PRÁTICA LABORATORIAL 05

Objetivos:
- Serviço de SSH

EXERCÍCIOS

SSH

O que é?

No mundo onde necessitamos a cada dia de mais mecanismos que facilitem a administração de servidores Linux, surgiu uma ferramenta para possibilitar o acesso remoto ao servidor. Essa ferramenta é o SSH (Secure SHell), permite que de qualquer lugar da rede, estando nós numa máquina com Linux ou Windows, consiga comunicar-se com o servidor a fim de realizar rotinas administrativas como se estivesse diante do próprio servidor.
Uma observação interessante é que para utilizar o Windows para administrar o Linux é necessário utilizar uma aplicação leve e gratuita chamada Putty, que deve ser instalada no Windows.
Antigamente tínhamos o telnet, ferramenta que era utilizada para administração remota e hoje temos o SSH, que é uma ferramenta muito mais segura e eficiente.

Instalar e configurar o SSH no servidor

Para instalarmos o SSH no Debian é muito simples. Basta, estando na shell como root, escrever um dos comandos:

apt install ssh

apt install openssh-server (usado em distribuições mais antigas)

E esperar que ele realize o download e instalação automática. O SSH, após instalado, gera alguns arquivos de configuração e o principal deles é o /etc/ssh/sshd_config - arquivo de configuração do servidor SSH.

Primeiro passo: vamos começar editando o principal arquivo de configuração, o sshd_config encontrado em: /etc/ssh/sshd_config. Para tal, estando na shell como root, digite:

nano /etc/ssh/sshd_config

E realize as seguintes alterações dentro do arquivo:

Em **port** coloque o padrão 22 ou uma de sua escolha. Esse campo diz ao SSH que ele estará à escuta das requisições vindas de outros computadores por esta porta ficando assim: **port 22**

Na linha **AllowUsers**, que pode existir ou não (se não existir pode criar), serve para especificar quais utilizadores pode aceder ao servidor via SSH. Caso deseje especificar apenas um utilizador para poder dar acesso ao servidor remotamente, a linha poderá ficar assim:

AllowUsers ciber

Para além da linha AllowUsers também podemos usar a linha DenyUsers para negar o acesso a um ou vários utilizadores:

DenyUsers xpto testes

Com esta linha de código os utilizadores xpto e testes não poderão fazer login remotamente usando o serviço de SSH.

Existe ainda a possibilidade de efectuar o controlo de acessos por grupos de utilizadores, devendo para isso usar os comandos **AllowGroups** e **DenyGroups**.

NOTA: Não deve utilizar em simultâneo as linhas AllowUsers e AllowGroups. Apenas deve utilizar uma de cada vez

Por defeito o utilizador root não pode aceder ao servidor, via ssh. Para tornar isso possível deve alterar a linha **PermitRootLogin prohibit-password** para **PermitRootLogin yes**

Segundo passo: agora precisamos reiniciar o serviço para que as nossas configurações entrem em vigor. Para isso, ainda estando como root, fazemos:

systemctl restart ssh

Para obter o estado do service podemos executar o comando **systemctl status ssh**

Quando obtemos o erro, a maneira mais fácil de detector um erro é usar o comando **journalctl -xe**

EXERCÍCIOS DE APLICAÇÃO

Usando o Debian Server, resolva os seguintes exercícios:

1. Crie um utilizador chamado ssh1 com a passwd cesae123

2. Use o comando apt para instalar o pacote ssh.

3. O ficheiro de configuração do servidor ssh fica instalado em /etc/ssh/sshd_config
   Faça uma cópia desse ficheiro para a pasta /etc/ssh/ com o nome sshd_config.original (Este ficheiro vai apenas servir de backup)

4. Usando o comando cat, visualize o ficheiro sshd_config. As linhas começadas pelo simbolo # são comentários, ou seja, não são interpretadas. Pode usar o comando **cat /etc/ssh/sshd_config | less** para poder usar as teclas direccionais para navegar no ficheiro. Use a tecla **q** (quit) para voltar para a sua prompt.

5. Para reiniciar o serviço do ssh (necessário após alterações do ficheiro de configuração), execute o comando **systemctl restart ssh**
   Se quiser verificar o estado do serviço ou descobrir eventuais erros, deve usar os comandos **systemctl status ssh** e **journalctl -xe** respectivamente.

6. Usando o programa putty, aceda ao servidor usando o utilizador ssh1.

7. Recorrendo a um editor de texto (nano ou vi), descomente e altere as seguintes linhas:
   a. Port 22 - Altere para Port 999;
   b. PermitRootLogin prohibit-password - Altere para PermitRootLogin **no**;

8. Tente aceder ao servidor, via ssh (putty) com o user root. O que acontece?

9. Tente agora aceder com o utilizador ssh1. O que acontece?

10. Crie um novo utilizador chamado ssh2 com a password cesae123.

11. Edite novamente o ficheiro sshd_config e adicione o seguinte código no final do ficheiro:
    ```
    # permitir os seguintes utilizadores
    AllowUsers ssh1
    ```

12. Execute novamente o código para reiniciar o serviço ssh.

13. Através do putty tente aceder com os utilizadores ssh1 e ssh2. Indique os resultados obtidos.

14. Comente a linha AllowUsers ssh1 (adicionada na questão 11) e adicione as seguintes linhas:
    ```
    # permitir os seguintes grupos
    AllowGroups ssh2
    ```

15. Repita novamente a questão 13.

16. Faça as alterações necessárias para que consiga fazer login com o utilizador root

GRUPO II

(Faça o restore ao ficheiro de configuração sshd_config de forma a utilizar o ficheiro original)

1. Crie uma pasta na raiz do disco com o nome SSH_share

2. Altere o grupo dono da pasta para sshuser (crie se não existir).

3. Altere as permissões da pasta e do seu conteúdo de modo a dar permissões para leitura ao dono do ficheiro, total permissões ao grupo dono e nenhumas aos restantes utilizadores.

4. Crie os utilizadores sshuser2, sshuser3 e sshuser4, com a password cesae123

5. Adicione os utilizadores criados na alínea anterior ao grupo sshuser.

6. Entre por ssh com o utilizador sshuser2 e crie em /SSH_share um ficheiro de texto com o nome sshuser2.dat

7. Repita a alínea anterior mas agora com o utilizador sshuser3.

8. Altere a porta para 997.

9. Faça as alterações necessárias para que o root possa aceder diretamente via ssh.

10. Altere o ficheiro de configuração de modo a permitir apenas o acesso via ssh a todos os utilizadores do grupo cesae (deve criar o grupo cesae para testar).

11. Peça ao seu colega do lado para criar um login para si na máquina Linux e aceda ao sistema dele através do serviço de ssh.

12. É possível fazer ligação por ssh a outro servidor Linux através da shell. Para isso é usado o comando “ssh”. Sabendo o nome do comando tente ligar a outro servidor Linux.
    Exemplo : ssh pedro@192.168.0.30 –p 999

13. Em linux podemos copiar ficheiros de um servidor para o outro através da linha de comando e de uma forma segura (encriptada), o comando usado é o “scp”. Tente copiar um ficheiro de texto, com o seu nome, e colocá-lo no seu servidor linux secundário.
    Exemplo : scp –P 999 /ssh_share/teste.txt pedro@192.168.0.30:/home/pedro

14. Criar um ficheiro com o seu nome na sua máquina Linux secundária. De seguida usando o comando scp na sua máquina primária, copie o ficheiro criado para a sua máquina, para a raiz do sistema.

Bom trabalho!