DuckDns: Un sencillo gestor de Dns dinámicas

¿Necesitas acceder a tu ordenador a través de Internet y tienes una Ip dinámica?

La solución es DuckDns.org: rápido, sencillo y gratis.

Todos los dispositivos conectados directamente a internet tienen asociada una dirección ip que los identifica dentro de la red. Esta dirección ip se compone de cuatro grupos de números, del 0 al 255. Simplificando mucho, podríamos comparar nuestra dirección Ip con un número de teléfono: Para que nuestro teléfono funcione y podamos hacer y recibir llamadas necesitamos disponer de un número de teléfono. En internet el concepto es el mismo: Para poder enviar y recibir datos necesitamos disponer de una dirección IP asignada. Si quieres conocer tu dirección ip, puedes consultar la página web www.cualesmiip.com.

Actualmente, al contratar nuestro servicio de internet (adsl, fibra, móvil, etc..) esta dirección ip es dinámica, esto es, que el número que se nos asigna puede cambiar en cualquier momento, de acuerdo a las necesidades de nuestro proveedor de internet.

Normalmente esto es algo que no afecta a un usuario medio de internet, pero las ip dinámicas suponen un problema a la hora de intentar acceder a los datos de nuestros ordenadores desde fuera de nuestra red interna. Imaginad que tenemos instalado un servidor de ficheros en nuestro ordenador al que queremos acceder desde nuestro móvil cuando estamos fuera de casa, o tenemos una cámara de vigilancia en nuestra tienda a la que queremos acceder desde casa para asegurarnos de que todo va bien. Al ser dinámica, nuestra dirección Ip puede haber cambiado, con lo cual literalmente no sabremos dónde conectarnos. Siguiendo con el ejemplo anterior, es como si de repente nos cambiaran el número de teléfono.

Para solucionarlo tenemos dos opciones: contratar una dirección Ip fija, con lo que nuestro proveedor de internet a cambio de una cuota mensual nos asegurar que nuestra dirección será siempre la misma, o utilizar un servidor de Dns dinámicas.

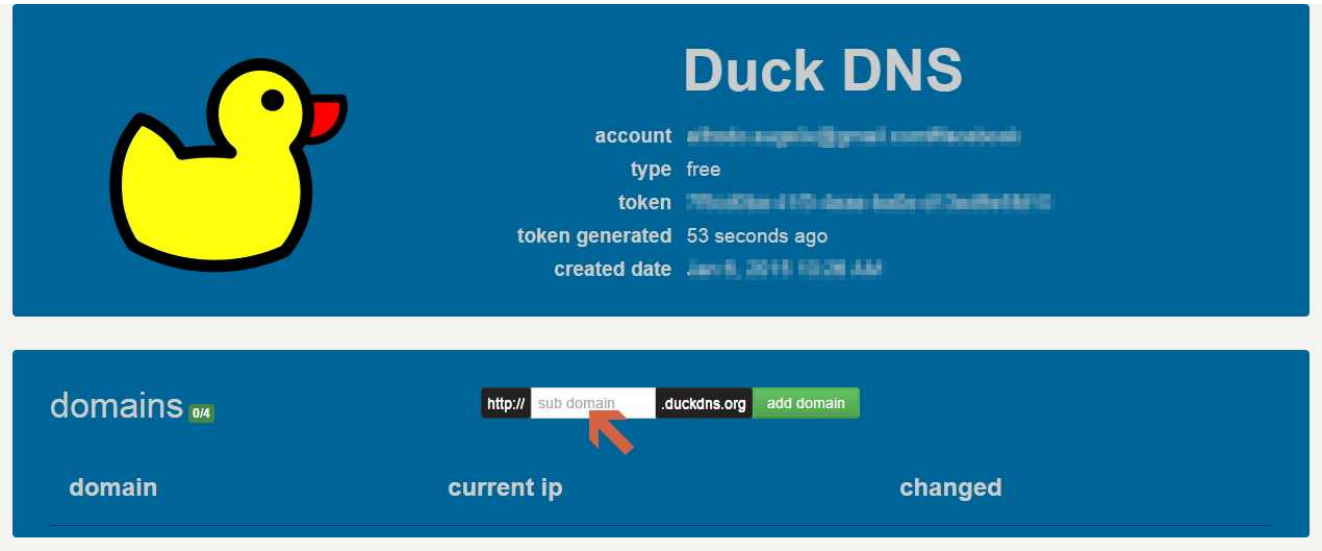
Los servidores de Dns dinámicas nos permiten asociar nuestra dirección Ip a un nombre de internet. El servidor de Dns dinámicas se encargará de actualizar la información, de tal forma que el nuestro nombre siempre esté apuntando a nuestra dirección Ip.

