Voz de locutor: Bienvenidos a otra clase de Hacking Desde Cero by Roadd Dogg. :)

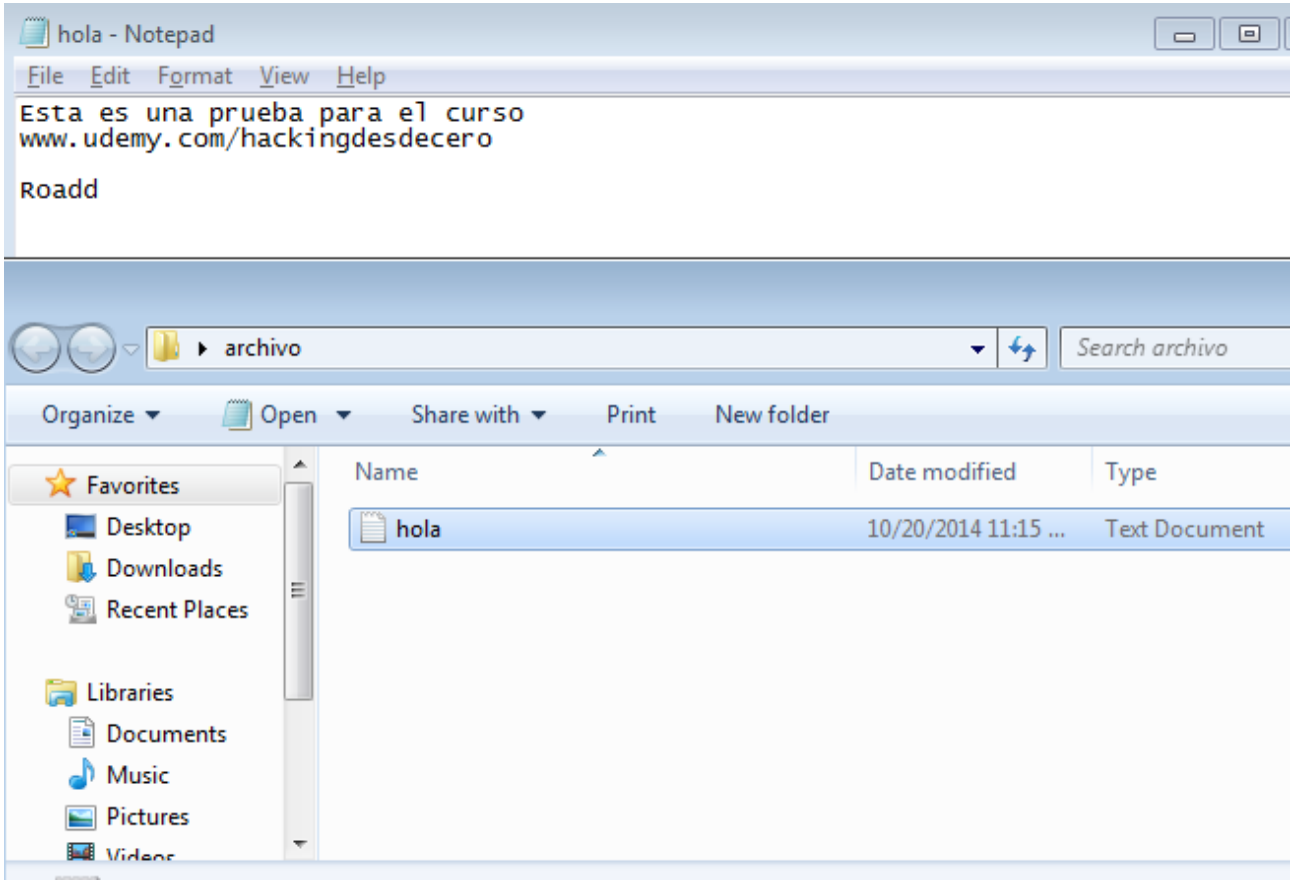
Hoy vamos a darle hincapié a los **formatos de archivo**. ¿Cuál es el formato de un archivo? Cuando hablamos del término "**formato**" hablamos de la **codificación** en que está cierto archivo, y que a **Windows** le ayudaría saber para poder **abrirlo** y el **usuario** pueda **interctuar**. Es necesario saber que cada programa tiene su **propósito** y puede abrir ciertos archivos. ¿Recuerdan cuando compilamos en C, que el software compilador ayudaba a la **interpretación** de esos comandos para pasarlo a lenguaje máquina? Bueno, el software que maneja cierto formato, se encarga de hacer más o menos lo mismo. Es decir que si no tenemos instalado un lector de PDF y nos encontramos con un archivo con ese formato, Windows **no sabrá con qué abrirlo**, ni como interpretarlo, ni mucho menos mostrarle algo coherente al usuario.

