

Aluno: Breno de Souza Silva - 04/08/2024

Checkpoint 1 – CyberSecurity for Dev

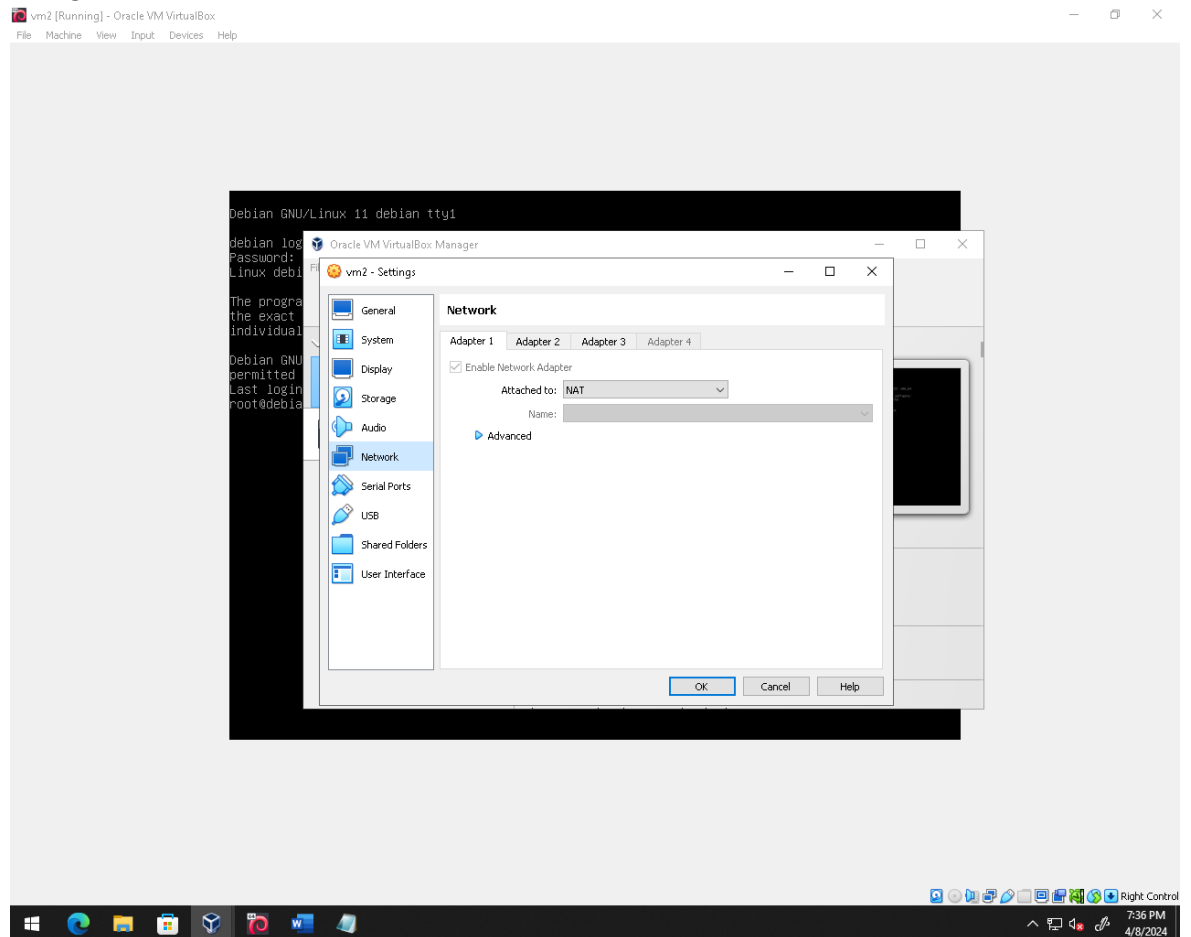
Relatório Técnico de CyberSecurity

Considerando o cenário abaixo para este relatório:

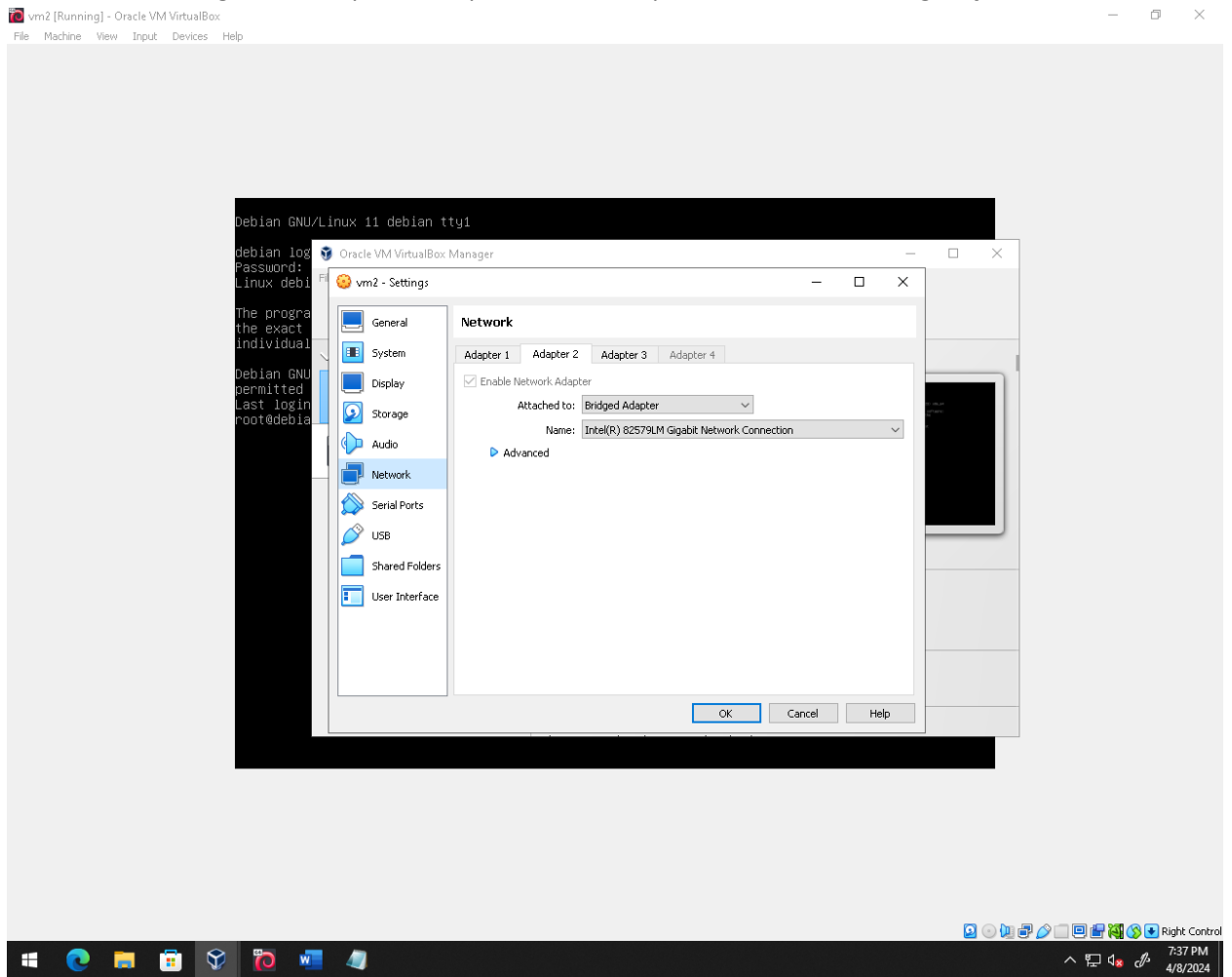
- **VM Debian – Server – IP 172.16.80.10**
- **VM Kali – Client – 172.16.80.20**

1. Iremos configurar as VMs e a comunicação entre Server x Cliente

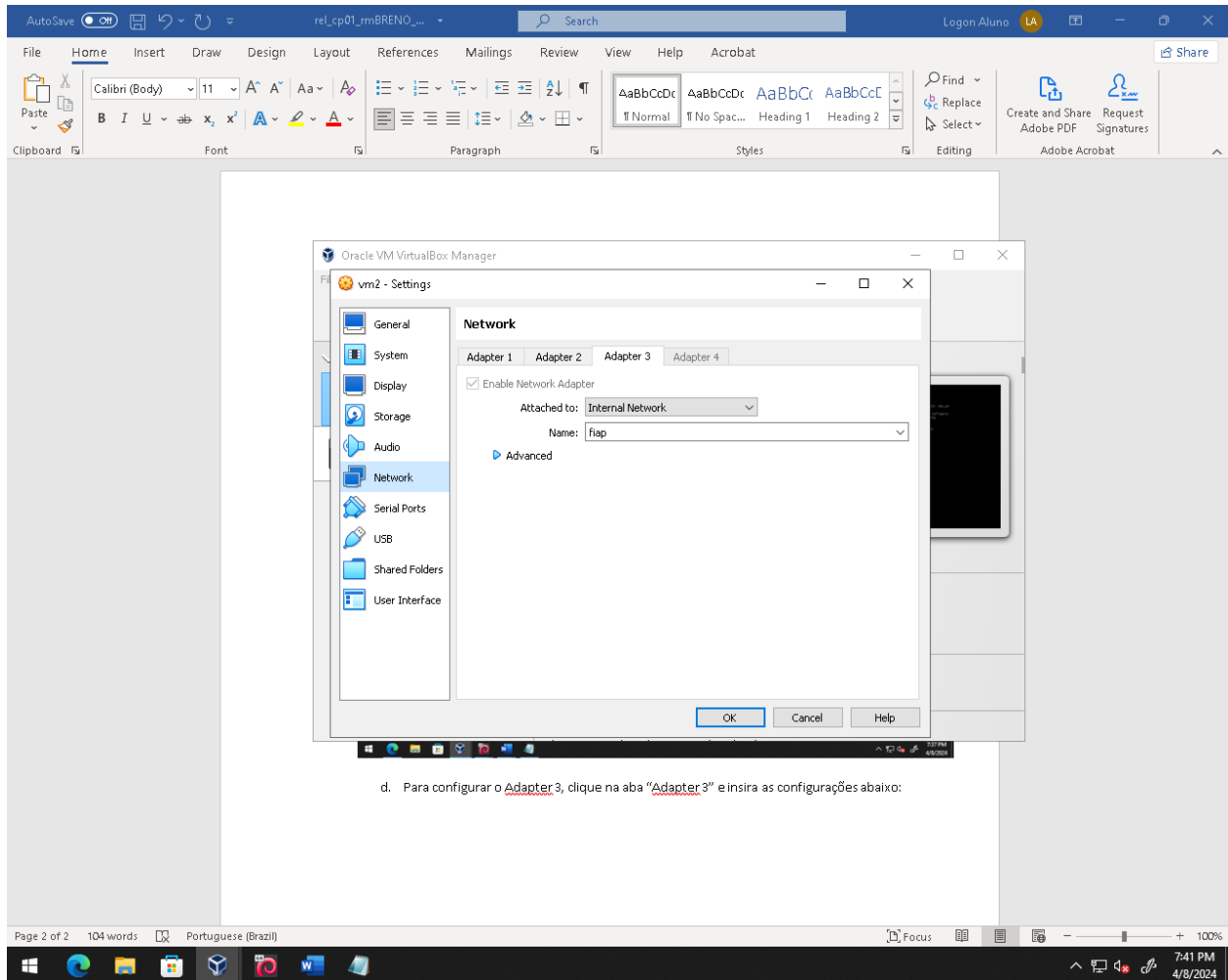
- Configurar as duas VMs para funcionar inicialmente:
- Na VM referente ao Server, clique em Settings e vá para a aba de Network para configurarmos a rede interna.



c. Para configurar o Adapter 2, clique na aba “Adapter 2” e insira as configurações abaixo:

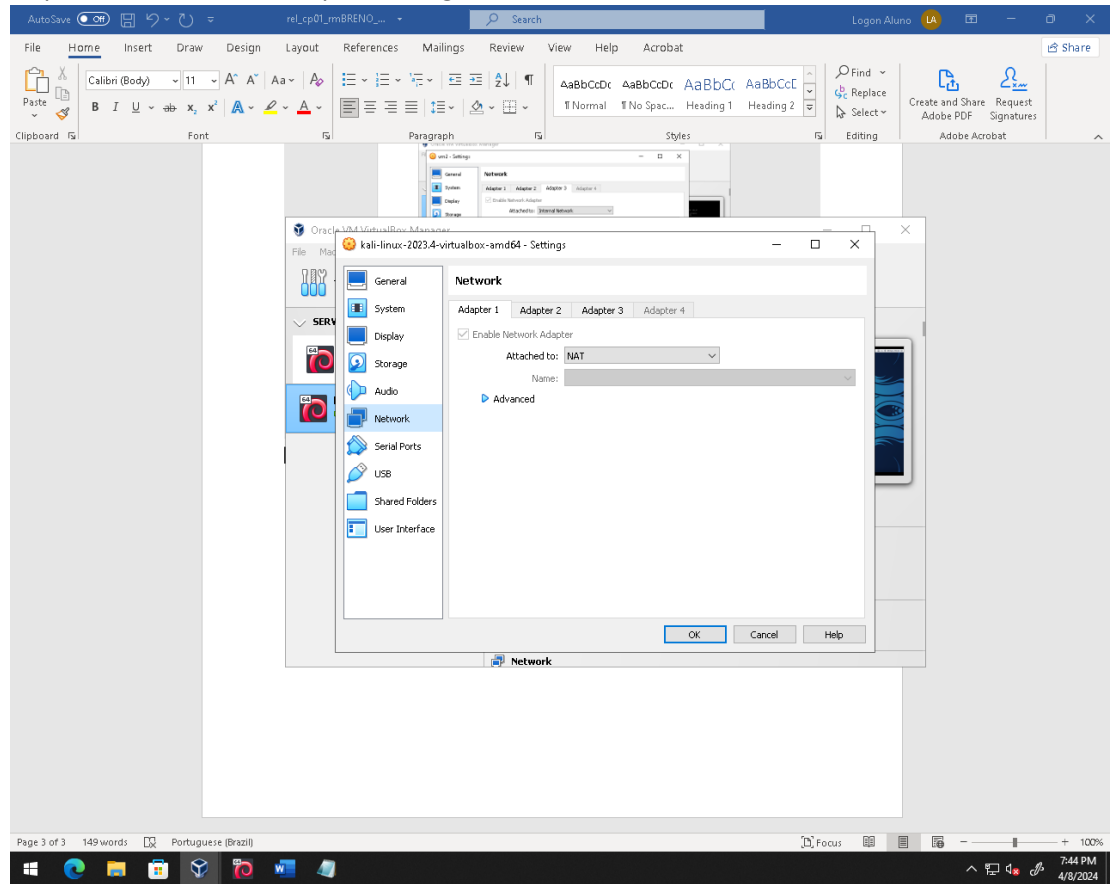


d. Para configurar o Adapter 3, clique na aba “Adapter 3” e insira as configurações abaixo:

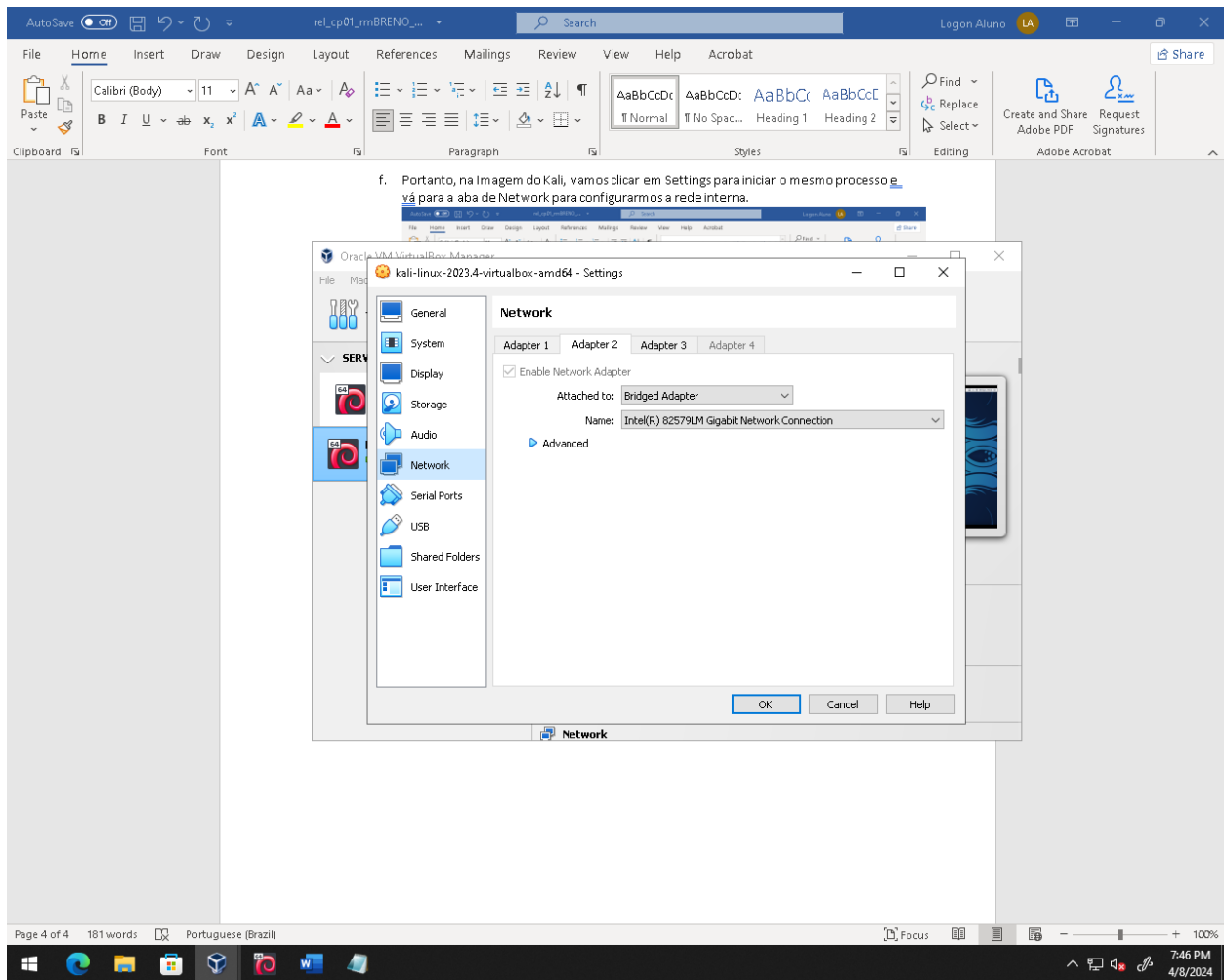


e. Agora precisamos repetir os mesmos passos, entretanto na VM referente ao cliente que é o KALI.

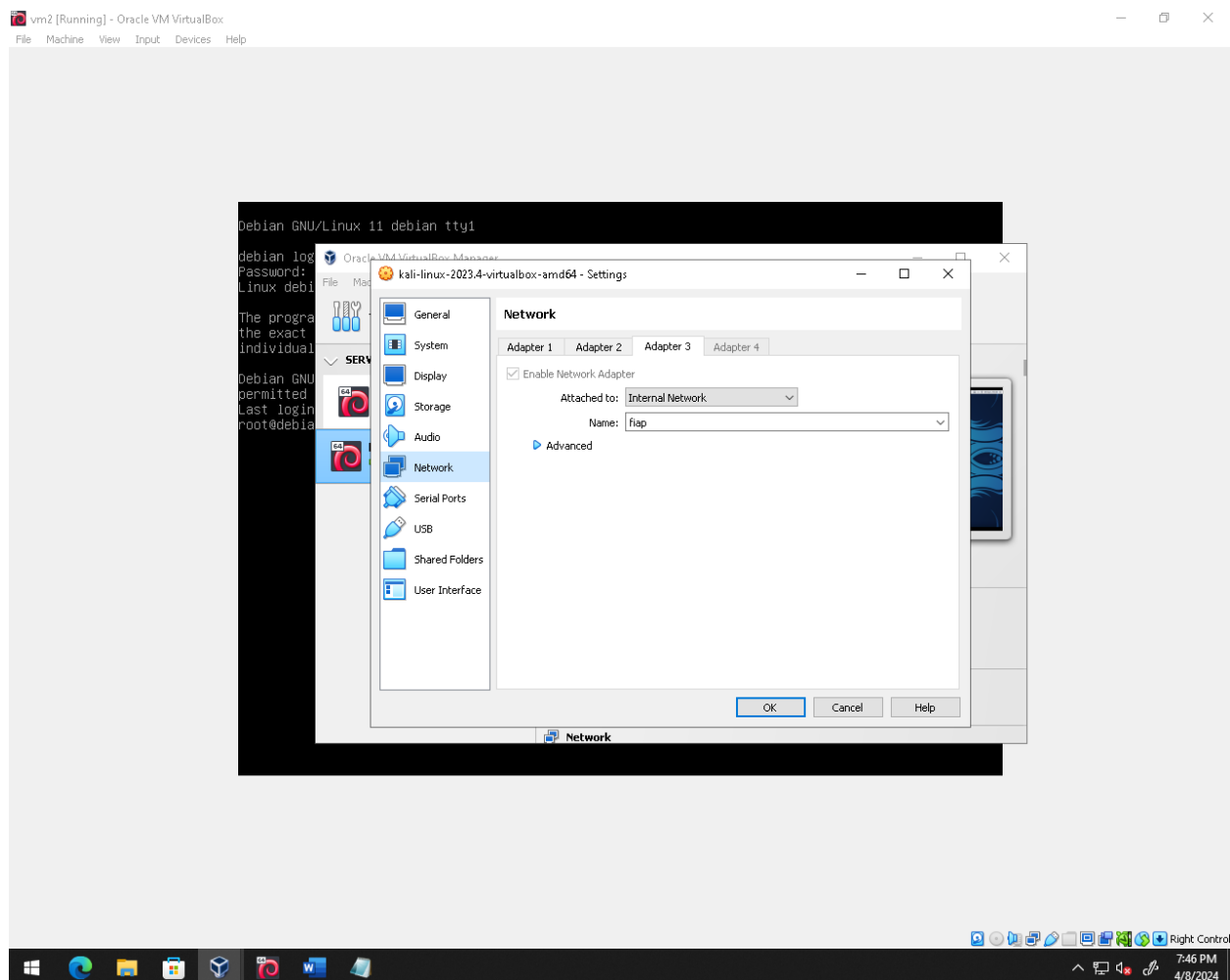
- f. Portanto, na Imagem do Kali, vamos clicar em Settings para iniciar o mesmo processo e vá para a aba de Network para configurarmos a rede interna.



g. Para configurar o Adapter 2, clique na aba “Adapter 2” e insira as configurações abaixo:



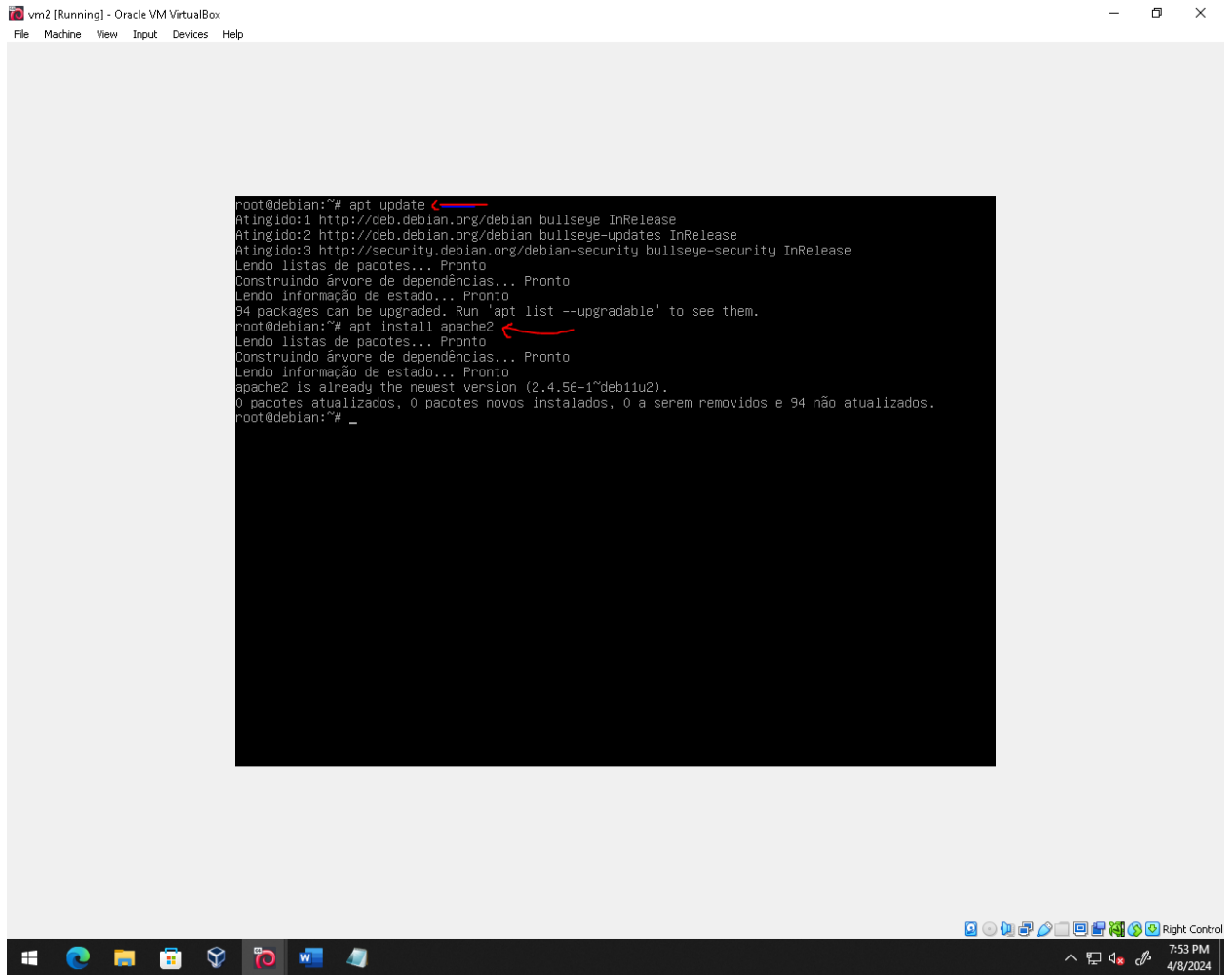
h. Para configurar o Adapter 3, clique na aba “Adapter 3” e insira as configurações abaixo:



- i. Agora precisamos, Iniciar as duas máquinas, logando com o usuário root
 - i. VM Debian - User root – Senha fiap
 - ii. VM Kali – User kali – Senha kali

2. Configurando o Servidor:

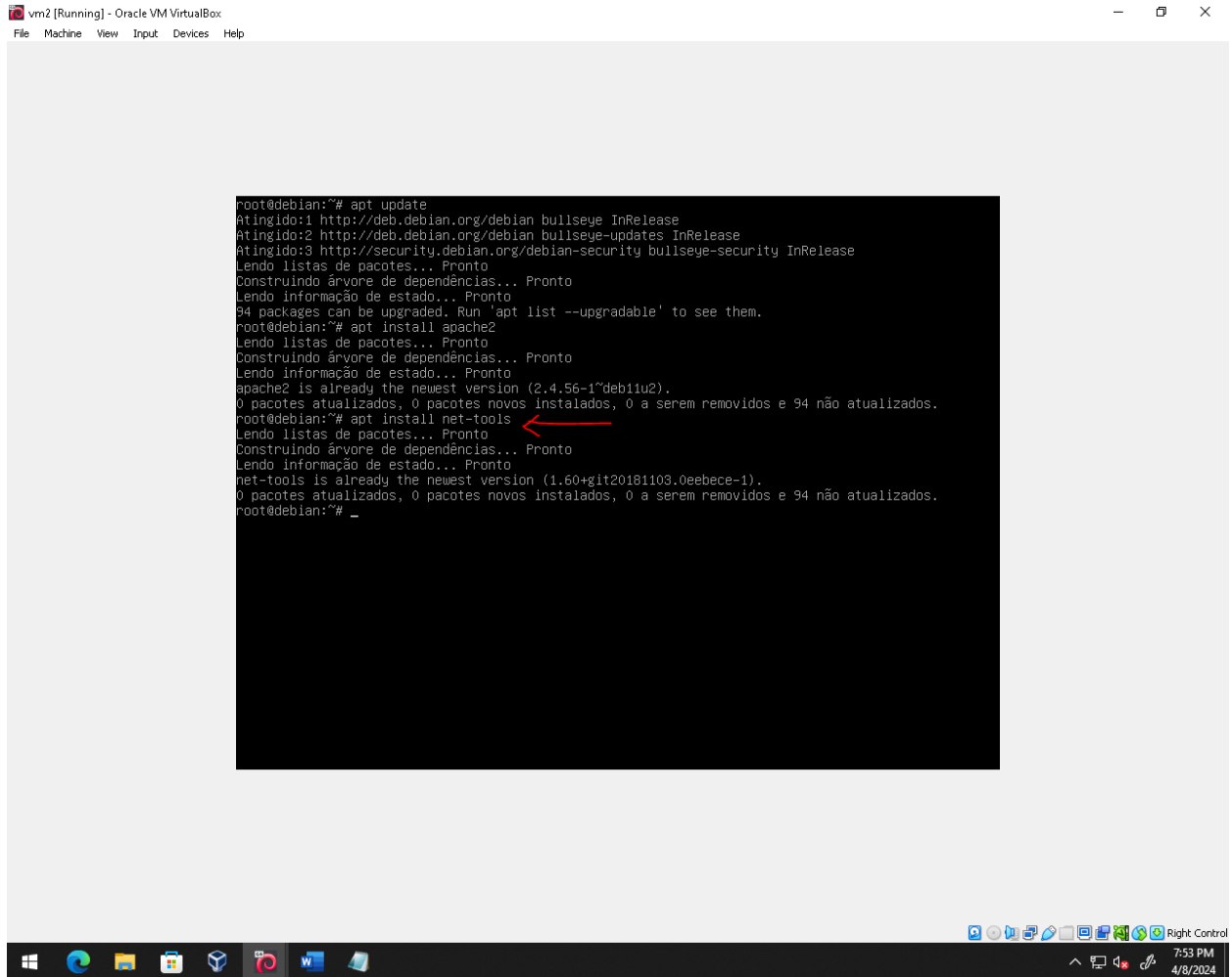
- Primeiro iremos precisar instalar o serviço apache2 no nosso servidor.
- Na máquina Debian rode o comando 'apt update' e em seguida 'apt install apache2' (digite 'S' se solicitado)



```
vm2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@debian:~# apt update
Atingido:1 http://deb.debian.org/debian bullseye InRelease
Atingido:2 http://deb.debian.org/debian bullseye-updates InRelease
Atingido:3 http://security.debian.org/debian-security bullseye-security InRelease
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
94 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@debian:~# apt install apache2
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
apache2 is already the newest version (2.4.56-1~deb11u2).
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 94 não atualizados.
root@debian:~#
```

