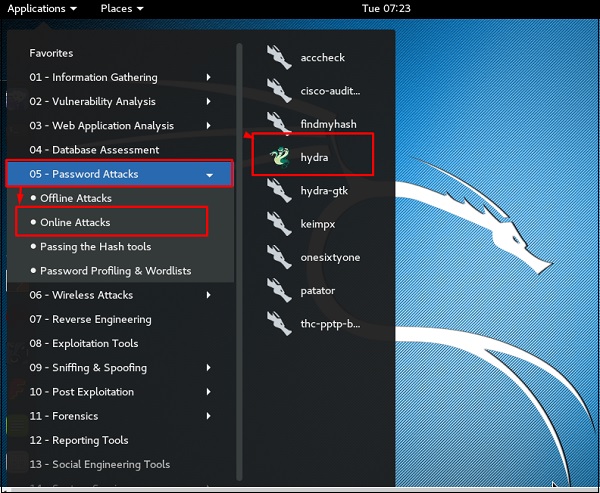
Hydra

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.



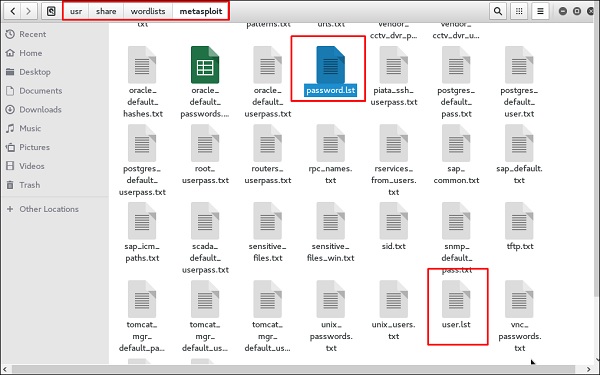
It will open the terminal console, as shown in the following screenshot.



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

Brute Force

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



The command will be as follows −

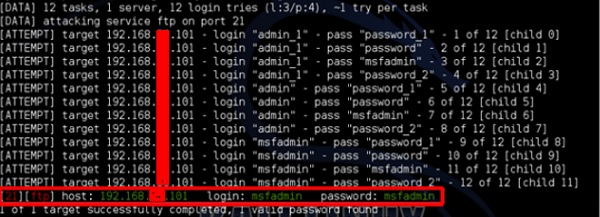
hydra -l /usr/share/wordlists/metasploit/user -P

/usr/share/wordlists/metasploit/ passwords ftp://192.168.1.101 –V

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

Hydra Command

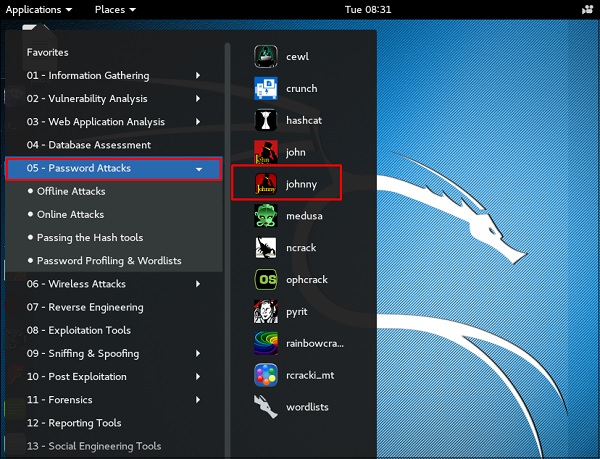
As shown in the following screenshot, the username and password are found which are msfadmin:msfadmin



Johnny

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

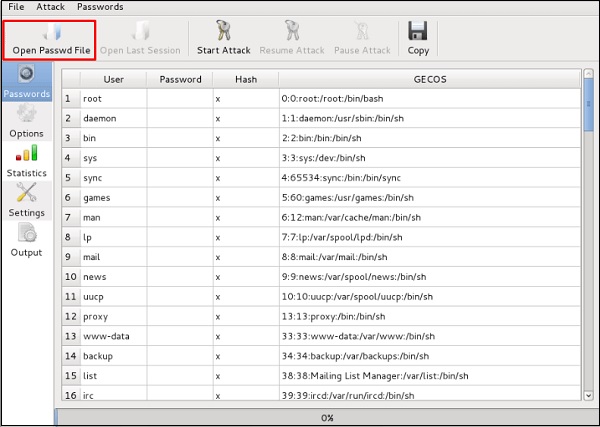
To open it, go to Applications → Password Attacks → johnny.