Hay muchos servidores DDns, pero hoy os voy a hablar de uno que he descubierto recientemente y que me ha gustado desde el primer momento. Se trata de DuckDns.org

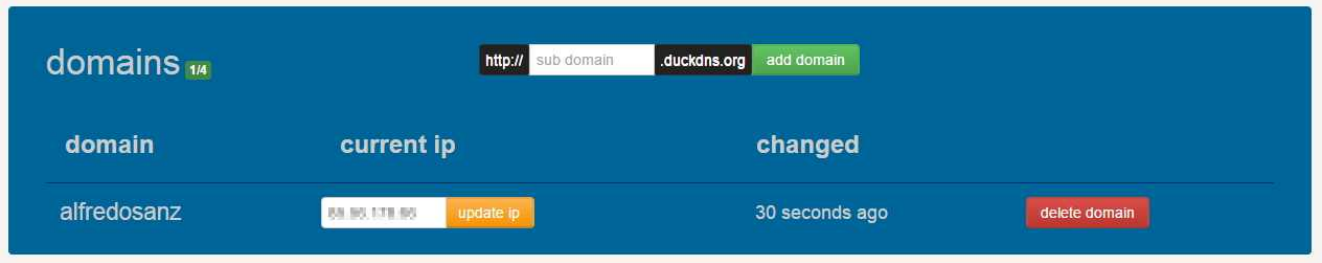
DuckDns.org es un servidor de DDns gratuito y que nos permite asignar nombres del tipo minombre.duckdns.org

Para crear nuestra dirección DDns, tan sólo tenemos que acceder a su página web en DuckDns.org y validarnos con nuestra cuenta de usuario en google, facebook o Twitter.

Una vez validados, nos aparecerá la siguiente pantalla, en la que sólo tenemos que indicar el nombre que queramos para nuestro subdomino DDns.



A continuación pulsamos «add domain» y si el nombre no ha sido registrado por nadie previamente, ya tenemos nuestra dirección DDns creada.



En este caso, hemos creado la dirección alfredosanz.duckdns.org, de tal forma que siempre que acceda a alfredosanz.duckdns.org, en realidad estaré accediendo al router de mi conexión a Internet.

Ahora sólo nos queda el último paso, que es automatizar el cambio de dirección Ip.

Para ello nos vamos al menú que encontraremos en la parte superior de la página web de duckdns y seleccionamos la opción «install». En ella seleccionaremos nuestro sistema operativo y el nombre de dominio para que que queremos las instrucciones y ¡listo!. Si tu nivel de informática no es muy alto y estás usando Windows, selecciona el botón «Windows-gui», que es el más fácil de instalar y configurar.

En resumen: Una herramienta para generar DDns muy sencilla, válida para gran cantidad de sistemas operativos ¡ si hasta tiene cliente para android! , y además gratis.

Cómo enviar ficheros de gran tamaño por email

A todos nos ha pasado alguna vez. Intentamos mandar un fichero de gran tamaño por email y resulta que o bien es demasiado grande para nuestro servicio de email, o bien la cuenta del destinatario está saturada y no tiene espacio suficiente para almacenarlo. Si usamos GMail o Hotmail podemos enviarlo a través de sus servicios de almacenamiento en la nube, pero hoy os voy a mostrar una solución mucho más simple:

Se trata de wetransfer.com y es una web especializada en este tipo de envíos.

Tan solo tenéis que acceder a su página web, y tras aceptar el

inevitable paso de aceptar sus condiciones de uso, veremos un cuadro en la parte izquierda de la página donde sólo tenemos que rellenar los datos correspondientes: fichero o ficheros a enviar, email del destinatario, email del remitente y un pequeño texto para adjuntar al email. Tras completarlos, pulsamos el botón «tranferencia» y ¡ya está!. Sin más complicaciones.

