4

GATHERING BUSINESS OSINT

Open Source Intelligence (OSINT) is any data you can find from publicly available, unhidden sources. The amount and significance of available public data can make or break your campaign. If you contact a target without any knowledge of their likes and dislikes, operating environment, organizational structure, or internal company lingo, you'll probably fail.

On the other hand, taking the time to understand what makes the target click will provide you with immediate context for the contact. Too often, people attempt to perform social engineering operations after either skipping or rushing the OSINT gathering, leaving them without a reason to talk to their target.

This chapter introduces three OSINT categories: business, people, and cyber threat intelligence. Then I'll go over some business OSINT tools for useful tasks like finding the names of company executives, discovering publicly available files, collecting email addresses, and reading document metadata.

Case Study: Why OSINT Matters

In 2017, I won DerbyCon's Social Engineering Capture the Flag (SECTF). This exercise pit me and five other competitors against an unknowing Fortune 500 business in the Louisville, KY area. We spent three weeks collecting OSINT, followed by 20 minutes in a (mostly) soundproof booth to vish the target company's employees. While researching my target company, I checked an executive's social media accounts and learned that he'd been late to a business meeting in Amsterdam because an airline had delayed his flight in Newark. This seemingly harmless piece of information gave me the perfect excuse for contacting him.

With this knowledge, I added that airline's phone number to my list of numbers to vish. I then acquired the executive's name, email address, and phone number, and added those to my list of targets. Had this been an engagement allowing phishing, I would have sent an apology email that mimicked the airline's template, and then followed up with a phone call, pretending to be the airline. Then I could have confirmed the information I already knew and asked "security questions" to convince the target that I was a trusted source. I might have even incorporated a few Windows operating system sounds to amplify my credibility. Finally, I would have asked him potentially lethal questions about the company's operating environment, such as the status of equipment upgrades, operating schedules, or other company-specific confidential data.

These attacks would be impossible if I had not first discovered the executive's post about his delayed flight. Rarely will an effective social engineering attack happen without an informed understanding of the target. Better OSINT makes better social engineering.

Understanding Types of OSINT

OSINT can be about an organization, a person, or a piece of code. In *business OSINT* gathering, we look for information about the company as a whole: technologies used, vendors, customers, operations, and locations.

For collecting *people OSINT*, we can go in two directions. We can target the person themselves, hunting for information such as their likes, dislikes, further connections, password-reset questions, and context for guessing passwords. Alternatively, we can leverage the person to learn about the business for which they work. This kind of OSINT could include pictures of the person at work, resumes, complaints or grievances, any bragging they've done about work, and travel they've done for work, to name a few.

NOTE *As a rule of thumb, I won't explicitly target a person's personal accounts as part of an engagement. I may gather information to use, but I won't try to contact them on a personal Facebook, Twitter, or LinkedIn account.*

OSINT can be used to enable *cyber threat intelligence (CTI)* which usually involves a piece of code or a specific adversary. We use it as a means to identify the perpetrator of an attack and their motives. For example, you might track down elements of code to determine its author or country. Or you might trace an email address or phone number that contacted your

organization. People debate the efficacy of OSINT for threat intelligence. Some organizations do it very well, while others try to make a quick buck at the expense of their customers.

Business OSINT

This section will get you started collecting business OSINT. What context can you use to build rapport when you communicate with a company's employees? I'll go over some OSINT collection tools here.

Getting Basic Business Information from Crunchbase

Various platforms can give you insight about a company. While most charge for in-depth information, some allow collection of a limited amount of information for free or without authentication. An example of such a site is *Crunchbase* (*https://www.crunchbase.com/*). Crunchbase has a free tier that meets most needs for casual OSINT enthusiasts. If you plan on using this heavily or as a professional consultant, I recommend paying for the Pro tier.

