División de Seguridad Informática

Configuración de TCP-Wrapper

1.- Introducción.

Linux, igual que cualquier sistema operativo, debe ser configurado para que sea seguro antes de conectarlo a una red, especialmente cuando nos conectamos a Internet.

Como un intruso puede atacarnos e ingresar a nuestra computadora?
Linux o cualquier otro Unix, ejecutan un conjunto de programas denominados daemons, que proveen servicios de red, como por ejemplo servidores: ftp, smtp, telnet, etc. Estos pueden tener problemas de seguridad, que son utilizados por el intruso para ganar acceso a nuestra computadora.

Normalmente, luego de finalizar la instalación de Linux, existen varios servicios de red ejecutándose que no son necesarios, debemos saber que servicios son, deshabilitar todos aquellos que no sean necesarios y configurar de forma segura los servicios que utilizaremos.

2.- El súper server o inetd.

Muchas veces necesitamos que una misma computadora brinde varios servicios de red, por lo tanto deberíamos tener en el sistema varios daemons ejecutándose simultáneamente. Esto nos podría producir una sobrecarga en nuestra computadora.

Para reducir la carga en el sistema, existe un "súper server" inetd, el cual se queda en espera por varios servicios de red, cuando un cliente quiere utilizar un servicio, ejecuta el servidor correspondiente y le da el control de la conexión, de esta manera solo tenemos un solo daemon ejecutándose y reducimos la carga del sistema.

Los pasos que realiza el inetd son los siguientes:

- Al ejecutarse en el arranque de la PC o cuando lo reincidamos, lee su archivo de configuración, /etc/inetd.conf , el cual le indica que servicios debe atender y que servidor ejecutar en caso de que se produzca un intento de uso de dicho servicio.

- Queda en espera hasta que intenten conectarse.

- Cuando intentan utilizar un servicio, ejecuta el servidor correspondiente (indicado en el inetd.conf) y le entrega el control de la conexión.

- Vuelve a su estado de espera.

3.- El inetd.conf.

El archivo de configuración del inetd (/etc/inetd.conf) esta compuesto por líneas, donde en cada una se indica el nombre del servicio que atenderá y su programa a ejecutar. Las líneas que comienzan con un '#' son ignoradas (están comentadas).

Veamos brevemente cada campo de una linea de este archivo:

- Nombre del servicio, (ftp, telnet, etc)
- Tipo de socket. (stream, dgram, etc)
- Protocolo. (tcp, udp)
- wait/nowait
- usuario con el que se ejecutara el servicio. (root, nobody, etc)
- programa que brindara el servicio. (/usr/sbin/tcpd /usr/sbin/in.telnetd)

Ejemplo:

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

Importante: observar que el ultimo campo (programa que brindara el servicio) es siempre: /usr/sbin/tcpd y el path del programa correspondiente al servicio, esto se explicara mas adelante.

Veamos un fragmento del archivo inetd.conf :

```
---------------------------------------------------------
#:STANDARD: These are standard services.
ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
telnet          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd

#:BSD: Shell, login, exec and talk are BSD protocols.
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd

#:INFO: Info services
finger          stream  tcp     nowait  nobody  /usr/sbin/tcpd  /usr/sbin/in.fingerd
ident           stream  tcp     nowait  nobody  /usr/sbin/identd        identd -i

#:BOOT: Tftp service is provided primarily for booting.  Most sites
# run this only on machines acting as "boot servers."
#tftp           dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd /boot
#bootps         dgram   udp     wait    root    /usr/sbin/bootpd        bootpd -i -t 120
---------------------------------------------------------
```

Los servicios habilitados son: ftp, telnet, shell, login, exec, finger, ident.
Y los deshabilitados (comentados con un '#' en el inicio) son: tftp y bootps.
También se observan líneas de comentarios, como :
#:INFO: Info services

Se ve que hay demasiados servicios habilitados en el ejemplo anterior.

