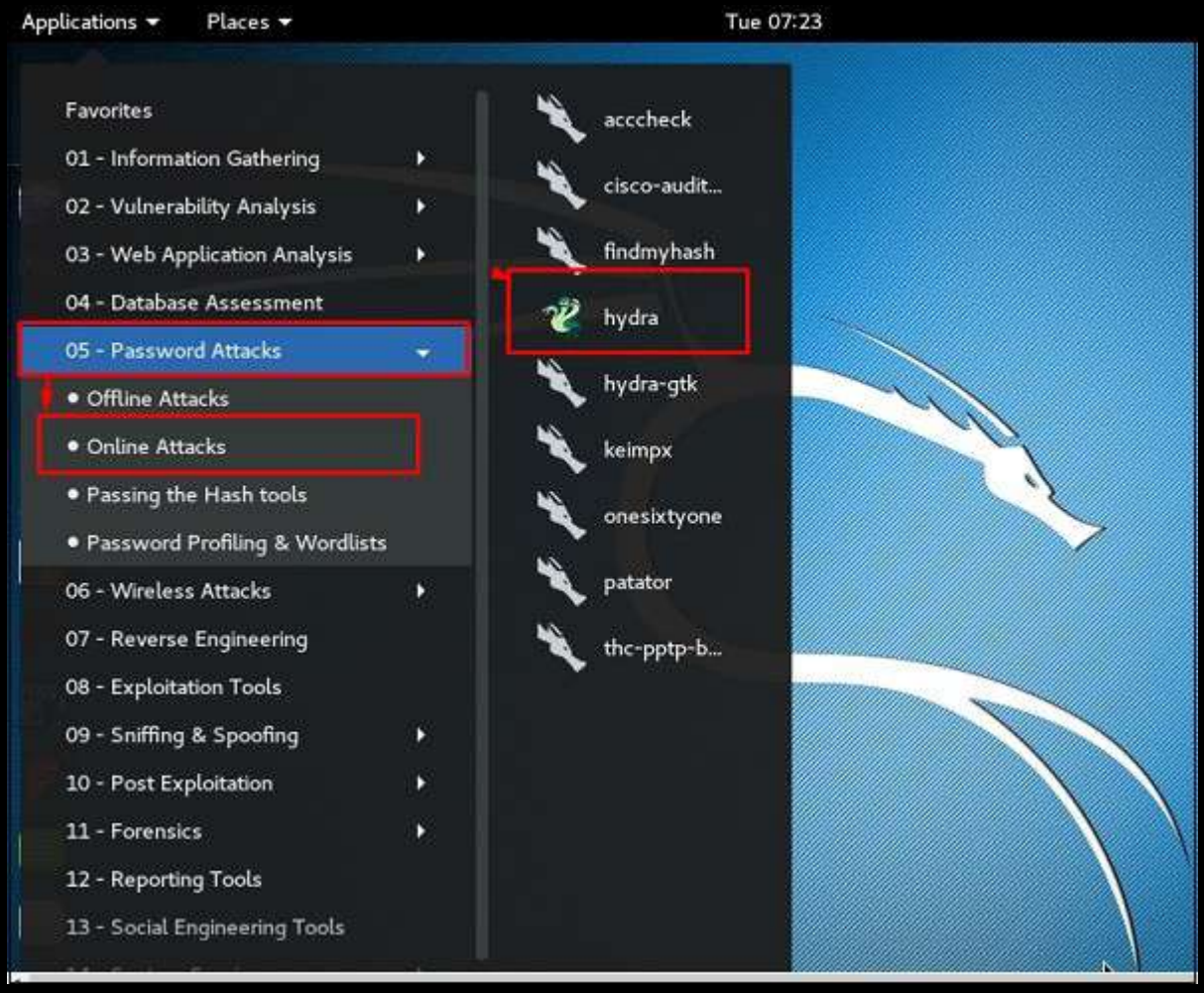
Password Cracking Tools

In this topic, we will learn about the important password cracking tools used in Kali Linux.

Hydra

Hydra is a login cracker that supports many protocols to attack (Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, HTTP(S)-FORM-POST, HTTP(S)-GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB(NT), SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP).

To open it, go to Applications → Password Attacks → Online Attacks → hydra.



