Caixa de ferramentas

SSH

http://www.inf.ufpr.br/marcos/caixa_de_ferramentas

Marcos Alexandre Castilho

DInf UFPR, Curitiba PR

24 de julho de 2020

SSH

- Secure Shell
- Permite a comunicação segura (criptografada) entre duas máquinas
- Essencial para quem quer se logar em outro sistema com segurança

Outros programas da família

- scp: para cópia segura de arquivos remotos
- sftp: para transferência segura de arquivos
- sshfs: para montagem remota do seu HOME (pacote sshfs)

Chaves RSA

- RSA é um protocolo de segurança baseado em uma parte pública e outra privada
- A parte pública pode ser conhecida por qualquer um
- A parte privada você deve guardar a sete chaves
- A parte privada pode ter segurança adicional pelo uso de uma passprhase

Criando um par de chaves

- No computador da sua casa, digite:
- `ssh-keygen -t rsa`

  `Enter file in which to save the key (/home/meuusuario/.ssh/id_rsa):`
- Qual local você quer guardar sua chave privada?
- Se teclar `ENTER` ela vai ficar no lugar padrão indicado na mensagem
- Se não quiser, talvez porque você já tenha uma chave lá e quer criar uma segunda, basta digitar um nome qualquer de arquivo, com caminho completo ou não
- Se não usar caminho completo vai criar no diretório corrente

Criando um par de chaves

```
Enter file in which to save the key (/home/meuusuario/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

- Uma *passphrase* é uma espécie de senha, que pode ser uma frase longa
- Exemplo: `We Will Rock You! by Queen, 1977 album News of the World.`
- É a criptografia da sua chave privada
- Se alguém roubar esta chave e não conhecer a *passphrase* você está mais seguro
- Ela pode ser vazia, mas isto não deve ser feito.
- Se quiser vazia, basta apertar `ENTER`
- O recomendado é escolher uma e digitá-la duas vezes

Criando um par de chaves

```
Your identification has been saved in /home/meuusuario/.ssh/id_rsa.
Your public key has been saved in /home/meuusuario/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:kNs5FPDUDjb9V2AarZH4Dt/iPktTaAWbuwdo6KQTL/A meuusuario@meucomputador
The key's randomart image is:
+---[RSA 2048]----+
|      ..oo .ooo. |
|       ++.+ oB. .|
|      o.o+ o+o.. |
|       = oo.++.  |
|    . o S o+=o.  |
|     o * o .++.  |
|      E o  .+..  |
|       o   .oo   |
|           .oo   |
+----[SHA256]-----+
```

- a *randomart* não serve para nada além de ser bonitinha
- SHA256 é o tipo de criptografia utilizado

Configurando suas chaves

- Seu par de chaves está agora no seu diretório
- `/home/meuusuario/.ssh`
- Foram criados dois arquivos neste diretório:
  - `id_rsa`: sua chave privada
  - `id_rsa.pub`: sua chave pública
- Guarde muito bem sua chave privada!
- Por exemplo, em um *pendrive*, ou no seu computador mesmo, mas garanta segurança dele também!

Sua chave pública tem esta cara

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKOxdpijGNfcI7hYXhn57hZnZSlHSVqQFTPMDzqJ/F
2S77rVVgwnxM0L/QJcWe1bTpd/9KllgLnId2Cpc/CWtisi4/U/pl11HKev8y/vAWz20DIgJOmh0c0HEs
OusELGmLaMRtK0AKuqUyLv9TmSowcq/4i4dzLPN7kqLSnA+6Ox0gvbHqnZFN9FqswTEKBblCvoBWNP47
FsaBwmCMbUZ1W01s0QaPtp4RBtVaxMLhexgeNv2xacxekkFIimZqIpK9A7xbBsvxrucucTOxv1W0AA3F
k6qUYxhSbAPdEtdNlmW/RePKuT1XSNmfh54glTtS+mBG4OSYNsTvGU3cDbpt meuusuario@meucomputador
```

- a parte `meuusuario@meucomputador` serve apenas para você saber onde esta chave foi gerada, na prática não serve para mais nada