- c. Instale o pacote 'net-tools' para facilitar o uso do serviço apache2. Para isso rode o comando 'apt install net-tools'



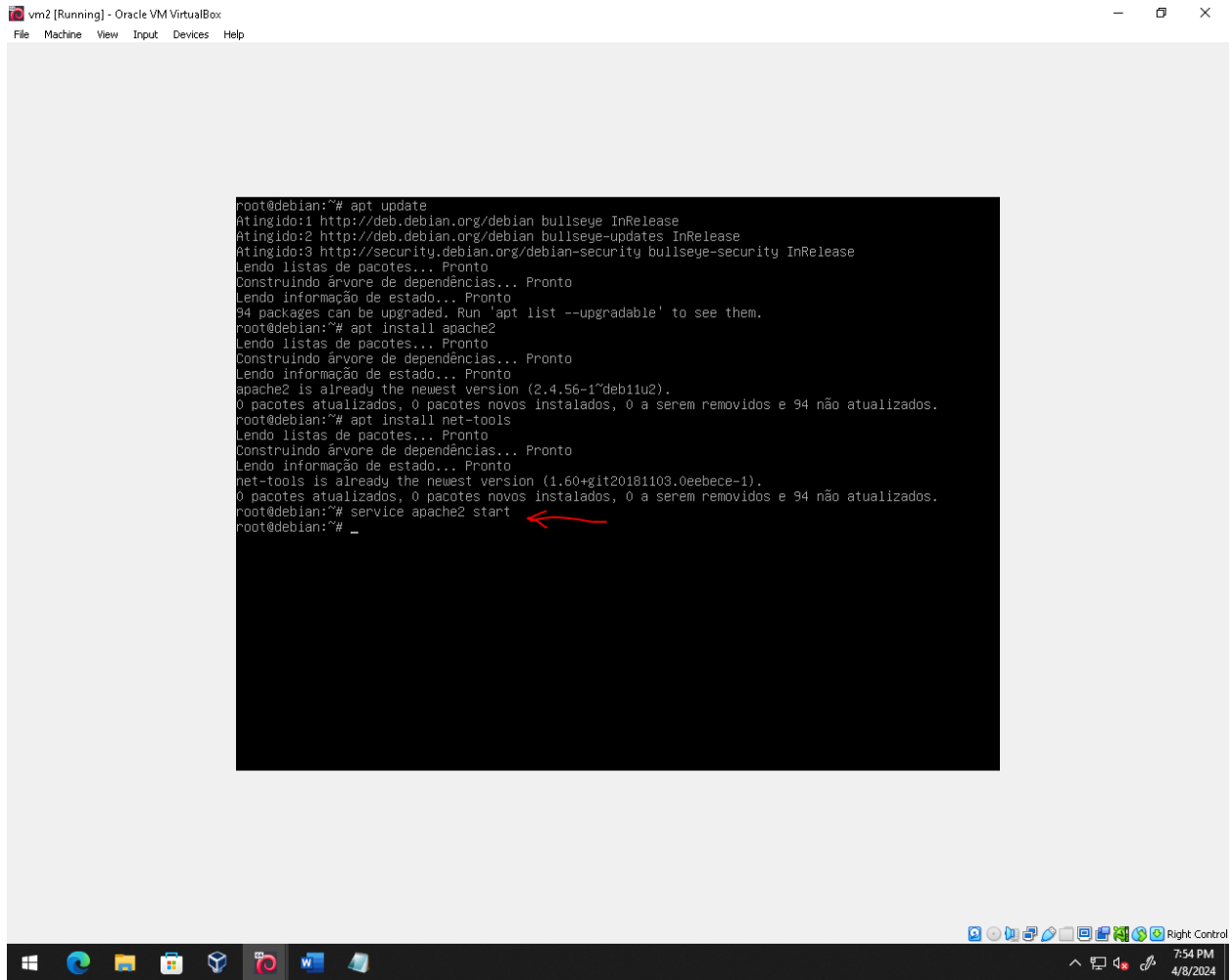
The screenshot shows a terminal window titled 'vm2 [Running] - Oracle VM VirtualBox'. The terminal output is as follows:

```
root@debian:~# apt update
Atingido:1 http://deb.debian.org/debian bullseye InRelease
Atingido:2 http://deb.debian.org/debian bullseye-updates InRelease
Atingido:3 http://security.debian.org/debian-security bullseye-security InRelease
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
94 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@debian:~# apt install apache2
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
apache2 is already the newest version (2.4.56-1~deb11u2).
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 94 não atualizados.
root@debian:~# apt install net-tools
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
net-tools is already the newest version (1.60+git20181103.0eebece-1).
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 94 não atualizados.
root@debian:~# _
```

A red arrow points to the command 'apt install net-tools' in the terminal output.

The bottom of the screenshot shows the Windows taskbar with various icons and the system clock indicating 7:53 PM on 4/8/2024.

d. Para iniciar o serviço apache2 rode o comando 'service apache2 start'



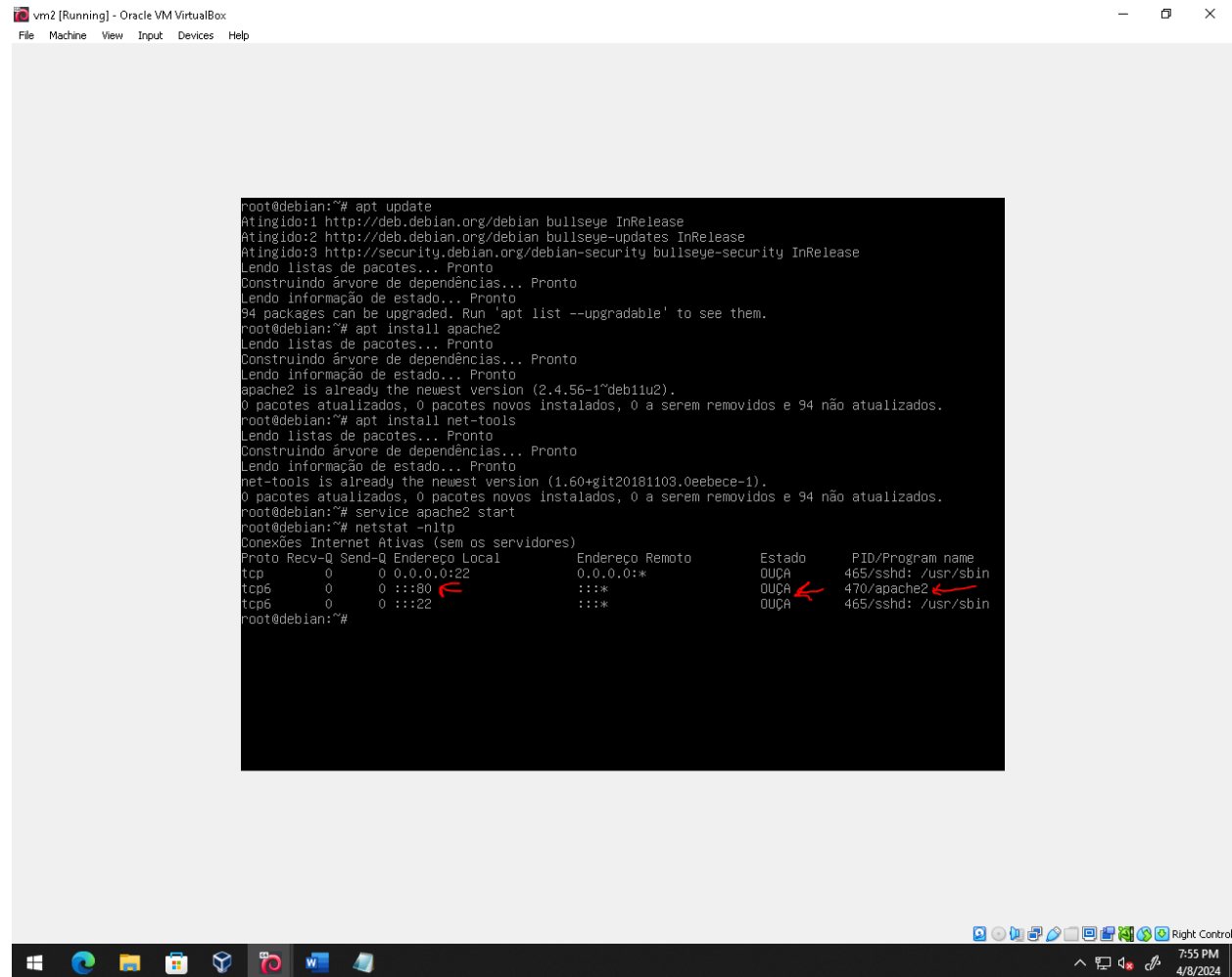
The screenshot shows a terminal window titled 'vm2 [Running] - Oracle VM VirtualBox'. The terminal output is as follows:

```
root@debian:~# apt update
Atingido:1 http://deb.debian.org/debian bullseye InRelease
Atingido:2 http://deb.debian.org/debian bullseye-updates InRelease
Atingido:3 http://security.debian.org/debian-security bullseye-security InRelease
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
94 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@debian:~# apt install apache2
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
apache2 is already the newest version (2.4.56-1~deb11u2).
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 94 não atualizados.
root@debian:~# apt install net-tools
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
net-tools is already the newest version (1.60+git20181103.0eebece-1).
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 94 não atualizados.
root@debian:~# service apache2 start
root@debian:~# _
```

A red arrow points to the command 'service apache2 start' in the terminal output.

The bottom of the screenshot shows the Windows taskbar with various icons and the system clock indicating 7:54 PM on 4/8/2024.

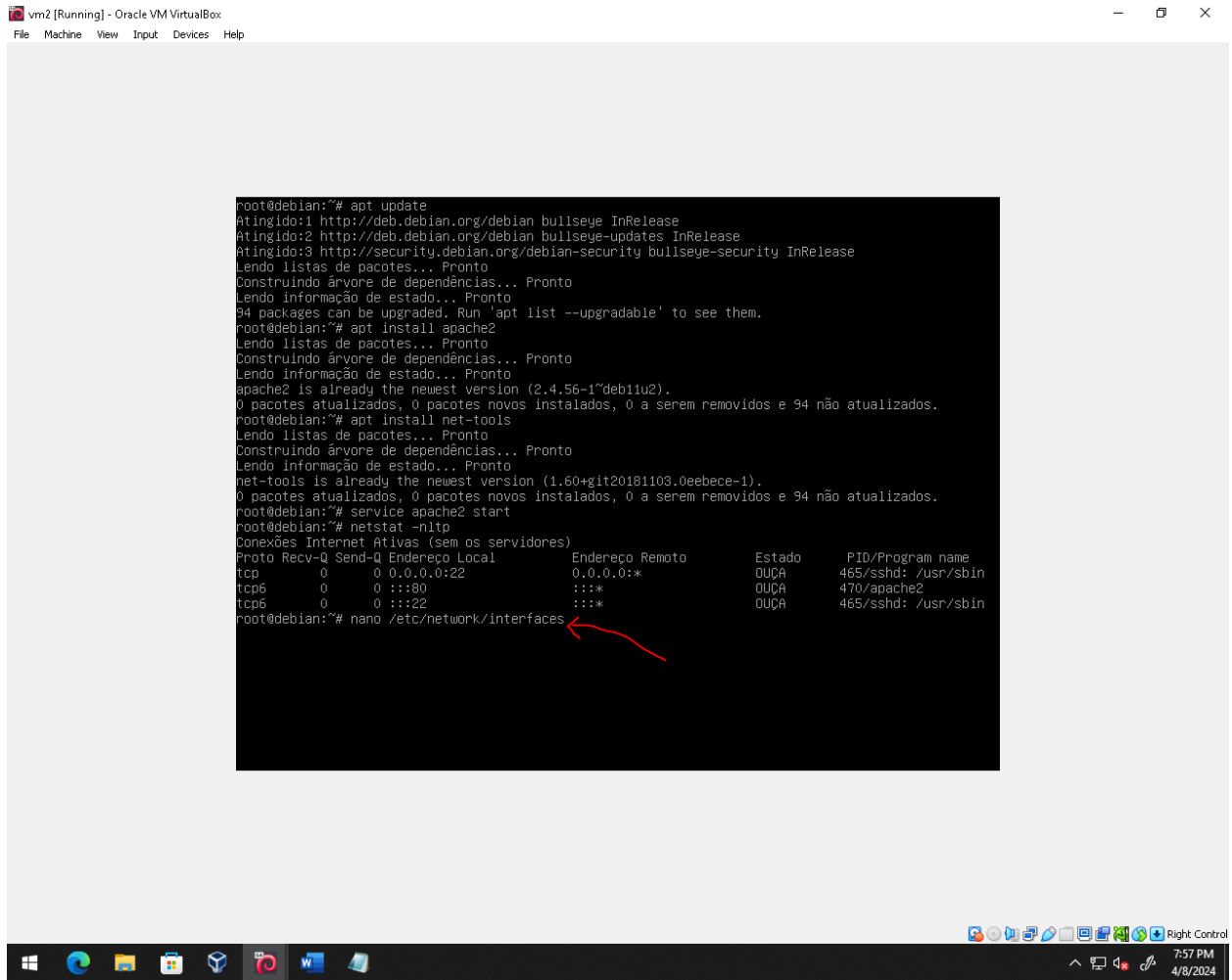
Para verificar se o serviço está funcionando, rode o comando 'netstat -nltp', a fim de verificar se a porta 80 está sendo usada pelo apache.



```
root@debian:~# apt update
Atingido:1 http://deb.debian.org/debian bullseye InRelease
Atingido:2 http://deb.debian.org/debian bullseye-updates InRelease
Atingido:3 http://security.debian.org/debian-security bullseye-security InRelease
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
94 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@debian:~# apt install apache2
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
apache2 is already the newest version (2.4.56-1~deb11u2).
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 94 não atualizados.
root@debian:~# apt install net-tools
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
net-tools is already the newest version (1.60+git20181103.0eebece-1).
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 94 não atualizados.
root@debian:~# service apache2 start
root@debian:~# netstat -nltp
Conexões Internet Ativas (sem os servidores)
Proto Recv-Q Send-Q Endereço Local      Endereço Remoto      Estado      PID/Program name
tcp        0      0 0.0.0.0:22          0.0.0.0:*             OUÇA       465/sshd: /usr/sbin
tcp6       0      0 :::80              :::*                   OUÇA       470/apache2 ←
tcp6       0      0 :::22              :::*                   OUÇA       465/sshd: /usr/sbin
root@debian:~#
```

- e. Agora vamos configurar o arquivo 'Interfaces' da pasta network para terminar a configuração da placa de rede.

