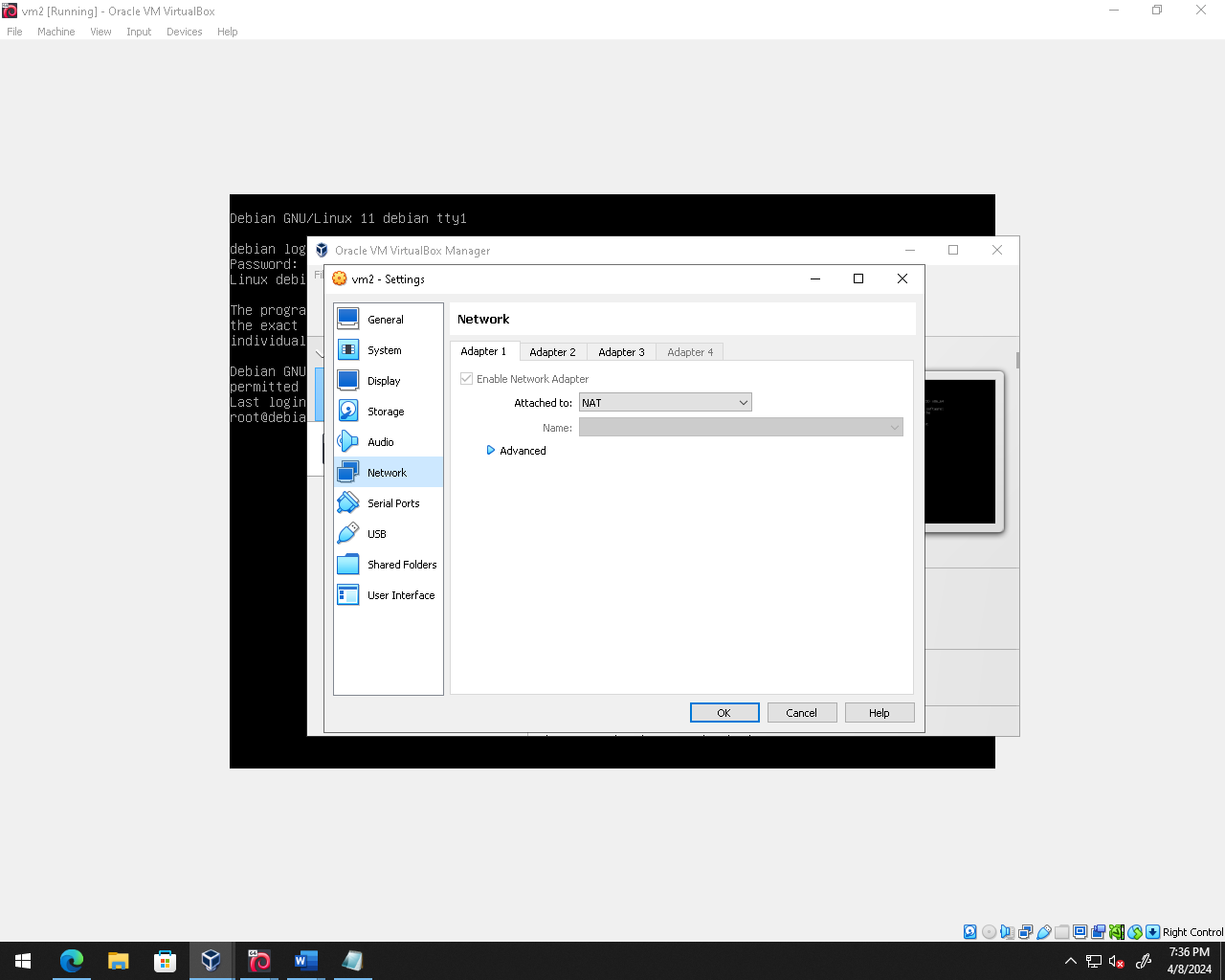
**Aluno: Breno de Souza Silva - 04/08/2024**

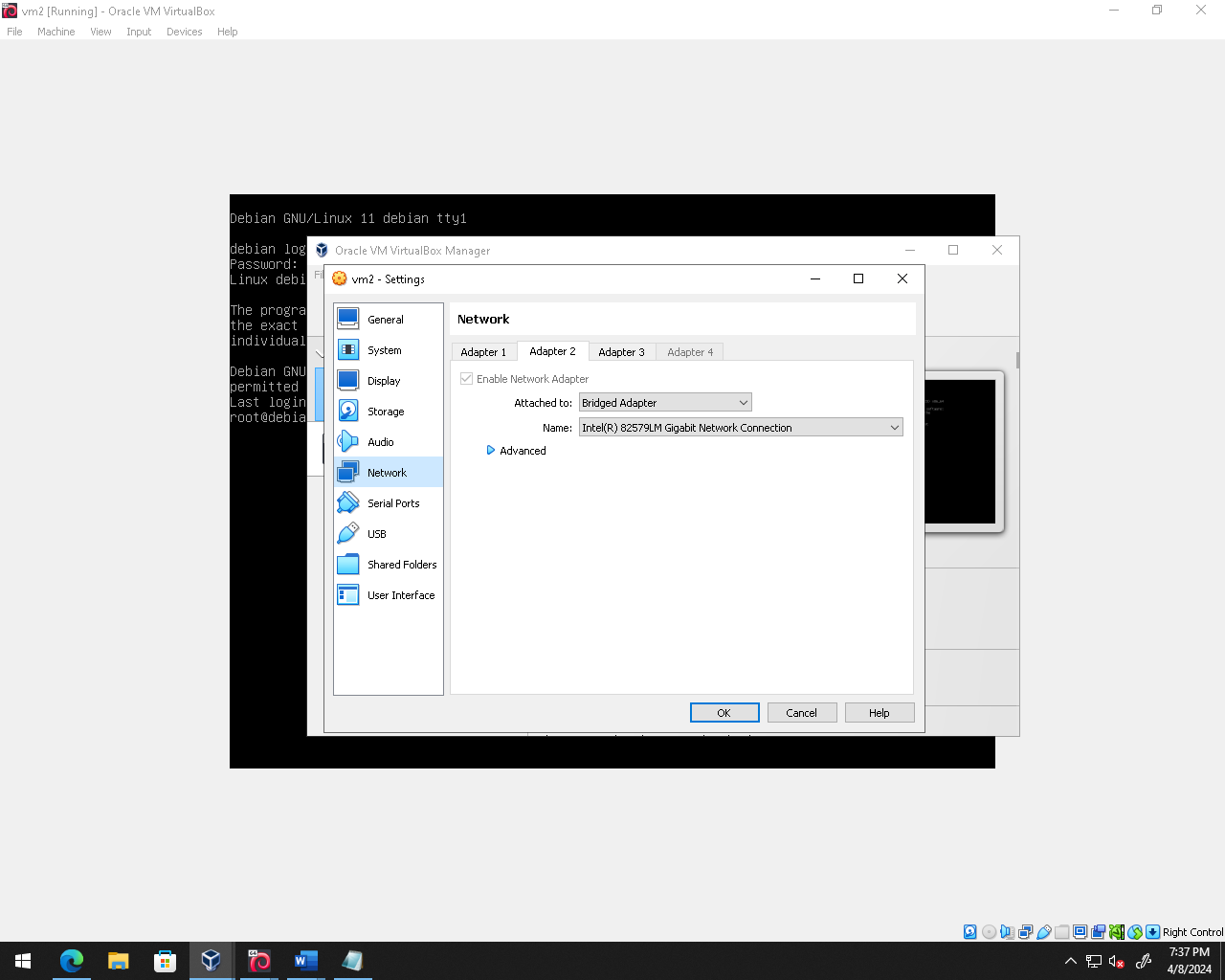
**Checkpoint 1 – CyberSecurity for Dev**

**Relatório Técnico de CyberSecurity**

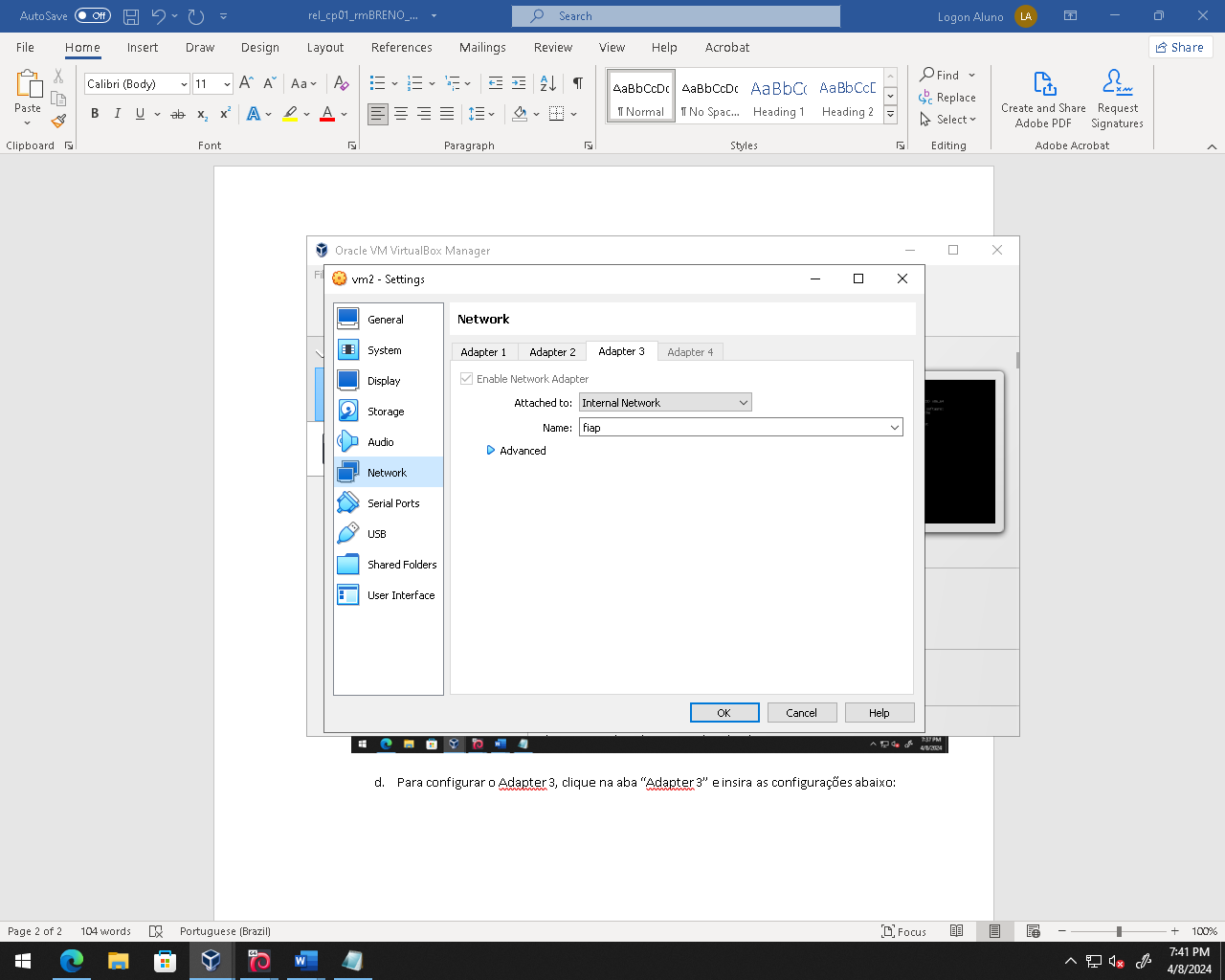
Considerando o cenário abaixo para este relatório:

