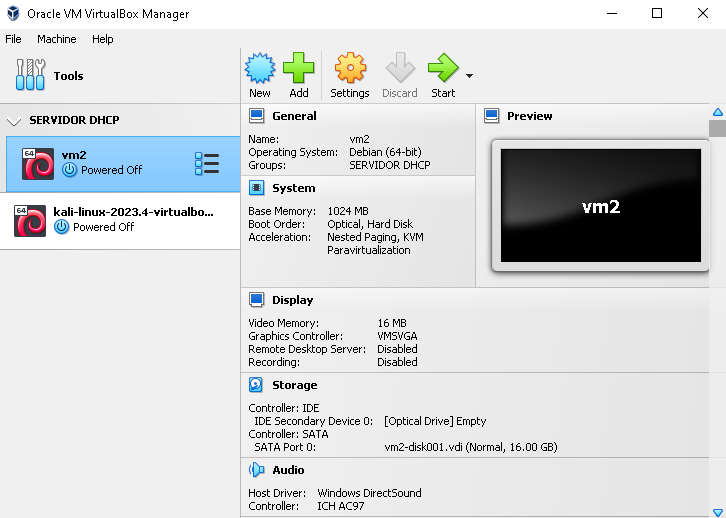
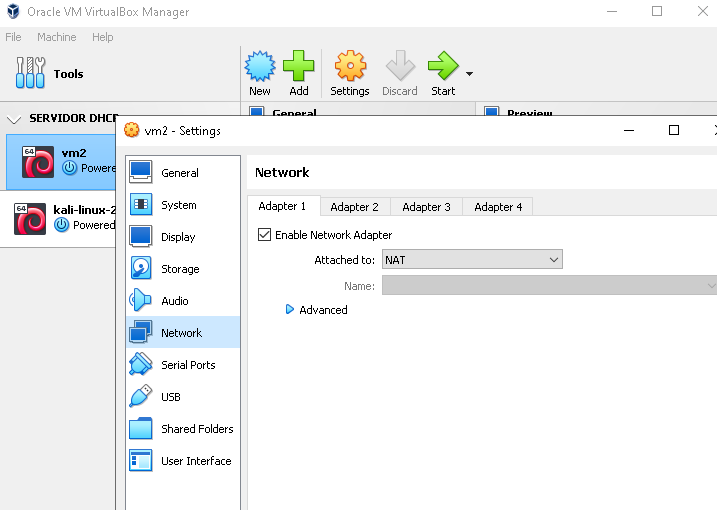
**How to**

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

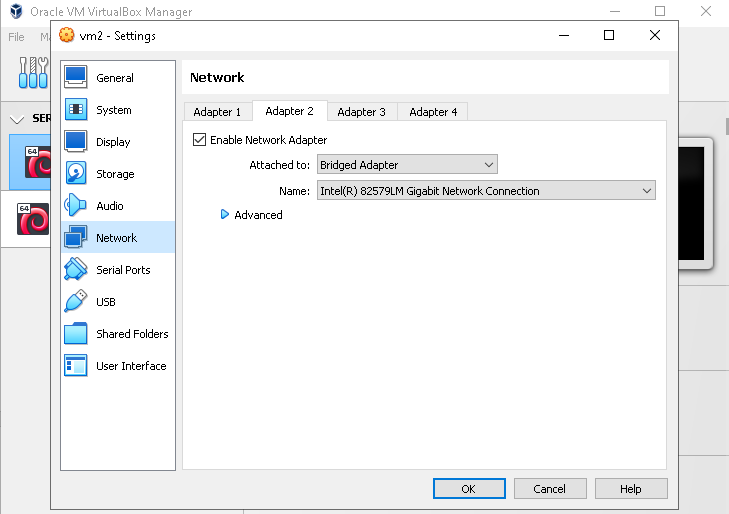
1. **Configurar uma comunicação entre Server x Cliente**
   1. Configure as duas VMs para funcionar



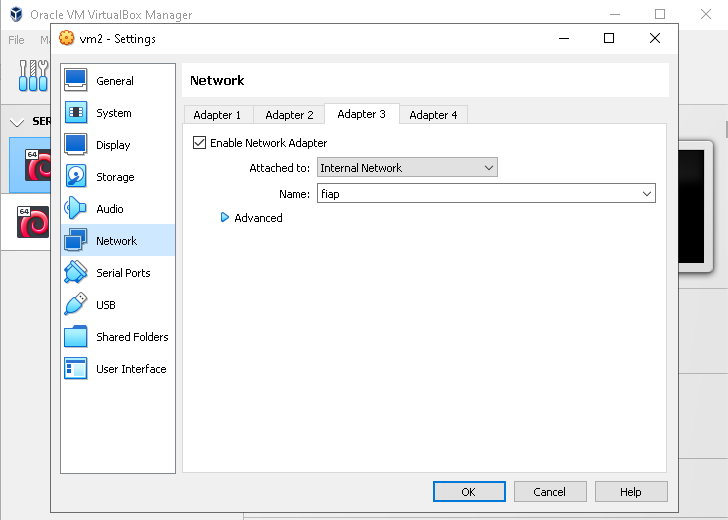
* 1. Clique em Settings e vá para a aba de Network



