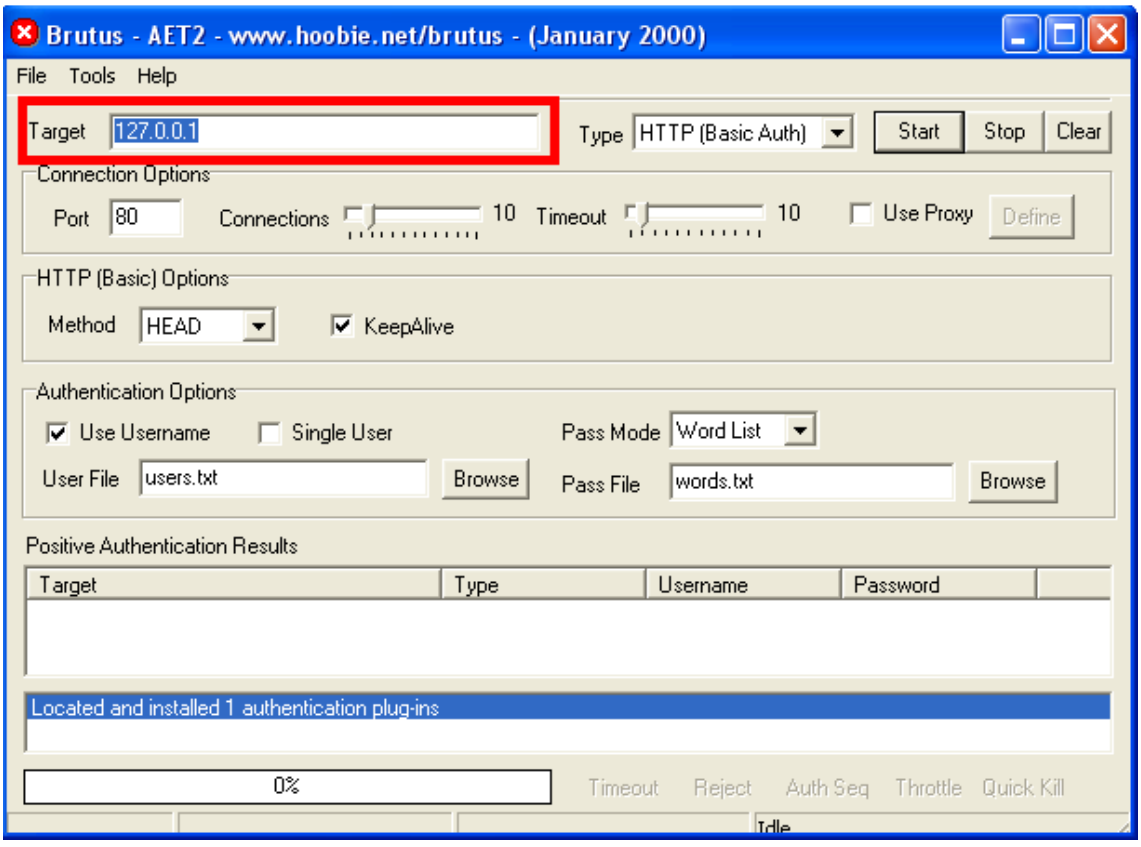
Manual Brutus AET2

Que es Brutus AET2 ???

Brutus AET2, es un potente crakeador que nos permite crakear varios tipos de servidores, entre ellos: HTTP (basic auth), HTTP(form), ftp, POP3, telnet, SMB (netbios), netbus, custom (mas servidores a mallores).