Searching Crunchbase for *Walmart* pulls up a profile with multiple tabs. Figure 4-1 shows the Summary tab, which allows you to get an address for corporate headquarters. Before having to scroll down, you can find out the number of mergers, acquisitions, and exits to which the company has been a party. You can see its stock ticker (if it's a publicly traded company), recent news about the company, and the beginning of foundational, sometimes historical, information about the company. Crunchbase gathers this information from a combination of input from analysts, web scraping, and self-reporting, which varies in accuracy.

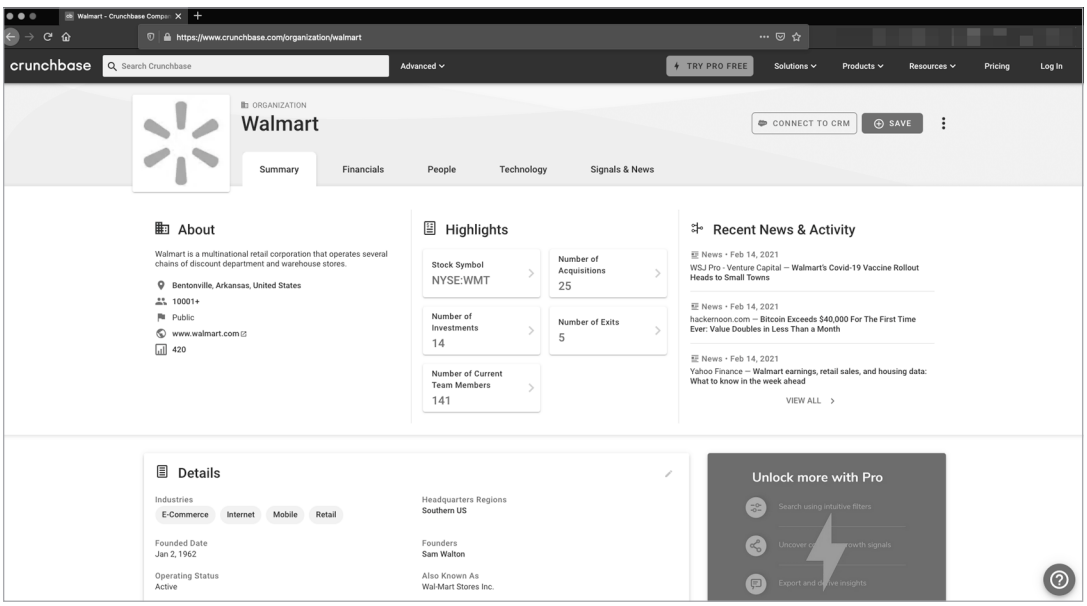

Figure 4-1: Crunchbase profile's Summary tab for Walmart

The Financials tab provides specific information about investments, exits, and fundraising (Figure 4-2).

If the company is publicly traded, you'll find the initial public offering (IPO) and stock price information. If you're researching a privately held company, you would see little to nothing in this section, or perhaps would learn about fundraising efforts, including amounts raised, investors, and dates. If the company has invested money or made donations, that will be listed next (Figure 4-3), followed by Exits and completed by Acquisitions (Figure 4-4).

