Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Seguridad con TCP Wrappers e ipchains (II) (10880 lectures)

Per **Javi Polo**, ***DrSlump*** (http://drslump.org)

Creado el 26/07/2000 00:00 modificado el 26/07/2000 00:00

En este articulo revisamos a groso modo la configuración de los servicios ofrecidos por inetd y como usar tcp wrappers e ipchains para aumentar la seguridad de nuestro sistema. Parte II : Tcp Wrappers

Anterior(1) Siguiente(2)

Bueno, el tcp wrappers es un programa que filtra las peticiones, y hace una u otra cosa dependiendo del demonio a lanzar y de la IP que pide el servicio. Esto lo hace mediante el `/etc/hosts.allow` y `/etc/hosts.deny`

En principio, se usa `/etc/hosts.deny` para indicar a quien y a que no se permite el acceso, y el `/etc/hosts.allow` para decir quien y a que puede acceder.

El formato de ambos ficheros es:

```
DEMONIO: IP[: OPCION1 [: OPCION2 ]]
```

donde `DEMONIO` puede ser el demonio a lanzar, como en el ejemplo puesto, el `in.ftpd`, o también puede ser `ALL`, refiriéndose a todos los demonios.

IP puede ser tanto una IP o una URL, como un rango de IPs (o de URLs), como cualquiera de los comodines que explico despues.

Para indicar un rango de IPs, por ejemplo, se hace poniendo: `123.32.' Esto englobaría todas las IPs 123.32.XXX.XXX Y lo mismo para las URLs: `.ml.org' englobaría todos los subdominios de ml.org

También se puede determinar un rango de IPs de la tradicional forma IP/MASCARA De forma que por ejemplo, para indicar el rango 127.0.0.0 a 127.0.255.255 se indicaría así: 127.0.0.0/255.255.0.0
Los comodines son:

`ALL`	que indica que coincide con cualquier dirección entrante
`LOCAL`	que coincide con cualquier nombre que no tenga un "."
`UNKNOWN`	que coincide con aquellas máquinas de las que no se conoce o su nombre o su IP
`KNOWN`	que coincide con las máquinas de las que se conoce tanto su nombre como su IP
`PARANOID`	que coincide con aquellas máquinas en las cual su nombre no coincida con su IP

las opciones pueden ser:

`allow`	hace que a lo indicado en esa entrada se debe aceptar conexión, independientemente de si está en el fichero hosts.allow o en hosts.deny. Debe ser la última opción de la línea.
`deny`	es como la anterior, pero denegando la conexión.
`spawn`	ejecuta un comando shell (por si se

	quiere ejecutar algo cada vez que se establece una conexión que coincida con la línea), yo por ejemplo hago que cuando recibo cualquier conexión de fuera, me suene un sonido para saber que alguien intenta conectar a mi máquina
`twist`	es como el comando spawn, pero cortando la conexión tras ejecutar el comando. También debe ser la última opción de la línea.

Para estos dos últimos comandos, se pueden usar las expansiones que permite el tcpd. Estas son:

%a	dirección de la máquina cliente
%c	Información del cliente (puede ser usuario@máquina, o lo que sea, dependiendo del cliente)
%d	
%h	nombre o IP de la máquina cliente, según esté disponible
%n	nombre de la máquina cliente
%p	PID del demonio
%s	información del servidor (demonio@máquina o solo demonio, depende)
%u	Nombre del usuario cliente
%%	Es un simple carácter %

Con estas expansiones y esos dos comandos se pueden hacer muchas cosas, por ejemplo, me se de uno que cada vez que intentaban entrarle por telnet, le mandaba automáticamente un "teardrop" al afortunado intruso :)

NOTA: Un teardrop es un DoS (Denial of Service, un ataque para colgar la máquina o provocar que se reinicie) que se basa en aprovecharse en el fallo de la defragmentación de los paquetes TCP que tienen (ahora ya tenían, puesto que muchos se han parcheado ya) gran parte de Sistemas Operativos. La información se manda a través de Internet por el protocolo TCP/IP (que se usa también en otro tipo de redes, aparte de Internet, como por ejemplo intranets), el protocolo TCP se encarga de trocear la información en paquetes que luego el protocolo IP se encarga de hacer llegar a su destino, y una vez allí, el protocolo TCP comprueba que estén todos los paquetes y los junta para recomponer la información original. Dicho ataque (y muchos basados en él) lo que hace es aprovecharse de que en muchos Sistemas Operativos no se comprobaba si el tamaño del paquete antes de juntarlos era muy pequeño, y al ser así la máquina se hacía un lío a la hora de juntarlo. Esto no estoy completamente seguro de que sea así, evidentemente, acepto todo tipo de aportaciones y críticas, tanto positivas como negativas. Finalizada esta "pequeña" aclaración, sigamos ... Anterior[1] Siguiente[2]

Lista de enlaces de este artículo:

1. http://bulma.net/body.phtml?nIdNoticia=84&nIdComentario=-1
2. http://bulma.net/body.phtml?nIdNoticia=86&nIdComentario=-1

E-mail del autor: javipolo _ARROBA_ drslump.org
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=85