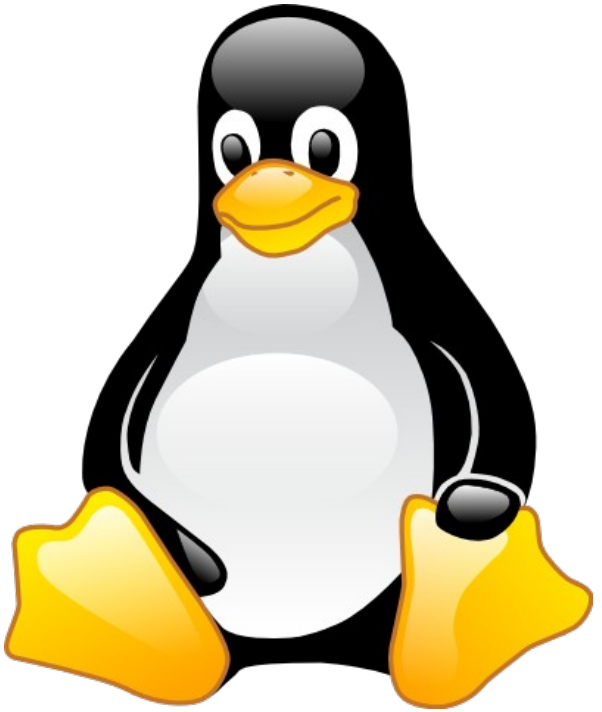
Linux System Administration 455

Aula 19 – 455



Aula 19 – 455

Os serviços de rede podem ser divididos em três tipos básicos:

[x]inetd

portmap

stand alone

Aula 19 – 455

aptitude install telnet telnetd openbsd-inetd

Aula 19 – 455

Configurando o telnet num ambiente que usa inetd:

Verifique que a linha de configuração do telnet não está comentada no arquivo de configuração do inetd, se estiver comentada, então descomente:

vi /etc/inetd.conf

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

Aula 19 – 455

Como eu faço para reiniciar o daemon do inetd?

/etc/init.d/openbsd-inetd stop
/etc/init.d/openbsd-inetd start

Vamos fazer agora uma check list para verificar se o serviço está funcionando:

netstat -anp | grep 23

tcp 0 0 0.0.0.0:23 0.0.0.0:* OUÇA 2922/inetd

Aula 19 – 455

fuser -v 23/tcp

23/tcp: root 2922 F.... inetd

Para fazer um acesso remoto em um servidor que tem o telnet habilitado é muito simples:

telnet <ip_do_servidor>

Exemplo:

telnet 192.168.0.1

É claro que você precisa ter um usuário na máquina remota. Para sair da máquina remota:

logout

Aula 19 – 455

```
# ls /etc/xinetd.d

telnetd
```

Red Hat:
/etc/xinetd.d
_ telnetd
_ cvspserver
_ samba

```
service telnet
{
        flags = REUSE
        socket_type = stream
        wait= no
        user= root
        server = /usr/sbin/in.telnetd
        log_on_failure += USERID
        disable= yes
}
```

Aula 19 – 455

Tenho duas máquinas na rede:

ServerSSH <--------------------> ClientSSH

Agora, como ocorre essa conexão a nível de TCP/IP... Quem sabe me dizer??

Qual o protocolo?

Qual a porta do cliente?

Qual a porta do servidor?

Aula 19 – 455

Protocolo: TCP

Servidor SSH: Porta 22

Cliente SSH: Qualquer porta alta

Aula 19 – 455

ServerSSH <--(Porta 22)------ ClientSSH

Toc Toc na porta 22 do Servidor!!!

Aula 19 – 455

O cliente pede a conexão para o servidor:

ServerSSH <--(Porta 22)----------(Portas Altas)--- ClientSSH

TOC TOC NA PORTA 22 DO SERVER!!!

Aula 19 – 455

ServerSSH <--(Porta 22)----------(Portas Altas)--- ClientSSH

ServerSSH--(Porta 22)----------(Portas Altas)---> ClientSSH

Aula 19 – 455

Instalando o SSH:

aptitude install ssh

Daí, já posso entrar no diretório onde ficam os arquivos de configuração.

Em qual diretório eles ficam mesmo?

cd /etc/ssh/

Aula 19 – 455

Lá terei 2 arquivos principais:

sshd_config - Arquivo de configuração do servidor

ssh_config - Arquivo de configuraçõ do cliente

Vamos editar o arquivo de configuração do servidor:

vi /etc/ssh/sshd_config

Aula 19 – 455

A primeira linha:

Port 22

Porta padrão usada pelo servidor sshd.