¿Cómo sabe el usuario cuál es el formato de cada archivo? Simple. Para ello existe la **extensión** de archivo. La extensión es un **agregado al nombre, y separado por un punto, única por cada formato**.

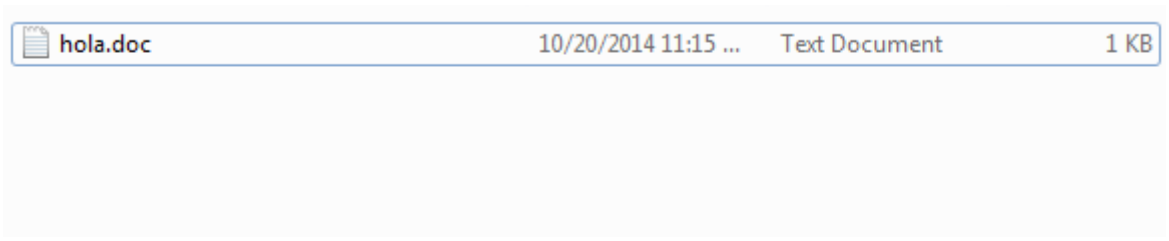
Por ejemplo, un archivo que se llama **hola.txt**, sabemos que el nombre es "**hola**" y la extensión del archivo es "**txt**". Entonces, seguro que el formato del archivo es "txt" tal y como dice, y que se pueda abrir con un **bloc de notas**.

"¿Tal y como dice? ¿Podría ser otra cosa?"

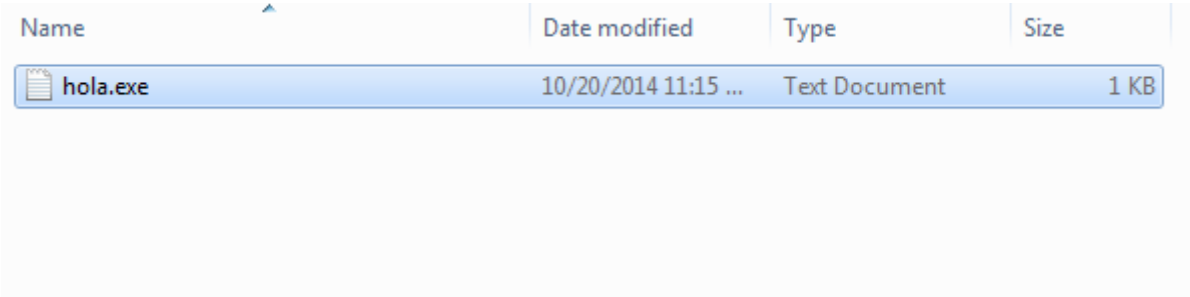
Claro. Hagamos una prueba de las cosas que se pueden hacer. Primero que nada abramos el bloc de notas (de ahora en más **notepad**), escribamos algo y guardémoslo como "**hola.txt**" en algun directorio.



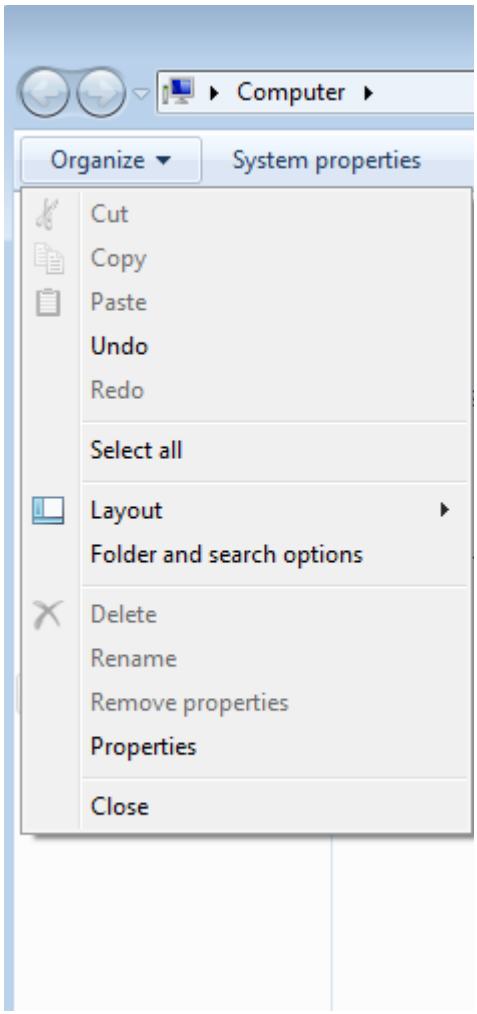
No sé si se dieron cuenta de lo que pasó, pero si tienen configurado a Windows por defecto, verán que no hay extensión -o mejor dicho, **estará oculta**- de archivo ".txt". Sólo aparece el nombre y un **ícono** del programa con el cual podemos abrirlo.
Ahora hagamos **click derecho -> Cambiar Nombre (Rename)**; y todavía no aparece la extensión, aunque sí podemos cambiar el nombre y me da de pensar. Intentemos cambiando el nombre a **hola.doc**.

