Recon-ng Cheat Sheet

by Simran Malakar

Workspace Commands

`workspaces create <name>`	Create a new workspace
`workspaces list`	List all workspaces
`workspaces load <name>`	Load a workspace
`workspaces remove <name>`	Remove a workspace

Marketplace Commands

`marketplace info <module>`	Get info about a module
`marketplace install <module>`	Install a module
`marketplace remove <module>`	Remove a module
`marketplace search <term>`	Search marketplace for a module

Module Commands

`modules load <path>`	Load a module
`info`	Display module information
`options`	Show module options
`options set <KEY> <VALUE>`	Set input option for the module
`run`	Execute the module

View Data Commands

`show hosts`	Display discovered hosts
`show domains`	Display discovered domains
`show contacts`	Show email/person contact data
`show credentials`	Show found credentials

Recon-ng Cheat Sheet

by Simran Malakar

Tips and Workflow

1. Start Recon-ng:
   - recon-ng

2. Create and Load Workspace
   - workspaces create test_project
   - workspaces load test_project

3. Install Required Modules
   - marketplace search whois
   - marketplace install recon/domains-contacts/whois_pocs
   - marketplace install recon/domains-hosts/google_site_web
   - marketplace install recon/hosts-hosts/resolve

4. Load a Module
   - modules load recon/domains-contacts/whois_pocs

5. View Module Info and Options
   - info
   - options

6. Set Required Options
   - options set SOURCE example.com

7. Run the Module
   - run

8. View Collected Data
   - show hosts
   - show domains
   - show contacts

9. Continue Enumeration with More Modules
   - modules load recon/domains-hosts/google_site_web
   - options set DOMAIN example.com
   - run

10. Export or Save Logs (Optional)
    - spool start output.txt
    - show hosts