INSTALAÇÃO E CONFIGURAÇÃO DOS SERVIÇOS DE REDE: TELNET, SSH e SUDO

Administração de Sistemas Operacionais de Rede
FATEC OURINHOS
Profº Paulo R. Galego H. Jr.
Última atualização: 23/02/2021

OBJETIVO

Este documento apresenta um breve resumo das informações discutidas em sala de aula na disciplina de Administração de Sistemas Operacionais de Redes, alunos do 3º ciclo do curso de Tecnologia em Segurança da Informação da FATEC Ourinhos.

Mesmo sendo este documento consistido de material que será utilizado durante o curso, ele deverá ser utilizado apenas como material de consulta prática, ficando o aluno ciente que as fontes de informação corretas cobradas posteriormente em avaliação são as apresentadas na ementa da disciplina.

1 – SISTEMA OPERACIONAL

1.1 – Por que Debian?

- Por ser o Debian um SO amplamente utilizado por profissionais do mundo “open”;
- Possui uma comunidade de desenvolvedores que garantem sua evolução e estabilidade;
- Dividido em categorias, como estável, desenvolvimento e teste, permitindo que o utilizador possa escolher a melhor opção para sua necessidade de implantação;
- Fácil administração, utilizando o aplicativo APT, que é responsável pelos processos de instalação, desinstalação, upgrade de versões, entre outras funcionalidades junto aos serviços e do próprio SO.

2 – INSTALAÇÃO E CONFIGURAÇÃO DO SERVIÇO “TELNET”

TELNET (TELecommunication NETwork)

O telnet é um serviço de acesso remoto em máquinas ou servidores através de terminal texto. Utilizado para administrar ambientes remotos, tem como característica principal a ausência de criptografia na transmissão dos dados entre as duas pontas da comunicação. Para instalar o serviço telnet em seu servidor Debian basta executar o comando abaixo:

apt-get install telnetd

mas ***atenção***, antes de instalá-lo é interessante observarmos o /etc/inetd.conf. Com um cat neste arquivo podemos observar seu conteúdo. Segue abaixo:

```
# /etc/inetd.conf:  see inetd(8) for further informations.
#
# Internet superserver configuration database
#
# Lines starting with "#:LABEL:" or "#<off>#" should not
# be changed unless you know what you are doing!
#
# If you want to disable an entry so it isn't touched during
# package updates just comment it out with a single '#' character.
#
# Packages should modify this file by using update-inetd(8)
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
#:INTERNAL: Internal services
#discard         stream  tcp     nowait  root    internal
#discard         dgram   udp     wait    root    internal
#daytime         stream  tcp     nowait  root    internal
#time            stream  tcp     nowait  root    internal

#:BSD: Shell, login, exec and talk are BSD protocols.
```

```
#:MAIL: Mail, news and uucp services.

#:INFO: Info services

#:BOOT: TFTP service is provided primarily for booting.  Most sites
#       run this only on machines acting as "boot servers."

#:RPC: RPC based services

#:HAM-RADIO: amateur-radio services

#:OTHER: Other services
```

após instalar o serviço, podemos observar as modificações realizadas no /etc/inetd.conf da seguinte forma. Segue:

```
# /etc/inetd.conf:  see inetd(8) for further informations.
#
# Internet superserver configuration database
#
#
# Lines starting with "#:LABEL:" or "#<off>#" should not
# be changed unless you know what you are doing!
#
# If you want to disable an entry so it isn't touched during
# package updates just comment it out with a single '#' character.
#
# Packages should modify this file by using update-inetd(8)
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
#:INTERNAL: Internal services
#discard         stream  tcp     nowait  root    internal
#discard         dgram   udp     wait    root    internal
#daytime         stream  tcp     nowait  root    internal
#time            stream  tcp     nowait  root    internal
```