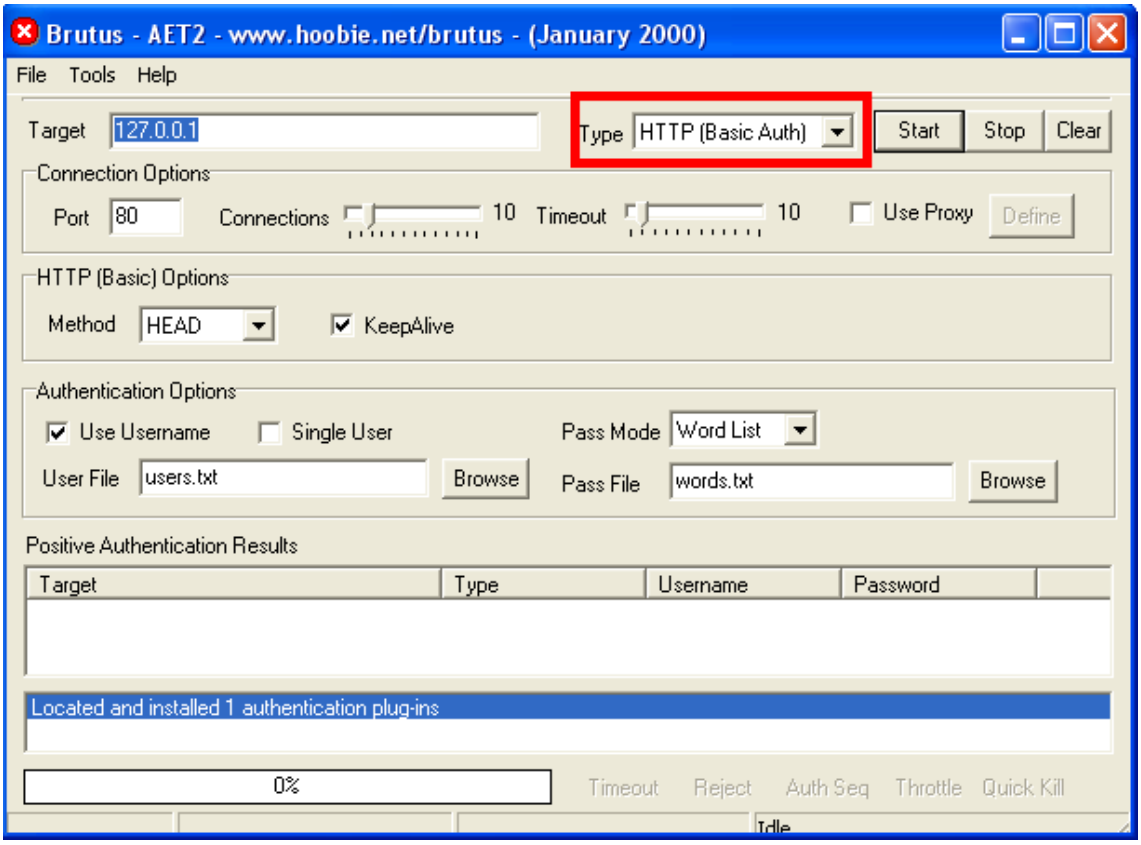
Partes de Brutus AET2

Target



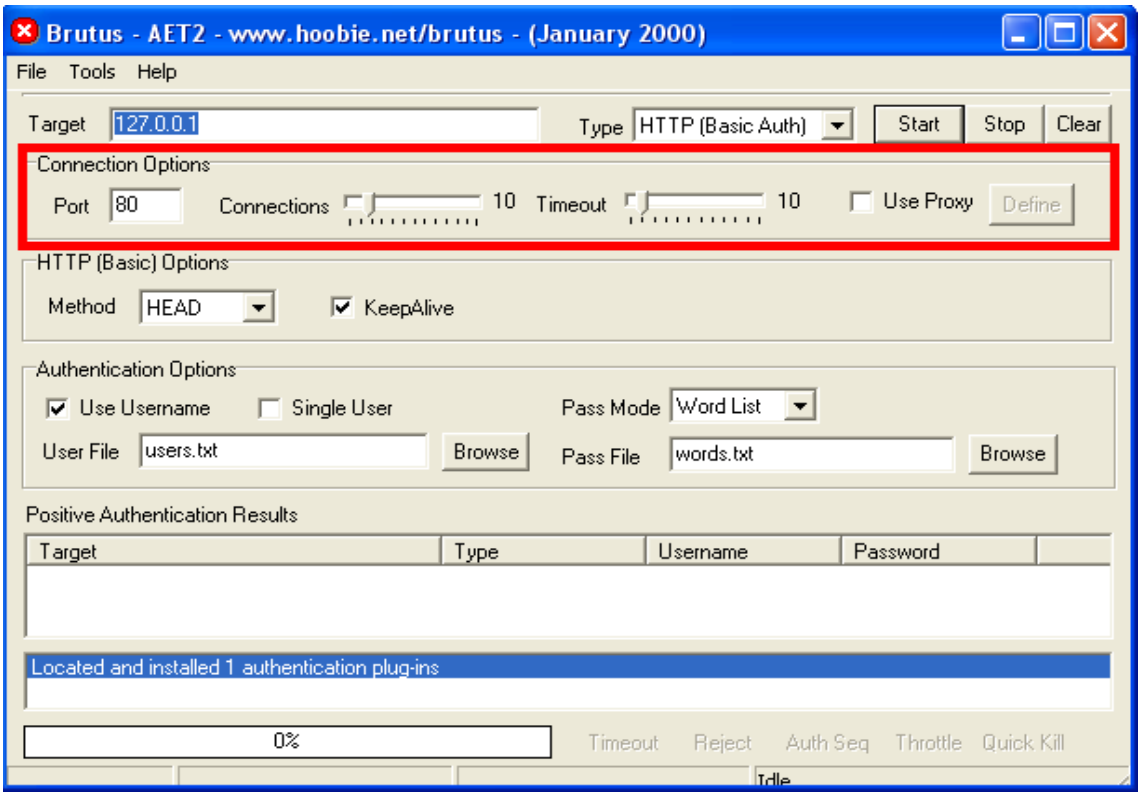
En la parte de arriba podemos encontrar el “target” en este sitio debemos de introducir la ip/host de nuestra victima

Type



Al lado de “target” esta “type” aquí tenemos que seleccionar el tipo de servidor que vallamos a crakear

