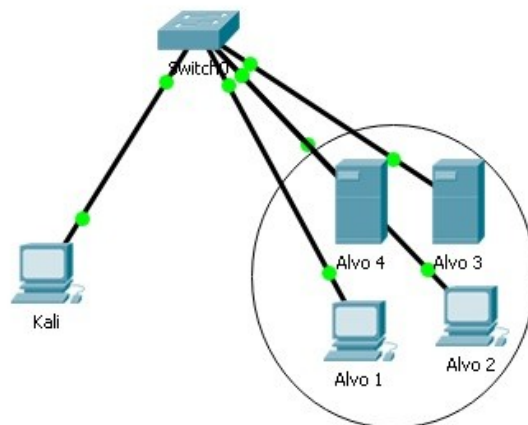


LABORATÓRIO E ATIVIDADE - CONFIGURANDO SERVIDOR SSH E SFTP:

Nome: Efraim de Almeida Lima
Nome: Giovanna Pardini Cansian
Nome: Gabriel Pereira

RA: 1680972323048
RA: 1680972323045
RA: 1680972323020

Topologia



Objetivos

Parte 1: Preparar as máquinas virtuais

Parte 2: Configuração do Servidor SSH e SFTP

Parte 1 – Preparando as Máquinas Virtuais:

- Escolher o modo **host-only** as duas máquinas virtuais;
- Kali Linux para realização dos testes;
 - Uma máquina virtual Linux como alvo (Metasploitable2).

```
root@kali:~/home/kali# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.2 netmask 255.0.0.0 broadcast 10.255.255.255
    inet6 fe80::a00:27ff:fe9d:2762/64 Scope:Link
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
    RX packets 42 bytes 5983 (5.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 11 bytes 866 (866.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~/home/kali#

root@metasploitable2:~/home/rsfadmin# ifconfig eth0 10.0.2.1
root@metasploitable2:~/home/rsfadmin# ifconfig
eth0
    Link encap:Ethernet Hwaddr 08:00:27:9a:27:62
    inet addr:10.0.2.1 Bcast:10.255.255.255 Mask:255.0.0.0
    inet6 addr: fe80::a00:27ff:fe9d:2762/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:221 errors:0 dropped:0 overruns:0 frame:0
    TX packets:83 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:3147 (3.0 KB) TX bytes:10351 (10.1 KB)
    Base address:0x010 Memory:00000000-f0020000

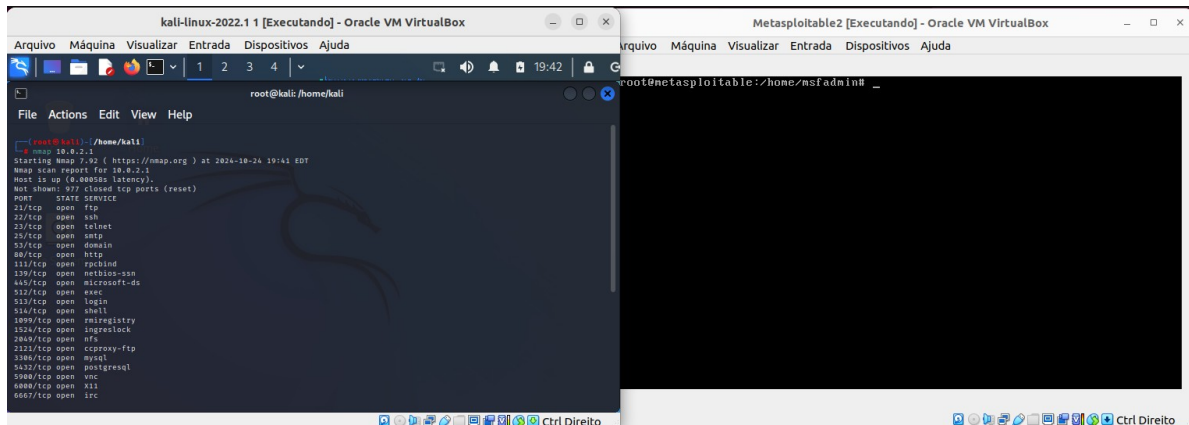
lo
    Link encap:Local Loopback
    inet addr:127.0.0.1 Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
    UP LOOPBACK RUNNING MTU:16436 Metric:1
    RX packets:10826 errors:0 dropped:0 overruns:0 frame:0
    TX packets:10826 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:7086045 (6.7 MB) TX bytes:7086045 (6.7 MB)

root@metasploitable2:~/home/rsfadmin#
```

Parte 2 – Testes na Máquina Linux (Kali <-> Metasploitable2) – Serviço SSH e SFTP:

2.1. 1. Verificar com o nmap os serviços:

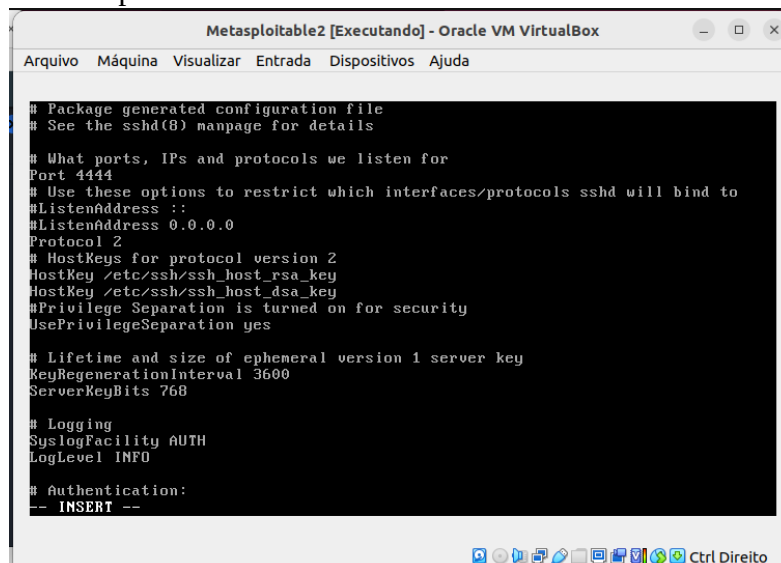
nmap IP (usar o endereço IP que estiver disponível no modo Host Only)



