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

Xprobe. Detección remota del sistema operativo. (16544 lectures)

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

Creado el 15/11/2001 18:53 modificado el 15/11/2001 18:53

> **Xprobe** es un programa que nos permite la identificación **remota** del **sistema operativo**. Esto es lo que se conoce en inglés como *remote active operating system fingerprinting* ...

La idea es **conocer el sistema operativo** que está ejecutando una determinada máquina conectada en red (ya sea red local o Internet) de forma **remota**, es decir, sin la posibilidad de entrar (**hacer login**) en esa máquina.
Esta detección remota de S.O., es realmente muy importante y es precisamente el primer paso que utilizan los cracker's, a la hora de recoger información de sus potenciales victimas, aunque como veremos aqui tiene muchos usos digamos **legales**: scanners de seguridad, detección de máquinas, estadísticas, seguridad, ...

El primer programa en utilizar este tipo de tecnicas fue **queso** (que significa ¿Que S.O?) desarrollado en España por el *desaparecido* grupo **Apostols**, aunque ahora podemos considerar que se ha quedado un poco obsoleto y ha sido totalmente superado por el scanner de puertos Nmap[1] -- Free Stealth Port Scanner For Network Exploration & Security Audits.

Aqui podemos ver un ejemplo de la ejecución del nmap, donde se detecta perfectamente un **Linux 2.1.122 - 2.2.14**:

```
# ./nmap -O  192.109.12.43

Starting nmap V. 2.53 by fyodor@insecure.org

Interesting ports on bar023.servidor.es (192.109.12.43):
(The 1512 ports scanned but not shown
        below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc
139/tcp    open        netbios-ssn
901/tcp    open        samba-swat
929/tcp    open        unknown
2049/tcp   open        nfs
3306/tcp   open        mysql

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=959436 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.14
Nmap run completed --
  1 IP address (1 host up) scanned in 35 seconds
```

La **detección remota** de sistema operativo, puertos y/o servicios, es muy utilizada en **Internet**, la empresa NetCraft[2], realiza cada mes un estudio (Web Server Survey [3]) en base a sus exhaustivos escaneos de **servidores WEB**. **Tienen una herramienta online[4], que detecta el sistema y servidor de la pagina web que le indiquemos.**
Para ver por elemplo el servidor web y el sistema operativo bajo el que corre Bulma :
The site bulma.net is running ... [5]

Xprobe utiliza el protocolo **ICMP**, en lugar del tipico protocolo **TCP** que utilizan otros scanners, este es el motivo por el cual el **Xprobe** es más invisible, que por ejemplo, el **nmap** (según su autor). Con invisible me refiero a que no deja rastro en los logs de la máquina a la que se le esta haciendo el escaneo.

Xprobe combines various remote active operating system fingerprinting methods using the ICMP protocol, which were discovered during the "ICMP Usage in Scanning" research project, into a simple, fast, efficient and a powerful way to detect an underlying operating system a targeted host is using.
Written and maintained by Fyodor Yarochkin and Ofir Arkin,

Aqui os dejo un ejemplo de la utilización del Xprobe identificando correctamente un W2K.

```
 ./xprobe maquineta
X probe ver. 0.0.2
------------------
Interface: fxp0/192.168.0.2

LOG: Target: 192.168.0.47
LOG: Netmask: 255.255.255.255
LOG: probing: 192.168.0.47
LOG: [send]-> UDP to 192.168.0.47:32132
LOG: [98 bytes] sent, waiting for response.
LOG: [send]-> ICMP echo request to 192.168.0.47
LOG: [68 bytes] sent, waiting for response.
FINAL:[ Windows 2k. SP1, SP2/Windows XP ]
```

En cambio no tuvo tanto exito a la hora de identificar una maquina FreeBSD

```
./xprobe freebsd
X probe ver. 0.0.2
------------------
Interface: fxp0/192.168.0.2

LOG: Target: 192.168.0.25
LOG: Netmask: 255.255.255.255
LOG: probing: 192.168.0.25
LOG: [send]-> UDP to 192.168.0.25:32132
LOG: [98 bytes] sent, waiting for response.
Receive timeout. Quitting..
Error while sending UDP query. Quiting
```

http://www.sys-security.com/html/projects/X.html[6]
http://www.sys-security.com/archive/tools/X/xprobe-0.0.2.tar.gz[7]
http://hig.beesecure.org/t001_xprobe.html[8]
http://www.sys-security.com/archive/papers/X_v1.0.pdf[9]
QueSO: http://packetstorm.decepticons.org/UNIX/scanners/queso-980922.tar.gz[10]

--
Carlos Cortes (aka carcoco)
http://bulma.net/todos.phtml?id_autor=132 [11]

Lista de enlaces de este artículo:

1. http://www.insecure.org/nmap/
2. http://www.netcraft.com/
3. http://www.netcraft.com/survey/
4. http://www.netcraft.com/whats/
5. http://uptime.netcraft.com/up/graph/?mode_u=off&mode_w=on&site=bulma.net&submit=
6. http://www.sys-security.com/html/projects/X.html
7. http://www.sys-security.com/archive/tools/X/xprobe-0.0.2.tar.gz
8. http://hig.beesecure.org/t001_xprobe.html
9. http://www.sys-security.com/archive/papers/X_v1.0.pdf
10. http://packetstorm.decepticons.org/UNIX/scanners/queso-980922.tar.gz

11. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco _ARROBA_ gmail.com