Segurança Informática e nas Organizações

Guiões das Aulas Práticas

João Paulo Barraca[1] e Hélder Gomes[2]

[1]Departamento de Eletrónica, Telecomunicações e Informática
[2]Escola Superior de Tecnologia e Gestão de Águeda
Universidade de Aveiro

2015–2016

Conteúdo

2

Comunicação Segura com SSH

Resumo:

- Autenticação de utentes de SSH.
- Autenticação de servidores SSH.
- Autenticação com segredos partilhados e com pares de chaves assimétricas.
- Comunicação segura.

2.1 Introdução

Com este trabalho pretende-se estudar a configuração e exploração de sessões seguras com SSH (Secure SHell). Para esse fim deverá usar as duas máquinas virtuais com o Linux Mint que criou no primeiro guião. Use a máquina com duas interfaces (Máquina M1) para a funcionalidade de servidor e a máquina da rede interna (M2) como cliente.

Este guião está preparado para ser usado de duas maneiras. Numa delas, mais simples, o servidor SSH já está instalado e configurado. Na outra, mais completa, os alunos têm de instalar e configurar um servidor SSH que depois usarão ao longo do guião. Adicionalmente são também dadas indicações sobre a utilização de um cliente SSH em ambiente Windows.

2.2 Instalação e configuração

2.2.1 Cliente SSH

Os sistemas operativos Linux por omissão trazem já instaladas as aplicações cliente de Telnet e SSH. Por isso, em princípio não é necessário instala-los. Caso seja necessário istalar algum deles use o correspondente comando:

```
sudo apt-get install telnet
```

e/ou

```
sudo apt-get install ssh
```

Para máquinas cliente Windows, é necessário descarregar e instalar a aplicação PuTTY, que está disponível em `http://www.chiark.greenend.org.uk/~sgtatham/putty`. Esta aplicação é um cliente de Telnet e SSH.

2.2.2 Servidor SSH

Verifique que os serviços Telnet e SSH estão ativos na máquina. Para isso, verifique se os respetivos portos TCP estão disponíveis para receber ligações, utilizando o seguinte comando:

```
netstat -atn
```

Caso esteja a usar uma máquina criada com base na imagem fornecida para a disciplina, os serviços Telnet e SSH estarão já instalados e ativos. Caso não esteja, os seguintes passos permitem a instalação e configuração

inicial de um servidor SSH numa máquina Linux.

Comece por atualizar os índices de pacotes do seu sistema, usando o seguinte comando:

```
sudo apt-get update
```

Instale um servidor de Telnet (`telnetd`), usando o seguinte comando:

```
sudo apt-get install telnetd
```

Caso seja necessário reiniciar o servidor, faça-o utilizando o seguinte comando:

```
sudo /etc/init.d/openbsd-inetd restart
```

Instale um servidor de SSH utilizando o seguinte comando:

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

Inicie o servidor de SSH utilizando o seguinte comando:

```
sudo service ssh start
```

Verifique que os serviços ficaram a funcionar.

2.2.3 Configuração de Rede

Em termos de rede, apenas é necessário garantir a conectividade entre a máquina cliente e a máquina servidora, independentemente das redes em que cada um se localize.

Para melhor confinarmos este trabalho, propomos que ele seja realizado na rede virtual desenvolvida no primeiro guião e que é composta por duas máquinas virtuais interligadas por uma rede interna. A implementação desta rede passou pela criação de uma interface virtual do tipo *Internal Network* em cada uma das máquinas virtuais, interfaces estas que a nível do Linux foram configuradas como sendo de configuração manual, tendo-lhes sido atribuído endereços IP estáticos.

No entanto, ele pode ser realizado em qualquer rede, desde que exista conectividade entre a máquina cliente e a máquina servidora.

Assim, antes de prosseguir, verifique o endereço IP e o nome da interface de rede da máquina servidora, utilizando o comando:

```
ifconfig
```

e verifique ainda a conectividade da máquina cliente para a máquina servidora utilizando o comando

```
ping
```

Daqui em diante vamos assumir que o endereço IP da máquina servidora é o `10.0.0.1`.