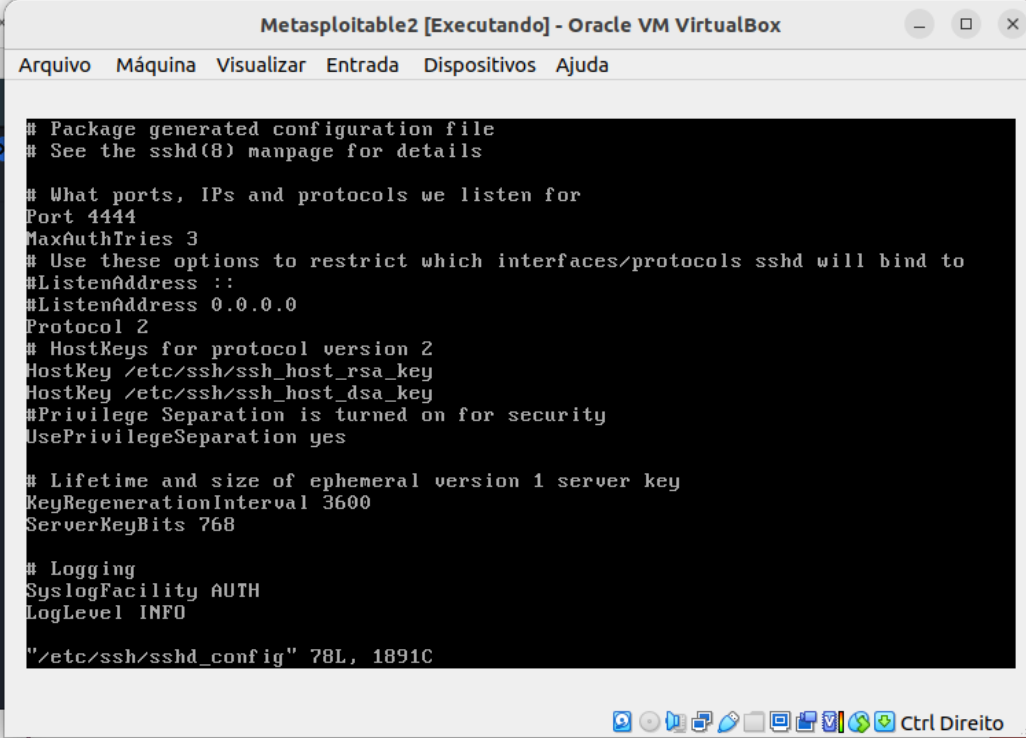
2.1.2. Alterando a porta no servidor (Metasploitable2).

nano /etc/ssh/sshd_config //editando as configurações no servidor SSH
Ctrl+O+enter // salvando
Ctrl+X // fechar a edição

Alterando a para **4444**.



2.1.3. Configurar o parâmetro **MaxAuthTries 3** no servidor SSH (Metasploitable)



```
# Package generated configuration file
# See the sshd(8) manpage for details

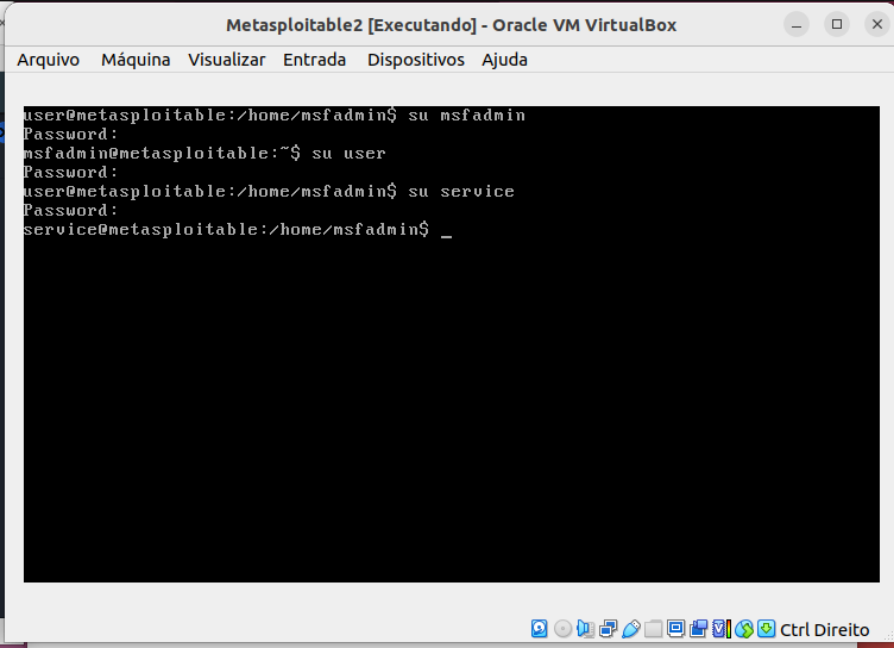
# What ports, IPs and protocols we listen for
Port 4444
MaxAuthTries 3
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

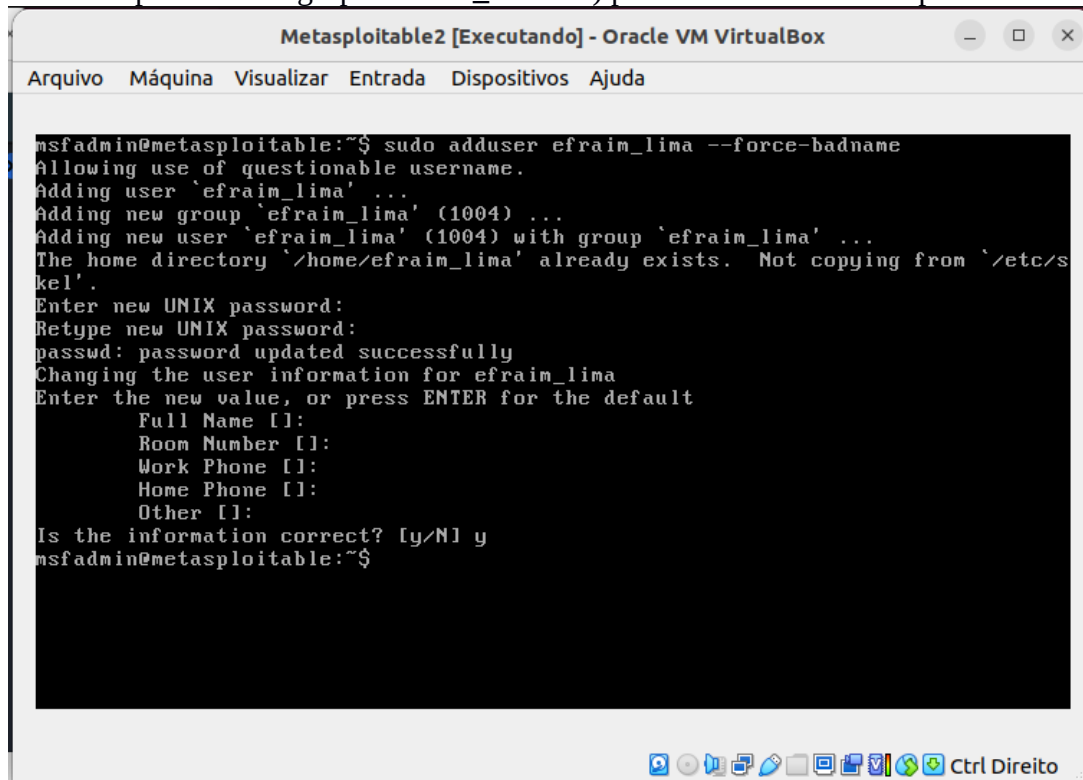
"/etc/ssh/sshd_config" 78L, 1891C
```

