Configuración del Firewall en servidores de producción

Todo lo que he instalado está en sus rutas los binarios y los ficheros de configuración en /etc/csf. Los servicios son /etc/init.d/csf y /etc/init.d/lfd (ya están puestos en el runlevel).

Toda la config como ya digo está en /etc/csf, y nos interesan sobre todo el fichero principal “csf.conf” y los ficheros csf.*

Guía rápida

- csf.allow: fichero donde dejaremos las IPs que no serán chequeadas por el sistema
- csf.conf: fichero principal de configuración
- csf.deny: se van metiendo las IPs que se irán bloqueando por el sistema (son bloqueos permanentes!! si alguien nos dice que no accede al server el primer sitio donde mirar es este).
- csf.ignore: ips que ignoraremos de los chequeos, solo está 127.0.0.1 y salvo causa mayor así debería ser
- csf.pignore: fichero donde meteremos los ejecutables o usuarios que el sistema ignorará (he metido el proceso de imap y el usuario nrpe).
- csf.tempban: lista las IPs baneadas temporalmente y la razón (segundo sitio donde mirar si alguien nos dice que no puede acceder al servidor) (es lo mismo que hacer “csf -t”

Comandos básicos:

```
csf -t  -> lista las ips baneadas temporalmente

csf -tr IP -> desbanea una IP
```

```
csf -a -> añade IP a lista blanca y csf.allow

csf -d -> añade IP a lista negra y csf.deny
```

```
/etc/init.d/csf restart (restartea el servicio) /etc/init.d/lfd restart
(restartea el servicio)
```

Para white-listear una IP en el Firewall (cuidado con esta opción, porque es abrir una puerta):

- Meter la IP en el fichero —–> /etc/csf/csf.allow
- Reiniciar el firewall ———> /etc/init.d/csf restart
- Probar desde consola (telnet, el cliente de mysql…)

Resumen de email tipo que llegarán al servidor

- lfd on merkatu2.ran.es: 212.34.154.52 (ES/Spain/correo.azierta.eu) blocked for port scanning El sistema ha encontrado que desde la IP 212.34.154.52 (fijaros que nos indica que es una IP

española) están haciendo un escaneo de puertos. Al ser IPs españolas, nosotros solemos desbloquearla de la misma (en este mail o uno posterior os indicaré cómo saber las IPs bloqueadas).

- lfd on merkatu2.ran.es: Excessive resource usage: panbetti (13984 (Parent PID:3572)) Este mail nos dice que hay un uso escesivo de recursos para un usuario en concreto. Dentro del mail nos aparece:

Account: panbetti

```
Resource:     Process Time
Exceeded:     2601090 > 3600 (seconds)
Executable:   /usr/libexec/dovecot/imap
Command Line: imap [iban@pan-betti.com 178.239.83.162]
PID:          13984 (Parent PID:3572)
Killed:       No
```

La info del mail nos dice que hay un proceso imap (/usr/libexec/dovecot/imap) para el usuario [iban@pan-betti.com 178.239.83.162] (desde esa IP) que lleva activa 2601090 segundos que es mayor de lo establecido en la configuración (3600) y uqe no se ha matado el proceso.

- lfd on merkatu2.ran.es: blocked 188.165.197.228 (FR/France/sv.irontec.com) Bloqueado una IP de francia. Dentro del mail nos aparece:

Time: Thu Feb 14 17:47:33 2013 +0100

```
IP:       188.165.197.228 (FR/France/sv.irontec.com)
Failures: 5 (sshd)
Interval: 300 seconds
Blocked:  Permanent Block
```

Log entries:

```
Feb 14 17:47:07 merkatu2 sshd[11594]: Failed password for invalid user root
from 188.165.197.228 port 54583 ssh2
Feb 14 17:47:13 merkatu2 sshd[11594]: Failed password for invalid user root
from 188.165.197.228 port 54583 ssh2
Feb 14 17:47:19 merkatu2 sshd[11594]: Failed password for invalid user root
from 188.165.197.228 port 54583 ssh2
Feb 14 17:47:25 merkatu2 sshd[11640]: Failed password for invalid user root
from 188.165.197.228 port 54585 ssh2
Feb 14 17:47:28 merkatu2 sshd[11640]: Failed password for invalid user root
from 188.165.197.228 port 54585 ssh2
```

Qué quiere decir esto? Pues que alguien (en este caso he sido yo desde un servidor que tenemos en francia) se ha intentado conectar por SSH a vuestro servidor usando el usuario root, y ha fallado 5 veces en meter la contraseña. Por lo tanto, es un ataque y lo bloqueamos. No nos gusta que nadie quiera entrar en nuestro server!!! Esto es un arma de doble filo, porque tenemos 5 posibilidades de meter la contraseña, pero la IP del servidor de Bilbao, la de Vitoria y nuestra ofi de Irontec están en lista blanca, por lo que desde estas IPs podremos fallar tantas veces como queramos :D

- lfd on merkatu2.ran.es: Suspicious process running under user nrpe Este tipo de mail nos dice que hay un proceso sospechoso corriendo bajo usuario “nrpe”. Dentro del mail nos dice:

Time: Thu Feb 14 17:29:54 2013 +0100

```
    PID:     3821 (Parent PID:3821)
    Account: nrpe
    Uptime:  5398848 seconds
```

```
Executable:
/usr/sbin/nrpe
```

```
Command Line (often faked in exploits):
/usr/sbin/nrpe -c /etc/nagios/nrpe.cfg -d
```

```
Network connections by the process (if any):
tcp: 0.0.0.0:5666 -> 0.0.0.0:0
```

Este tipo de mails nos pasa a nosotros también, pero lo que hacemos es whitelistear el usuario.

- lfd on merkatu2.ran.es: SSH login alert for user merkatu_sat from 188.165.197.228 (FR/France/sv.irontec.com) Tal como dice el subject del mail nos dice que desde la IP de francia 188.165.197.228 (he sido yo, después de quitarme el bloqueo) me he conectado por SSH con el usuario merkatu_sat. Esto viene muy bien para saber quién y desde donde se conecta la gente a nuestro servidor.
- Bloqueos de UDP:

Ha llegado algún mail de bloqueo desde la IP 212.34.128.219 (ES/Spain/srv01.iwork.es). Os suena esa IP o el dominio que indica?

Metidos nuevas configuraciones para que ignore ciertos procesos y usuarios en el fichero csf.pignore

Casos en los que se bloquea una IP

- escaneo de puertos
- intento de conexión SSH y falla más de 5 veces
- intento de conexión IMAP/POP3 y falla más de 5 veces,

Casos en los que se bloquea una IP

Algunas configuraciones:

Para que falle al de 10 intentos la autenticación a la hora de conectarnos al SMTP deberéis modificar la variable LF_SMTPAUTH, que actualmente está a “5” en el fichero /etc/csf/csf.conf

Si queréis en otro caso aumentar los intentos de POP3 o IMAP las variables son LF_POP3D y LF_IMAPD respectivamente (que ahora son 10 intentos).