Veamos brevemente la función de algunos de los servicios que maneja el inetd:

Servicios internos.

echo:	Realiza un eco en la conexión, ósea todo lo que enviamos lo recibimos.
chargen:	Generador de caracteres, nos envía constantemente caracteres.
discard:	Descarta, ósea no hace nada con lo que recibe y tampoco envía nada.
daytime	Nos envía la fecha en formato legible por nosotros, por ejemplo: Wed Jun 14 10:32:20 2000.
time	Nos envía la fecha en un formato ilegible para nosotros, pero si legible para otra computadora, es el numero de segundos transcurridos desde el primero de enero de 1900.
	Nota: los cinco servicios anteriores se denominan internos, porque son atendidos por el mismo inetd, pueden ser todos desabilitados en la mayoría de los casos.

Servicios estandart.

ftp:	Se utiliza para realizar a través de la red transferencias de archivos, con autentificacion mediante usuario y contraseña.
telnet:	Se utiliza para obtener sesión remota, ósea una consola remota, con autentificacion mediante usuario y contraseña.

Protocolos BSD.

shell:	Provee ejecución remota de comandos, con autentificacion basada en puertos privilegiados y hosts de confianza (trust).
login:	Provee una sesión remota, con autentificacion basada en puertos privilegiados y hosts de confianza.
exec:	Provee ejecución remota de comandos, con autentificacion basada en usuario y contraseña.
talk:	Los dos siguientes se utilizan para conversar con otro usuario.
ntalk:	

Servicios de información.

finger:	Server que provee información remota, retorna un reporte de estado del sistema o de un usuario en particular.
ident:	Escucha en determinados ports TCP y retorna el usuario que realiza la conexión.
tftp	Ambos se utilizan normalmente como servidores de booteo, para PCs sin disco riguido.
bootps	

Supongamos que queremos deshabilitar los siguientes servicios: shell, login, exec, finger y ident, en el ejemplo anterior, el archivo inetd.conf nos quedara así:

```
---------------------------------------------------------------
#:STANDARD: These are standard services.
ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
telnet          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd

#:BSD: Shell, login, exec and talk are BSD protocols.
#shell          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
#login          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
#exec           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd

#:MAIL: Mail, news and uucp services.

#:INFO: Info services
#finger         stream  tcp     nowait  nobody  /usr/sbin/tcpd  /usr/sbin/in.fingerd
#ident          stream  tcp     nowait  nobody  /usr/sbin/identd        identd -i

#:BOOT: Tftp service is provided primarily for booting.  Most sites
# run this only on machines acting as "boot servers."
#tftp           dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd /boot
#bootps         dgram   udp     wait    root        /usr/sbin/bootpd        bootpd -i -t 120
---------------------------------------------------------------
```

ftp y telnet quedan habilitados para su uso.

Para que los cambios tengan efecto debemos reiniciar el inetd, para que vuelva a leer su archivo de configuración. Esto lo podemos realizar de la siguiente manera:

1- Hallamos el PID del inetd, con el siguiente comando:

```
# ps aux | grep inetd
root        97  0.0  1.7  1292   536  ?  S    10:54   0:00 inetd
```

El PID corresponde a la segunda columna, en este ejemplo es 97.
2- luego reiniciamos el inetd con el siguiente comando (con el usuario root):

```
# kill -HUP 97
```

Los servicios que normalmente se utilizan son : telnet, ftp, smtp.
Servicios que es recomendable deshabilitarlos (comentarlos): shell, login, exec, finger, ident, tftp, bootps.

Ya hemos deshabilitado los servicios que no vamos a utilizar, ahora debemos configurar de forma segura los que utilizaremos

4.- El tcpd.

Aquí se entenderá porque el ultimo campo del archivo inetd.conf es siempre /usr/sbin/tcpd seguido por el path del servidor.
La operación del inetd con el tcpd en conjunto, es la siguiente:

- Cuando inetd recibe un pedido por un servicio, en vez de ejecutar el programa servidor correspondiente, ejecuta el tcpd y le pasa como parámetro el nombre del servidor correspondiente.

- El tcpd decide si permite el acceso o no al servicio, dependiendo de unas reglas de acceso y la dirección del cliente que lo solicita. Dichas reglas se encuentran en los archivos hosts.allow y hosts.deny en el directorio /etc.

