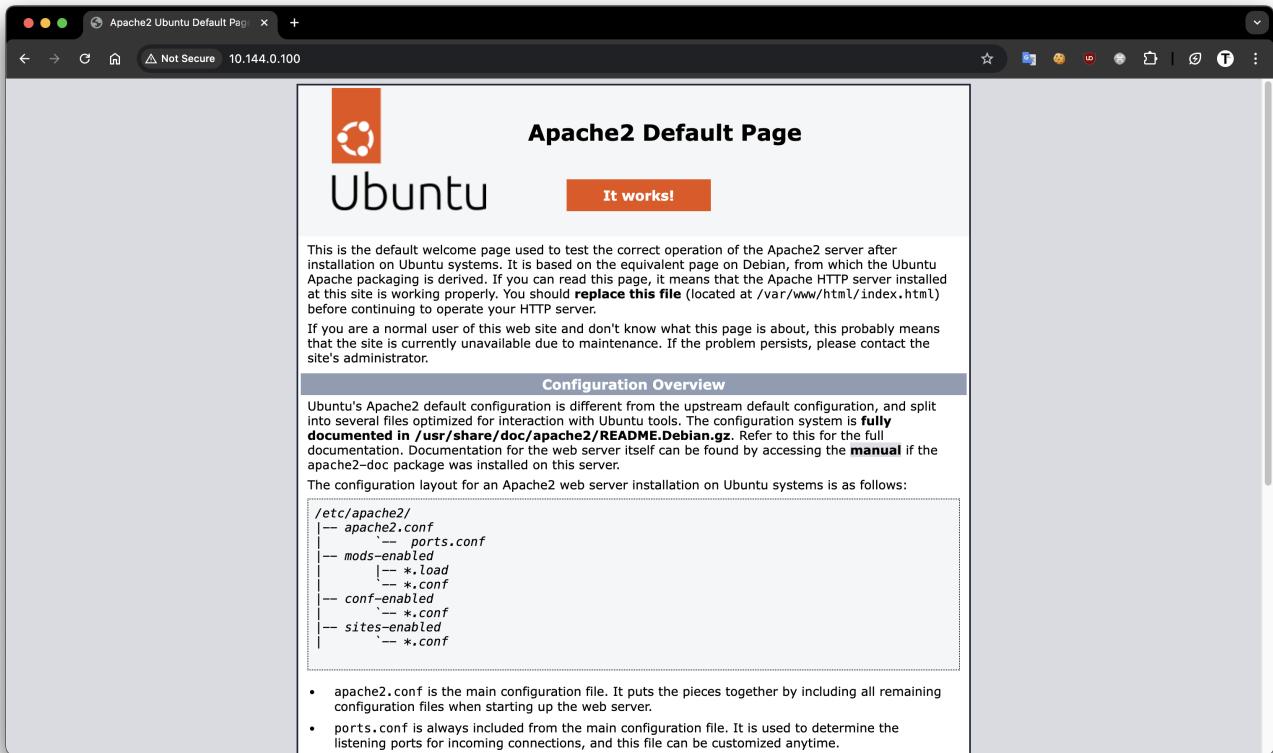
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Oct 13 15:37:35 2024 from 10.144.0.101
jackkahod@ubuntu:~$
```

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:~
```

```
❯ nmap -T4 -A -v localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-14 19:34 +07
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:34
Completed NSE at 19:34, 0.00s elapsed
Initiating NSE at 19:34
Completed NSE at 19:34, 0.00s elapsed
Initiating NSE at 19:34
Completed NSE at 19:34, 0.00s elapsed
Initiating NSE at 19:34
Completed NSE at 19:34, 0.00s elapsed
Initiating Ping Scan at 19:34
Scanning localhost (127.0.0.1) [2 ports]
Completed Ping Scan at 19:34, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 19:34
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 21/tcp on 127.0.0.1
Discovered open port 8021/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Discovered open port 5000/tcp on 127.0.0.1
Discovered open port 7070/tcp on 127.0.0.1
Discovered open port 7000/tcp on 127.0.0.1
Discovered open port 49153/tcp on 127.0.0.1
Discovered open port 1123/tcp on 127.0.0.1
Discovered open port 8081/tcp on 127.0.0.1
Completed Connect Scan at 19:34, 0.02s elapsed (1000 total ports)
Initiating Service scan at 19:34
Scanning 11 services on localhost (127.0.0.1)
Completed Service scan at 19:37, 136.05s elapsed (11 services on 1 host)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 19:37
Completed NSE at 19:37, 8.16s elapsed
Initiating NSE at 19:37
Completed NSE at 19:37, 1.04s elapsed
Initiating NSE at 19:37
Completed NSE at 19:37, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000064s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 989 closed tcp ports (conn-refused)
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, TLS SessionReq, TerminalServerCookie, 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)
```

```
titor@Titors-MacBook-Pro-4TB-32GB:~
```

