Recon-ng 5.1 Cheat Sheet

https://github.com/lanmaster53/recon-ng
@BHInfoSecurity && @BBhacKing
https://www.blackhillsinfosec.com/
2019-11-21

4.x	5.x	Note
<nothing>	`marketplace install all`	installs the modules
`workspaces add`	`workspaces create`	makes a new workspace
`workspaces select x`	`workspaces load x`	moves into workspace x context
`add companies`	`db insert companies`	manually load seed data
`load $module`	`modules load $module`	"use" is gone
`ls`	`!ls` or `shell ls`	OS commands require a prefix
`set verbosity 2`	`options set VERBOSITY 2`	tab-completes from any case, but execution requires ALL CAPS
`set source query ...`	`options set SOURCE query ...`	case-sensitive 'SOURCE'
`show dashboard`	`dashboard show`	bare "dashboard" works, too

Object	Verbs
workspaces	`create` | `load` | `list` | `remove`
db	`insert` | `delete` | `query` | `schema` | `notes`
modules	`load` | `reload` | `search`
options	`set` | `unset` | `list` *`option names are ALL_CAPS`*
marketplace	`install` | `remove` | `info` | `refresh` | `search`
keys	`add` | `remove` | `list`
script	`record [filename]` | `execute [filename]` | `stop` | `status`
snapshots	`take` | `remove` | `list` | `load [snapshot_name]`
spool	`start [filename]` | `stop` | `status`

Handy Command	Why Handy
`marketplace install all`	Because there are no modules installed by default.
`show companies`	Shows the whole table, incluing the "rowid" which you sometimes need.
`db query select * from companies`	Basic query syntax. Gives same result as "show companies" except omits the "rowid" column.
`dashboard`	Shows which modules have been run in the current workspace.
`modules search $regex`	Gives a list of modules matching $regex. "modules" is plural, and $regex is a literal regex
`shell ls`	runs operating system's "ls" command in your current working directory
`!ls`	Same as above
`marketplace search`	Shows modules available in the marketplace (there is no "marketplace list" command)
`marketplace search $regex`	Shows marketplace modules matching $regex
`marketplace info $string`	Shows details of modules in the marketplace that contain $string

Things to Know
Read the wiki. It's not long. The inline 'help' command is far more helpful if you've read the wiki.
The framework warns you at startup with a red "key not set" message for specific modules whose API keys are not present.
Spool files are written to your current working directory in the filename you pass to 'spool record [filename]'
Script files are written to your current working directory in the filename you pass to 'script record [filename]'
Snapshots are stored in the .recon-ng/workspaces/$current_workspace directory and named automatically with embedded timestamp
The word for "get rid of" varies by object type among {delete, remove, unset}
The word for "create" varies by object type among {create, insert, add, install, record, take, start}