- Si las reglas de acceso dicen que la computadora que solicito el servicio no tiene acceso a el, rechaza la conexión. Si tiene acceso al servicio, el tcpd ejecuta el programa que brinda el servicio correspondiente y le entrega el control de la conexión.

- Por ultimo el programa servidor puede pedir usuario y contraseña para autentificar.

Se ve que el tcpd agrega un nivel mas de seguridad mediante reglas de acceso, es intermediario entre el súper server (inetd) y el servidor correspondiente.

5.- hosts.allow y hosts.deny.

El archivo hosts.allow, indicara las direcciones de las PCs o hosts que pueden acceder a un determinado servicio y hosts.deny indicara las direcciones a las que se les niega el acceso a determinados servicios de red.

En cada linea de estos archivos se indica el nombre del o los programas servidores y la dirección o nombre de uno o varios hosts.

Por ejemplo:
in.ftpd : 150.185.1.2
Si esto se encuentra en el archivo hosts.allow, le dice al tcpd que el host 150.185.1.2 puede acceder al servidor ftp.
Si estaría lo mismo en el archivo hosts.deny significa que le va a negar el acceso.

Veamos mas en detalle cada linea de estos archivos, están formadas de la siguiente manera :

daemon_list : client_list

> **daemon_list:** Lista de uno o mas nombres de procesos (daemons) sobre los cuales se aplica el acceso o no, dependiendo si esta en hosts.allow o hosts.deny. También puede ser la palabra ALL, que significa todos los procesos

Ejemplos:

in.ftpd in.telnetd
ALL

> **client_list:** Lista de uno a mas direcciones o nombres de hosts sobre los cuales se aplica el acceso o no, dependiendo si se encuentra en hosts.allow o hosts.deny. También puede ser la palabra ALL, que significa todos los hosts.

client_list puede tener alguna de las siguientes formas:

1-Una palabra que comienza con un '.' (punto).
Todos los nombres de hosts que finalicen con ella, se les dejara acceder o no, dependiendo si esta en hosts.allow o hosts.deny respectivamente .

Ejemplo .ing.ula.ve

mail.ing.ula.ve
ns1.ing.ula.ve
hosts12323.ing.ula.ve
rdu1256.ing.ula.ve
Todos estos cumplen con .ing.ula.ve

2- Una palabra que finaliza con un '.' (punto).
Todas las direcciones IP que comiencen con dicha palabra, se les dejara acceder o no.

Ejemplo: 150.185.1.
Regla valida para todas las IPs desde 150.185.1.0 hasta 150.185.1.255

3- Una expresión de la forma: n.n.n.n/m.m.m.m
Donde n.n.n.n es la dirección de red y m.m.m.m es la mascara de red.

Ejemplo:
150.185.1.1/255.255.255.0
A todas las IPs desde 150.185.1.0 hasta 150.185.1.255 se les dejara acceder o no.

Los elementos que forman cada lista deben estar separados por espacios en blanco y/o comas.

Veamos los pasos que realiza el tcpd con los archivos hosts.allow y hosts.deny:

1- Lee el archivo hosts.allow y verifica si la dirección o nombre del host que trata de conectarse, tiene acceso al servicio. Si es así, ejecuta el servicio correspondiente y le da el control de la conexión, **no lee el archivo hosts.deny.**

2- Si en el paso anterior, no encontró el host, lee el archivo hosts.deny y busca la dirección o nombre del host. Si lo encuentra, rechaza la conexión.

3- Si en ninguno de los dos archivos encontró el nombre o dirección de host, le permite el acceso. Estos nos dice que nos conviene **negar el acceso a todo en el hosts.deny y dar acceso a lo que necesitamos en el hosts.allow**

6.- Ejemplos.

Ejemplo 1:

Este ejemplo no tiene utilidad practica, pero sirve para aclarar conceptos.

1- Editamos el inetd.conf y habilitamos el telnet.

2- Reiniciamos el inetd, como se indico mas arriba.