2.1.4. Acessando usuários **msfadmin**, **user**, **service**. Desabilitar esses usuários?



```
user@metasploitable:/home/msfadmin$ su msfadmin
Password:
msfadmin@metasploitable:~$ su user
Password:
user@metasploitable:/home/msfadmin$ su service
Password:
service@metasploitable:/home/msfadmin$ _
```

2.1.5. Criando um usuário no servidor (criar o usuário com o nome de um dos componentes do grupo - **nome_usuario**) para conexão via chave pública:

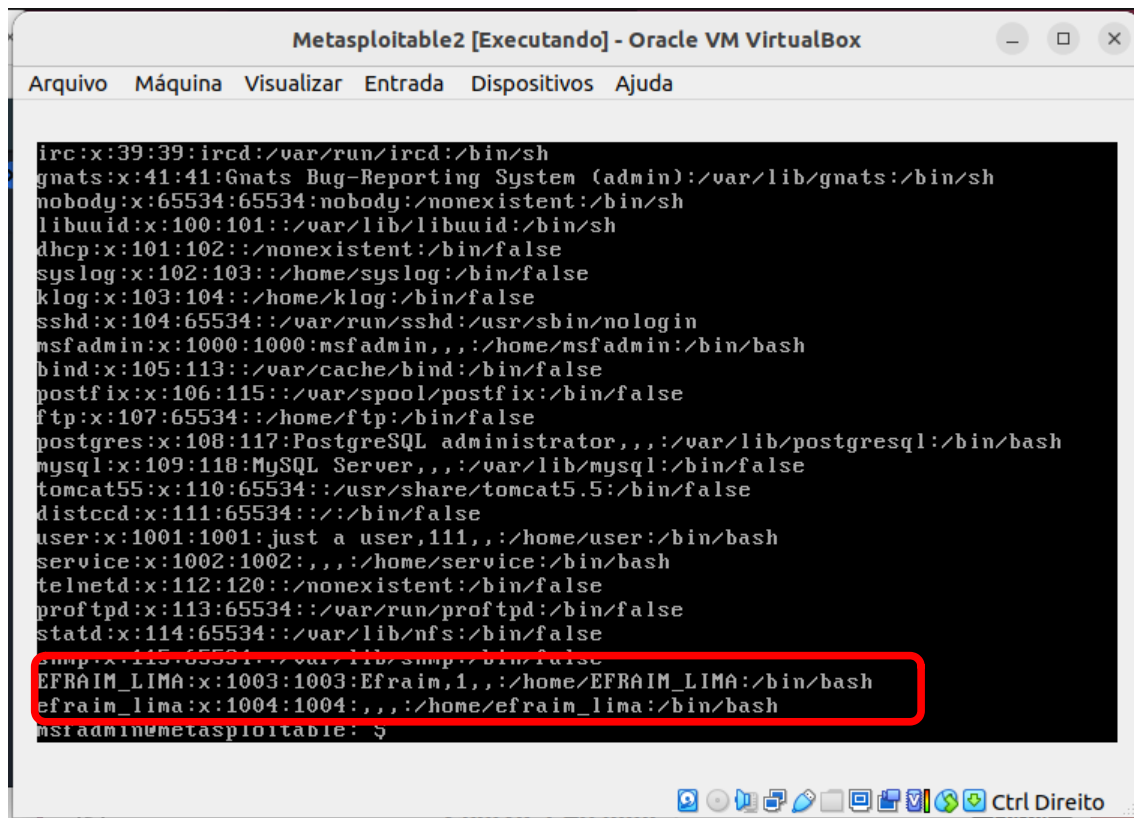


The screenshot shows a terminal window titled "Metasploitable2 [Executando] - Oracle VM VirtualBox". The terminal output is as follows:

```
msfadmin@metasploitable:~$ sudo adduser efrain_lima --force-badname
Adding user 'efrain_lima' ...
Adding new group 'efrain_lima' (1004) ...
Adding new user 'efrain_lima' (1004) with group 'efrain_lima' ...
The home directory '/home/efrain_lima' already exists. Not copying from '/etc/skel'.
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for efrain_lima
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [y/N] y
msfadmin@metasploitable:~$
```