* 1. Configurar o Adapter 2



* 1. Configurar o Adapter 3



* 1. Repetir a configuração para a outra máquina virtual
  2. Iniciar as duas máquinas, logando com o usuário root
     1. VM Debian - User root – Senha fiap
     2. VM Kali – User kali – Senha kali
  3. Na máquina Kali, rode o comando ‘sudo su’, digitando a senha ‘kali’ quando necessário.
  4. Rodar o seguinte comando em cada uma das máquinas: ‘nano /etc/network/interfaces’
  5. Na máquina Kali, vá até o final do arquivo e digite o seguinte:

# Placa de rede interna – 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. Na máquina Debian, vá até o final do arquivo e digite o seguinte:

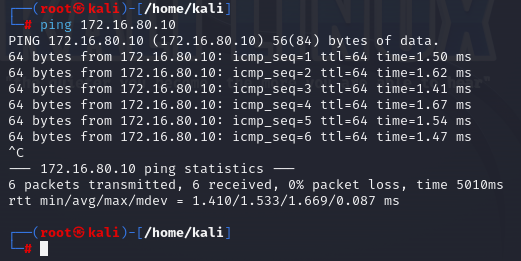
# Placa de rede interna – fiap

allow-hotplug enp0s9

iface enp0s9 inet static

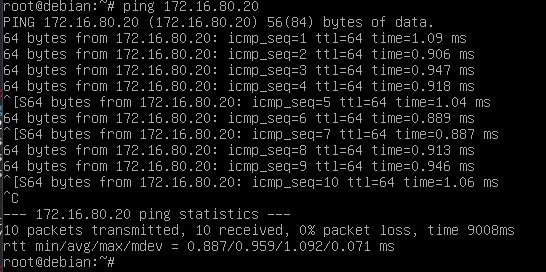
address 172.16.80.10

* 1. Digite o comando ‘init 6’ em ambas máquinas para reiniciar
  2. 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.
  3. Na máquina Kali rode o comando ‘ping 172.16.80.10’ e verifique se há resposta do servidor.



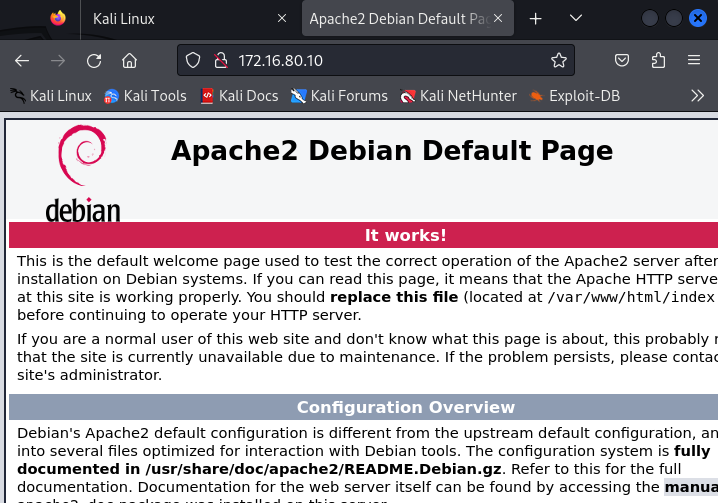
(Aperte ‘Ctrl c’ para sair do comando)

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



(Aperte ‘Ctrl c’ para sair do comando)

* 1. Isso nos mostra que as duas máquinas conseguem se comunicar

1. **Simular vulnerabilidade de acesso ao Apache**
   1. Primeiro precisamos 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)
   3. Instale o pacote ‘net-tools’ para facilitar o uso do serviço apache2. Para isso rode o comando ‘apt install net-tools’
   4. Para iniciar o serviço apache2 rode o comando ‘service apache2 start’
   5. 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.  
      