Sua chave privada tem esta cara

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,E72291EFB35DCC40EFF09BFB16DBF8AD

rP1y0v/Kj9FSAvV9oCGxwCUD/xn0skyb8lzAtIThFVtAhG20YYNbzTA9YkREN/eo
iy6zXs8Vm4BPFDo1cPZ+LlfYiZMNecvIlghaE3kLJghxIAWgbKpn2W5Dm0g96E2Y
otlRd1ytjfcKAvT1TXjBacxEKy+KdmSwrcmnCqOczeLFoZ5PKFXamG/GgDPIfGyB
cp42K7svWgQmjrGb5Iw2STZ6brLmybFt7bWIBhQK2NOOsDFYNXEoPS3sf7Yvg2Na
s2y5VMd/c6/Fdrh3kF8dSMXbMT1HM2/Uqz9VWUEiy5AYbSUhpMetJhUCt5s53Sz0
crvsYwFlAHN2m34NUVpWvqAFrpQMn90ib3AaHcDPTOCXgvG6ZJ9VM29D973KMtSS
Al6SUdbKQ8v42opXzrB4x7hywTrCyylLCGjI/RGaCE/ovbaig6+QzpjePvLv2eYD
xNE2e5wGo+Q92ywM7eTQRhJ9YHmIFXtGQSgEui9DV8TuCJYhN6/47F0vsIuvJJV+
027KqmIfP97isX6PxjKCFBZVFMWhTah13BvckfvutGlT0aZIaN5dXkg57uk4cLsI
vAqBZO/MwSGjZXKZVCn1zMwrK5qXPfOfPiJNf7iNzOPBTtSFvCn9XBdX6iILrbDz
fzd0+55gI7xJl/euS2wBGN8/xy0YNV3EXXQhXih6dC57Qh+5eoN376KNxxIo86ga
6GJdd6ctIxHUAGNElX3L7nESIFTA6u0LNsboiazz0p5efOozX84KmyyoQbJj8ica
UwHTVbLDzFYhYbtWI7frsfcq9N/oeqxzTFPXfqDGZDE3srMckzGZ8E0hPf3Uut4E
AY14hlPZRhIOAEuJpygS0YwwMF6doPSiVse9V5rmfKUM0KJGBat9SJFsJnwde+oF
AjS8mz6JP09cW8W/B5d2Gr9ewZEH+o5F6KdS3gxbKzMuQuJKSOWlBd4UakebURsY
tB8ugfaatwF8iIcFQA73c7m8K6tWNprRX82VnAiVjAbxB7PgRL+uNSOmAM9fv5Wa
XypsjIn2BQZM9EdKvabd3yR3rQOZWwqm0BxmCEKOYB+w650QdWwP1K4rsVWTf6Wk
reiaLrakF9CXqvwCU/xXE6B7MWDPhFWcVRpK+XRqcIHI1lZtUX/0UORXC9fzWIg7
rJ+l3+cNKXW6o9Adwjcvcqbm9brjmLmMPx7RfqMgy0ZM1Sxxe3QoUegK+pMeymbv
61NGmV3vQY0E5pIpre8VOy1z202AyXlZzhX3itxKV6ilwxNOImZhj+tNK1iPIQXf
BfEJBRhIjYirRbbUWXCwf88ZbWVdVPvno9cwngBtkMDbV7CYpQaYrDqiAbjSr8WR
0MXHtCDtrfSykl5drA9T/DvN2nLTPjOyOPltSlvjt+QQN8V4FV1pNRnqtDAKqpMs
vuPel/F18yOwtcycajbrcYFUWgAFoLFCKbARZKxTTNfMDaGBZ53TlGhgCjokg96X
7rSPHHzNkeix0I2ohP0rHFL0pAlSPXyUJlKZRW/hsIwHqkPSAP2z932wrjAcgSvs
3vQC6DX3Vdyxumio/UHte9Ky7yLuYvpwRp4QcL9m7eK9ZxOoJJFFU5+YbAg1EW5B
-----END RSA PRIVATE KEY-----
```

Observações

- Observe a linha contendo `Proc-Type: 4,ENCRYPTED`
- Quer dizer que você criptografou com alguma *passphrase*
- Senão, sua segurança teria sido quebrada, a menos do fato de que:
- **A chave só foi mostrada porque é fictícia!**

Colocando sua chave em outro computador

- Copie sua chave na máquina de seu desejo, por exemplo, na máquina de nome `ssh` do dinf:
- `scp ~/.ssh/id_rsa.pub meuusuarionodinf@ssh.c3sl.ufpr.br:`
- Para isto será necessário digitar sua senha de forma aberta
- Ou então, copie a chave pública em um *pendrive* e traga fisicamente para o dinf se não quiser digitar sua senha aberta na Internet...

Colocando sua chave em outro computador

- Logue-se no dinf, remota ou presencialmente, digitando sua senha
- Execute este comando:
  `cat id_rsa.pub >> ~/.ssh/authorized_keys`
- Se você não tiver um diretório `.ssh` então crie um com a permissão correta (*macalan* é o nome verdadeiro da máquina cujo apelido é *ssh*):

