

Windows Meterpreter

Core Commands

- Help menu — ?
- Backgrounds the current session — **background**
- Alias for background — **bg**
- Kills a background meterpreter script — **bgkill**
- Lists running background scripts — **bglist**
- Executes a meterpreter script as a background thread — **bgrun**
- Displays information or control active channels — **channel**
- Closes a channel — **close**
- Detach the meterpreter session (for http/https) — **detach**
- Disables encoding of unicode strings — **disable_unicode_encoding**
- Enables encoding of unicode strings — **enable_unicode_encoding**
- Terminate the meterpreter session — **exit**
- Get the current session timeout values — **get_timeouts**
- Get the session GUID — **guid**
- Help menu — **help**
- Displays information about a Post module — **info**
- Open an interactive Ruby shell on the current session — **irb**
- Load one or more meterpreter extensions — **load**
- Get the MSF ID of the machine attached to the session — **machine_id**
- Migrate the server to another process — **migrate**
- Manage pivot listeners — **pivot**
- Open the Pry debugger on the current session — **pry**
- Terminate the meterpreter session — **quit**
- Reads data from a channel — **read**
- Run the commands stored in a file — **resource**
- Executes a meterpreter script or Post module — **run**
- (Re)Negotiate TLV packet encryption on the session — **secure**
- Quickly switch to another session — **sessions**
- Set the current session timeout values — **set_timeouts**
- Force Meterpreter to go quiet, then re-establish session — **sleep**
- Modify the SSL certificate verification setting — **ssl_verify**
- Manage the transport mechanisms — **transport**
- Deprecated alias for "load" — **use**
- Get the UUID for the current session — **uuid**
- Writes data to a channel — **write**

File system Commands

- cat** — Read the contents of a file to the screen
- cd** — Change directory
- checksum** — Retrieve the checksum of a file
- cp** — Copy source to destination
- del** — Delete the specified file
- dir** — List files (alias for ls)
- download** — Download a file or directory
- edit** — Edit a file
- getlwd** — Print local working directory
- getwd** — Print working directory
- lcat** — Read the contents of a local file to the screen
- lcd** — Change local working directory
- lls** — List local files
- lpwd** — Print local working directory
- ls** — List files
- mkdir** — Make directory
- mv** — Move source to destination
- pwd** — Print working directory
- rm** — Delete the specified file
- rmdir** — Remove directory
- search** — Search for files
- show_mount** — List all mount points/logical drives
- upload** — Upload a file or directory

System Commands

- clearev** — Clear the event log
- drop_token** — Relinquishes any active impersonation token.
- execute** — Execute a command
- getenv** — Get one or more environment variable values
- getpid** — Get the current process identifier
- getprivs** — Attempt to enable all privileges available to the current process
- getsid** — Get the SID of the user that the server is running as
- getuid** — Get the user that the server is running as
- kill** — Terminate a process
- localtime** — Displays the target system local date and time
- pgrep** — Filter processes by name
- pkill** — Terminate processes by name
- ps** — List running processes
- reboot** — Reboots the remote computer
- reg** — Modify and interact with the remote registry
- rev2self** — Calls RevertToSelf() on the remote machine
- shell** — Drop into a system command shell
- shutdown** — Shuts down the remote computer
- steal_token** — Attempts to steal an impersonation token from the target process
- suspend** — Suspends or resumes a list of processes
- sysinfo** — Gets information about the remote system, such as OS

User interface Commands

- enumdesktops** — List all accessible desktops and window stations
- getdesktop** — Get the current meterpreter desktop
- idletime** — Returns the number of seconds the remote user has been idle
- keyboard_send** — Send keystrokes
- keyevent** — Send key events
- keyscan_dump** — Dump the keystroke buffer
- keyscan_start** — Start capturing keystrokes
- keyscan_stop** — Stop capturing keystrokes
- mouse** — Send mouse events
- screenshare** — Watch the remote user desktop in real time
- screenshot** — Grab a screenshot of the interactive desktop
- setdesktop** — Change the meterpreters current desktop
- uictl** — Control some of the user interface components

Webcam Commands

- record_mic** — Record audio from the default microphone for X seconds
- webcam_chat** — Start a video chat
- webcam_list** — List webcams
- webcam_snap** — Take a snapshot from the specified webcam
- webcam_stream** — Play a video stream from the specified webcam

Networking Commands

- Display the host ARP cache — **arp**
- Display the current proxy configuration — **getproxy**
- Display interfaces — **ifconfig**
- Display interfaces — **ipconfig**
- Display the network connections — **netstat**
- Forward a local port to a remote service — **portfwd**
- Resolve a set of host names on the target — **resolve**
- View and modify the routing table — **route**

Privilege: Elevate Commands

- Attempt to elevate your privilege to that of local system. — **getsystem**

Privilege: Password Database Commands

- Dumps the contents of the SAM database — **hashdump**

Privilege: Timestomp Commands

- Manipulate file MACE attributes — **timestomp**



@hackinarticles



https://github.com/Ignitetechnologies



https://in.linkedin.com/company/hackingarticles