



### Activity File: Recon-ng

- In this activity, you will continue to play the role of a pen tester conducting an engagement on MegaCorpOne.
- You are tasked with determining whether MegaCorpOne's domain server info is accessible using OSINT tools.
- You will use the Shodan API and Recon-ng to perform your tests, and then you'll summarize your findings in a report.

**⚠ Reminder:** Don't forget to save your findings, as you will add them to your report on Day 4!

### Instructions

1. In Ubuntu, log in with the credentials `root:kali` and start Recon-ng.
  - In Recon-ng, run `modules search` to view all the currently installed modules.
  - Run `modules load recon/domains-hosts/hackertarget`.
  - This will load the `hackertarget` scanner module.
  - Modules need to be loaded before use.
2. In Recon-ng, type the command to view all the currently installed modules.
  - For this activity, we'll use the following two modules:
    - `recon/domains-hosts/hackertarget`
    - `reporting/html`
3. Type the command that will query hackertarget.com for a scan against megacorpone.com.

```
[recon-ng][default][hackertarget] > info

Name: HackerTarget Lookup
Author: Michael Henriksen (@michenriksen)
Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name      Current Value      Required  Description
  -----
SOURCE     megacorpone.com           yes       source of input (see 'info' for details)

Source Options:
  default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>     string representing a single input
  <path>       path to a file containing a list of inputs
  query <sql>  database query returning one column of inputs

[recon-ng][default][hackertarget] > run

MEGACORPONE.COM

[*] Country: None
[*] Host: admin.megacorpone.com
[*] Ip_Address: 167.114.21.64
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: beta.megacorpone.com
[*] Ip_Address: 167.114.21.65
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
```

- The results will automatically display verbosely in the terminal window.
- 4. Install the reporting module, then use the module.
  - `marketplace install reporting/html`
- 5. Type the command that shows which parameters need to be set.
  - The `CREATOR` and `CUSTOMER` parameters need to be set.
  - Set the parameters as follows:
    - `CREATOR`: Pentester
    - `CUSTOMER`: MegaCorpOne

- Type the command that runs the query so the results are saved to `/root/.recon-ng/workspaces/default/results.html`.

```
[recon-ng][default][hackertarget] > modules load reporting/html
[recon-ng][default][html] > info
```

Name: HTML Report Generator			
Author: Tim Tomes (@lanmaster53)			
Version: 1.0			
Description: Creates an HTML report.			
Options:			
Name	Current Value	Required	Description
CREATOR		yes	use creator name in the report
footer			
CUSTOMER		yes	use customer name in the report
header			
FILENAME	/root/.recon-ng/workspaces/default/results.html	yes	path and filename for report output
SANITIZE	True	yes	mask sensitive data in the report

```
[recon-ng][default][html] > options set CREATOR Pentester
CREATOR ⇒ Pentester
[recon-ng][default][html] > options set CUSTOMER MegaCorpOne
CUSTOMER ⇒ MegaCorpOne
[recon-ng][default][html] > info
```

Name: HTML Report Generator			
Author: Tim Tomes (@lanmaster53)			
Version: 1.0			
Description: Creates an HTML report.			
Options:			
Name	Current Value	Required	Description
CREATOR	Pentester	yes	use creator name in the report
footer			
CUSTOMER	MegaCorpOne	yes	use customer name in the report

- Type the command that verifies whether the configuration took effect after setting the options.

## 6. View the report.

- Generate the report so that it can be viewed as HTML in the web browser.
- How many hosts did Recon-ng discover? **33**

```
(root@kali)~# xdg-open /root/.recon-ng/workspaces/default/results.html
```

# MegaCorpOne

## Recon-ng Reconnaissance Report

### [-] Summary

table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	33
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

### [+] Hosts

Created by: Pentester  
Sun, Apr 13 2025 19:12:34