f. Rodar o seguinte comando em cada uma das máquinas: 'nano /etc/network/interfaces'



```
root@debian:~# apt update
Atingido:1 http://deb.debian.org/debian bullseye InRelease
Atingido:2 http://deb.debian.org/debian bullseye-updates InRelease
Atingido:3 http://security.debian.org/debian-security bullseye-security InRelease
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
94 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@debian:~# apt install apache2
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
apache2 is already the newest version (2.4.56-1~deb11u2).
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 94 não atualizados.
root@debian:~# apt install net-tools
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
net-tools is already the newest version (1.60+git20181103.0eebece-1).
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 94 não atualizados.
root@debian:~# service apache2 start
root@debian:~# netstat -ntlp
Conexões Internet Ativas (sem os servidores)
Proto Recv-Q Send-Q Endereço Local          Endereço Remoto        Estado      PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               OÚÇA       465/sshd: /usr/sbin
tcp6       0      0 :::60                  :::*                    OÚÇA       470/apache2
tcp6       0      0 :::22                  :::*                    OÚÇA       465/sshd: /usr/sbin
root@debian:~# nano /etc/network/interfaces
```

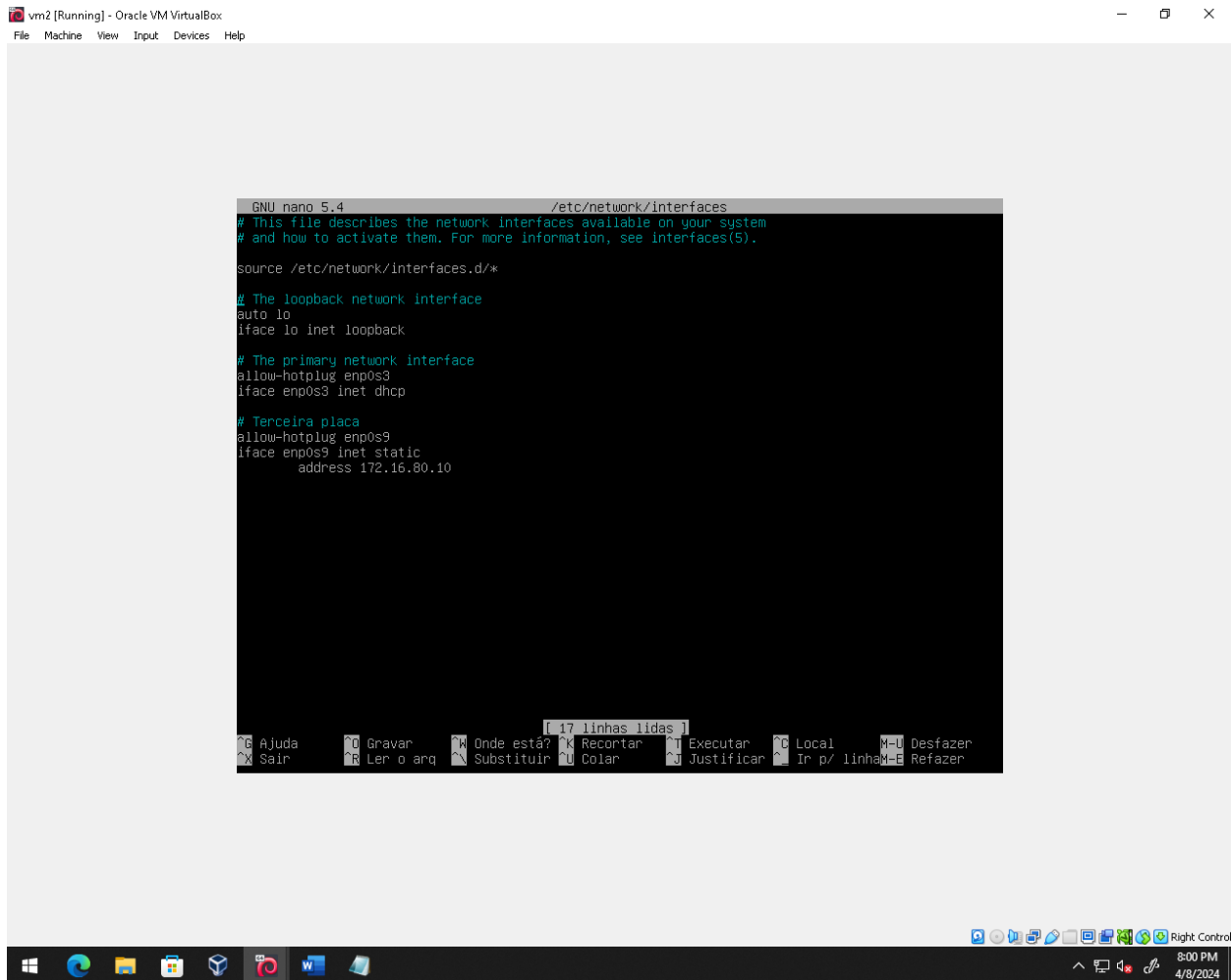
g. No arquivo final do arquivo, vamos digitar o seguintes linhas para configurar o arquivo:

```
# Terceira Placa – fiap
```

```
allow-hotplug enp0s9
```

```
iface enp0s9 inet static
```

```
address 172.16.80.10
```



The screenshot shows a Windows desktop with a VirtualBox VM window titled 'vm2 [Running] - Oracle VM VirtualBox'. The VM is running a Linux system. The terminal window shows the nano editor editing the file '/etc/network/interfaces'. The content of the file is as follows:

```
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet dhcp

# Terceira placa
allow-hotplug enp0s9
iface enp0s9 inet static
    address 172.16.80.10
```

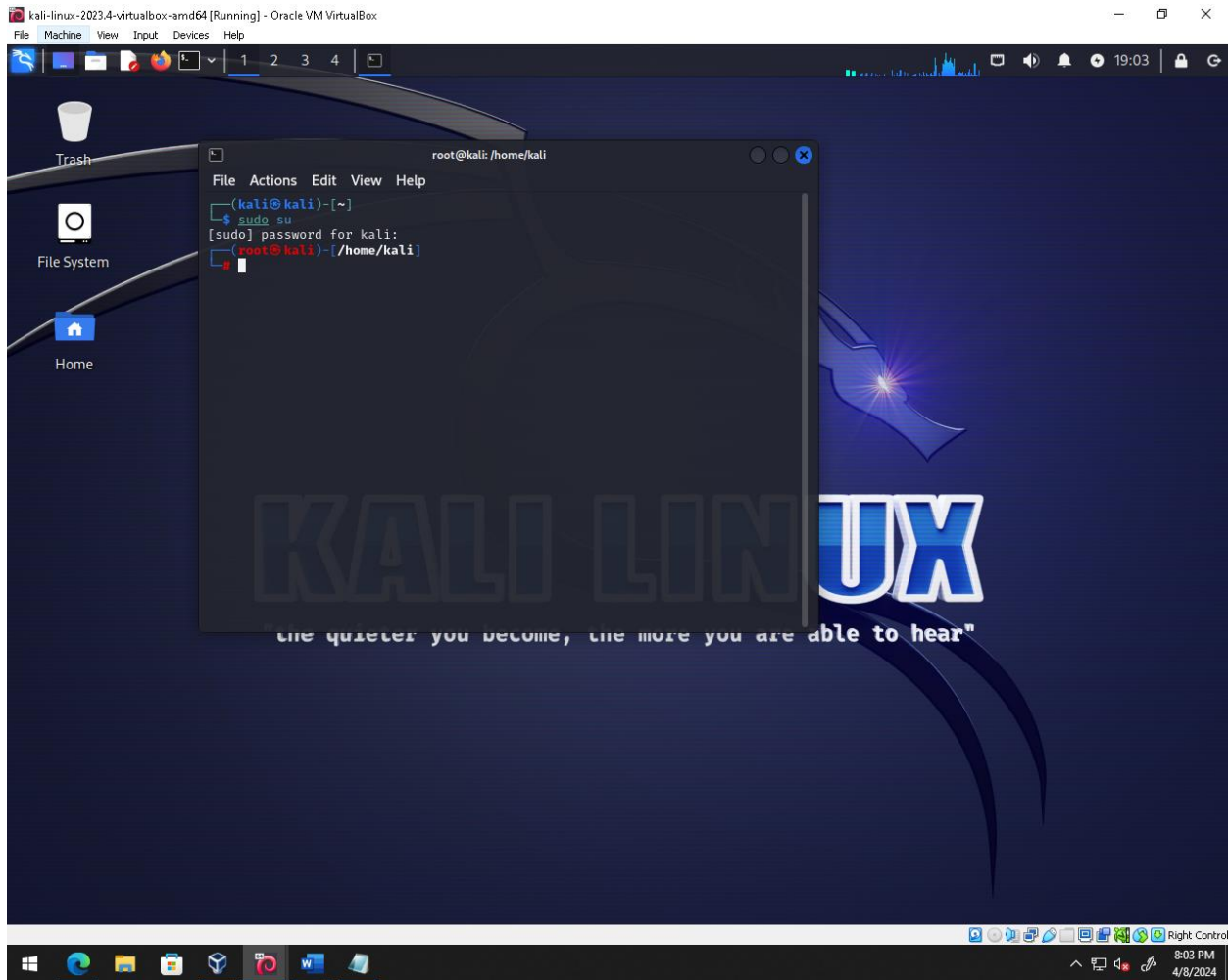
The nano editor's status bar at the bottom shows '17 linhas lidas' (17 lines read). The Windows taskbar at the bottom shows the time as 8:00 PM on 4/8/2024.

h. Aperte as teclas 'Ctrl O' -> 'Enter' -> 'Ctrl X' para salvar o arquivo e configuração

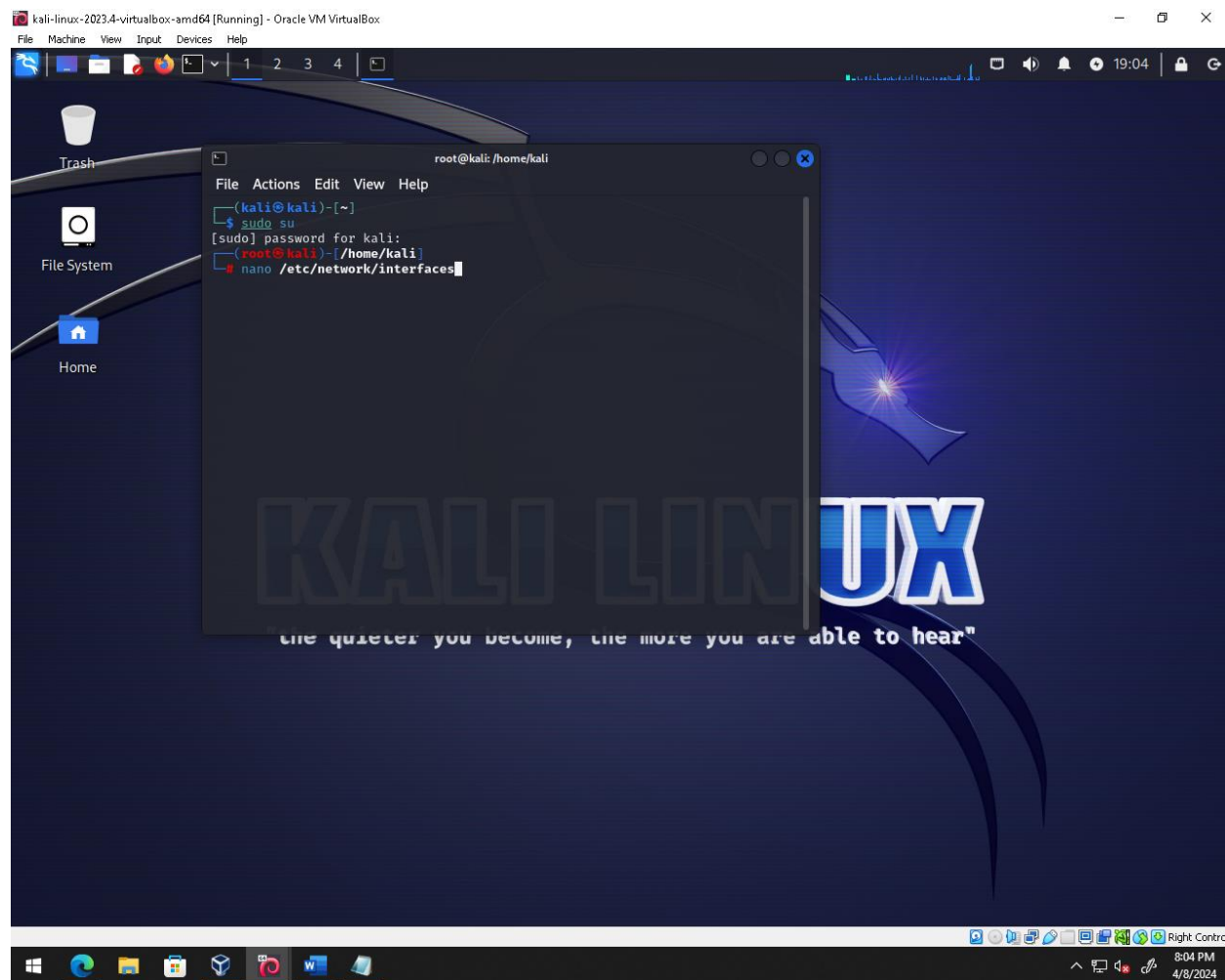
i. Digite o comando 'init 6' para reiniciar a máquina com a nova configuração

3. Configurando o Cliente:

- a. Na máquina Kali, rode o comando 'sudo su', digitando a senha 'kali' quando necessário.



b. Rodar o seguinte comando em cada uma das máquinas: 'nano /etc/network/interfaces'



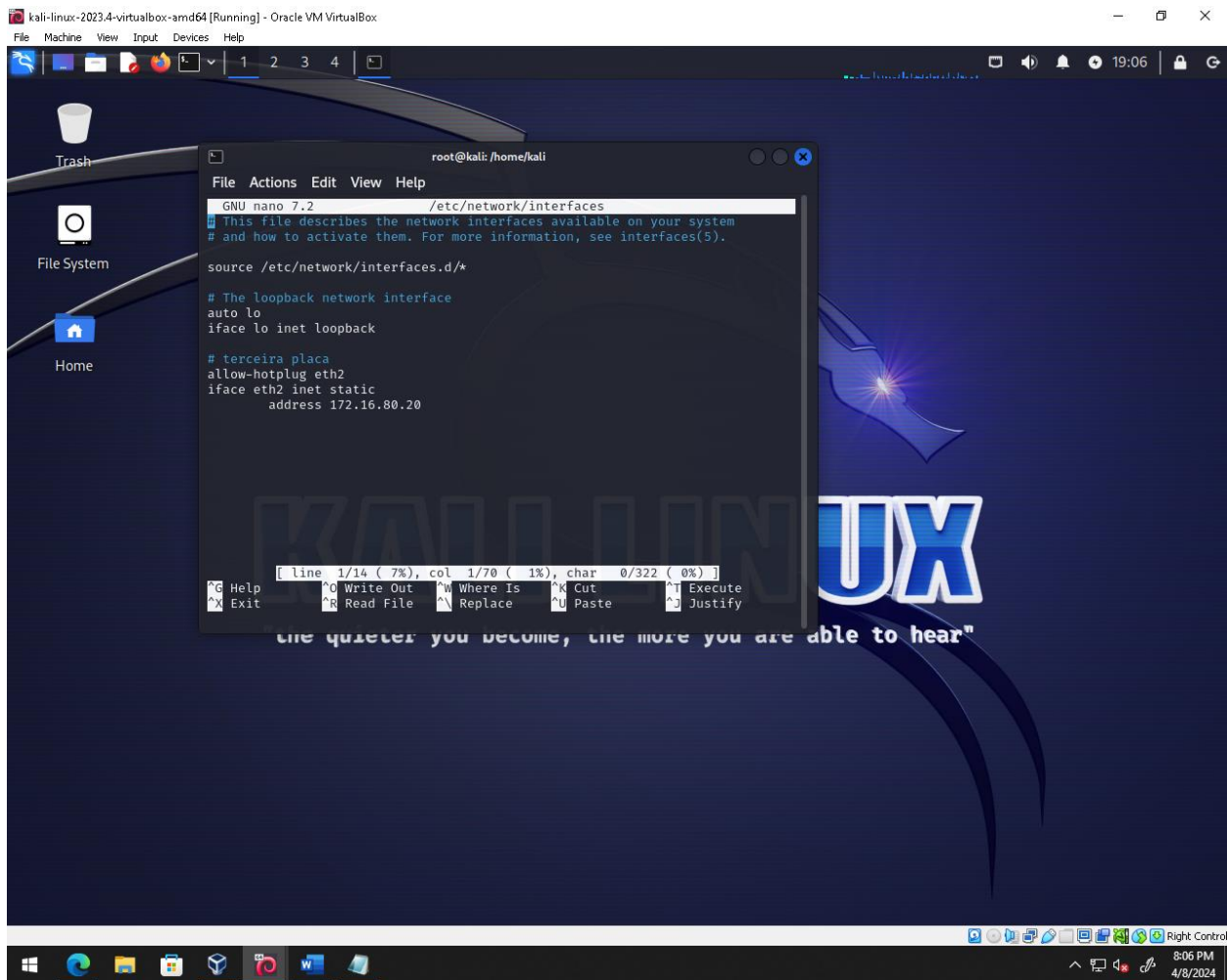
c. Na máquina Kali, vá até o final do arquivo e digite o seguinte:

Terceira Placa – fiap

allow-hotplug eth2

iface eth2 inet static

address 172.16.80.20



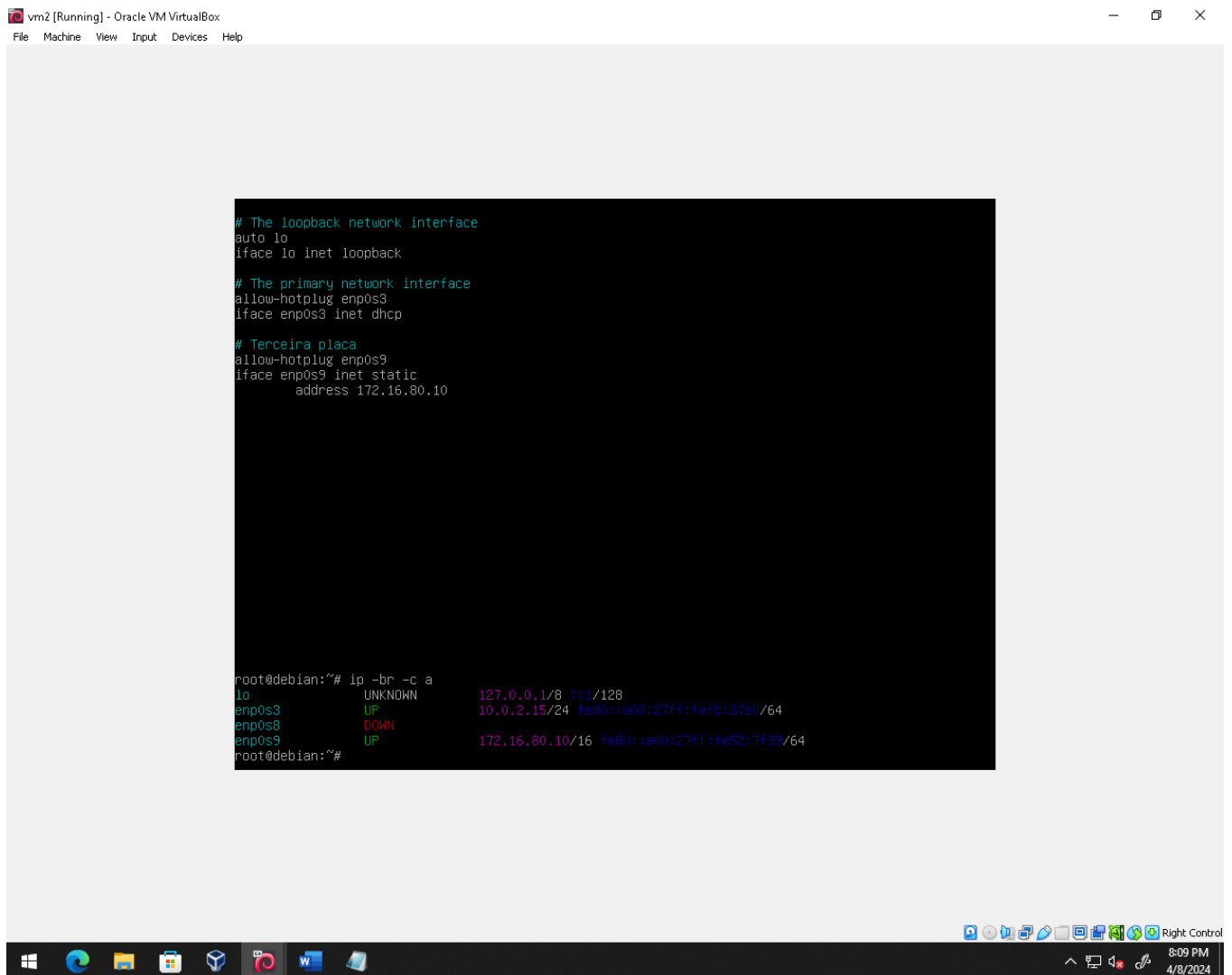
d. Ainda no Kali, aperte as teclas 'Ctrl O' -> 'Enter' -> 'Ctrl X'

e. Digite o comando 'init 6' para reiniciar a máquina com a nova configuração

4. Verificando a comunicação entre Servidor e Cliente:

- a. Digite os comandos 'ip -br -c a' e verifique se as interfaces eth2 e enp0s9 estão com os IPs 172.16.80.20 e 172.16.80.10 respectivamente.

- SERVER:



The screenshot shows a terminal window titled 'vm2 [Running] - Oracle VM VirtualBox'. The terminal output displays network configuration for three interfaces: 'lo' (loopback), 'enp0s3' (primary), and 'enp0s9' (terceira placa). The configuration for 'enp0s9' sets a static IP of 172.16.80.10. Below the configuration, the command 'ip -br -c a' is executed, showing the status of the interfaces. The output indicates that 'lo' is UNKNOWN, 'enp0s3' is UP, 'enp0s8' is DOWN, and 'enp0s9' is UP with the assigned IP and MAC address.

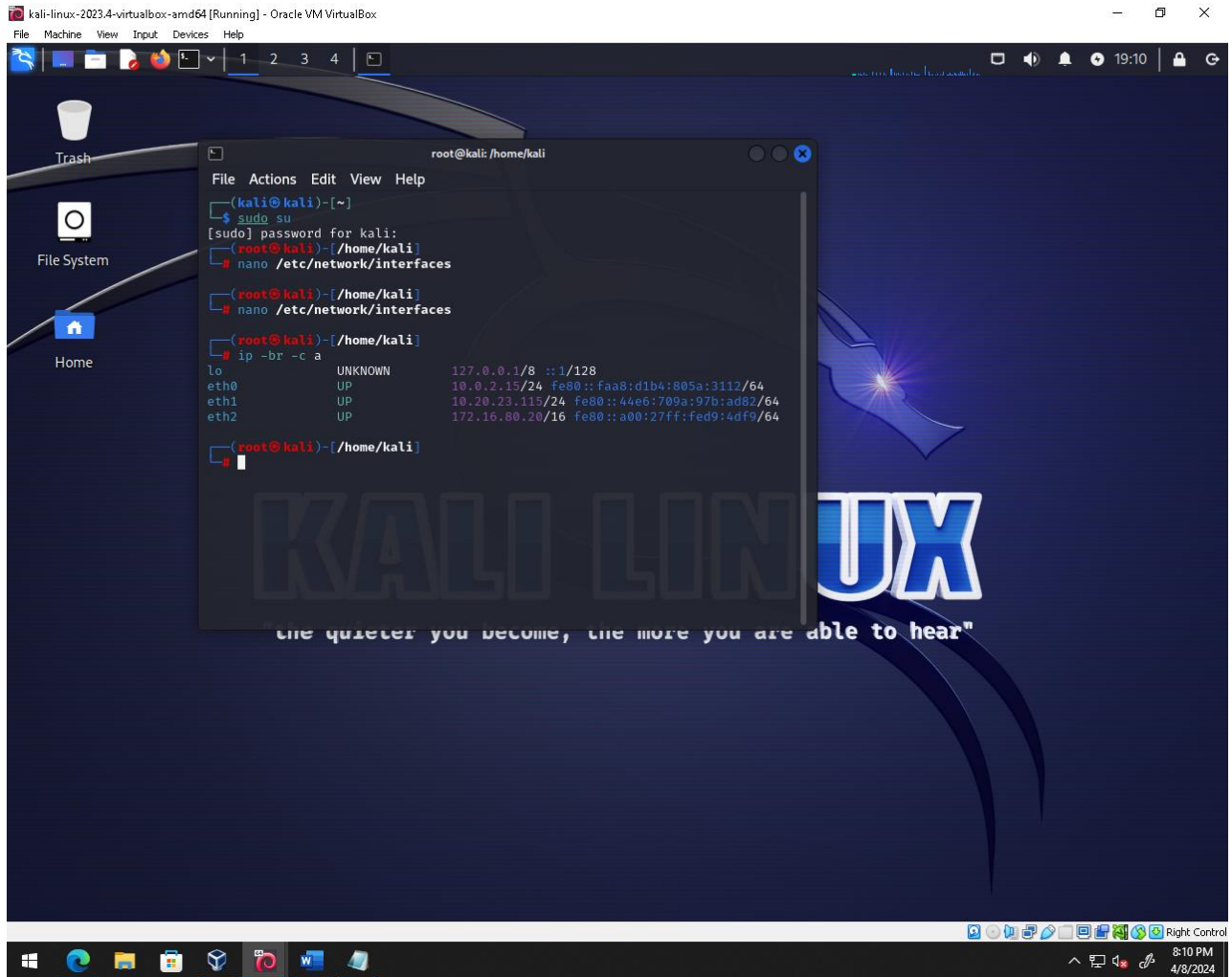
```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet dhcp

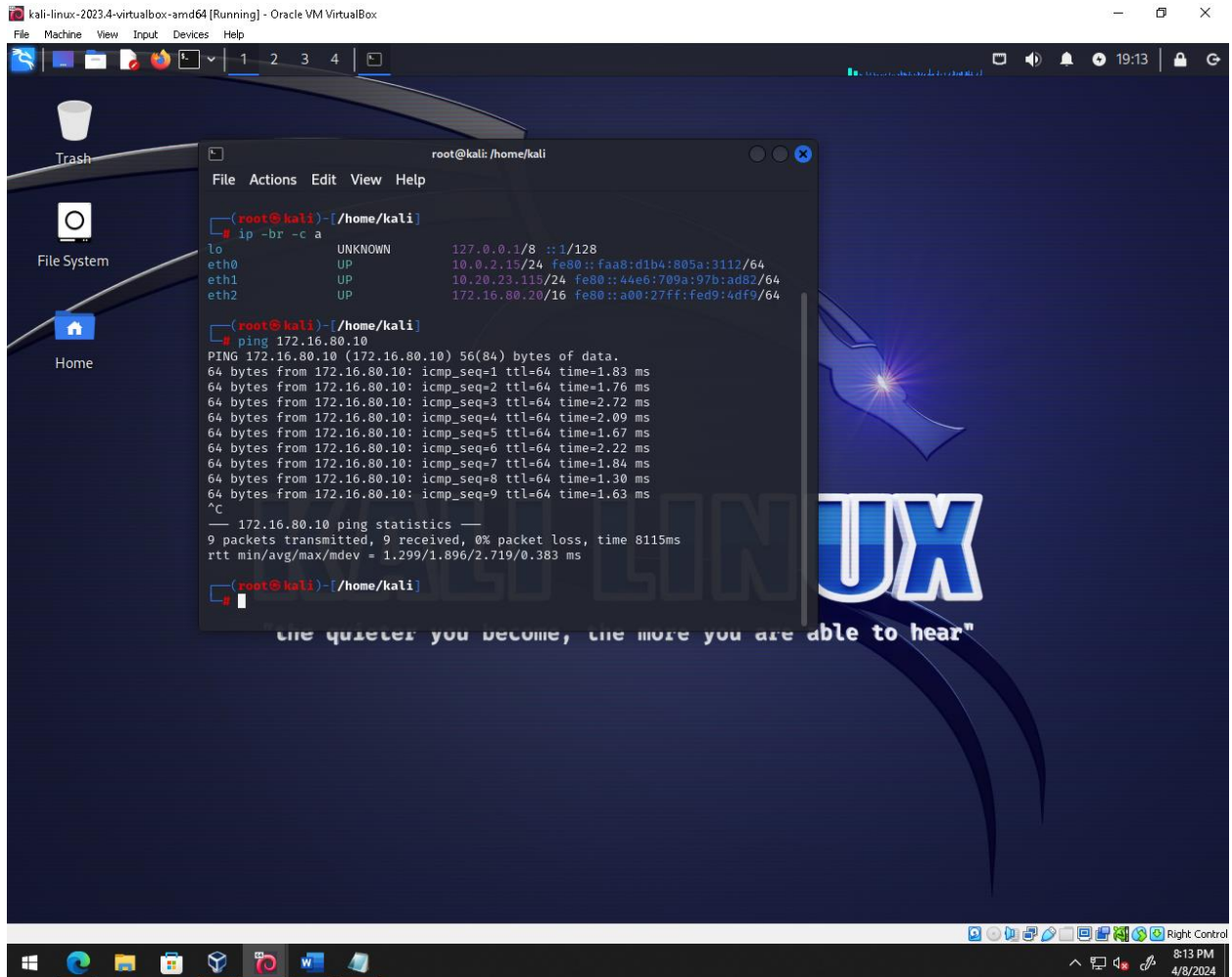
# Terceira placa
allow-hotplug enp0s9
iface enp0s9 inet static
    address 172.16.80.10

root@debian:~# ip -br -c a
lo                UNKNOWN    127.0.0.1/8 ::1/128
enp0s3            UP          10.0.2.15/24 fe80::a00:27ff:febf:37e0/64
enp0s8            DOWN
enp0s9            UP          172.16.80.10/16 fe80::a00:27ff:fe52:7f39/64
root@debian:~#
```


- CLIENTE:



- b. Na máquina Kali rode o comando 'ping 172.16.80.10' e verifique se há resposta do servidor.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the output of the 'ip -br -c a' command, showing network interfaces and their status. Below that, the 'ping 172.16.80.10' command is executed, showing successful ping results with 9 packets transmitted and 9 received, 0% packet loss, and a time of 8115ms.

