Atividades – Autenticação por Chaves SSH

ssh-keygen cria as chaves públicas e privadas. **ssh-copy-id** cópia a chave pública de localhost para o arquivo *authorized_keys* do remote-host. **ssh-copy-id** também atribui a devida permissão para o HOME do remote-host, ~/.ssh e ~/.ssh/authorized_keys.

1. Gerando as chaves pública e privada

Abra um terminal e execute o seguinte comando:

```
jsmith@local-host$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jsmith/.ssh/id_rsa):
[pressione enter]
Enter passphrase (empty for no passphrase): [informe a chave]
Enter same passphrase again: [informe a chave]
```

Pronto. Suas chaves foram geradas.

Para confirmar, entre no diretório **.ssh** (não esqueça do ponto) e veja seu conteúdo:

```
$ cd ~/.ssh
$ ls
id_rsa  id_rsa.pub  known_hosts
```

O arquivo **id_rsa** tem sua **chave privada** e o arquivo ***id_rsa.pub*** sua ***chave pública***.

2. Crie uma conta de usuário no servidor

Acesse o servidor que você deseja logar com chave e crie um usuário, informando a senha que desejar:

```
$ adduser joao
```

3. Colocando a chave pública no outro servidor

Copiando a chave para a sua conta:

```
jsmith@local-host$ ssh-copy-id -i ~/.ssh/id_rsa.pub -l joao <IP Servidor>
```

Pronto. Você já pode acessar sua conta usando a chave.

```
jsmith@local-host$ ssh -l joao -i ~/.ssh/id_rsa.pub <IP Servidor>
```

4. Utilizando agentes para a autenticação

```
jsmith@local-host$ ssh-agent $SHELL

jsmith@local-host$ ssh-add -L
The agent has no identities.

jsmith@local-host$ ssh-add -i /home/jsmith/.ssh/id_rsa
Identity added: /home/jsmith/.ssh/id_rsa (/home/jsmith/.ssh/id_rsa)

jsmith@local-host$ ssh-add -L
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAsJIEILxftj8aSxMa3d8t6JvM79DyBVaHrtPhTYpq
7kIEMUNzApnyxsHpH1tQ/Ow== /home/jsmith/.ssh/id_rsa
```

Agora tente autenticar novamente no servidor:

```
jsmith@local-host$ ssh -l joao <IP Servidor>
```