

Checkpoint 04 – Segundo Semestre – FIAP

Professor Jaci - Cybersecurity FOR DEV

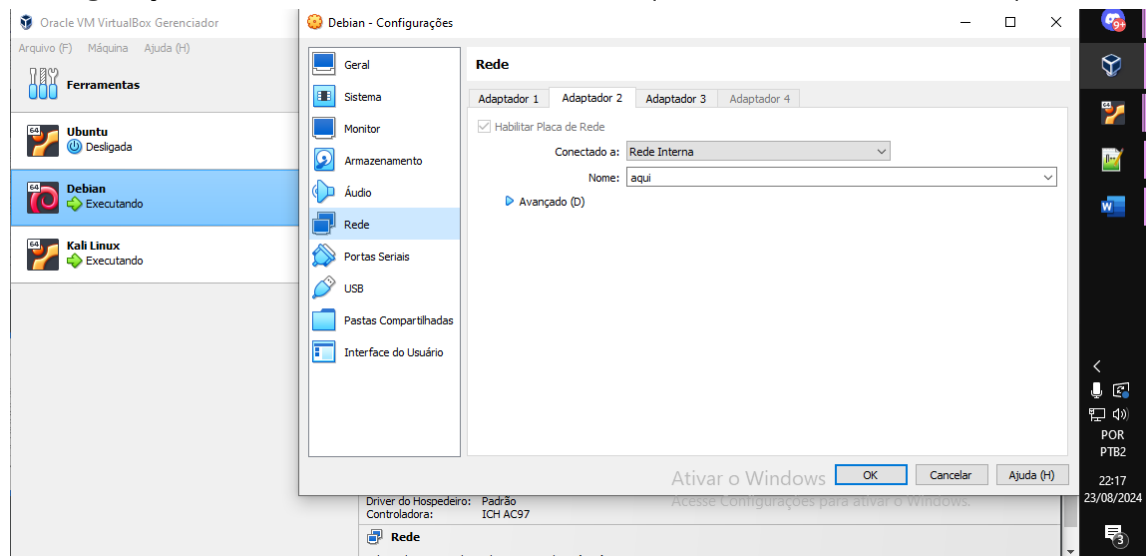
Alunos:

- **Gabriel Kazuki Onishi. RM 87182.**
- **Breno de Souza Silva. RM 88332.**

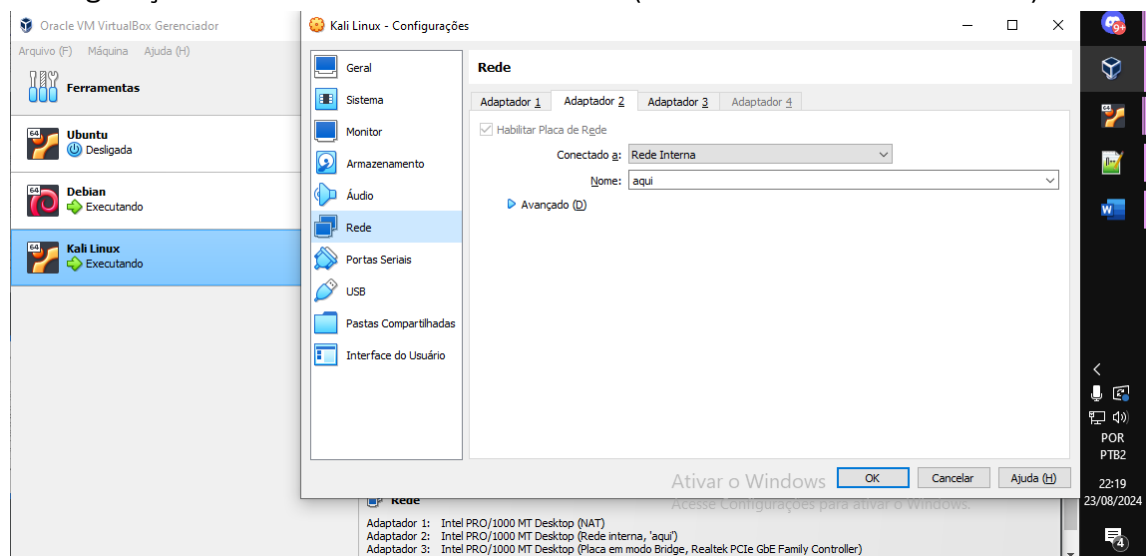
Prints solicitados:

Item 1: Configuração das placas de redes do cliente e servidor

- Configuração da interface de rede do Servidor (Debian no meu VirtualBox):



- Configuração da interface de rede do Cliente (Kali Linux no meu VirtualBox):



- Arquivo /etc/network/interfaces do Servidor:

```

gabriel@gabriel-d-pc: ~
Arquivo Editar Exibir Pesquisar Terminal Ajuda
GNU nano 7.2 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

# placa de rede - interna
allow-hotplug enp0s8
iface enp0s8 inet static
    address 192.168.10.10

allow-hotplug enp0s9
iface enp0s9 inet dhcp

```

[17 linhas lidas]

^G Ajuda ^O Gravar ^W Onde está? ^K Recortar ^T Executar ^C Local ^M-U Desfazer
^X Sair ^R Ler o arq ^N Substituir ^U Colar ^J Justificar ^V Ir p/ linha ^M-E Refazer

- Arquivo /etc/network/interfaces do Cliente:

```

root@kali: /etc/network
File Actions Edit View Help
GNU nano 7.2 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

# placa de rede - interna
allow-hotplug eth1
iface eth1 inet static
    address 192.168.10.20

allow-hotplug eth2
iface eth2 inet dhcp

```

[Read 16 Lines]

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location ^M-U Undo
^X Exit ^R Read File ^N Replace ^U Paste ^J Justify ^V Go To Line ^M-E Redo

- Mostrando os IPs do Servidor:

```

gabriel@gabriel-d-pc: ~
Arquivo Editar Exibir Pesquisar Terminal Ajuda
root@gabriel-d-pc:/etc/network# ip -br -c a
lo                UNKNOWN    127.0.0.1/8 ::1/128
enp0s3            UP          10.0.2.15/24 fe80::a00:27ff:fe3f:8fc0/64
enp0s8            UP          192.168.10.10/24 fe80::a00:27ff:fed4:9a67/64
enp0s9            UP          192.168.15.25/24 2804:431:8252:d901:a00:27ff:fe77:7157/64 fe80::a00:27ff:fe77:7157/64
root@gabriel-d-pc:/etc/network#