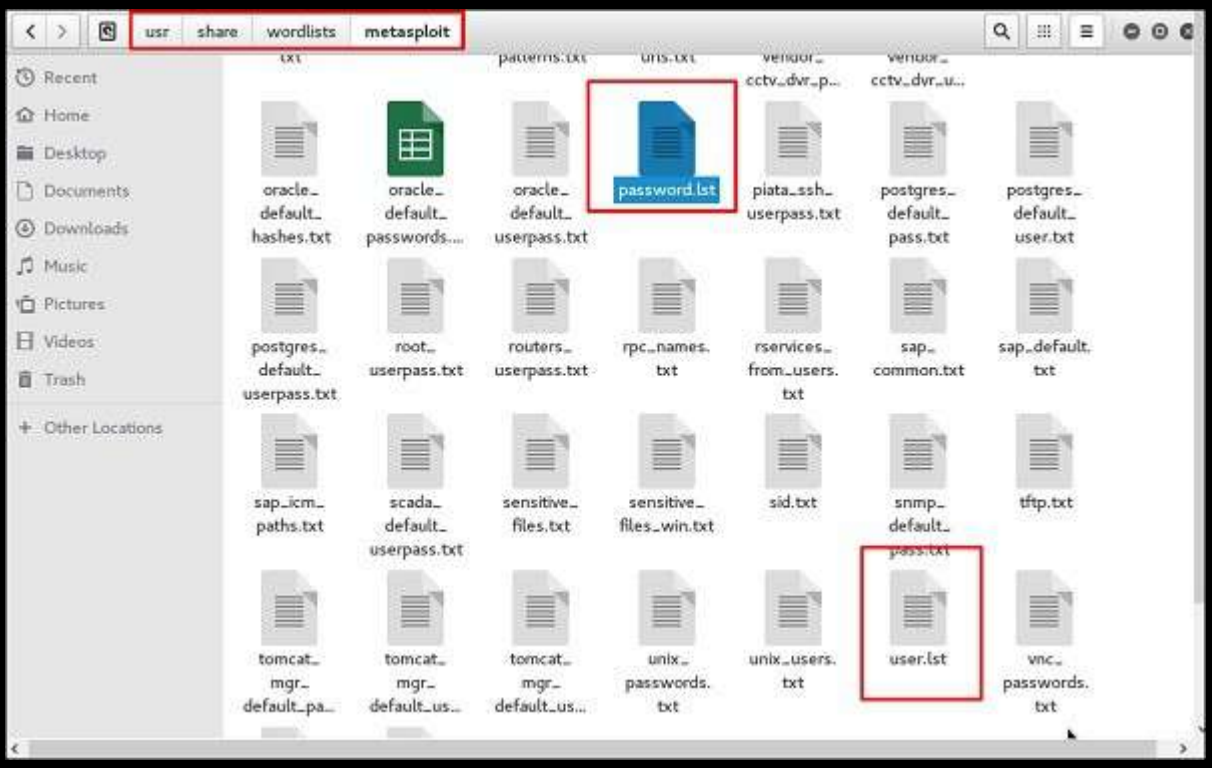
It will open the terminal console, as shown in the following screenshot.

```
Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
  hydra -l admin -p password ftp://[192.168.0.0/24]/
  hydra -L logins.txt -P pws.txt -M targets.txt ssh
root@kali:~#
```

In this case, we will brute force FTP service of metasploitable machine, which has IP 192.168.1.101

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:0c:c9:6e
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0c:c96e/64 Scope:Link
```

We have created in Kali a word list with extension 'lst' in the path **usr\share\wordlist\metasploit**.



