**The Metasploit Framework**

**Open-Source exploitation framework**

Can perform:

* Recon
* Reporting/logging
* Keeps track of exploits for the framework
* Meterpreter
  + Special shell that allows you to load in tools without touching the disk

**Msfconsole**

Everything done in msf is considered a ‘job’

Module commands: recon, exploit, payloads, priv escalation

**The Meterpreter**

**Can be used to execute many different exploits** (--help)

* Hashdump
* Timestomp

**Getsystem** – attempt to elevate your privileges to that of the local system

* By trying all known privilege escalation techniques
* Best to research and understand what this cmd does because sometimes it could be too invasive for what you’re trying to do for example

Enumdesktops

* Shows what windows are open

Keyscan

* Keylog

Idletime

* See how long user has been idle for
* Knowing that there aren’t any browser windows open and they’ve been idle for a while can indicate the user isn’t currently at the machine

Persistence

User impersonations

Meterpreter doesn’t start its own process; it sits inside an already running process/executable

**Modules**

Usr/share/metasploit-framework/modules 🡪 /exploits/windows

* Auxiliary (Recon)
* Encoders
* Exploits
* Nops
* Payloads (e.g., Meterpreter)
* Post

**Example of SSH exploit in Ruby:**

Graphical user interface, text, application

Description automatically generated

**MsfVenom**

Payload generator

Msfvenom -p windows/meterpreter/reverse\_tcp -f python

* -p generates payload
* -f formats code into op code
* Python specifies in which way we want it to be formatted
  + Will dump meterpreter shell in python and generate the shell code which can be copy and pasted into exploit
* Most people generally use C as it doesn’t care what the variable isa

Badchar (0x0)

-b ‘\0x0’ will kick out the bad character

* Some encoders won’t work with badchars

Graphical user interface, application, Word

Description automatically generated