

TUTORIAL DE SUBSEVEN

PARTE 1 - INTRODUCCION

ADVERTENCIA

Bueno, primero el saludo, la intención de este tutorial es para la gente que desea con toda sus fuerzas aprender a usar un troyano, en este caso: SubSeven. Pero advertencia, si ya eres alguien experimentado en este tipo de cosas, te aviso que este tutorial está en formato de "DUMMIES" en español un termino algo asi como "Tooontos" - si eres un "Principiante" tampoco te sientas ofendido, porque de algo se empieza, y si eres "Experimentado" no te ofendas, los otros se creen SuperHackers cuando utilizan esto, y no conocen de las consecuencias que esto trae, cuando un verdadero Hacker utiliza el 80% de su potencial intelectual para crear sus propios metodos de infiltración.

¡AH! Tambien te aviso que este tutorial tiene intenciones educativas, y no para utilizarse en actos delictivos en la red... aunque no te niego que muchas veces se puede hacer cosas buenas con el uso de este programa. "HACKEAR" Puede ser divertido tambien.

¿QUE ES SUBSEVEN?

SubSeven o " SUB7 " de ahora en adelante es un troyano elaborado por una persona que se hace llamar "MobMan". La mayor ventaja de Sub7 sobre otros troyanos similares (BACK ORIFFICE - NETBUS - INCOMMAND - ETC) es que Sub7 es fácil de usar, muy confiable y estable y se actualiza frecuentemente... Sub7 tiene un estilo más que de troyano es un RAT (Remote Administration Tool), esto quiere decir que tienes la capacidad de controlar a la otra computadora... siempre y cuando la otra persona esté conectada a la RED.

Sub7 (y muchos otros troyanos también) se compone de tres archivos principales:

SERVER
CLIENTE
EDITSERVER

¿QUE ES EL SERVER?

La primera parte (Server) es un pequeño programa de alrededor de 370KB , este archivo se instala en la computadora remota mejor conocida como "VICTIMA". El Server puede ser empaquetado con otro ejecutable para esconderlo pero de cualquier forma debe instalarse en la "VICTIMA" (si no está infectada la victima no puedes hacerle nada). Una vez que el server se abre, se instrala para que se abra automáticamente cuando se encienda la PC. Tambien hace algunas cosas para esconderse en el DD (Disco Duro). El server básicamente lo unico que hace es abrir un puerto del IP de la VICTIMA, esperando que el CLIENTE (o sea tu) le envíe instrucciones.

¿QUE ES UN PUERTO DEL IP?

Cualquier dirección IP tiene más de 65000 puertos, los cuales son como "entradas" a las direcciones IP, las direcciones IP son como "la casa"... entonces "LA CASA" (el IP) tiene 65000 "puertas" (PUERTOS) Lo que hacen los puertos es recibir informacion (ejemplo: el puerto 21 es del FTP, el 80 de HTTP, el 110 del SMTP) el puerto predeterminado para los servers de las versiones 1.9 de Sub7 o anteriores es el "1243" y de las versiones 2.0 a la actual es "27374"

¿Y LOS IPs?

Bueno, cada vez que te conectas a internet, tu "ISP" (Internet Service Provider) te asigna una dirección IP, los IPs constan de 4 grupos de 3 dígitos, pero solo del 1 al 255, por ejemplo

172.133.124.45 , pero cada grupo no puede ser menor a 1 y mayor que 255 . Si tu usas conexión por módem, cada vez que te conectas tu dirección IP cambia, pero la mayoría de las veces solo cambia el último grupo de números, es decir, si tu te conectas con módem, y tu dirección IP es 200.33.146.12 , la próxima vez tu dirección IP probablemente tu IP será 200.33.146.13 (no hay ningún orden preestablecido para los IPs).

¿Y EL CLIENTE?

La otra cara de la moneda es el CLIENTE: El cliente es desde donde tú le mandas ordenes al Server, el Cliente es un programa alrededor de 610KB y es el programa que debes tener tu en tu PC para controlar a tu VICTIMA (el cliente no te puede hacer daño)... con un solo cliente puedes conectarte a varios servers, pero no a la vez. Necesitarás el IP de tu VICTIMA para conectarte a el (más acerca de esto luego).

¿Y QUE DEL EDITSERVER?

