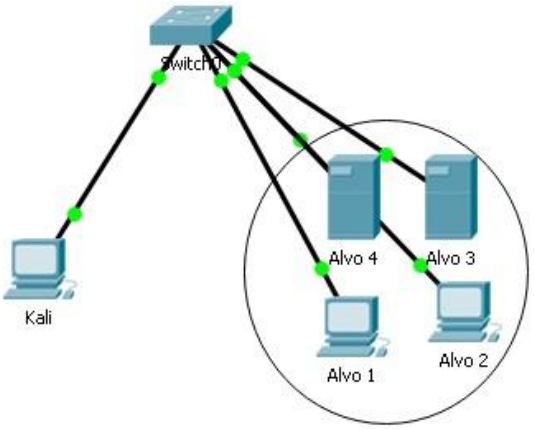
LABORATÓRIO E ATIVIDADE - CONFIGURANDO SERVIDOR SSH E SFTP:

Nome: Enzo Arrue

Topologia



Objetivos

Parte 1: Preparar as máquinas virtuais

Parte 2: Configuração do Servidor SSH e SFTP

Parte 1 – Preparando as Máquinas Virtuais:

1. Escolher o modo **host-only** as duas máquinas virtuais;

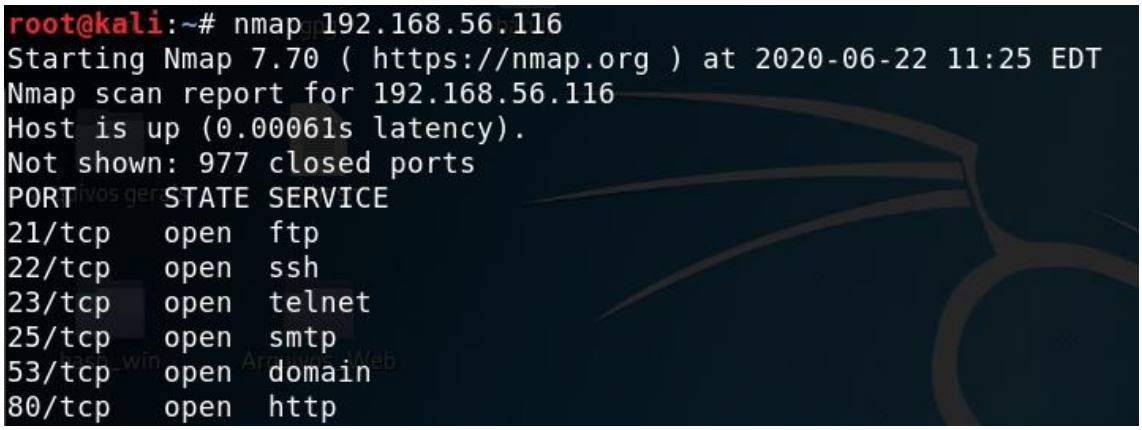
1.1. Kali Linux para realização dos testes;

1.2. Uma máquina virtual Linux como alvo (Metasploitable2).

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
Ctr+O+enter // salvando
Ctr+X // fechar a edição
```

Alterando a para **4444**.

Foi alterado no arquivo "/etc/ssh/sshd_config" : O login por root (no), Apenas nomes especificos, apenas com chave pública, alterado a porta e no máximo 3 tentativas para maior segurança

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

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

```
cat /etc/passwd
```

2.1.4. 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
```