The command will be as follows −

```
hydra -l /usr/share/wordlists/metasploit/user -P
/usr/share/wordlists/metasploit/ passwords ftp://192.168.1.101 –V
```

where **–V** is the username and password while trying

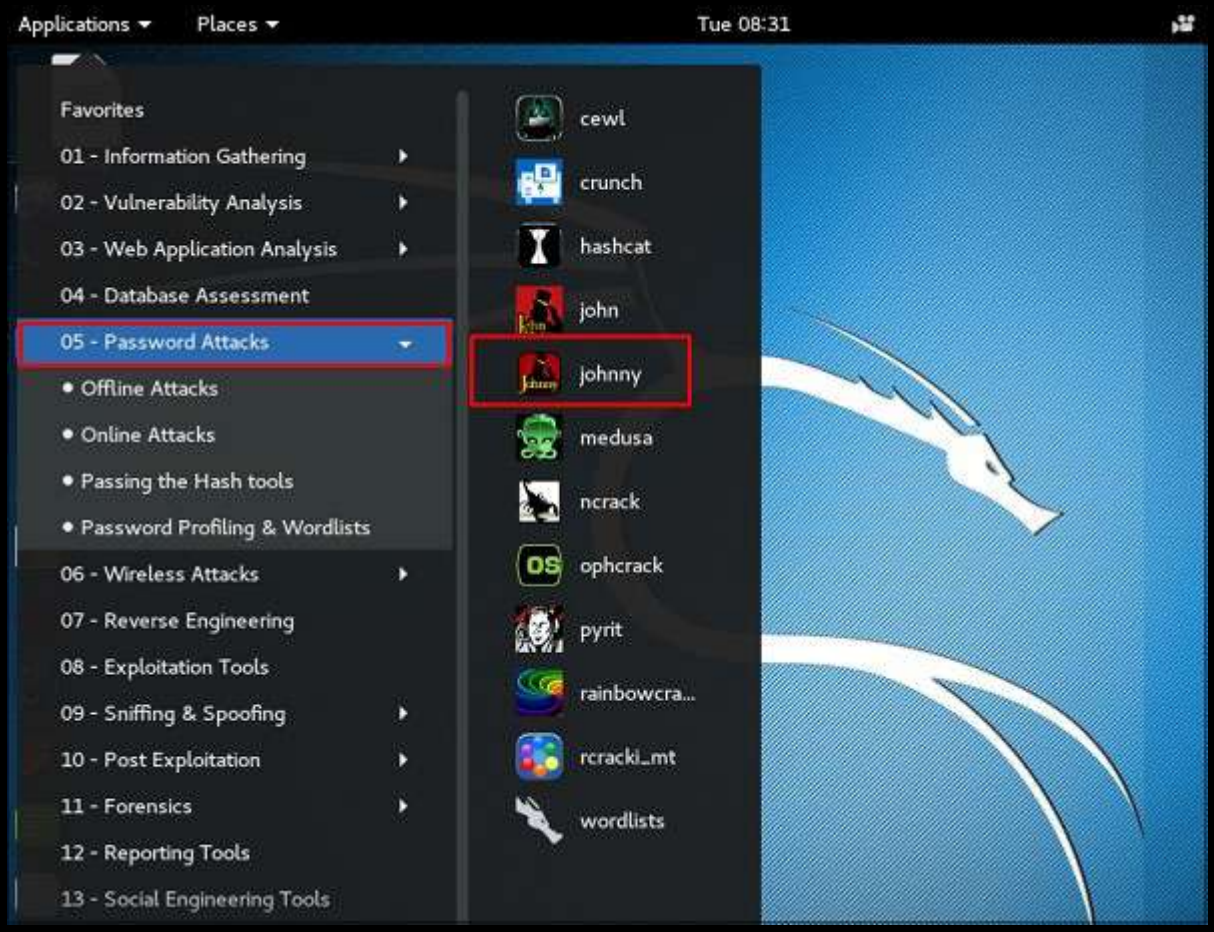
```
root@kali:~# hydra -l /usr/share/wordlists/metasploit/user -p /usr/share/wordlists/metasploit/password ftp://192
.168.1.101 -V
```

As shown in the following screenshot, the username and password are found which are msfadmin:msfadmin

Johnny

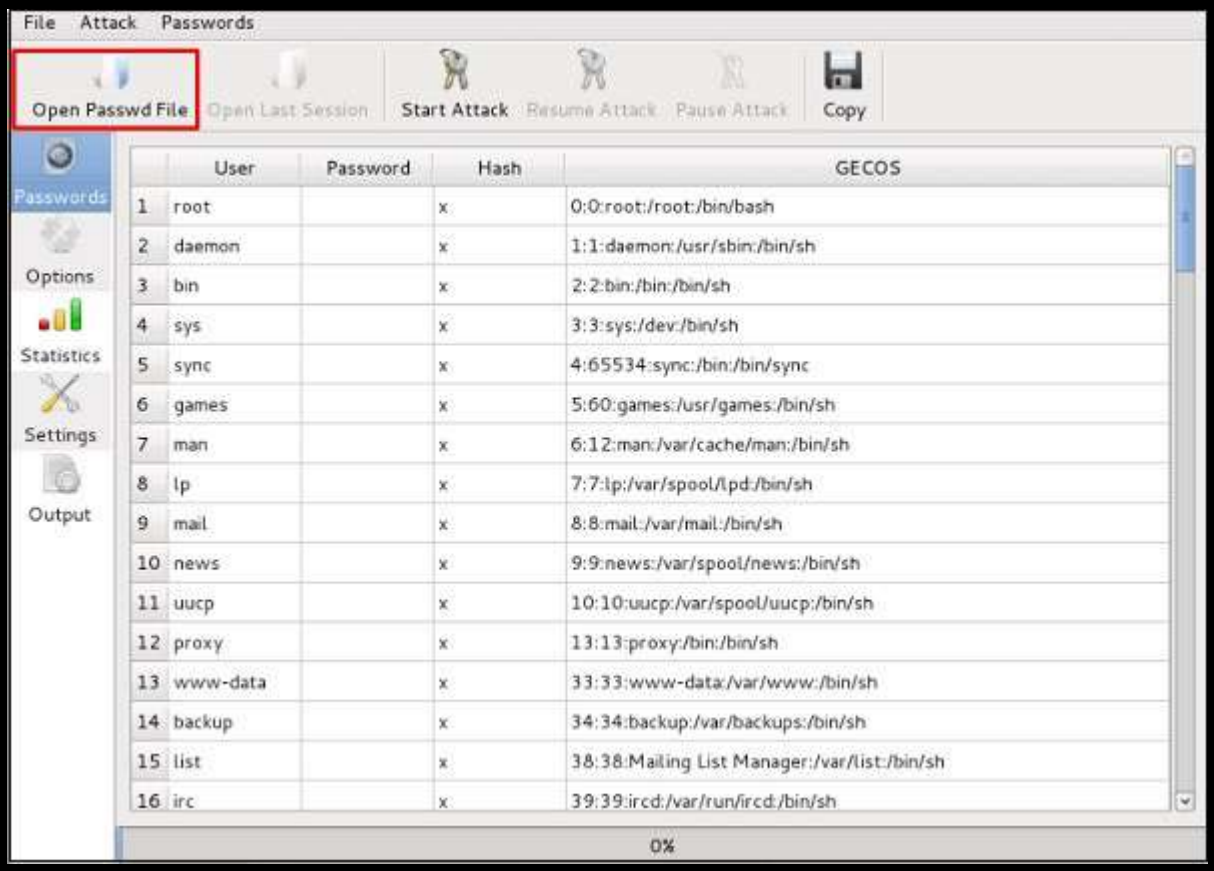
Johnny is a GUI for the John the Ripper password cracking tool. Generally, it is used for weak passwords.