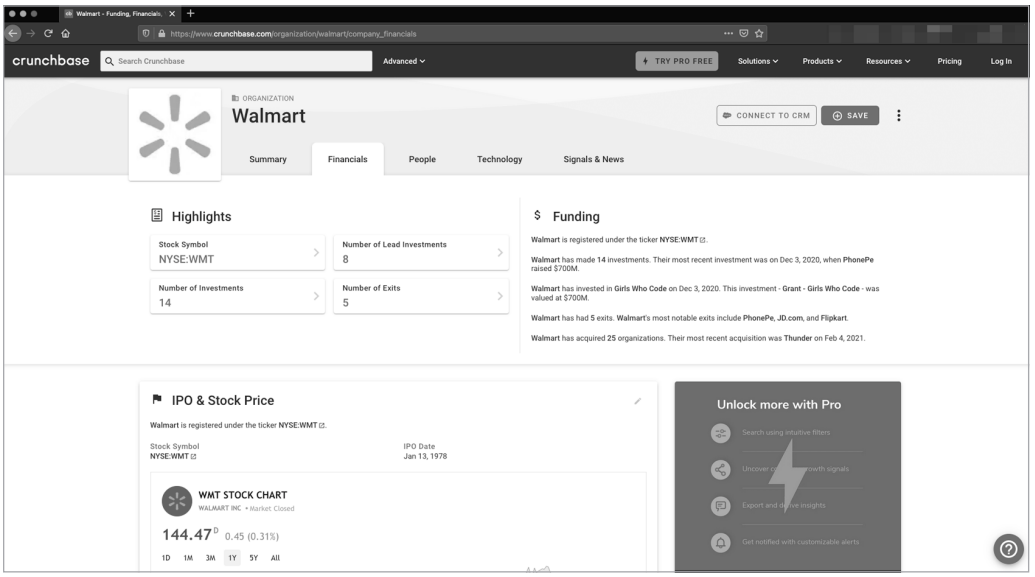

Figure 4-2: Walmart's stock information in the Crunchbase Financials tab

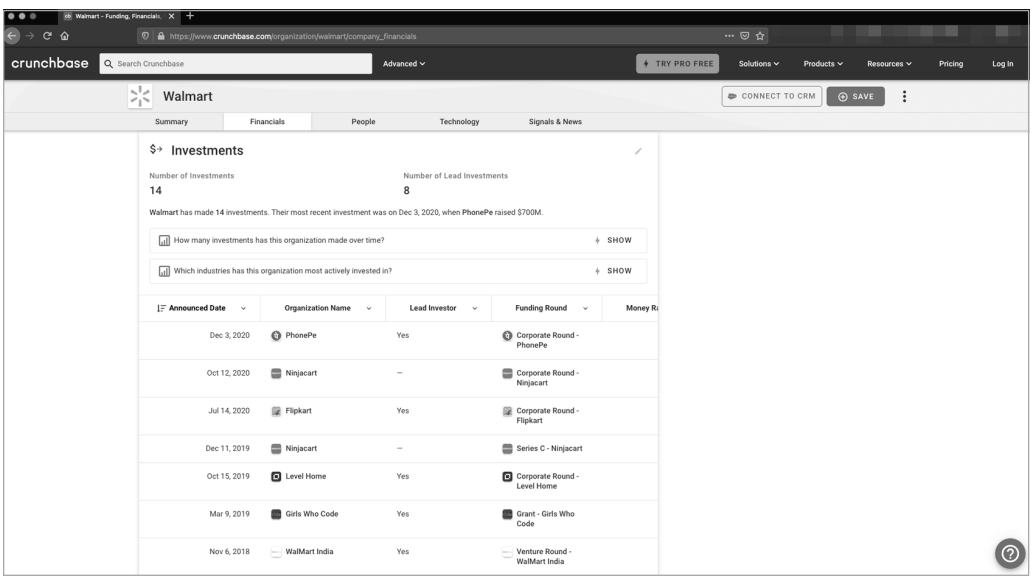

Figure 4-3: Walmart's investment information in the Crunchbase Financials tab

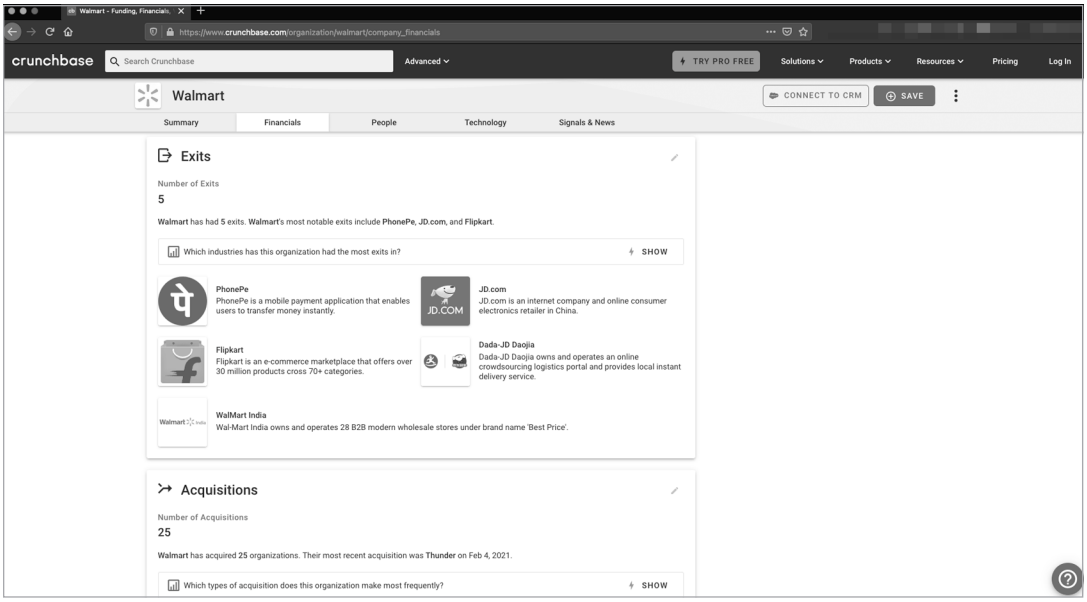

Figure 4-4: Walmart's acquisition information in the Crunchbase Financials tab

Next is the People tab, which includes important employees. These are typically executives overseeing certain key areas or people who have had an impact on the organization's history. For example, Figure 4-5 lists Sam Walton, the founder of Walmart, as a "Founder & Admin" under Current Team and a member of the Board of Directors despite having passed away in 1992.