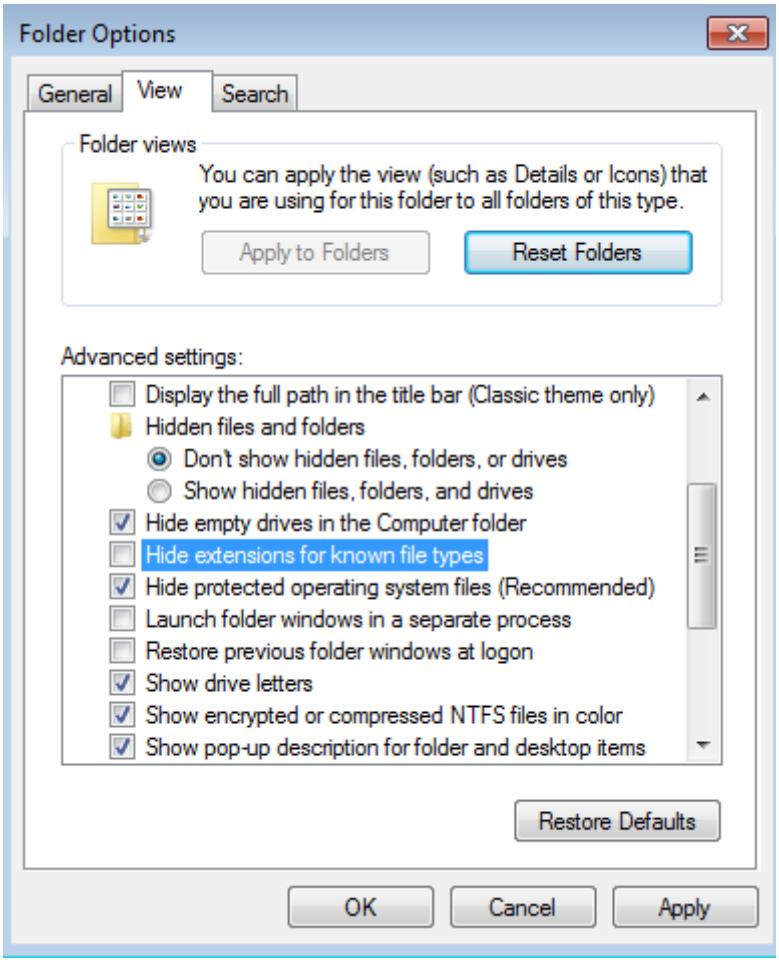


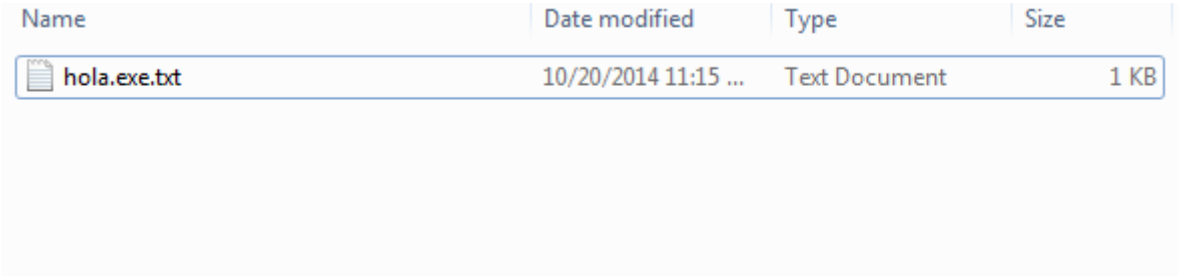
Que interesante. No pasó **nada**. El archivo sigue con el ícono del notepad (aunque .doc es la extensión del formato del programa **Word**). A ver, hagamos otra prueba. **Cambiemos** el "doc", por "**exe**".



