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

Escaneador de puertos Nmap (71324 lectures)

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

Creado el 26/03/2002 00:24 modificado el 26/03/2002 00:24

> La *"herramienta de exploración de red y escáner de seguridad"* **Nmap** es posiblemente el mejor escaneador de puertos existente, permitiendo determinar, de una forma rápida y sencilla, que servidores están ativos y qué servicios ofrecen (puertos abiertos) ...

Es una de esas herramientas de seguridad imprescindible para cualquier administrador de sistemas, siendo muy utilizada diariamente en todo el mundo (tanto por **crackers** como por **sysadmins**). Es uno de los programas más populares de **Freshmeat**.

Entre las características del nmap podemos encontrar:

- **Flexible**: Soporta técnicas avanzadas para el mapeado de sistemas y redes que esten detras de filtros IP, firewalls, routers y otros obstaculos. Estas incluyen mecanismos de escaneado de puertos (tanto TCP, como UDP), detección del sistema operativo, escaneos invisibles, conexiones semiabiertas, ...
- **Potente**: **Nmap** ha sido utilizado para escanear redes de ordenadores con cientos de cientos de máquinas.
- **Portable**: Existen versiones para la gran mayoría de los sistemas operativos modernos, entre ellos: Linux, Open/Free/Net BSD, Solaris, IRIX, Mac OS X, HP-UX, Sun OS, Windows (fase beta) ....
- **Fácil**: Aunque existen una gran cantidad de opciones disponibles, se puede realizar un sencillo escaneado de puertos con "nmap -O -sS maquina".
- **Libre**: El objetivo del proyecto **Nmap** es proveer a administradores/auditores/hackers con una potente herramienta de seguridad con la que explorar sus redes. Nmap se distribuye con licencia **GPL** por lo que el código fuente está disponible para su descarga libremente.
- **Buena Documentación**: Se ha realizado un gran esfuerzo en mantener actualizados y traducidos tanto las páginas man, como los tutoriales y el resto de documentación relacionada con **Nmap**.
- **Soportado**: Aunque **Nmap** viene sin garantia explicita de ningún tipo, puede escribir al autor y/o utilizar las diferentes listas de distribución sobre **Nmap**. Existen varias empresas que incluyen soporte entre sus servicios.
- **Premiado**: **Nmap** ha recibido multitud de premios y reconocimientos por revistas del sector.
- **Popular**: Diariamente cientos de personas descargan **Nmap**, además está incluido de serie en muchos sistemas operativos. Esta gran popularidad es la mejor garantia de su calidad, soporte y desarrollo.

Tal y como he comentado, el uso del **Nmap** es muy sencillo, por ejemplo, para averiguar los servicios (puertos) accesibles de una determinada máquina, bastará con ejecutar:

```
# nmap -O -sS carlets

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on carlets.home.org (192.168.0.99):
(The 1537 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     filtered    ssh
25/tcp     filtered    smtp
80/tcp     open        http
111/tcp    filtered    sunrpc
139/tcp    filtered    netbios-ssn
143/tcp    open        imap2
515/tcp    open        printer
3128/tcp   filtered    squid-http
3306/tcp   filtered    mysql
6000/tcp   filtered    X11
```

```
6001/tcp   filtered    X11:1
6002/tcp   filtered    X11:2
6003/tcp   filtered    X11:3
6004/tcp   filtered    X11:4
6005/tcp   filtered    X11:5
6006/tcp   filtered    X11:6
8080/tcp   filtered    http-proxy

Remote operating system guess: Linux Kernel 2.4.0 - 2.4.17 (X86)
Uptime 0.030 days (since Mon Mar 25 22:34:58 2002)

Nmap run completed -- 1 IP address (1 host up) scanned in 8 seconds
```

Existen muchas más opciones y alternativas, por lo que es más que recomendable acceder a la documentación incluida con **Nmap**, así como a la página **man** del mismo.

```
# nmap --help

# man nmap

# lynx nmap_manpage-es.html
```

Estos escaneos de máquinas y redes, suelen dejar huellas de su ejecución en los registros logs de las máquinas escaneadas (por ejemplo, en **/var/log/messages**), por lo que es interesante el utilizar alguno de los modos de escaneos invisibles tales como **-sF,-sX,-sN Stealth FIN, Xmas, or Null scan**, de forma que se evitar finalizar la negoción **TCP**, evitando al mismo tiempo el comentado registro en los ficheros **logs**.

Fyodor, el desarrollador de esta magnifica herramienta, tiene un gran sentido de humor, tal y como lo demuestra al implementar la opción **-oS**, que muestra la salida del **Nmap** en un formato que les encantará a los **Script-kiddies**, como podemos ver:

```
# nmap -oS - carlets

$taRt|ng nmap V. 2.54B3T431 ( www.1n$ecur3.ORg/nmap/ )
|nt3r3sting pOrtz 0n carletz.home.org (192.168.0.99):
(The 1545 Portz scannEd but nOT sh0wn bel0w ar3 In $tatE: cLOS3D)
POrt       Stat3       S3rv1Ce
22/tcp     OpeN        $$H
25/Tcp     0pEn        smtp
80/tcp     0p3n        htTp
139/tcP    op3n        N3Tb1Oz-Ssn
143/tCP    0pen        imap2
515/tcp    f!lt3red    prinT3r
3128/tcp   Op3n        squ|d-HtTP
3306/tCp   Op3n        my$ql
6000/tcp   0p3n        x11


Nmap rUn c0mpl3ted -- 1 !P aDdr3Sz (1 hOst uP) scANnEd !n 3 $econdS
```

Incluido con **Nmap** se encuentra **nmapfe** que es un Front-end gráfico, que permite ejecutar **Nmap** usando el ratón.
(Ver imagen del nmapfe: http://nou.bulma.net/~carcoco/bulma/nmap.jpg[1]).
Indicar que existen otros front-end gráficos para facilitar aún más el uso de esta potente aplicación (KNmap, KNmapFE, QNMap, Kmap, Web-NMap, vnmap, ...)

Nmap es una herramienta ideal para Verificar/auditar el Firewall[2], tal como dice uno de los banner de **Nmap**, "Audite la seguridad de sus Redes antes que los chicos malos lo hagan" (*Audit your network security before the bad guys do*).

Nmap Free Security Scanner:
http://www.insecure.org/nmap/ [3]

--
$ alias **carcoco**="echo Carlos Cortés"
http://bulma.net/todos.phtml?id_autor=132 [4]

Lista de enlaces de este artículo:

1. http://nou.bulma.net/~carcoco/bulma/nmap.jpg
2. http://bulma.net/body.phtml?nIdNoticia=1100
3. http://www.insecure.org/nmap/
4. 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=1240