To open it, go to Applications → Password Attacks → johnny.



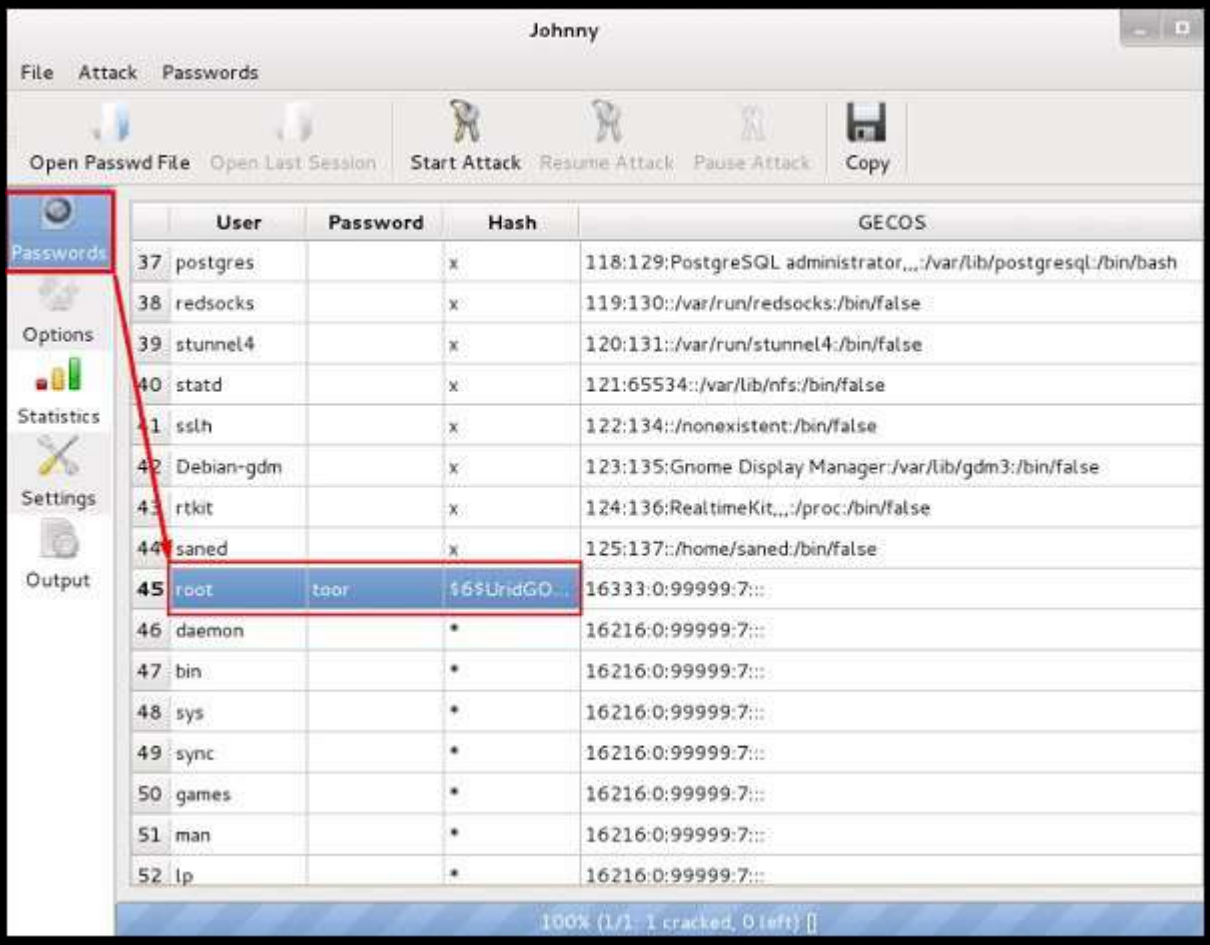
In this case, we will get the password of Kali machine with the following command and a file will be created on the desktop.

Click “Open Passwd File” → OK and all the files will be shown as in the following screenshot.



Click “Start Attack”.

After the attack is complete, click the left panel at “Passwords” and the password will be unshaded.



John

John is a command line version of Johnny GUI. To start it, open the Terminal and type "**john**".

```
root@kali:~# john
John the Ripper password cracker, version 1.8.0.6-jumbo-1-bleeding [linux-x86-64-avx]
Copyright (c) 1996-2015 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION]        "single crack" mode
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
                  --pipe  like --stdin, but bulk reads, and allows rules
--loopback[=FILE]         like --wordlist, but fetch words from a .pot file
--dupe-suppression        suppress all dupes in wordlist (and force preload)
--prince[=FILE]           PRINCE mode, read words from FILE
--encoding=NAME           input encoding (eg. UTF-8, ISO-8859-1). See also
                          doc/ENCODING and --list=hidden-options.
