
una
O MELHOR
CENTRO UNIVERSITÁRIO
PRIVADO DE BH
Fonte: MEC

una

O MELHOR
CENTRO UNIVERSITÁRIO
PRIVADO DE BH
Fonte: MEC

Protocolos Telnet e SSH

Professor Leonardo Larback

Protocolo Telnet

O modelo de referência TCP/IP inclui um protocolo simples de terminal remoto: Telnet. O telnet é tanto um programa quanto um protocolo, sendo que o programa utiliza o protocolo para oferecer uma interface para logins remotos.

Protocolo Telnet

O telnet funciona em um ambiente cliente/servidor, onde os toques do teclado do usuário são transmitidos diretamente ao servidor e o resultado do comando é retornado ao cliente que o solicitou.

O telnet utiliza a porta 23 e suas especificações são descritas na RFC 854 (http://www.ietf.org/rfc/rfc854.txt)

Protocolo SSH

Embora o protocolo Telnet funcione muito bem, ele não é seguro e portanto não deve ser utilizado quando segurança é um fator relevante (e quando não é?). Como alternativa ao protocolo Telnet, podemos utilizar o protocolo SSH (Secure Shell) que traz as mesmas funcionalidades do Telnet mas com um foco muito maior em segurança.

Protocolo SSH

O SSH utiliza a porta 22 e é descrito pela RFC 4251 (http://www.ietf.org/rfc/rfc4251.txt) e é descrito pela mesma como “... is a protocol for secure remote login and other secure network services over an insecure network”, ou seja, “... é um protocolo para acesso remoto seguro e outros serviços de rede seguros através de uma rede insegura” - Tradução livre.

Protocolo SSH

O SSH prevê resposta para diversos tipos de ataques conhecidos. O SSH detecta, por exemplo, casos onde o servidor tenha sido substituído por outra máquina e tentativas de se injetar dados na conexão.

A ideia central é garantir que mesmo em situações onde seja fácil interceptar a transmissão, não se tenha acesso ao conteúdo dos pacotes devido a encriptação.

Protocolo SSH

O SSH utiliza chaves assimétricas para fazer a autenticação. As chaves assimétricas são um sistema muito interessante, onde temos um par de chaves em vez de uma única chave simétrica. Uma (a chave pública), permite apenas encriptar dados, enquanto a segunda (a chave privada) permite desencriptar as informações embaralhadas pela primeira.

Protocolo SSH

Qualquer informação embaralhada usando a chave pública pode ser recuperada apenas usando a chave privada correspondente. Como o nome sugere, a chave pública pode ser distribuída livremente, pois serve apenas para gerar as mensagens encriptadas, sem permitir lê-las posteriormente.

Protocolo SSH

Quando você se conecta a um servidor SSH, seu micro e o servidor trocam suas respectivas chaves públicas, permitindo que um envie informações para o outro de forma segura. Através deste canal inicial é feita a autenticação, utilizando chaves de 512 bits ou mais (de acordo com a configuração).

Protocolo SSH

O SSH é dividido em dois módulos. O **sshd** é o módulo servidor, um serviço que fica residente na máquina que será acessada, enquanto o **ssh** é o módulo cliente, um utilitário que você utiliza para acessá-lo.

A configuração do servidor, fica no arquivo **/etc/ssh/sshd_config**, enquanto a configuração do cliente vai no **/etc/ssh/ssh_config**

Protocolo SSH

Para instalar o servidor, podemos instalar o pacote openssh-server:

 # apt-get instal openssh-server

Existem outras versões do SSH, como o **Tectia** (uma versão comercial, disponível no http://ssh.com) e o **SunSSH** que, embora conservem diferenças no funcionamento e na configuração, são compatíveis entre si. O SSH é, na verdade, um protocolo aberto e não o nome de uma solução específica.

Protocolo SSH

Ao ser ativado, o padrão do servidor SSH é permitir o acesso a qualquer usuário do sistema, pedindo apenas a senha de acesso.

