Servidor de terminal remoto

Sistemas Unix podem ser acessados via rede, oferecendo um interpretador de comandos para o usuário conectado. **Telnetd**, **rlogind** e **rshd** permitem sessões interativas, sendo ativados pelo servidor **xinetd**. Os arquivos de configuração em **/etc/xinetd.d** indicam se estes serviços estão ativos e ***/etc/hosts.allow*** e ***/etc/hosts.deny*** permitem restringir os clientes remotos que têm acesso a estes serviços.

A transmissão de dados nesses *shells*, contudo, não é encriptada.

1 SERVIDOR SSH

Secure shell (ou *shell* seguro) é um utilitário para acesso remoto com transmissão de dados de forma encriptada. O processo servidor **sshd** permite o acesso de **clientes ssh**, atendendo à configuração mantida em **/etc/ssh/sshd_config**.

- **/etc/ssh/ssh_config**: configuração do programa **cliente ssh**
- **/etc/ssh/sshd_config**: configuração do **servidor ssh**

Para a configuração do servidor, algumas opções importantes do arquivo de configuração são destacadas:

Port *n* : indica o número da porta no qual são aceitas as conexões seguras [22].
Protocol : indica a versão do protocolo aceito (1, 2 *ou* 2,1)
PermitRootLogin *yes*|*no* : indica se, em uma sessão, o usuário pode ser *root*; caso não possa, o usuário deve entrar com seu *login* normal e então usar o comando **su**.
IgnoreRhosts *yes*|*no* : permite ignorar arquivos na lista de *hosts* confiáveis (para os quais não é solicitada senha).
KeepAlive *yes*|*no* : mantém aberta uma sessão, mesmo que ociosa.
PermitEmptyPasswords *no*|*yes* : aceita ou rejeita usuários sem senha.
AllowUsers *xxx yyy* : permite acesso apenas dos usuários listados
AllowGroups *xxx yyy* : permite acesso apenas de membros dos grupos listados
DenyUsers : nega acesso dos usuários listados
DenyGroups : nega acesso dos membros dos grupos listados
X11Forwarding *yes*|*no* : habilita o encaminhamento de janelas da interface gráfica. Isto faz com que seja iniciada uma nova instância do servidor X no sistema remoto, passando a ser responsável pelo tratamento do *display* das aplicações remotas. Dados do display são encaminhados pela sessão SSL aberta.

Embora este serviço possa ser atendido pelo servidor ***inetd/xinetd***, a ativação do servidor **ssh** é normalmente feita através de um *script* próprio (***/etc/rc.d/init.d/sshd***).

Menu Principal->Configurações Sistema->Configurações de Servidor->Serviços

sshd

Ou, manualmente:

/etc/rc.d/init.d/sshd start|restart|stop: manipula o servidor SSH.

O acesso de outros computadores ao servidor SSH, contudo, requer o ajuste das polícias do *firewall* (***iptables***):

Aplicações -> Configurações do Sistema -> Nível de Segurança

Serviços de confiança: [X] SSH (22:tcp)

2 CLIENTE SSH

O acesso a um **servidor ssh** é feito com o programa **ssh**.

Ex.

ssh serv.dom.com.br // inicia uma sessão ssh com o servidor, fazendo o *login* na máquina remota com o mesmo usuário atual

ssh serv -l fulano // inicia sessão ssh com o servidor, fazendo *login* como usuário ***fulano***

ssh serv -X // inicia sessão ssh com o servidor, redirecionando o DISPLAY dos aplicativos gráficos para a máquina local

3 REDIRECIONAMENTO DO DISPLAY EM CONEXÕES REMOTAS

A variável de ambiente **$DISPLAY** define quem é o servidor responsável pelo tratamento dos eventos associados à exibição de janelas. Normalmente associada ao servidor gráfico na máquina local, pode ser redirecionada para servidores remotos.

Para tanto, o máquina destino deve anteriormente habilitar o recebimento de informações referentes ao *display* remoto. Isto é feito com o comando ***xhost***, que gerencia os nomes de **usuários** e ***hosts*** que podem realizar conexões com o servidor X local.

Ex: ***xhost + host.dom.com***

No ***Fedora Core 3***, contudo, é preciso ainda desfazer um ajuste de segurança que limita as conexões ao servidor local:

Aplicações -> Configurações do Sistema -> Tela de Login: Segurança:
[ ] Sempre desabilitar conexões TCP para o servidor X