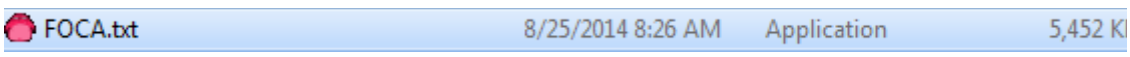
Muy extraño. Aunque "**exe**" es la extensión de un archivo **ejecutable** de **Windows**, me aparece que el notepad es el programa ideal para la apertura del mismo. Esto quiere decir que la extensión del archivo viene **oculta por defecto en el sistema**.
Hagamos esto: Vamos a **Mi PC, Organize, Folder & Search Options. En la pestaña View, tenemos dentro de las opciones el "Hide extensions for known file types" que podemos destildar y nos revelará las extensiones de todos los archivos.** De allí, en el archivo que modificamos, vemos esto:





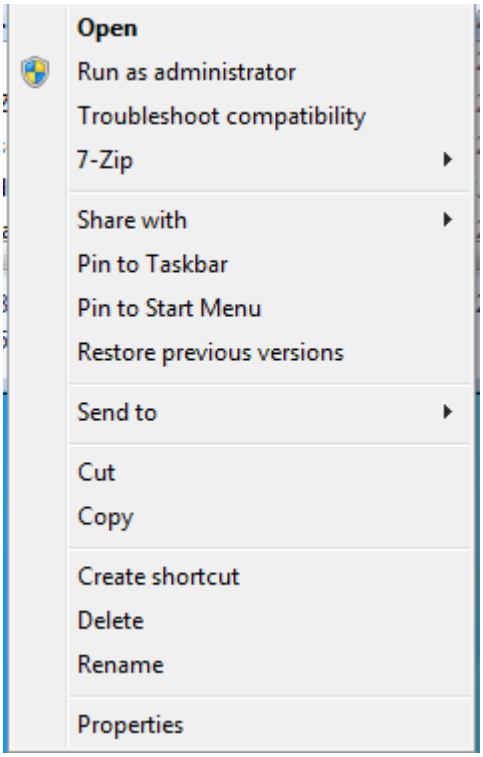


¿Por qué es **importante** ésto? Bueno, con un notepad no tenemos peligro porque en última instancia, tendremos que leer. Intentemos hacerlo con un **.exe**. Cada uno elija un ejecutable de **confianza** que pueda modificar. En mi caso voy a utilizar el **ejecutable** de "**FOCA**" un software de extracción de metadatos y otras yerbas.
Le voy a cambiar el nombre, por **FOCA.txt**.



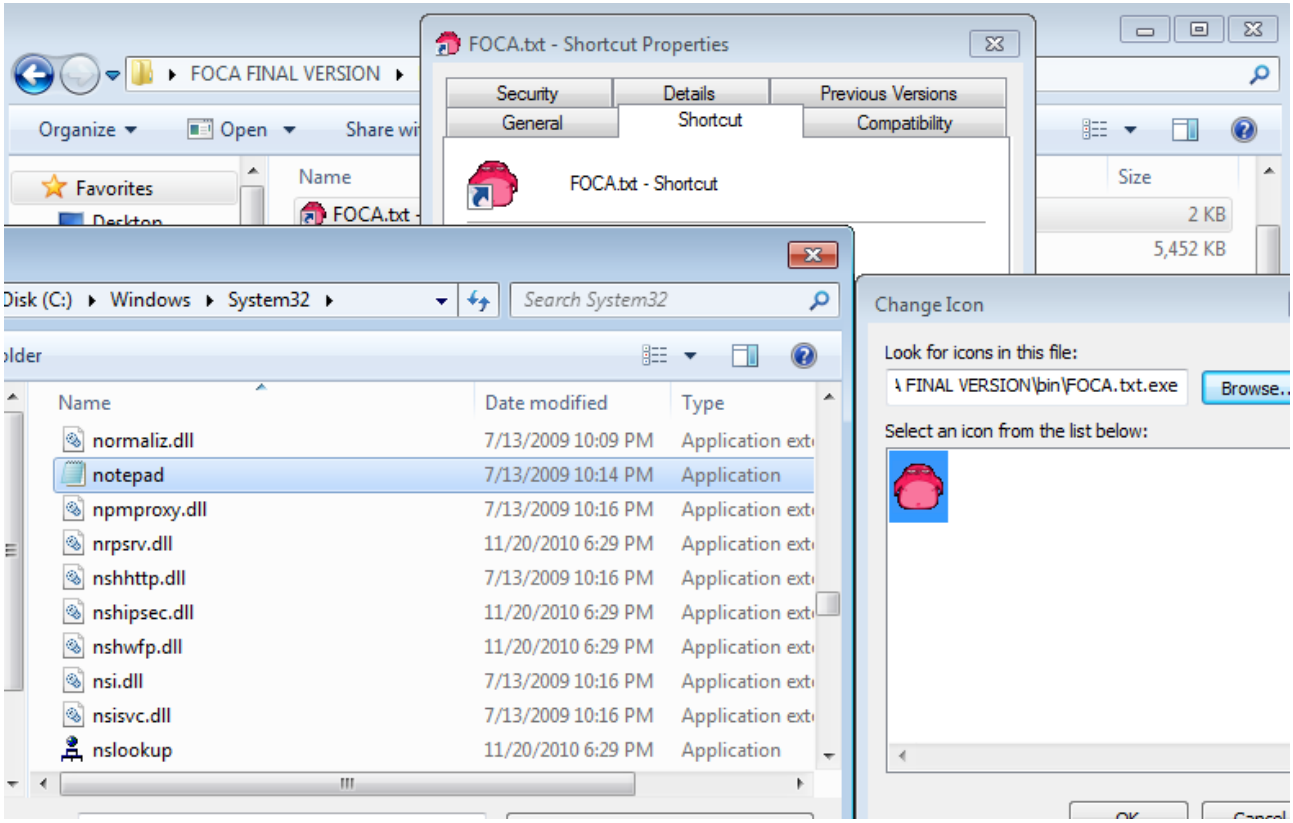
Cuando lo que tenemos es un exe da miedo, porque aunque diga "**.txt**", esto es parte del nombre y no es la extensión del archivo. Es decir que si le damos doble click, innocentemente, para leer un texto, nos vamos a encontrar con la **ejecución de un software** (y aquí, los futuros desarrolladores de malware empapan de baba el escritorio). Aunque todavía tiene el **ícono** de FOCA. Necesitamos

que sea coherente con la supuesta extensión del archivo. Para esto, como no podemos personalizar el programa, vamos a crear un **acceso directo**. (Click derecho -> Create shortcut).

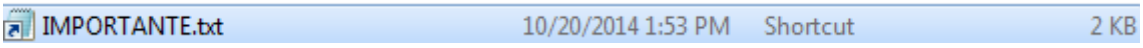


A éste, podemos darle **click derecho -> Properties. En la pestaña Shortcut, le damos a "Change Icon". Ahora, para elegir el ícono, debemos ir a Windows/System32/notepad.exe, dentro de la partición principal.**

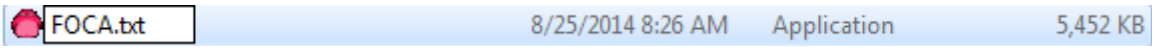
Ahora que ya tenemos el ícono, podemos cambiarle el nombre por **"hola.txt"**.