   6. Na máquina Kali, abra o Mozilla Firefox e acesse a URL: <http://172.16.80.10:80>  
      
   7. Agora para visualizar a vulnerabilidade, volte na máquina Debian e rode os seguintes comandos:

service apache2 stop

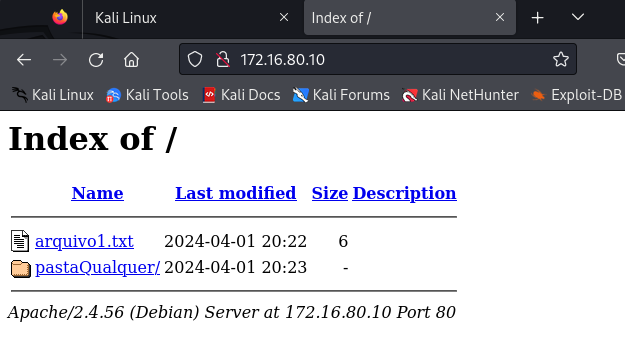
mv /var/www/html/index.html /var/www/

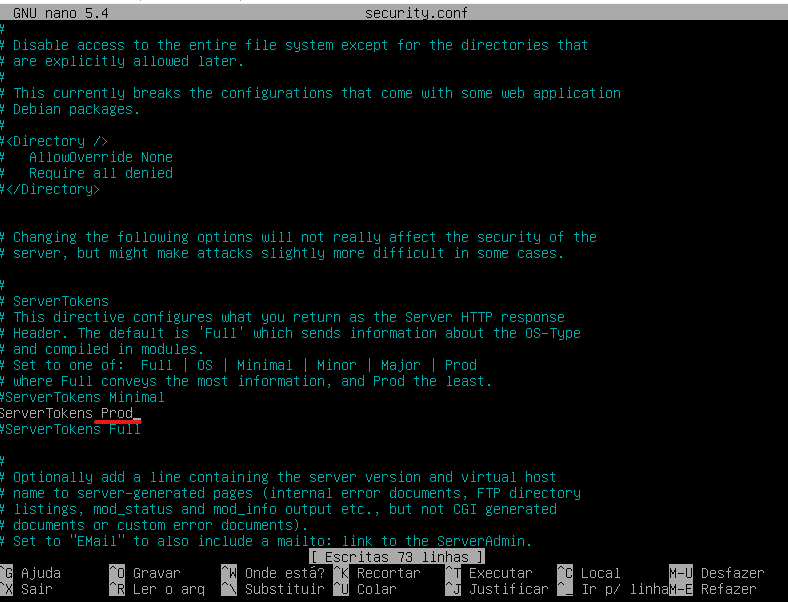
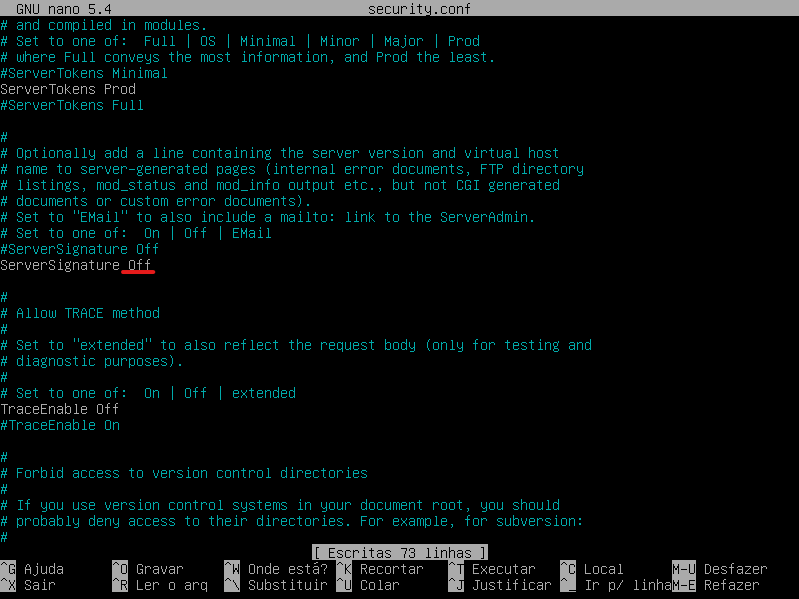
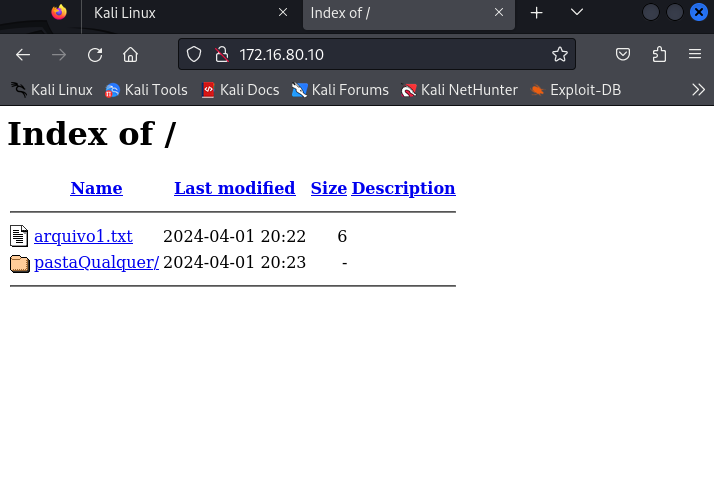
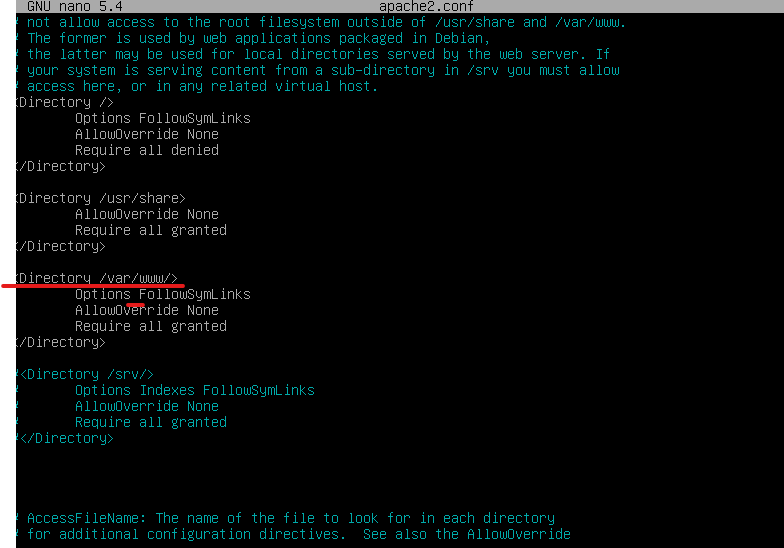
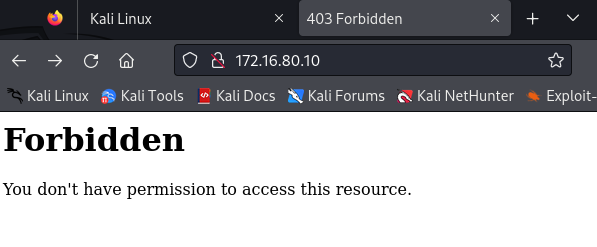
touch /var/www/html/arquivo1.txt