```

- Mostrando os IPs do Cliente:

```

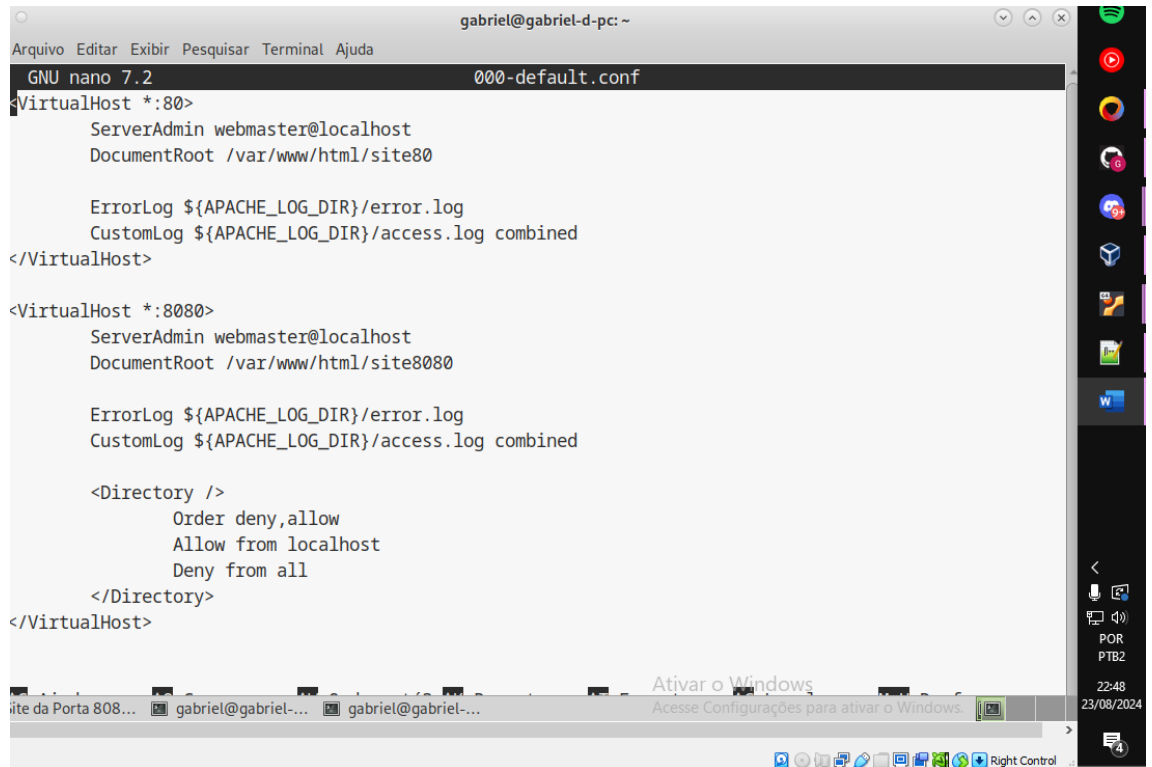
root@kali: /etc/network
File Actions Edit View Help
root@kali)-[/etc/network]
# ip -br -c a
lo                UNKNOWN    127.0.0.1/8 ::1/128
eth0              UP          10.0.2.15/24 fe80::a00:27ff:fe09:fa69/64
eth1              UP          192.168.10.20/24 fe80::a00:27ff:fec4:e5d8/64
eth2              UP          192.168.15.26/24 2804:431:8252:d901:a00:27ff:feaf:b75b/64 fe80::a00:27ff:feaf:b75b/64
root@kali)-[/etc/network]
#

```

Item 2 e 3: Arquivo de configuração do servidor da porta 80 e 8080 (Servidor)

- Comando para ir até a pasta com o arquivo de configuração e abrir o arquivo:
 'cd /etc/apache2/sites-enabled'
 'nano 000-default.conf'

- Mostrando o conteúdo do arquivo 000-default.conf, onde configuramos os hosts virtuais na porta 80 e 8080 do apache2.

