IDENTIFICANDO SERVIDORES CON AMAP

Todos somos conscientes de la enorme cantidad de aplicaciones que GNU/Linux pone a disposición de sus usuarios y de los distintos usos que podemos hacer de ellas. Amap es una de esas pequeñas maravillas que podremos utilizar por ejemplo cuando descubramos un puerto abierto en nuestro sistema y no sepamos que anda funcionando por ahí, aunque claro, como muchos están pensando, también vamos a poder identificar servicios corriendo en hosts ajenos. Su funcionamiento se basa en las respuestas que los distintos servidores hacen ante el envío de unos determinados paquetes.
Pero la información es poder y no es bueno que este en manos de unos pocos. Así que vamos a ver un pequeño tutorial de esta herramienta.
Lo primero que hemos de hacer es acudir a su página web y descargarnoslo, así que pinchamos en http://thc.segfault.net/releases.php y nos hacemos con la versión mas reciente de Amap. Una vez en nuestro poder hemos de descomprimirla y compilarla a mano:

tar -zxvf amap-5.2.tar.gz
cd amap-5.2/
./configure
make
make install

Si todo ha ido bien y no ha habido problemas con las dependencias ya estamos listos para usarlo. Lo primero que vamos a hacer es ver que puertos tcp hay “escuchando” en nuestro sistema, así que:

root@saruman:/home/vlad# netstat -an | grep LISTEN | grep tcp
tcp 0 0 127.0.0.1:8118 0.0.0.0:* LISTEN
tcp6 0 0 :::22 :::* LISTEN

Vemos que hay dos, el 22 y el 8118. Solo nos queda que Amap haga su trabajo:

root@saruman:/home/vlad# amap 127.0.0.1 22 8118
amap v5.2 (www.thc.org/thc-amap) started at 2006-09-27 22:43:03 - MAPPING mode

Protocol on 127.0.0.1:22/tcp matches ssh
Protocol on 127.0.0.1:22/tcp matches ssh-openssh
Protocol on 127.0.0.1:8118/tcp matches http
Protocol on 127.0.0.1:8118/tcp matches webmin

Unidentified ports: none.

amap v5.2 finished at 2006-09-27 22:43:12

¿Ha quedado claro? Pues eso. Amap tiene muchas posibilidades, para echarles un vistazo solo tenéis que hacer un:

/usr/local/bin/amap –help

Solo nos resta por decir que Amap tiene en su archivo appdefs.resp las claves para identificar los distintos servidores que es capaz de reconocer. Al día de hoy el comando "***amap -W***" que sirve para actualizar ese archivo da un error, así que para estar actualizados hemos de ir compilando las distintas versiones.

Por Vl@d.
Para www.fentlinux.com.