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, TLS SessionReq, TerminalServerCookie, 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(),event:"gtm.js"})};var mst=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" href="/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="/manifest.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:~ base ✘ < at 19:39:43 ⟲
❯ nmap -T4 -A -v 10.144.0.101
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-14 19:39 +07
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:39
Completed NSE at 19:39, 0.00s elapsed
Initiating NSE at 19:39
Completed NSE at 19:39, 0.00s elapsed
Initiating NSE at 19:39
Completed NSE at 19:39, 0.00s elapsed
Initiating Ping Scan at 19:39
Scanning 10.144.0.101 [2 ports]
Completed Ping Scan at 19:39, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:39
Completed Parallel DNS resolution of 1 host. at 19:39, 0.02s elapsed
Initiating Connect Scan at 19:39
Scanning 10.144.0.101 [1000 ports]
Discovered open port 5900/tcp on 10.144.0.101
Discovered open port 7000/tcp on 10.144.0.101
Discovered open port 3000/tcp on 10.144.0.101
Discovered open port 5000/tcp on 10.144.0.101
Completed Connect Scan at 19:40, 11.83s elapsed (1000 total ports)
Initiating Service scan at 19:40
Scanning 4 services on 10.144.0.101
Completed Service scan at 19:42, 156.87s elapsed (4 services on 1 host)
NSE: Script scanning 10.144.0.101.
Initiating NSE at 19:42
Completed NSE at 19:42, 14.19s elapsed
Initiating NSE at 19:42
Completed NSE at 19:42, 1.17s elapsed
Initiating NSE at 19:42
Completed NSE at 19:42, 0.00s elapsed
Nmap scan report for 10.144.0.101
Host is up (0.0088s latency).
Not shown: 996 closed tcp ports (conn-refused)
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
```

```
titor@Titors-MacBook-Pro-4TB-32GB:~
```

```
| 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, TLS SessionReq, 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:
|   Genericles:
|     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?

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.

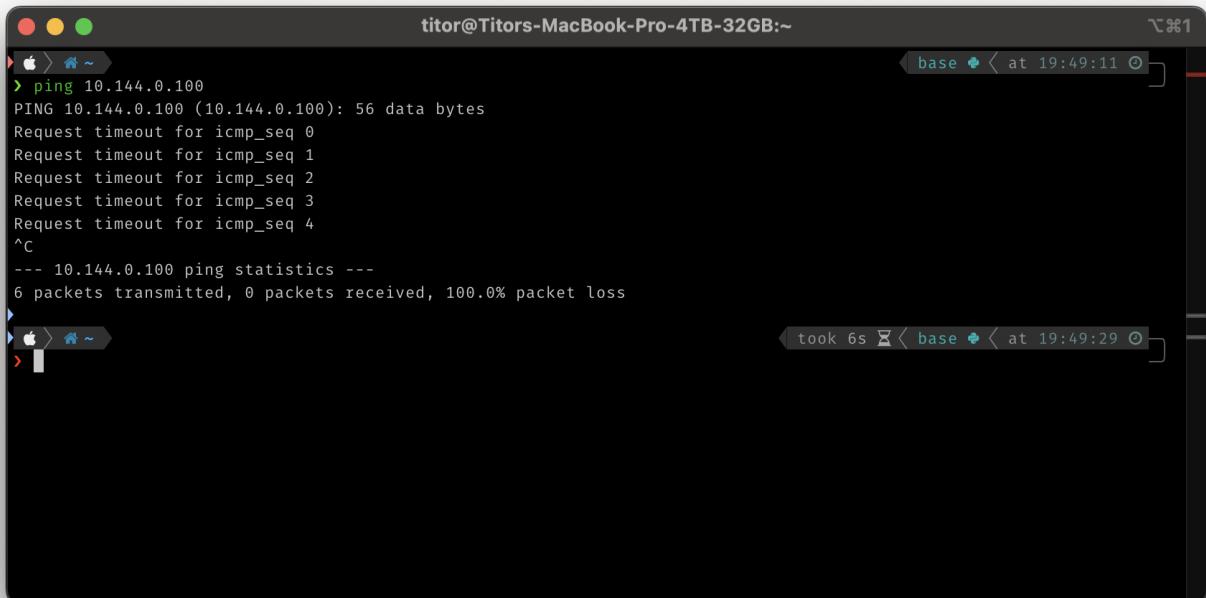
Q5. Find the nmap scan in the web server log. Copy the lines from the log file that were created because of the nmap scan.