A screenshot of a terminal window titled 'gabriel@gabriel-d-pc: ~'. The window shows the nano 7.2 editor editing the file '000-default.conf'. The file contains two VirtualHost configurations. The first is for port *:80, with ServerAdmin webmaster@localhost and DocumentRoot /var/www/html/site80. The second is for port *:8080, with the same ServerAdmin and DocumentRoot /var/www/html/site8080. Inside the *:8080 VirtualHost, there is a <Directory /> block with 'Order deny,allow', 'Allow from localhost', and 'Deny from all'. The terminal window has a menu bar with 'Arquivo', 'Editar', 'Exibir', 'Pesquisar', 'Terminal', and 'Ajuda'. The status bar at the bottom shows 'Ativar o Windows' and 'Acesse Configurações para ativar o Windows.'.

```
GNU nano 7.2 000-default.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/site80

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<VirtualHost *:8080>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/site8080

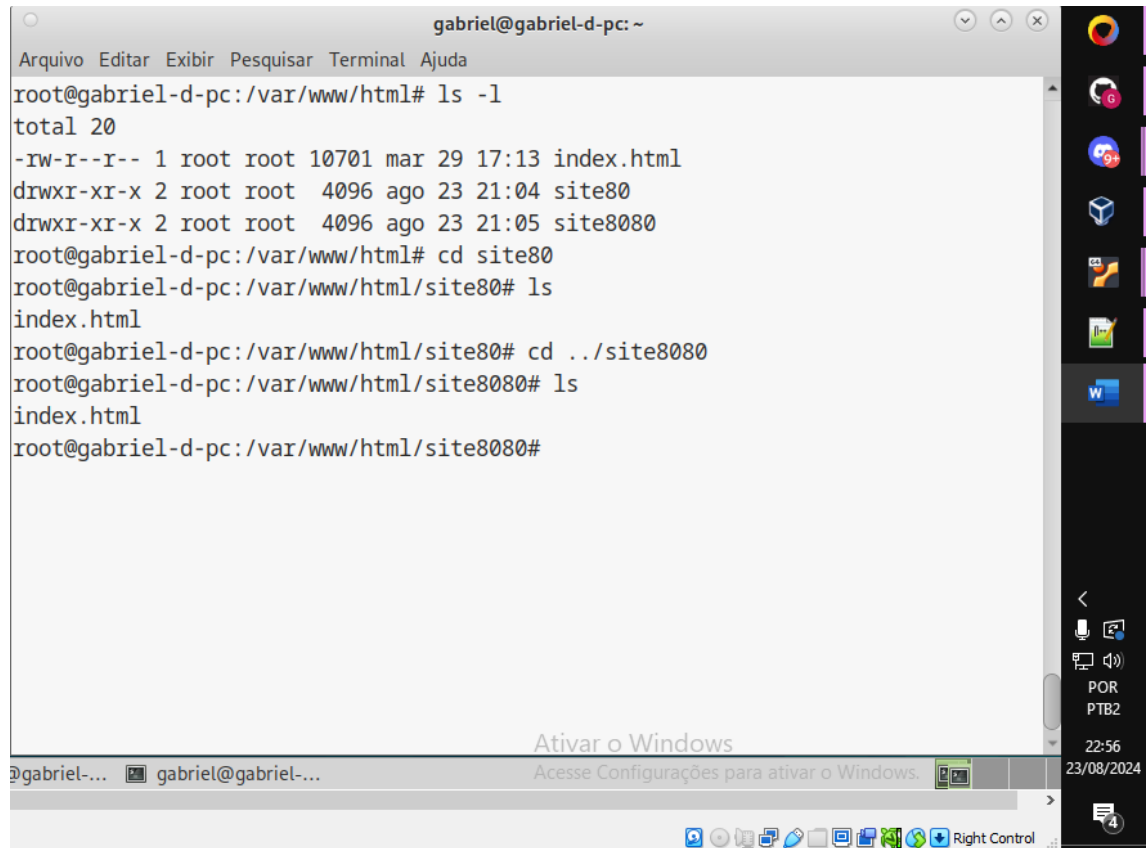
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory />
        Order deny,allow
        Allow from localhost
        Deny from all
    </Directory>
</VirtualHost>
```

Salvando o arquivo usando as teclas [Ctrl + O] e [Ctrl + X]

- A diretiva <VirtualHost> permite configurar o acesso do servidor em uma determinada porta, em que configuramos para a porta 80 e 8080.
- O atributo DocumentRoot permite associar cada host virtual a uma determinada pasta com o index.html, perceba que o host da porta 80 está associado à pasta '/var/www/html/site80', enquanto o da 8080 está na 'var/www/html/site8080'.
- A diretiva <Directory> dentro do host 8080 é onde configuramos o acesso a ele apenas a partir do localhost ('Allow from localhost'), bloqueando todos os demais acessos ('Deny from all').

- Agora basta criar os arquivos index.html para cada um dos hosts virtuais, conforme configurado anteriormente.



