Capítulo 14

Servidor SSH

14.1. Objetivos

- Iremos utilizar o ssh para realizar as conexões até as outras máquinas;
- O ssh criptográfa os dados pela rede, ao contrário do telnet;
- O ssh é muito utilizado por administradores Linux e Unix;

14.2. Introdução Teórica

Secure Shel ou SSH é o conjunto de padrões e o protocolo associado que permite estabelecer um canal seguro entre dois computadores. Ele utiliza o sistema de chave criptográfica pública para autenticar um computador remoto, podendo utilizar esse sistema de chaves, também para autenticar usuários. A idéia do SSH é prover confidencialidade e integridade dos dados trocados entre dois computadores usando criptografia e mensagens de autenticação codificadas (MACs).

Esse protocolo é tipicamente utilizado para conectar-se à máquinas remotas e executar comandos, entretanto, há inúmeras outras funcionalidades como realizar tunelamentos, redirecionamento de portas, conexões X11 (interface gráfica) além de transferência de arquivos.

Em geral, o SSH utiliza a porta 22/tcp e é a alternativa segura ao TELNET e FTP uma vez que eles não utilizam criptografia.

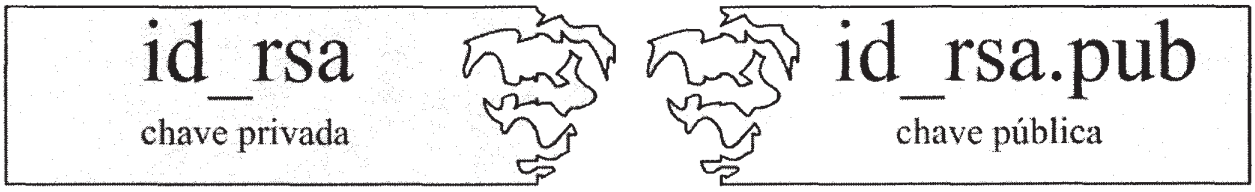
14.3. Chaves de Criptografia Assimétricas

Criar um par de chaves assimétricas tem basicamente duas funções:

- aumentar o nível de segurança - ``definindo uma frase senha'';
- facilitar a execução de scripts remotamente - ``não definir uma frase senha''.

A criação de chaves assimétricas consiste na geração de dois arquivos que contém seqüências de caracteres aleatórios (pseudo) e que só têm funcionalidade se os dois trabalharem em conjunto. Ou seja, quando criamos um par de chaves será criada uma chave pública e uma chave privada. A chave privada é sua e absolutamente ninguém deve ter acesso a ela; a sua chave pública você coloca no servidor remoto. Quando você tentar estabelecer uma conexão ela só será possível se a chave privada se encaixar na chave pública. Com esse sistema, existe apenas uma única chave privada que se encaixa em uma única chave pública.

Como só há um par que se completa, apenas quem possuir a chave privada poderá estabelecer uma conexão utilizando a respectiva chave pública. Uma ilustração do par de chaves assimétricas pode ser vista na figura:



Quando criamos um par de chaves assimétricas devemos tomar o cuidado com a chave privada para que ninguém tenha acesso a ela.

14.4. Formas de Utilização

O SSH possui diversas formas de utilização; a mais básica de todas serve para estabelecer uma simples shell remota:

```
# ssh nome_usuario_remoto@ip_servidor
```

Para copiar arquivos de uma máquina para outra, deve-se seguir a mesma lógica do comando cp que funciona da seguinte forma:

```
# cp origem destino
```

No caso do SCP a sintaxe é praticamente a mesma:

```
# scp origem destino
```

A diferença é que a origem e/ou o destino podem ser remotos, ficando, por exemplo:

```
# scp arquivo-local usuario-remoto@ip-remoto:path-destino
```

para copiar da máquina local para a máquina remota, ou para copiar da máquina remota para a máquina local!

```
# scp usuario-remoto@ip-remoto:path-origem destino-local
```

14.5. Prática Dirigida

14.5.1. Configuração do Servidor de SSH

1) Instale o servidor de SSH:

```
# aptitude install ssh
```

Red Hat:

```
# yum install ssh
```

Há diversos parâmetros de configuração que podem ser alterados de forma a ajustar seus parâmetros de funcionamento.

