Preparação de segurança

TCP Wrapper

www.4linux.com.br

Sumário

Índice de tabelas

Índice de Figuras

Capítulo 1

Preparação de segurança

- Usando o TCP Wrapper.

1.1. Mãos a obra

Através do do TCP Wrapper o administrador configura um controle de acesso, permitindo ou não a uma rede e/ou domínio, acesso aos serviços, tudo feito a nível de aplicação. Os TCP Wrappers foram devolvidos quando não existiam filtros de pacotes disponíveis.

Como configurar um serviço com TCP Wrapper?

Um serviço tem suporte ao TCP Wrapper devido a bibloteca libwrap.so.0. Muito desses serviços instalados no sistema, são executados de duas formas:

1 - Carregados através do serviço tcpwrappers (tcpd). Exemplos:

finger, swat, telnet, ftp entre outros.

2 - Compilados com o suporte a libwrapper embutido. Exemplos:

portmap, gdm, ssh in.talk, rpc.statd entre outros.

Vamos verificar a biblioteca em serviços tcpwrappers(tcp)

 # ldd /usr/sbin/tcpd | grep libwrap

```
        libwrap.so.0 => /lib/libwrap.so.0 (0xb7f84000)
```

Neste exemplo podemos classificar o telnet, pois no arquivo de configuração do inetd, o /usr/sbin/tcpd é executado primeiro.

 # grep telnet /etc/inetd.conf

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

Vamos verificar a biblioteca em serviços com o suporte libwrapper embutido

 # ldd $(which sshd) | grep libwrap

```
        libwrap.so.0 => /lib/libwrap.so.0 (0xb7f01000)
```

O exemplo acima é o serviço SSH compilado com TCP Wrapper.

Configurando ...

A configuração de regras de acesso é feita por dois arquivos, o hosts.allow para liberar e hosts.deny para bloquear.

Na prova de certificação é questionado sobre a mesma regra presente nos dois arquivos. A resposta da questão é que ira valer a regra do arquivo hosts.allow, pois este é o primeiro a ser lido

A sintaxe dos arquivos hosts.allow e hosts.deny é seguinte:

serviço:host:comando

Exemplo:

 # vim /etc/hosts.deny

```
sshd: ALL EXCEPT 192.168.200.0/24
```

No exemplo acima o serviço SSH será bloqueado a qualquer maquina, exceto da rede 192.168.200.0.

Para testar a sintaxe dos arquivos hosts.allow e hosts.deny use o comando tcpdchk -v

```
Using network configuration file: /etc/inetd.conf

>>> Rule /etc/hosts.deny line 21:
daemons:  sshd
clients:  ALL EXCEPT 192.168.200.0/24
access:   denied
```

Capítulo 2

Gerenciando

2.1. Objetivos

•Trobleshooting: Enviar mensagem quando um serviço negado tiver acesso

2.1. Troubleshooting

Como posso enviar um email ao Administrador do sistema, assim que for tentado um acesso a um serviço negado?

Isso é possível configurando o comando SPAWN no arquivo /etc/hosts.deny. Vamos a prática:

Abra o arquivo hosts.deny e inclua a seguinte configuração

```
# vim /etc/hosts.deny
```

```
ALL: ALL: SPAWN ( \
echo -e "\n\
TCP Wrappers\: Connection refused\n\
By\: $(uname -n)\n\
Process\: %d (pid %p)\n\
User\: %u\n\
Host\: %c\n\
Date\: $(date)\n\
" | /usr/bin/mail -s "Conexão bloqueada para %d" root) &
```

Para o root receber emails abra o arquivo /etc/aliases e configure root:root e restarte o Exim4.

 # vim /etc/aliases

```
# /etc/aliases
mailer-daemon: postmaster
postmaster: root
nobody: root
hostmaster: root
usenet: root
news: root
webmaster: root
www: root
ftp: root
abuse: root
noc: root
security: root
root: root
```

Testando ...

Faça uma conexão de outro computador via SSH, em seu servidor. Para visualizar o acesso recusado use o comando tail no arquivo /var/mail/mail.

 # tail /var/mail/mail

```
TCP Wrappers: Connection refused
By: server
Process: sshd (pid 2728)
User: unknown
Host: 192.168.200.254
Date: Mon Jan 31 17:38:58 BRST 2011
```