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

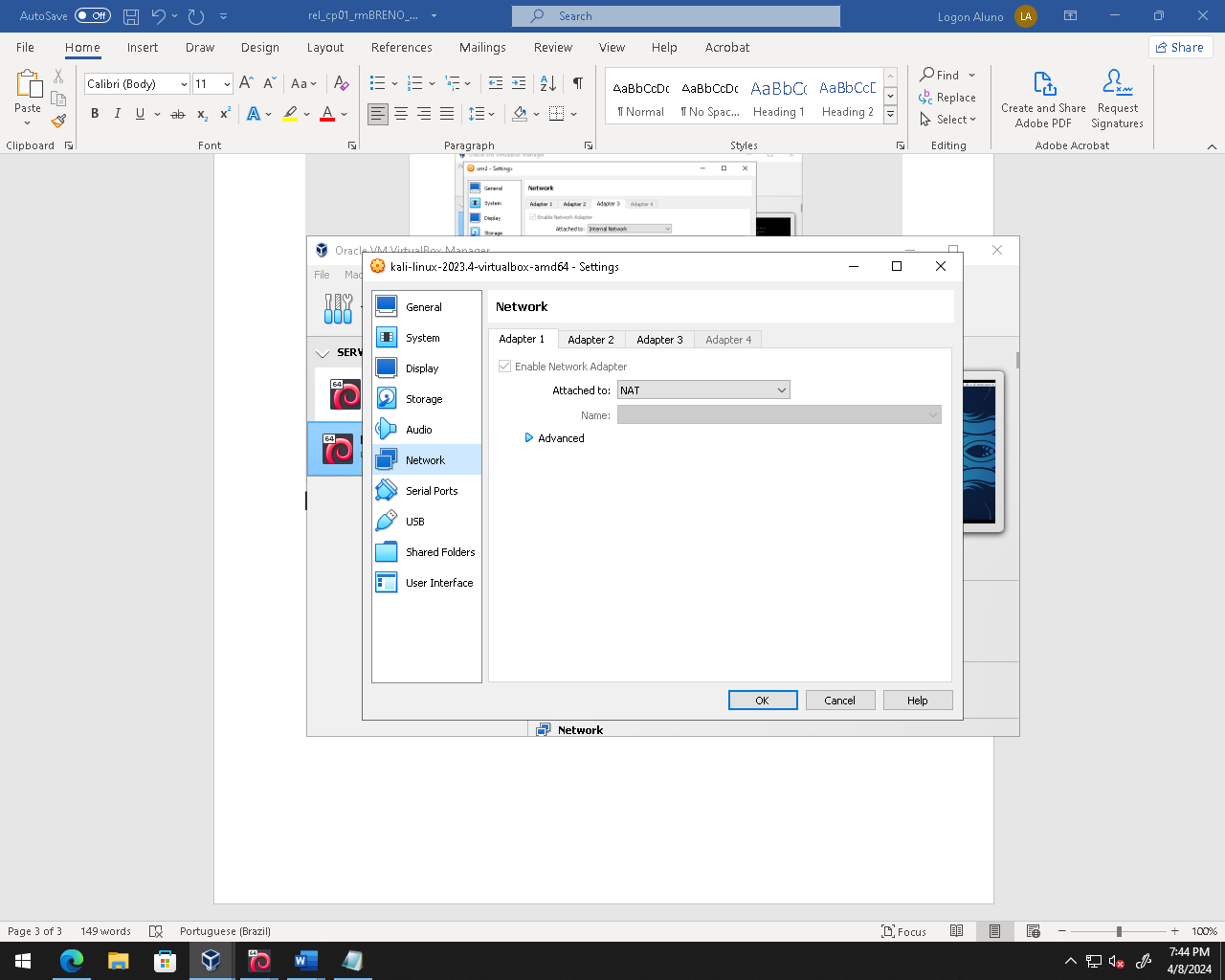
1. **Iremos configurar as VMs e a comunicação entre Server x Cliente**
   1. Configurar as duas VMs para funcionar inicialmente:
   2. Na VM referente ao Server, clique em Settings e vá para a aba de Network para configurarmos a rede interna.
   3. Para configurar o Adapter 2, clique na aba “Adapter 2” e insira as configurações abaixo:



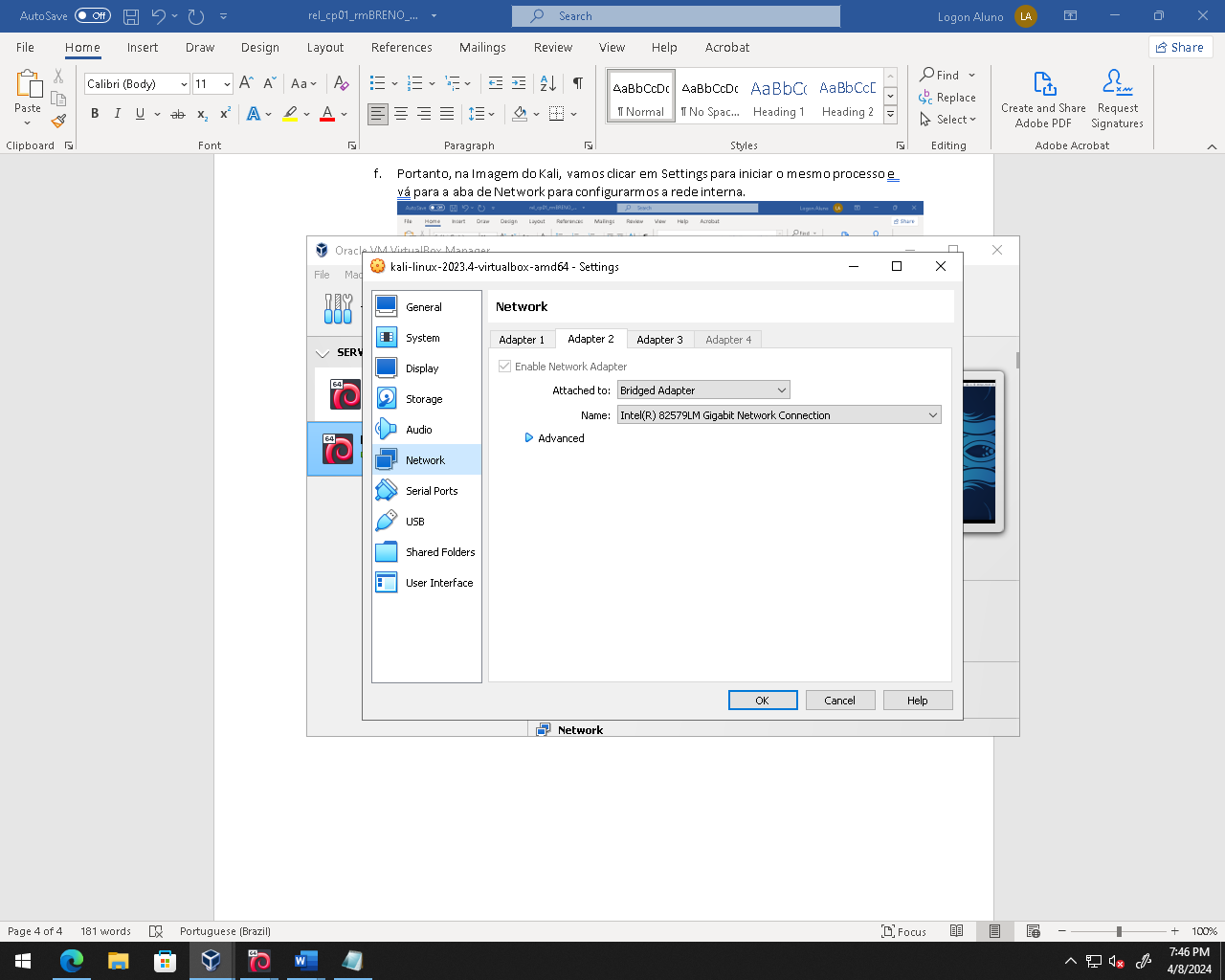
* 1. Para configurar o Adapter 3, clique na aba “Adapter 3” e insira as configurações abaixo:



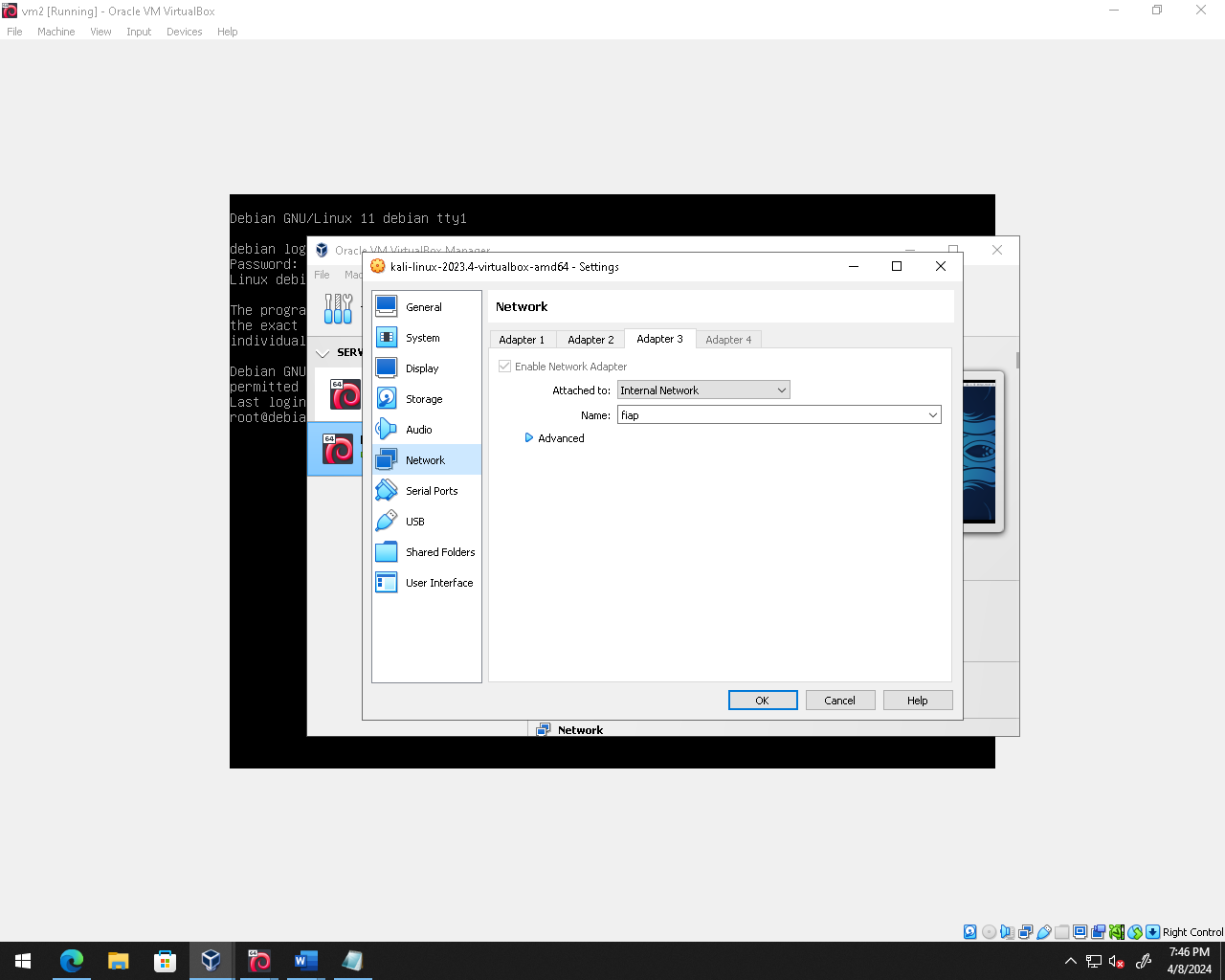
* 1. Agora precisamos repetir os mesmos passos, entretanto na VM referente ao cliente que é o KALI.
  2. Portanto, na Imagem do Kali, vamos clicar em Settings para iniciar o mesmo processo e vá para a aba de Network para configurarmos a rede interna.



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

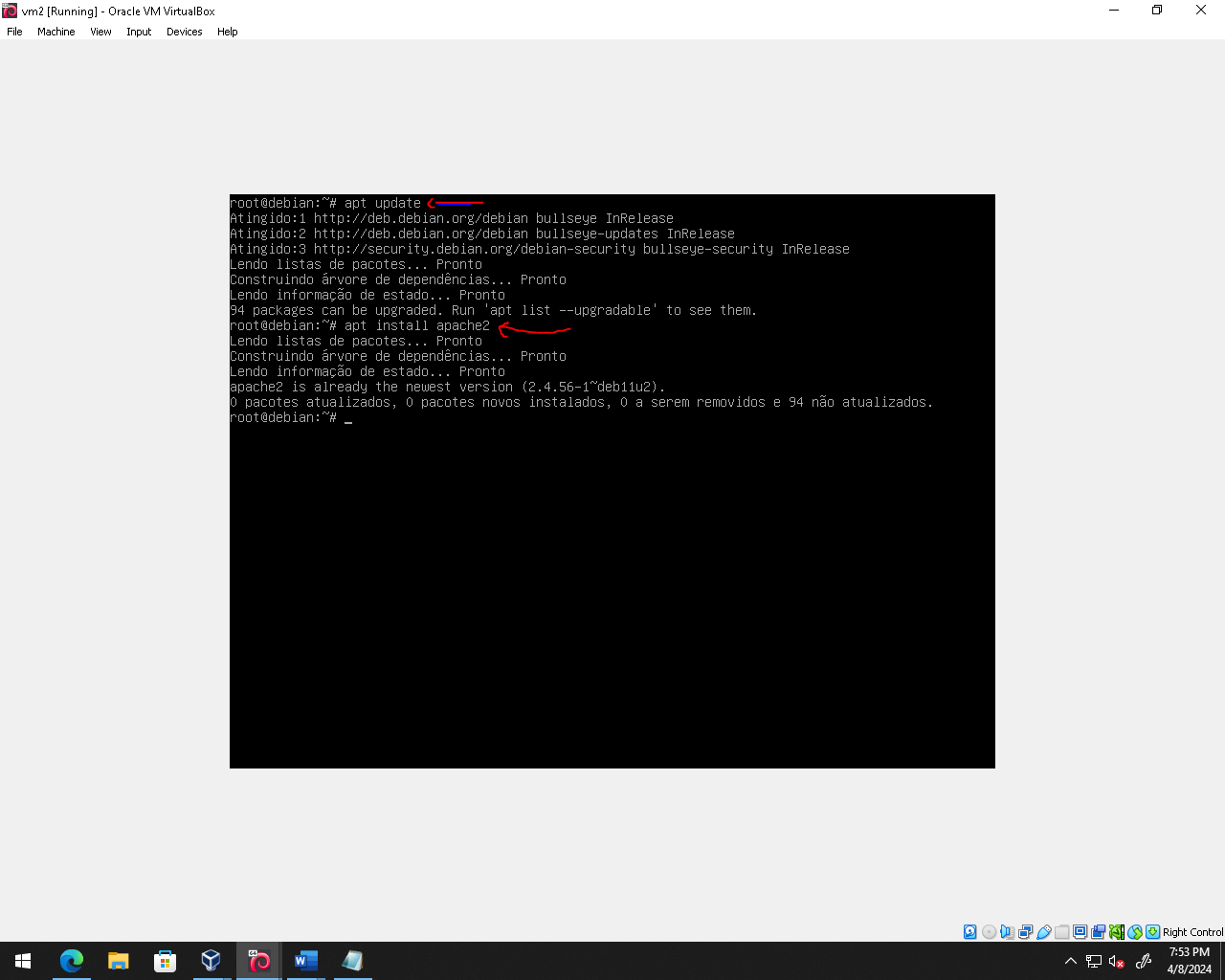


* 1. Para configurar o Adapter 3, clique na aba “Adapter 3” e insira as configurações abaixo:

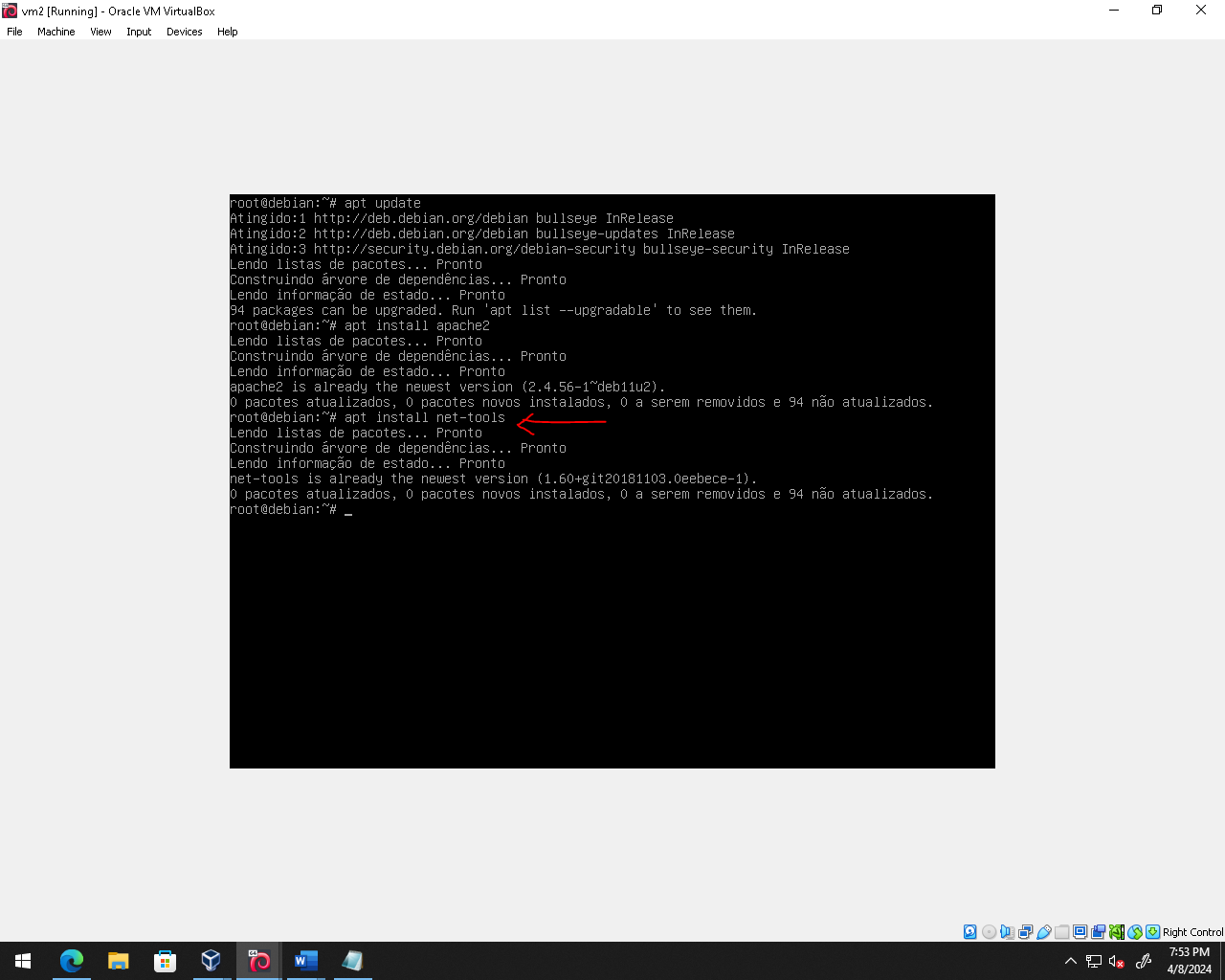


* 1. Agora precisamos, Iniciar as duas máquinas, logando com o usuário root
     1. VM Debian - User root – Senha fiap
     2. VM Kali – User kali – Senha kali

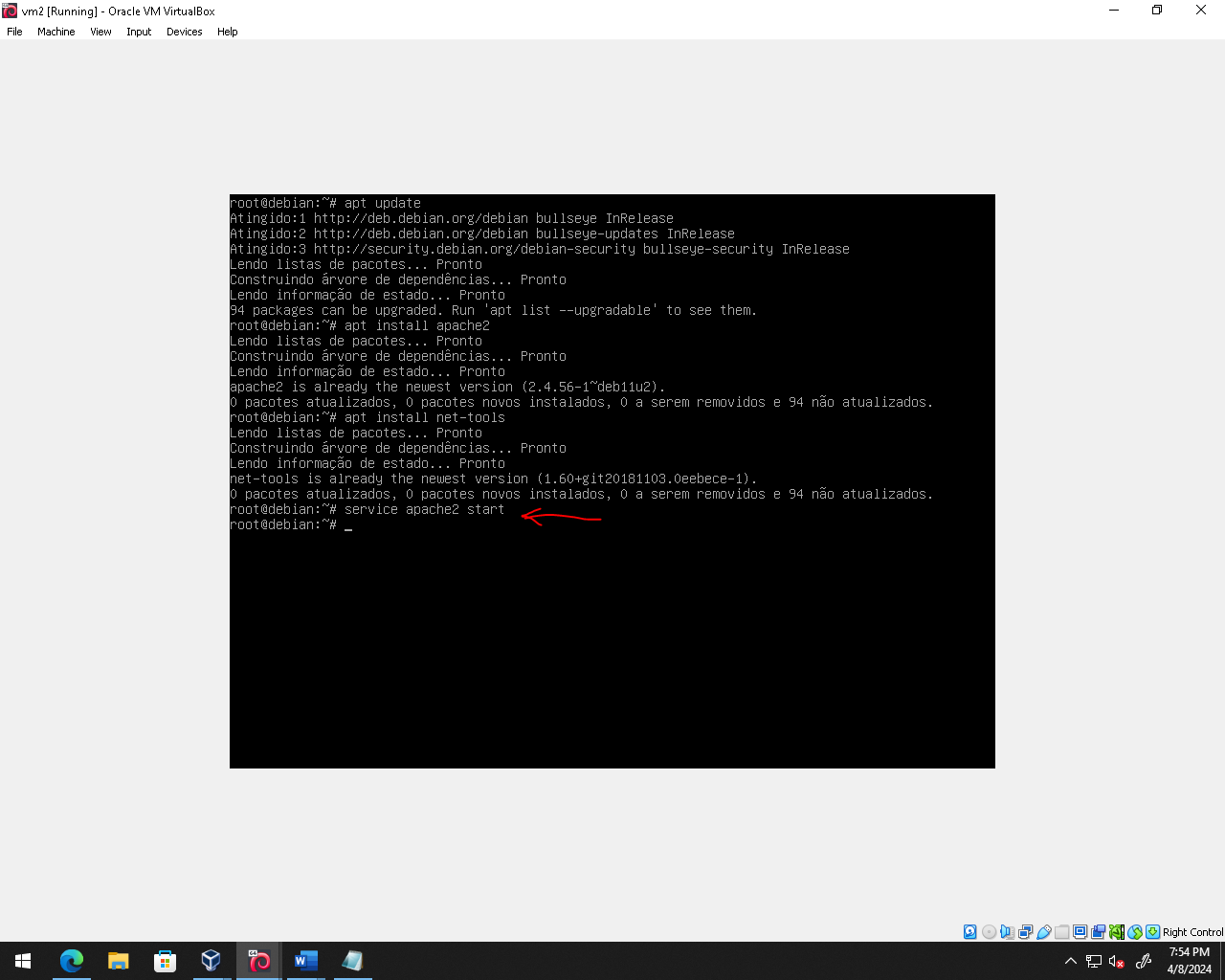
1. Configurando o Servidor:
   1. Primeiro iremos precisar instalar o serviço apache2 no nosso servidor.
   2. Na máquina Debian rode o comando ‘apt update’ e em seguida ‘apt install apache2’ (digite ‘S’ se solicitado)



* 1. Instale o pacote ‘net-tools’ para facilitar o uso do serviço apache2. Para isso rode o comando ‘apt install net-tools’

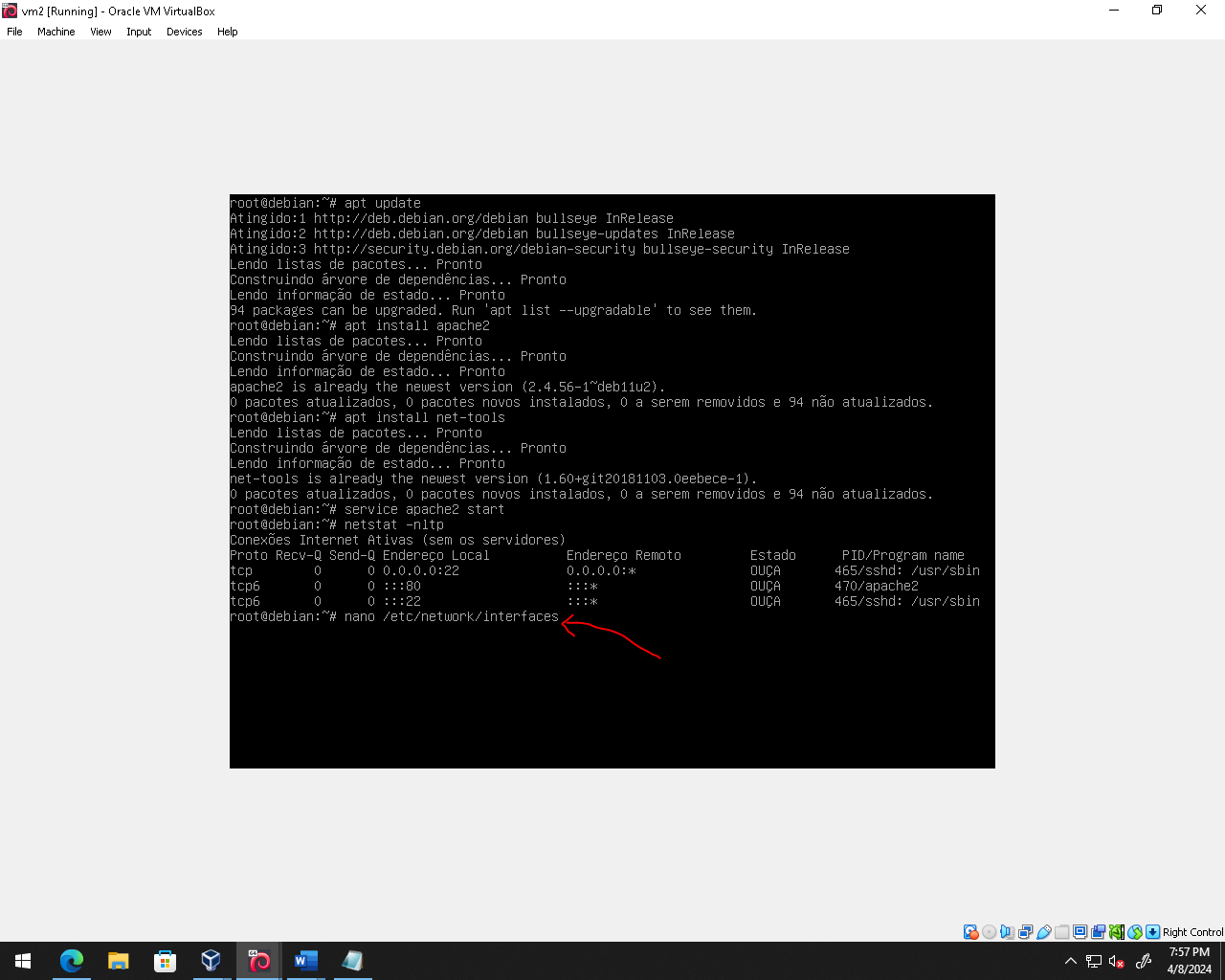


* 1. Para iniciar o serviço apache2 rode o comando ‘service apache2 start’



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.  