Connection options



Aquí es donde están unas de las opciones “importates” a la hora de crakear,

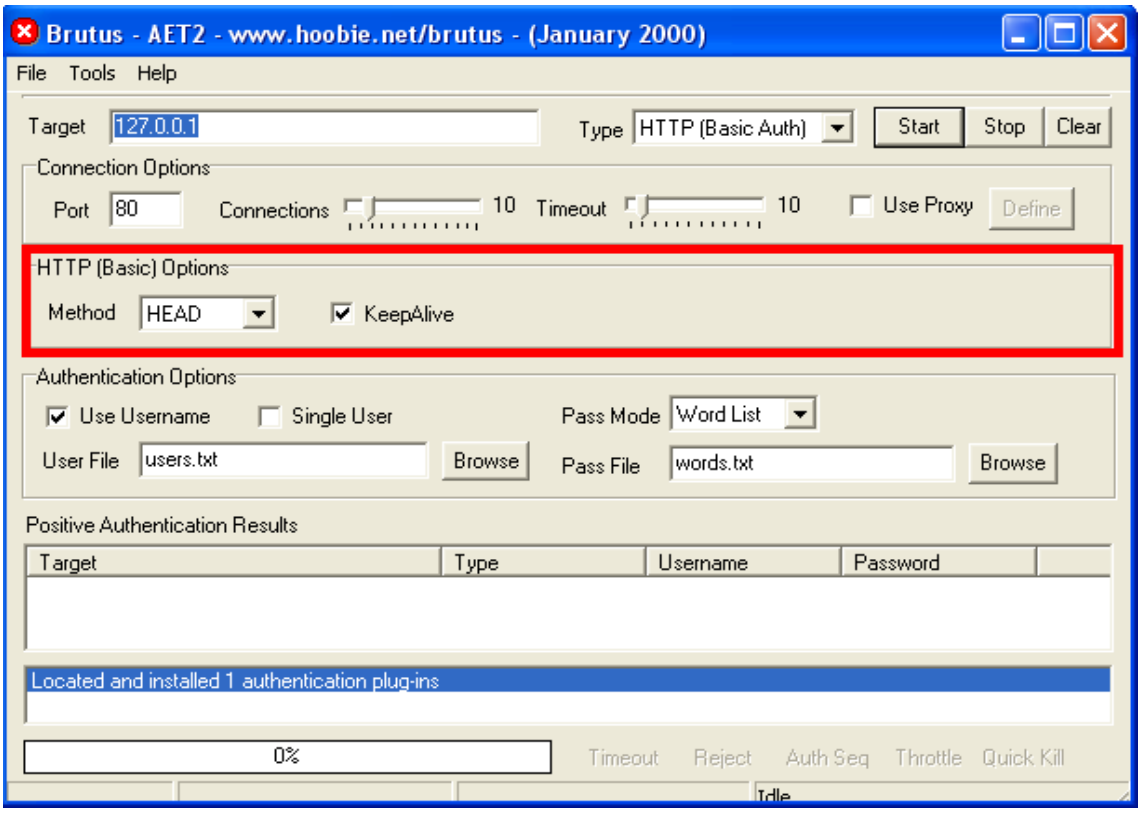
Puerto: aqui introduciremos el puerto por el que vallamos a crakear, según el tipo de servidor tendremos que utilizar un puerto, ej: telnet(23), FTP(21), SMB(139), estos son los puertos por defecto, aunque esto no quiere decir que siempre valla a ser ese puerto, el puerto puede variar según la victima lo cambiase.

Connections: aquí seleccionaremos el numero de conexiones que queremos para crakear, cuantas mas conexiones mas rápido será el crakeo, pero también ai que tener en cuenta el ancho de línea que tenemos, si ponemos muchas conexiones podemos tirar nuestra conexión o incluso el servidor mismo puede desconectarnos.

TimeOut: aquí introduciremos cada cuanto tiempo queremos que el brutus haga una reconexion (desconectarse y volverse a conectar), si ponemos mucho tiempo el servidor nos desconectara.

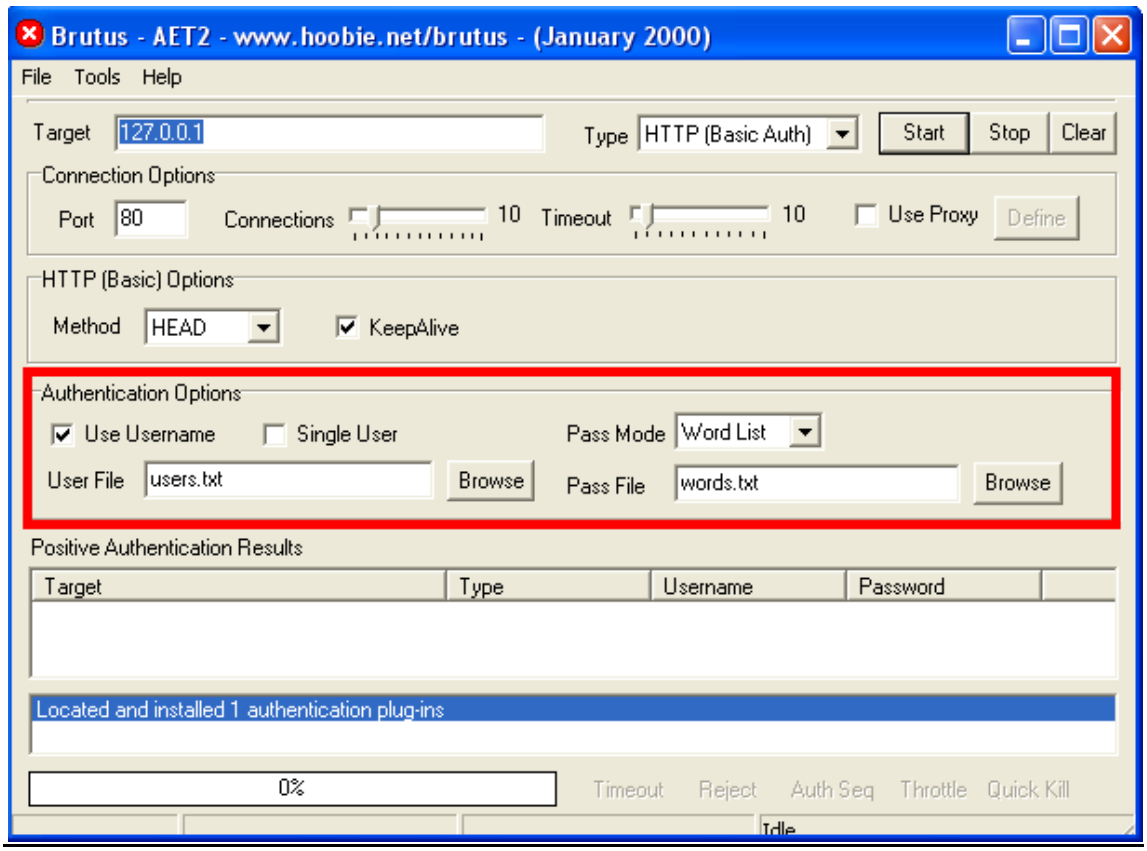
Use proxy: si queremos ocultar nuestra ip a la hora de crakear podemos usar un proxy, en este caso marcamos la casilla y después en “define” ponemos la dirección del proxy

