

MANUAL DEL BRUTUS AET2

1. [Introducción](#)
2. [Como empezar a craquear](#)
3. [Disclamer](#)
4. [Notas del Autor](#)

INTRODUCCION

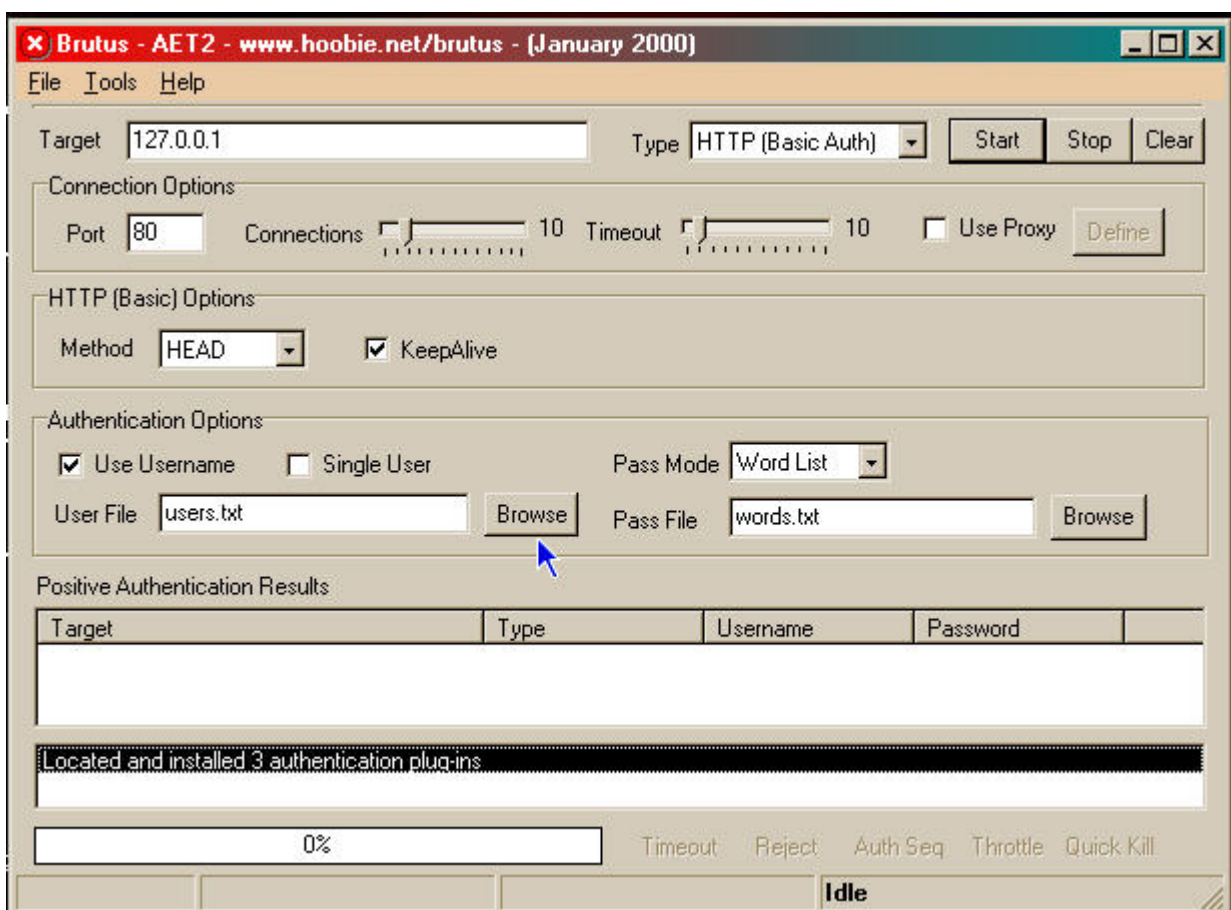
Brutus es un craqueador de passwords, es bastante rápido y muy fácil de manejar, los pass que puede craquear son: HTTP (Autenticación Básica), HTTP (HTML Form/CGI), POP3, Ftp, SMB, Telnet, otros tipos tales como IMAP, NNTP, NetBus etc .

Y esta versión contiene estas funciones: Motor gradual de la autenticación, 60 conexiones simultaneas por target, Ningún username, solo username y modos múltiples del username, Lista de contraseñas, lista combo (user/password) y modos configurables de la fuerza bruta, Secuencias altamente configurable de la autenticación, Importe y exporte los tipos de encargo de la autenticación como BAD archivos seamlessly, Poder usar SOCKS proxy para cada sesión, El usuario y la contraseña enumeran funcionalidad de la generación y de la manipulación, El HTML forma la interpretación para los tipos de la autenticación del HTML Form/CGI, Poder salvar la sesión de craqueo y poder volver a ella cuando se desee.

