Acesso Remoto

Introdução

Em um ambiente de rede, é sempre importante salientar o uso de ferramentas que possam facilitar procedimentos de manutenção, gerenciamento e execução de procedimentos em uma determinada máquina, sem necessariamente estar diretamente interagindo com ela. Uma das formas de se obter isso é através da possibilidade de **acessos remotos** para alguns clientes (estações) da rede nos servidores passíveis de alguma intervenção ou execução de utilitários.

Baseado nesse formato, iremos comentar sobre dois métodos de acesso remoto bastante comuns hoje em dia, o serviço do **telnet** e do **ssh**.

O acesso via telnet

O método de acesso remoto baseado no telnet é um dos mais conhecidos, pois se trata de um acesso que pode ser totalmente multiplataforma (até em roteadores podemos acessar remotamente via telnet)! Essa é a grande vantagem do telnet, que possibilita o seu uso em vários tipos de arquiteturas. A desvantagem é que o acesso telnet não é criptografado, ou seja, as informações de acesso podem ser capturadas e analisadas através de algum mecanismo de sniffer na rede.

Para o acesso via telnet, temos uma interface cliente (que seria quem solicita o login remoto) e a interface servidor (que seria o servidor que disponibiliza o acesso remoto).

Instalando os pacotes do telnet

Para acessar o telnet através do Linux, precisamos ter os seguintes pacotes instalados: o **telnet** (interface cliente) e o **telnetd** (interface servidor).

 # apt-get install telnet telnetd

 # dpkg -l | grep telnet

```
ii   telnet      0.17-18      The telnet client
ii   telnetd     0.17-18      The telnet server
```

OBS: Para que o servidor telnet disponibilize o acesso remoto, temos que habilitá-lo para ser executado através do super daemon de rede, o **inetd**, através do seu arquivo de configuração.

Configurando o inetd

O inetd utiliza para configuração um arquivo chamado **/etc/inetd.conf**. Dentro desse arquivo devemos ter uma linha relacionada com o serviço telnet, fazendo com que toda vez que o super daemon seja iniciado, o servidor telnet também já esteja disponível. No arquivo, devemos ter uma linha semelhante como abaixo:

telnet stream tcp nowait telnetd.telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd

Vamos verificar a seguir o que cada opção desta linha representa:

Configurando o inetd (cont.)

telnet – nome do servidor, assim como está no /etc/services

stream – tipo de socket de rede usado pelo protocolo; possíveis valores são: stream (geralmente quando TCP) e dgram (geralmente quando UDP), raw, rdm e seqpacket.

tcp – o protocolo utilizado (deve constar no /etc/protocols)

nowait/wait – significativo para tipos de sockets dgram; outros protocolos usam valor nowait

telnetd.telnetd – usuário e grupo que executarão o processo

/usr/sbin/tcpd – programa utilizado pelo TCPWrappers

/usr/sbin/in.telnetd – argumento do programa servidor (no caso, o executável do próprio servidor)

Executando o telnet

O serviço já está habilitado, basta agora reiniciar o daemon do inetd para que as configurações entrem em vigor:

 # /etc/init.d/inetd restart

Se o serviço subiu corretamente, podemos executar um teste:

 # adduser tux (adicionando o usuário tux)

No **cliente telnet**, podemos executar o acesso com o login:

 # telnet <ip do servidor telnet>

OBS: por padrão o telnet **não permite conexões como root**

O acesso via ssh

Um outro tipo de servidor remoto de login no Linux é o que utiliza o protocolo **SSH (Secure Shell Protocol)**, que implementa (diferente do telnet) o método de autenticação segura e criptografia dos dados, além de execução e cópias de arquivos de forma remota.

Para instalar o pacote do ssh, basta executar:

 # apt-get install ssh

OBS: o procedimento acima só é necessário se durante a instalação do sistema você optou por **não instalar o ssh**, pois por padrão ele já é instalado.

Configurando o ssh

Agora veremos detalhes do arquivo de configuração do servidor:

 # vi /etc/ssh/sshd_config

Port 22 – Porta em que o servidor atenderá as conexões
Protocol 2 – Versão do protocolo SSH (a versão 2 é a mais segura)
LoginGraceTime 600 – Timeout de conexão via SSH, se não houve sucesso no login. Esse tempo é dado em segundos
PermitRootLogin yes – Permite o login de root via SSH. Altere, por segurança, esse valor para no.
PermitEmptyPasswords no – Desabilita a autenticação de usuários sem senha
DenyUsers user1 – Negando acesso via SSH para o usuário user1 no servidor

Executando o SSH

Editado o arquivo, vamos reiniciar o daemon do SSH:

 # /etc/init.d/ssh restart

No cliente, podemos realizar a conexão através de um desses modos, utilizando um usuário válido para login no servidor:

 # ssh <ip servidor ssh>

 # ssh <usuario>@<ip servidor ssh>

 # ssh -l <usuario> <ip servidor ssh>

Trabalhando com scp

Através do servidor ssh também podemos realizar transferências (download e upload) de arquivos ou diretórios remotamente, via o comando scp. A sintaxe é essa:

 # scp tux@10.0.0.1:/tmp/teste.txt /usr/dados (fazendo o download de um arquivo para o diretório **/usr/dados** do cliente)

 # scp /tmp/arquivo.zip tux@10.0.0.1:/home/tux (fazendo o upload de um arquivo para o diretório **/home/tux** do servidor)

 # scp -r tux@10.0.0.1:/var/dir1 /usr/dados (fazendo o download de um diretório para o diretório **/usr/dados** do cliente)

 # scp -r /usr/dados tux@10.0.0.1:/tmp/ (fazendo o upload de um diretório para o diretório **/tmp** do servidor)

Referências Bibliográficas

Linux – Guia do Administrador do Sistema
Autor: Rubem E. Pereira
Editora: Novatec

Manual Completo do Linux (Guia do Administrador)
Autor: Evi Nemeth, Garth Snyder, Trent R. Hein
Editora: Pearson Books

Guia Foca GNU/Linux
http://focalinux.cipsga.org.br/