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 /nmapowercheck17289998228 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 /HNAPI/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] "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

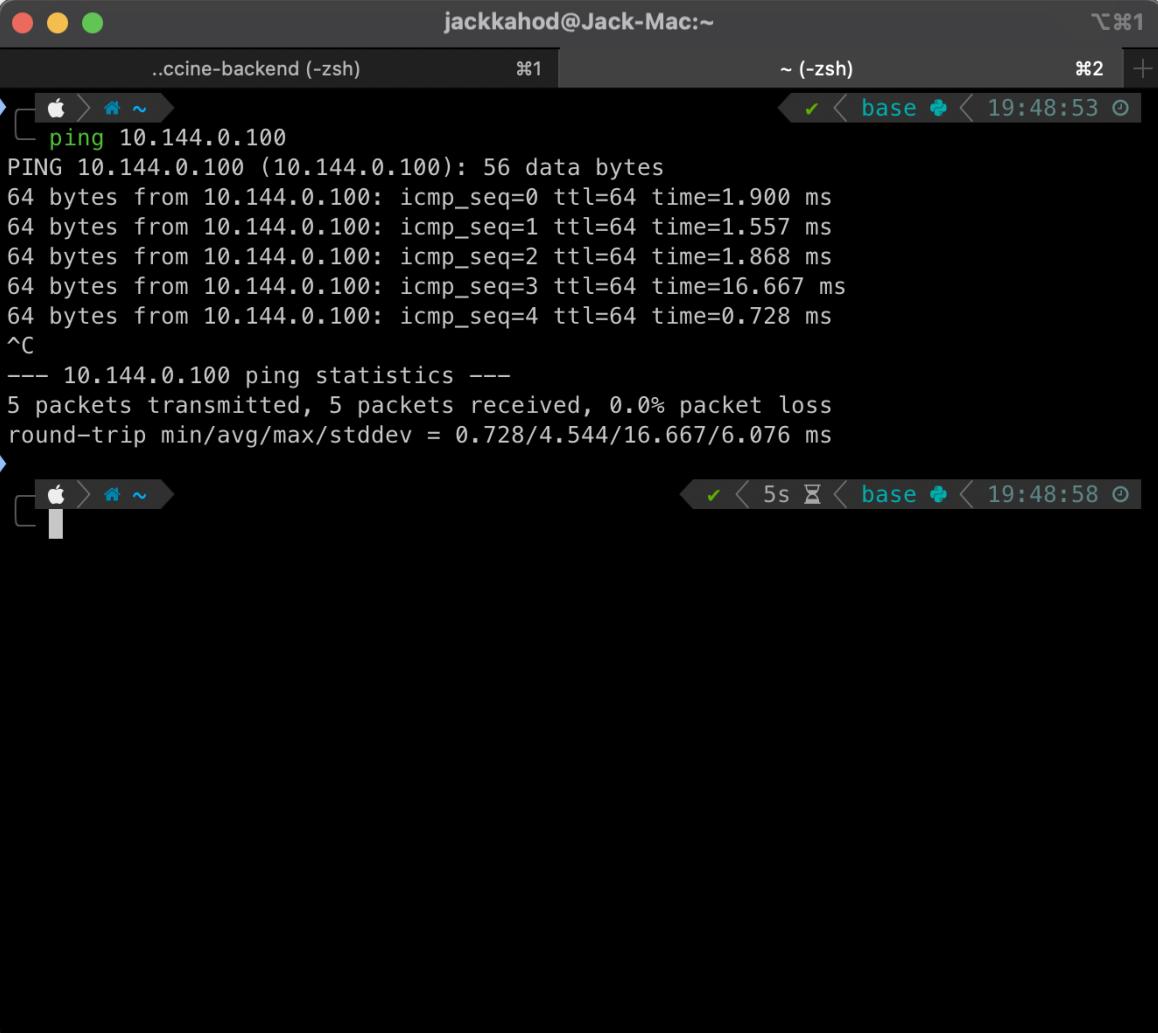
Test 1: Ping your VM from your two notebooks. You should not see any responses.