El EditServer es utilizado para configurar al Server lo que debe hacer llegando a la VICTIMA, la forma en que se coloca para ejecutarse cada vez que la PC se inicie, el puerto que abrirá, formas de avisarte cuando una victima se conecta, (ICQ, IRC o EMAIL), el ICONO, el nombre que tomará cuando lo ejecuten, y passwords para protegerlo (hay más del edit server luego).

PARTE 2 - INSTALACIÓN

CONSEGUIR SUBSEVEN

Primero, baja Sub7 de aquí o de <http://www.sub7page.org> - Te aconsejo que siempre los bajes desde sus Sitios Oficiales, porque muchas veces los Hackers consiguen victimas con trampas y ejecutables ya infectados.

INSTALAR SUBSEVEN

En realidad solo tienes que copiar los archivos a una carpeta nueva para hacer tus travesuras en esa carpeta, por ejemplo C:\Sub7

Ya conoces los 3 archivos más importantes:

Subseven.exe = Este es el CLIENTE

EditServer.exe = Este es el EDITSERVER

Server.exe = Este es el SERVER

Ahora te recomiendo que abras el cliente para que lo vayas conociendo, luego te explicaré con calma todas las funciones del CLIENTE. No te preocupes, Sub7 no hara nada en los registros de tu PC, asi que si lo quieres desinstalar, solo borra el directorio. (No ejecutes el SERVER para nada, pues te infectarás , aunque si se puede quirar, luego te digo como).

PARTE 3 - INFECTAR Y BUSCAR VICTIMAS

INFECTAR

Bueno, infectar si que es un arte, pues no es tan fácil y cada quien tiene su estilo... para infectar lo primero que tienes que hacer es configurar tu server, después darle tu toque para que la víctima lo ejecute, pero debes saber como engañarlo, para que él crea que es algo... lo que sea que crea es bueno, mientras no piense que es un virus todo está bien. Usa el editserver para que le digas a tu server que es lo que va a ser llegando con la víctima. En este tutorial hay una parte donde se describen todas las funciones de Sub7, CLIENTE, SERVER y EDITSERVER... puedes hacer tus servers y buscar tus víctimas, los configuras y listo, a jugar!

BUSCAR VICTIMAS

Hay dos tipos de víctimas: Las que buscas al Azar o las que tu infectaste. Las que tu infectaste seguramente sabrás donde están, pues en el editserver hay formas de avisarte cuando una víctima se conecta. ICQ, IRC o EMAIL, el aviso te da todos los datos para conectarte : IP, PUERTO, hora etc... El otro tipo de víctimas son las que buscas al azar, ellas son más difíciles, pero caen más rápido... En la ficha de CONNECTIONS está el IP Scanner, ahí te pide dos cosas, el STARTING IP y el ENDING IP... Y mas abajo te pide el PUERTO (PORT)... ahórrate te explico que va en cada lugar.

RANGOS

Mira, un ip se ve como 127.0.0.1... digamos que tu no sabes que tu víctima es 127.0.0.76 pero sabes que está entre 127.0.0.1 y 127.0.0.255 entonces el STARTING IP y el ENDING IP son... (redoble de tambor) 127.0.0.1 y 127.0.0.255 respectivamente - para entender mejor esto va a escanear:

127.0.0.1
127.0.0.2
127.0.0.3
127.0.0.4
127.0.0.5
127.0.0.XXX
127.0.0.255

o sea 255 IPs, te recomiendo que no pongas el rango muy amplio porque puede tardar mucho tiempo. El puerto debe ser 1) Si son tus víctimas, se supone que tu configuraste un puerto, entonces ese será el puerto que tu configuraste , por ejemplo : 24454.... si niquiera sabes que es esto, lo más seguro es que hayas dejado el puerto predeterminado, o sea, 27374 (version 2.0 o posterior) o 1243 (version 1.9 o anterior. Si así pasó, pues pon 27374 o 1243 respectivamente. 2) Si son víctimas al azar, pues lo más seguro es el puerto predeterminado. (27374)

¿CUAL ES MI IP?

Facil: Solo ve al menu inicio, ejecutar y escribe **winipcfg**, Listo! aparecerá una ventana con tu IP.