Requisitos del sistema: Windows 95, Windows 98, Windows NT 4 o Windows 2000. 24 Mb RAM, 5Mb libres en tu HD (disco duro) y claro conexión a Internet.

COMO EMPEZAR A CRACKEAR

Lo primero que tenemos que hacer es abrir el Brutus AET2, y nos aparecerá una ventana como esta:



A continuación explicare para que sirve cada sección del programa: En "File" si le damos nos sale una ventana despegable con varias opciones, Import Service, que sirve para importar algún Servicio que no viene incluido en el programa como...HTTP (Autenticación Básica), HTTP (HTML Form/CGI), POP3, Ftp, SMB, Telnet, IMAP, NNTP, NetBus etc.

Export Service, sirve para exportar si tienes algún servicio nuevo para el programa. Load Sesión, sirve para cargar alguna sesión que dejemos a medias. Save Sesión sirve para guardar la sesión que estemos ejecutando y poder volver a ella siempre que queramos, Restore Last sirve para restaurar todo lo que anteriormente hallamos elegido.

En "Tools", encontramos Word List Generador que sirve como su nombre indica para generar, gestionar y optimizar tu Word List (lista de password).

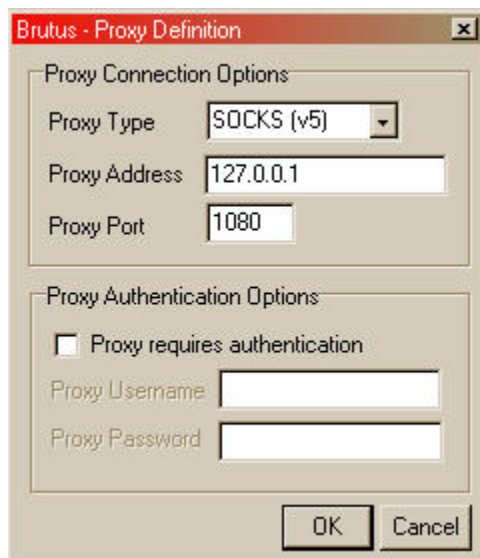
Y creo que hay poco que explicar.

En "Target" sirve para poner la clase de Target que queremos craquear o sea la IP, si es tipo HTML pondremos la dirección URL y el programa la convertirá en IP, así mismo pasara si ponemos un FTP que vamos a craquear.

En "Type" se selecciona el tipo de auto identificación que vas a craquear y ya hemos visto mas arriba todo los tipos que hay así que sobra el volver a explicarlos. En "Port", no tendrás que prestarle mucha atención, ya que al seleccionar el "Type" que quieres cambiara solo,

si seleccionas Telnet se pondrá automáticamente el puerto 23 y así sucesivamente con todos.

El "Use proxy" es para utilizar SOCKS proxys a la hora de hacer el crackeo véase esta imagen:

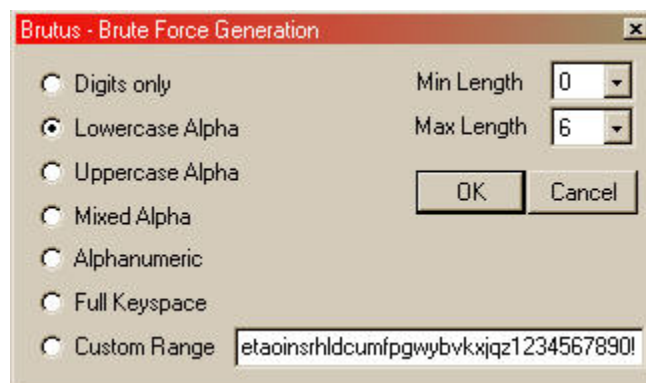


Creo que hay poco que explicar, en "Proxy Type" tienes que seleccionar el tipo de proxy, En "Proxy Address" la IP o en su defecto el host del Proxy y en "Proxy Port" el numero del puerto que vas a conectar recordando que, si escaneas HTTP (Autenticación Básica) o HTTP tienes que usar el puerto 80 o 8080y si escaneas, FTP, Telnet, etc. usar un SOCKET proxy o sea por el puerto 1080.

En "Authentications Options" hay varias opciones, empecemos: Si no sabemos el Usermane de la victima ya sea al intentar hackear HTML, Telnet, FTP, etc. podemos utilizar un archivo en el que tengamos

posibles nombres de usuarios entonces dejamos la opción "User Username" activada y en el botón "Browse" te buscas en tu disco duro el archivo que contenga posibles nombres de usuarios. Pero si sabes el nombre del usuario pues entonces activas la opción "Single User" y la casilla "User file" se trasformara en "User ID" y ahí es donde tienes que poner el nombre de usuario que conoces.