Aula 19 – 455

Protocol 2,1

São Protocolos aceitos pelo servidor.

Devemos sempre apenas usar o Protocolo 2

Aula 19 – 455

Próxima linha:

LoginGraceTime 120

A função dessa linha é determinar o tempo limite em segundos permitido para fazer login.

Aula 19 – 455

Próxima linha:

PermitRootLogin yes

Aula 19 – 455

Exemplo:

AllowUsers leo maria gaby

Nesse caso, apenas os usuários leo,maria e gaby conseguiriam fazer acesso remoto.

O contrário é: DenyUsers

Exemplo:

DenyUsers joao

Aula 19 – 455

PermitEmptyPasswords no

Essa linha permite ou não que o SSH aceite senhas vazias. O padrão é no. Deixe como no.

Aula 19 – 455

Próxima linha:

ListenAddress 0.0.0.0

Especifica o endereço IP das interfaces de rede que o servidor sshd servirá requisições.

Aula 19 – 455

Banner /etc/issue.net

Se você quer exibir uma mensagem antes do prompt de login, a mensagem é especificada através dessa linha.

Aula 19 – 455

Próxima linha:

X11Forwarding yes

Essa linha define se o servidor permitirá que os clientes executem aplicativos gráficos remotamente.

Aula 19 – 455

Leitura sugerida:

man sshd_config

Aula 19 – 455

/etc/init.d/ssh restart

Red Hat

service sshd restart

Aula 19 – 455

#ps aux

ou

#pgrep ssh

ou

#ps aux | grep ssh

Aula 19 – 455

Executo esse comando para isso:

netstat -anp | grep 22

tcp 0 0 0.0.0.0:22 0.0.0.0:* OUÇA 2248/sshd

Aula 19 – 455

aptitude install nmap

#nmap localhost -p 22

Starting nmap 3.75 (http://www.insecure.org/nmap/) at 2005-06-20 19:40 BRT

Interesting ports on localhost.localdomain (127.0.0.1):

PORT STATE SERVICE
22/tcp open ssh
Nmap run completed -- 1 IP address (1 host up) scanned in 0.136 seconds

Aula 19 – 455

Para fazer um acesso remoto:

ssh <nome_usuario_remoto>@<ip_do_servidor>

Exemplo:

ssh leo@201.6.255.3

Aula 19 – 455

```
# ssh leo@201.6.255.3 -p 4444
```

Aula 19 – 455

As identificações de todos os servidores conhecidos ficam armazenadas no arquivo .ssh/known_hosts dentro do diretório pessoal do cliente.

Aula 19 – 455

Para copiar arquivos de uma máquina para outra, deve-se seguir a mesma lógica do comando cp, que funciona da seguinte forma:

cp <origem> <destino>

Só que o comando de cópia no SSH chama-se scp:

scp <origem> <destino>

A diferença agora é que a origem e/ou destino podem ser remotos.

Aula 19 – 455

Da máquina local para a máquina remota (upload):

scp <arquivo_local> <nome_usuario_remoto>@<ip_do_servidor>

Da máquina remota para a máquina local(download):

scp <nome_usuario_remoto>@<ip_do_servidor>:<caminho_do_arquivo> <caminho_local>

Aula 19 – 455

Então faço assim:

#scp leo@201.6.255.3:/tmp/arquivo.txt /tmp

Aula 19 – 455

#scp -r leo@201.6.255.3:/home/leo/ /tmp

Aula 19 – 455

Mandando um arquivo da minha máquina para o servidor (upload):

$ scp -P 4444 aula1211_l1b.tar.bz2 leo@201.6.255.3:/home/netclass

Aula 19 – 455

Consiste em 2 arquivos:

- Chave privada (id_rsa);

- Chave pública (id_rsa.pub);

Aula 19 – 455

Vamos criar a chave (isso na máquina cliente):

$ ssh-keygen -t rsa

Vai ser pedido a passphrase, aí você escolhe uma.

As chaves vão ficar em:

$ cd ~/.ssh

Isso vai gerar os arquivos id_rsa e id_rsa.pub dentro do seu diretório home

Aula 19 – 455

A chave pública deve ser mandada para a máquina remota (servidor):

$ scp ~/.ssh/id_rsa.pub
seu_login@ip_do_servidor:.ssh/authorized_keys

Ou você pode fazer isso (é bem mais prático):

$ ssh-copy-id login@servidor

O ssh-copy-id copia o conteúdo do arquivo .ssh/id_rsa.pub, dentro do seu diretório home para dentro do arquivo .ssh/authorized_keys dentro do diretório home do servidor remoto.