Instalação do Servidor SSH

Prof. Dr. Márcio Andrey Teixeira
Instituto Federal de São Paulo – Campus Catanduva
Catanduva, SP
Membro Sênior do IEEE
marcio.andrey@ifsp.edu.br

Servidor de Acesso Remoto - SSH

O ssh é um programa utilizado para fazer acesso remoto criptografado, onde esta é a principal diferença com relação ao serviço telnet padrão ou outros serviços que não utilizam criptografia.

Em conexões sem criptografia (rsh, rlogin) os dados trafegam na rede de forma desprotegida. Ou seja, caso exista algum *sniffer* instalado na rede, é possível capturar o tráfego da rede, incluindo as senhas.

Os principais utilitários são encontrados no pacote do ssh são:

ssh - Cliente ssh (console remoto).
sshd - Servidor de shell ssh.
scp - Programa para transferência de arquivos entre cliente/servidor
sftp - Cliente ftp com suporte a comunicação segura.
sftp-server - Servidor ftp com suporte a comunicação segura.

SSH - Instalação

Para instalar o servidor ssh no Ubuntu, abra um terminal e execute os seguintes comandos:

sudo apt-get install openssh-server

Para verificar se o processo está em execução:

sudo service ssh status

Sub-Process /usr/bin/dpkg returned an error code (1)

Execute os seguintes comandos:

cd /var/lib/dpkg/info/
ls | grep "install-info" sudo rm install-info*
sudo rm install-info*
sudo apt-get install -f
sudo dpkg --configure -a

SSH - Configuração

Os arquivos utilizados para a configuração do ssh são:

/etc/ssh/sshd_config - Arquivo de configuração do servidor ssh.
/etc/ssh/ssh_config - Arquivo de configuração do cliente ssh.
~/.ssh/config - Arquivo de configuração pessoal do cliente ssh.

Abra o arquivo de configuração e verifique as opções existentes. Dentro do diretório **/etc/ssh** digite:

sudo pico sshd_config

SSH - Configuração

A configuração padrão é funcional, porém, existe algumas opções que são importantes. Por exemplo:

Port //Especifica as portas que o servidor SSH receberá as conexões dos clientes. O padrão é a porta 22.

Allow Users //Especifica a lista de usuários que poderão conectar ao servidor.

PermitRootLogin //Permite o acesso remoto utilizando a conta de root.

Acessando o computador remoto

Para acessar o computador remoto, execute o seguinte comando:

ssh numero_IP

ou

ssh nome_usuario@numero_IP

ou

ssh nome_usuario@numero_IP –p numero_porta

ou

ssh –l nome_usuario numero_IP –p numero_porta

Usando o scp

Permite a cópia de arquivos entre o cliente/servidor ssh. A sintaxe usada por este comando é a seguinte:

scp [*origem*] [*destino*]

Os parâmetros de *origem* e *destino* são semelhantes ao do comando cp mas possui um formato especial quando é especificado uma máquina remota.

Um caminho padrão - Quando for especificado um arquivo local. Por exemplo: /usr/src/arquivo.tar.gz.

Exemplo:

usuario@host_remoto:/diretório/arquivo - Quando desejar copiar o arquivo **de/para** um servidor remoto usando sua conta de usuário. Por exemplo:

Exemplos:

scp user@domain:/pasta-remota/arquivo-remoto.txt /pasta-local/arquivo-local.txt

sudo scp -C /root/mat.pdf root@192.168.0.10:/root
root@192.168.0.10's password:
mat.pdf **100% 142KB 141.9KB/s 00:00**

sudo scp -C root@192.168.0.10:/root/imprimir .

root@192.168.0.10's password:
imprimir 100% 51 0.1KB/s 00:00

A opção *-C* é recomendável para aumentar a taxa de transferência de dados usando compactação. Caso a porta remota do servidor sshd seja diferente de 22, a opção *-P porta* deverá ser especificada

Permitindo login sem senha na máquina remota

Primeiramente, vamos criar nossa chave privada e chave pública. Para isso, execute o seguinte comando.

```
ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
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:
a6:02:aa:d2:22:3b:8e:71:fc:99:65:eb:c6:0f:92:be root@reacted.localdomain
```

Executando o comando acima será criado o arquivo **id_rsa** que contém a chave privada e o arquivo **id_rsa.pub** que contém a chave pública.

Permitindo login sem senha na máquina remota (cont.)

O proximo passo é exportar a chave pública para o servidor

Considerando que o usuário já possua uma conta no servidor, execute o seguinte comando:

sudo scp id_rsa.pub root@192.168.0.10:/marcio

marcio@192.168.0.10's password:

Feito isto, copie o conteúdo do arquivo **id_rsa.pub** para o arquivo **authorized_keys**. Para tanto, entre dentro do diretório .ssh localizado na pasta home do usuário da máquina servidora.

cat id_rsa.pub >> authorized_keys

Agora acesse o servidor da seguinte forma: ssh usuario@numero_IP

Prof. Dr. Marcio Andrey Teixeira

marcio.andrey@ifsp.edu.br

http://marcioandrey.pro.br

Bibliografia

SILVA, G. M.. Segurança em sistemas Linux. 1. ed. Rio de Janeiro: Ciência Moderna, 2008. 240p.
THOMPSON, M. A.. Windows Server 2012: fundamentos. 1. ed. São Paulo: Érica, 2012. 232p.
VIANA, E. R. C.. Virtualização de servidores Linux para redes corporativas: guia prático. 1.
ed. Rio de Janeiro: Ciência Moderna, 2008. 342p.
6 - BIBLIOGRAFIA COMPLEMENTAR:
KUROSE, J. F.; ROSS, K. W.. Computer networking: a top-down approach. 6. ed. AddisonWesley, 2012. 864p.
SCHRODER, C.. Redes Linux: livro de receitas. 1. ed. Rio de Janeiro: Alta Books, 2006. 569p.