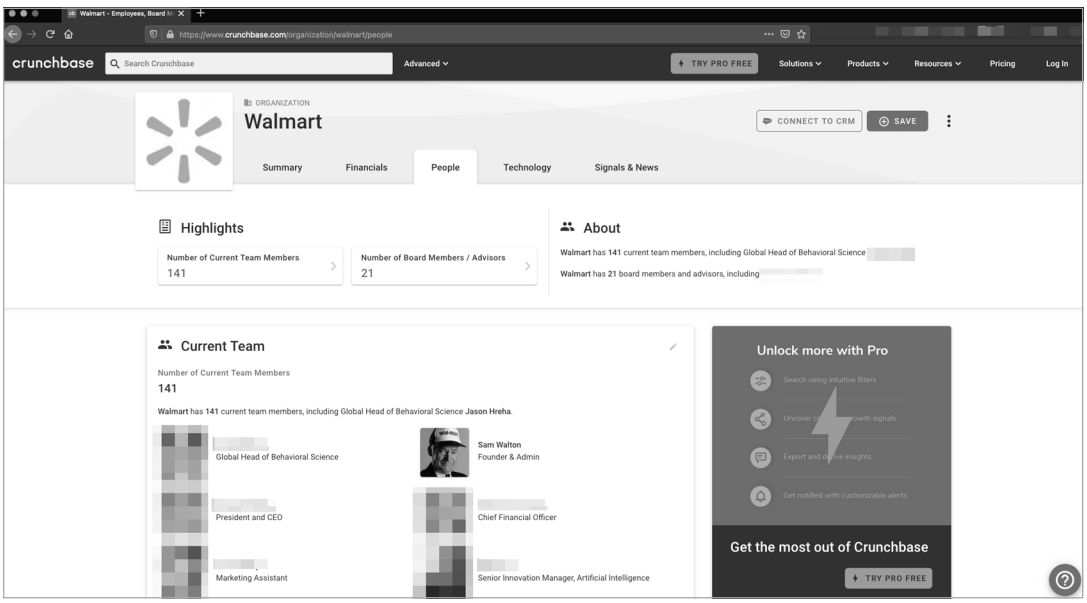

Figure 4-5: Crunchbase profile's People tab for Walmart

The Technology tab is mostly locked unless you have a Pro tier account. If you do have such an account, this tab will show you web traffic statistics, mobile app metrics, and limited information about the company's patents and other intellectual property filings. This information can be found elsewhere on the internet, so being locked out isn't a terribly big deal. Try looking at BuiltWith (*https://www.builtwith.com/*), Wappalyzer (*https://www.wappalyzer.com/*), or Shodan (*https://www.shodan.io/*).

The final tab, Signals & News, aggregates relevant news and leadership changes (Figure 4-6).

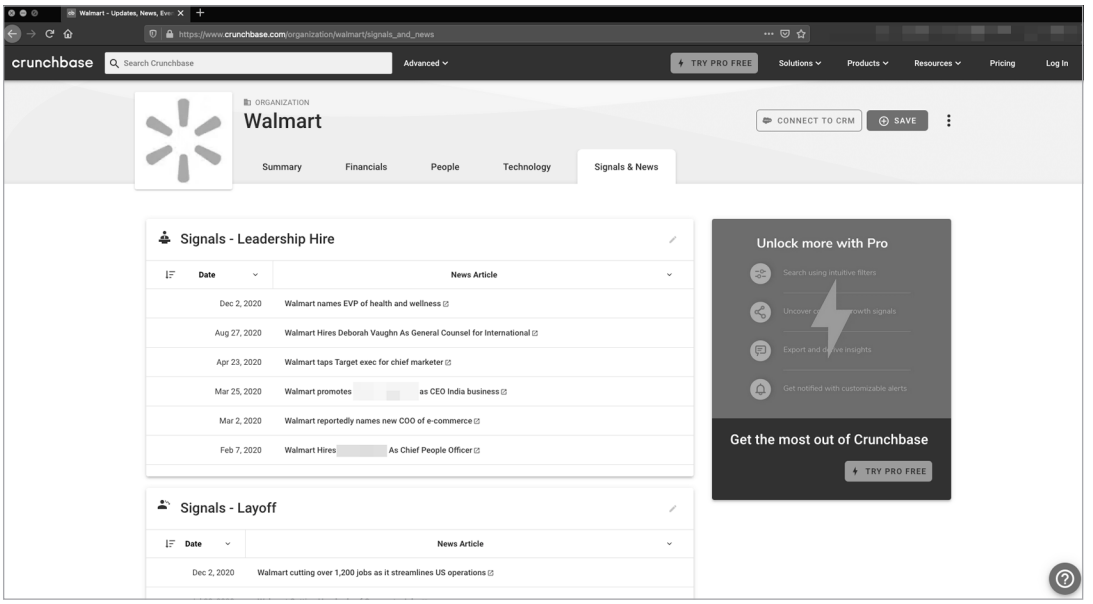

Figure 4-6: Crunchbase profile's Signals & News tab for Walmart

This tab also lists events that the organization has some affiliation with, either by sponsoring them or having employees speak at them. This is a good starting point, but not a replacement for other sources of information, including public filings, press releases, and reports by the media. (We'll discuss these sources in the next few chapters.) This tab may also suggest possible search terms you could enter on the search engine of your choice.

Identifying Website Owners with WHOIS

Pronounced "who is," *WHOIS* is a directory of websites, their owners, their network blocks, and their points of contact. Its purpose is to allow people with legitimate business inquiries to contact companies' web teams regarding the web presence. To read more about it, see RFC 9312.

You can search WHOIS via DomainTools, as shown in Figure 4-7. The `whois` command is built in on both the Offensive Security and Trace Labs Kali versions and can be added to any Linux system via `apt-get` or similar commands for other Linux distributions.

