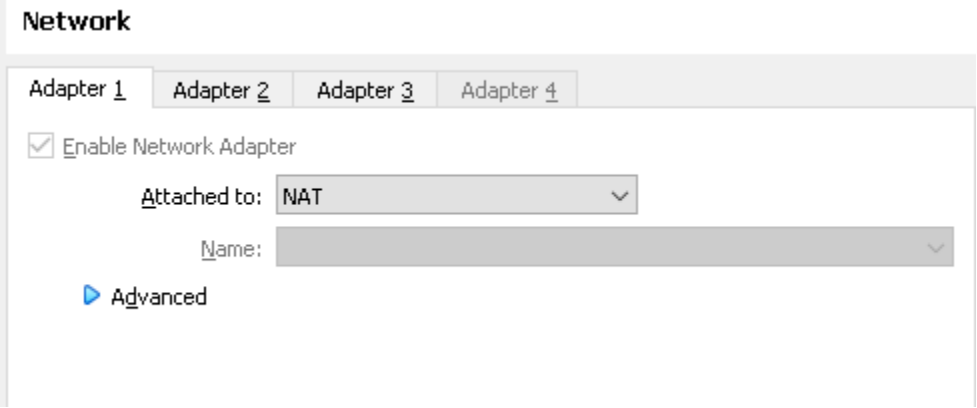
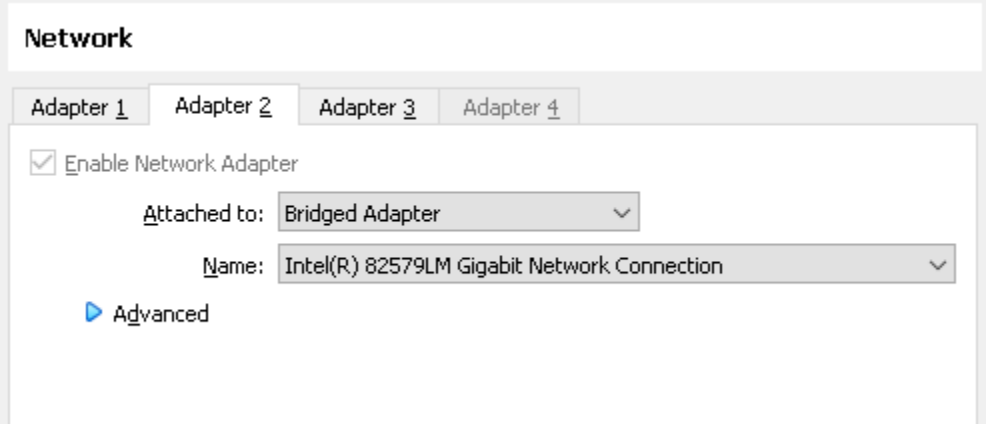
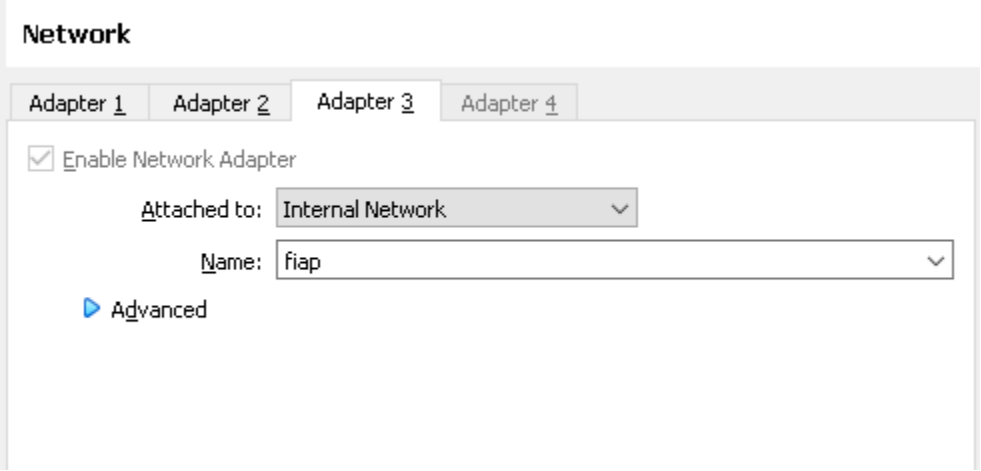
Relatório atividade Cybersecurity for DEV