PRECAUCIONES PARA ESCANEAR

El mayor problema se presenta cuando la gente a la que escaneaste tiene Paranoia o sea, se cuida por donde sea, lo que quiere decir que seguramente tiene registros de todas las conexiones, por lo que te puede delatar con tu ISP, para esto hay dos soluciones.

a) Cuando estés conectado con tu víctima, puedes usar los dos botones de abajo que dicen "REMOTE SCAN", así, tu víctima aparecerá como el culpable del escaneo.

b) Con Sub7 tu puedes robar los datos de las cuentas de Internet de tu víctima, así que te puedes conectar con sus datos y hacer lo que tengas que hacer, pero si el telefono no es local, te recomiendo que no lo hagas.

PARTE 4 - CONECTARSE A LA VÍCTIMA

¿QUE NECESITAS?

Para conectarte a tu víctima, necesitarás tener: EL IP DE TU VÍCTIMA O EL UIN DE TU VICTIMA (Ahorita te explico) - EL PUERTO DEL SERVER, una vez que tengas todos esos datos , solo tienes que colocarlos en sus respectivos lugares: El IP/UIN en donde dice: IP/UIN! y el PUERTO donde dice PORT y después presionar el boton que dice CONNECT, entonces aparecerá en la barra de abajo algo asi como "Conectando...". Una vez que diga Conectado, LISTO!, ahora te puedes poner a llorar de emocion pensando que fue tu primera victima Hackeada!... (nope ;-)
Bueno, una vez conectado, puedes hacer cualquiera de las maravillas que te permite hacer Sub7.

¡CUIDADO!

No te dejes llevar por tus impulsos y te vayas a dejar llevar por tus ganas de destruir las cosas, trata de no darte a notar cuando estes conectado, porque no lograrás hacer nada bueno, a menos que ya lleves bastante tiempo, conozcas a tu victima y quieras hacer travesuras por ahi. Ya casi al final encontrarás unos tips para ocultarte y/o protegerte.

IP/UIN

IP es la direccion que se forma de 4 grupos de numeros, (200.200.200.212) pero... ¿y el UIN?, el UIN (Unique Identification Number) para el ICQ es el número del ICQ de tu víctima y en lugar de poner el IP, si él tiene una conexion con el ICQ en el momento que tu tratas de conectarte, pero también es bueno que tengas su dirección IP por ahi guarda, para obtener su IP a través del ICQ, solo tienes que hacer clic en la barra de titulo de Sub7 donde dice IP, asi abrirás el llamado "IP Tool", muy util por cierto. Ahi te da opciones para localizar el IP de tu víctima, ya sea con su UIN, su dominio o al revés con su IP buscar su dominio. Bastante útil no?

PARTE 5 - ¿QUE PUEDES HACER CONECTADO?

INTRODUCCIÓN

Una vez que ya estás conectado (para hacer una prueba, puedes conectarte a ti mismo, solo tienes que ejecutar el server, pero antes configuralo para que no se reinicie, más adelante te explico eso, ya que lo configuraste, lo ejecutas, y se debe instalar en tu PC, y despues te conectas a 127.0.0.1, que es tu dirección IP mientras estés desconectado de Internet), podrás utilizar todas las funciones de Sub7 con tu víctima, esto es bueno para que te familiarices con Sub7. Aqui te voy a poner todas y cada una de las funciones de Sub7, voy a empezar por los menús, y describiré todos los comandos de Sub7 brevemente:

CONNECTION

Ip Scanner: Sencillo, es la herramienta para buscar las PCs Infeectadas.

Get PC Info: Obtendrás información General de la PC infectada.

Get Home Info: Esto funciona solo para alrededor del 5% de las personas, te dará datos personales del usuario.

Server Options: Aqui podrás hacer varias configuraciones del Server de la PC infectada, siempre y cuando el Server no esté protegido para ser modificado. Si no tiene Password podrás

- CAMBIAR EL PUERTO
- PONERLO AL PUERTO PREDETERMINADO
- PONERLE PASSWORD
- QUITARLE PASSWORD
- DESCONECTAR A LA VÍCTIMA
- REINICIAR EL SERVER
- QUITAR EL SERVER
- CERRAR EL SERVER
- ACTUALIZAR EL SERVER DESDE TU PC
- ACTUALIZAR EL SERVER DESDE UN URL.

Ip Notify: Aqui programas la forma en que tu server te va a avisar cuando tu víctima esté conectado(a). Puedes ponerlo por ICQ, IRC o por EMAIL.

