Exploitation

< Previous Page: Scanning | Next >
Medusa

Medusa is a log-in brute forcer that attempts to gain access to remote services by guessing at the user password. Medusa is capable of attacking a large number of remote services including FTP, HTTP, MySQL, Telnet, VNC, Web Form, and more. In order to use Medusa, you need several pieces of information including the target IP address, a username or username list that you are attempting to log in as, a password or dictionary file containing multiple passwords to use when logging in, and the name of the service you are attempting to authenticate with.

Medusa comes installed on Backtrack 5. However, if you are using a different version of backtrack without Medusa type:

apt-get update
apt-get install medusa

When using online password crackers, the potential for success can be greatly increased if you combine this attack with information gathered from reconnaissance and scanning. An example of this is when you find usernames, passwords, and email addresses. Programs like Medusa will take a username and password list and keep guessing until it uses all the passwords. Be aware that some remote access systems employ a password throttling technique that can limit the number of unsuccessful log-ins you are allowed. Your IP address can be blocked or the username can be locked out if you enter too many incorrect guesses.

Backtrack includes a few word lists that you can use for your brute forcing adventures. You can find one list at:

/pentest/passwords/wordlists/

Backtrack Tutorials: Password ListIn order to execute the brute-force attack, you open a terminal and type the following:

medusa –h target_ip –u username –P path_to_password_dictionary –M service_to_attack

“-h” is used to specify the IP address of the target host. The “-u” is used for a single username that Medusa will use to attempt log-ins. “-P” is used to specify an entire list containing multiple passwords. The “-P” needs to be followed by the actual location or path to the dictionary file. The “-M” switch is used to specify which service we want to attack.