PENTESTING

Y

SEGURIDAD

AUTOR: Darwin Silva TWITTER: @SECURITY_ZERO

Team: ROMEO Q

ZERO

Nota del Autor:

Mi nombre es Darwin Alexander Silva Pérez (zero) soy el autor de esta revista.

Mi facebook asi como twitter, correo y canal de youtube.

https://www.facebook.com/dawin.silva.3

@security_zero

http://www.youtube.com/user/zerndate

Portada: Darwin Alexander Silva Pérez

correo: zerndate@gmail.com

Tomo numero : 2°

Hecho con Software Libre:

• Kali linux
• LibreOffice 4.0.2.2

INDICE

Pharming

Bueno un saludo a todos los que me leen xd bueno vamos ya de lleno con lo que nos interesa el pentesting y seguridad el primer tomo vimos teoria y un poco de practica con sqlmap esta ves vamos mas de lleno asi que empezemos.

El pharming es una modalidad de ataque utilizada por los atacantes, que consiste en suplantar al Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducirte a una página Web falsa. El atacante logra hacer esto al alterar el proceso de traducción entre la URL de una página y su dirección IP.

Comúnmente el atacante realiza el redireccionamiento a las páginas web falsas a través de código malicioso. De esta forma, cuando se introduce un determinado nombre de dominio que haya sido cambiado, por ejemplo http://www.0byt3s.org en tu explorador de Internet, accederá a la página Web que el atacante haya especificado para ese nombre de dominio.

Una técnica muy utilizada para realizar éste tipo de ataque es a través del envío masivo de correos electrónicos. El correo electrónico puede provenir de distintas fuentes, las cuales, resultan llamativas para el usuario; algunos de los principales temas que se utilizan son los siguientes:

- Noticias falsas o amarillistas.

  En este tipo de correos los intrusos crean una noticia llamativa y, en la mayoría de las ocasiones, utilizan un tema actual y de interés general para la sociedad.

- Envío de tarjetas postales electrónicas.

  En este caso, el intruso enviará un correo invitando al usuario a abrir una postal que supuestamente le ha enviado un amigo.

- Supuesta obtención de algún premio.

  Estos correos intentan engañar al usuario diciéndole que ha sido ganador de algún premio: viaje, dinero en efectivo, autos, etcétera.

- Supuestos boletines informativos de una institución pública o privada.

  Los intrusos que utilizan este tipo de temas invitan al usuario al usuario a descargar un archivo o visitar una página que supuestamente contiene un "boletín" o archivo elaborado por alguna institución reconocida y de confianza para la sociedad.

Que la gran mayoria ya sabe auque no participes en nada si una web o correo te dice ganaste un premio te emosionas y chalan te clikeas algo y infectado.

Esta técnica de ataque a su vez tiene tres variantes conocidas:

Pharming local:

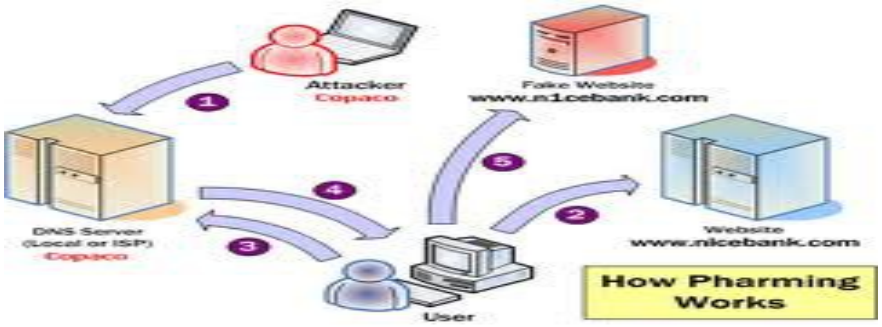
El que se logra al introducir un troyano o virus en el equipo de la víctima, el cual se encarga de alterar los registros de nombres que se encuentran el el archivo "hosts" (sin extensión) que se ubica en diferentes direcciones dependiendo del sistema operativo de la víctima. Se denomina local porque el ataque se realiza en el equipo del usuario. Aquí es precisamente donde el proceso se parece más al phishing debido a que los usuarios se infectan uno a la vez y el término de "granja" pierde sentido.