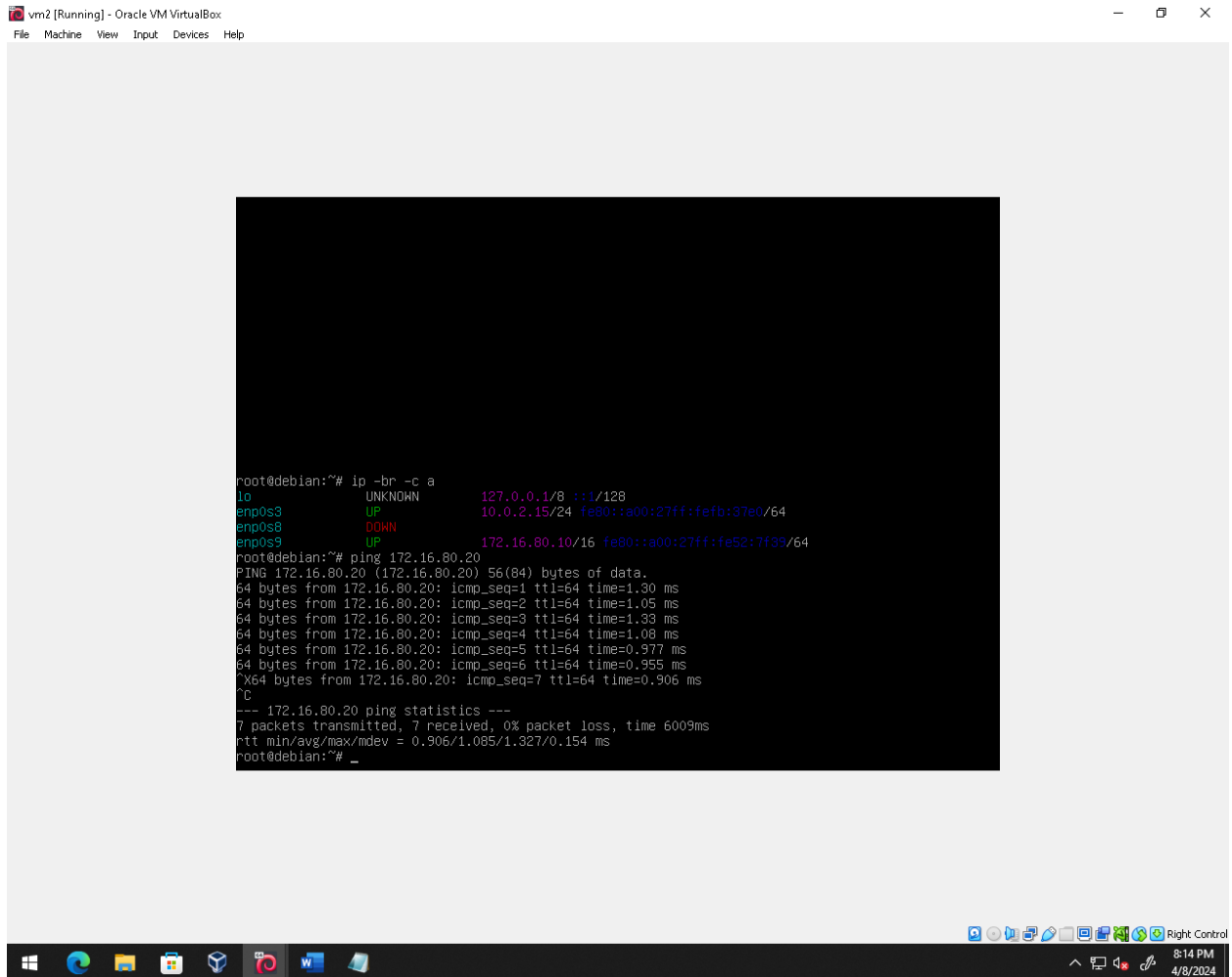
```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)~[/home/kali]
# ip -br -c a
lo UNKNOWN 127.0.0.1/8 ::1/128
eth0 UP 10.0.2.15/24 fe80::faa8:d1b4:805a:3112/64
eth1 UP 10.20.23.115/24 fe80::44e6:709a:97b:ad82/64
eth2 UP 172.16.80.20/16 fe80::a00:27ff:fed9:4df9/64

(root@kali)~[/home/kali]
# ping 172.16.80.10
PING 172.16.80.10 (172.16.80.10) 56(84) bytes of data.
64 bytes from 172.16.80.10: icmp_seq=1 ttl=64 time=1.83 ms
64 bytes from 172.16.80.10: icmp_seq=2 ttl=64 time=1.76 ms
64 bytes from 172.16.80.10: icmp_seq=3 ttl=64 time=2.72 ms
64 bytes from 172.16.80.10: icmp_seq=4 ttl=64 time=2.09 ms
64 bytes from 172.16.80.10: icmp_seq=5 ttl=64 time=1.67 ms
64 bytes from 172.16.80.10: icmp_seq=6 ttl=64 time=2.22 ms
64 bytes from 172.16.80.10: icmp_seq=7 ttl=64 time=1.84 ms
64 bytes from 172.16.80.10: icmp_seq=8 ttl=64 time=1.30 ms
64 bytes from 172.16.80.10: icmp_seq=9 ttl=64 time=1.63 ms
^C
--- 172.16.80.10 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8115ms
rtt min/avg/max/mdev = 1.299/1.896/2.719/0.383 ms

(root@kali)~[/home/kali]
#
```

- c. Na máquina SERVER rode o comando 'ping 172.16.80.20' e verifique se há resposta do servidor.



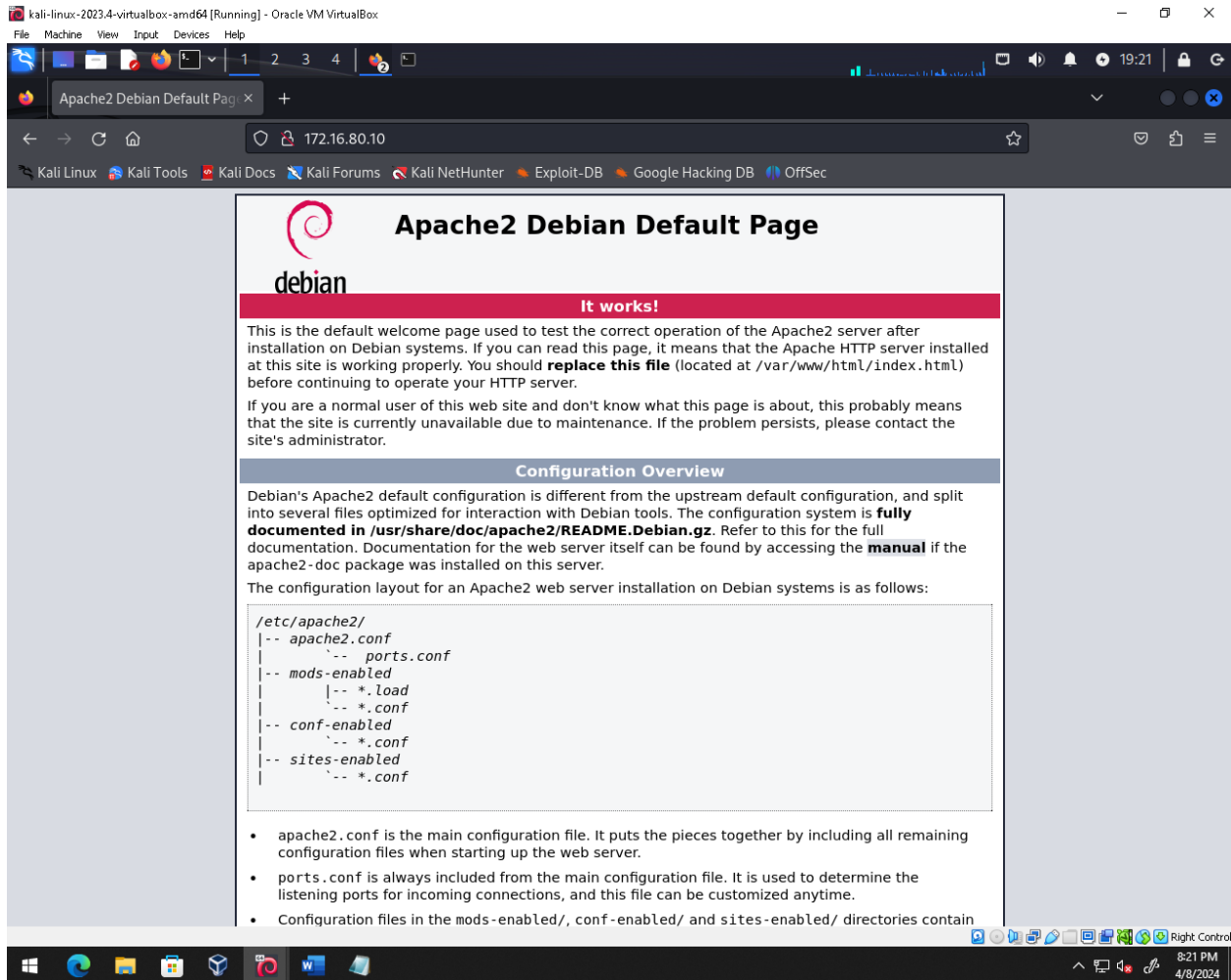
```
vm2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@debian:~# ip -br -c a
lo                UNKNOWN    127.0.0.1/8 ::1/128
enp0s3            UP          10.0.2.15/24 fe80::a00:27ff:fe52:7f39/64
enp0s8            DOWN
enp0s9            UP          172.16.80.10/16 fe80::a00:27ff:fe52:7f39/64
root@debian:~# ping 172.16.80.20
PING 172.16.80.20 (172.16.80.20) 56(84) bytes of data:
64 bytes from 172.16.80.20: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 172.16.80.20: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 172.16.80.20: icmp_seq=3 ttl=64 time=1.33 ms
64 bytes from 172.16.80.20: icmp_seq=4 ttl=64 time=1.08 ms
64 bytes from 172.16.80.20: icmp_seq=5 ttl=64 time=0.977 ms
64 bytes from 172.16.80.20: icmp_seq=6 ttl=64 time=0.955 ms
^X64 bytes from 172.16.80.20: icmp_seq=7 ttl=64 time=0.906 ms
^C
--- 172.16.80.20 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 0.906/1.085/1.327/0.154 ms
root@debian:~# _
```

Com isso verificamos que as máquinas estão se conectando entre si normalmente.

5. Simulando vulnerabilidades

a) Na máquina Kali, abra o Mozilla Firefox e acesse a URL: <http://172.16.80.10>



b) Agora para visualizar a vulnerabilidade, volte na máquina Debian e rode os seguintes comandos:

```
service apache2 stop
```

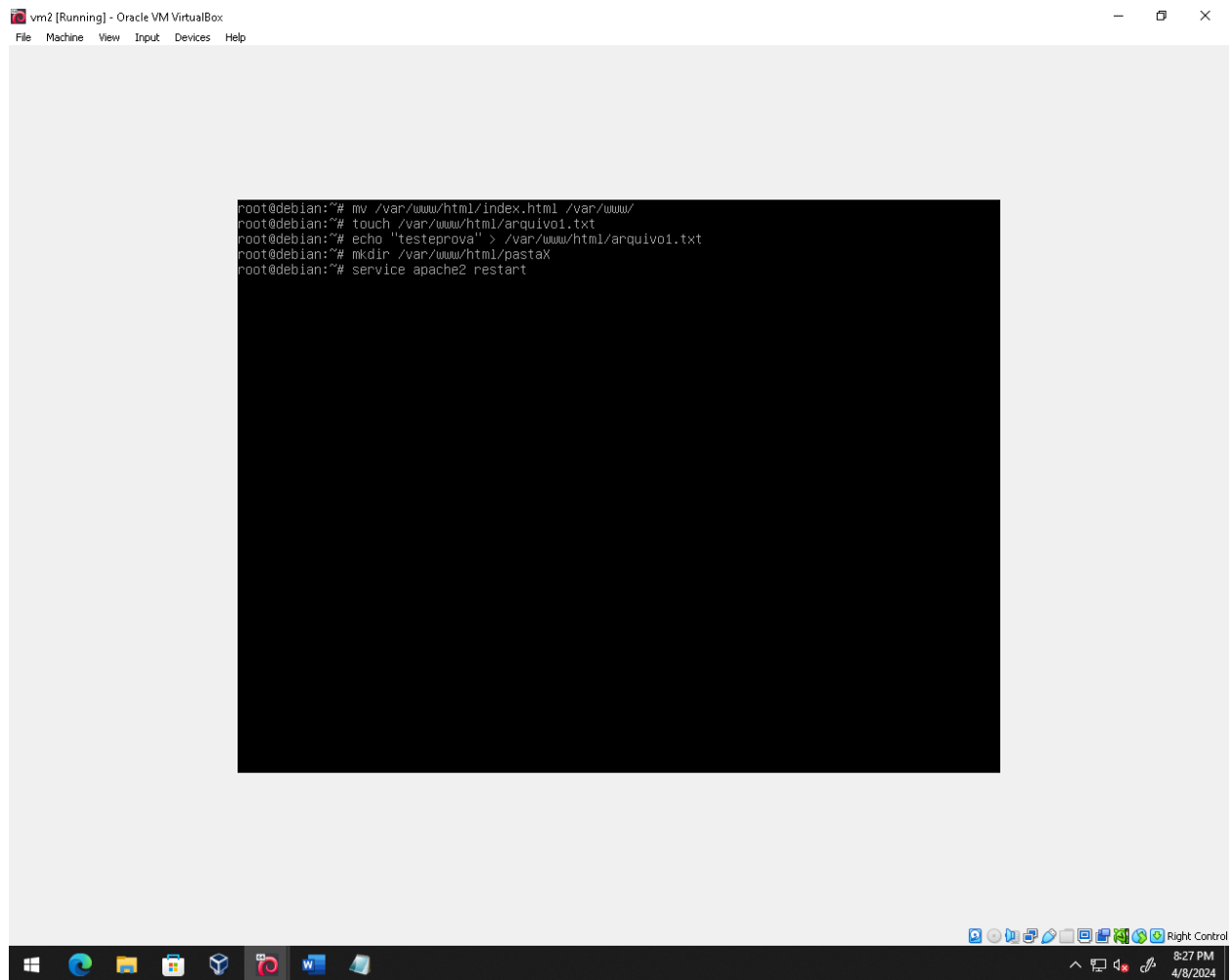
```
mv /var/www/html/index.html /var/www/
```

```
touch /var/www/html/arquivo1.txt
```

```
echo "Teste" > /var/www/html/arquivo1.txt
```

```
mkdir /var/www/html/pastaX
```

```
service apache2 restart
```