--rules[=SECTION]         enable word mangling rules for wordlist modes
--incremental[=MODE]      "incremental" mode [using section MODE]
--mask=MASK               mask mode using MASK
--markov[=OPTIONS]        "Markov" mode (see doc/MARKOV)
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
```

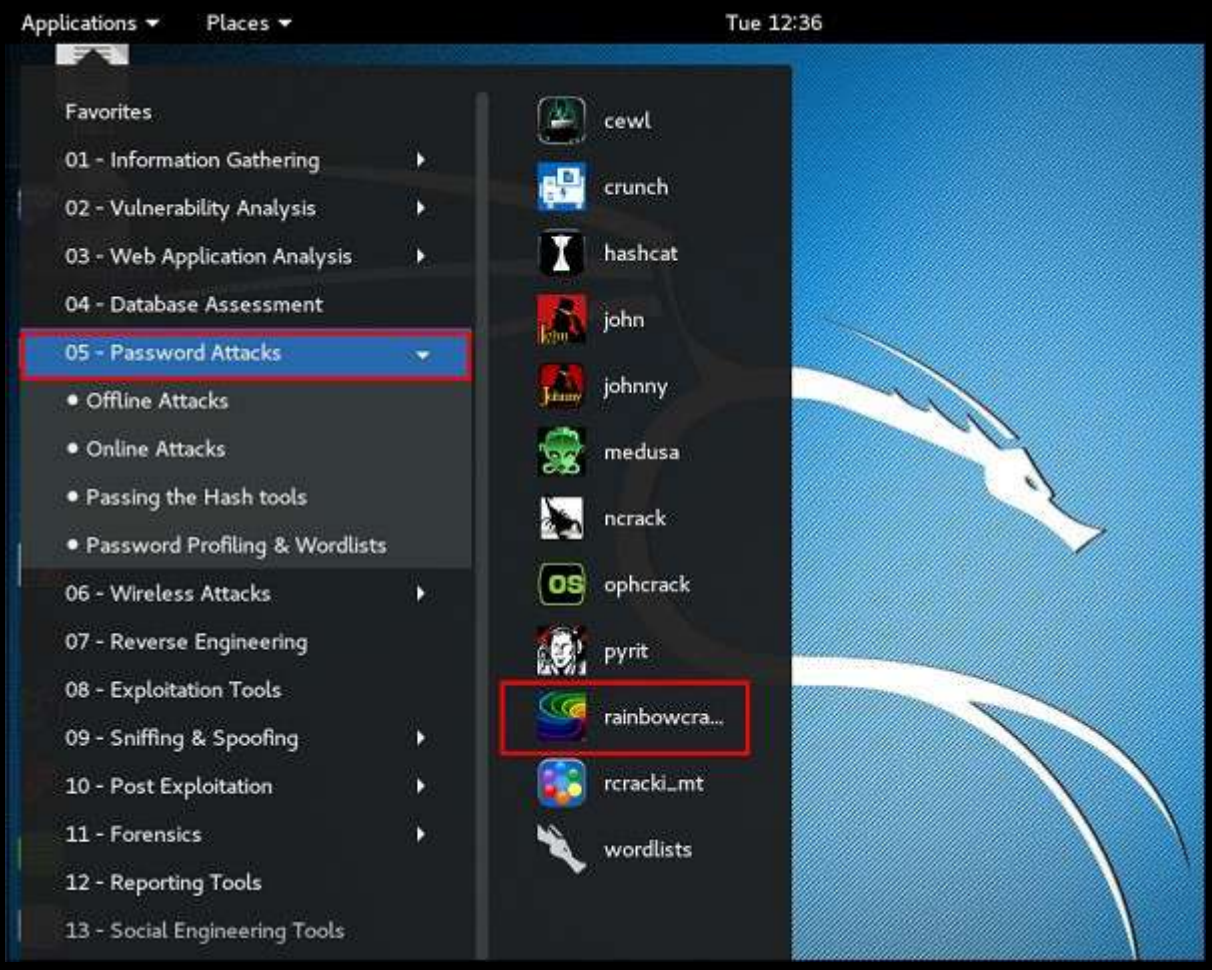
In case of unshadowing the password, we need to write the following command –

```
root@kali:~# unshadow passwd shadow > unshadowed.txt
```

Rainbowcrack

The RainbowCrack software cracks hashes by rainbow table lookup. Rainbow tables are ordinary files stored on the hard disk. Generally, Rainbow tables are bought online or can be compiled with different tools.

To open it, go to Applications → Password Attacks → click “rainbowcrack”.