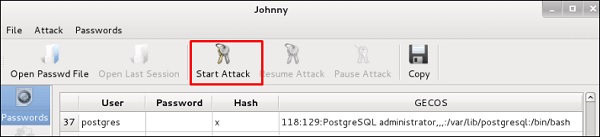
In this case, we will get the password of Kali machine with the following command and a file will be created on the desktop.



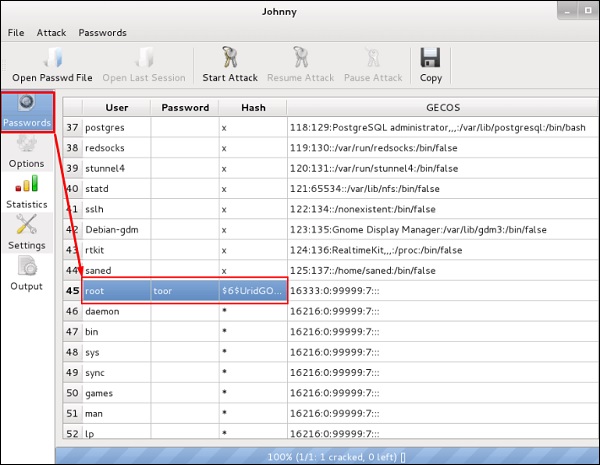
Click “Open Passwd File” → OK and all the files will be shown as in the following screenshot.



Click “Start Attack”.

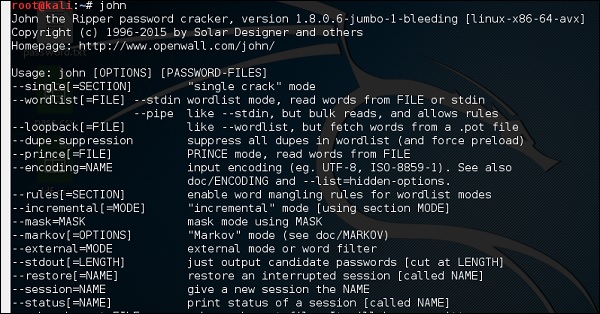


After the attack is complete, click the left panel at “Passwords” and the password will be unshaded.



John

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



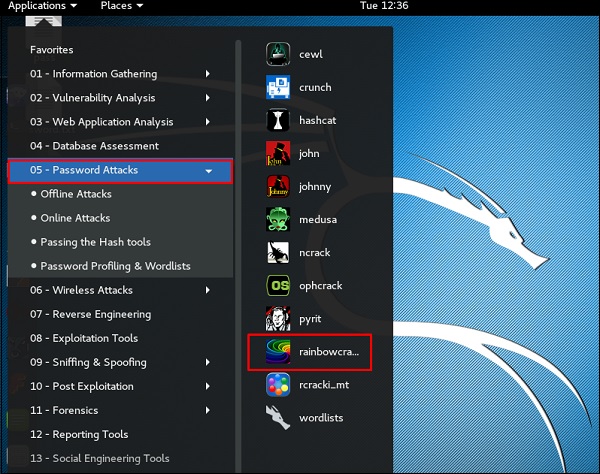
In case of unshadowing the password, we need to write the following command −

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”.

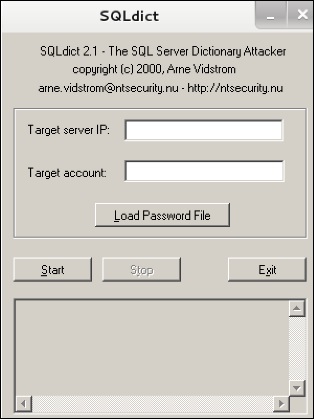


The command to crack a hash password is −

rcrack path\_to\_rainbow\_tables -f path\_to\_password\_hash

SQLdict

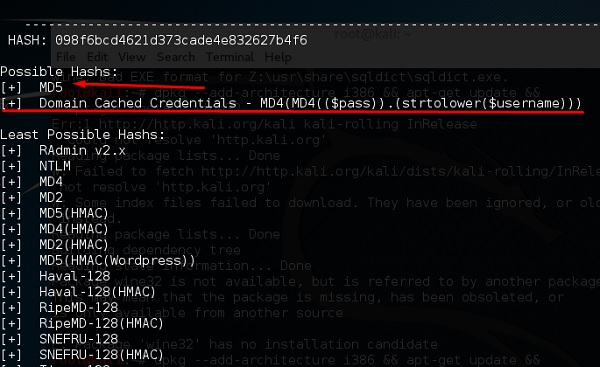
It is a dictionary attack tool for SQL server and is very easy and basic to be used. To open it, open the terminal and type **“sqldict”**. It will open the following view.



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.

Print Page