c) Agora no kali, criar um arquivo indexTeste.html para testar ele futuramente:

```
include ports.conf

# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Require all denied
</Directory>

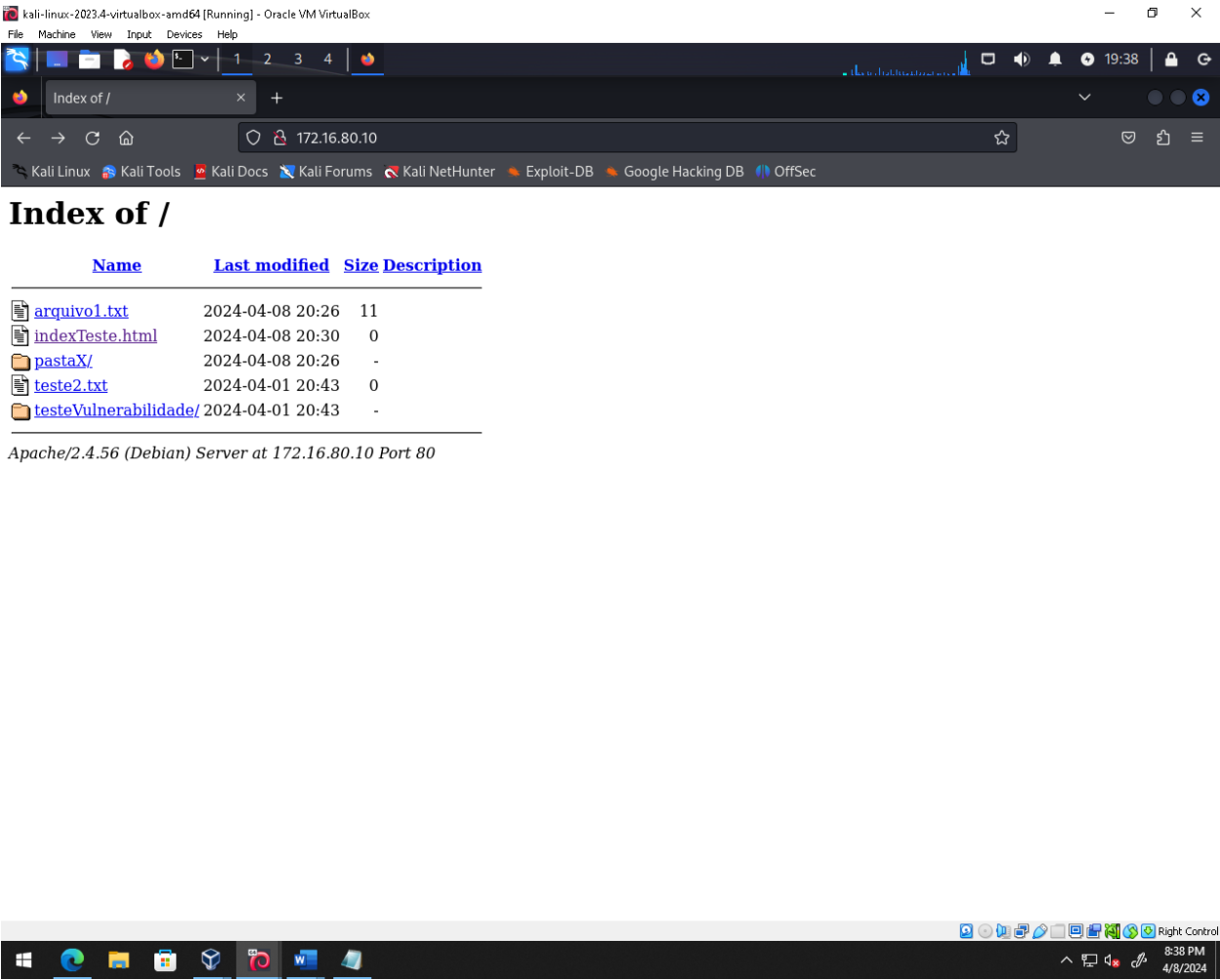
<Directory /usr/share>
    AllowOverride None
    Require all granted
</Directory>

<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

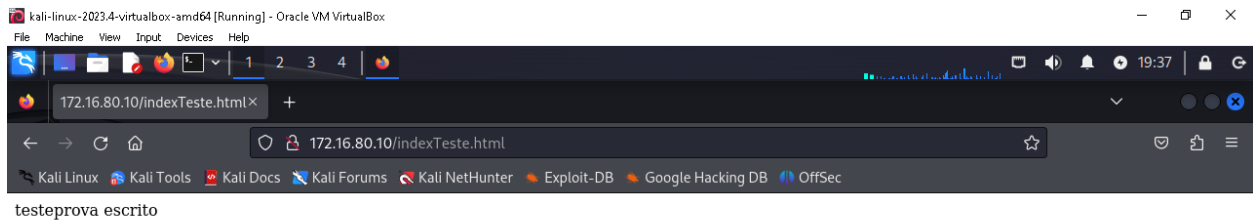
#<Directory /srv/>
#     Options Indexes FollowSymLinks
#     AllowOverride None

root@debian:~# service apache2 restart
root@debian:~# touch /var/www/html/indexTeste.html
root@debian:~# service apache2 restart
root@debian:~# echo "teste prova escrito" > /var/www/html/indexTeste.html
root@debian:~# service apache2 restart
root@debian:~#
```

d) Depois vamos reiniciar o servidor e recarregar a página no KALI:



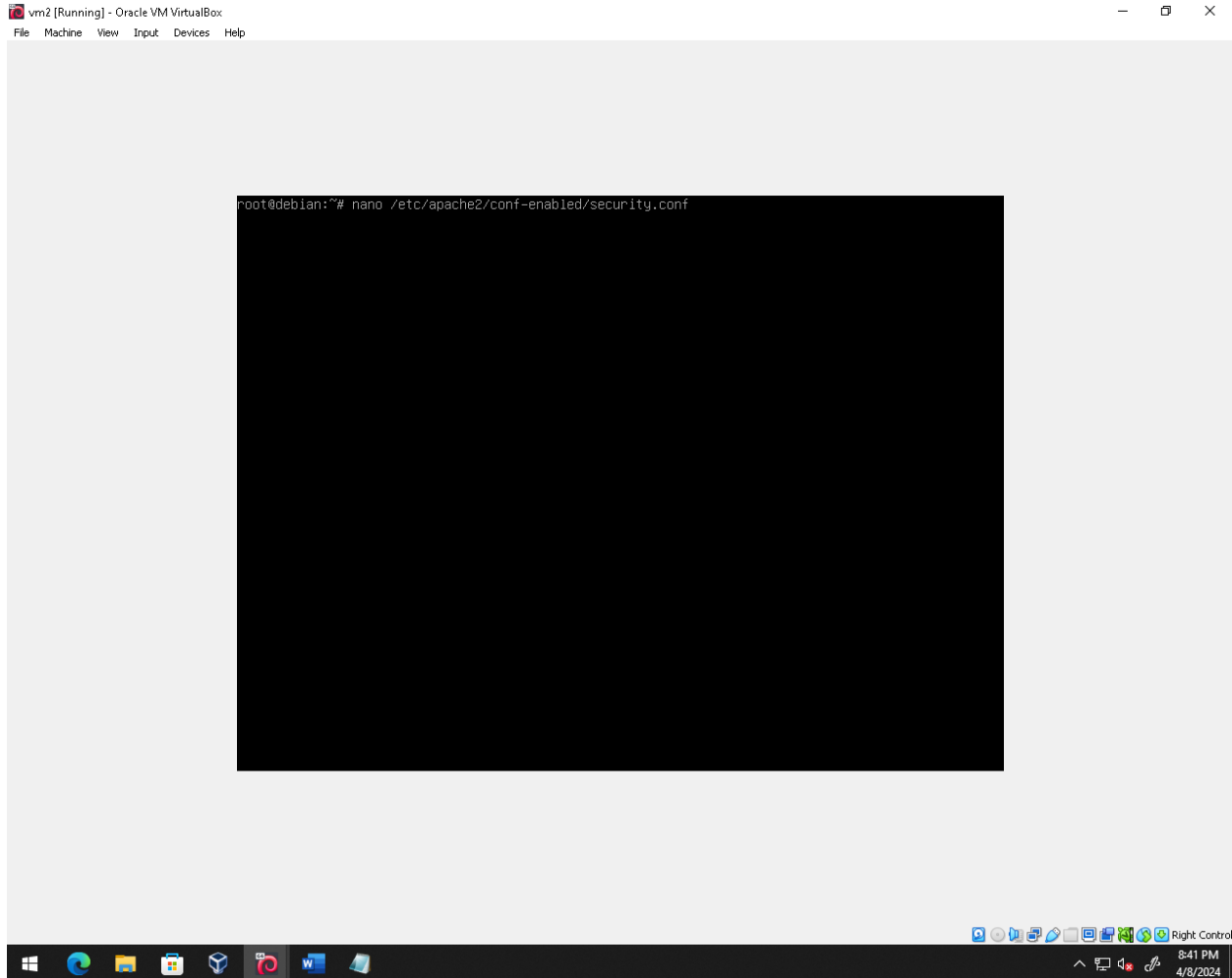
e) Ao clicar no arquivo IndexTeste.html:



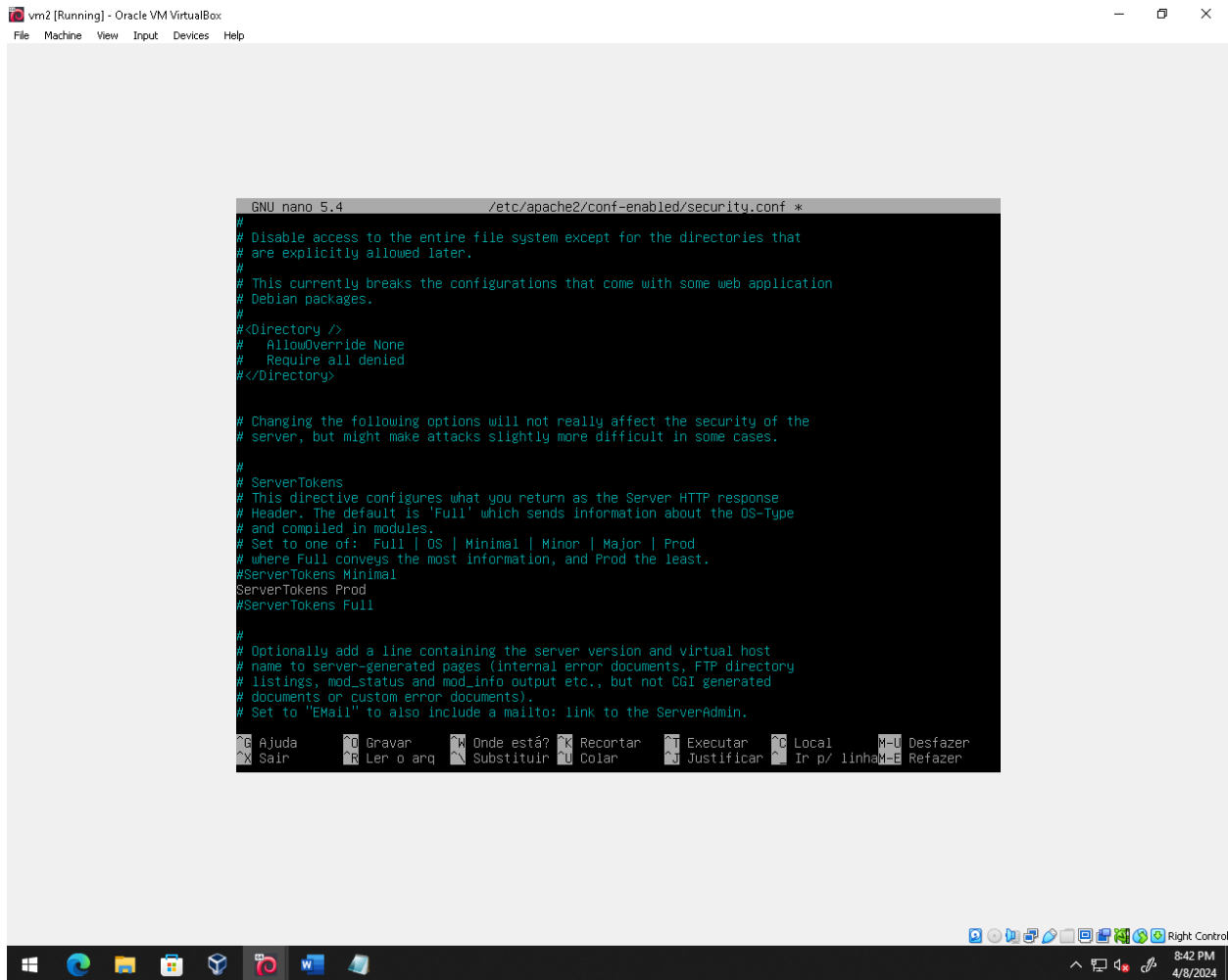
Podemos perceber que estamos mostrando a versão do servidor e o IP, para retirar isso vamos precisar configurar algumas coisas.

6. Corrigindo a vulnerabilidade:

- a. Para corrigir a vulnerabilidade, precisamos alterar algumas configurações do apache2.
- b. Primeiro vamos configurar o servidor para o modo produção, de forma que esconda o SO e a versão do servidor.
- c. Na máquina Debian rode o comando 'nano /etc/apache2/conf-enabled/security.conf'



- d. Nesse arquivo vamos precisar alterar o parâmetro seguinte: no arquivo onde estiver escrito 'ServerTokens OS', troque o 'OS' para 'Prod'



e. Altere onde estiver escrito 'ServerSignature On' para 'ServerSignature Off'

vm2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
GNU nano 5.4 /etc/apache2/conf-enabled/security.conf *
# AllowOverride None
# Require all denied
#</Directory>

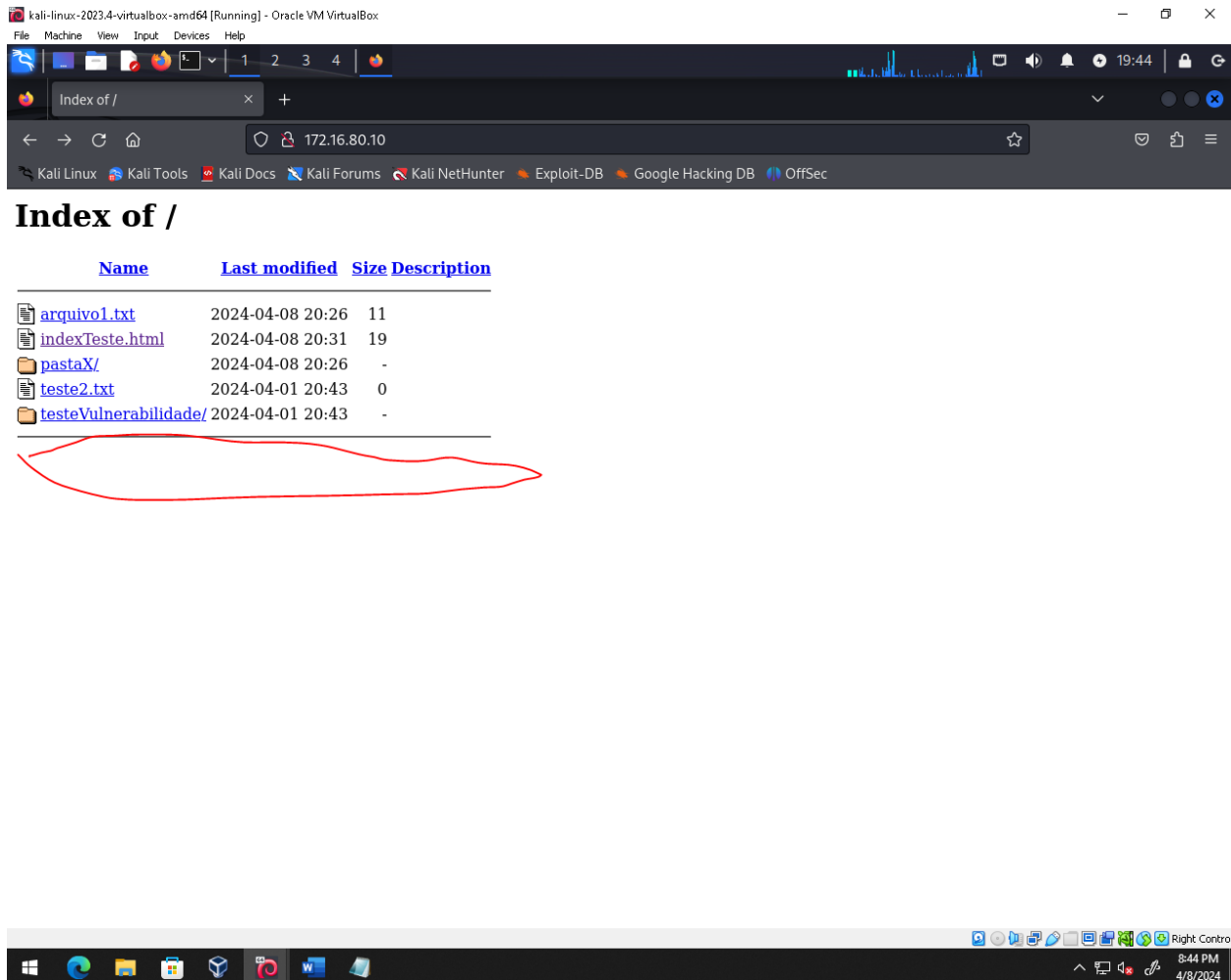
# Changing the following options will not really affect the security of the
# server, but might make attacks slightly more difficult in some cases.