Drive-By Pharming:

Este se realiza atacando directamente a los firewalls o routers (enrutadores), y cambiando la dirección del servidor DNS a la de un servidor DNS bajo poder del hacker, que indudablemente resolverá las direcciones tal como éste lo desee. Esta técnica hasta hace poco era utilizada solo para propósito académico debido a la dificultad que existe para acceder a los routers empresariales, sin embargo ha cobrado auge en la actualidad debido a las plataformas wireless que en muchos casos utilizan enrutadores cuyos usuarios no han cambiado la clave administrativa que traen estos equipos por defecto.

DNS Poisoning (Envenenamiento de DNS):

Aunque esta técnica es bastante difícil de ejecutar, se basa en vulnerabilidades de los servidores DNS en lo que respecta al control de su caché de direcciones. Aunque es muy peligrosa actualmente son muy pocos los casos, debido a que los servicios de DNS de gran escala están en manos de proveedores de Internet que ya han corregido este tipo de fallas. Sin embargo sigue latente la posibilidad de que se descubra alguna nueva vulnerabilidad que permita este tipo de ataque nuevamente.



Mi video demostrando el pharming------>http://www.youtube.com/watch?v=Iwm1mfLGEls

Bien ahora a mostrar unas cosillas el code que mandariamos a la victima es el siguiente lo podemos hacer en notepad o regedit.

La ip 65.55.129.167 es donde mandaran a la victima al momento ella de poner una web cualquiera en el navegador esa ip podemos poner la ip de nuestro phishing digamos de un banco por ejemplo para carding.

Donde dice facebook es donde la victima queria entrar podemos suponerlo por que solo alli vive la gente, pero en fin cambiamos la url de facebook por la del banco a suplantar o otra web que queramos suplantar.

Al final se guarda el archivo con extension .bat y lo mandan a otra persona diciendo algo de que hace mas rapido la pc o que se yo usen la imaginacion o para que no sospechen pueden convertir el .bat en .exe con unos programas para eso en google pueden encontrar algunos con una simple busqueda cabe destacar que este metodo es para pcs windows tambien hay para linux.

En resumen este metodo es para redireccionar a la victima de una web determinada a otra que nosotros queramos mandarle espero les guste y practiquen pero no lo usen para el mal recuerda:

Aprende practicando y para aprender,no aprendas para dañar.

Grampus Forense

Bueno este tema es para los que buscan mucho la famoso foca de informatica64 no lo niego foca es una gran herramienta de analisis de metadatos yo mismo la he usado bastante y pues trabaja como debe en windows pero si eres amante del software libre (gnu/linux) sabras que hay un monton de pasos para instalarlo sobre todo buscar cada dll de foca ademas que es privativo pues ya no busqueis mas con grampus forense podemos hacer analisis de metadatos.

Para el que no sepa que es un metadato:Metadatos (del griego *μετα*, *meta*, 'después de, más allá de'1 y latín *datum*, 'lo que se da', «dato»2), literalmente «sobre datos», son datos que describen otros datos. En general, un grupo de metadatos se refiere a un grupo de datos, llamado *recurso*. El concepto de metadatos es análogo al uso de índices para localizar objetos en vez de datos. Por ejemplo, en una biblioteca se usan fichas que especifican autores, títulos, casas editoriales y lugares para buscar libros. Así, los metadatos ayudan a ubicar datos.

Al leer notaras y tienes razon me copie la definición de metadatos de la wikipedia pero era necesario pues ahora que ya seguro la leiste te lo simplificare de esta manera cada ves que tomas una foto,video o creas un pdf etc... se crean datos aveces visibles otras oculto de hora,dia,dispositivo desde el cual se realizo o creo dicho archivo eso es metadatos una data base del archivo pequeña pues como esto es pentesting y seguridad sabran que con estos datos un atacante puede empezar a realizar un test sobre tu informacion,posibles password, users etc.. así que debemos eliminarlos por nuestra seguridad.