* 1. Agora vamos configurar o arquivo ‘Interfaces’ da pasta network para terminar a configuração da placa de rede.
  2. Rodar o seguinte comando em cada uma das máquinas: ‘nano /etc/network/interfaces’



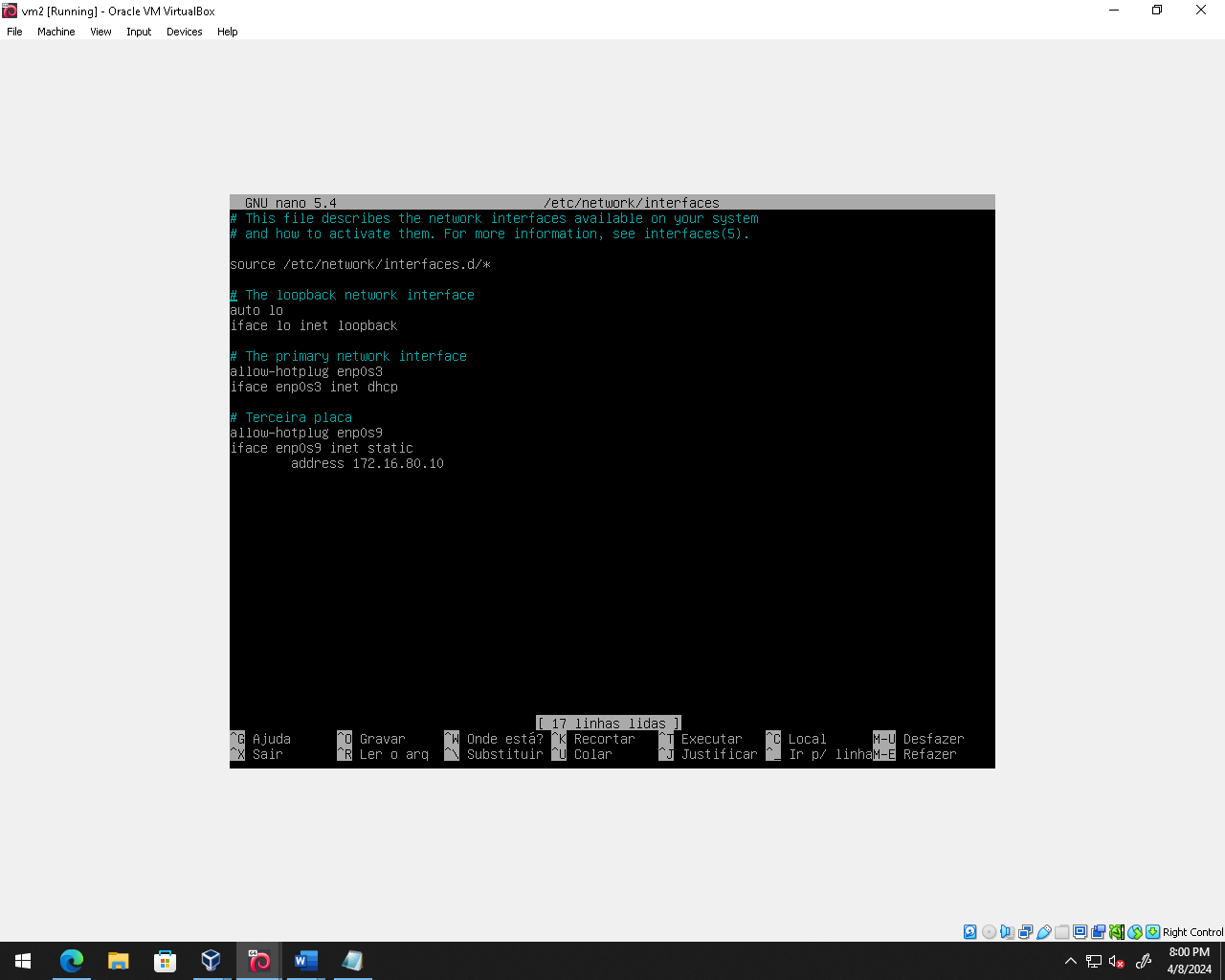
* 1. No arquivo final do arquivo, vamos digitar o seguintes linhas para configurar o arquivo:

# Terceira Placa – fiap

allow-hotplug enp0s9

iface enp0s9 inet static

address 172.16.80.10



* 1. Aperte as teclas ‘Ctrl O’ -> ‘Enter’ -> ‘Ctrl X’ para salvar o arquivo e configuração
  2. Digite o comando ‘init 6’ para reiniciar a máquina com a nova configuração

1. Configurando o Cliente:
   1. Na máquina Kali, rode o comando ‘sudo su’, digitando a senha ‘kali’ quando necessário.



* 1. Rodar o seguinte comando em cada uma das máquinas: ‘nano /etc/network/interfaces’



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

# Terceira Placa – fiap

allow-hotplug eth2

iface eth2 inet static

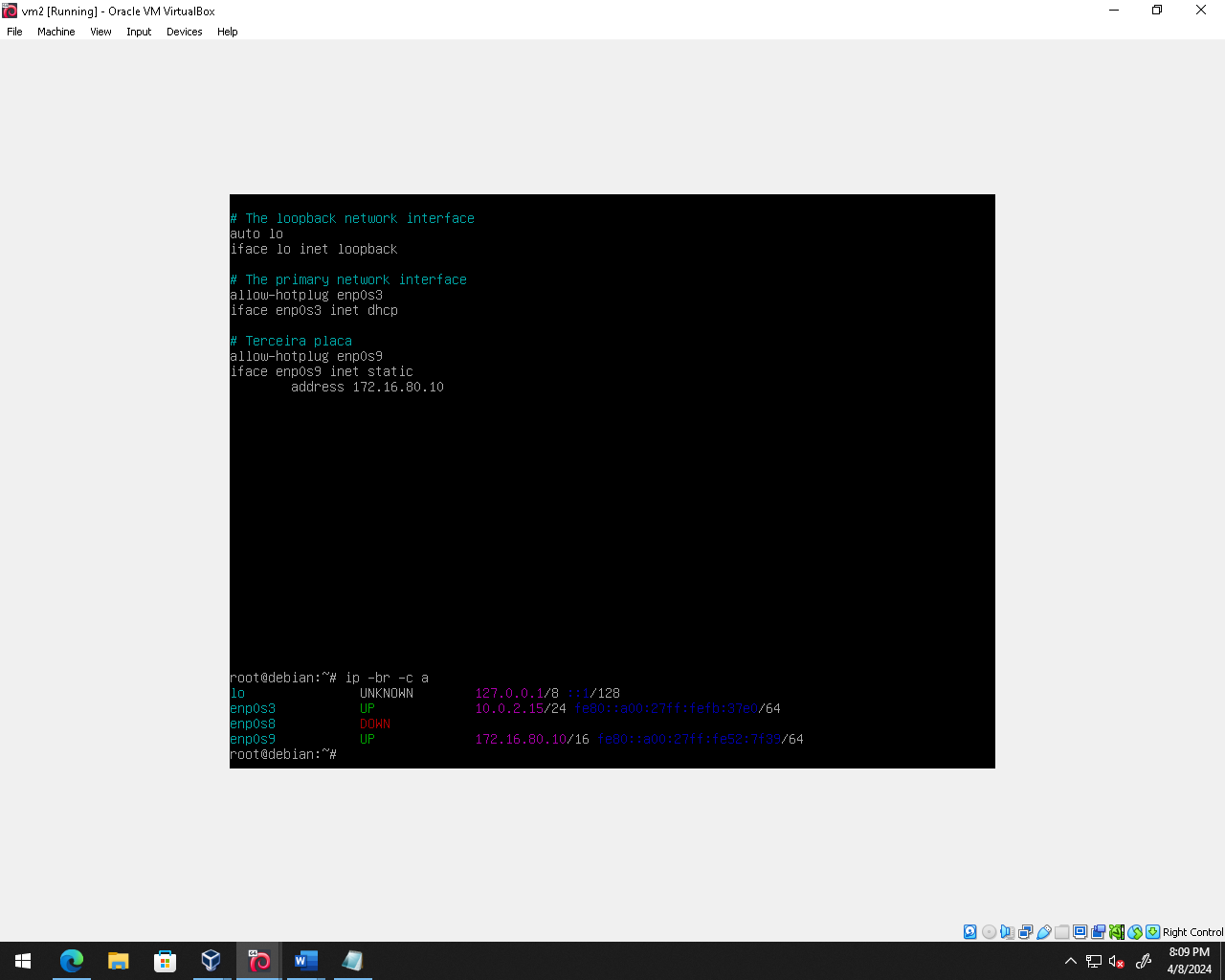
address 172.16.80.20



* 1. Ainda no Kali, aperte as teclas ‘Ctrl O’ -> ‘Enter’ -> ‘Ctrl X’
  2. Digite o comando ‘init 6’ para reiniciar a máquina com a nova configuração

1. Verificando a comunicação entre Servidor e Cliente:
   1. 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.

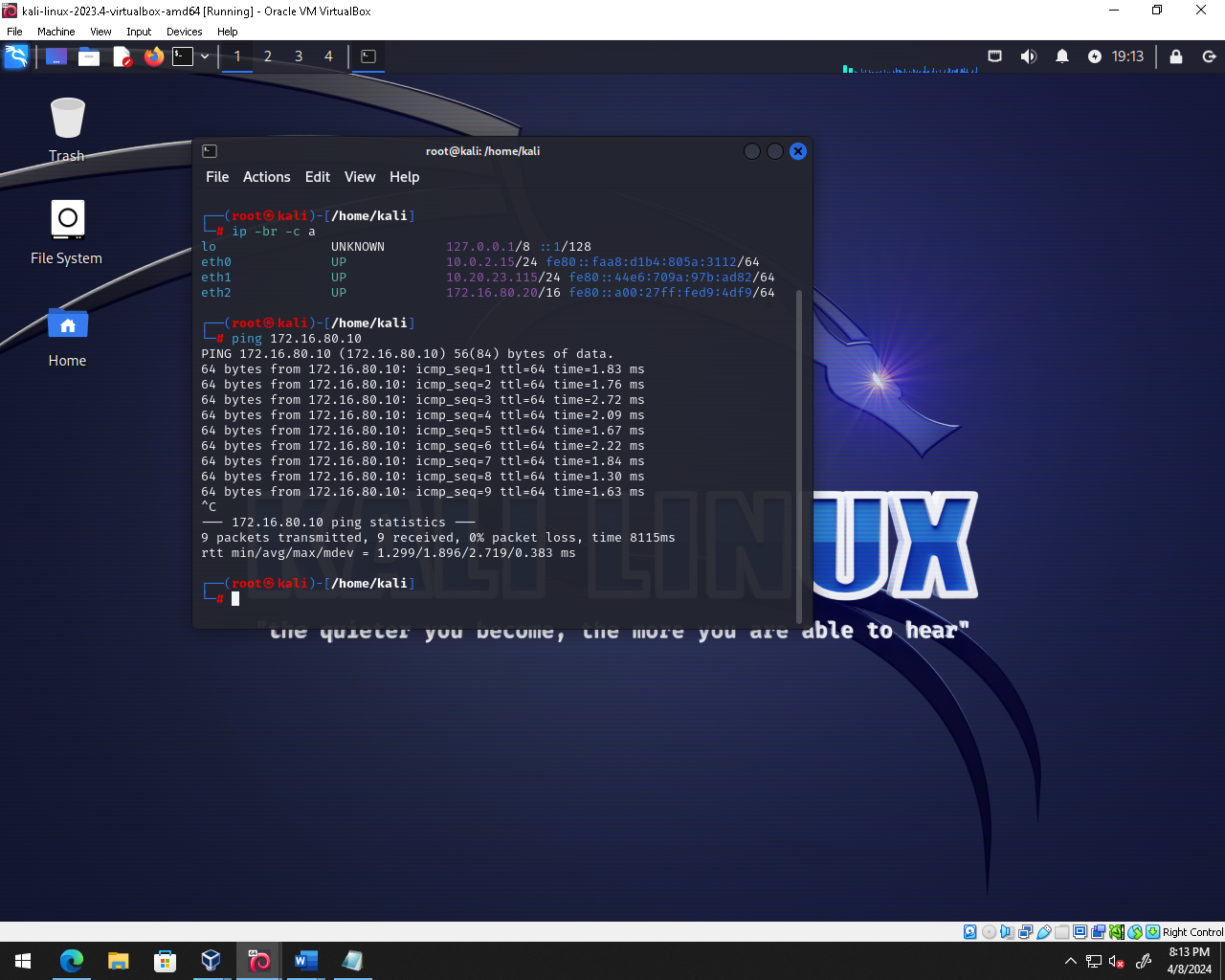
* SERVER:



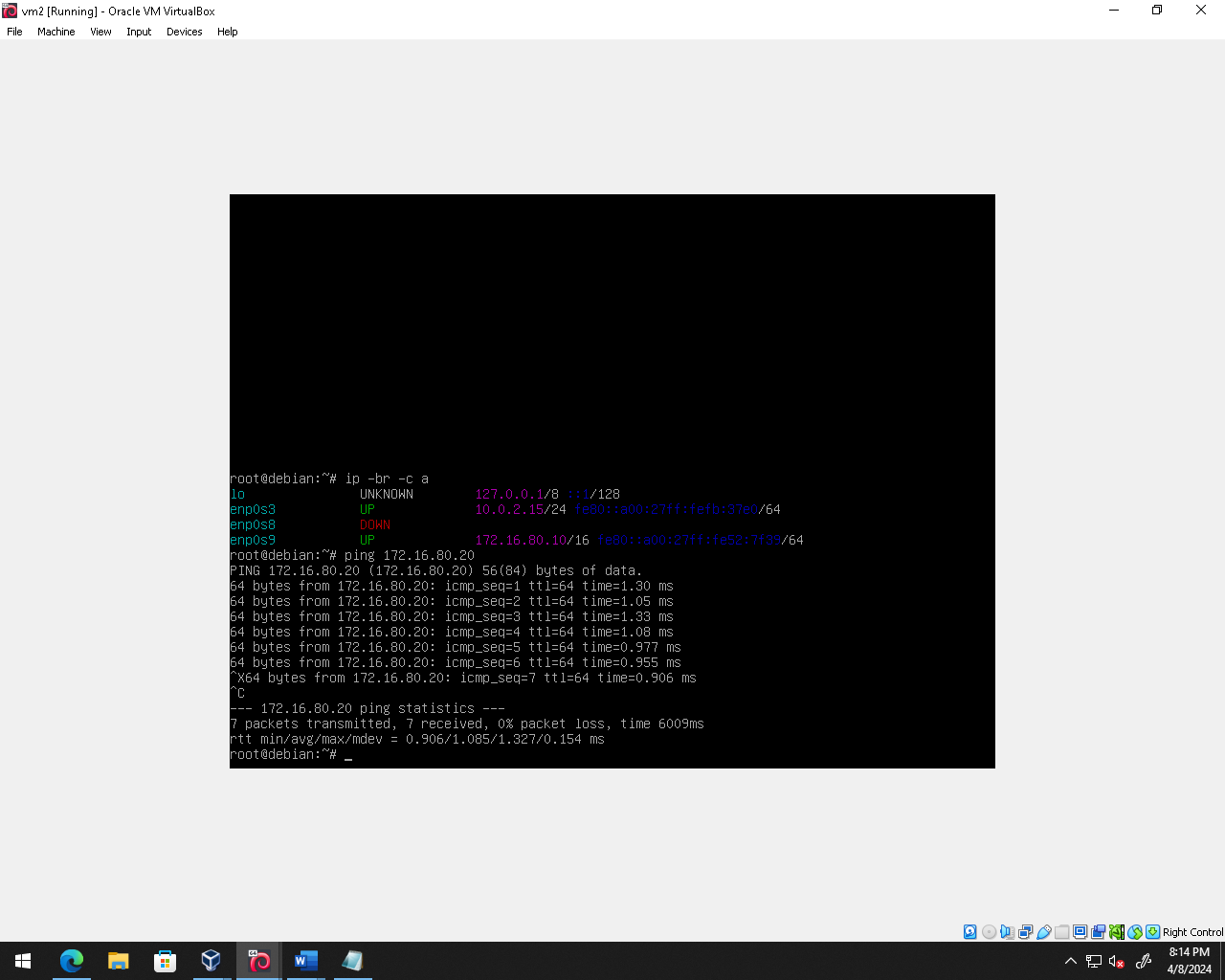
* CLIENTE:



* 1. Na máquina Kali rode o comando ‘ping 172.16.80.10’ e verifique se há resposta do servidor.

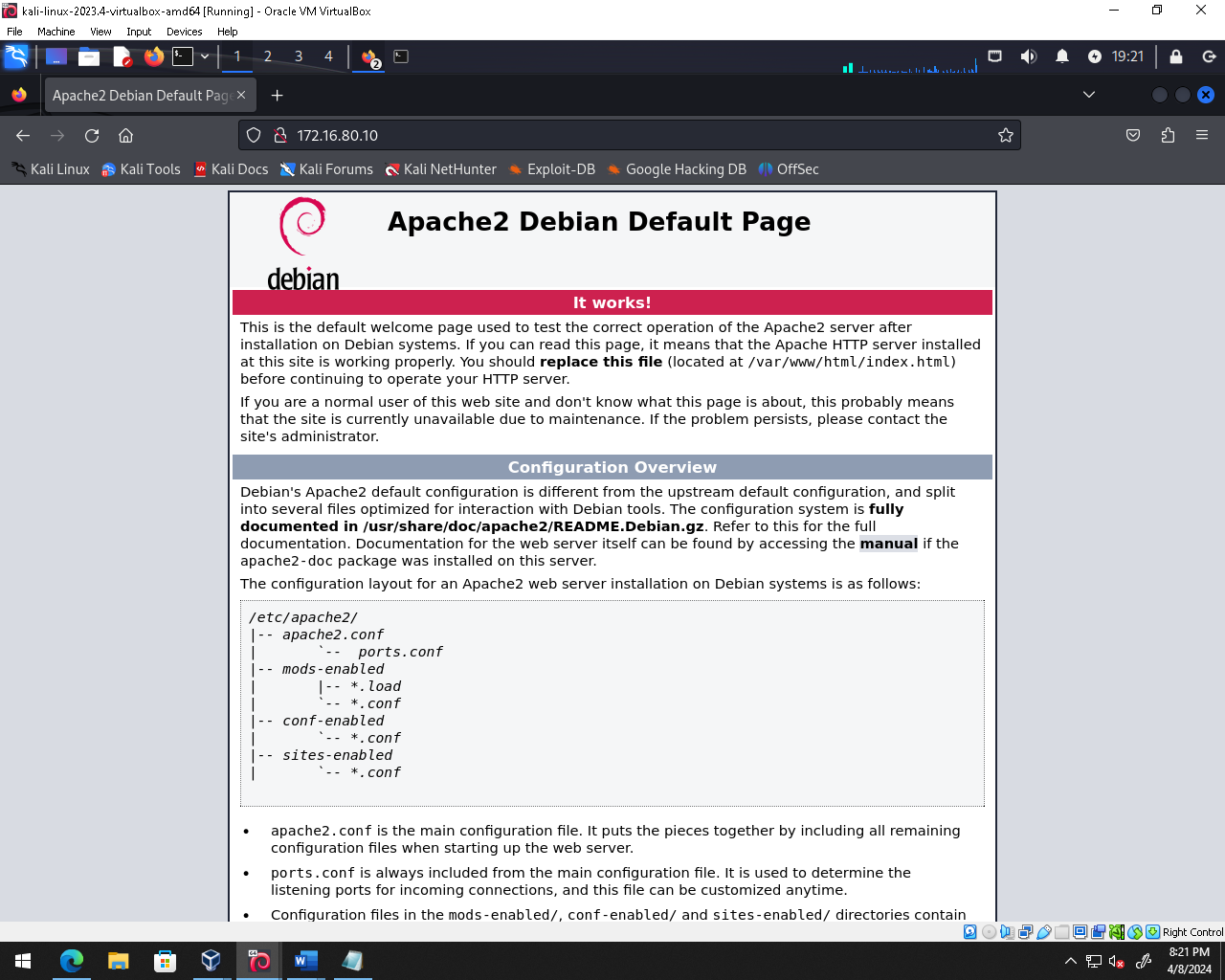


* 1. Na máquina SERVER rode o comando ‘ping 172.16.80.20’ e verifique se há resposta do servidor.



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

1. Simulando vulnerabilidades
2. Na máquina Kali, abra o Mozilla Firefox e acesse a URL: http://172.16.80.10



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

service apache2 stop

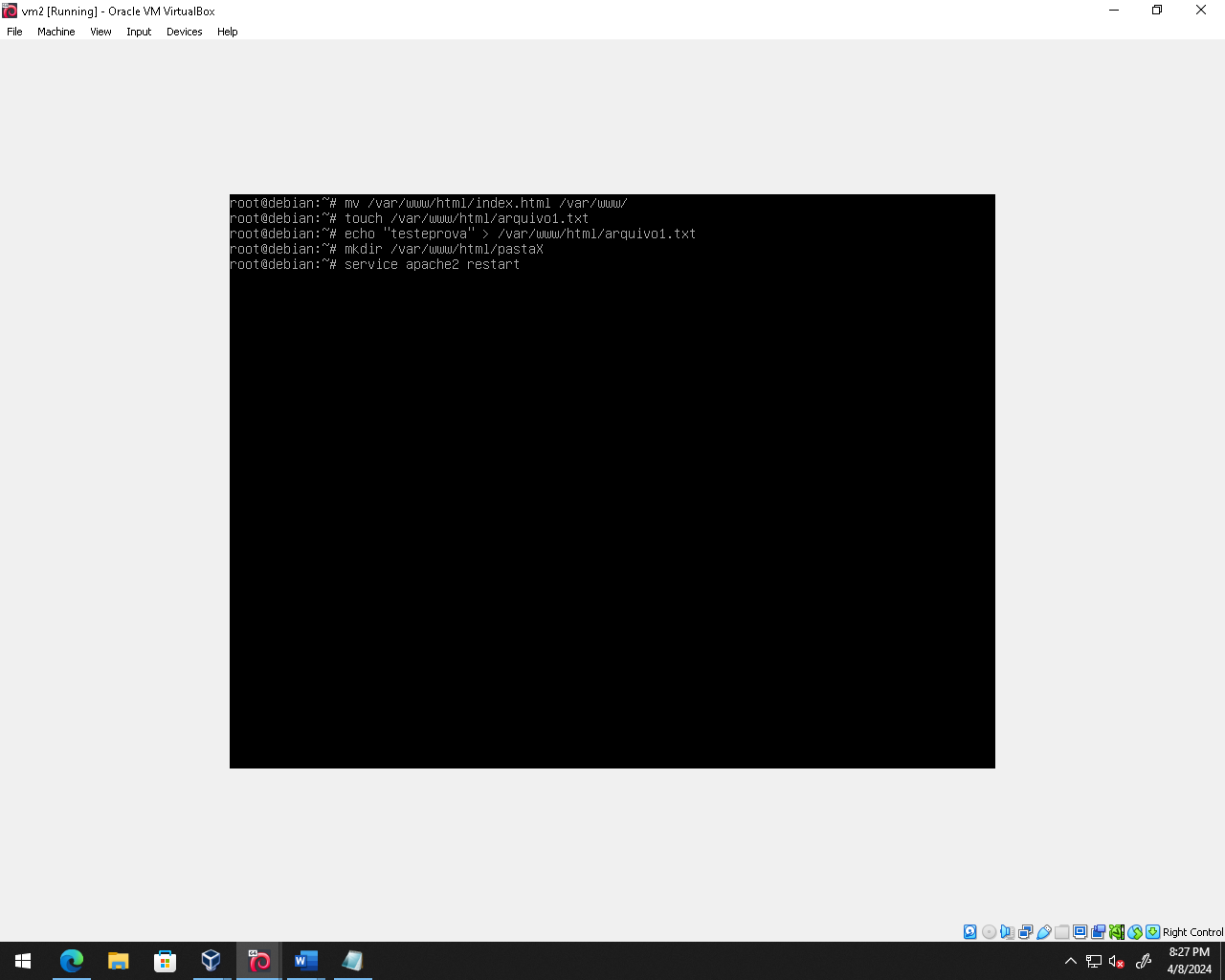
mv /var/www/html/index.html /var/www/

touch /var/www/html/arquivo1.txt

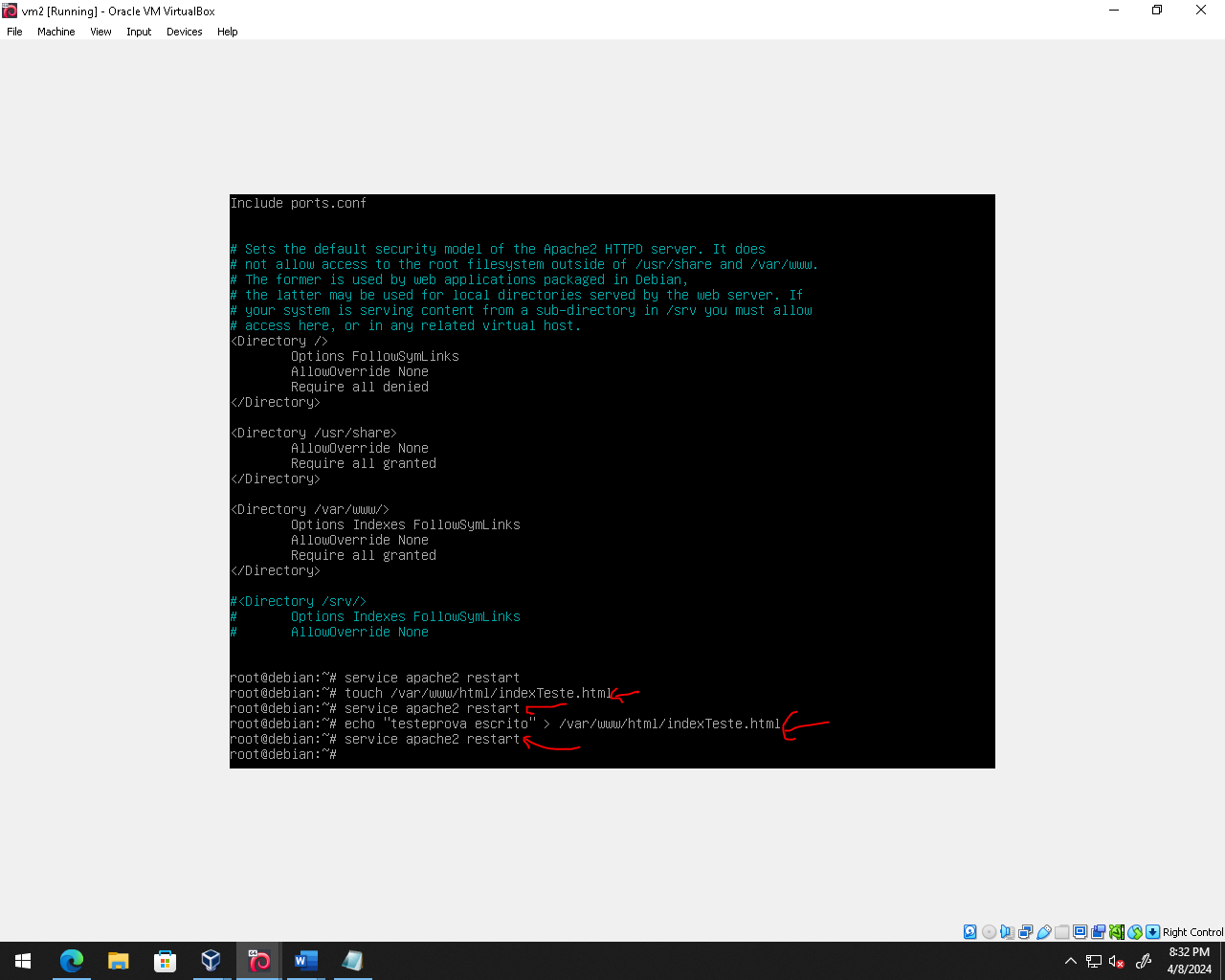
echo “Teste” > /var/www/html/arquivo1.txt