#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of: Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens Prod
#ServerTokens Full
#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "Email" to also include a mailto: link to the ServerAdmin.
# Set to one of: On | Off | Email
#ServerSignature Off
ServerSignature Off
#
# Allow TRACE method
#
# Set to "extended" to also reflect the request body (only for testing and
```

Ajuda Gravar Onde está? Recortar Executar Local M-L Desfazer
Sair Ler o arq Substituir Colar Justificar In p/ linha E Refazer

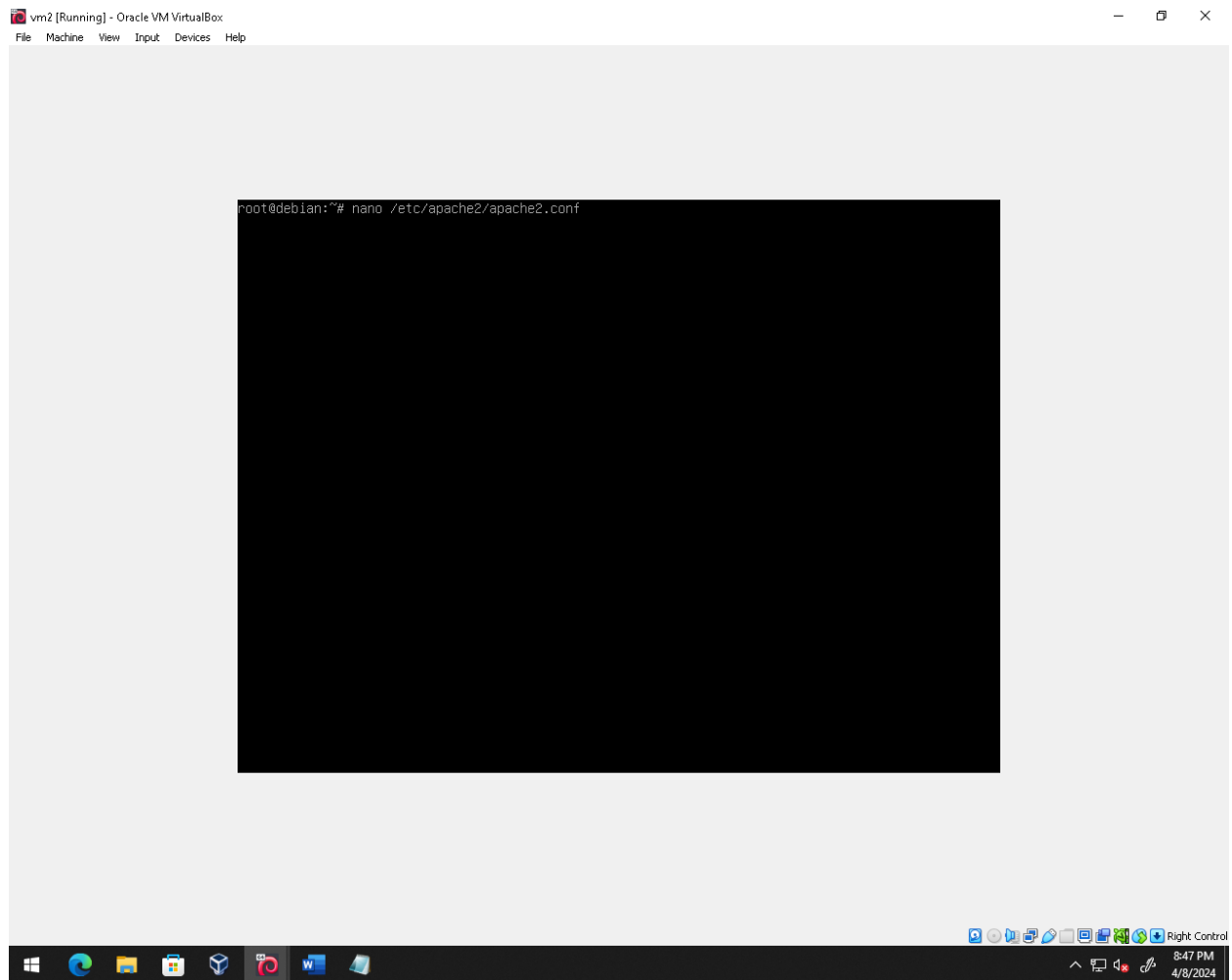
Right Control 8:43 PM 4/8/2024

- f. Aperte 'Ctrl O' -> Enter -> 'Ctrl X'
- g. Reinicie o serviço com o comando 'service apache2 stop' -> 'service apache2 start'
- h. Na máquina Kali recarregue a guia do Mozilla

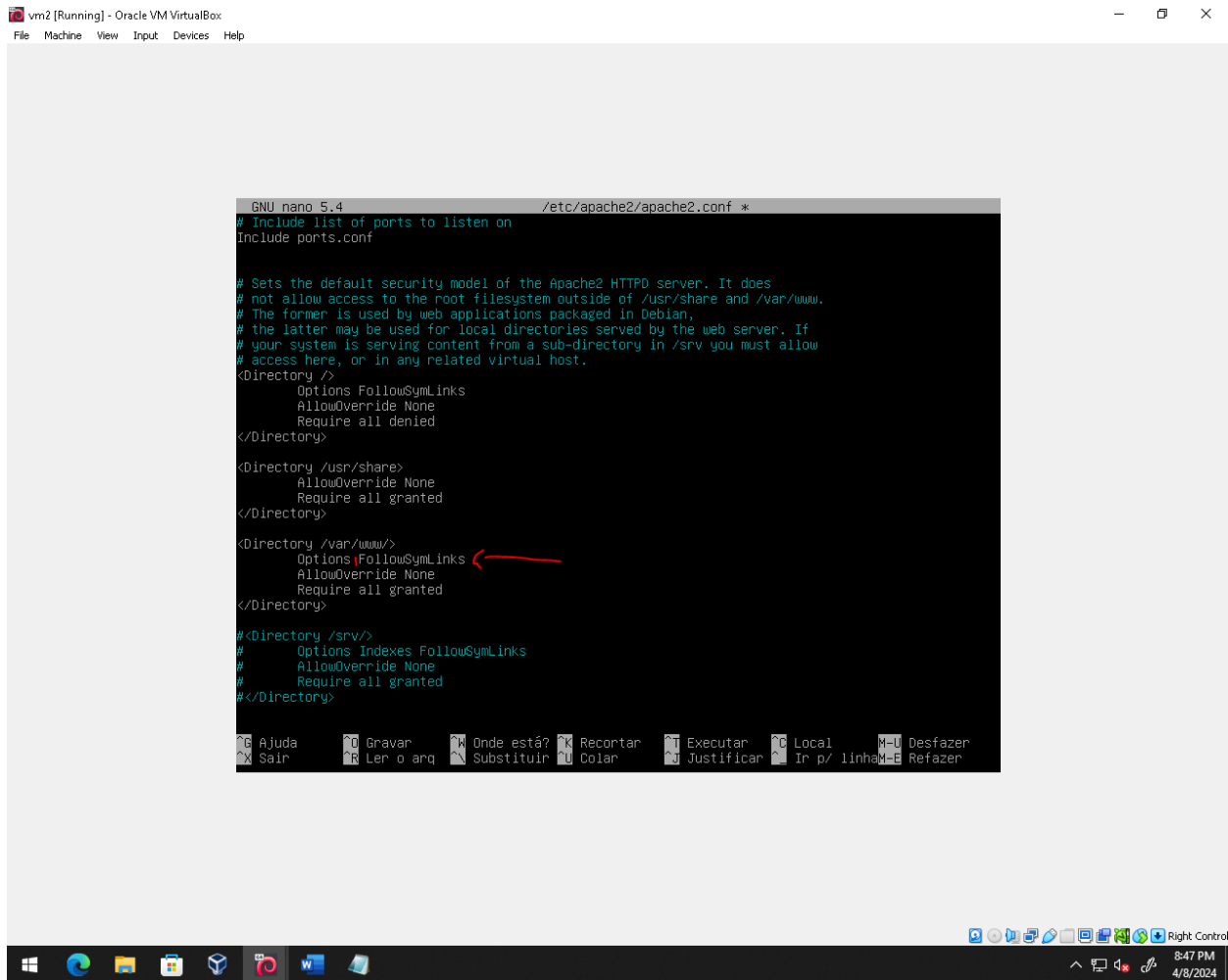


Perceba que o banner exibindo informações do servidor e do sistema operacional sumiram.

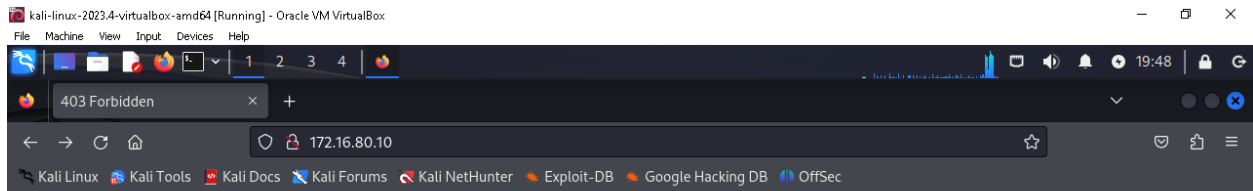
- i. Agora para impedir o acesso à tela com as pastas e arquivos do servidor, precisamos realizar uma outra configuração.
- j. Rode o comando no Debian 'nano /etc/apache2/apache2.conf'



- k. Procure pelo texto '<Directory /var/www/>', e na linha abaixo, remova a palavra 'Indexes'



- I. Reinicie o serviço com o comando 'service apache2 stop' -> 'service apache2 start'
- m. Na máquina Kali, recarregue a guia

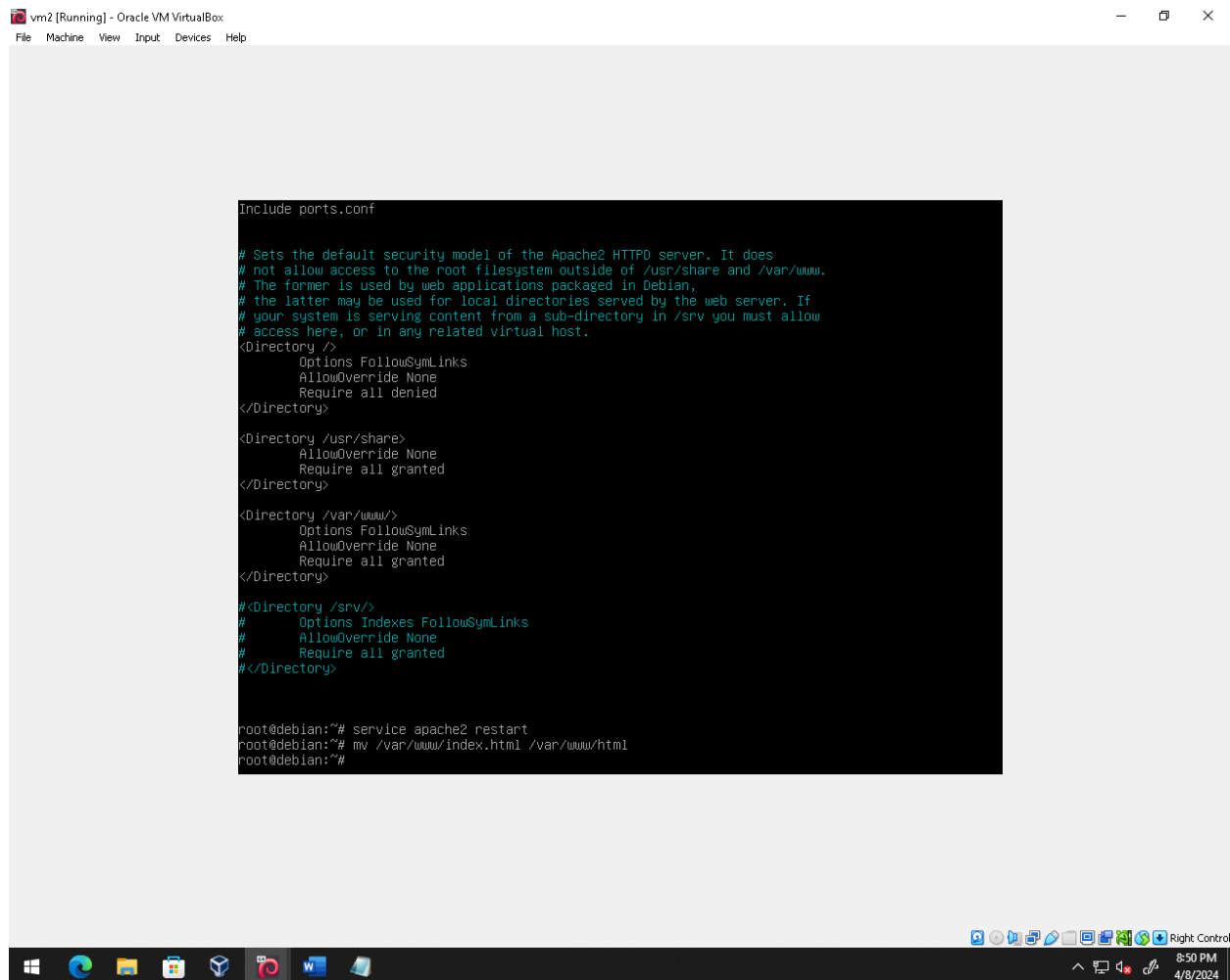


Forbidden

You don't have permission to access this resource.



- n. Perceba que agora já não conseguimos mais ver os arquivos do servidor
- o. Agora podemos adicionar um index.html novamente para visualizar a tela inicial do servidor.
- p. Para isso rode o comando `'mv /var/www/index.html /var/www/html/'`,



- q. Reinicie o servidor com os comandos 'service apache2 stop' e 'service apache2 start'
- r. Na máquina Kali recarregue a guia e perceba que a tela exibe o que aparecia antes:


kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

FileMachineViewInputDevicesHelp

1234

172.16.80.10

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

 **Apache2 Debian Default Page**

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. 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

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian 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 Debian 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

8:51 PM
4/8/2024