Grampus Project nace para todos aquellos usuarios que necesitan automatizar sus procesos en auditorias web.

Como sabemos la recopilación de información a la hora de realizar un ataque a un objetivo es esencial y a veces este proceso puede ser muy largo y pesado.

Fear the FOCA, de Chema Alonso y su equipo, cubre las necesidades de automatización que necesitamos a la hora del proceso de Fingerprinting y la extracción y el análisis de metadatos lo que no cubre es algo para muchos esencial, la cómoda multiplataforma.

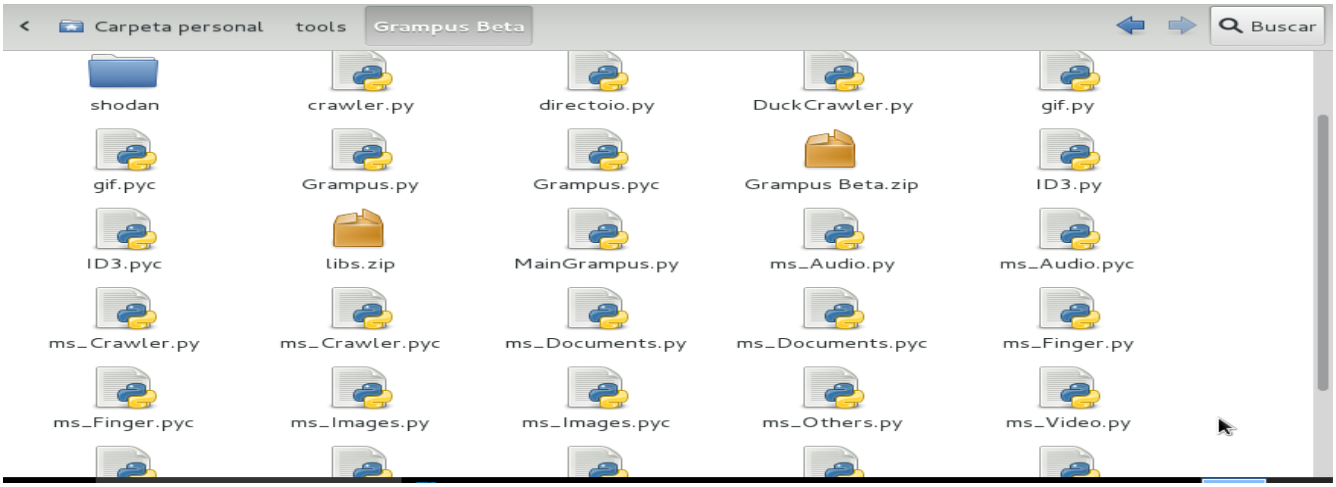
Muchos somos usuarios Linux y nos resulta complicado tener que rompernos el coco para emularlo con WINE o incluso virtualizarlo en una maquina virtual con entorno Windows...

Grampus es una herramienta multiplataforma de extracción de metadatos y Footprinting, algo así como una FOCA en Python y de código abierto. Desde haces meses The_Pr0ph3t y SankoSK y otros desarrolladores como sniferl4bs, don_once, OverxFlow o Kodeinfect han estado trabajando duramente para por fin publicar la versión beta.

