Exercício orientado - Configuração de autenticação baseada em chave SSH

Instruções

1. Faça login na máquina `serverb` como o usuário `student`.

```
[student@workstation ~]$ssh student@serverb...output omi
tted...
[student@serverb ~]$
```

2. Alterne para o usuário `operator1` na máquina `serverb`. Use `redhat` como a senha.

```
[student@serverb ~]$su - operator1
Password:redhat
[operator1@serverb ~]$
```

3. Gere um conjunto de chaves SSH. Não insira uma senha.

```
[operator1@serverb ~]$ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/operator1/.ss
h/id_rsa):Enter
Created directory '/home/operator1/.ssh'.
Enter passphrase (empty for no passphrase):Enter
Enter same passphrase again:Enter
Your identification has been saved in /home/operator1/.s
sh/id_rsa.
Your public key has been saved in /home/operator1/.ssh/i
d_rsa.pub.
The key fingerprint is:
SHA256:JainiQdnRosC+xXh operator1@serverb.lab.example.co
m
```

```
The key's randomart image is:
+---[RSA 3072]----+
|E+*+ooo .        |
|.= o.o o .       |
|o.. = . . o      |
|+. + * . o .     |
|+ = X . S +      |
| + @ +   = .     |
|. + =   o        |
|.o . . . .       |
|o     o..        |
+----[SHA256]-----+
```

4. Envie a chave pública do par de chaves SSH para o usuário `operator1` na máquina `servera`, com `redhat` como senha.

```
[operator1@serverb ~]$ssh-copy-id operator1@servera
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be insta
lled: "/home/operator1/.ssh/id_rsa.pub"
The authenticity of host 'servera (172.25.250.10)' can't
be established.
ED25519 key fingerprint is SHA256:h/hEJa/anxp6AP7BmB5azI
PVbPNqieh0oKi4KWOTK80.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fi
ngerprint])?yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with th
e new key(s), to filter out any that are already install
ed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be instal
led -- if you are prompted now it is to install the new
keys
operator1@servera's password:redhat

Number of key(s) added: 1

Now try logging in to the machine, with:   "ssh 'operato
r1@servera'"
```

```
and check to make sure that only the key(s) you wanted w
ere added.
```

5. Execute o comando `hostname` na máquina `servera` remotamente usando o comando `ssh` sem acessar o shell interativo remoto.

   ```
   [operator1@serverb ~]$ssh operator1@servera hostname
   servera.lab.example.com
   ```

   O comando `ssh` anterior não solicita uma senha, porque usa a chave privada sem senha em relação à chave pública exportada para autenticar com o usuário `operator1` na máquina `servera`.

   Essa abordagem não é segura, porque qualquer pessoa que tenha acesso ao arquivo de chave privada pode fazer login na máquina `servera` com o usuário `operator1`.

   Em uma etapa posterior deste exercício, você tornará sua chave privada mais segura criptografando-a e protegendo o acesso a ela ao adicionar uma senha.

6. Gere outro conjunto de chaves SSH com o nome padrão e sem uma senha, e substitua os arquivos de chave SSH gerados anteriormente. Tente se conectar à máquina `servera` usando as novas chaves SSH. O comando `ssh` solicita uma senha, pois não é possível autenticar com a chave SSH. Execute novamente o comando `ssh` com a opção `v` (detalhada) para verificar a mensagem de erro.

   Envie a chave pública do par de chaves SSH para o usuário `operator1` na máquina `servera` para substituir a chave pública anterior. Use `redhat` como senha para o usuário `operator1` na máquina `servera`. Execute o comando `hostname` na máquina `servera` remotamente usando o comando `ssh` sem acessar o shell interativo remoto para verificar se ele está funcionando novamente.

   1. Novamente, gere outro conjunto de chaves SSH com o nome padrão e sem uma senha, e substitua os arquivos de chave SSH gerados anteriormente.

