Problemas de seguridad del protocolo Ftp

¿Alguna vez te has planteado la seguridad de los datos que envías por ftp a tu página web o a tu servidor de copias de seguridad ?
¿Viajan de forma segura, o por el contrario son fáciles de hackear?
Si no lo sabes, o no estás seguro, sigue leyendo… te sorprenderás.

Hoy vamos a hablar del Ftp, uno de los sistemas más empleados para el envío de datos a través de redes Tcp/IP, incluida Internet.

Ftp es un sistema de envío y recepción de ficheros utilizado desde los primeros tiempos de Internet. Su función principal es la de enviar una gran cantidad de archivos a un servidor de ficheros encargado de almacenarlos, así como de posteriormente poder recuperar dichos ficheros.

Que Ftp sea un sistema tan veterano tiene como principal ventaja su amplia implantación, ya que hace décadas que se

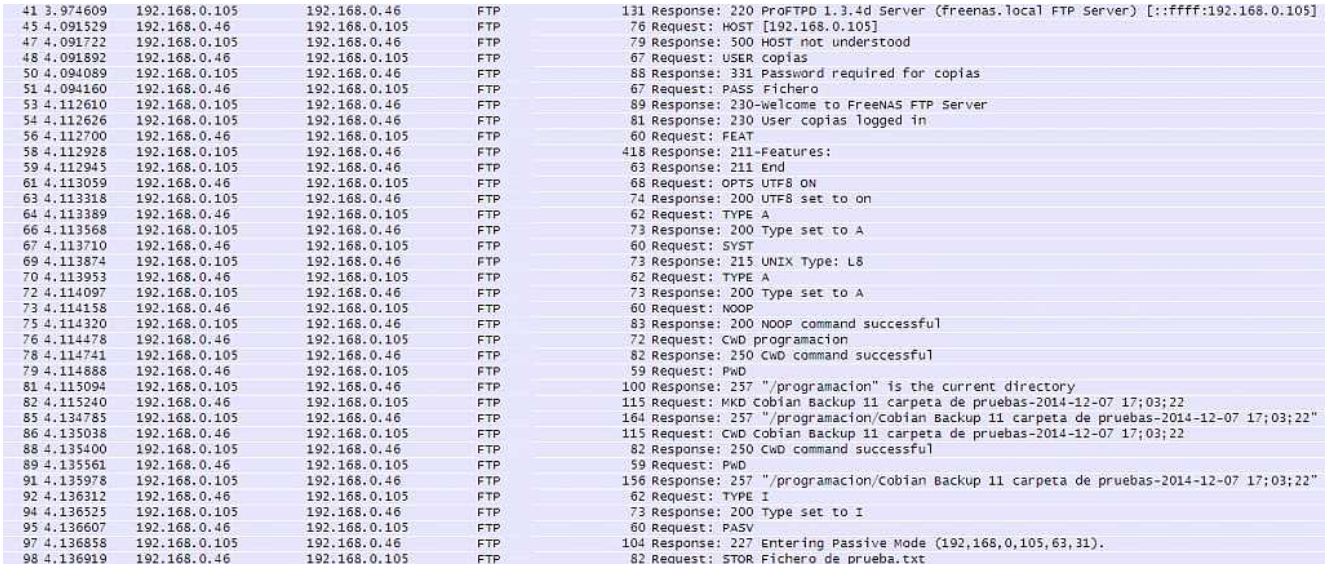
utiliza. Pero también tiene como principal inconveniente el de la seguridad: Cuando se pensó el protocolo ftp los usuarios de la red se contaban sencillamente por miles de personas y no por miles de millones como hoy en día, y la seguridad era un tema menor, pues poca gente tenía los medios y conocimiento necesarios para hackear la web (seguramente ni existía la palabra «hacker» cuando se diseñó el protocolo ftp inicial).

Actualmente, utilizar Ftp tanto en Internet para el envío de archivos y páginas web como internamente para conectarnos a un servidor propio y almacenar, por ejemplo, una copia de seguridad de nuestros archivos en nuestra intranet local, ha de considerarse un potencial problema de seguridad, ya que toda la información viaja sin encriptar y es muy fácil de interceptar.

Cualquier persona con acceso a nuestra red (pensemos, por ejemplo, que estamos usando una red wifi de un hotel, o que un vecino ha «pinchado» nuestra wifi), o cualquier troyano instalado en nuestro ordenador capaz de interceptar un puerto de comunicaciones que hemos descargado sin darnos cuenta junto a ese correo tan divertido, puede hacerse fácilmente con nuestro nombre de usuario y contraseña tan sólo con que accedamos una vez a nuestro servidor.