#:STANDARD: These are standard services.
telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd

```
#:BSD: Shell, login, exec and talk are BSD protocols.

#:MAIL: Mail, news and uucp services.

#:INFO: Info services

#:BOOT: TFTP service is provided primarily for booting.  Most sites
#       run this only on machines acting as "boot servers."

#:RPC: RPC based services

#:HAM-RADIO: amateur-radio services

#:OTHER: Other services
```

agora basta realizar o restart do inetd para que o novo serviço de telnet passe a funcionar. Para isso, digite a sequência de comandos abaixo:

/etc/init.d/openbsd-inetd restart e verifique se o serviço está no ar com o comando:

debian-asor:/etc# netstat -a | grep telnet
tcp 0 0 *:telnet *:* OUÇA
debian-asor:/etc#

Após estes comandos podemos testar o serviço fazendo um telnet na própria máquina. Observe que ainda não é possível realizar o login com o usuário root, caso isso for necessário (mesmo sendo totalmente contra as boas práticas de segurança), devemos editar o arquivo **/etc/securetty** e incluir alguns **pts** para acesso ao root. Segue exemplo:
pts/0

pts/1
pts/2

estes comandos permitem o usuário abrir até 3 conexões remotas e simultâneas na máquina com o usuário root.

OBS: O serviço TELNET deve ser utilizado apenas em último caso em servidores e máquinas finais. Sua segurança é pequena devido ao fato de não haver criptografia entre as pontas deste protocolo, facilitando um usuário mal intencionado a capturar as informações de login. É altamente recomendado a utilização do servidor SSH para acessos remotos.

3 – INSTALAÇÃO E CONFIGURAÇÃO DO SERVIÇO "SSH"

SSH (Secure Shell)

O SSH tem a mesma funcionalidade do TELNET, acesso remoto através de interface texto. A maior diferença entre esses dois serviços é que o SSH provê a comunicação através de um canal criptografado, o que dá mais segurança aos acessos remotos.
Para instalar o servidor SSH em uma máquina com Debian deve-se seguir os passos abaixo:

apt-get install ssh

Após a instalação do serviço podemos encontrar seus arquivos de configuração no diretório **/etc/ssh** e o arquivo de configuração dos parâmetros do SSH é o **sshd_config**. Uma configuração padrão que devemos mudar é a possibilidade do usuário root do sistema realizar o login através do SSH. Este tipo de acesso não é interessante, já que o root tem controle total do sistema. Abaixo segue o parâmetro que deve ser modificado no **/etc/ssh/sshd_config** para que o root não possa mais fazer acesso direto via SSH.

PermitRootLogin no

Outras configurações de segurança no SSH podem ser obtidas em http://www.debian.org/doc/manuals/securing-debian-howto/ch-sec-services.pt-br.html#s5.1

OBS: Mesmo sendo utilizado o Debian como sistema base para nossos laboratórios, muitas das definições de segurança encontradas neste material podem ser utilizadas para muitas ou até todas distribuições Linux/Unix.

4- ALGUNS COMANDOS QUE SERÃO ÚTEIS

useradd: O comando useradd é usado para adicionar um usuário ao Linux. No Debian precisamos especificar alguns parâmetros:
-m Cria a pasta home do usuário
-d Especifica qual a pasta home do usuário. Caso não seja especificada uma pasta, será usada a pasta /home/
-s Especifica qual será o interpretador de SHELL do usuário. Se não for especificado um SHELL será usado o sh
Exemplo de criação do usuário paulo:
useradd -m -s /bin/bash paulo

passwd: Altera a senha de um usuário (precisa ser o root). Se não for especificado um usuário, será alterada a senha do usuário atual.
Exemplo para alterar a senha do usuário paulo:
passwd paulo

who ou w: Mostra quais usuários estão logados no Linux neste momento

which: Busca por executáveis (binários) associados ao comando nos PATHs atuais

PATH: É uma lista de diretórios em que o sistema procura os comandos que podem ser executados, sem que o usuário preciso digitar sempre o caminha completo de um comando.
Por exemplo ao invés de termos que trocar a senha de um usuário digitando:
/usr/bin/passwd paulo