KEYS/MESSAGES

Keyboard: Funciones para ver las teclas que tu víctima ha presionado, hay 5 botones:

OPEN KEYLOGGER: Abre una ventana donde verás todas las teclas que tu víctima presione.

SEND KEYS: Envía una o varias teclas a tu víctima.

GET OFFLINE KEYS: Te muestra todas las teclas que tu victima ha presionado desde que encendió su máquina.

CLEAR OFFLINE KEYS: Elimina el registro de todas las teclas que presionó.

DISABLE KEYBOARD: Hace que el teclado no le funcione, pero no lo podrás volver a activar.

Chat: Abre una ventana para chatear con tu víctima, ahí configuras varias cosas.

Matrix: Ideal para asustar, abre una ventana que ocupa toda la pantalla, y no se puede cerrar, totalmente negra con el texto en verde, no podrá hacer nada más a menos que tu cierres la ventana, pero si podrá escribirte.

Msg Manager: Podrás enviarle ventanas a tu gusto, marcarle errores falsos, en fin, a tu gusto.

Spy: Ahí abres las ventanas que te permitirán espiar ICQ - AIM - MSN Messenger - Yahoo Messenger.

ICQ Takeover: Busca los usuarios que están instalados en la PC de la víctima, eliges uno y queda en tu poder!.

ADVANCED

(Si no eres experto, te recomiendo que no toques esto)

FTP / HTTP:	Hace que tu víctima sea un FTP, privado o publico.
Find Files:	Buscas archivos en los discos de la víctima.
Passwords:	Buscas los Passwords guardados de la víctima.
Reg Editor:	Abre el editor del registro de tu víctima.
App Redirect:	Ejecuta aplicaciones en la víctima, y obtienes los resultados.
Port Redirect:	Con esto te escondes, luego te explico.

MISCELLANEOUS

File Manager:	Es como el explorador de Windows, pero de la víctima.
Window Manager:	Abres, cierras, activas ventanas.
Process Manager:	Para avanzados. Cierras actividades de la PC víctima.
Text2Speech:	Escribes texto, y se oye con la víctima.
Clipboard Manager:	Ver lo que hay en el Portapapeles de la víctima, también le puedes poner.
IRC Bot:	Para avanzados. Mandas comandos al IRC para que se ejecuten.

FUN MANAGER

Desktop/Webcam: Abre una pequeña ventana donde verás el escritorio de la víctima, además puedes mover su ratón en esa pantallita como si fuera tuya. Si tiene WebCam, puedes activarla y ver que hace tu conejillo de indias.

Flip Screen:	Voltea la pantalla de tu víctima.
Print:	Envia texto y lo imprime si su impresora está encendida (ohh!)
Browser:	Abre el navegador predeterminado en un sitio que tu elijas.
Resolution:	Cambias la resolución del monitor de la víctima.
Win Colors:	Cambias los colores de las ventanas etc.

EXTRA FUN:

Screen Saver:	Configuras el protector de pantalla de la víctima.
Restart Win:	Para reiniciar Windows. Hay 5 opciones:

NORMAL SHUTDOWN: Apaga normalmente windows.
FORCE WINDOWS SHUTDOWN: Lo apaga brúscamente.
LOG OFF WINDOWS USER: Cierra la sesión actual
SHUTDOWN AND POWER OFF: Cierra windows y apaga la PC
REBOOT SYSTEM: Reinicia el equipo.

Mouse: Haces varias travesuras con el mouse.
Sound: Ahora con el sonido.
Time/Date: Configuras hora y fecha.
Extra: Travesuras adicionales.

LOCAL OPTIONS

Quality: Configuras la calidad de las imágenes que recibes y de la WebCam.
Local Folder: Especificas tu directorio de trabajo.
Skins: Elijes y configuras tus Skins, luego te ayudo con esto.
Misc Options: Cosas sencillas, checalo tu mismo.
Advanced: Si no sabes, ni le muevas.
Run EditServer: Abre el editor de Servers.

Bueno, ya terminé con el cliente, ahora vamos a ver cosas sobre el Server y Editserver. Asi que pasemos a otra parte del tutorial.

PARTE 6 - PREPARAR LOS SERVERS

EDITSERVER

EditServer y Server es todo lo que necesitas para empezar a enviar servers a todo aquel que quieras infectar, pero debes planear bien tu estrategia para que logres atrapar a alguien. Con esto empezamos a ver al EditServer a detalle:

Primero tienes que abrir EditServer.exe en tu directorio de Trabajo, una vez que lo abras te aparecerá una ventana bastante grande.