Verificar o usuário que foi criado com o comando no servidor:

```
cat /etc/passwd
```

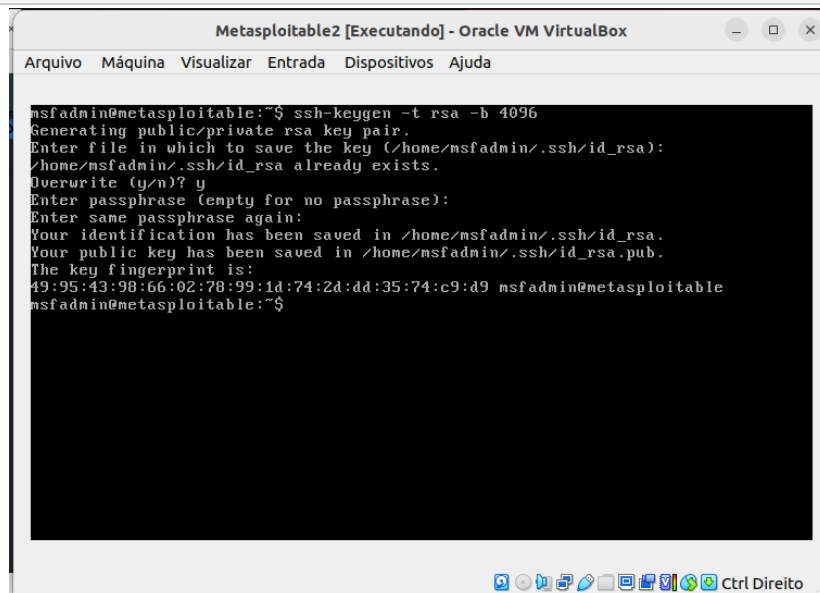


```
Metasploitable2 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002::,/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
EFRAIM_LIMA:x:1003:1003:Efrain,1,,:/home/EFRAIM_LIMA:/bin/bash
efrain_lima:x:1004:1004::,/home/efrain_lima:/bin/bash
msfadmin@metasploitable: $
```

2.1.6. Criando o par de chaves (chave pública e chave privada) no Kali e comprovando o envio da chave pública no servidor:

ssh-keygen -t rsa -b 4096 // gerando o par de chaves



```
Metasploitable2 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

msfadmin@metasploitable:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/msfadmin/.ssh/id_rsa):
/home/msfadmin/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/msfadmin/.ssh/id_rsa.
Your public key has been saved in /home/msfadmin/.ssh/id_rsa.pub.
The key fingerprint is:
49:95:43:98:66:02:78:99:1d:74:2d:dd:35:74:c9:d9 msfadmin@metasploitable
msfadmin@metasploitable:~$
```