El destinatario recibirá un correo con el texto del mensaje y un botón para la descarga de los archivos adjuntos. Si has adjuntado varios ficheros en el envío (fotos, etc..), el destinatario recibirá un fichero comprimido .zip con todos los adjuntos.

En lugar de enviar el fichero por email, también podemos obtener un enlace de descarga del tipo http://we.tl/Bqkdoo si lo que queremos es compartirlo en redes sociales o mandarlo a muchas personal.

Las únicas limitaciones del servicio gratuito son el límite de los ficheros adjuntos, hasta 2 Gb en cada envío y que el fichero estará disponible para descarga durante 7 días, pasados los cualeso se borrará de forma automática.

Tienen también una versión de pago que te permite adjuntar hasta 10 Gb por envío y permite almacenar los ficheros indefinidamente , pero el precio (10€ mensuales) me parece demasiado elevado para las pocas veces que se nos puede dar tener que enviar más de 2Gb.

En resumen: Un servicio limpio, y sobre todo muy muy sencillo de usar, en el que ni siquiera tienes que darte de alta para empezar a enviar ficheros.

¡Ah!. Y, por supuesto, tenemos disponebles versiones tanto para Iphone como para Android

Lastpass: La última contraseña que tendrás que recordar.

La gestión de nuestras claves de acceso personales en internet se ha convertido en un verdadero quebradero de cabeza para todos los usuarios que estamos mínimamente preocupados por nuestra seguridad en La Red. Todos sabemos que hemos de tener una contraseña distinta para cada sitio, y que han de ser difíciles de deducir (nada de cumpleaños, 1234, etc…).

Pero entonces…. ¿Cómo hacemos para recordar docenas de contraseñas?.

¡LassPast tiene la solución!

LastPass es un servicio web encargado de administrar todas nuestras contraseñas de acceso a las distintas páginas web en las que estamos registrados.

Por supuesto, toda la información almacenada es codificada antes de abandonar nuestro ordenador, lo cual hace prácticamente imposible una fuga de seguridad de nuestros datos.

Su uso es realmente sencillo. Tan solo tenemos que instalar el programa desde su página web y el conector correspondiente de nuestro navegador. Así, una vez identificados con nuestro usuario y contraseña le LastPass, cada vez que accedamos por primera vez a una página donde se nos pidan nuestros datos de acceso, LastPast nos mostrará un mensaje indicando si queremos guardar los datos de identificación. Si le decimos que los guarde, la próxima vez que accedamos a este sitio, nuestros datos de usuario y contraseña aparecerán rellenados automáticamente.

Una de las grandes ventajas de LastPass es que si accedemos a un mismo sitio con varias cuentas de usuario, guarda todas las claves de cada cuenta y al acceder nos muestra un menú desplegable con todas ellas para poder elegir. Por ejemplo: Yo administro unas 20 cuentas de correo de gmail. Imaginaos: Si me cuesta recordar todas las direcciones de email que administro, ¡Como para recordar sus contraseñas!. Antes, no tenía más remedio que simplificarlo usando la misma contraseña para todas, con el riesgo de seguridad que ello suponía. Ahora, con LastPass, tan solo tengo que elegir de la lista de cuentas de gmail aquella a la que quiero entrar.

Ademas, dado que no tenemos que recordar las contraseñas, podemos usar contraseñas desectructuradas, del tipo «34=^q99». El propio LastPass tiene una utilidad en la que le decimos la longitud que queremos para nuestra contraseña y el tipo de caracteres a utilizar y él solito nos genera la nueva contraseña.

Otras opciones interesantes son:

– Registro de acceso a cada web, indicando la fecha y hora de

la última vez que hemos accedido a cada sitio.

– Posibilidad de agrupar las contraseñas en carpetas

– Creación de notas seguras, esto es, información que nos son contraseñas de acceso pero que queremos guardar en un lugar seguro. Podemos almacenar tanto texto como imágenes (nº póliza del seguro, fotocopia DNI, etc…).

– Almacén de formularios: Podemos crear un formulario, por ejemplo, con nuestro nombre, dirección, teléfono, etc… y utilizarlo posteriormente cuando se nos soliciten estos datos.