3- Utilizamos la interfaz loopback para hacer algunas pruebas.
Para los que no estén enterados, esta interfaz es virtual, todo lo que enviamos por el loopback nos vuelve, en nuestro caso la utilizaremos para hacer pruebas como si estuviéramos en una red.
Toda la red 127.x.x.x es el loopback, usamos la IP 127.0.0.1

Verificamos que en los archivos hosts.allow y hosts.deny no haya ninguna regla (todo comentado, ósea poner '#' al principio de las líneas).

4- Nos hacemos telnet a nosotros mismo:

```
ariel:~# telnet 127.0.0.1
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.


ariel login:
```

Vemos que el tcpd nos dejo acceder, al servidor de telnet.

5- Editamos el hosts.deny y agregamos:
ALL : ALL

Con eso negamos el acceso a todo.
Hacemos telnet otra vez:

```
ariel:/etc# telnet 127.0.0.1
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Connection closed by foreign host.
```

Nos negó el acceso, funciona !

Ejemplo 2:

Continuamos configurando.
Supongamos que nuestra PC se conecta a Internet y también tiene una placa ethernet para conectarse a una red interna, con dirección 150.185.1.0 y mascara 255.255.255.0
Necesitamos que telnet y ftp estén habilitados para la red interna pero no para Internet.

Entonces los archivos nos quedan así:
-Habilitamos telnet y ftp en inetd.conf:

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

En hosts.deny negamos todo:
ALL : ALL

En hosts.allow, le damos permiso a los usuarios de la red interna para que accedan a ftp y telnet, colocando lo siguiente:

in.ftpd, in.telnetd : 150.185.1.0/255.255.255.0

Listo !

7.- Misceláneas.

Aclaremos que no todos los servicios de red que esta brindando nuestra PC son manejados por inetd y tcpd. Por lo tanto son independientes de la configuración realizada.
Un ejemplo típico de servidores que no son manejados por inetd son: sendmail y apache, necesitaran su propia configuración para brindar su servicio en forma segura.

Para visualizar los servicios de red que están disponibles, podemos utilizar el siguiente comando:

```
# netstat -a | grep LISTEN
tcp        0      0 *:printer               *:*
LISTEN
tcp        0      0 *:www                   *:*
LISTEN
tcp        0      0 *:6000                  *:*
LISTEN
tcp        0      0 *:smtp                  *:*
LISTEN
tcp        0      0 *:telnet                *:*
LISTEN
tcp        0      0 *:sunrpc                *:*
LISTEN
unix  1      [ ACC ]     STREAM     LISTENING     1808   /tmp/.X11-
unix/X0
unix  1      [ ACC ]     STREAM     LISTENING     1293   /var/run/gpmctl
unix  1      [ ACC ]     STREAM     LISTENING     1209   /dev/log
```

Los servicios de red son los que comienzan con tcp o udp.

los servicios que están disponibles, según lo que nos dice el netstat en este ejemplo son:

printer
www
6000 (Xserver)
smtp
telnet
sunrpc

Supongamos que el servidor web (www) no es necesario para nuestro caso y lo queremos deshabilitar, lo que podemos hacer es:

- Desinstalar la aplicación que brinda el servicio (apache).

- Deshabilitar el servicio, mediante el script de arranque.
Esto dependerá de la distribución.

Otra precaución fundamental es asegurarse que los servicios que necesitamos ejecutar no tengan problemas de seguridad y que sean las ultimas versiones.
Existen varios sitios web y listas de correo que nos alertan cuando se encuentran dichos problemas.
Normalmente cada distribución, en su sitio oficial publica las actualizaciones necesarias, por problemas de seguridad.

También es muy recomendable configurar un firewall, colocando otra barrera mas de seguridad.

8.- Bibliografía.

Quedan muchos detalles para conocer, solo se explicaron los conceptos básicos como para realizar una configuración básica y poder entender luego mas profundamente el tema.

Para aquellos que quieran profundizar en el tema, pueden leer las siguientes paginas del manual.

Pagina.	**Sección.**	**Descripción.**
inetd	8	Funcionamiento del súper server.
services	5	Estructura del archivo services.
hosts_acces s	5	Estructura de hosts.allow y hosts.deny.
tcpd	8	Funcionamiento del tcpd.

Nota: para ver una pagina del manual, usar el comando: $ man sección pagina

9.- Fuente.

Hispasec