Vamos esta url y nos la bajamos –-----> https://bitbucket.org/grampusteam/grampus/downloads

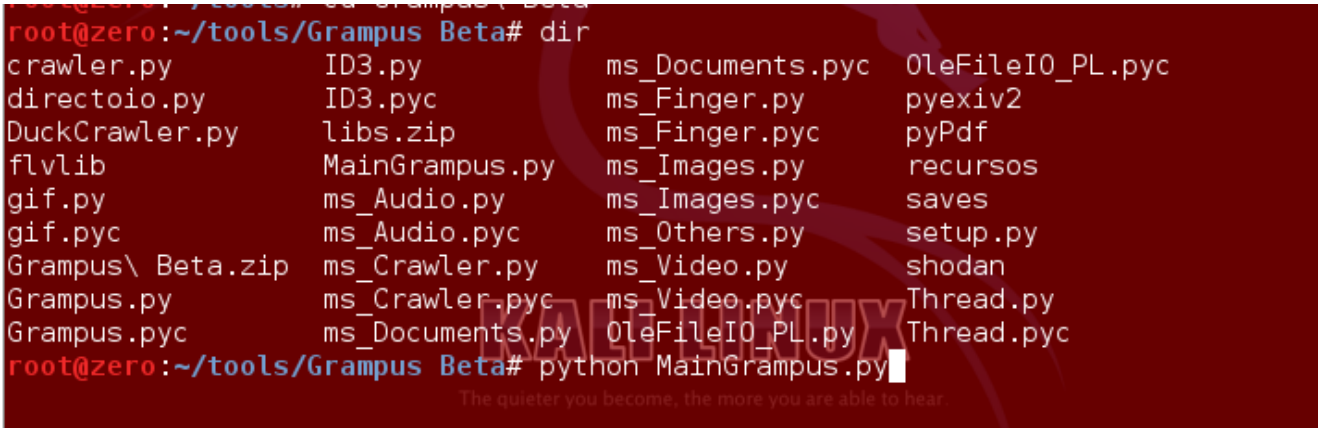
Bueno despues de descargarla la descomprimimos en el directorio que gustemos,tambien descomprimimos un zip de nombre libs estan quedaran dentro de una carpeta pues sacamos todo lo de la carpeta y pegamos junto con todos los demas archivos.

La carpeta libs tiene el archivo ID3.py entre otros al sacar todo nos quedara así.



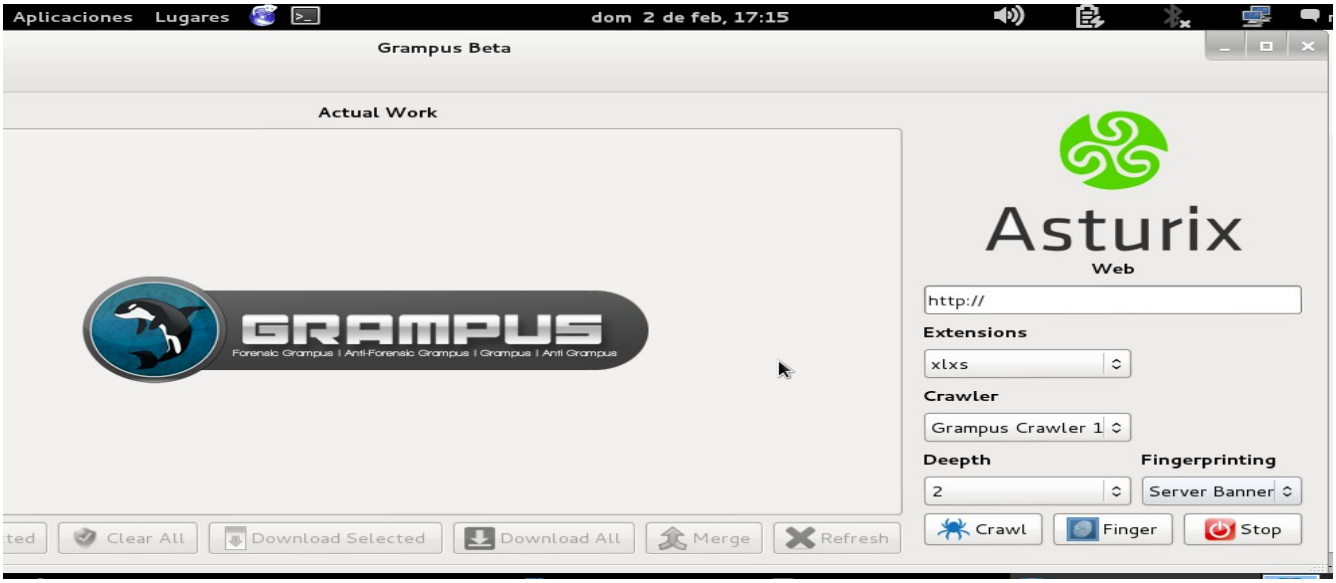
Marcamos todo,vamos a propiedades y damos todos los permisos de ejecucion necesario ahora abrimos nuestra terminal entramos al directorio donde esten los archivos y escribimos:

python MainGrampus.py y damos enter nos aparece su version visual.



Al ejecutarlo nos saldra asi solo vamos a abrir y escojemos 3 opciones: file para doc y pdfs; url para analizar una web y directory para analizar un directorio completo de la computadora.

En la opcion url nos apareceran mas opciones como que tipo de analis queremos pausarlo continuar y otras funciones que podemos experimentar y probar según probemos la herramienta como ven es lo mismo que foca y de software libre solo lo abrimos desde terminal y listo.



Recuerden esta en su version beta si encontraran alguna falla pueden informarla en su web oficial que es la misma donde descargan la tools y si saben python pueden modificarla a sus gustos pero pidiendo su debido permiso a sus creadores.

Asi que hasta la promima foca y bienvenida orca a menos que uses windows sigue probando foca que igual recomiendo es una gran tool tanto la version free,paga y la evil foca.

Aunque igual pueden correr grampus en windows solo instalando el IDE DE python en windows.

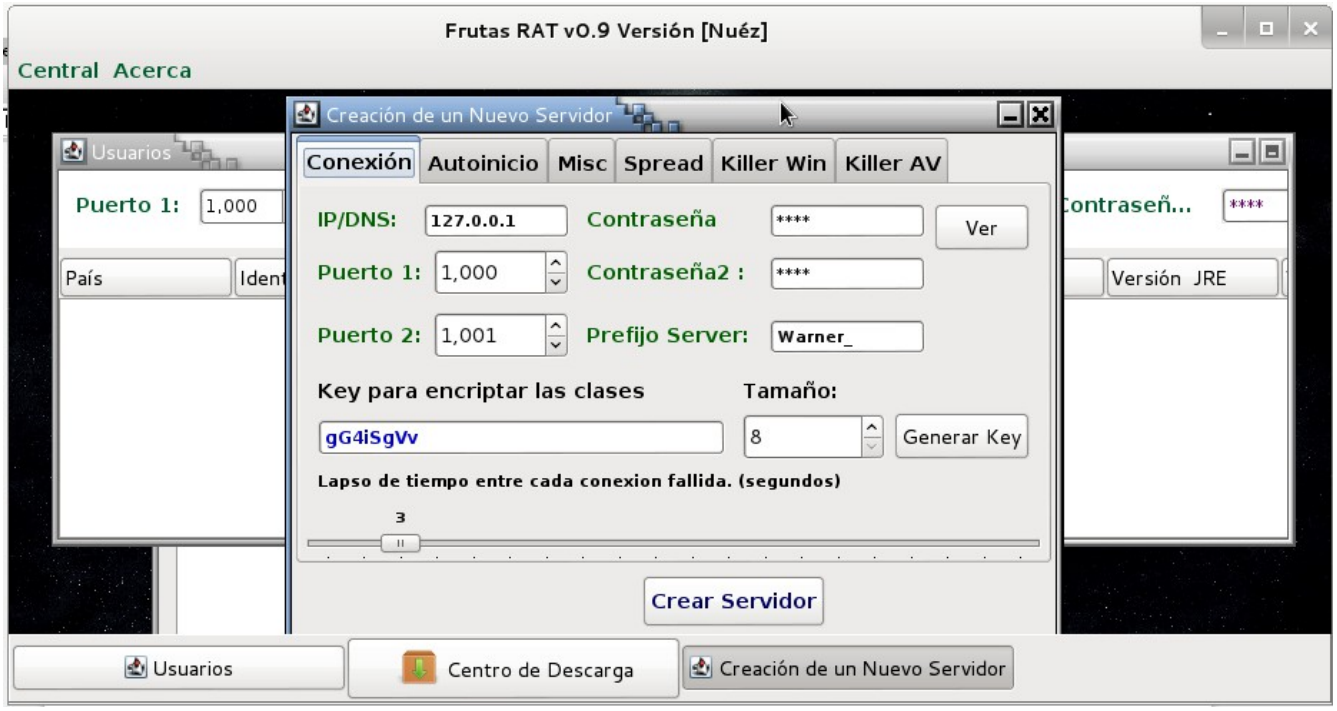
Primer troyano con frutas rat

Descargar frutas rat –----------> http://www.sendspace.com/file/13x5x8

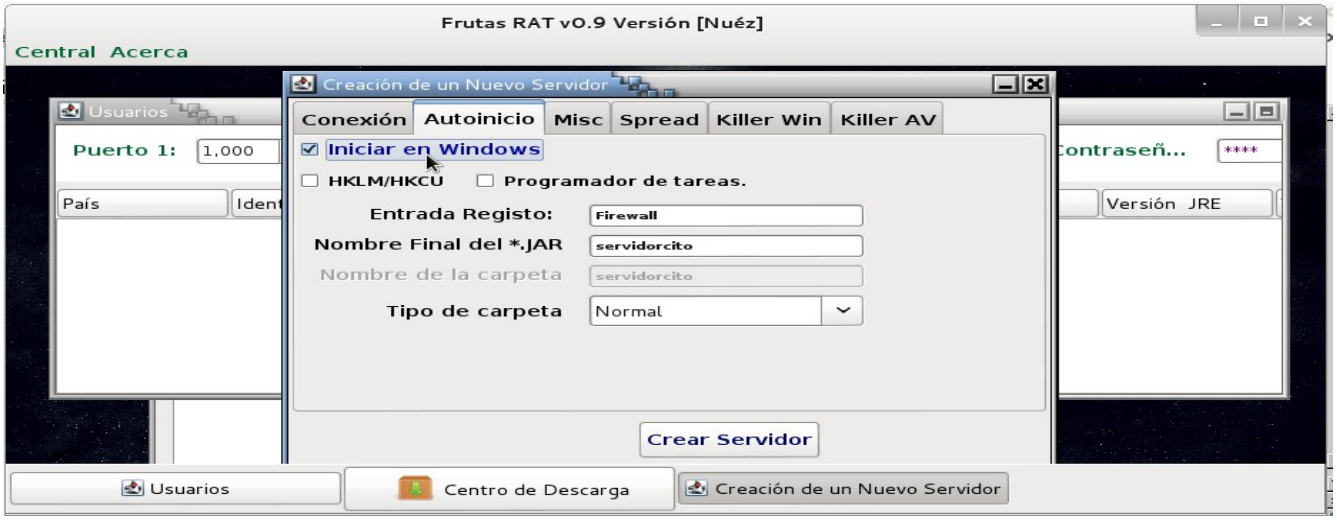
En resumen este es un Rat (remote administration tool) o herramienta de administracion remota este esta creado en java y su version mas reciente nos permite hasta encriptar el rat que hallamos creado pero no alarguemos esto mas y empezemos.

Tras abrir o ejecutar el frutas rat nos aparecera esto.

Vamos a la pestaña Central y damos a nuevo servidor nos saldra esto.



Aca configuramos los datos ip/dns es nuestra ip ojo debe ser ip estatica si es dinamica podemos poner un dns que tengamos en un servidor local o con no-ip,contraseña ponemos la que queramos luego los puertos tambien ponemos lo que gustemos los recomendados son 8483-8384 respectivamente puerto 1 y puerto 2,pestaña tamaño 8 es el tamoño de encriptacion para mas precaucion lo detecte un AV ponemos el maximo 30 y damos a generar key.



