Brutus - Authentication Engine Test Release 2 **www.hoobie.net/brutus**

28th January 2000

Changes in release AET2 :

1 – All user specified server response strings are converted to lowercase now as are the actual server responses.
2 – Fixed the problem encountered whilst trying to change the timeout during operation.
3 – Fixed problem with the default POP3 settings (related to fix 1 above.)
4 – Added brute force password generation
5 – Added save current session
6 – Added auto-save current session
7 – Added restore saved session
8 – Added save custom service
9 – Added load custom service
10 – Added password permutations
11 – Added word list creation functions
12 – Fixed update problems in the Auth. Seq. Definition window
13 – Added pause/resume functions
14 – Added semi-automatic 'learn' function for HTML form/CGI based services
15 – Added skip user on multiple password prompt failures
16 – Added 'use updated form fields' option to HTML form based services to enable attacks against services which use one time values in HTML form fields.
17 – Created a few example services, Netbus, IMAP, Cisc0 console, Cisc0 enable etc….only tested NetBus.
18 – Completed the 'view authentication sequence' display.
19 - Added SMB authentication for Windows and Samba servers (Only uses API at the moment so is very sloow)

What does it do?

This component of Brutus is capable of authenticating against a wide range of character based application protocols. This is used to facilitate dictionary based user/password attacks against various network applications. This release comes with the following built-in network applications :

HTTP - Basic authentication
HTTP - CGI application authentication (typically used with HTML forms)
FTP
POP3
Telnet

There is also a **custom** facility which allows you to create your own authentication sequences tailored to your target in addition to being able to modify the built in applications. Using the custom facilty for instance it is possible to authenticate against IMAP, NNTP, IRC or nearly anything that uses plaintext user/password negotiation.

Using the pre-authentication option gives you the ability to perform some quite twisted dictionary attacks, for instance :

You can define an authentication sequence that will connect via some public SOCKS proxy to a UNIX server on 192.168.1.10 offering telnet. Brutus can then log in to the UNIX server and then issue commands such as 'telnet 172.16.10.10', Brutus will then run the dictionary attack against the target at 172.16.10.10. What you have now is a 3 node hop online dictionary attack.

A simpler example of using a pre-authentication sequence might be to have Brutus connect to the target, again a UNIX server running telnet, and perhaps log in as an unprivileged user. It is then possible to have Brutus run a dictionary attack using *su* in an attempt to obtain the root password. At all times Brutus will maintain the 'conduit' telnet session which improves performance.

Features

- Support for up to 60 simultaneous sessions
- Fully multi-threaded
- Highly customisable authentication sequences
- Single user mode, User List mode, User/Pass combo mode, Password only mode
- Brute force password mode
- Word list creation/generation/processing
- Import/Export custom services
- Load/Save position
- SOCKS support (with optional authentication)
- Capable of 2500+ authentications/second over high speed connections

What is happening?

Brutus is still under development as is this component (the authentication engine). When Brutus is eventually finished, it will be made available, I have no idea when that will be. However, the next release (barring bug-fix releases) will contain my own SMB authentication routines which are much faster than using the WNet API, initially Protocols up to and including LANMAN2 will be available. I am also working on getting SSL support in without using wininet.dll although that may take a bit longer. The next release will be an extension of Brutus AET2 rather than a rewrite.

Issues (which are being worked on)

1 - HTML Form Learning does not recognise the values for SELECT fields with HTML Forms.
2 - Remove Duplicates in word list tools is disabled.
3 - Update cookies is inactive in HTTP POST, the cookies are currently static.
4 - SMB mode will not handle target addresses that are not in UNC format.
5 - In HTTP (FORM/CGI) HTTP status codes such as 302 moved are read but not interpreted.

There are lots more issues...I'll update when I know what they are

Hints

DONT use lots of simultaneous connections unless it's beneficial to do so - Usually slow responding targets (like many POP3 servers which have 10 second + failure notification times) are the best candidates.
There are many variables to take into account, connection speed, authentication notification speed, server capacity, even your machine's capacity in some scenarios. Very often you will find less connections will give you more speed...this is important.

DON'T use the keepalive/stayconnected options if you are having problems - it is usually better to troubleshoot these things in one authentication per connection mode.

DO use keepalive/stay connected options if you can -they can greatly increase speed.

DO use positive authentication responses in your custom sequences - they are usually more reliable.

DO take note of the error indicators in the bottom right of the brutus main window -if they are flashing too often then consider changing some settings.

DO use a network sniffer if you can - to understand and troubleshoot authentication sequences to various services. Also consider using netcat or telnet to 'manually' authenticate against a service to see exactly what the server is responding with and what you need to tell it.

DO create custom word lists for your specific targets – If the target user(s) is/are known then create user specific wordlists using the built in password generator. Using target specific lists in conjunction with perhaps a list of common passwords probably offers you the best chance of positive authentication in a reasonable amount of time.

DON'T do anything with this tool that you might regret later

C*redits*

François PIETTE - TWSocket (a Winsock wrapper that is part of the ICS for Delphi - http://www.rtfm.be/fpiette.)
Borland - becasue Delphi is actually not bad

Misc

For updates see http://www.hoobie.net/brutus/
Mail to brutus@hoobie.net
28th January 2000