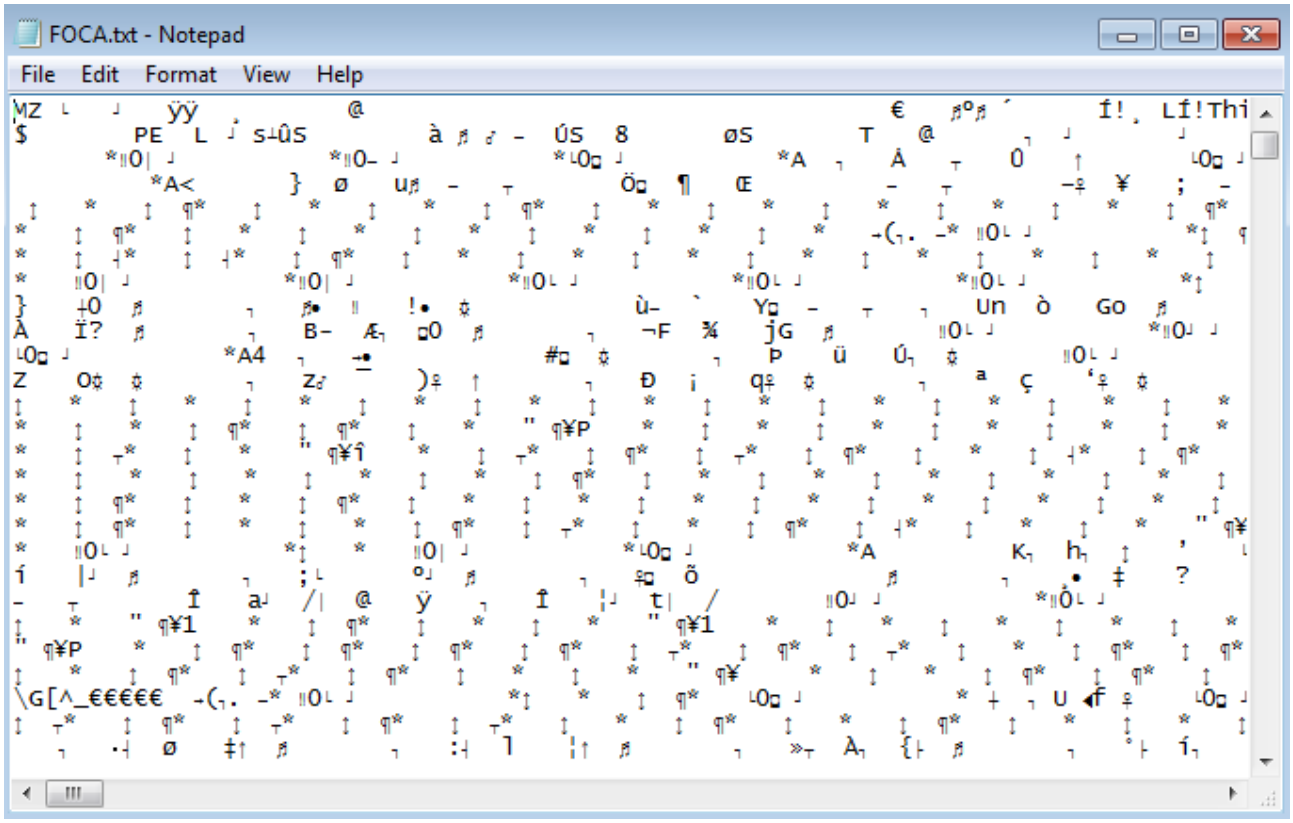
Lo único molesto es esa **flecha** que nos delata como acceso directo, pero para sacarlo, debemos **editar el registro de Windows**. Vamos a intentar de no meternos en éso aún, porque estamos en la **fase anterior** a ejecutar el Malware.
De todos modos, jugar con la **ignorancia** del usuario es cosa mundana, y es fácil ponerle "**IMPORTANTE LEER.txt**" al archivo y generarle **ansiedad** a la **víctima**. Acuérdense que contamos con que el usuario deja por **default** el "Hide[...]".
Así que **cuidado** con lo que descargan. Hay que conocer las técnicas de ataque para poder defenderse.



Pasemos a una **segunda parte**. Si cuando dejamos **destildada** la opción del **hide**, le damos a "**Rename**", vemos que podemos **cambiar la extensión del archivo**. Pongámosle "**.txt**".



Ahora vamos a poder abrirlo (Windows lo leerá como si estuviese codificado así) con el notepad. Aunque claramente no va a decir **nada coherente**, sino una mezcla de símbolos y mamarrachos. Y si le quitamos la extensión o le ponemos una que desconocemos bla bla bla.



Aunque si queremos, podemos abrirlo con el programa que nosotros queramos hasta dar con el blanco. Es un buen tip para poder pasar archivos ejecutables a través de muchos medios que no dejan subirlos con esa extensión y que luego funcionen correctamente con solo **cambiarle** la extensión.

Vamos a dejar aquí este tema. La próxima, veremos un poco de administración del sistema (sobre todo para ver cuáles herramientas tenemos por defecto) y ya tenemos el examen. Más adelante nos adentraremos con la programación en Batch y el desarrollo de Malware.

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.