The top of the page shows domains that are similar to the target's domain and up for auction. These may come in handy for domain squatting and further phishing or baiting attempts. Spoofing is easy to detect, and most mail clients have protections against it, weakening your potential as a social engineer. Domain squatting or typo squatting are more likely to get emails through filters and into inboxes.

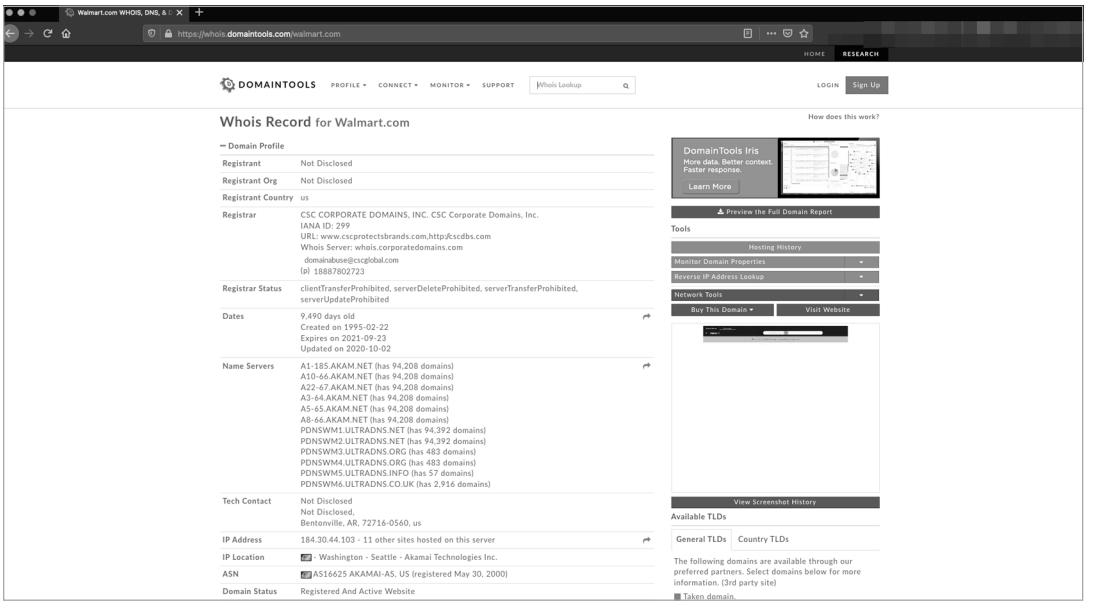

Figure 4-7: Walmart WHOIS record via DomainTools

Next, notice that *transfer* is prohibited, meaning you likely won't be able to transfer that domain to a different provider, an activity that red teams often attempt. Also notice the age of the domain. This helps confirm that you're looking at the right target. Alternatively, this same feature can reveal that the domains you use are fake. That's why it's a good idea to purchase domains and wait six months to a year before using them.

Next are the domain name servers that the site uses. These can sometimes indicate other software employed by the company. For example, Walmart uses Akamai and UltraDNS. Akamai also provides content distribution network (CDN) services (to allow faster page loading and mitigate DOS attacks) and performs web protection and load balancing (further DOS mitigation). This is important to know if you're preparing for a penetration test.

Be aware that, as of May 25, 2018, the EU General Data Protection Regulation (GDPR) has changed the way that WHOIS is handled in its jurisdiction. This prompted the Internet Corporation for Assigned Names and Numbers (ICANN), the governing body for WHOIS, to change the information presented for companies and contacts located in the EU.

Collecting OSINT from the Command Line with Recon-ng

Recon-ng is a command line tool for Linux, written by Tim Tomes, for collecting OSINT. It operates a lot like Metasploit: you can input information, set targets, and then use the `run` command to perform a search.