Options



Según el tipo de servidor que elijamos tendremos unas opciones u otras, estas opciones sirven para que podamos expecificar mas sobre el servidor a crakear (normalmente dejando las opciones por defecto se puede crakear con normalidad)

Authentification options



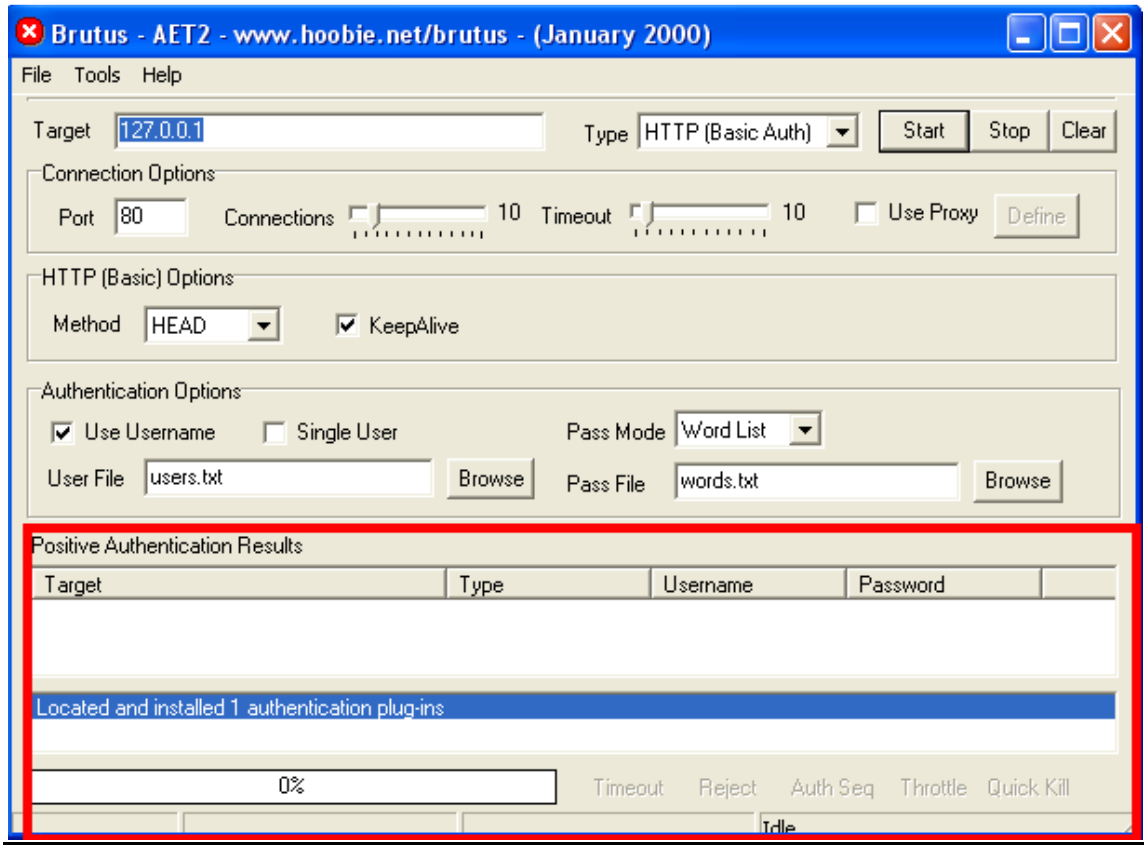
Use username: si no necesitamos ningún user para acceder al servidor entonces dejaremos esta casilla desmarcada, si necesitamos un user pues la dejaremos marcada (normalmente siempre se necesita user)

User File: en caso de que no sepamos cual es el user, pondremos la dirección de un diccionario para que el programa valla probando con los users que ai en el diccionario, si sabemos el user pues marcamos la casilla “single user” y escribimos el nombre del user

Pass Mode: aquí seleccionaremos el modo que queremos usar para crakear la contraseña, los modos que nos da son: Word list (Con este modo usamos un diccionario), Combo list (con este modo también usamos un diccionario para que el programa use combos de palabras), Brute forcé (con este método el programa prueba todas las combinaciones de letras que existen, podemos indicarle que solo lo aga con

letras, con números…….etc, nos da varias opciones, este método es poco recomendable ya que emplea mucho tiempo)

Informacion



En la parte de debajo de todo se nos muestra la información:

Positive Authentication Results: aquí se nos muestran todas las contraseñas obtenidas

General information loggin area: aquí se nos muestra toda la informacio del loggin de programa.