Veamos un ejemplo:

Utilicemos un programa de sniffer al alcance de cualquier usuario de windows como puede ser wireshark y probemos a conectarnos a nuestro servidor ftp. Este es el resultado:



41	3.974609	192.168.0.105	192.168.0.46	FTP	131 Response: 220 ProFTPD 1.3.4d Server (freenas.local FTP Server) [::ffff:192.168.0.105]
45	4.091529	192.168.0.46	192.168.0.105	FTP	76 Request: HOST [192.168.0.105]
47	4.091722	192.168.0.105	192.168.0.46	FTP	79 Response: 500 HOST not understood
48	4.091892	192.168.0.46	192.168.0.105	FTP	67 Request: USER copias
50	4.094089	192.168.0.105	192.168.0.46	FTP	88 Response: 331 Password required for copias
51	4.094160	192.168.0.46	192.168.0.105	FTP	67 Request: PASS Fichero
53	4.112610	192.168.0.105	192.168.0.46	FTP	89 Response: 230-Welcome to FreeNAS FTP Server
54	4.112626	192.168.0.105	192.168.0.46	FTP	81 Response: 230 User copias logged in
56	4.112700	192.168.0.46	192.168.0.105	FTP	60 Request: FEAT
58	4.112928	192.168.0.105	192.168.0.46	FTP	418 Response: 211-Features:
59	4.112945	192.168.0.105	192.168.0.46	FTP	63 Response: 211 End
61	4.113059	192.168.0.46	192.168.0.105	FTP	68 Request: OPTS UTF8 ON
63	4.113318	192.168.0.105	192.168.0.46	FTP	74 Response: 200 UTF8 set to on
64	4.113389	192.168.0.46	192.168.0.105	FTP	62 Request: TYPE A
66	4.113568	192.168.0.105	192.168.0.46	FTP	73 Response: 200 Type set to A
67	4.113710	192.168.0.46	192.168.0.105	FTP	60 Request: SYST
69	4.113874	192.168.0.105	192.168.0.46	FTP	73 Response: 215 UNIX Type: L8
70	4.113953	192.168.0.46	192.168.0.105	FTP	62 Request: TYPE A
72	4.114097	192.168.0.105	192.168.0.46	FTP	73 Response: 200 Type set to A
73	4.114158	192.168.0.46	192.168.0.105	FTP	60 Request: NOOP
75	4.114320	192.168.0.105	192.168.0.46	FTP	83 Response: 200 NOOP command successful
76	4.114478	192.168.0.46	192.168.0.105	FTP	72 Request: CWD programacion
78	4.114741	192.168.0.105	192.168.0.46	FTP	82 Response: 250 CWD command successful
79	4.114888	192.168.0.46	192.168.0.105	FTP	59 Request: PWD
81	4.115094	192.168.0.105	192.168.0.46	FTP	100 Response: 257 "/programacion" is the current directory
82	4.115240	192.168.0.46	192.168.0.105	FTP	115 Request: MKD Cobian Backup 11 carpeta de pruebas-2014-12-07 17;03;22
85	4.134785	192.168.0.105	192.168.0.46	FTP	164 Response: 257 "/programacion/Cobian Backup 11 carpeta de pruebas-2014-12-07 17;03;22"
86	4.135038	192.168.0.46	192.168.0.105	FTP	115 Request: CWD Cobian Backup 11 carpeta de pruebas-2014-12-07 17;03;22
88	4.135400	192.168.0.105	192.168.0.46	FTP	82 Response: 250 CWD command successful
89	4.135561	192.168.0.46	192.168.0.105	FTP	59 Request: PWD
91	4.135978	192.168.0.105	192.168.0.46	FTP	156 Response: 257 "/programacion/Cobian Backup 11 carpeta de pruebas-2014-12-07 17;03;22"
92	4.136312	192.168.0.46	192.168.0.105	FTP	62 Request: TYPE I
94	4.136525	192.168.0.105	192.168.0.46	FTP	73 Response: 200 Type set to I
95	4.136607	192.168.0.46	192.168.0.105	FTP	60 Request: PASV
97	4.136858	192.168.0.105	192.168.0.46	FTP	104 Response: 227 Entering Passive Mode (192,168,0,105,63,31).
98	4.136919	192.168.0.46	192.168.0.105	FTP	82 Request: STOR Fichero de prueba.txt

Como podéis ver, la información viaja sin ningún tipo de codificación de un extremo a otro de la comunicación, y es más, es completamente inteligible: podemos ver cómo se conecta el usuario copias y el servidor solicita la contraseña, que es la palabra «Fichero». El servidor la acepta y le da la bienvenida, tras lo cual cambiamos al directorio «programacion», se nos listan los ficheros que contiene y finalmente enviamos el fichero «prueba.txt»

Espeluznante, ¿verdad?. Sobre todo si se trata de nuestro servidor de copias de seguridad, o de nuestro servidor de Internet y nuestra página web. Pensad de qué forma tan sencilla, cualquiera puede hacerse con el contenido de ~~un~~ vuestro servidor y borrar o modificar ~~una~~ vuestra copia de seguridad, o hackerar ~~una~~ vuestra página web.

Una fórmula matemática a tener presente siempre que os conectéis a Internet: Ftp + Ordenador = Problemas de seguridad

Pero no desesperéis. En un próximo capítulo veremos algunas soluciones que nos aportan más seguridad a la hora de conectarnos a nuestros servidores.

Bibliografía:

- Video Curso wireshark en español

- TUTORIAL WIRESHARK
- ¿Como capturar tráfico WiFi con Wireshark en Windows?