Después de esto, necesitarás seleccionar el archivo que contiene la información de server, para esto, ahí donde dice server: tendrás que elegir el server, en tu directorio de trabajo se llama server.exe, si lo guardas en otro lado, haz click en browse, para buscar el archivo. A lado hay otros 2 botones, el primero, "Read Current Settings", te muestra la información que tiene el server, y el segundo, "Change Server Icon" te da la opción de cambiarle el icono al server, si te pide algún password, es porque el server está protegido para que no lo modifiquen tan fácilmente.

La ventana se divide en 4 partes: STARTUP METHOD(S) - INSTALLATION - NOTIFICATION OPTIONS - PROTECT SERVER, vamos a verlas detalladamente:

STARTUP METHOD(S)

En esta parte, tienes la opción de elegir la forma en que el server se va a iniciar la próxima vez que

se encienda la PC víctima.

Registry Run y"Registry RunServices: Hace que se guarde en el Registro de Windows y lo ejecute cada vez que se inicie la PC, para esto tendrás que elegir el nombre de la Clave, para más ayuda, haz click en el signo de interrogacion para más informacion (todos están en ingles)

Win.ini: esto agrega una línea a ese archivo.

Less known method y _not_known method: No te las recomiendo, pero son utiles cuando tu víctima es una persona con mucha experiencia en estos asuntos, para ellos puedes elegir todas esas opciones para tener más oportunidades de que se queden infectados.

NOTIFICATION OPTIONS

En esta parte configuras la forma en que el server te avisará cuando la víctima este conectada.

Victim name: Aqui pones un nombre para identificar a tu víctima.

Enable ICQ Notify to UIN: (La mejor) Pones tu numero de ICQ, para que el server te avise.

IRC Notify: Para que te avise por medio del IRC, ahí pones el canal, server, y el puerto.

Email: (Muy lenta) te avisa por email, pones tu server.

INSTALLATION

Aqui se deciden opciones del server, aunque las puedes cambiar desde el cliente ya que estes conectado a la víctima. He aquí una por una:

Automatically start server on port: Eliges el puerto en el que estará el server esperando ordenes.

Use random port: Útil si no quieres ser descubierto facilmente, pero tendrás que confiarte de las formas de notificación, ya que no lo podrás escanear con el IP scanner.

Server password: Con esto le pones un password, así cada vez que te conectes al server, te pedira tu password, util para proteger a tus víctimas.

Protect Server port and password: Es lo mismo que el anterior.

Enable IRC BOT: Ahí configuras scripts para el IRC, solo para avanzados.

Server name: Si eliges "random name", el server se guarda en C:/Windows con un nombre generalmente raro, si eliges "specify filename" le pones un nombre fijo al archivo, util para que no se te pierda el server en tu PC. (este no es el nombre del archivo original, sino el nombre que tomará el server cuando lo instale la víctima).

Melt Server after installation: Esta opcion borra el archivo original despues de que se instala

Enable Fake Error message: Con esto preparas una ventana indicando un error falso.

Bind Server with exe file: Esto hacer que dos archivos EXE (Server y cualquier otro) se hagan un solo archivo, y al ejecutarse, el server se instala y ejecuta el programa restante. Util para esconder el server.

PROTECT SERVER

Esto es fácil, ahí le pones un password para que no se modifique a menos que tengas el password, esto por si la víctima sabe, y tiene Editserver, no te vaya cambiar el server y ver tus opciones.

Pues eso es todo acerca de los servers y editserver. Ahora voy a dedicarme a preparar un documento acerca de protección que puedas necesitar, pero antes publicaré un documento para explicar a fondo la forma de lograr que tu no seas el culpable.

Nos vemos pronto...

Este texto fue escrito por el mismo individuo que esta encargado del sitio: <http://alberto.tlsecurity.com> Se hace llamar Hacker, aunque no lo sea. Espero que no hagas copias de este texto y te recuerdo que solo es par propositos educativos y cualquier acto ilícito que cometa cualquier individuo que lea este documento, yo no me hago responsable, si no aceptas esto, nisiquiera debiste haber bajado este archivo.

Si me quieres contactar, escíbeme a: alberto_hermosillo@flashmail.com