Configurando as portas de cada máquina virtual:







Configurando o lado servidor:

Acessando a pasta network onde o arquivo de configuração das interfaces está localizado

```
root@debian:~# cd /etc/network
root@debian:/etc/network# cp interfaces interfaces.old
root@debian:/etc/network# nano 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

allow-hotplug enp0s8
iface enp0s8 inet static
address 172.16.80.10
```

Reiniciando o serviço de rede e a máquina para aplicar as configurações

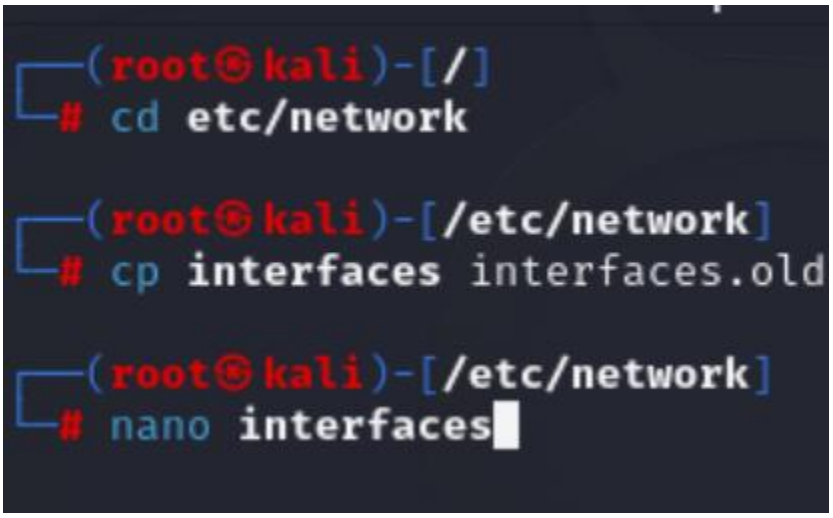
```
root@debian:/etc/network# service networking restart
root@debian:/etc/network# init 6
```

Configurando o cliente

- Entrando no modo root

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
\
┌──(root㉿kali)-[/home/kali]
└─#
```

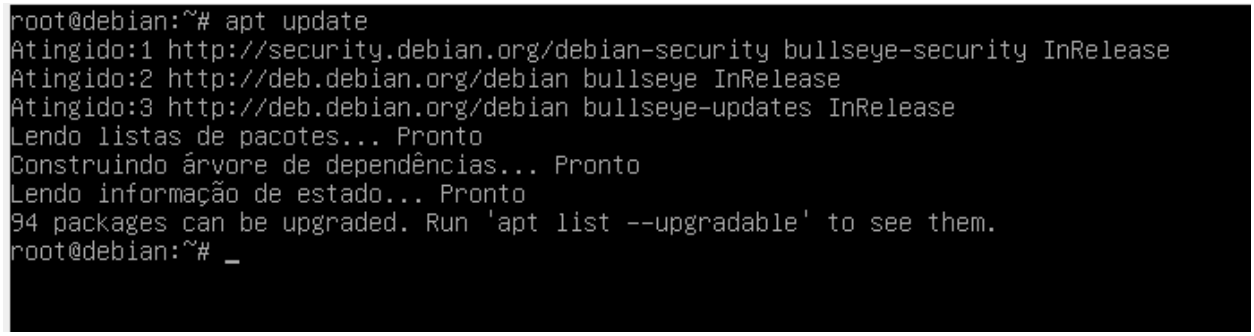
Acessando a pasta network onde o arquivo de configuração das interfaces está localizado



Reiniciando o serviço de rede e a máquina para aplicar as configurações

Instalando o servidor

- Atualizando a VM



Instalar o Apache