ls -l /root/.ssh // verificando o par de chaves

```
Metasploitable2 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

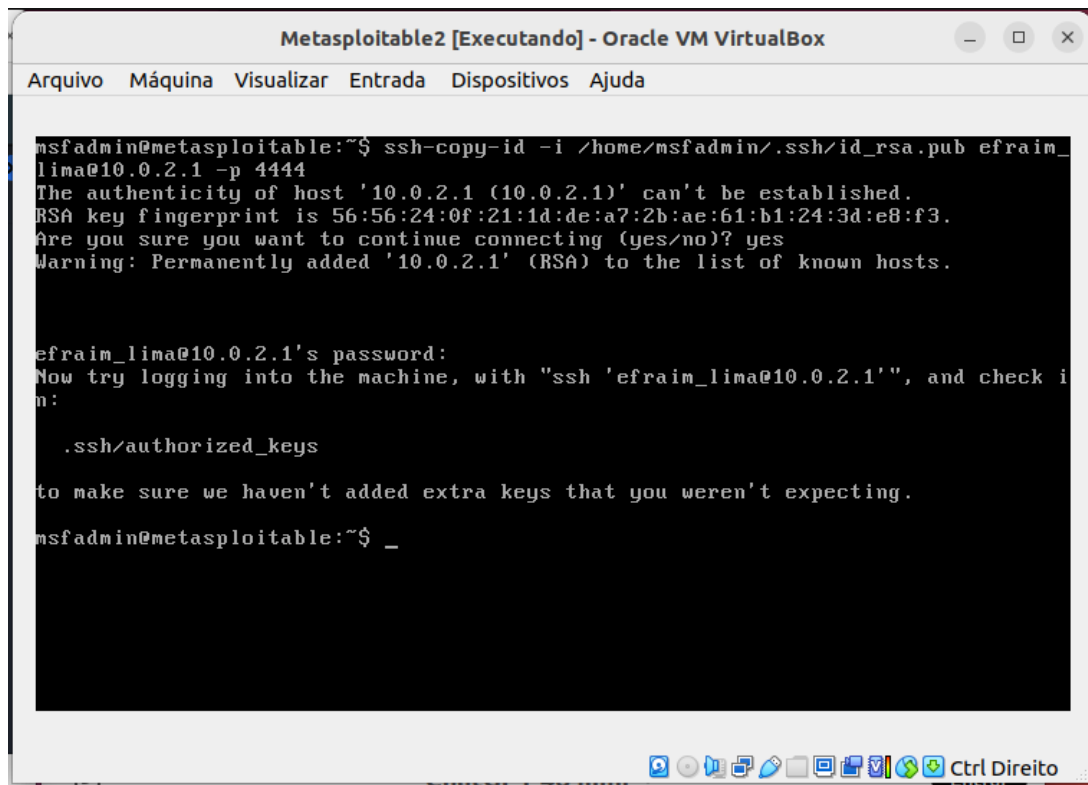
msfadmin@metasploitable:~$ ls -l /root/.ssh
total 8
-rw-r--r-- 1 root root 405 2010-05-17 21:44 authorized_keys
-rw-r--r-- 1 root root 442 2012-05-20 14:21 known_hosts
msfadmin@metasploitable:~$ cat /home/msfadmin/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAgUQBn+WIkV4fnceLB/EgGLDoLNsF+M6Z1TCAvguj9MmM
DyCqaa6d01/L0/z806KtdAbM6/HrIN+ADv5C4pd3HNggvbAgPzB+Mgg/085CpBmgCcCP80QIpr57SzY
xwxu0sqQt50hFuNszt8iuLXusM96CQY2kI60acMmLKhdk1+e4wQ7THyaZD8LuIU2fjz98ZVNfcv0CfF
gksaEuW2yfWQwNb/OblyRSomlNu2xE09MaH4z0yIqu40HEOrMKX91EfEyrkMcw6pGxCiBG1kYCjLnnb5
t9IqUFQGmewNXD+dfT7Q/bZh0jBqq0Un17WqTU05fzq3HYE0mNsdTMKhwl1qfzYf3gKLaMq+kqZHfJt1
NjEjtWrd07nPrRa7FzS00fzg0mvHtR881Y1NWODrLBcp0QVTepmmU6v28m8TFU2Tuowt/d0s5wAGP6/
7JqBusPuYtmcYkG5gTIQsMPZBjXRlvtbnJP7Zu3/Z/9NQiLrHHc5R0nbuMzvGuFW0ImAHmLLoNTn+g9R
X8AbFhIxEk5r6h5Y+DLADbHch070eR/r+cr8Nik2rK4jhgr4Acx1uHiDdBZ4NDoaFBldNZ8amSqmieE
ARWKKULNxyf6aRJUh60sdb0tTntmjaJON+RVCEQCHqW0My/K0H+9T21tas/G34XTg/Ieafufh0jLMsw8=
msfadmin@metasploitable
msfadmin@metasploitable:~$
```

cat /root/.ssh/id_rsa.pub // visualizando a chave pública

```
Metasploitable2 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

msfadmin@metasploitable:~$ ls -l /root/.ssh
total 8
-rw-r--r-- 1 root root 405 2010-05-17 21:44 authorized_keys
-rw-r--r-- 1 root root 442 2012-05-20 14:21 known_hosts
msfadmin@metasploitable:~$ cat /home/msfadmin/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAgUQBn+WIkV4fnceLB/EgGLDoLNsF+M6Z1TCAvguj9MmM
DyCqaa6d01/L0/z806KtdAbM6/HrIN+ADv5C4pd3HNggvbAgPzB+Mgg/085CpBmgCcCP80QIpr57SzY
xwxu0sqQt50hFuNszt8iuLXusM96CQY2kI60acMmLKhdk1+e4wQ7THyaZD8LuIU2fjz98ZVNfcv0CfF
gksaEuW2yfWQwNb/OblyRSomlNu2xE09MaH4z0yIqu40HEOrMKX91EfEyrkMcw6pGxCiBG1kYCjLnnb5
t9IqUFQGmewNXD+dfT7Q/bZh0jBqq0Un17WqTU05fzq3HYE0mNsdTMKhwl1qfzYf3gKLaMq+kqZHfJt1
NjEjtWrd07nPrRa7FzS00fzg0mvHtR881Y1NWODrLBcp0QVTepmmU6v28m8TFU2Tuowt/d0s5wAGP6/
7JqBusPuYtmcYkG5gTIQsMPZBjXRlvtbnJP7Zu3/Z/9NQiLrHHc5R0nbuMzvGuFW0ImAHmLLoNTn+g9R
X8AbFhIxEk5r6h5Y+DLADbHch070eR/r+cr8Nik2rK4jhgr4Acx1uHiDdBZ4NDoaFBldNZ8amSqmieE
ARWKKULNxyf6aRJUh60sdb0tTntmjaJON+RVCEQCHqW0My/K0H+9T21tas/G34XTg/Ieafufh0jLMsw8=
msfadmin@metasploitable
msfadmin@metasploitable:~$
```

ssh-copy-id -i /root/.ssh/id_rsa.pub nome_usuario@192.168.56.116 -p 4444 //
enviando a chave pública para o servidor



