Universidade da Beira Interior
Faculdade de Engenharia
Departamento de Informática

Segurança de Sistemas Informáticos
Guia para Aula Laboratorial 5
2º Ciclo em Engenharia Informática
2º Ciclo em Eng. Eletrotécnica e de Computadores
2º Ciclo em Matemática e Aplicações

Computer Systems Security
Guide for Laboratory Class 5
M.Sc. in Computer Science and Engineering
M.Sc. in Electrical and Computer Engineering
M.Sc. in Mathematics and Applications

Sumário
Instalação e utilização do *Secure Shell* (SSH).

Summary
Installation and utilization of the Secure Shell (SSH).

Pré-requisitos:
Este enunciado pressupõe o acesso a um sistema para o qual possui privilégios de instalação de *software* ou, complementarmente, no qual já tem o *Secure Shell* (SSH) –programas cliente e servidor– instalado. As tarefas abaixo contidas foram testadas no sistema operativo Fedora 13 e 15.

1 Instalação do SSH e SSHd
Instalation of SSH and SSHd

Como qualquer aplicação que implemente uma arquitetura cliente/servidor, o *Secure SHell* (SSH) é constituído por dois programas:

- o programa cliente, que normalmente é usado para ligação a um servidor noutro computador (mais ou menos) remoto;
- o programa servidor, que escuta as tentativas de ligação à porta a que está afeto e aceita as de programas compatíveis, mediando acesso às que apresentarem os requisitos certos.

Em sistemas operativos da família Unix com o SSH instalado, o cliente é invocado pela popular instrução `> ssh username@hostname`, enquanto que o *daemon* do servidor dá tipicamente pelo nome de `sshd`.

Tarefa 1 *Task 1*

Só para estimar se estamos exatamente no mesmo barco, responda à questão: **Q1.: Por quantos programas é constituída uma instalação funcional do SSH?**
☐ 1. ☒ 2. ☐ 3. ☐ 4.

Verifique se o SSH já está instalado na sua máquina. E.g., emita comandos como
`> ssh -help` e
`> sudo systemctl restart sshd`
(deve funcionar na maior porte das distribuições Linux). Caso já estejam ambos os programas instalados, os comandos anteriores devem devolver mensagens úteis acerca da sua utilização, caso contrário, darão origem a erros.

Tarefa 2 *Task 2*

Mesmo já estando instalados, pode emitir ou ao menos estudar os comandos que permitem instalar o SSH na sua máquina. Pode também começar por desinstalar os programas para repor ficheiros de configuração, etc.

No caso do **Fedora**, a desinstalação do SSH acarreta a emissão de um comando parecido com:
`> sudo dnf erase openssh`

No caso do **Ubuntu**, a desinstalação completa (incluindo ficheiros de configuração) é normalmente conseguida usando a opção `purge` do gestor de pacotes `apt-get`:
`> sudo apt-get purge openssh-client`
`> sudo apt-get purge openssh-server`

No caso do **Arch Linux**, a desinstação é conseguida via:
`> sudo pacman -Rns openssh`

A instalação segue trâmites semelhantes aos anteriores. No caso do **Fedora**, a instalação é conseguida com o seguinte comando:

```
> sudo dnf install openssh-clients
openssh-server
```

No caso do **Ubuntu**, a instalação é parecida com:

```
> sudo apt-get install openssh-client
openssh-server
```

No caso do **Arch Linux**, a instalação pode ser conseguida pela emissão do comando seguinte:

```
> sudo pacman -S openssh
```

Q2.: Por que é que esta implementação se chama `openssh`?

☒ Porque já existia outra implementação do SSH que não era gratuita nem código aberto, e que motivou o desenvolvimento desta.
☐ Porque quando se usa esta instalação, a autenticação do SSH está sempre aberta.
☐ Chama-se `OpenSSH` em analogia ao (por inspiração ao) *toolkit* de criptografia `OpenSSL`.

Q3.: Caso apenas quisesse aceder a uma máquina remota com o SSH instalado, precisava de ambos os programas (cliente+servidor) instalados?

☐ Sim, precisava.
☐ Não, só precisava do servidor.
☒ Não, só precisava do cliente.