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

mkdir /var/www/html/pastaQualquer

service apache2 start

* 1. Perceba que a tela exibe informações sensíveis, como os arquivos dentro do servidor, o sistema operacional, o servidor e sua versão etc.  
     
  2. Isso se trata da vulnerabilidade em questão, pois abre portas para pessoas maliciosas explorarem falhas na versão do Servidor, no SO e entre outras falhas de segurança.

1. **Corrigir 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’
   4. Onde estiver escrito ‘ServerTokens OS’, troque o ‘OS’ para ‘Prod’  
      
   5. Aperte ‘Ctrl O’ -> Enter -> ‘Ctrl X’
   6. Digite o comando novamente (nano /etc/apache2/conf-enabled/security.conf)
   7. Altere onde estiver escrito ‘ServerSignature On’ para ‘ServerSignature Off’  
      
   8. Reinicie o serviço com o comando ‘service apache2 stop’ -> ‘service apache2 start’
   9. Na máquina Kali recarregue a guia do Mozilla  
      
   10. Perceba que o banner exibindo informações do servidor e do sistema operacional sumiram.
   11. Agora para impedir o acesso à tela com as pastas e arquivos do servidor, precisamos realizar uma outra configuração.
   12. Rode o comando ‘nano /etc/apache2/apache2.conf’
   13. Procure pelo texto ‘<Directory /var/www/>’, e na linha abaixo, remova a palavra ‘Indexes’  
       
   14. Na máquina Kali, recarregue a guia  
       
   15. Perceba que agora já não conseguimos mais ver os arquivos do servidor
   16. Agora podemos adicionar um index.html novamente para visualizar a tela inicial do servidor.
   17. Para isso rode o comando ‘mv /var/www/index.html /var/www/html/’
   18. Reinicie o servidor com os comandos ‘service apache2 stop’ e ‘service apache2 start’
   19. Na máquina Kali recarregue a guia e perceba que a tela exibe o que aparecia antes:  
       