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

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

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

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

2.1.5. 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
```

2.1.6. Gerar os prints de tela comprovando as configurações.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.56.108
Starting Nmap 7.92 ( https://nmap.org ) at 2025-05-06 06:50 EDT
Nmap scan report for 192.168.56.108
Host is up (0.00049s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
4444/tcp open  krb524
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:D0:53:FD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.57 seconds

┌──(root㉿kali)-[/home/kali]
└─# ssh msfadmin@192.168.56.108
ssh: connect to host 192.168.56.108 port 22: Connection refused

┌──(root㉿kali)-[/home/kali]
└─# ssh msfadmin@192.168.56.108 -p 4444
The authenticity of host '[192.168.56.108]:4444 ([192.168.56.108]:4444)' can'
t be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.56.108]:4444' (RSA) to the list of known
 hosts.
msfadmin@192.168.56.108's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6
```

```
┌──(root㉿kali)-[/home/kali]
└─# ssh msfadmin@192.168.56.108 -p 4444
msfadmin@192.168.56.108's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

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/
No mail.
Last login: Tue May  6 06:51:17 2025 from 192.168.56.109
msfadmin@metasploitable:~$ adduser user1
adduser: Only root may add a user or group to the system.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# adduser user1
adduser: The user `user1' already exists.
root@metasploitable:/home/msfadmin# adduser user2
adduser: The user `user2' already exists.
root@metasploitable:/home/msfadmin# adduser usuario1
Adding user `usuario1' ...
Adding new group `usuario1' (1005) ...
Adding new user `usuario1' (1005) with group `usuario1' ...
Creating home directory `/home/usuario1' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for usuario1
Enter the new value, or press ENTER for the default
        Full Name []: Yasmily Souza
        Room Number []: 40028922
        Work Phone []: 6666666
        Home Phone []: 777777
        Other []:
Is the information correct? [y/N] y
root@metasploitable:/home/msfadmin# exit
exit
msfadmin@metasploitable:~$ exit
logout
Connection to 192.168.56.108 closed.
```

```
┌──(root㉿kali)-[/home/kali]
└─# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /root/
/root/ already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Saving key "/root/" failed: Is a directory

┌──(root㉿kali)-[/home/kali]
└─# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /root/.ssh/_rsa^[[D^

Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:r5kxILMiT0MVDRK/r+KM0FP6WEt80gJts41n7WUIylM root@kali
The key's randomart image is:
+---[RSA 4096]----+
|  o.oo           |
|   o ..          |
|    o            |
|   o .           |
|  o O E S        |
| o B & + o       |
|o B & B = +      |
|.*.O X . O       |
|..=.+   =        |
+----[SHA256]-----+

┌──(root㉿kali)-[/home/kali]
└─# ls -l /root/.ssh
total 12
-rw------- 1 root root 3369 May  6 07:06 id_rsa
-rw-r--r-- 1 root root  735 May  6 07:06 id_rsa.pub
-rw-r--r-- 1 root root  442 May  6 06:51 known_hosts

┌──(root㉿kali)-[/home/kali]
└─# cat /root/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCn2JY87mO6dnbNpPE9PGVKu1LbItj2F0AMC6f1O
reWb1c+Qo4vOJsVV+NB33aB4mYb0xyn8ODjM0yae07UisoqMf6D1UA7NTDOdks89h3Q1l+lhrvCnK
AVRarPZZAzgw6SGuOdLgSewKgqCDixv0nDcDvDOgzL3HBsfXbC/8rPSyNeHVMlzeqtTeUtWRkiiaX
4YORA+p9RaVyxCvsso/vfvaInVQvJHbqAZbRbGGpA22K7Z4Iov3qkklLRsD6ckyR4djiwLv7393AX
kENDXmEiR+TYkCAsSSZfV9TRP7vSNZZf/zTAfJL05DzMHBkV5VQBPD78tYAaKzZB+oqP9vMG74Jg4
HS29zpAu7OieXY92GBjf6MzLdrs93pQwntbpvqIsroh8Mbrb3U4TYfd55y3+oX+t4lTG7ZUCDcJXC
+yewlfRsqrKKMObY4Kc9B08rt+yCMm8DLIAibKQmSN67Vxh/FCKI+bDf9JJ8U2T0evB2cBBqY7pN/
ncbGOONXACrUols2v4Pupo2VsWjaLUDuapuWpL1fRn+g3Q1/ofS9vm+e6aw3LZ9jgbbXwVJt1JXH6
```

```
# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

Subsystem sftp /usr/lib/openssh/sftp-server

UsePAM yes

MaxAuthTries 3

AllowUsers usuario1
```

[Wrote 82 lines]

```
root@metasploitable:/home/msfadmin# /etc/init.d/ssh restart
 * Restarting OpenBSD Secure Shell server sshd                      [ OK ]
root@metasploitable:/home/msfadmin#
```

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

O SSH é mais seguro que o Telnet porque criptografa todos os dados transmitidos, protegendo senhas e informações. Ele também permite autenticação por chave e transferência segura de arquivos. Já o Telnet transmite tudo em texto simples, sendo considerado obsoleto e vulnerável.

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

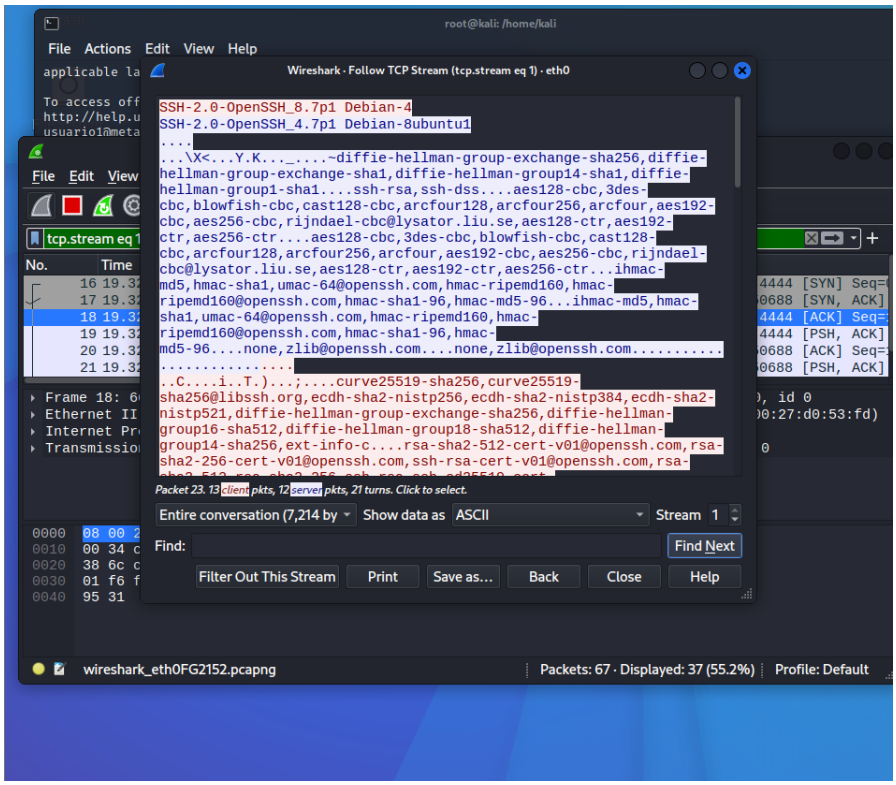
As principais configurações são desativar o login como root, mudar a porta padrão 22, usar autenticação por chave no lugar de senha e limitar o acesso por IP ou usuários. Essas medidas dificultam ataques e protegem melhor o servidor contra acessos indevidos.

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.

O SFTP é mais seguro que o FTP porque criptografa todos os dados, incluindo senhas, evitando interceptações. Ele também usa apenas uma porta, facilitando a configuração da rede. Já o FTP transmite informações em texto simples, sendo vulnerável a ataques.

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