Tarefa 3 *Task 3*

No fim da instalação, teste os comandos referentes ao cliente e ao servidor, só para se certificar de que ficaram bem instalados. Verifique também que foram criados / existem dois ficheiros de configuração distintos na diretoria `/etc/ssh/`.

Q4.: Como se chamam esses ficheiros de configuração?

☒ `ssh_config` ☐ `ssh_config_keys`
☐ `server_config` ☐ `rc.local`
☒ `sshd_config`

Nota: colocar o servidor a correr é sinónimo de ativação de um serviço em Unix ou Unix *like*. Com a adoção geral do `systemd`, o comando a emitir para conseguir essa ativação deve ser semelhante a: `> systemctl start sshd`

2 *Firewall* - Aceitar ligações SSH

Firewall - Accept SSH Connections

Não basta colocar um serviço a correr para que este funcione. Colocar o *daemon* a correr significa, neste caso, que o `sshd` vai estar à escuta na porta *Transmission Control Protocol* (TCP) 22 (por defeito), mas se tiver funcionalidades de *firewall* ativadas no sistema operativo que estiver a utilizar, as ligações podem não lhe chegar. No sistema operativo **Fedora**, o conjunto de regras definido pelo `iptables` no núcleo do sistema costuma estar ativo.

Em alguns sistemas, a *firewall* pode variar. Por isso, procure saber qual a *firewall* que está a funcionar no seu sistema e como se ativa, desativa e configura. Para efeitos desta aula, pode simplesmente desligar a *firewall* durante a elaboração do guia laboratorial, mas uma utilização capaz acarreta a configuração correta da mesma, nomeadamente através da autorização da passagem de tráfego TCP pela porta 22.

Tarefa 4 *Task 4*

Num terminal[1], mude para o utilizador `root` e verifique a cadeia de regras de `INPUT` do `iptables` usando o seguinte comando:

```
> iptables -L
```

As regras listadas pelo `iptables` são aplicadas de cima para baixo, por cada pacote *Internet Protocol* (IP) que entra na máquina. **Q5.: Sabendo isto e observando o conjunto de regras da sua máquina, acha que a sua máquina vai aceitar ligações SSH?**

☒ Sim. ☐ Não.

Nota: em caso de dúvida, discuta este assunto com o Professor.

Tarefa 5 *Task 5*

Depois de descobrir o seu IP (`> ifconfig` ou `> ip addr`), peça a um(a) colega que faça SSH para a sua máquina (e.g., `> ssh aluno@xxx.yyy.zzz.www`).

Q6.: Foi bem sucedido(a)? ☒ Sim. ☐ Não.

Caso não tenha sido bem sucedido(a), use

[1] Pressupõe-se que esta tarefa é feita num computador com sistema operativo Fedora ou com as funcionalidades de filtragem de pacotes do núcleo do Linux ativas.

as seguintes questões para fazer *troubleshooting* desta situação. **Q7.: Experimentou desativar o `iptables` (`> systemctl stop iptables` ou `> systemctl stop firewalld`)?**

☐ Sim. ☐ Não.

Q8.: Tem o *daemon* SSHd a correr na sua máquina?

☐ Sim. ☐ Não.

Tarefa 6 *Task 6*

Por via das dúvidas, vamos inserir uma regra no `iptables` que aceite ligações SSH na porta 22. **Nota:** se já lá existir uma regra para o SSH, remova-a com um comando parecido com o seguinte, antes de prosseguir:

```
> iptables -D INPUT numero_da_regra
```

Para inserir a nova regra que aceita iniciar ligações SSH para a máquina, emite-se o seguinte comando no terminal:

```
> iptables -I INPUT 3 -p tcp -m conntrack
--ctstate NEW --dport 22 -j ACCEPT
```

Se estiver com tempo, procure o significado de cada um dos parâmetros / opções no comando anterior:

`-I INPUT 3` _____

_____

`-p tcp` _____

_____

`-m conntrack -ctstate NEW` _____

_____

`-dport 22` _____

_____

`-j ACCEPT` _____

_____

Nota: pode ser necessário reiniciar o serviço do `iptables` depois de fazer alterações:

```
> sudo systemctl iptables restart
```

.

Tarefa 7 *Task 7*

Daqui a pouco pode vir a ser útil inserir uma regra que não permita ligações SSH. Experimente, por isso, inserir já a regra seguinte:

```
> iptables -I INPUT 4 -p tcp -dport 22 -j
DROP
```

Depois da inserção, verifique novamente o `iptables` com:

```
> sudo iptables -L
```

Q9.: Depois desta verificação e de tudo o que já foi dito neste guia, acha que a regra que inseriu vai ser colocada em execução ou não?

☐ Sim, vai.

☐ Não, não vai, porque está numa posição a que os pacotes SSH já não chegam, porque passam primeiro noutras regras!

Não se esqueça que, para apagar regras, basta inserir no terminal um comando parecido com:

```
> iptables -D INPUT numero_da_regra
```

Q10.: O que é que aconteceria se apagasse a regra 3[2]?

☐ As ligações à porta 22 deixavam de ser permitidas.

☐ Do ponto de vista de *firewall*, e dada a configuração atual, nada.

3 Funcionalidades Básicas do SSH

Basic SSH Functionalities

Os ficheiros `ssh_config` e `sshd_config` permitem-lhe alterar as configurações do cliente e do servidor SSH, respetivamente, de uma forma mais intuitiva. Nesta secção vão apenas explorar-se algumas funcionalidades básicas do SSH que demonstram o seu enorme potencial, e deixa-se a exploração de todas as funcionalidades ao critério do(a) aluno(a).

Tarefa 8 *Task 8*

Altere a porta TCP em que o serviço `SSHd` fica à escuta para a porta 80. **Q11.: Qual o ficheiro que precisa de abrir e alterar?**

☐ `ssh_config` ☐ `ssh_config_keys`
☐ `server_config` ☐ `rc.local`
☒ `sshd_config`

Depois de fazer as alterações que achou necessárias, não se esqueça de reiniciar o serviço, para que as configurações façam efeito.

[2] Note que se está a levar em consideração de que está a seguir o guia laboratorial com zelo e ordenadamente.

Tarefa 9 *Task 9*

Peça a um(a) colega(a) que faça a ligação à sua máquina por SSH. Desta vez, esse(a) colega vai precisar de **indicar a porta** para onde o está a fazer. **Q12.: Qual ou quais das seguintes concretizam opções válidas para o fazer?**

- ☐ Colocar `-dest 80` no final do comando SSH.
- ☒ Colocar `-p 80` no final do comando SSH.
- ☐ Colocar `:80` a seguir ao endereço IP da máquina que recebe a ligação.
- ☐ Não é necessário colocar nada.

Caso não esteja a ser bem sucedido, faça o *troubleshooting* já sugerido em cima.

Quando se liga a um computador por SSH, tem de indicar um nome de utilizador e o anfitrião. Depois, é-lhe pedida uma palavra-passe. **Q13.: Que palavra-passe é essa?**

- ☒ A palavra-passe do utilizador com que me estou a ligar na máquina destino.
- ☐ A palavra-passe do utilizador com que me estou a ligar na máquina origem.
- ☐ A palavra-passe do utilizador com que estou autenticado na máquina local.
- ☐ A palavra-passe do *root*.

Quando se liga, usa um comando parecido com `> ssh user@host`. **Q14.: O utilizador com que se está a ligar, i.e. `user`, tem de existir na máquina local ou na remota?**

☐ Só na local. ☒ Só na remota.
☐ Em ambas. ☐ Em nenhuma.

Tarefa 10 *Task 10*

Depois de estar corretamente ligado à máquina do colega, peça-lhe para guardar todo o trabalho que está a fazer e para se **afastar da máquina**! Depois, escreva o seguinte comando na máquina:

```
> shutdown -r now
```

Q15.: O que é que acabou de fazer?

- ☐ Asneiras. Muahahahahah!
- ☐ Aparentemente nada... não parece ter resultado...

Caso não queira que tal lhe seja feito a si, desligue o SSH ou coloque uma regra na *firewall* que previna isso.

Tarefa 11 *Task 11*

Faça SSH para o computador de um(a) colega. **Q16.: Depois de estar ligado a essa máquina, consegue fazer SSH para outras máquinas?**

☐ Sim, consigo. ☐ Não, não consigo.

Depois de responder à questão anterior, pense como deveria responder ao seguinte. **Q17.: Se tiver uma rede privada com vários computadores, e quiser aceder a todos eles de uma rede externa, quantas ligações SSH tem de pemitir / configurar na *gateway/firewall*?**

- ☐ Tantas ligações como computadores.
- ☒ Só uma ligação a um dos computadores. Os outros estão imediatamente acessíveis via aquele computador.
- ☐ nenhuma.

Tarefa 12 *Task 12*

Se tiver atualmente ligado via SSH, saia com o comando `> exit`. Recorde nos apontamentos teóricos o facto do SSH permitir assinaturas digitais para autenticação. O uso de criptografia de chave pública torna o SSH mais seguro e, na verdade, o processo de autenticação muito mais simples de executar, após configuração inicial. É claro que, para se usarem assinaturas digitais, é necessário criar um par de chaves. Para tal, emita o comando:

```
> ssh-keygen
```

Q18.: Em que localização é que o programa tenta guardar o par de chaves que gera por definição?

- ☒ Em `/home/username/.ssh/id_rsa`
- ☐ Em `/root/.ssh/id_rsa`
- ☐ Em `/etc/ssh/id_rsa`
- ☐ Tenta guardar logo numa localização remota. Impecável.

Q19.: O programa gerou alguma arte ASCII durante execução?

- ☐ Claro que não.
- ☒ Eishh. Pois gerou. Mas para que é que isto serve?

representação visual da chave

Experimente abrir o ficheiro que guarda as chaves, e verifique se o formato é já do seu conhecimento. **Q20.: Já agora, no contexto desta operação, é gerado mais algum ficheiro na diretoria de**

repositório de chaves, para além do `id_rsa`?

☐ Não que eu tenha notado.

☒ É gerado outro ficheiro.

id_rsa.pub

Tarefa 13 *Task 13*

Havendo criado um par de chaves, torna-se necessário instalar uma dessas chaves no(s) servidor(es) remoto(s) onde irá fazer autenticações. Complete o comando seguinte, e emita-o para proceder à instalação no servidor remoto a que se quer ligar (e.g., a do(a) seu(ua) colega):

`> ssh-copy-id` ssh-copy-id -p 80 joaom@10.0.2.15

Q21.: Que chave é instalada remotamente através da utilização do comando `> ssh-copy-id`?

☒ A chave pública do utilizador gerada no passo anterior.

☐ A chave privada do utilizador gerada no passo anterior.

☐ Ambas as chaves geradas no passo anterior.

☐ A chave pública do servidor remoto.

☐ A chave privada do servidor remoto.

Tarefa 14 *Task 14*

Depois de ter concluído o passo anterior com sucesso, experimente ligar-se ao servidor remoto onde instalou a chave novamente. **Q22.: O que tem a dizer do processo de autenticação?**

☐ Que ficou mais difícil e lento, porque é preciso fazer assinaturas digitais.

☐ Que se tornou muito mais simples e rápido, apesar de ser muito mais inseguro.

☒ Nenhuma das anteriores.

4 Funcionalidades Avançadas do SSH

Advanced SSH Functionalities

Tarefa 15 *Task 15*

Se tiver uma ligação SSH ativa, termine-a. Crie o ficheiro local `ssi.txt` com um pouco de texto como conteúdo. Depois, engendre e emita o comando que permite copiar o ficheiro para a localização remota para a qual tem estado a ligar-se. A resposta à questão seguinte pode ajudar a moldar o raciocínio: **Q23.: Qual dos seguintes comandos permite transmitir ficheiros via SSH?**

☐ `> ssh-copy-file`

☐ `> sporting-clube-portugal`

☐ `> secure-copy`

☒ `> scp`

☐ `> slb`

☐ `> ssh -c`

Guarde o comando que utilizar para a posteridade na linha seguinte:

scp -P 80 ssi.txt joaom@10.0.2.15:~

No final, não se esqueça de verificar se o ficheiro foi efetivamente transmitido para o destino.

Tarefa 16 *Task 16*

Só para cimentar este conhecimento, considere agora apagar o ficheiro `ssi.txt` localmente, e depois voltar a obtê-lo da localização remota. Escreva o comando utilizado para esse efeito na linha seguinte:

scp -P 80 joaom@10.0.2.15:~/ssi.txt .

Q24.: Seria possível copiar um ficheiro entre duas localizações remotas com uma só instrução, e usando a sua máquina como mediador?

☐ Teria sempre de utilizar dois comandos: um para copiar o ficheiro para a minha máquina, e outro para o transmitir para a máquina remota.

☐ Podia usar um só comando, mas emitido na máquina remota.

☒ Sim, seria. Curte!

Q25.: Como se copiam diretorias com o `> scp`?

☐ Não se copiam... porque não dá.

☒ Com a opção `-r`.

☐ Com a opção `-d`.

☐ Com a opção `-pasta` (ou `--spaghetti`).

Tarefa 17 *Task 17*

Se tiver alguma ligação ativa, termine-a, e volte a tentar essa ligação com a opção `-X`:

```
> ssh -X user@host -p 80
```

Q26.: Para que serve esta opção?

Serve para interfaces gráficas.

Q27.: Conseguiu fazer a ligação? ☒ Sim. ☐ Não.

Caso não tenha conseguido, peça ao(à) colega que verifique a configuração do seu servidor, nomeadamente a linha que diz: `X11Forwarding no` ou

`X11Forwarding yes`. O ideal é que este ficheiro tenha a linha

```
X11Forwarding yes
```

descomentada e com o parâmetro `yes` especificado. Caso esta alteração tenha sido feita, o servidor tem de ser reiniciado:

```
> systemctl restart sshd
```

Depois de ter conseguido a ligação com o parâmetro `-X`, emita o comando incluido em baixo e espere um pouco.

```
> nautilus &
```

Q28.: Onde é que o programa correspondente à janela que acabou de se abrir está a correr?
☒ No computador do(a) colega.
☐ No meu computador.

Q29.: Onde é que a janela do programa que acabou de executar está a ser mostrada?
☐ No computador do(a) colega.
☒ No meu computador.

No momento em que está a fazer esta tarefa, deve estar ligado ao servidor SSH do(a) colega, mas tem na sua própria máquina um servidor X que, basicamente, imprime as janelas que vê no ecrã. O que SSH está a fazer é a encaminhar o fluxo, que devia ir para o servidor X da máquina remota, para o seu próprio servidor X. A aplicação remota está a enviar informação para o seu servidor X.

Tarefa 18 *Task 18*

Esta tarefa é a que mais dificuldade coloca em termos de observação dos seus efeitos. Contudo, experimente fazer SSH com um comando parecido ao seguinte:

```
> ssh -ND 4000 user@host
```

Depois de conseguida a ligação com o comando anterior, configure o *browser* para usar um proxy na ligação à Internet. E.g., no Firefox, siga até *Edit* → *Preferences* → *General* → *Network Proxy* → *Settings* e escolha *Manual Proxy Configuration*. Depois, no *SOCKS host*, coloque *localhost* e, na porta, coloque 4000. No final, verifique se continua a conseguir aceder a páginas na Internet.

A verdade é que a partir do momento em que fez a ligação SSH com os parâmetros acima indicados e configurou o proxy, começou a aceder à Internet via máquina remota. I.e., o *browser* envia o pedido para a porta 4000 do *localhost*, que a envia via SSH para o computador a que está ligado. Esse computador faz o pedido da página, e volta a enviar a página para o seu computador. Para o resto do mundo, é como se todos os pedidos do seu *browser* viessem do computador a que está ligado.

Tarefa 19 *Task 19*

Esta tarefa é só para pensar, e vem no encaminhamento da anterior. Por favor, use o conhecimento que adquire e os recursos que lhe são disponibilizados com responsabilidade.
Considere que queria aceder a um artigo científico que estava na ACM *digital library*. Quando acede a partir da rede da universidade, o site da ACM reconhece o IP e permite descarregar os artigos em formato *Portable Document Format* (PDF). Caso contrário, só deixa descarregar se tiver uma conta paga (um *membership*) ao serviço. O problema é que está em casa a tentar fazer um trabalho, e precisa do artigo neste momento. **Q30.: Como pode resolver este problema com os recursos e conhecimentos que possui?**