The screenshot shows a terminal window titled 'gabriel@gabriel-d-pc: ~'. The user is root. The terminal output is as follows:

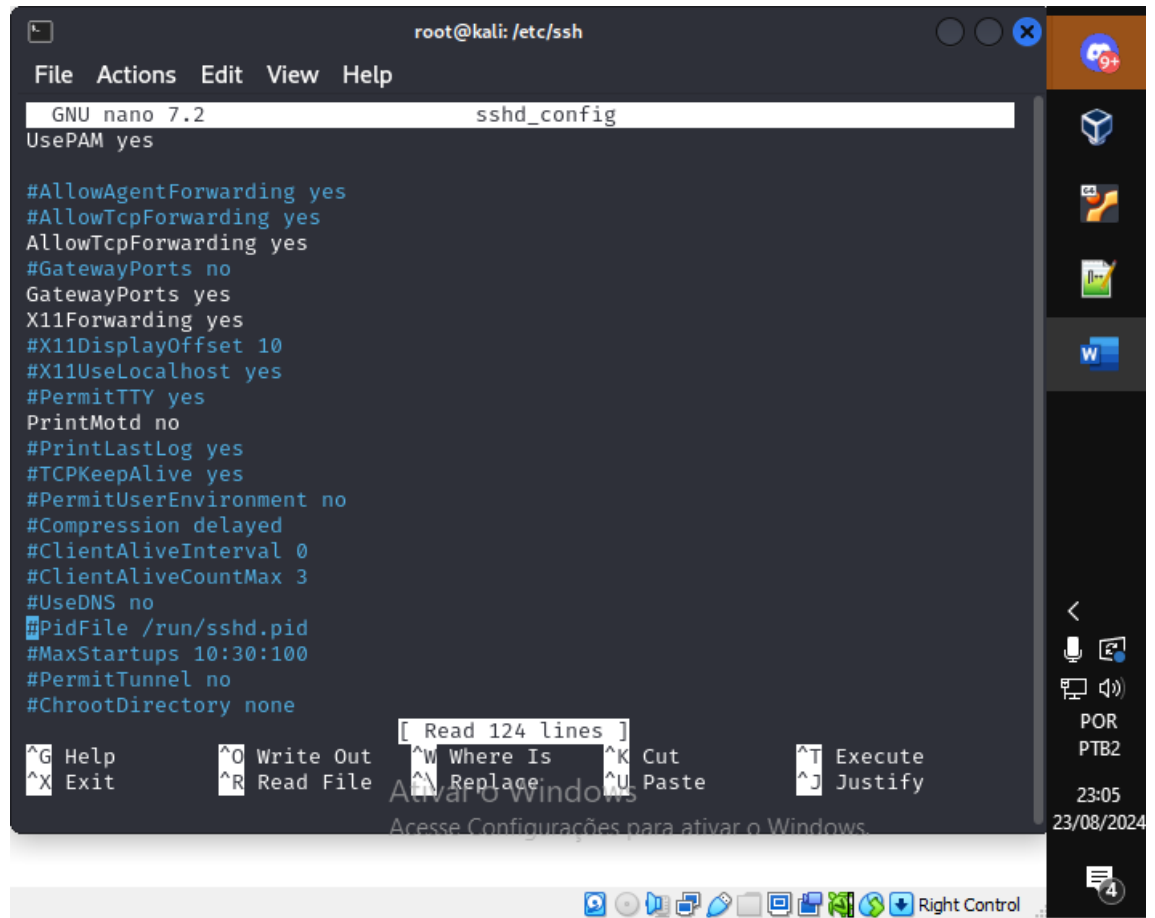
```
Arquivo Editar Exibir Pesquisar Terminal Ajuda
root@gabriel-d-pc:/var/www/html# ls -l
total 20
-rw-r--r-- 1 root root 10701 mar 29 17:13 index.html
drwxr-xr-x 2 root root 4096 ago 23 21:04 site80
drwxr-xr-x 2 root root 4096 ago 23 21:05 site8080
root@gabriel-d-pc:/var/www/html# cd site80
root@gabriel-d-pc:/var/www/html/site80# ls
index.html
root@gabriel-d-pc:/var/www/html/site80# cd ../site8080
root@gabriel-d-pc:/var/www/html/site8080# ls
index.html
root@gabriel-d-pc:/var/www/html/site8080#
```

The terminal window is part of a desktop environment. On the right side, there is a vertical dock with icons for various applications. At the bottom, there is a taskbar with system icons and a notification area showing the date '23/08/2024' and time '22:56'. A watermark 'Ativar o Windows' is visible in the bottom right corner of the terminal window.