– Compartir contraseñas: Esta opción es muy interesante ya que nos permite compartir el acceso a un sitio web con otros usuarios de LastPass, pero sin necesidad de darles la contraseña de acceso, de tal forma que en cualquier momento podemos anularlo y el otro usuario dejará de tener acceso a la web.

LastPass está disponible en versión gratuita, que permite el acceso a través de página web, y en versión de pago (10€ año), que además permite el acceso a través de teléfonos móviles.

En resumen: Una herramienta imprescindible para poner un cierto orden en el caótico mundo de las contraseñas personales.

Patrocinado por dcalidad.com

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

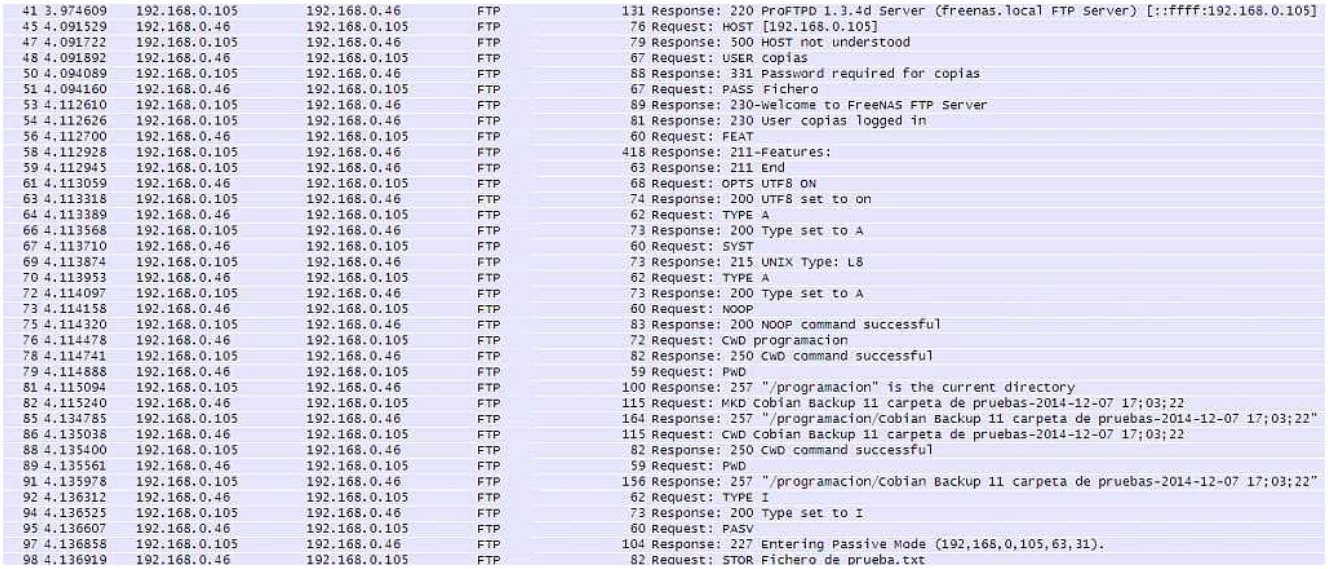
– FTPS : Para entendernos, podemos decir que han cogido el protocolo FTP de siempre y le han añadido un sistema de seguridad