Attacker notebook:



```
titor@Titors-MacBook-Pro-4TB-32GB:~
> ping 10.144.0.100
PING 10.144.0.100 (10.144.0.100): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
^C
--- 10.144.0.100 ping statistics ---
6 packets transmitted, 0 packets received, 100.0% packet loss
took 6s base ✘ at 19:49:11
```

Target notebook:



```
jackkahod@Jack-Mac:~
```

```
..ccine-backend (-zsh)   ~ (-zsh)   ☁1 ☁2 +
```

```
ping 10.144.0.100
PING 10.144.0.100 (10.144.0.100): 56 data bytes
64 bytes from 10.144.0.100: icmp_seq=0 ttl=64 time=1.900 ms
64 bytes from 10.144.0.100: icmp_seq=1 ttl=64 time=1.557 ms
64 bytes from 10.144.0.100: icmp_seq=2 ttl=64 time=1.868 ms
64 bytes from 10.144.0.100: icmp_seq=3 ttl=64 time=16.667 ms
64 bytes from 10.144.0.100: icmp_seq=4 ttl=64 time=0.728 ms
^C
--- 10.144.0.100 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.728/4.544/16.667/6.076 ms
```

```
✓ < 5s ✎ < base ⚡ < 19:48:53 ⏹
```

```
✓ < 5s ✎ < base ⚡ < 19:48:58 ⏹
```

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.

The screenshot shows a macOS terminal window with two tabs. The active tab, labeled 'jackkahod@ubuntu: ~', displays the following output:

```
jackkahod@ubuntu: ~
..ccine-backend (-zsh)   %1
jackkahod@ubuntu: ~ (ssh) %2 +
```

SSH session details:

```
ssh -l jackkahod 10.144.0.100
jackkahod@10.144.0.100's password:
```

Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-122-generic aarch64)

System information as of Mon Oct 14 01:36:23 PM GMT 2024

System load, Usage of /, Memory usage, Swap usage, Processes, Users logged in, IPv4 address, and IPv6 address are listed.

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See <https://ubuntu.com/esm> or run: sudo pro status

New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Oct 14 13:36:23 2024 from 10.144.0.101
jackkahod@ubuntu:~\$ █

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 /nmapPowercheck1728911263 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] "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.lco 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 /NMAP1 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/2024:13:07:44 +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/2024:13:07:48 +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.

```
jackkahod@ubuntu:~$ sudo iptables -P INPUT DROP
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -m state -p tcp --dport 22 -s 10.144.0.101 --state NEW,ESTABLISHED,RELATED -j ACCEPT
jackkahod@ubuntu:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source          destination
ACCEPT    tcp  --  anywhere        anywhere          tcp dpt:http
ACCEPT    tcp  --  10.144.0.101     anywhere          state NEW,RELATED,ESTABLISHED tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
jackkahod@ubuntu:~$
```