Metasploitable2 [Executando] - Oracle VM VirtualBox

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

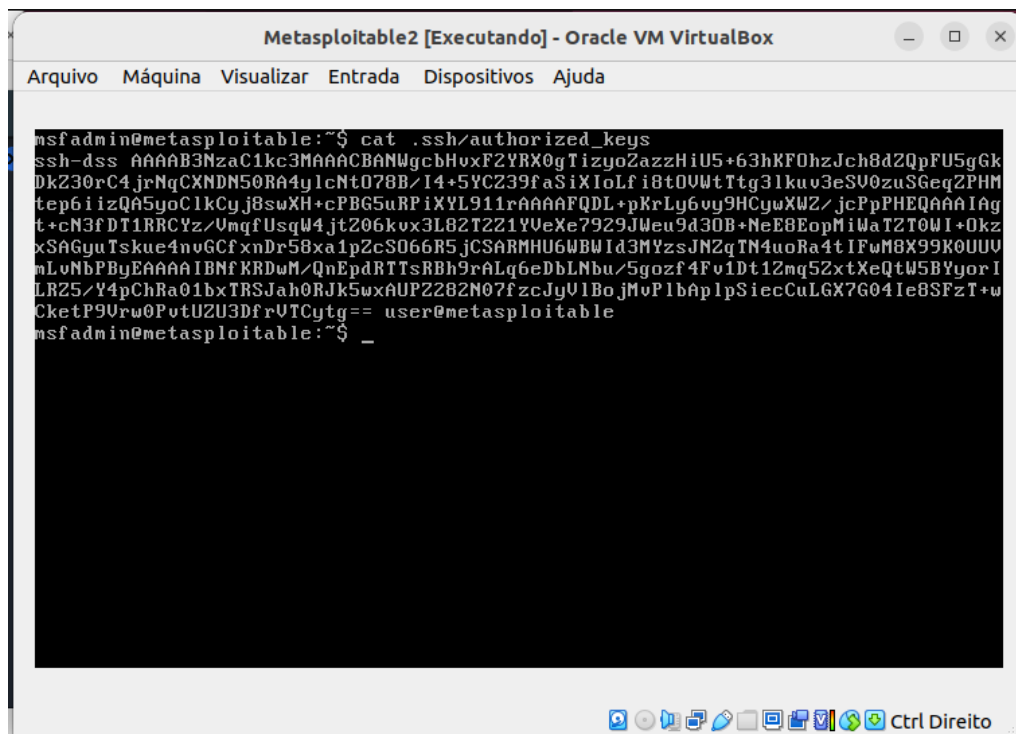
```
msfadmin@metasploitable:~$ ssh-copy-id -i /home/msfadmin/.ssh/id_rsa.pub efrain_
lima@10.0.2.1 -p 4444
The authenticity of host '10.0.2.1 (10.0.2.1)' can't be established.
RSA key fingerprint is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.1' (RSA) to the list of known hosts.

efrain_lima@10.0.2.1's password:
Now try logging into the machine, with "ssh 'efrain_lima@10.0.2.1'", and check i
n:

    .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
msfadmin@metasploitable:~$ _
```

cat .ssh/authorized_keys // verificando a chave pública no servidor



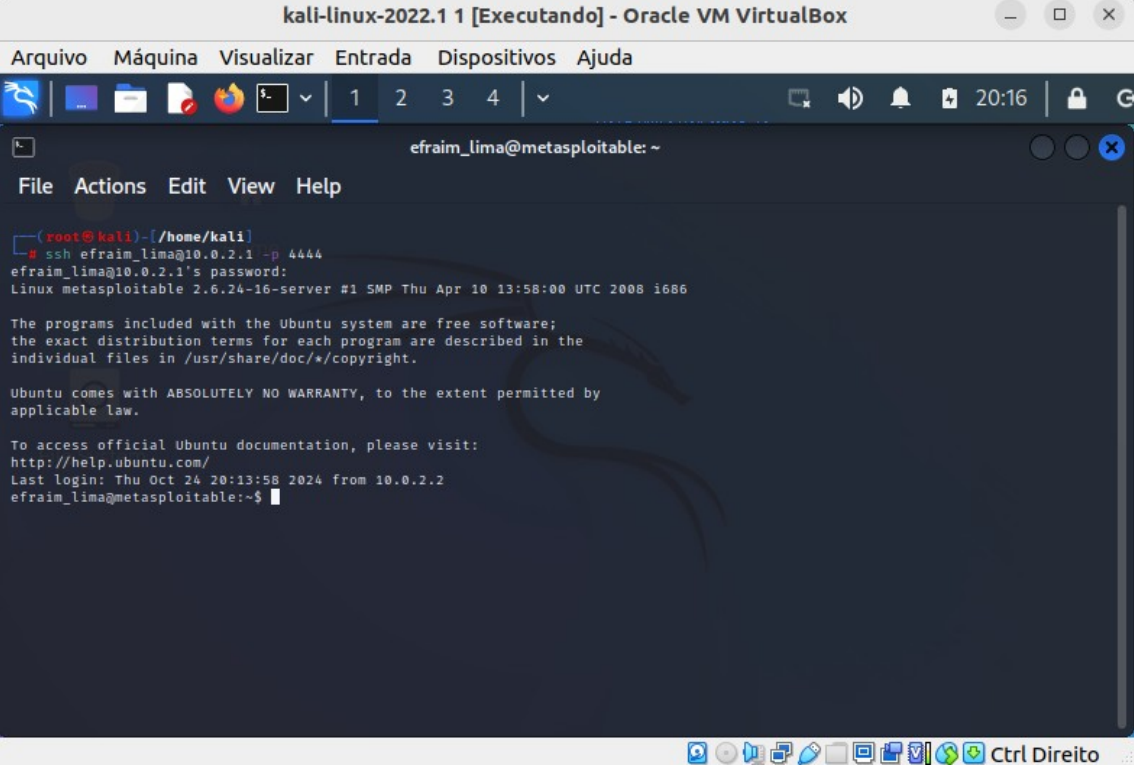
Metasploitable2 [Executando] - Oracle VM VirtualBox

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

```
msfadmin@metasploitable:~$ cat .ssh/authorized_keys
ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvxY2YRX0gTizyo2azzHiU5+63hKF0hzJch8d2QpFU5gGk
DkZ30rC4jrNqCXNDN50RA4ylcNt078B/I4+5YC239faSiXIoLf i8t0UWtTtg31kuv3eSU0zuSGeq2PHM
tep6iizQA5yoC1kCyj8swXH+cPBG5uRpiXVL911rAAAAFQDL+pKrLy6uy9HCyW2/jcPpPHEQAAAIAg
t+cN3fDT1RRCYz/UmqfUsqW4jt206kux3L82T221YUeXe7929JWu9d30B+NeE8EopMiWaT2T0WI+0kz
xSAGyuTskue4nuGCFxnDr58xa1p2cS066R5jCSARMHU6WBWId3MYzsJN2qTN4uoRa4tIFwM8X99K0UUU
nLvNbPByEAAAAIBNfKRdWm/QnEpdRTTsRBh9rALq6eDbLNbu/5gozf4Fv1Dt12mq52xtXeQtW5BYgorI
LR25/Y4pChRa01bxTRSJah0RJk5wxAUP2282N07fzcJyV1BojMvPlbAp1pSiEcCuLGX7G04Ie8SFzT+w
CketP9Vrw0PvtU2U3DfrUTCygt== user@metasploitable
msfadmin@metasploitable:~$ _
```

2.1.7. Configurando o servidor com a opção **AllowUsers nome_usuario** (nome de usuário criado no servidor)

ssh nome_usuario@192.168.56.116 -p 4444 // conectando com o usuário criado



The screenshot shows a Kali Linux terminal window titled "kali-linux-2022.1 1 [Executando] - Oracle VM VirtualBox". The terminal displays the following text:

```
(root@kali)-[/home/kali]
# ssh efrain_lima@10.0.2.1 -p 4444
efrain_lima@10.0.2.1's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Thu Oct 24 20:13:58 2024 from 10.0.2.2
efrain_lima@metasploitable:~$
```

2.1.8. Gerar os prints de tela comprovando as configurações.

2.1.9. Quais as principais vantagens de se usar o serviço ssh se comparado ao serviço telnet? Justifique.

R.: O serviço ssh, além de contar com um serviço de autenticação muito mais eficiente, conta com criptografia para a transferência de comandos entre as máquinas, isso previne que o tráfego seja interceptado e facilmente lido por um possível atacante.

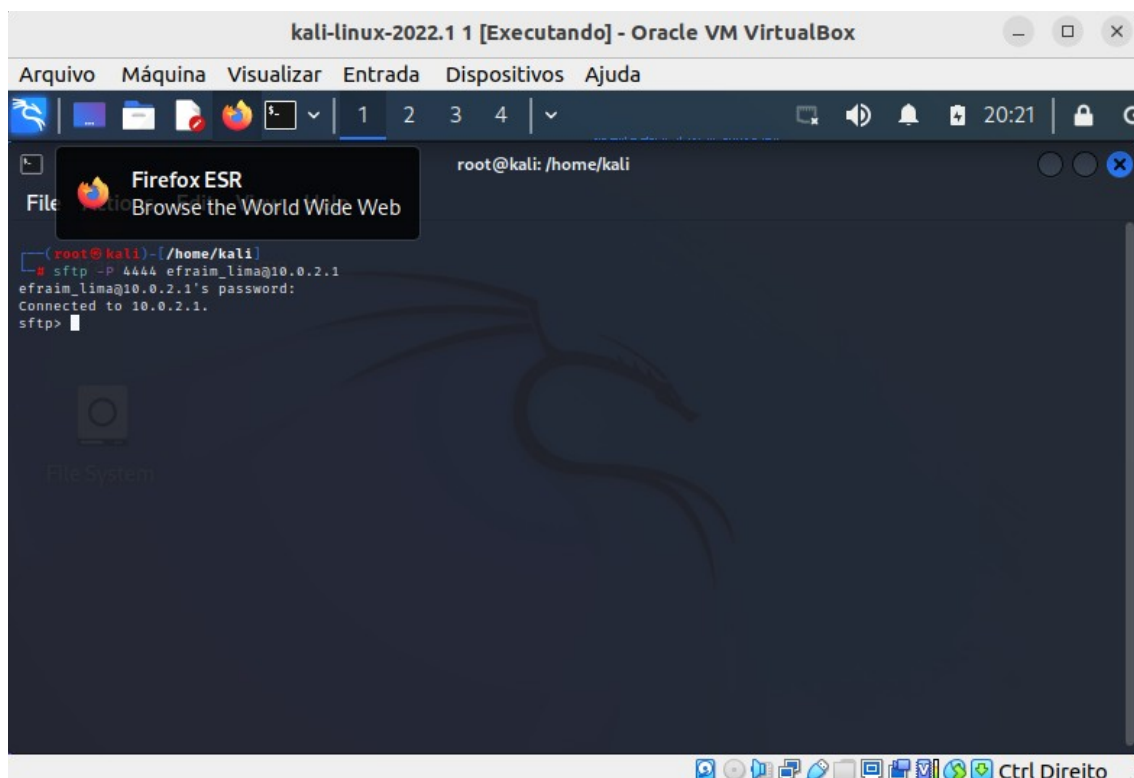
2.1.10. Quais as principais configurações realizadas para garantir uma maior segurança no servidor SSH? Justifique.

R.: O primeiro ponto é o processo de permitir apenas algumas poucas tentativas de autenticação, para evitar ataques de brute-force; mas o mais interessante é alterar sua porta padrão, com o objetivo de evitar que um atacante tenha fácil acesso a porta em que o serviço está funcionando (sendo que alterar a porta já evitaria o brute-force)

