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

Identificación remota de servidores FTP/SMTP. (15799 lectures)

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

Creado el 14/12/2001 16:06 modificado el 14/12/2001 16:06

> **ftpmap/smtpmap** nos permite identificar **servidores ftp/smtp** de forma remota, aunque el administrador haya tenido la precación de quitar los mensajes de identificación del servicio **ftp/smtp** ...

Básicamente lo que hacer, es enviar diversas peticiones de forma que el servidor de ftp contestará, de una determinada forma dependiendo de la versión en cuestión, de forma que analizando esta respuesta (independiente para cada servidor ftp) denominada **fingerprint**, podamos identificar la versión del servidor ftp.
If you know the name of the FTP server you just scanned, please contribute to this program by sending the fingerprint and the name of the server software to : ftpmap@jedi.claranet.fr

Parece que no termina de ir muy fino, aunque es una cuestión de tiempo y de colaboración entre todos, pues tal como dice su autor, si no es detectada alguna versión en concreto, nos pide que le mandemos el registro de las fingerprint generadas y la versión del servidor, para que se puede añadir esta información al **ftpmap**.

```
$ ftpmap -h
FTP-Map 0.3

Usage : ftpmap [-h] [-P ] [-u ] [-p ] -s

-h          : help
-P    : connect to port   (default=21)
-u   : login to the server as   (default=ftp)
-p    : use this password (default=mickey@disneyland.com)
-s    : connect to FTP server running on   (IP or name)
```

En el caso de que la maquina en cuestión no tenga el servidor **ftp** activo, obtendremos el siguiente resultado.

```
ftpmap -s maquineta
*** Scanning IP : [192.168.0.3]

*** Fingerprint :

Sorry, I'm unable to connect: Connection refused

./ftpmap -s bsdalcoy
*** Scanning IP : [192.168.0.2]

*** Fingerprint :

2933,2450,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2933,2933,2981,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
3076,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2942,3023,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2969,
3047,3174,3043,3225,3675,3048,2937,3071,2958,3581,2120,2933,2933,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2551,
2933,2450,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
```

```
2933,2933,2933,2981,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
3076,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2942,3023,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2972,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2969,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,
2933,2933,2933,2933,2933,2933,2933,2933,2933,2551,

*** This may be running :
[Wuftpd 2.6]    (error=0.609062 %)
[Microsoft ftpd 5]      (error=1.29329 %)
[Microsoft ftpd 3]      (error=1.70462 %)

*** Unable to determine FTP port sequence numbers

If you know the name of the FTP server you just scanned, please
contribute to this program by sending the fingerprint and the
name of the server software to : ftpmap@jedi.claranet.fr
```

Curiosamente esto es lo que obtengo en este mismo servidor al conectar usando ftp, tal como os he comentado, parece que aún le falta una buena colección de fingerprints:

```
$ ftp bsdalcoy
Connected to bsdalcoy.
220 bsdalcoy FTP server (Version 6.00LS) ready.
Name (bsdalcoy:carlets):
```

http://www.jedi.claranet.fr/(1)

---

smtpmap, aunque de un autor distinto, comparte totalmente con **ftpmap**, el funcionamiento y la idea, pero enfocado a la identificación de servidores **smtp**, es decir, los servidores que utilizamos para enviar correo electrónico.

```
$ smtpmap -h
SMTP-Map 0.2-27

Usage : smtpmap [-h] [-P ] [-u ] [-p ] -s

-h          : help
-P    : connect to port   (default=25)
-u   : login to the server as   (default=root)
-p    : use this password (default=mickey@disneyland.com)
-d          : enable debug output (not quite useful)
-s    : connect to SMTP server running on   (IP or name)
-n    : show all hits below  Percent

./smtpmap -s server
*** Scanning IP : [192.168.0.2]

*** Fingerprint :

3124,3124,4706,2217,1642,1781,2217,3648,3648,2978,2975,3379,3248,
1950,4112,1568,630,4098,1568,4095,1568,3541,3244,2187,1568,3261,
2187,1568,3057,2187,1568,3248,2898,2767,2217,3648,3648,3648,3648,
3648,3648,4054,3648,2187,3648,1568,1950,3648,1568,3648,3215,3648,
630,3648,4502,3058,1568,2187,2918,2187,2187,1568,1950,3815,1568,
1781,1642,2224,1568,2470,3022,4956,2669,503,3248,3234,1655,2217,
7585,1642,7724,1781,2217,3648,2978,2975,3379,3248,1950,4112,1568,
630,4098,1568,4095,1568,3541,3244,2187,1568,3261,2187,1568,3057,
2187,1568,3248,2898,2767,2217,3648,3648,3648,3648,3648,3648,4054,
3648,2187,3648,1568,1950,3648,1568,3648,3215,3648,630,3648,4502,
3058,1568,2187,2918,2187,2187,1568,1950,3815,1568,7724,1781,7585,
1642,8167,2224,1568,
3124,3124,4706,2217,1642,1781,2217,3648,3648,2978,2975,3379,3248,
1950,4112,1568,630,4098,1568,4095,1568,3541,3244,2187,1568,3261,
2187,1568,3057,2187,1568,3248,2898,2767,2217,3648,3648,3648,3648,
3648,3648,4054,3648,2187,3648,1568,1950,3648,1568,3648,3215,3648,
```

```
630,3648,4502,3058,1568,2187,2918,2187,2187,1568,1950,3815,1568,
1781,1642,2224,1568,2470,3022,5150,2669,503,3248,3234,1655,2217,
7585,1642,7724,1781,2217,3648,2978,2975,3379,3248,1950,4112,1568,
630,4098,1568,4095,1568,3541,3244,2187,1568,3261,2187,1568,3057,
2187,1568,3248,2898,2767,2217,3648,3648,3648,3648,3648,3648,4054,
3648,2187,3648,1568,1950,3648,1568,3648,3215,3648,630,3648,4502,
3058,1568,2187,2918,2187,2187,1568,1950,3815,1568,7724,1781,7585,
1642,8167,2224,1568,

*** This may be running :
[Sendmail 8.10.2]       (error=88.9964 %)
[Sendmail 8.11.3]       (error=90.6785 %)
[MDeamon 2.7 SP5]       (error=100 %)

*** Unable to determine SMTP port sequence numbers

If you know the name of the SMTP server you just scanned, please
contribute to this program by sending the fingerprint and the
name of the server software to : plasmahh@gmx.net
```

http://plasmahh.purespace.de/smtpmap-0.2.tar.gz[2]

Recomiendo que le hecheis un vistazo al resultado obtenido por estos 2 programas en vuestras propias máquinas, siempre es interesante saber como nos ven desde el exterior, sobretodo los posibles crackers.

Enlaces Relacionados:

- Cheops-ng: herramienta de administracion de redes, para controlar y monitorizar tu red. http://cheops-ng.sourceforge.net/[3]
- ldistfp - remote linux distribution fingerprinting http://teso.scene.at/releases.php3[4]
- p.0.f. passive OS fingerprinting tool. http://www.stearns.org/p0f/[5]

--
Carlos Cortes (aka carcoco)
http://bulma.net/todos.phtml?id_autor=132 [6]

Lista de enlaces de este artículo:

1. http://www.jedi.claranet.fr/
2. http://plasmahh.purespace.de/smtpmap-0.2.tar.gz
3. http://cheops-ng.sourceforge.net/
4. http://teso.scene.at/releases.php3
5. http://www.stearns.org/p0f/
6. 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=1063