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

Verificando/auditando el Firewall. (22272 lectures)

Per **Carlos Cortes Cortes**, ***carcoco*** (http://bulma.net/~carcoco/)

Creado el 02/01/2002 22:21 modificado el 02/01/2002 22:21

> Has pasado varios horas configurando, repasando y probando tus reglas de tu **Firewall**, por fin parece que la cosa va fina del todo, pero no te acabas de fiar y te gustaría **verificar** que todo va como es de esperar ...

Existen **al menos** tres formas más o menos sencillas de verificar el correcto funcionamiento de las reglas de filtrado de un **Firewall**:

- **netstat**
- **nmap**
- **hping2**

Netstat:

```
# netstat -pan | grep tcp.*LISTEN
tcp  0  0 0.0.0.0:515   0.0.0.0:*   LISTEN   184/lpd
tcp  0  0 0.0.0.0:3306  0.0.0.0:*   LISTEN   276/mysqld
tcp  0  0 0.0.0.0:111   0.0.0.0:*   LISTEN   156/portmap
tcp  0  0 0.0.0.0:80    0.0.0.0:*   LISTEN   1794/httpd
tcp  0  0 0.0.0.0:6000  0.0.0.0:*   LISTEN   402/X
tcp  0  0 0.0.0.0:22    0.0.0.0:*   LISTEN   173/sshd
tcp  0  0 0.0.0.0:119   0.0.0.0:*   LISTEN   322/inetd
tcp  0  0 0.0.0.0:25    0.0.0.0:*   LISTEN   333/sendmail: accep
```

Nmap:

```
$ nmap linuxalcoy

Starting nmap V. 2.54BETA30
Interesting ports on linuxalcoy.home.org (127.0.0.2):
(The 1541 ports scanned but not shown
                below are in state: closed)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc
119/tcp    open        nntp
515/tcp    open        printer
3306/tcp   open        mysql
6000/tcp   open        X11
```

hping2:

Voy a comprobar si el servidor **SSH** (suele estar en el puerto 22) está activo.

```
# hping2 -S -c 1 -p 22 -t 1 linuxalcoy
HPING linuxalcoy (lo 127.0.0.2):
    S set, 40 headers + 0 data bytes
len=44 ip=127.0.0.2 flags=SA DF
    seq=0 ttl=64 id=0 win=32767 rtt=3.0 ms
```

```
--- linuxalcoy hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.0/3.0/3.0 ms
```

En cambio podemos obserbar que el **telnet** (puerto 23) no esta activo o esta correctamente configurado en nuestro Firewall.

```
# hping2 -S -c 1 -p 23 -t 1 -V linuxalcoy
using lo, addr: 127.0.0.1, MTU: 1500
HPING linuxalcoy (lo 127.0.0.2):
     S set, 40 headers + 0 data bytes

--- linuxalcoy hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Si os interesa el tema, no os perdaís el interesante artículo: **Auditing Your Firewall Setup** de *Lance Spitzner*, seguro que aprendereís muchas cosas sobre como verificar el correcto funcionamiento de vuestro **firewall**:

Articulos

- Auditing Your Firewall Setup: http://www.enteract.com/~lspitz/audit.html[1]
- Firewall penetration testing. http://www.wittys.com/files/mab/fwpentesting.html[2]
- Auditing Firewalls: A Practical Guide http://www.hideaway.net/Server_Security/Library/Firewalls/firewall/audit.htm[3]
- Test the firewall system: http://www.cert.org/security-improvement/practices/p060.html[4]
- Building Your Firewall Rulebase: http://www.enteract.com/~lspitz/rules.html[5]

Herramientas

- nmap http://www.insecure.org/nmap/[6]
- Hping & hping2 & hping3 http://www.hping.org/index.html[7]
- FireWalk http://www.packetfactory.net/Projects/Firewalk/[8]
- Firewall Tester http://www.infis.univ.trieste.it/~lcars/ftester/[9]
- Nessus http://www.nessus.org[10]
- Nemesis packet injection tool-suite: http://www.packetfactory.net/projects/nemesis/[11]

--
Carlos Cortes(aka carcoco)
http://bulma.net/todos.phtml?id_autor=132 [12]

Lista de enlaces de este artículo:

1. http://www.enteract.com/~lspitz/audit.html
2. http://www.wittys.com/files/mab/fwpentesting.html
3. http://www.hideaway.net/Server_Security/Library/Firewalls/firewall/audit.htm
4. http://www.cert.org/security-improvement/practices/p060.html
5. http://www.enteract.com/~lspitz/rules.html
6. http://www.insecure.org/nmap/
7. http://www.hping.org/index.html
8. http://www.packetfactory.net/Projects/Firewalk/
9. http://www.infis.univ.trieste.it/~lcars/ftester/
10. http://www.nessus.org
11. http://www.packetfactory.net/projects/nemesis/
12. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco _ARROBA_ gmail.com
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1100