      ```
      [operator1@serverb ~]$ssh-keygen
      Generating public/private rsa key pair.
      ```

```
Enter file in which to save the key (/home/operator
1/.ssh/id_rsa):Enter
/home/operator1/.ssh/id_rsa already exists.
Overwrite (y/n)?y
Enter passphrase (empty for no passphrase):Enter
Enter same passphrase again:Enter
Your identification has been saved in /home/operator
1/.ssh/id_rsa
Your public key has been saved in /home/operator1/.ss
h/id_rsa.pub
...output omitted...
```

2. Tente se conectar à máquina `servera` usando as novas chaves SSH. O comando `ssh` solicita uma senha, pois não é possível autenticar com a chave SSH. Pressione **Ctrl**+**c** para sair do comando `ssh` quando ele solicitar uma senha. Execute novamente o comando `ssh` com a opção `v` (detalhada) para verificar a mensagem de erro.
Pressione **Ctrl**+**c** novamente para sair do comando `ssh` quando ele solicitar uma senha.

```
[operator1@serverb ~]$ssh operator1@servera hostname
operator1@servera's password:^C
[operator1@serverb ~]$ssh -v operator1@servera hostna
me
OpenSSH_8.7p1, OpenSSL 3.0.1 14 Dec 2021
debug1: Reading configuration data /etc/ssh/ssh_confi
g
debug1: Reading configuration data /etc/ssh/ssh_confi
g.d/01-training.conf
...output omitted...
debug1: Next authentication method: publickey
debug1: Offering public key: /home/operator1/.ssh/id_
rsa RSA SHA256:ad597Zf64xckV26xht8bjQbzqSPuOXQPXksGEW
VsP80
debug1: Authentications that can continue: publickey,
gssapi-keyex,gssapi-with-mic,password
debug1: Trying private key: /home/operator1/.ssh/id_d
sa
```

```
debug1: Trying private key: /home/operator1/.ssh/id_e
cdsa
debug1: Trying private key: /home/operator1/.ssh/id_e
cdsa_sk
debug1: Trying private key: /home/operator1/.ssh/id_e
d25519
debug1: Trying private key: /home/operator1/.ssh/id_e
d25519_sk
debug1: Trying private key: /home/operator1/.ssh/id_x
mss
debug1: Next authentication method: password
operator1@servera's password:^C
```

3. Envie a chave pública do par de chaves SSH para o usuário `operator1` na máquina `servera` para substituir a chave pública anterior.
   Use `redhat` como senha para o usuário `operator1` na máquina `servera`.
   Execute o comando `hostname` na máquina `servera` remotamente usando o comando `ssh` sem acessar o shell interativo remoto para verificar se ele está funcionando novamente.

```
[operator1@serverb ~]$ssh-copy-id operator1@server
a...output omitted...
operator1@servera's password:redhat

Number of key(s) added: 1

Now try logging in to the machine, with:   "ssh 'oper
ator1@servera'"
and check to make sure that only the key(s) you wante
d were added.
[operator1@serverb ~]$ssh operator1@servera hostname
servera.lab.example.com
```

7. Gere outro conjunto de chaves SSH com proteção de senha. Salve a chave como `/home/operator1/.ssh/key2`. Usar `redhatpass` como a senha da chave privada.

```
[operator1@serverb ~]$ssh-keygen -f .ssh/key2
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):redhatpass
Enter same passphrase again:redhatpass
Your identification has been saved in .ssh/key2.
Your public key has been saved in .ssh/key2.pub.
The key fingerprint is:
SHA256:OCtCjfPm5QrbPBgqb operator1@serverb.lab.example.c
om
The key's randomart image is:
+---[RSA 3072]----+
|O=X*             |
|OB=.             |
|E*o.             |
|Booo   .         |
|..= . o S        |
| +.o   o         |
|+.oo+ o          |
|+o.O.+           |
|+ . =o.          |
+----[SHA256]-----+
```

8. Envie a chave pública do par de chaves protegido por senha para o usuário `operator1` na máquina `servera`. O comando não solicita uma senha, porque usa a chave pública da chave privada sem senha que você exportou para a máquina `servera` na etapa anterior.

```
[operator1@serverb ~]$ssh-copy-id -i .ssh/key2.pub opera
tor1@servera
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be insta
lled: ".ssh/key2.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with th
e new key(s), to filter out any that are already install
ed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be instal
led -- if you are prompted now it is to install the new
keys
```

```
Number of key(s) added: 1

Now try logging in to the machine, with:   "ssh 'operato
r1@servera'"
and check to make sure that only the key(s) you wanted w
ere added.
```

9. Execute o comando `hostname` na máquina `servera` remotamente usando o comando `ssh`. Use a chave `/home/operator1/.ssh/key2` como o arquivo de identidade. Especifique `redhatpass` como senha, que você definiu para a chave privada na etapa anterior.