  ```
  seuusuarionodinf@macalan:~$ mkdir ~/.ssh
  seuusuarionodinf@macalan:~$ chmod og-w ~/.ssh
  ```

- Isto é, somente você pode escrever neste diretório

Pronto!

- O arquivo `authorized_keys` pode ter várias chaves, por exemplo
- Uma do seu laptop
- Outra do seu computador desktop
- Uma outra do computador do seu trabalho
- O ideal é que você tenha então três chaves privadas com três *passphrases* diferentes...

Testando

- Agora volte para sua casa e execute
- `ssh meuusuarionodinf@ssh.c3sl.ufpr.br`
- Será pedida sua *passphase*, digite-a e você estará logado na *macalan*, vulgo *ssh* (veja no próximo slide):

Logando no DInf

- Existe uma máquina de nome ssh.c3sl.ufpr.br que permite login de casa
  - `ssh <seulogin>@ssh.c3sl.ufpr.br`
- Esta máquina dá acesso às outras máquinas do departamento, em particular a máquina `orval` (16 cores, 70Gb RAM, nobreak, gerador) ou aos terminais dos laboratórios

Logado remotamente na *macalan*!

```
Welcome to Linux Mint 18.3 Sylvia (GNU/Linux 4.19.16+ x86_64)

Welcome to Linux Mint
 * Documentation:  http://www.linuxmint.com
======================================================================

Macalan (alias ssh) tem poucos recursos de memoria e processadores,
com limites rigidos de processos, memoria e arquivos abertos.

          >>> NAO DEVE SER USADA PARA PROCESSAMENTO <<<

Esta maquina deve ser usada apenas como acesso a outras servidoras.

Use uma das maquinas abaixo para jobs:

Servidoras de uso geral, para qualquer usuario:
- orval

Servidoras exclusivas para grupos:
- fradim: exclusiva para professores
- mumm: exclusiva para C3SL
Last login: Thu Aug 15 11:34:30 2019 from 10.254.229.23
seuusuarionodinf@macalan:~$
```

Observações finais

- Agora você pode fazer *ssh* para qualquer máquina interna do DInf!
- Por exemplo, a orval tem grande capacidade de CPU e RAM, use-a bem!
- Outro exemplo: `ssh h17`: um terminal de um dos laboratórios do DInf.
- Quando quiser (e puder) pode se logar no cluster HPC (High Performance Computer), uma espécie de supercomputador do C3SL.

Exercícios

- Se você não tem ssh instalado em seu computador, instale imediatamente!
  - Nas distros variantes de Debian,
    `apt install openssh-server openssh-client sshfs`
- Crie pelo menos duas chaves, cada uma para ser usada em diferentes situações (uso normal, uso de superusuário, etc).
- Aprenda a configurar o arquivo `~/.ssh/config`
- No seu computador, verifique os arquivos `/etc/ssh/sshd_config` e `/etc/ssh/ssh_config`. Veja se sua máquina está segura contra invasores. Procure na Internet dicas de como configurar corretamente estes arquivos.
- Copie algum arquivo do DInf para sua casa usando *scp*.