Hack real usando

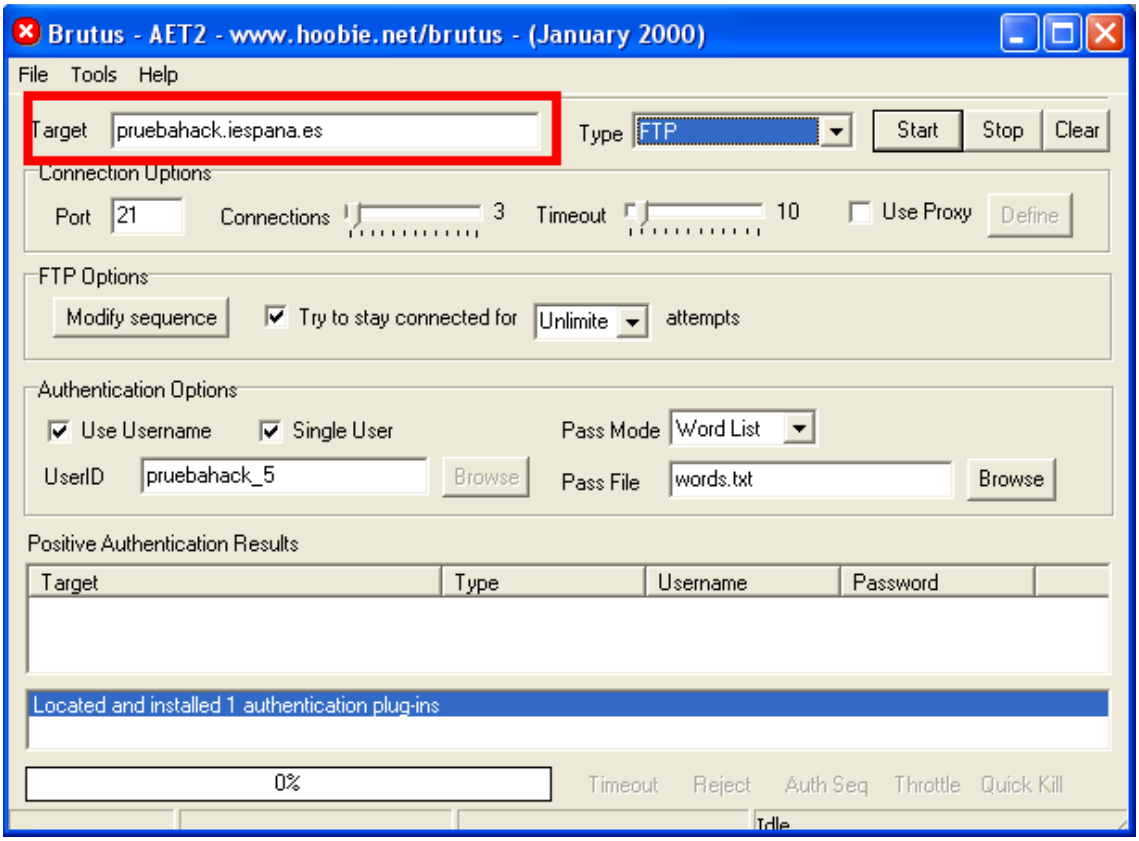
brutus AET2

Aquí os mostrare como usar el brutus en un caso real, en esta ocasión crakeare un ftp.

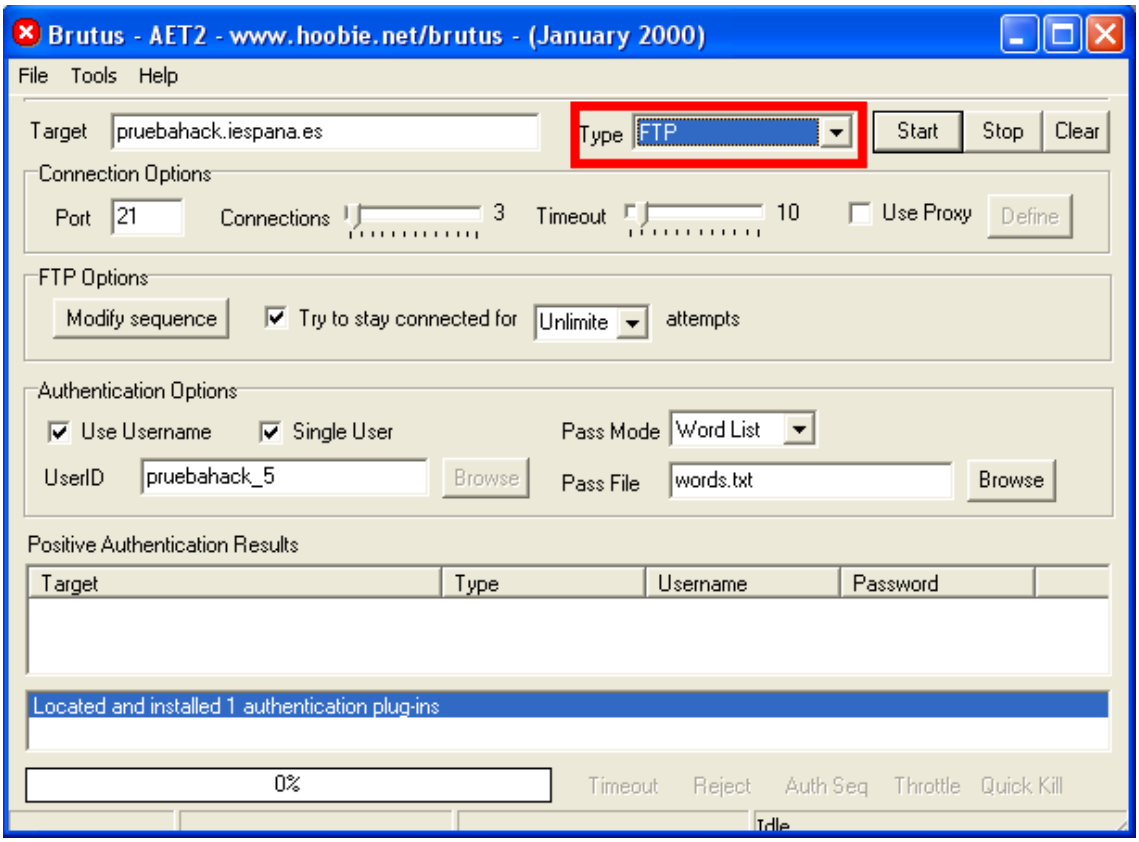
Lo primero es elegir una victima, en este caso será: **pruebahack.iespana.es**