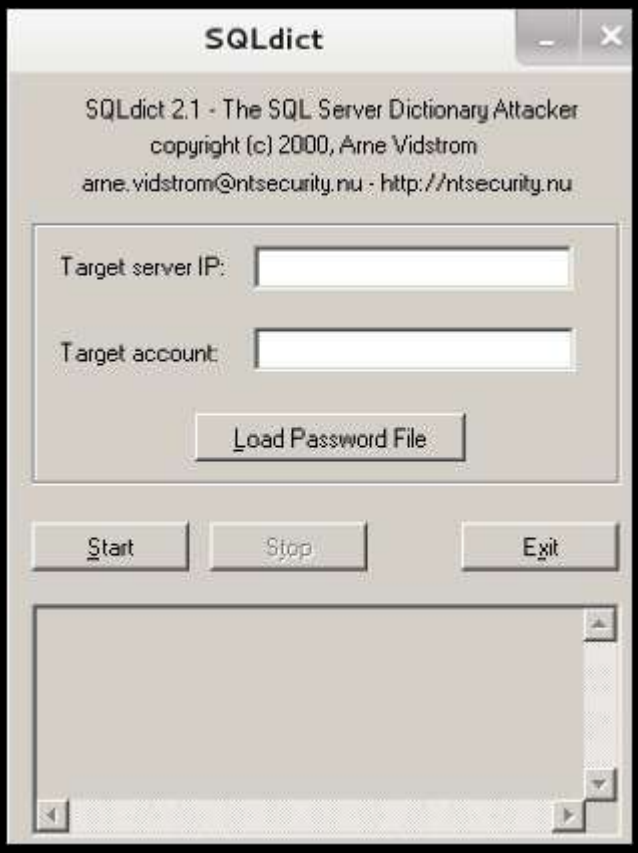


The command to crack a hash password is −

```
rcrack path_to_rainbow_tables -f path_to_password_hash
```

SQLdict

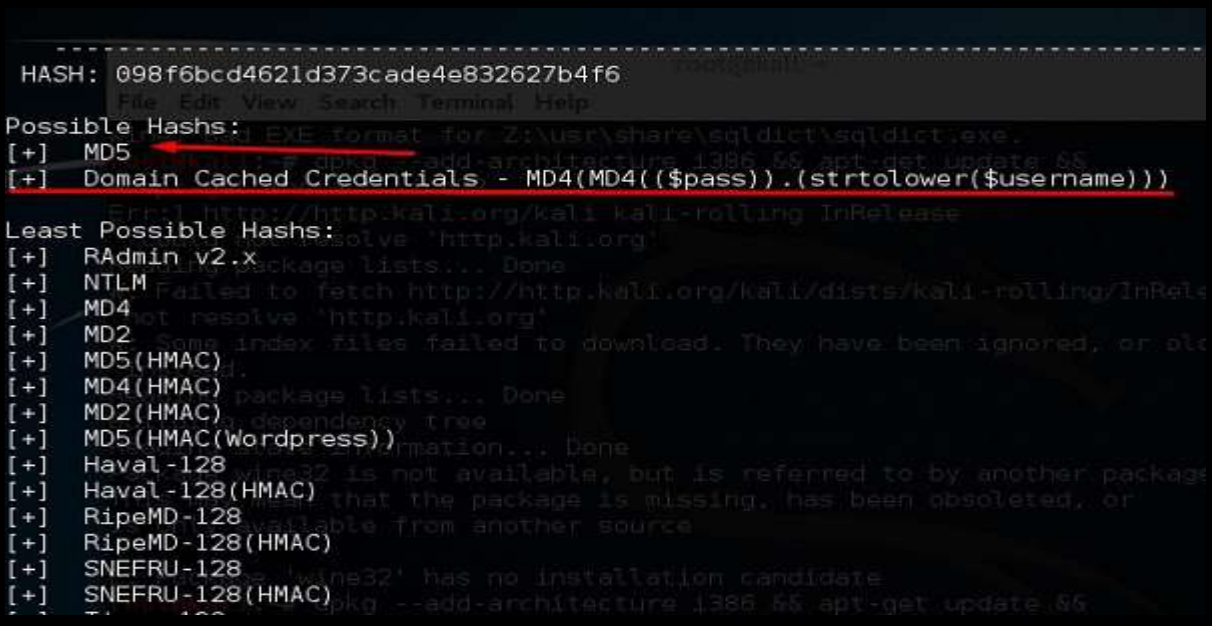
It is a dictionary attack tool for SQL server and is very easy and basic to be used. To open it, open the terminal and type “**sqldict”**. It will open the following view.



Under “Target IP Server”, enter the IP of the server holding the SQL. Under “Target Account”, enter the username. Then load the file with the password and click “start” until it finishes.

hash-identifier

It is a tool that is used to identify types of hashes, meaning what they are being used for. For example, if I have a HASH, it can tell me if it is a Linux or windows HASH.



The above screen shows that it can be a MD5 hash and it seems a Domain cached credential.