mkdir /var/www/html/pastaX

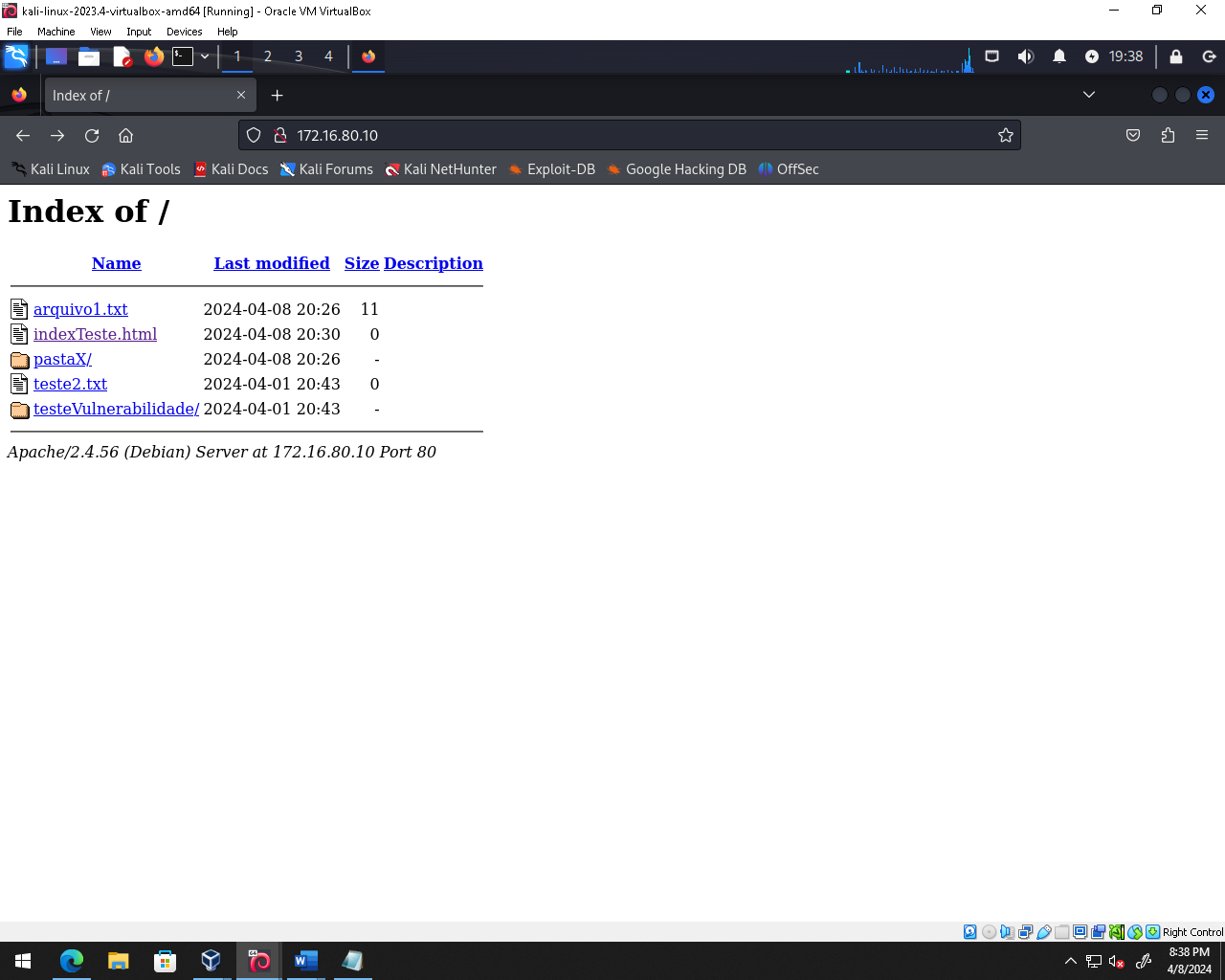
service apache2 restart



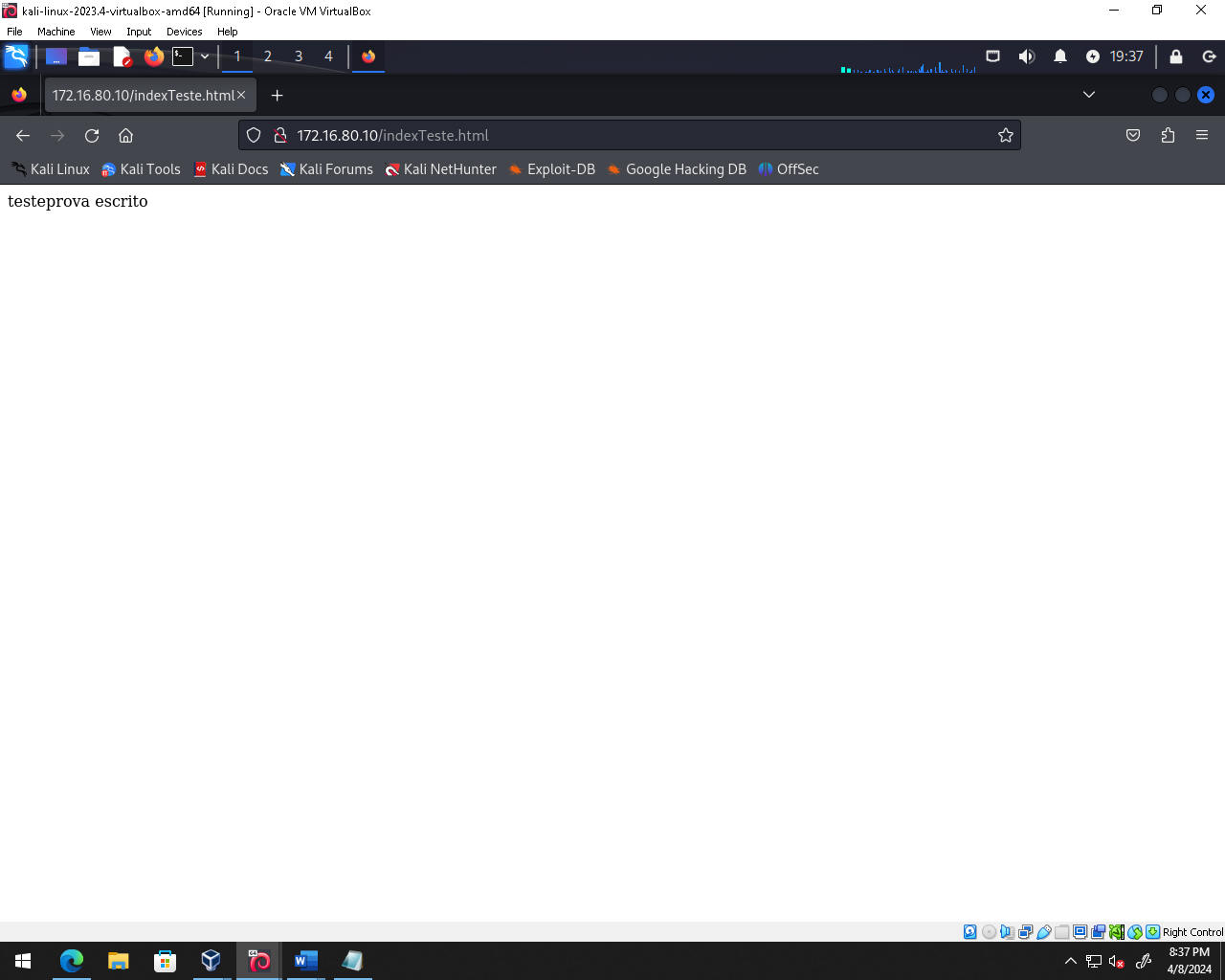
1. Agora no kali, criar um arquivo indexTeste.html para testar ele futuramente:



1. Depois vamos reiniciar o servidor e recarregar a página no KALI:

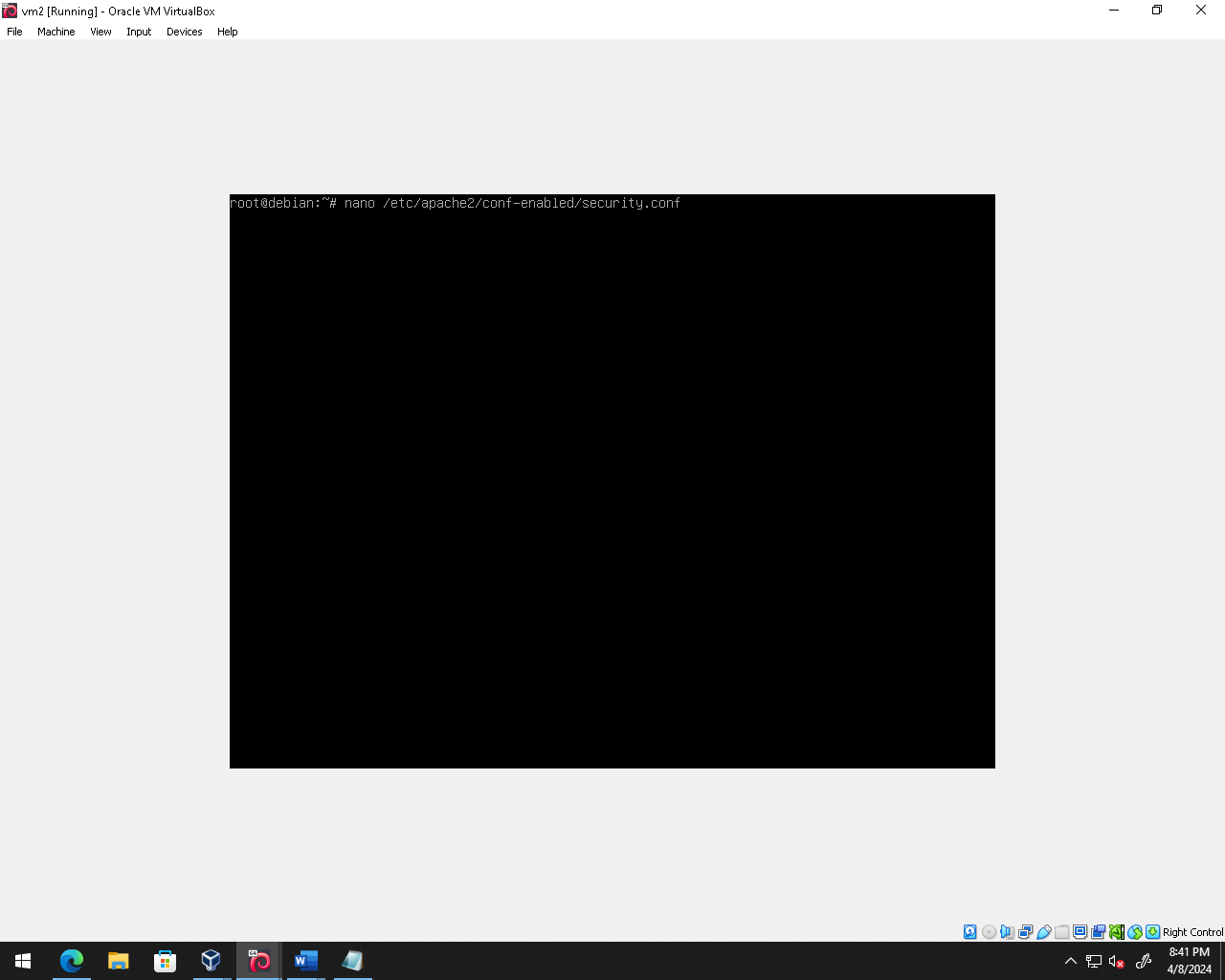


1. Ao clicar no arquivo IndexTeste.html:

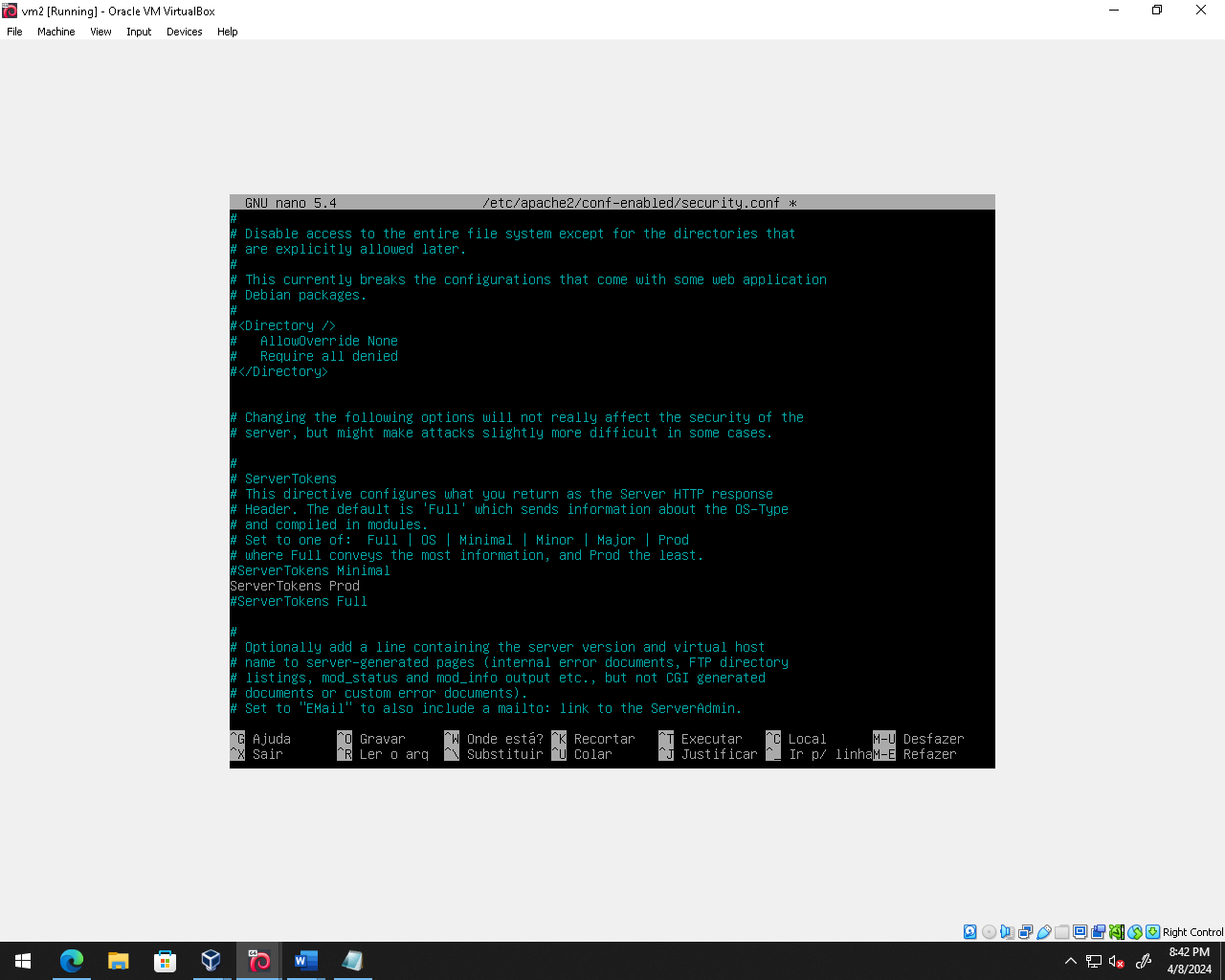


Podemos perceber que estamos mostrando a versão do servidor e o IP, para retirar isso vamos precisar configurar algumas coisas.

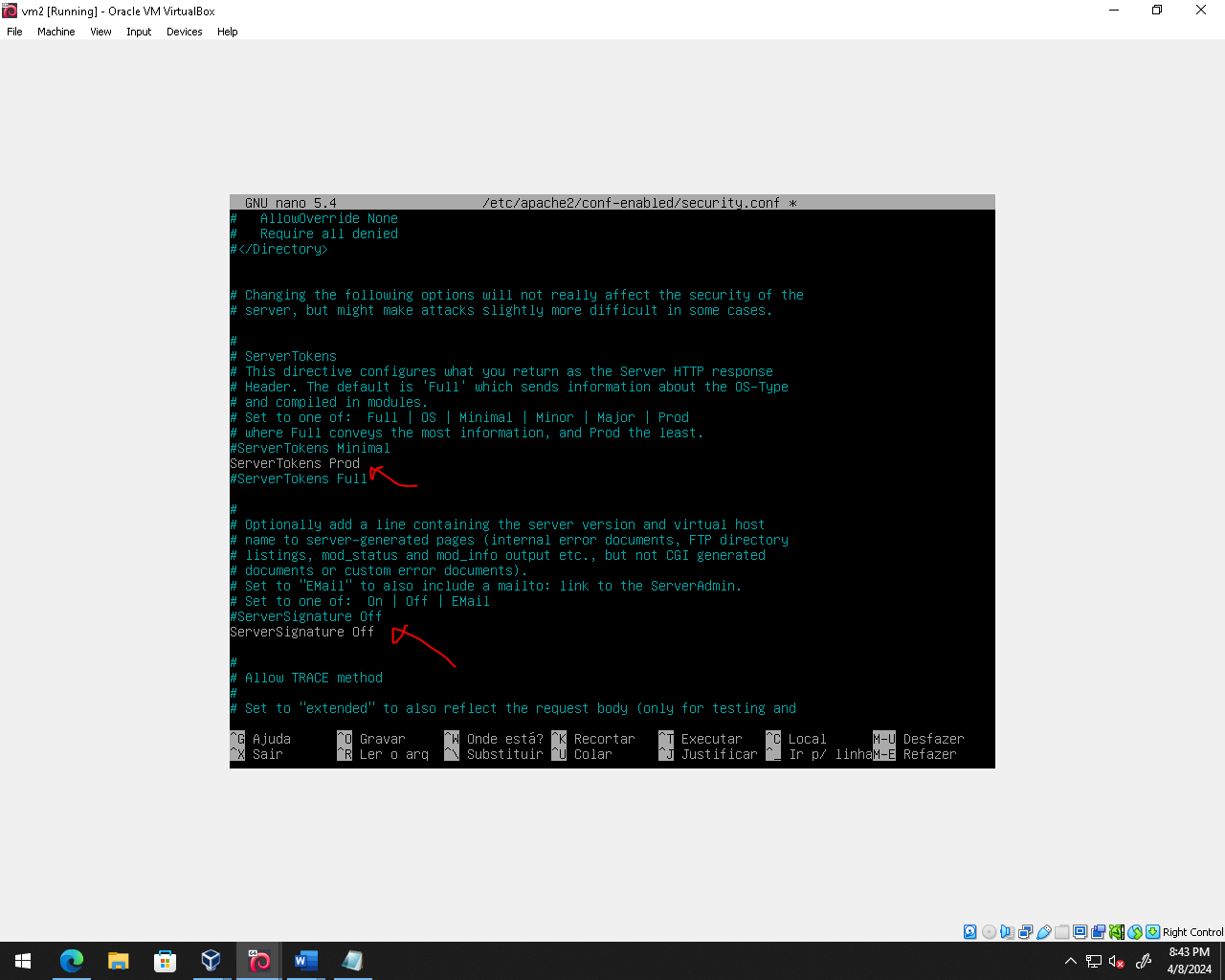
1. Corrigindo a vulnerabilidade:
   1. Para corrigir a vulnerabilidade, precisamos alterar algumas configurações do apache2.
   2. Primeiro vamos configurar o servidor para o modo produção, de forma que esconda o SO e a versão do servidor.
   3. Na máquina Debian rode o comando ‘nano /etc/apache2/conf-enabled/security.conf’



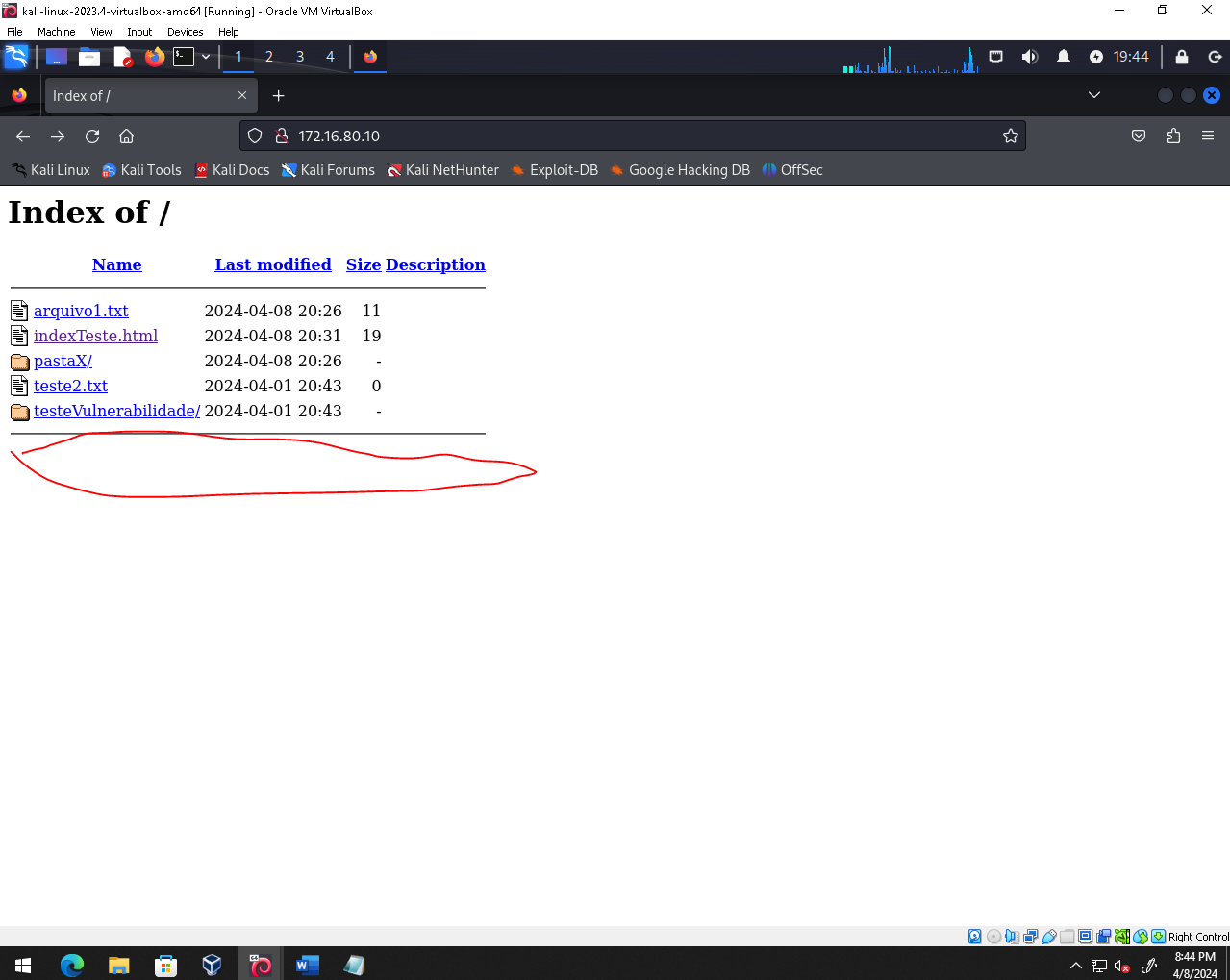
* 1. Nesse arquivo vamos precisar alterar o parâmetro seguinte: no arquivo onde estiver escrito ‘ServerTokens OS’, troque o ‘OS’ para ‘Prod’



* 1. Altere onde estiver escrito ‘ServerSignature On’ para ‘ServerSignature Off’

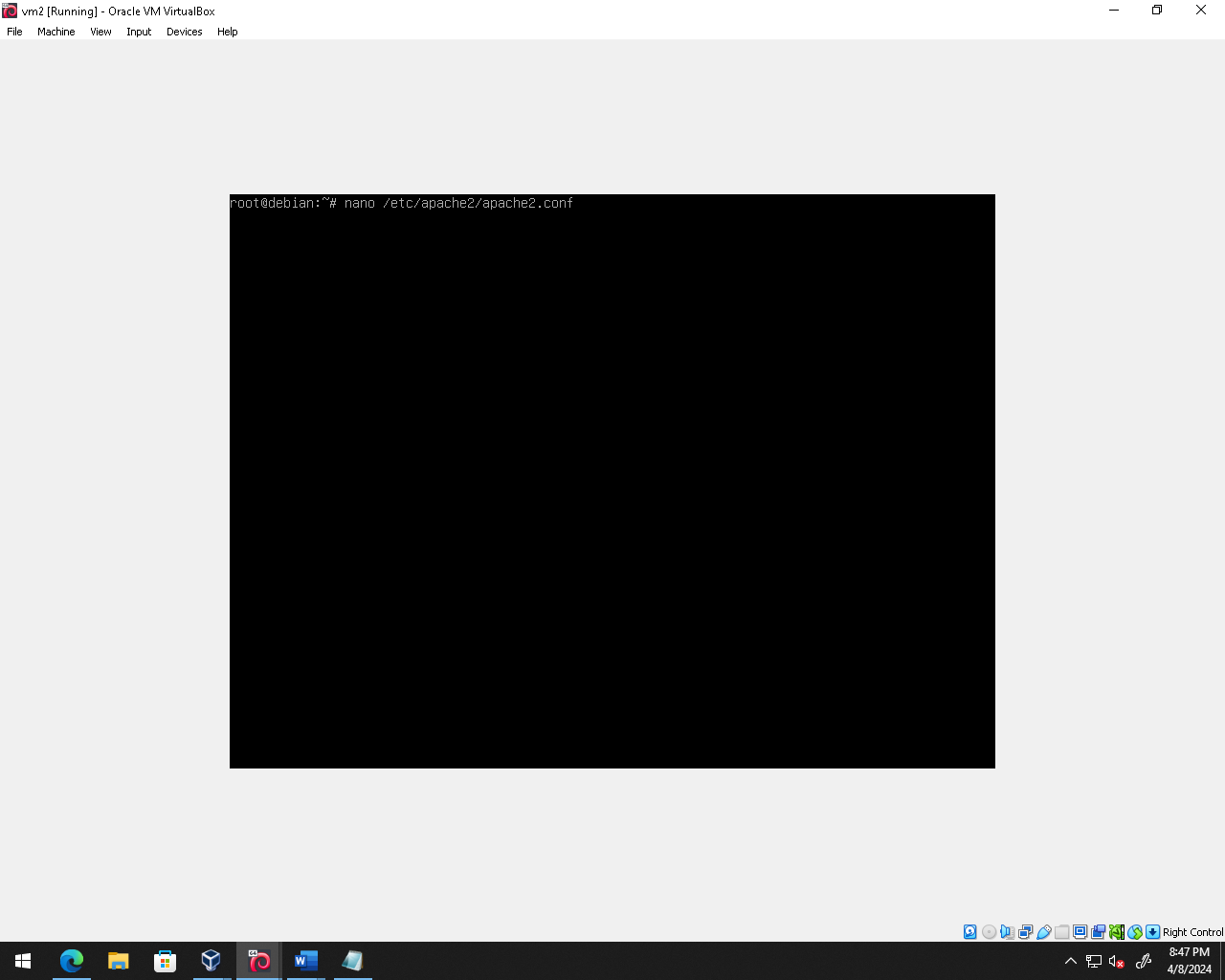


* 1. Aperte ‘Ctrl O’ -> Enter -> ‘Ctrl X’
  2. Reinicie o serviço com o comando ‘service apache2 stop’ -> ‘service apache2 start’
  3. Na máquina Kali recarregue a guia do Mozilla