Lo que hare será crakear la pass de esa web mediante el ftp (por si alguien no lo sabe, las paginas alojadas en iespana.es se pueden modificar mediante ftp, asi que aprovechare esto para sacar la contraseña de la web)

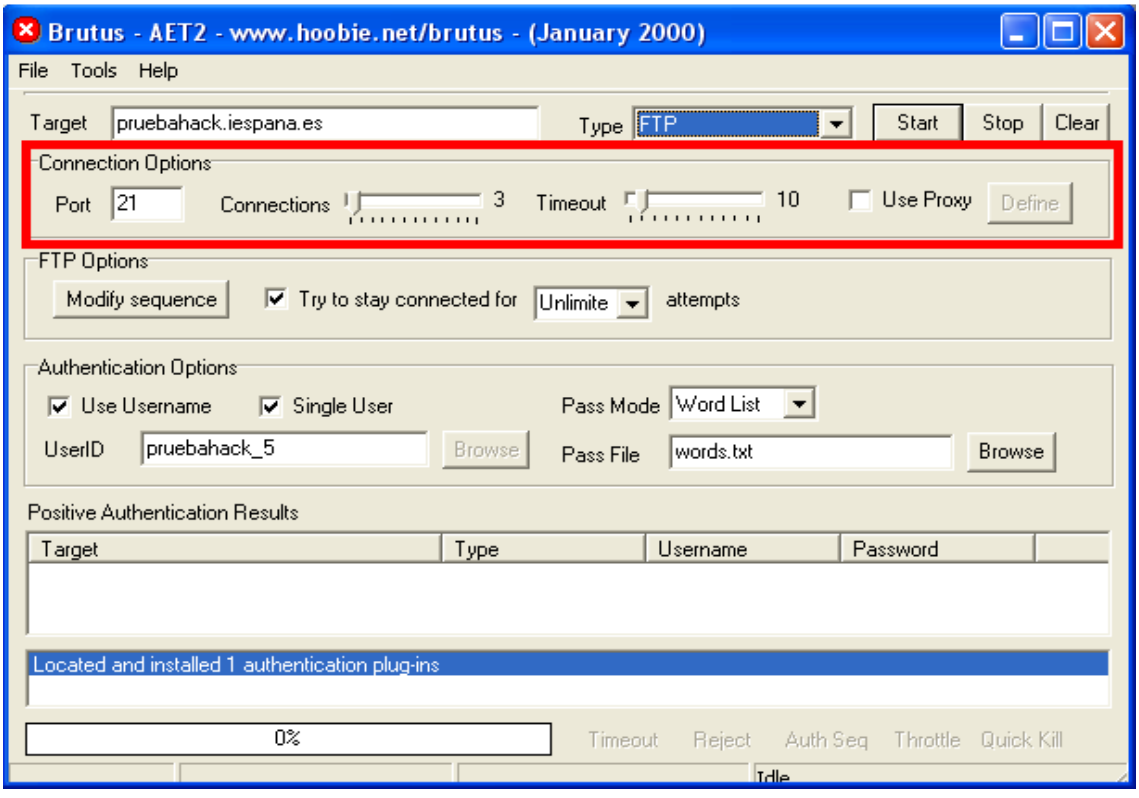
Primero introducimos la dirección de la web en el target, en este caso **pruebahack.iespana.es**



