Metasploit Cheat Sheet

Step 1: Core Commands

At its most basic use, meterpreter is a Linux terminal on the victim's computer. As such, many of our basic Linux commands can be used on the meterpreter even if it's on a Windows or other operating system.

Here are some of the core commands we can use on the meterpreter.

- **?** - help menu
- **background** - moves the current session to the background
- **bgkill** - kills a background meterpreter script
- **bglist** - provides a list of all running background scripts
- **bgrun** - runs a script as a background thread
- **channel** - displays active channels
- **close** - closes a channel
- **exit** - terminates a meterpreter session
- **help** - help menu
- **interact** - interacts with a channel
- **irb** - go into Ruby scripting mode
- **migrate** - moves the active process to a designated PID
- **quit** - terminates the meterpreter session
- **read** - reads the data from a channel
- **run** - executes the meterpreter script designated after it
- **use** - loads a meterpreter extension
- **write** - writes data to a channel

Step 2: File System Commands

- **cat** - read and output to stdout the contents of a file
- **cd** - change directory on the victim
- **del** - delete a file on the victim
- **download** - download a file from the victim system to the attacker system
- **edit** - edit a file with vim
- **getlwd** - print the local directory
- **getwd** - print working directory
- **lcd** - change local directory
- **lpwd** - print local directory
- **ls** - list files in current directory
- **mkdir** - make a directory on the victim system
- **pwd** - print working directory
- **rm** - delete a file
- **rmdir** - remove directory on the victim system
- **upload** - upload a file from the attacker system to the victim

Step 3: Networking Commands

- **ipconfig** - displays network interfaces with key information including IP address, etc.
- **portfwd** - forwards a port on the victim system to a remote service
- **route** - view or modify the victim routing table

Step 4: System Commands

- **clearav** - clears the event logs on the victim's computer

- **drop_token** - drops a stolen token
- **execute** - executes a command
- **getpid** - gets the current process ID (PID)
- **getprivs** - gets as many privileges as possible
- **getuid** - get the user that the server is running as
- **kill** - terminate the process designated by the PID
- **ps** - list running processes
- **reboot** - reboots the victim computer
- **reg** - interact with the victim's registry
- **rev2self** - calls RevertToSelf() on the victim machine
- **shell** - opens a command shell on the victim machine
- **shutdown** - shuts down the victim's computer
- **steal_token** - attempts to steal the token of a specified (PID) process
- **sysinfo** - gets the details about the victim computer such as OS and name

Step 5: User Interface Commands

- **enumdesktops** - lists all accessible desktops
- **getdesktop** - get the current meterpreter desktop
- **idletime** - checks to see how long since the victim system has been idle
- **keyscan_dump** - dumps the contents of the software keylogger
- **keyscan_start** - starts the software keylogger when associated with a process such as Word or browser
- **keyscan_stop** - stops the software keylogger
- **screenshot** - grabs a screenshot of the meterpreter desktop
- **set_desktop** - changes the meterpreter desktop
- **uictl** - enables control of some of the user interface components

Step 6: Privilege Escalation Commands

- **getsystem** - uses 15 built-in methods to gain sysadmin privileges

Step 7: Password Dump Commands

- **hashdump** - grabs the hashes in the password (SAM) file

Note that hashdump will often trip AV software, but there are now two scripts that are more stealthy, "run hashdump" and "run smart_hashdump". Look for more on those on my upcoming meterpreter script cheat sheet.

Step 8: Timestomp Commands

- **timestomp** - manipulates the modify, access, and create attributes of a file