A plethora of tools are built into Recon-ng for collecting both business and people OSINT, ranging from breached emails from Have I Been Pwned (discussed in Chapter 6) and netblocks from DNS records to hosts or ports from Shodan (discussed in Chapter 5). You can find most things that you seek to learn about a company by using Recon-ng.

Installing Recon-ng

Recon-ng comes preinstalled on both the Offensive Security and Trace Labs Kali versions. To use Recon-ng on a different Linux system, you'll need Python 3, the pip3 package management tool, and Git. Then you can install it in the */opt* directory with the following commands:

```
root@se-book:/opt# git clone https://github.com/lanmaster53/recon-ng
Cloning into 'recon-ng'...
---snip--
Resolving deltas: 100% (4824/4824), done.
root@se-book:/opt# cd recon-ng/
root@se-book:/opt/recon-ng# ls -la
--snip--
-rw-r--r-- 1 root root    97 Sep 25 18:37 REQUIREMENTS
--snip--
-rwxr-xr-x 1 root root  2498 Sep 25 18:37 recon-ng
-rwxr-xr-x 1 root root    97 Sep 25 18:37 recon-web
root@se-book:/opt/recon-ng# python3 -m pip install -r REQUIREMENTS
Requirement already satisfied: pyyaml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS
(line 2))
Collecting dnspython (from -r REQUIREMENTS (line 3))
  Downloading https://files.pythonhosted.org/packages/ec/d3/3aa0e7213ef72b8585747aa0e271a9523e7
13813b9a20177ebe1e939deb0/dnspython-1.16.0-py2.py3-none-any.whl (188kB)
    100% |████████████████████████████████| 194kB 5.6MB/s
```

Setting Up a Workspace

Recon-ng lets you define separate workspaces, which are great for keeping your collected information segmented. You can define the workspace as you open Recon-ng and store the data collected in its own unique SQLite database. If I am searching for various entities or companies as part of the same investigation, I will give them their own workspace so to not confuse myself as I review the information collected. If you don't define a workspace, Recon-ng will write all results to the default workspace and associated database.

To use a workspace when starting Recon-ng, run the following:

```
recon-ng -w workspace name
```

For example, if I were investigating Walmart, I might run this:

```
recon-ng -w walmart
```

The resulting workspace would look like this:

```
[recon-ng][walmart]
```

If you're already in Recon-ng, you can view available workspaces by issuing the `workspace list` command.

NOTE *You cannot do this while a module is loaded, so in that situation, you'll need to issue the back command.*

If you want to load an existing workspace, you can issue this command:

```
workspace load workspace name
```

You can also create a workspace by using the following:

```
workspace create workspace name
```

After you no longer need any of the information within a workspace and your retention requirements have passed, you can remove it:

```
workspace remove workspace name
```

Installing Recon-ng Modules

Next, you have to enable and install modules. Let's see which modules are available by using `marketplace search`:

```
[recon-ng][walmart] > marketplace search
+-------------------------------------------------------------------------------------------+
|.            Path                          | Version |     Status    |  Updated   | D | K |
+-------------------------------------------------------------------------------------------+
| discovery/info_disclosure/cache_snoop     | 1.0     | not installed | 2019-06-24 |   |   |
| discovery/info_disclosure/interesting_files |     1.0 | not installed | 2019-06-24 |   |   |
| exploitation/injection/command_injector.  | 1.0     | not installed | 2019-06-24 |   |   |
| exploitation/injection/xpath_bruter       | 1.1     | not installed | 2019-08-19 |   |   |
| import/csv_file                           | 1.1     | not installed | 2019-08-09 |   |   |
| import/list                               | 1.0     | not installed | 2019-06-24 |   |   |
```

You can install modules in two ways: one by one or all at once. To install a single module, enter the following command, replacing *import/csv_file* with the complete path of the module:

```
[recon-ng][walmart] > marketplace install import/csv_file
[*] Module installed: import/csv_file
[*] Reloading modules...
```