Item 4: Arquivo de configuração e conexão ssh (Cliente)

- Comando para ir até a pasta com a configuração e depois acessar:
‘cd /etc/ssh’
‘nano sshd_config’

- Conteúdo que precisa ser alterado para possibilitar o redirecionamento de portas no cliente:



```
root@kali: /etc/ssh
File Actions Edit View Help
GNU nano 7.2 sshd_config
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
AllowTcpForwarding yes
#GatewayPorts no
GatewayPorts yes
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^A Replace    ^U Paste      ^J Justify

[ Read 124 lines ]
Acesse Configurações para ativar o Windows.
```

- Os atributos ‘AllowTcpForwarding’ e ‘GatewayPorts’ devem estar com o valor ‘yes’ para possibilitar o redirecionamento de porta local do ssh.

Item 5: Comunicação entre as placas de redes

- Mostrando que o Cliente (IP 192.168.10.20) consegue se comunicar com o Servidor (IP 192.168.10.10)

```
root@kali: /etc/ssh
File Actions Edit View Help
(root@kali)-[/etc/ssh]
# ip -br -c a
lo                UNKNOWN          127.0.0.1/8  ::1/128
eth0              UP                10.0.2.15/24 fe80::a00:27ff:fe09:fa69/64
eth1              UP                192.168.10.20/24 fe80::a00:27ff:fec4:e5d8/64
eth2              UP                192.168.15.26/24 2804:431:8252:d901:a00:27ff:
feaf:b75b/64 fe80::a00:27ff:feaf:b75b/64

(root@kali)-[/etc/ssh]
# ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
64 bytes from 192.168.10.10: icmp_seq=1 ttl=64 time=0.888 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=64 time=0.695 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=64 time=0.865 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=64 time=0.806 ms
64 bytes from 192.168.10.10: icmp_seq=5 ttl=64 time=0.657 ms
64 bytes from 192.168.10.10: icmp_seq=6 ttl=64 time=0.695 ms

```

Ativar o Windows
Acesse Configurações para ativar o Windows

23:10
23/08/2024

Right Control

- Mostrando que o Servidor (IP 192.168.10.10) consegue se comunicar com o Cliente (IP 192.168.10.20)

```

gabriel@gabriel-d-pc: ~
Arquivo Editar Exibir Pesquisar Terminal Ajuda
root@gabriel-d-pc:/etc/ssh# ip -br -c a
lo                UNKNOWN        127.0.0.1/8 ::1/128
enp0s3            UP                10.0.2.15/24 fe80::a00:27ff:fe3f:8fc0/64
enp0s8            UP                192.168.10.10/24 fe80::a00:27ff:fed4:9a67/64
enp0s9            UP                192.168.15.25/24 2804:431:8252:d901:a00:27ff:fe7:7157/64 fe80::a00:27ff:fe7:7157/64
root@gabriel-d-pc:/etc/ssh# ping 192.168.10.20
PING 192.168.10.20 (192.168.10.20) 56(84) bytes of data.
64 bytes from 192.168.10.20: icmp_seq=1 ttl=64 time=1.10 ms
64 bytes from 192.168.10.20: icmp_seq=2 ttl=64 time=0.694 ms
64 bytes from 192.168.10.20: icmp_seq=3 ttl=64 time=0.711 ms
64 bytes from 192.168.10.20: icmp_seq=4 ttl=64 time=0.696 ms
64 bytes from 192.168.10.20: icmp_seq=5 ttl=64 time=0.745 ms

```

Item 6: Portas abertas do servidor

- Mostrando as portas abertas do Servidor (Debian) através do comando 'netstat -nltp':

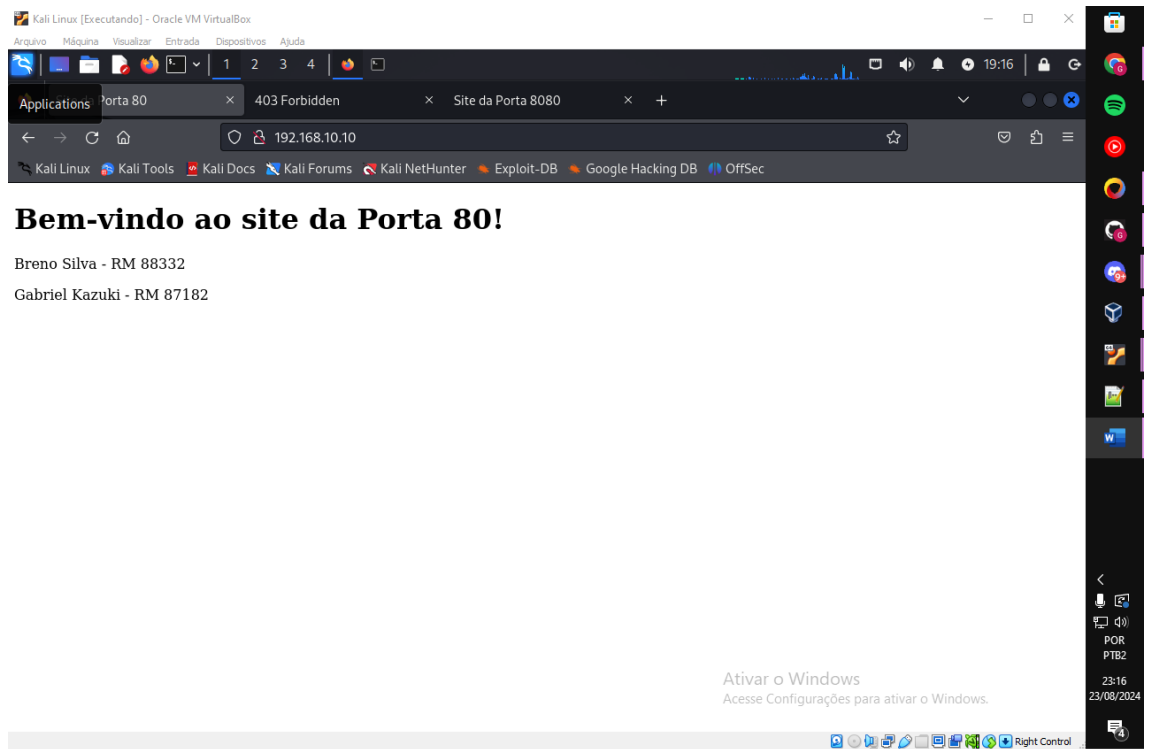
```

gabriel@gabriel-d-pc: ~
Arquivo Editar Exibir Pesquisar Terminal Ajuda
root@gabriel-d-pc:/etc/ssh# 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        10680/sshd: /usr/sb
tcp        0      0 127.0.0.1:631       0.0.0.0:*             OUÇA        640/cupsd
tcp6       0      0 :::22              :::*                  OUÇA        10680/sshd: /usr/sb
tcp6       0      0 :::80              :::*                  OUÇA        10012/apache2
tcp6       0      0 :::1:631           :::*                  OUÇA        640/cupsd
tcp6       0      0 :::8080            :::*                  OUÇA        10012/apache2
root@gabriel-d-pc:/etc/ssh#

```

Item 7: Site do servidor acessado através do cliente na porta 80

- Acessando o site 192.168.10.10:80 no Cliente (Kali Linux) usando o Mozilla



Item 8: Site do servidor acessado através do cliente na porta 8080
acessado no localhost

- Acessando o site localhost:2222 no Cliente (Kali Linux) usando o Mozilla, que está sendo redirecionado para a porta 8080 do localhost da máquina do Servidor via SSH.