2.2.4 Inspeção do tráfego de rede

Na máquina cliente utilize a aplicação Wireshark para monitorizar o tráfego entre o cliente e o servidor. Depois de ativar a captura de tráfego na interface usada para comunicar com o servidor, filtre o tráfego capturado para observar apenas os protocolos que lhe interessam (Telnet ou SSH), usando a seguinte regra na janela de escrita dos filtros:

```
telnet || ssh
```

Esta aplicação, configurada desta forma, irá mostrar todos os dados trocados com a máquina servidora via Telnet ou SSH.

2.3 Inspeção de tráfego Telnet

Na máquina cliente inicie e mantenha uma captura de tráfego Telnet com o Wireshark. Inicie uma sessão Telnet para a máquina servidora, faça *login* e liste o conteúdo da pasta raiz com o comando

```
ls /
```

Termine a sessão Telnet, analise os pacotes capturados no Wireshark e conclua quanto à segurança do protocolo Telnet.

Utilizando o Wireshark consegue descobrir a senha utilizada na iniciação da sessão Telnet?

O protocolo Telnet não é seguro porque é possível ver em claro toda a informação que circula. Não é possível visualizar imediatamente a password nas capturas do Wireshark, porque o protocolo Telnet envia para o servidor os dados introduzidos pelo cliente, caráter a caráter. No entanto, selecionando o comando *Follow TCP Stream* no menu *Analyze* do Wireshark é possível obter uma imagem do que aconteceu na sessão e lá a password é visível.

Na máquina cliente altere a filtragem do tráfego capturado no Wireshark para mostrar apenas tráfego SSH. Inicie agora uma sessão SSH para a máquina servidora. Caso seja a sua primeira ligação SSH ao servidor, o servidor

irá identificar-se através da sua chave pública e aparecerá uma janela a perguntar se pretende guardar essa chave; responda afirmativamente. Faça *login* e liste o conteúdo da pasta raiz com o comando

```
ls /
```

Analise os pacotes SSH capturados pelo Wireshark e conclua quanto à segurança do protocolo SSH.

Com o Wireshark não foi possível observar qualquer informação referente ao conteúdo dos pacotes que circularam, ipelo que não é possível capturar a senha usada para iniciar a sessão, pelo que o SSH garante a confidencialidade da comunicação, ao contrário do que acontece com o Telnet.

2.4 SSH com autenticação de utentes com chaves assimétricas

Na máquina cliente gere um par de chaves para utilizar na autenticação do utente cliente no acesso ao servidor SSH. Essas chaves são geradas em Linux com o comando

```
ssh-keygen -t rsa
```

Prima `Enter` para aceitar o nome por omissão para o ficheiro para guardar a chave e introduza uma password de proteção.

Em Windows estas chaves são geradas com a aplicação interativa `puTTYgen`.

É agora necessário instalar no servidor de SSH a chave pública do par de chaves que se gerou. Em Linux, para esse efeito, use o seguinte comando:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub <username>@<server>
```

no qual `~/.ssh/id_rsa.pub` é o nome do ficheiro com a chave pública criado por omissão (caso não tenha usado o nome por omissão, deve indicá-lo aqui), o nome de utilizador e o nome do servidor SSH onde se pretende instalar a chave pública. Este comando coloca o ficheiro com a chave pública do utilizador no ficheiro `~/.ssh/authorizedkeys` localizado na pasta pessoa do utilizador no servidor de SSH. Esta chave será usada para validar a autenticidade do utente quando o mesmo, para sua autenticação, usar a chave privada correspondente.

Caso o seu cliente seja uma máquina Windows, é necessário copiar a sua chave pública para o servidor SSH, por exemplo usando o programa SCP, que vem em conjunto com o PUTTY, e depois adicioná-lo ao ficheiro `~/.ssh/authorizedkeys` dentro da pasta do utilizador no servidor SSH. Para isso deve usar o comando:

```
cat ~/id_rsa.pub >> ~/.ssh/authorizedkeys
```

Caso a pasta `.ssh` e o ficheiro `authorizedkeys` ainda não existam é necessário previamente criá-los manualmente.

Na sua máquina cliente, repita a criação de um sessão SSH para a máquina servidora, usando agora o par de chaves atrás instalado para a autenticação do utilizador.

Analise as vantagens e desvantagens da autenticação por chaves assimétricas em relação à autenticação por senha partilhada (senha).

2.5 Bibliografia

`http://en.wikipedia.org/wiki/Secure_Shell`