Podemos apenas digitar:
passwd paulo

Para saber os diretórios do seu PATH, exiba o conteúdo da variável $PATH:
echo $PATH

date: O comando date pode além de exibir a data e hora atuais do sistema, alterar a data e a hora.
Exemplo: Para alterar a hora para 9h00min o comando seria:
date -s 0900

5 – INSTALAÇÃO E CONFIGURAÇÃO DO SERVIÇO “sudo”

Sudo (Substitute User DO)

O sudo é um serviço que possibilita um usuário sem privilégios administrativos executar comandos como um usuário administrador. Esta utilização é muito comum e importante em ambientes de administração de servidores onde não é permitido a conexão do usuário root através de SSH, por exemplo.

Para instalação do sudo siga os passos abaixo:

apt-get install sudo

Após a instalação do sudo, todas configurações de acesso de máquinas, usuários e recursos disponibilizados podem ser configurados através do arquivo **/etc/sudoers**. Abaixo segue um exemplo deste arquivo em seu formato original:

```
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset

# Host alias specification
```

```
# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
%sudo ALL=(ALL) NOPASSWD: ALL
```

Originalmente apenas o root pode utilizar o sudo, sendo assim, caso outro usuário tentar desligar a máquina, por exemplo, mesmo utilizando o sudo, ocorrerá o erro abaixo:

```
paulo@debian-asor:~$ sudo shutdown -h now

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for paulo:
paulo is not in the sudoers file.  This incident will be reported.
paulo@debian-asor:~$
```

Para a configuração do Sudo, **DEVE** ser usado o utilitário **visudo**, que é um utilitário que faz a análise sintática e semântica do arquivo sudoers assim que o arquivo é salvo, e informa se há algum erro neste arquivo. Pelo visudo é usado o editor de textos padrão do seu Linux. O autor desta apostila recomenda fortemente que seja desinstalado o editor nano, e seja usado apenas o vi para a edição do sudoers.

Para abrir o visudo deve-se digitar na linha de comando: **visudo**

A sintaxe para a configuração de um comando no sudo é a seguinte:

Usuário HOST=/caminho/do/comando parâmetros

Usuário: Nome do usuário que poderá executar o comando como root;
HOST: Nome da máquina que será rodado o comando. Pode-se usar ALL ou localhost
caminho/do/comando: Caminho completo do comando que será executado. Por exemplo /bin/date ou /sbin/ifconfig. Pode-se usar ALL para todos os comandos. Usa-se o comando which para saber este caminho. Ex: which date
parâmetros: Os parâmetros do comando que será executado. Se não forem especificados os parâmetros, o usuário poderá não conseguir executar corretamente os comandos.

OBS: O operador ' ! ' em todos os casos é utilizado para negar o item que o segue.

NOPASSWD and PASSWD

Por padrão o sudo requisita a autenticação do usuário ao tentar executar algum comando. Esta necessidade pode ser retirada com o comando **NOPASSWD**.

Abaixo segue uma configuração básica do sudoers para que o usuário “paulo” possa desligar a máquina a partir de uma conexão originada de qualquer máquina. Segue:

OBS: o arquivo /etc/sudoers deve ser editado com o utilitário ' visudo '.

```
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
paulo   ALL=/sbin/shutdown -h now
root    ALL=(ALL) ALL

# Allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
%sudo ALL=(ALL) NOPASSWD: ALL
```

O comando em negrito acima permite o usuáro paulo executar o comando shutdown com os parâmetros ' -h now ' de qualquer máquina.

Para que o usuário paulo possa executar o comando date -s e alterar a data/hora do sistema, sem que seja pedida a senha, faremos o seguinte:

paulo ALL=NOPASSWD:/bin/date -s *

para que peça a senha dos usuários que estão digitando o comando:
paulo ALL=/bin/date -s *

Lembrando que o * é para que possa ser usado qualquer argumento após o -s.
Para testarmos, é só fazer o login com o usuário paulo, e digitar no prompt:

sudo date -s 0900

Este comando vai alterar a hora do sistema para 09:00h.

Maiores informações em: http://www.sudo.ws/sudo/man/sudoers.html