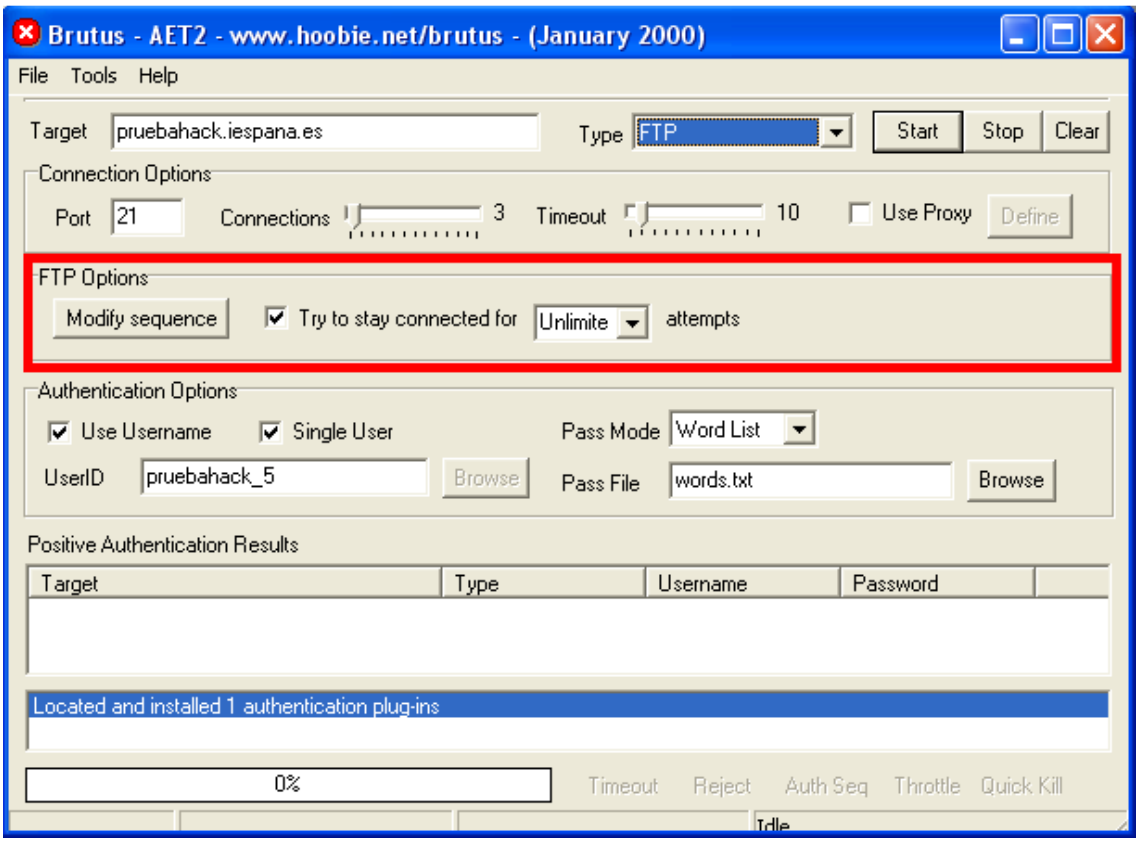
Despues seleccionamos el tipo de servidor, en este caso “FTP”



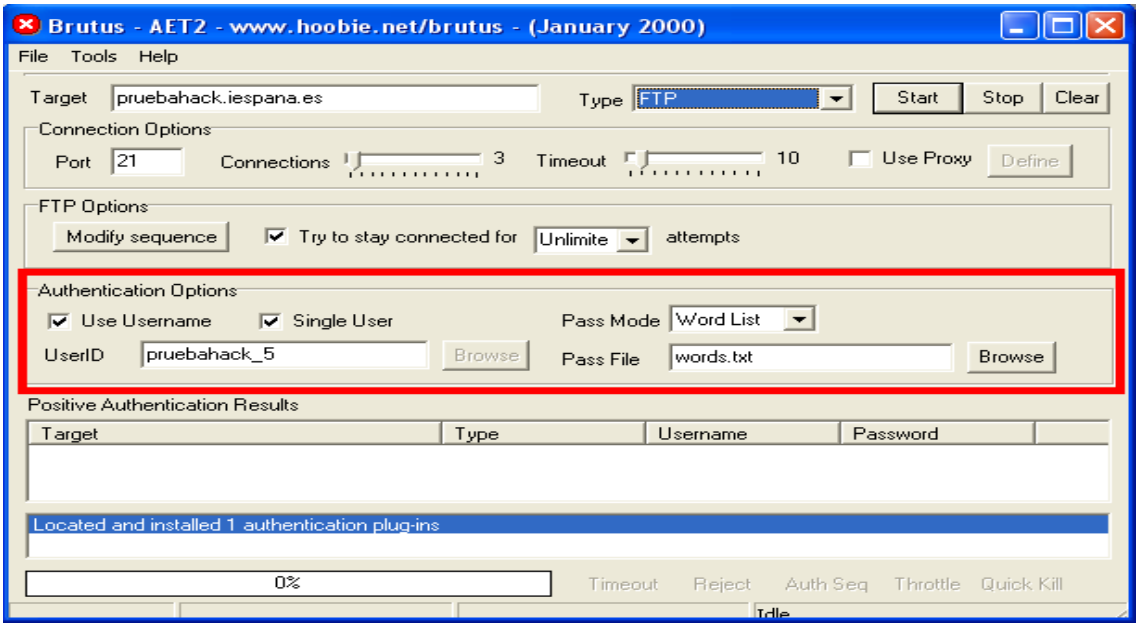
El puerto lo dejamos como esta “21” , en conexiones ponemos “3” (puedes probar a poner mas conexiones, pero el servidor te puede desconectar, o incluso puedes tirarte a ti mismo) , en timeout ponemos “10” y en este caso no voi a usar proxy