Para acessar um servidor usamos:

$ ssh usuario@servidor

ou

$ ssh -l usuario servidor

Protocolo SSH

Para verificar a identidade do servidor, o SSH utiliza um sistema baseado em chaves assimétricas. O servidor possui uma chave pública que é enviada ao clienta na primeira conexão. As identificações de todos os servidores conhecidos ficam no diretório .ssh/known_hosts – dentro do diretório home.

Protocolo SSH

A partir deste ponto, toda vez que você se conecta, o cliente SSH envia um “desafio” ao servidor – Uma frase encriptada usando a chave pública (do servidor) que só pode ser entendida usando a chave privada.

Este procedimento previne um tipo comum de ataque chamado “man in the middle”

Protocolo SSH

```
xterm
kurumin@sempao:~$ ssh 192.168.1.200
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
d3:8a:48:b9:34:43:1f:e8:37:f0:c2:b2:bb:94:e1:1e.
Please contact your system administrator.
Add correct host key in /home/kurumin/.ssh/known_hosts to get rid of this message.
Offending key in /home/kurumin/.ssh/known_hosts:5
RSA host key for 192.168.1.200 has changed and you have requested strict checking.
Host key verification failed.
kurumin@sempao:~$
```

Protocolo SSH

Ao encontrar um problema com as chaves, você só poderá prosseguir com a conexão se remover a linha de identificação do servidor salva no arquivo .ssh/known_hosts

$ ssh-keygen -R servidor

Na próxima conexão, o SSH exibirá uma mensagem perguntando se você deseja adicionar a nova chave.

Protocolo SSH

A configuração do servidor é feita pelo arquivo **/etc/ssh/sshd_config** e, em geral, a primeira opção é:

Port 22 – Define a porta que será usada pelo servidor SSH. Se mudarmos a porta, na hora de conectar será necessário adicionar o parâmetro -p (ou editar o arquivo /etc/ssh/ssh_config) e informar a porta.

ssh -p PORTA usuario@servidor

Protocolo SSH

ListenAddress – Permite limitar o acesso a uma única interface de rede. Por exemplo, digamos que o endereço do servidor seja 192.168.0.1 e que não desejamos que o servidor seja acesso de fora da rede local:

ListenAddress 192.168.0.1

Protocol – Define o protocolo que será utilizado pelo servidor. A maioria dos servidores usa o SSH 2.

Protocolo SSH

PermitRootLogin - Determina se o servidor aceitará ou não que os usuários se loguem como root.

Por padrão, o SSH permite que todos os usuários do sistema se loguem remotamente, se não desejarmos isso, podemos utilizar as opções **AllowUsers** ou **DennyUsers**

Protocolo SSH

O SSH permite o uso de um par de chaves para a autenticação. A chave pública é instalada no servidor e a chave privada é protegida por uma passphrase. Assim, temos dois níveis de segurança – é preciso ter a chave privada e saber a passphrase.

Protocolo SSH

Para criar o par de chaves, usamos (no cliente):

$ ssh-keygen -t rsa

O comando gerará os arquivos **.ssh/id_rsa** e **.ssh/id_rsa.pub** dentro do seu diretório home. O **.ssh/id_rsa** é um arquivo secreto, que deve usar obrigatoriamente o modo de acesso 600 (que você define usando o chmod), para evitar que outros usuários da máquina possam lê-lo.

Depois de gerar o par de chaves,devemos instalar a chave pública no servidor, permitindo que ela seja usada para autenticação:

$ ssh-copy-id -i ~/.ssh/id_rsa.pub usuario@servidor

Protocolo SSH

Para a transferência de arquivos, o SSH oferece o SFTP – uma solução similar ao FTP. Porém, todos os arquivos transferidos pelo sftp trafegam em um túnel encriptado, criado através do SSH. Na prática, temos uma espécie de VPN temporária, criada no momento em que é efetuada a conexão.

Protocolo SSH

Para acessar o SFTP:

$ sftp usuario@servidor

A partir daí, você tem o prompt do sftp. Use o comando **put** para fazer upload de um arquivo e get para baixar um arquivo do servidor para a pasta local. Para navegar entre as pastas do servidor, use o comando **cd**. Para listar os arquivos use **ls** e **pwd** para ver em qual diretório você está.