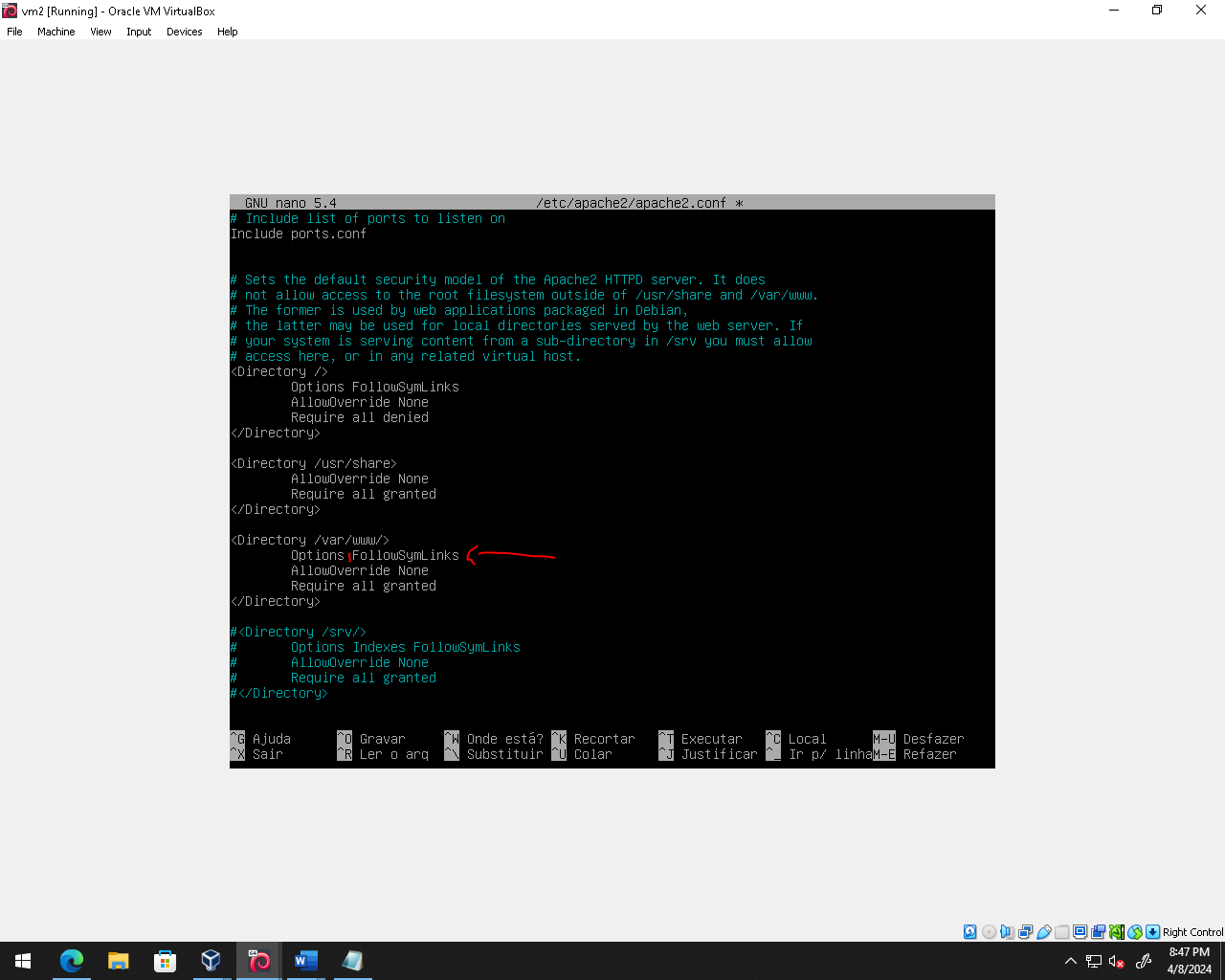


Perceba que o banner exibindo informações do servidor e do sistema operacional sumiram.

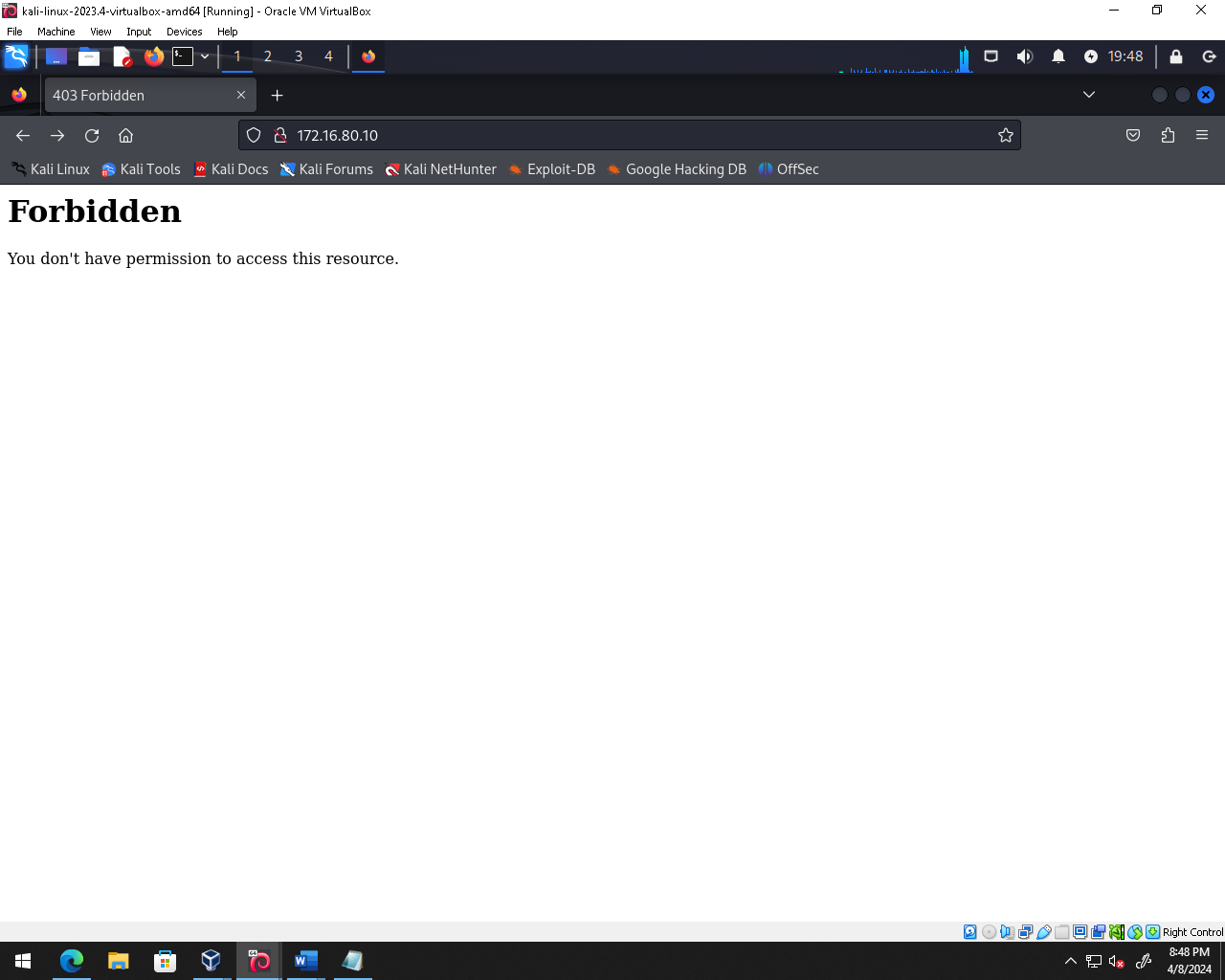
* 1. Agora para impedir o acesso à tela com as pastas e arquivos do servidor, precisamos realizar uma outra configuração.
  2. Rode o comando no Debian ‘nano /etc/apache2/apache2.conf’



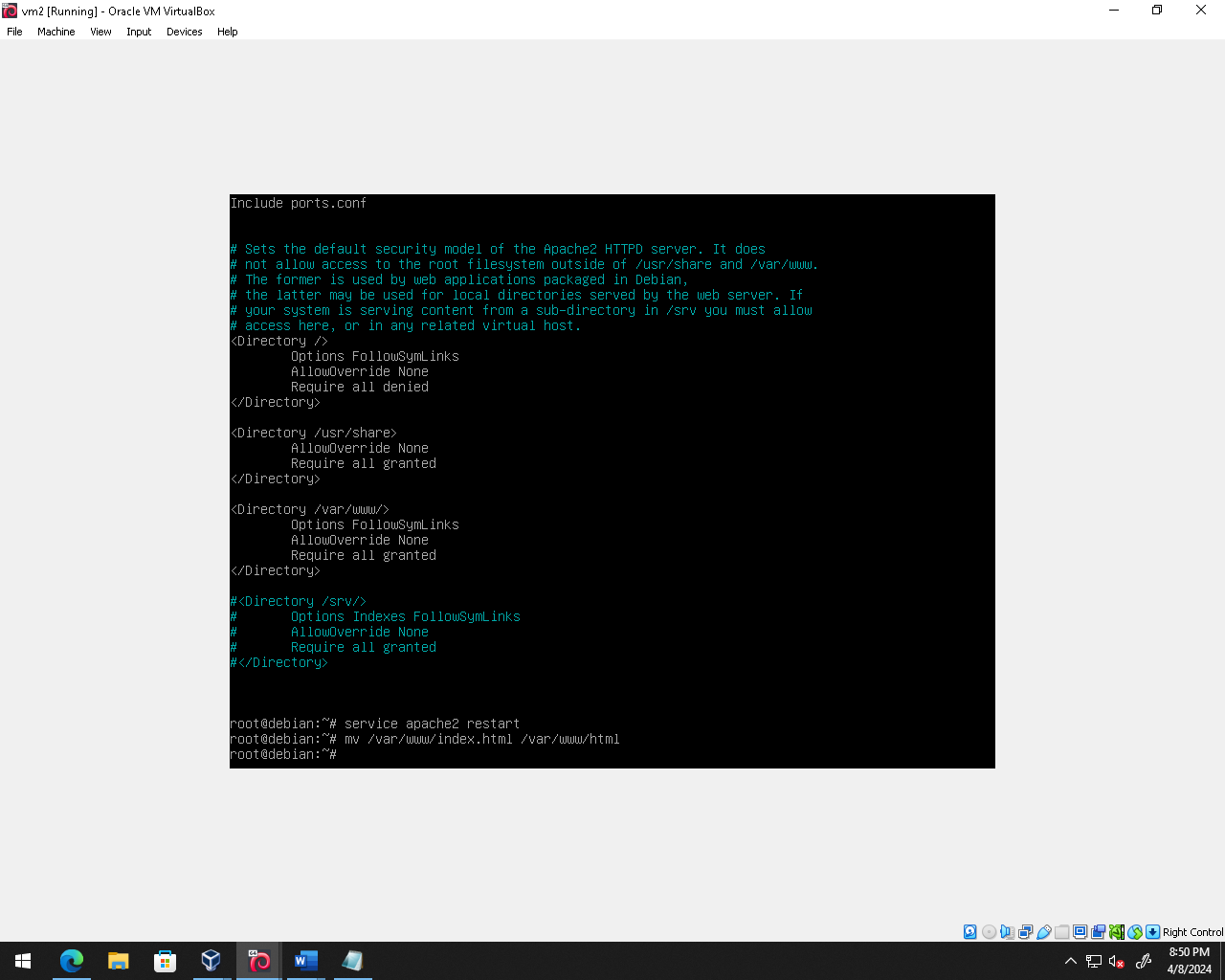
* 1. Procure pelo texto ‘<Directory /var/www/>’, e na linha abaixo, remova a palavra ‘Indexes’



* 1. Reinicie o serviço com o comando ‘service apache2 stop’ -> ‘service apache2 start’
  2. Na máquina Kali, recarregue a guia



* 1. Perceba que agora já não conseguimos mais ver os arquivos do servidor
  2. Agora podemos adicionar um index.html novamente para visualizar a tela inicial do servidor.
  3. Para isso rode o comando ‘mv /var/www/index.html /var/www/html/’,



* 1. Reinicie o servidor com os comandos ‘service apache2 stop’ e ‘service apache2 start’
  2. Na máquina Kali recarregue a guia e perceba que a tela exibe o que aparecia antes:

