Cómo mejorar la seguridad de las transmisiones Ftp

Hace unos días os hablaba de los problemas de seguridad del protocolo FTP. Hoy veremos qué opciones tenemos para mejorar la transmisión de datos entre ordenadores.

De todo lo que podemos llegar a tener en nuestro ordenador LO MÁS IMPORTANTE es tener al menos una copia de seguridad.

Actualmente existen soluciones muy cómodas para realizar la copia de seguridad: Un disco duro externo junto con un programa de backup programable que nos permita realizar copias de forma automática a una determinada hora, es una de las soluciones más utilizadas.

Sin embargo, usando este sistema, nos podemos encontrar con sorpresas realmente desagradables. Existe una nueva generación de virus, conocidos como ransomware. Este tipo de virus se caracterizan por encriptar toda la información a la que nuestro ordenador tiene acceso y, una vez encriptada, ofrecernos la clave de desencriptación a cambio de una cantidad de dinero, vamos: secuestrarnos nuestra información y pedirnos un rescate para devolvérnosla.

Estos virus, además de encriptar nuestro disco duro, encriptarán también todos los discos externos y conexiones de red a las que tengamos acceso. En tal caso, de poco nos servirá tener una copia de seguridad, pues también estará codificada y nos será imposible recuperarla.

La solución obvia es tener una copia de seguridad en algún lugar donde el virus no tenga la posibilidad de acceder a la información. Ahí es donde entra en juego nuestro servidor FTP. Pero ya hemos visto lo fácil que resulta interceptar una conexión FTP y describir el usuario y la contraseña de acceso. Por eso es importante utilizar un protocolo de comunicaciones seguro, que impida que nuestra información sea interceptada.

La solución viene de la mano de dos sistemas muy similares al FTP tradicional. los protocolos FTPS y SFTP. Aunque ambos tienen un nombre muy similar, en realidad son completamente distintos.

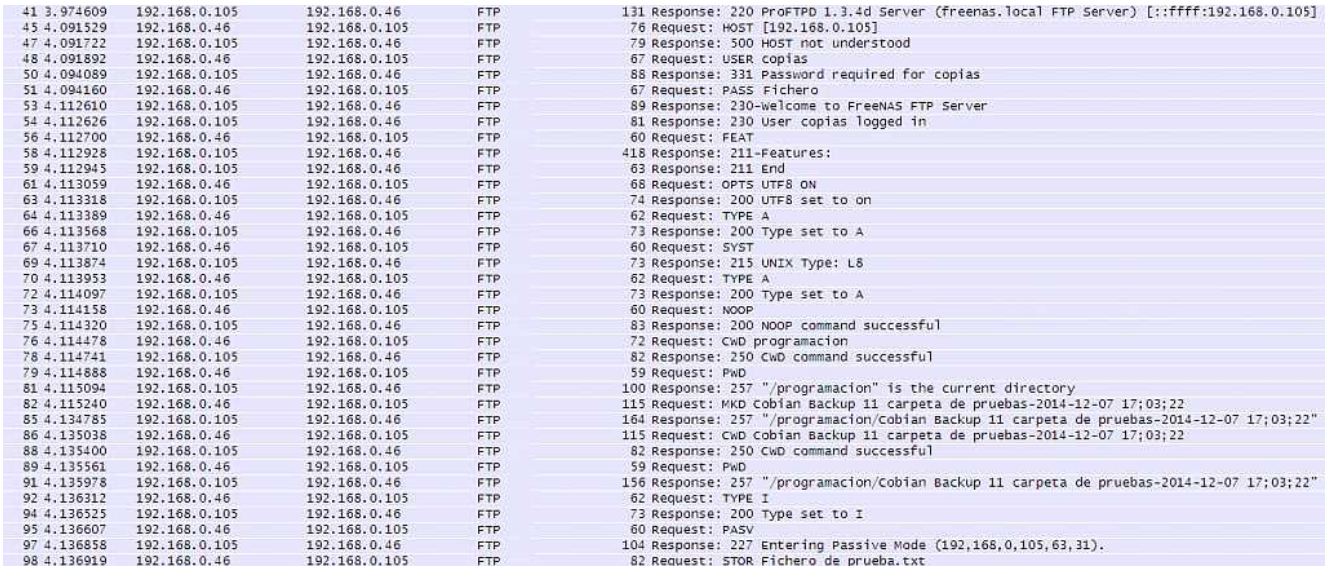
No entraremos en tecnicismos, pero sí es importante saber distinguirlos, pues el que tengan un nombre tan parecido suele hacer que se confundan los términos

– FTPS : Para entendernos, podemos decir que han cogido el protocolo FTP de siempre y le han añadido un sistema de seguridad

– SFTP: En este caso ha sido al revés, al protocolo de seguridad SSH le han añadido la capacidad de enviar y recibir ficheros.

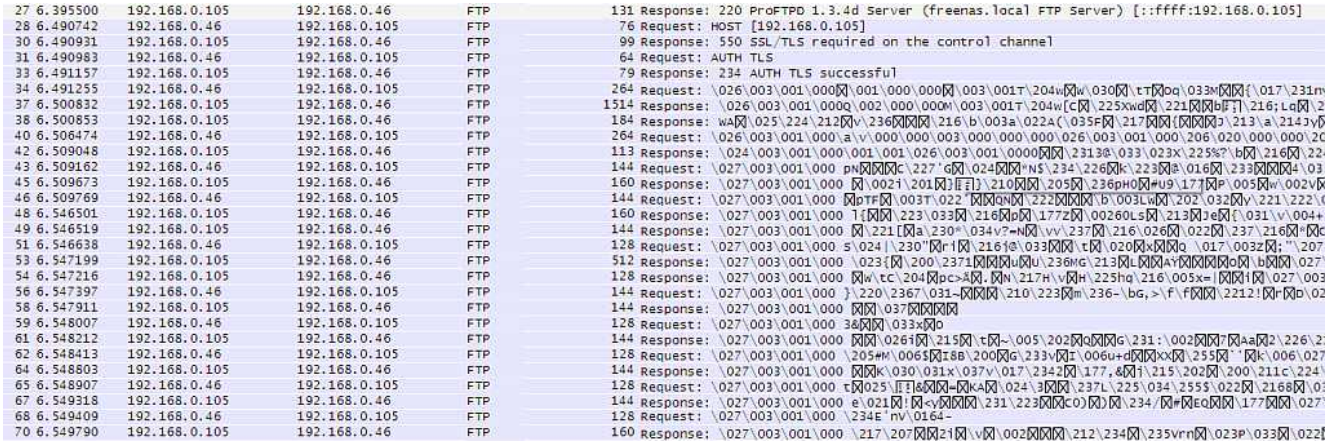
Personalmente, para realizar copias de seguridad prefiero utilizar FTPS, ya que al tratarse en realidad de una ampliación del protocolo original, en la mayoría de los casos ya viene implementado en el servidor ftp y además, suele estar soportado por todos de los programas de copias seguridad que aceptan conexiones FTP convencionales.

Para que tengáis clara la diferencia entre una conexión FTP tradicional y una conexión FTPS codificada, os vuelvo a mostrar la conexión interceptada que vimos en el artículo sobre los problemas de seguridad en FTP, y la misma conexión, pero esta vez usando FTPS



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

Usando FTP tradicional, sin encriptar



27	6.395500	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]
28	6.490742	192.168.0.46	192.168.0.105	FTP	76 Request: HOST [192.168.0.105]
30	6.490931	192.168.0.105	192.168.0.46	FTP	99 Response: 550 SSL/TLS required on the control channel
31	6.490983	192.168.0.46	192.168.0.105	FTP	64 Request: AUTH TLS
33	6.491157	192.168.0.105	192.168.0.46	FTP	79 Response: 234 AUTH TLS successful
34	6.491255	192.168.0.46	192.168.0.105	FTP	264 Request: \026\003\001\000□\001\000\000□\003\001T\204w□w\030□\tT□Oq\033M□□{\017\231m
37	6.500832	192.168.0.105	192.168.0.46	FTP	1514 Response: \026\003\001\000Q\002\000\000M\003\001T\204w[c□\225Xwd□\221□□bF]\216;Lq□\2
38	6.500853	192.168.0.105	192.168.0.46	FTP	184 Response: wA□\025\224\212□v\236□□□\216\b\003a\022A(\035F□\217□□{□□□J\213\a\214Jv□
40	6.506474	192.168.0.46	192.168.0.105	FTP	264 Request: \026\003\001\000\a\v\000\000\003\000\000\000\026\003\001\000\206\020\000\000\20
42	6.509048	192.168.0.105	192.168.0.46	FTP	113 Response: \024\003\001\000\001\001\026\003\001\0000□□\2313@\033\023X\225%?\b□\216□\22
43	6.509162	192.168.0.46	192.168.0.105	FTP	144 Request: \027\003\001\000 pN□□□c\227'G□\024□□*N$\234\226□k\223□@\016□\233□□□4\03
45	6.509673	192.168.0.105	192.168.0.46	FTP	160 Response: \027\003\001\000 □\002i\201□}[□]}\210□□\205□\236pHO□#u9\177[□P\005□w\002V□
46	6.509769	192.168.0.46	192.168.0.105	FTP	144 Request: \027\003\001\000 □pTF□\003T\022'□□QN□\222□□□\b\003LW□\202\032□v\221\222\(
48	6.546501	192.168.0.105	192.168.0.46	FTP	160 Response: \027\003\001\000 l{□□\223\033□\216□p□\177Z□\00260Ls□\213□Je□{\031\v\004+
49	6.546519	192.168.0.105	192.168.0.46	FTP	144 Response: \027\003\001\000 □\221[□a\230*\034v?=N□\vv\237□\216\026□\022□\237\216□*□
51	6.546638	192.168.0.46	192.168.0.105	FTP	128 Request: \027\003\001\000 s\024|\230"□r!□\216j@\033□□\t□\020□x□□□ \017\003Z□;"\207
53	6.547199	192.168.0.105	192.168.0.46	FTP	512 Response: \027\003\001\000 \023{□\200\2371□□□u□U\236MG\213□L□□AY□□□□o□\b□□\027
54	6.547216	192.168.0.105	192.168.0.46	FTP	128 Response: \027\003\001\000 □w\tC\204□pc>A□.□N\217H\v□H\225hq\216\005x=|□□!□\027\003
56	6.547397	192.168.0.46	192.168.0.105	FTP	144 Request: \027\003\001\000 }\220\2367\031~□□□\210\223□m\236-\bG,>\f\f□□\2212!□r□b\02
58	6.547911	192.168.0.105	192.168.0.46	FTP	144 Response: \027\003\001\000 □□\037□□□□
59	6.548007	192.168.0.46	192.168.0.105	FTP	128 Request: \027\003\001\000 3&□□\033x□o
61	6.548212	192.168.0.105	192.168.0.46	FTP	144 Response: \027\003\001\000 □□\026i□\215□\t□~\005\202□q□□G\231:\002□□7□Aa□2\226\2
62	6.548413	192.168.0.46	192.168.0.105	FTP	128 Request: \027\003\001\000 \205#M\006$□I8B\200□G\233v□I\006u+d□□XX□\255□``□k\006\027
64	6.548803	192.168.0.105	192.168.0.46	FTP	144 Response: \027\003\001\000 □□K\030\031x\037v\017\2342□\177,&□1\215\202□\200\211c\224\
65	6.548907	192.168.0.46	192.168.0.105	FTP	128 Request: \027\003\001\000 t□025\[□]&□□=□KA□\024\3□□\237L\225\034\255$\022□\2168□\0
67	6.549318	192.168.0.105	192.168.0.46	FTP	144 Response: \027\003\001\000 e\021□!□<y□□□\231\223□□CO)□)□\234/□#□EQ□□\177□□\027
68	6.549409	192.168.0.46	192.168.0.105	FTP	128 Request: \027\003\001\000 \234E'nV\0164-
70	6.549790	192.168.0.105	192.168.0.46	FTP	160 Response: \027\003\001\000 \217\207□□21□\v□\002□□□\212\234□\235Vrn□\023P\033□\022[

Usando Ftps

Como podéis ver, en la conexión FTPS resulta imposible extraer ningún dato relevante, siendo, esta sí, una conexión realmente segura para la transmisión de datos.

En un próximo artículo veremos cómo configurar nuestro propio servidor FTPS utilizando el sistema operativo FreeNAS.