Esta pestaña marcamos autoinicio para que encienda junto a la pc aveces esto puede ser un punto debil si alguien analiza sus procesos de inicio se dara cuenta que inicia el frutas rat, nombre final de .jar es como se llamara el jar infectado podemos ponerle el nombre que queramos según la victima; las otras opciones son sencillas, matar procesos de windows,matar AV etc... luego damos solo a crear servidor especificamos la ruta donde se guardara y guardar y ya esta solo enviarlo a la victima que lo ejecute y listo incluso recuerden los .jar podemos hacerlos .apk para los celulares android yo probe en un android ice cream sanwich y funciona no se en otras versiones.

Famosos bitcoins

Bitcoin es una moneda, como el euro o el dólar estadounidense, que sirve para intercambiar bienes y servicios. Sin embargo, a diferencia de otras monedas,Bitcoin es una divisa electrónica que presenta novedosas características y destaca por su eficiencia, seguridad y facilidad de intercambio.

Veamos algunas de estas características:

- No pertenece a ningún Estado o país y puede usarse en todo el mundo por igual.
- Está descentralizada: no es controlada por ningún Estado, banco, institución financiera o empresa.
- Es imposible su falsificación o duplicación gracias a un sofisticado sistema criptográfico.
- No hay intermediarios: Las transacciones se hacen directamente de persona a persona.
- Las transacciones son irreversibles.
- Puedes cambiar bitcoins a euros u otras divisas y viceversa, como cualquier moneda.
- No es necesario revelar tu identidad al hacer negocios y preserva tu privacidad.
- El dinero te pertenece al 100%; no puede ser intervenido por nadie ni las cuentas pueden ser congeladas.

Tus bitcoins son sólo tuyos.

El sistema descentralizado de seguridad que hay detrás Bitcoin hace imposible que cualquier otra persona que no disponga de tus credenciales pueda acceder a tu dinero. Tus bitcoins son tuyos y no pueden ser congelados o secuestrados, no se puede cerrar ninguna cuenta y sólo tú tienes acceso a ellos las 24 horas del día, 365 días al año. Este aspecto es para muchas personas quizá el más importante: sentirse realmente dueños de su dinero y poder estar seguros de ello.

¿Cómo se consiguen Bitcoins ?

Minando: Para obtenerlos tenemos que “extraerlos de una mina virtual”. Las Bitcoin se encuentran en lo que se llaman bloques, que se generan entre todos los nodos de la red. Cuando un nodo de la red genera un bloque, automáticamente gana 50 Bitcoin. Para evitar que la gente emita todo el dinero que le diese la gana, para que un bloque sea aceptado por la red debe calcularse un hash (una función matemática muy compleja) con determinado nivel de dificultad que regula la propia red, el cual se va ajustando de acuerdo a la cantidad de “usuarios minando” para que la cantidad de Bitcoins descubiertos no crezca, sino que se mantenga constante.

¿Qué es una dirección Bitcoin?

Toda persona que participa en la red bitcoin tiene una billetera que contiene un número arbitrario, el cual funciona como una dirección remitente o receptor para todos los pagos realizados por el usuario. Las direcciones no tienen ninguna información sobre su dueño y son generalmente anónimas, son una secuencia de números y letras aleatorios de 33 caracteres de largo, como 1rYK1YzEGa59pI314159KUF2Za4jAYYTd por ejemplo. Los Usuarios de bitcoin pueden tener múltiples direcciones, y de hecho pueden generar direcciones nuevas sin límite, debido a que generarlas es relativamente instantáneo, simplemente equivale a generar un par de llaves pública/privada, y no requiere ningún contacto con nodos de la red.

Si tienen un gran computador con buenos recursos aca el programa para minar.

Link –--------> http://www.bitcoinx.com/bitcoin-mining-software/

Billetera mas facil de usar multibit recibe,envia y muestra las transacciones.

Link –----------> https://multibit.org/