2) Vamos entender alguns desses parâmetros editando o arquivo de configuração do servidor de SSH:

```
# vi /etc/ssh/sshd_config
```

```
Port 22
Protocol 2
LoginGraceTime 60
PermitRootLogin yes
PubkeyAuthentication yes
PermitEmptyPasswords yes
```

Dica LPI: Leitura Sugerida: Para conhecer mais detalhes cobrados na prova leia o man sshd_config

3) Após realizar as devidas alterações, vamos subir o daemon do servidor SSH:

```
# /etc/init.d/ssh stop
# /etc/init.d/ssh start
```

4) Determine qual é a porta utilizada pelo SSH:

```
# grep ssh /etc/services
```

5) Verifique que a porta 22 está aberta e escutando:

```
# netstat -ltan | grep 22
# fuser -v 22/tcp
```

14.5.2. Utilização do Cliente de SSH

Agora, como usuário comum, vamos realizar as seguintes tarefas:

1) Conecte-se ao servidor na máquina de um colega utilizando o usuário criado para você durante o capítulo do telnet:

```
$ ssh ip_servidor
$ ssh usuario@ip_servidor
$ ssh -l usuario ip_servidor
```

2) Execute um comando na máquina remota sem estabelecer conexão:

```
$ ssh   usuário@ip_servidor  du -hs /usr
```

14.5.3. Copiando Arquivos Remotos

1) Copie um arquivo da sua máquina local para a máquina remota utilizando o scp:

```
$ echo "Meu primeiro SCP" > /tmp/seu_nome
$ scp /tmp/seu_nome <usuario>@<ip_servidor>:diretorio_destino
```

2) Crie um arquivo na sua máquina e dê permissão para que qualquer usuário possa copiá-lo:

```
$ echo "Alguma frase" > /tmp/$HOSTNAME
$ chmod 777 /tmp/$HOSTNAME
```

3) Agora, utilizando o scp, copie o respectivo arquivo da máquina de um colega:

```
$ scp seu_nome@ip_servidor:/tmp/micronumero .
```

14.5.4. SSH com Chaves Assimétricas

Quando criarmos o par de chavs assimétricas, será criado um diretório ~/.ssh na home do usuário.

1) Em nossa máquina local, sem ser via ssh, vamos criar o par de chaves

$ ssh-keygen -t rsa

```
Generating public/private rsa key pair.
Enter file in which to save the key
(/home/;lt;seu_usuario;gt;/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
/home/;lt;seu_usuario;gt;/.ssh/id_rsa.
Your public key has been saved in
/home/;lt;seu_usuario;gt;/.ssh/id_rsa.pub.
The key fingerprint is:
c6:51:3e:75:0e:10:b7:98:5d:6d:81:5f:8a:8f:38:2a
The key's randomart image is:
+--[ RSA
 seu_usuario;gt;@micro#
```

Obs.: o nome do arquivo pode ser escolhido o padrão mesmo! Basta pressionar a tecla enter. Mas, repare que ele pede uma ``passphrase'' não uma ``password''. Isso porque a idéia é aumentar a segurança, o que inclui uma senha maior!

2) Verifique que as chaves foram criadas:

$ ls ~/.ssh

3) Agora que criamos essa chave, precisamos copiar a chave pública para a máquina remota!Copie a chave pública para a máquina remota:

$ scp ~/.ssh/id_rsa.pub seu_nome@ip_servidor:.ssh/authorized_keys

4) Agora é só acessar o servidor normalmente, e ver se ele pede a passphrase para a chave criada:

```
# ssh seu_nome@ip_servidor
```

5) Vamos entender alguns desses parâmetros editando o arquivo de configuração do servidor de SSH:

```
# vi /etc/ssh/sshd_config
```

```
Port 65100
PermitRootLogin no
PubkeyAuthentication yes
PermitEmptyPasswords no
Banner /etc/issue.net
```

14.6. **Exercícios Teóricos**

1) Considere o seguinte parâmetro de configuração do servidor de SSH:

```
PermitRootLogin forced-commands-only
```

O que esse parâmetro faz e qual a diferença entre usar forced-commands-only e no?

_____

_____

2) Considere os dois comandos a seguir:

```
# scp /tmp/arquivo usuario@192.168.200.254:
# scp /tmp/arquivo usuario@192.168.200.254:/home/teste
```

Qual é a diferença entre eles?

_____

_____

3) Para que serve o arquivo knowhosts dentro de ~/.ssh/ ?

_____

_____

14.7. Laboratório

1. Utilizando o comando scp, envie uma cópia do diretório /etc local para o diretório home remoto do seu usuário.

2. Altere a configuração do servidor para que o root não possa se conectar via ssh mas possa dar comandos remotos. Realize testes para ver se funciona.

3. Gere uma chave assimétrica para o root, sem senha, e realize testes para ver se funcionou.