– 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

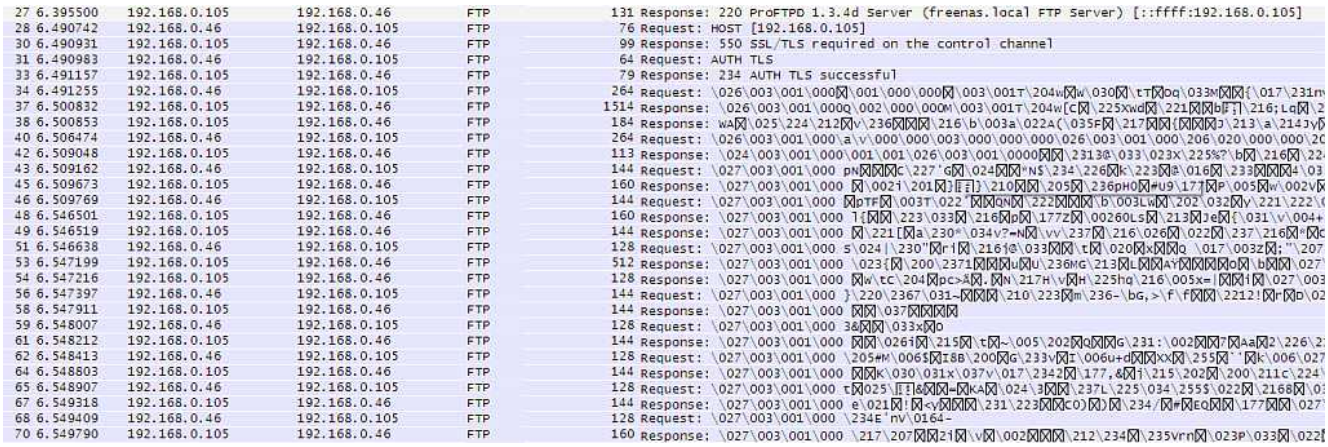
soportado por todos de los programas de copias seguridad que aceptan conexiones FTP convencionales.

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\231n
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 b \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 1 \223\033 \216p \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" r1 \216j@\033 \t \020 x q \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 A Y 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=| i \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 D\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,& i\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 ! <v 231\223 C0) 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 2i \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.

Cómo prevenir el robo de datos en internet

KeyScrambler

Hoy os hablaré de uno de los problemas de seguridad más serios de internet: El robo de nuestra información personal y la suplantación de identidad.

Pero empecemos con un poquito de humor.

Sofocleto decía en sus sinlogismos: La ignorancia consiste en saberlo todo, pero de otro modo.

Por desgracia, en internet, la ignorancia puede salirnos muy cara. Cada día es más frecuente recurrir a internet para realizar compras, consultar nuestros datos bancarios,

comunicarnos con la administración, etc..

Y, a pesar de que mucha gente ya está utilizando las nuevas tecnologías para realizar estos trámites, pocos siguen unas mínimas normas de seguridad para evitar posibles problemas.

A nadie se nos ocurría salir a la calle con 100.00 € y llevarlos colgados de la mano en una bolsa trasparente ¿verdad?. Pues mucha gente, sin saberlo, está haciendo eso mismo en internet.

Para hacerse con nuestros datos, los hacker se sirven de unos programas llamados keylogger , que son un tipo de programa espía cuya función es capturar las pulsaciones de nuestro teclado y guardar esa informa en ficheros de texto que son enviados al hacker en cuestión.

Estos programas maliciosos suelen llegar a nuestro ordenador «disfrazados» de programas que hacen otras cosas o «escondidos» dentro de un correo electrónico o de un programa pirata. Esta habilidad que tienen de esconderse dentro de otra cosa hace que también se les suela conocer con el nombre de troyanos

De este modo, una vez infectado nuestro ordenador con este tipo de virus, TODO lo que escribamos (cartas, correos, claves del banco, contraseñas, cuentas corrientes, etc… pasará a estar en poder del hacker que ha diseñado el programa espía, quien podrá usar tranquilamente la información robada.

Si, por ejemplo, accedemos a nuestra cuenta bancaria, la persona que ha interceptado nuestras comunicaciones recibirá algo como esto:

http://www.santander.com/cuentasbanco <enter >alfredo <enter> Arc45T44 <enter>

La página web del banco, vuestro nombre de usuario y vuestra contraseña. Ni mas ni menos. Y da igual si el banco tiene una

página web con conexión segura, o si codifica los datos antes de enviarlos. El virus actúa ANTES de que entren en funcionamiento estas medidas de seguridad, así que resultan ineficaces.

Pero no nos pongamos paranoicos, por suerte contamos con algunas herramientas para neutralizar este tipo de virus.

La más conocida de todas es KeyScramble, de QxfSoftware.

Keyscramble se encarga de encriptar todas las pulsaciones del teclado a nivel interno de windows, de manera que cuando la información es capturada por el key logger ya se encuentra encriptada. Posteriormente, cuando los datos llegan a la aplicación, se desencriptan, quedando así a salvo de miradas indiscretas.

