Gathering OSINT on a Domain

Scenario

Before you begin dedicating time and resources to actively scanning the target's network, you want to start out by taking a less intrusive approach: open source intelligence (OSINT) gathering. Publicly available sources of information can reveal a great deal about a target—enough to hone your eventual attack on the organization. You will use Recon-ng to teach new team members to perform passive reconnaissance. You want them to learn how to glean as much information as they can on the people and technology that the target organization employs.

You'll be using your Kali Linux computer to gather OSINT.

You'll be gathering intelligence on a real domain so that your results will be more meaningful.

Start Recon-ng and prepare a workspace

1. On your Kali Linux machine, log in your account
2. In Kali Linux, open a terminal.
3. At the prompt, enter `recon-ng`

   Recon-ng is a useful tool for gathering many different types of OSINT. Take a few minutes and review OSINT on the web if necessary.

4. Enter `workspaces create pen_test`
5. Verify that your prompt changes to **[recon-ng][pen_test] >**, indicating that your new workspace is active.
6. Enter `workspaces list` to list the workspaces

Examine some of the available modules

1. Enter `marketplace search`

   Examine the list of modules.

   A module is a specific task that Recon-ng will execute based on the parameters you provide it. The Recon category has the most modules by far. There are a few modules that focus on discovery and exploitation, and there are also modules for importing data and generating reports.

Search the domain for contact information.

1. Enter `marketplaces search whois`
2. Enter `marketplaces install recon/domains-contacts/whois_pocs`
3. Enter `modules load recon/domains-contacts/whois_pocs`
4. Verify that your prompt changes to **[recon-ng][pen_test][whois_pocs] >**

    > If your prompt stays at **[recon-ng][pen_test] >** you'll need to press the **Up** arrow on your keyboard and then enter the command again. This also goes for any other modules used in this activity.

5. Enter `info`
6. Verify that the only option you can set is the **SOURCE** option.

    This is the target of the scan, and because you added a domain to your workspace earlier, the default target will be that domain.

7. Enter `options set SOURCE comptia.org`
8. Enter `run`
9. Verify that some contacts were found, including the contacts' names and email addresses.

Search an account for evidence of compromise

1. From the Kali Linux, open the **Firefox**
2. Navigate to **https://haveibeenpwned.com**

    The Have I Been Pwned? (HIBP) database identifies if a particular email account is known to have been affected by any major breaches in the last few years.

3. In the text box, type any one of the accounts you enumerated in the Recon-ng modules, then select **pwned?**
4. Verify that you received results for the account. If no results are found, try one of the other email addresses until you get a hit.

Identify the organization's social media presence

1. Enter `marketplaces search profiler`
2. Enter `marketplaces install recon/profiles-profiles/profiler`
3. Enter `modules load recon/profiles-profiles/profiler`
4. Enter `info`
5. Enter `options set SOURCE comptia.org`
6. Enter `run`
7. Examine the list of social media sites and look for matches.

Matches have a green bullet and contain the full URL of the organization's social media profile for that site.

Identify the organization's mail-based DNS records

1. Enter `marketplaces install recon/domains-hosts/mx_spf_ip`
2. Enter `modules load recon/domains-hosts/mx_spf_ip`
3. Enter `info`
4. Enter `options set SOURCE comptia.org`
5. Enter `run`
6. Verify that Recon-ng discovered mail exchanger (MX) and Sender Policy Framework (SPF) records for the domain, as well as a public IP address range.

Search for subdomains

1. Enter `marketplaces install recon/domains-hosts/hackertarget`
2. Enter `modules load recon/domains-hosts/hackertarget`
3. Enter `info`
4. Enter `options set SOURCE comptia.org`
5. Enter `run`
6. As the scan runs, verify that some active subdomains were identified.
7. Wait for the scan to complete.

Crawl the domain for common files available for download

1. Enter `marketplaces install recon/domains-contacts/metacrawler`
2. If there are dependencies, install it first. For example, PyPDF3
    1. Open a new terminal
    2. Enter sudo apt install pip
    3. Enter sudo pip install PyPDF3
3. Enter `modules load recon/domains-contacts/metacrawler`
4. Enter `info`
5. Enter `options set SOURCE comptia.org`
6. Enter `run`
7. Scroll up to the top of the list and verify that Recon-ng essentially performed a Google search for common file types associated with the domain.
8. Right-click any of the links and select **Copy Link**.
9. In Firefox, paste the link in the address bar, then press **Enter**.
10. Examine the file and note anything of interest.
11. Close Firefox.

Generate a report of your findings

1. Enter `marketplaces install reporting/html`
2. Enter `modules load reporting/html`
3. Enter `info`
4. Verify that this module has several options, all of which are required.
5. Enter `options set CREATOR <your name>`
6. Enter `options set CUSTOMER <your name>`
7. Enter `options set FILENAME /home/rvillaver/Desktop/recon-report.html`
8. Enter `run` and verify that the report was generated

Open the report

1. From the Kali Linux desktop, double-click **recon-report.html** to open it in Firefox.
2. Verify that there are several categories in the report page, with the summary automatically expanded.
3. Expand the rest of the categories to see the relevant information.