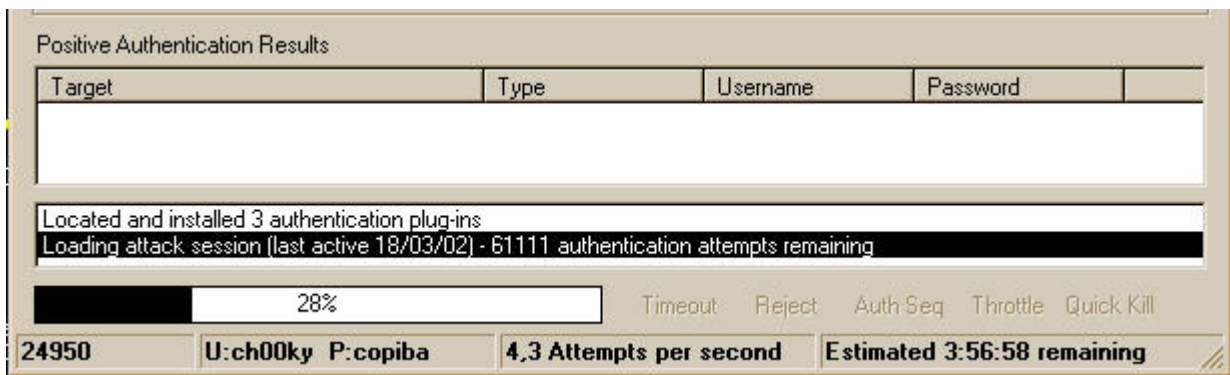
En "Pass Mode" seleccionamos el tipo de fichero que vamos a utilizar: "Word List" es la opción en la que elegiremos un archivo que tengamos con posibles passwords y la buscaremos en el disco duro con el botón "Browse" y aparecerá en la casilla "Pass File" la dirección completa donde tienes el archivo de Passwords. Puedes seleccionar también la opción "Combo List", esa opción nos permite con una misma lista de passwords sacar el nombre de usuario y el password. La otra opción es "Brute Force" que esta no necesita ningún archivo con passwords ni nada, osea que lo hace por fuerza bruta , es algo mas lento que las demás opciones ya que tardara algo mas en encontrar los pass, pero es mas efectiva, si quieres configurar los rangos de passwords que vas a utilizar por fuerza bruta entonces apretar el botón "Range" y aparecerá una ventana como esta:



En esta ventana podrás elegir que tipo de password que vas a utilizar por fuerza bruta, lo primero que tienes que hacer es elegir si va a empezar desde 0 hasta los dígitos que ocupe el passwords, para eso nos vamos a "Min Length" y a "Max Length" y hay eliges desde donde va a comenzar, Ejemplo: si seleccionas Min Length 0 y Max Length 6 pues empezara con un solo digito o letra (desde "a" hasta "zzzzzz") e ira pasando por todas las letras y símbolos, si eliges Min Length 6 y Max Length 6 pues empezara con 6 dígitos o letras ("aaaaaa" hasta "zzzzzz") y así sucesivamente con el numero que elijas.

Luego en la parte izquierda es donde vamos a elegir el tipo de password que quieras craquear, ya sean letras, numero, números y letras..... esto lo explico a continuación, "Digits Only" solo números osease, que buscara pass por fuerza bruta que contengan solo números, ya sea una fecha, etc. "Lowercase Alpha" esta opción son letras solo en minúscula, "Aperchase Alpha" lo mismo que el anterior pero en mayúsculas, "Mixed Alpha" buscaría letras pero no en orden alfabético, "Alphanumeric" seria entre mezclando números y letras, "Full Keyspace" como su nombre indica, utilizara todas las teclas del teclado, letras, símbolos, números etc. "Custom Range" utiliza todo, letras, números, símbolos etc.

"Positive Authentication Results" es donde te va marcar como va el progreso de buscar Passwords y los que va encontrando véase este ejemplo



Y poco mas que explicar de este programa espero que este manual sirva de ayuda y si no lo explico muy bien pues ya lo ire perfeccionando en próximas ediciones :)

GRACIAS A HACKING PARA NOVATOS POR LA INFO

<http://www.hackingparanovatos.com>



**CORRECCIONES ORTOGRAFICAS Y ADAPTACIÓN A PDF
POR MESIN NET**

<http://mx.geocities.com/mesinnet>



Autor: By S4D^|^3ND