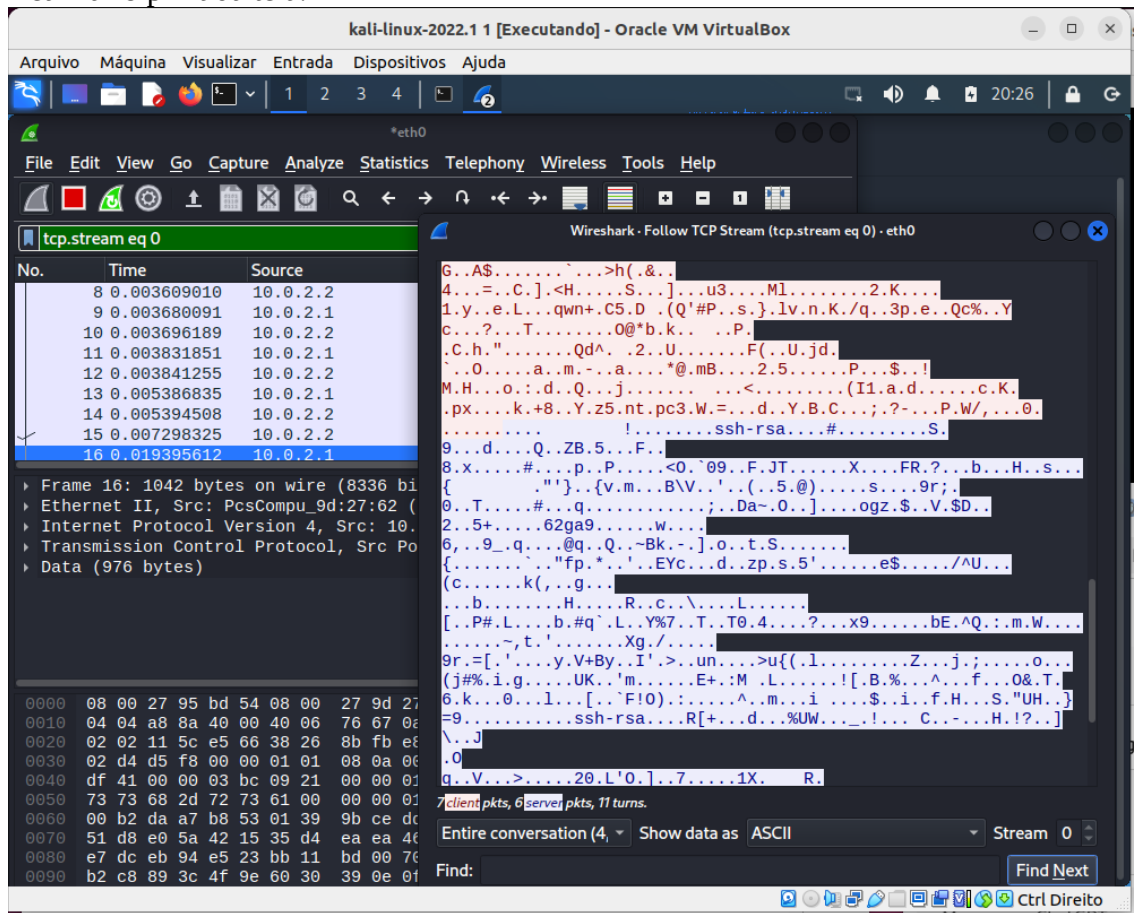
2.2. Testando o servidor SFTP:

2.1.1. Iniciar o Wireshark no Kali e na sequência acessar o serviço SFTP:

```
sftp -P 4444 nome_usuario@IP // conectando com o usuário criado na porta 4444
```

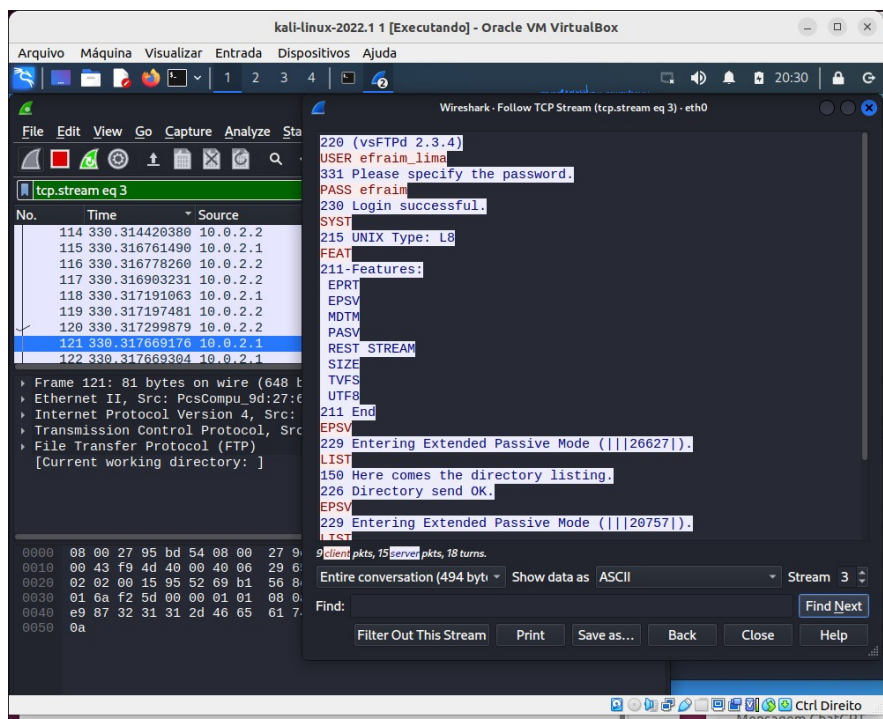


2.1.2. Finalizar a captura no Wireshark e realizar a análise offline:
 Digitar Analyse → Follow → TCP Stream (verificar o que está sendo observado).
 Realizar o print da tela.



2.1.3. Confronte o serviço ftp X sftp. Quais as principais vantagens do sftp se comparado com o ftp? Justifique.

R.: Primeiro começa que o tráfego rodado em ftp é transmitido em texto claro na rede, fazendo com que possamos interceptar e ler facilmente o que está



sendo transmitido. Já no sftp ocorre o processo de criptografia de todo o tráfego na rede, tornando sua leitura mais complexa.

Referências:

1. RFC4250 e RFC4256. The Secure Shell (SSH). Disponível em:
<https://www.ietf.org/rfc/rfc4250.txt>
<https://www.ietf.org/rfc/rfc4256.txt>