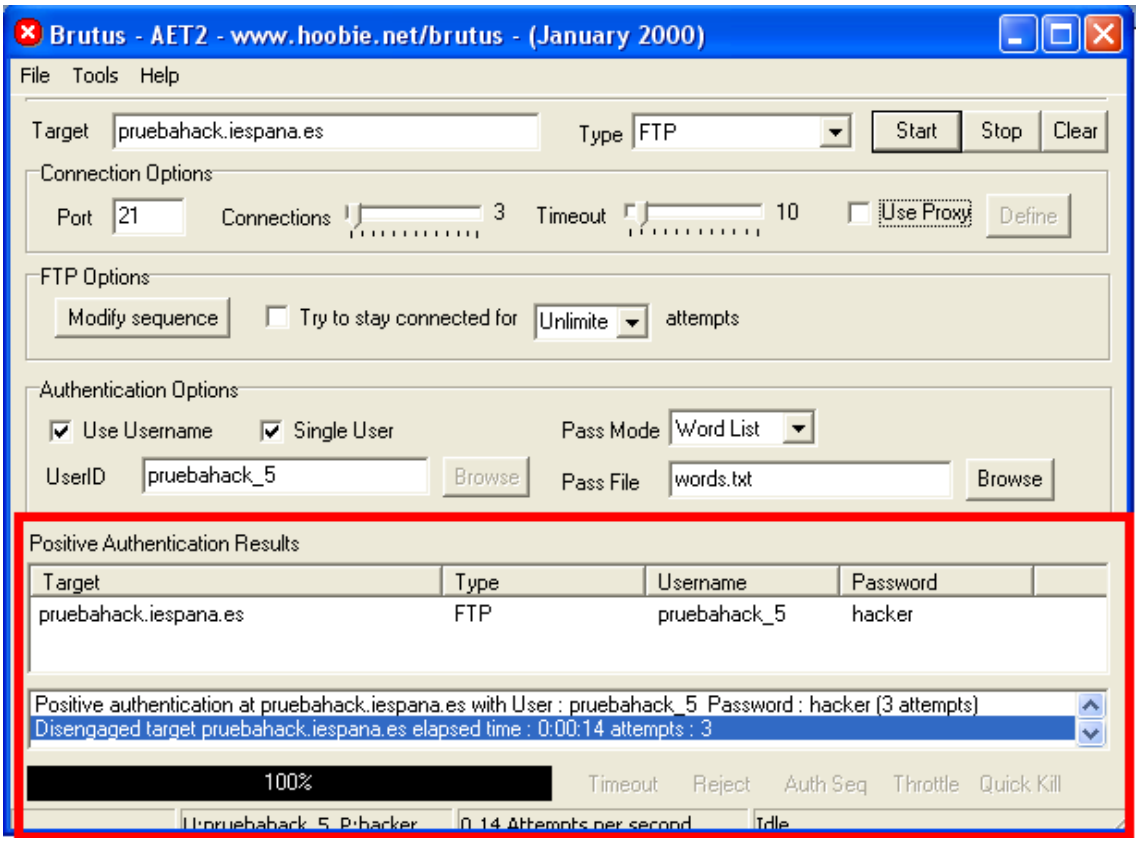
En las opciones de FTP marcaremos la casilla “try to star connected for” y al lado seleccionamos “ulimited”



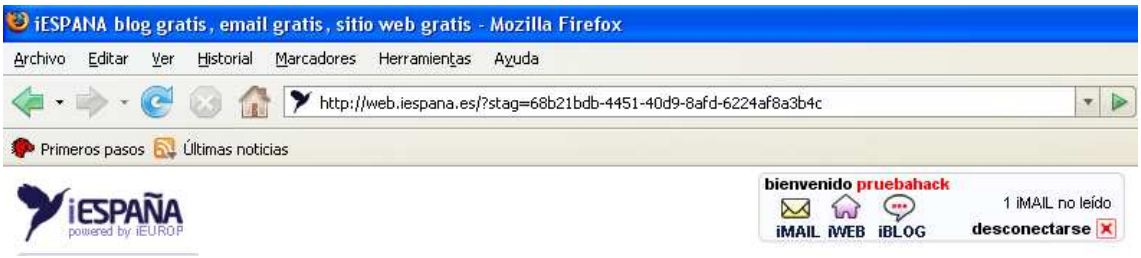
Ahora en “authentification options” marcamos la casilla de “Use username” y la casilla de “single username” y ponemos el nombre del user, en este caso es **pruebahack_5**, por si os lo estais preguntando, el user del ftp de las paginas de iespana.es siempre es el nombre de la pagina mas **_5** en este caso **pruebahack**_5 despues en “Pass mode” seleccionamos “World list” y seleccionamos un diccionario.



Despues de hacer todo esto le damos a “Start” y el programa empezara a crakear, en caso de que el programa se desconecte cada 2x3 bajaremos el numero de conexiones y bajaremos el timeout, (antes de comenzar a crakear asegurate de tener el firewall desconectado o configurado para permitir que el brutus se pueda conectar).



Bueno, el crakeo ha acabado y me ha dado como resultado “hacker” (si os fijais en la parte de abajo el programa iva a 0.14 palabras por segundo, la verdad eske es bastante lento, esto es debido a k he tenido que poner un numero de conexiones muy bajo además de que el servidor es bastante lento) asi que ahora nos vamos a iespana.es introducimos el user “pruebahack” (desde la web no ace falta poner el _5 si quieres entrar por el ftp si que ace falta) y las pass “hacker”



y…… BINGO !!!!!! ya estamos dentro, ahora podemos modificar lo k keramos…..

PD: no destruyas nada…

Manual creado para la Comunidad de Programadores de Ale666.com

www.ale666.com