```
root@debian:~# apt install apache2
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libcurl4 liblua5.3-0 ssl-cert
Pacotes sugeridos:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
```

Instalar net-tools

```
root@debian:~# apt install net-tools
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
Os NOVOS pacotes a seguir serão instalados:
  net-tools
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
É preciso baixar 250 kB de arquivos.
Depois desta operação, 1.015 kB adicionais de espaço em disco serão usados.
0% [Conectando a debian.map.fastlydns.net]
```

Iniciando o servidor e verificando se esta no ar

```
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       8704/sshd: /usr/sbi
tcp6       0      0 :::80                   :::*                    OUÇA       16196/apache2
tcp6       0      0 :::22                   :::*                    OUÇA       8704/sshd: /usr/sbi
root@debian:~# _
```

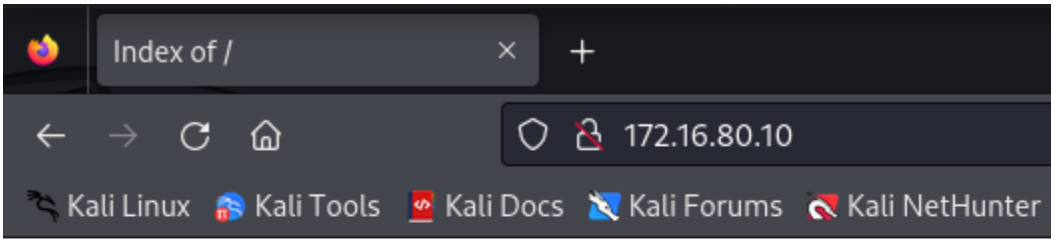
Acessando a pasta www:

- cd /var/www

  movendo o index.html (mostrando erro e vunerabilidade ao mover o arquivo padrão do projeto)

  - Todo projeto deve ter um arquivo de segurança!
  - mv index.html ..

```
root@debian:/# cd /var/www/html
root@debian:/var/www/html# mv index.html ..
root@debian:/var/www/html#
```



Index of /

Name Last modified Size Description

Apache/2.4.56 (Debian) Server at 172.16.80.10 Port 80

Corrigindo o erro:

Corrigindo falha de segurança

- cd /etc/apache2
- nano apache2.conf
- achar a opção diretório <Directory /var/www>
- apagar Indexes

```
root@debian:~# cd /etc/apache2
root@debian:/etc/apache2# nano apache2.conf _
```

```
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

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

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

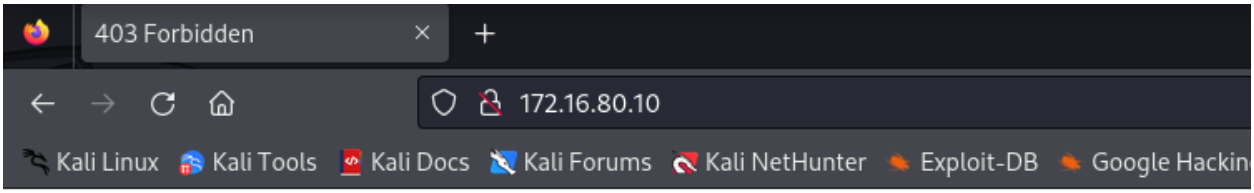
Acessando arquivo de configuração de segurança

- cd /etc/apache2/conf-enabled
- nano security.conf
    - limitando o acesso a informações sobre o SO:
        - ServerTokens Prod
    - limitando o acesso a informações sobre o ip e a porta:
        - ServerSignature Off

```
root@debian:/etc/apache2# cd conf-enabled/
root@debian:/etc/apache2/conf-enabled# nano security.conf
```

```
#
# 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 OS
#ServerTokens Full
ServerTokens Prod

#
# 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 On
```



Forbidden

You don't have permission to access this resource.