   O comando solicita a você a senha usada para proteger a chave privada do par de chaves SSH. Se um invasor obtém acesso à chave privada, ele não poderá usá-la para acessar outros sistemas, pois a própria chave privada é protegida por uma senha. O comando `ssh` usa uma senha diferente do usuário `operator1` na máquina `servera` e, portanto, os usuários devem conhecer ambas as senhas.

   ```
   [operator1@serverb ~]$ssh -i .ssh/key2 operator1@servera
   hostname
   Enter passphrase for key '.ssh/key2':redhatpass
   servera.lab.example.com
   ```

   Use o programa `ssh-agent`, como na etapa a seguir, para evitar a digitação interativa da senha ao fazer login com SSH. Usar o programa `ssh-agent` é mais conveniente e mais seguro quando os administradores fazem login em sistemas remotos regularmente.

10. Execute o programa `ssh-agent` no seu shell `Bash` e adicione a chave privada protegida por senha (`/home/operator1/.ssh/key2`) do par de chaves SSH para a sessão do shell.

    O comando inicia o programa `ssh-agent` e configura essa sessão de shell para usá-lo. Em seguida, use o comando `ssh-add` para fornecer a chave privada desbloqueada ao programa `ssh-agent`.

    ```
    [operator1@serverb ~]$eval $(ssh-agent)
    Agent pid 1729
    [operator1@serverb ~]$ssh-add .ssh/key2
    ```

```
Enter passphrase for .ssh/key2:redhatpass
Identity added: .ssh/key2 (operator1@serverb.lab.exampl
e.com)
```

11. Execute o comando `hostname` na máquina `servera` remotamente sem acessar um shell interativo remoto. Use a chave `/home/operator1/.ssh/key2` como o arquivo de identidade.

    O comando não solicita que você digite a senha de forma interativa.

    ```
    [operator1@serverb ~]$ssh -i .ssh/key2 operator1@servera
    hostname
    servera.lab.example.com
    ```

12. Abra outro terminal na máquina `workstation` e faça login na máquina `serverb` como o usuário `student`.

    ```
    [student@workstation ~]$ssh student@serverb...output omi
    tted...
    [student@serverb ~]$
    ```

13. Na máquina `serverb`, alterne para o usuário `operator1` e faça login remotamente na máquina `servera`. Use a chave `/home/operator1/.ssh/key2` como o arquivo de identidade para autenticar usando as chaves SSH.

    a. Use o comando `su` para alternar para o usuário `operator1`. Use `redhat` como a senha do usuário `operator1`.

    ```
    [student@serverb ~]$su - operator1
    Password:redhat
    [operator1@serverb ~]$
    ```

    b. Faça login na máquina `servera` como o usuário `operator1`.

    O comando solicita que você digite a senha de modo interativo, porque você não invocou a conexão por SSH do mesmo shell em que iniciou o programa `ssh-agent`.

```
[operator1@serverb ~]$ssh -i .ssh/key2 operator1@serv
era
Enter passphrase for key '.ssh/key2':redhatpass...out
put omitted...
[operator1@servera ~]$
```

14. Saia e feche todos os terminais adicionais e retorne para a máquina `workstation`.

    a. Saia e feche as janelas adicionais do terminal. Os comandos `exit` saem do shell do usuário `operator1`, encerrando a sessão do shell em que `ssh-agent` está ativo e voltando ao shell do usuário `student` na máquina `serverb`.

    ```
    [operator1@servera ~]$exit
    logout
    Connection to servera closed.
    [operator1@serverb ~]$
    ```

    b. Retorne ao sistema `workstation` como o usuário `student`.

    ```
    [operator1@serverb ~]$exit
    logout
    [student@serverb ~]$exit
    logout
    Connection to serverb closed.
    [student@workstation ~]$
    ```

Encerramento

Na máquina `workstation`, altere para o diretório pessoal do usuário `student` e use o comando `lab` para concluir este exercício. Essa etapa é importante para garantir que recursos de exercícios anteriores não afetem exercícios futuros.

```
[student@workstation ~]$lab finish ssh-configure
```

Isso conclui a seção.