Existen tres versiones distintas del programa:

– Gratuita: Sólo es capaz de proteger los datos enviados los navegadorer web más utilizados (explorer, chrome, firefox, safari, etc…). Esta versión cubre los niveles mínimos de seguridad para cualquier usuario, ya que nos protegerá de cualquier intento de acceder a nuestra información cuando usamos la página web de una tienda online, nuestro banco, etc…

– Profesional: También nos protege cuando utilizamos otro tipo de programas que no son un navegador web, como programas gestores de contraseñas, email, editores de texto, etc… Tiene un precio de $29.99 y se puede instalar en 3 ordenadores

– Premium: Además de todos los programa anteriores, protege también software financiero, Dropbox, Google drive, el explorador de archivos de Windows, etc… Tiene un precio de $44.99 y se puede instalar también en 3 ordenadores.

En resumen: cuando menos, todos deberíamos tener instalada al menos la versión gratuita. Las otras dos versiones también son recomendables y como podéis ver, tampoco tienen un precio

demasiado elevado, sobre todo si podéis aprovechar la licencia múltiple; ya que en ese caso la versión premium os saldrá a menos de 15 euros por ordenador.

Como todo en esta vida, nada es infalible, y aún contando con estas herramientas podemos estar en peligro, pero al menos no saldremos a la calle con el dinero en una bolsa trasparente.

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).

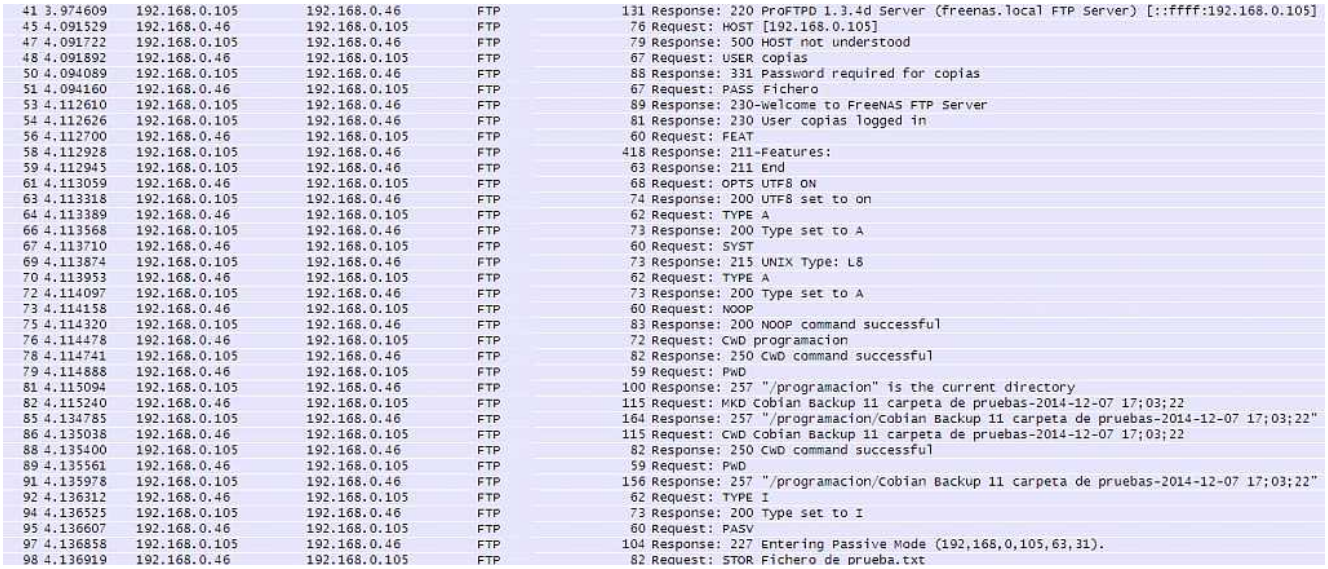
Actualmente, utilizar Ftp tanto en Internet para el envío de archivos y páginas web como internamente para conectarnos a un servidor propio y almacenar, por ejemplo, una copia de seguridad de nuestros archivos en nuestra intranet local, ha de considerarse un potencial problema de seguridad, ya que toda 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?