To install all available modules, use the following command:

```
[recon-ng][walmart] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
--snip--
[*] Module installed: reporting/xml
[*] Reloading modules...
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys
add'.
[!] 'censysio_id' key not set. censysio module will likely fail at runtime. See 'keys add'.
```

NOTE *Ignore the warnings about missing API keys. We'll import API keys for only the modules we need.*

Acquiring and Adding API Keys

In order for some of the tools to access outside resources, you'll need to add API keys from various websites. Each website has its own process for getting these keys, and those procedures tend to change frequently. You can find my up-to-date tutorial for obtaining these API keys at *https://www.theosintion.com/practical-social-engineering/* or check the pages for API keys on the websites for each tool.

Once you have the keys, use the following syntax in Recon-ng to add them:

```
keys add name of module value
```

Verify that Recon-ng has the key in the database with the following command:

```
keys list
```

Finding and Running Recon-ng Modules

There are five kinds of Recon-ng modules: discovery, exploitation, import, recon, and reporting. In this book, we'll use the discovery, recon, and reporting module types.

To see the modules relative to a specific type, use the `search` command, followed by the type's name:

```
modules search discovery
```

If you know part of the module's name, you can use the `search` function to locate it, like this:

```
modules search hibp
```

You can also invoke a module directly with the `modules load` command if you know either the module's name or the beginning of the module's name:

```
modules load metacr
```

The preceding command will load the `metacrawler` module. Now let's explore some of these modules in more detail.

To set a target for a module, you'll need to know what inputs the module accepts. Find this out by issuing the `info` command. Once you're ready to enter a target or value in one of the accepted fields, issue the `options set` *`NAME OF FIELD VALUE OF FIELD`* command.

Enumerating Files with Metacrawler

The `metacrawler` module searches a target site or sites for Microsoft PowerPoint, Word, Excel, and PDF files. It's the equivalent of doing a *Google dork*—writing long search queries, like this:

```
site:nostarch.com Filetype:XLS* OR Filetype:DOC* OR Filetype:PPT* or Filetype:PDF
```

For example, to search *nostarch.com* for all file types, use the following commands:

```
[recon-ng][default][metacrawler] > options set SOURCE nostarch.com
SOURCE => nostarch.com
[recon-ng][default][metacrawler] > run
------------
NOSTARCH.COM
------------
[*] Searching Google for: site:nostarch.com filetype:pdf OR filetype:docx OR
filetype:xlsx OR filetype:pptx OR filetype:doc OR filetype:xls OR
filetype:ppt
[*] https://www.nostarch.com/download/WGC_Chapter_3.pdf
[*] Producer: Acrobat Distiller 6.0 (Windows)
[*] Title: Write Great Code
[*] Author: (c) 2004 Randall Hyde
[*] Creator: PScript5.dll Version 5.2
[*] Moddate: D:20041006112107-07'00'
[*] Creationdate: D:20041006111512-07'00'
[*] https://www.nostarch.com/download/wcss_38.pdf
[*] Producer: Acrobat Distiller 5.0 (Windows)
[*] Title: wcss_book03.book
[*] Author: Riley
[*] Creator: PScript5.dll Version 5.2
[*] Moddate: D:20040206172946-08'00'
[*] Creationdate: D:20040116180100Z
```

If `Extract` is set to `True`, this command outputs all documents on the target's public website that are in PDF or Microsoft Office formats (Excel, Word, or PowerPoint) with a link to the file and metadata, including the

author, the software that created it, the modification date, the software that produced it, and the date on which it was created. If `Extract` is set to `False`, the output provides the filename and link only.

Given this information, you can do numerous things. From the metadata, you can enumerate users, operating systems, and software used. From the files themselves, you might be able to find information the target intended to keep private, including names, email addresses, phone and fax numbers, locations, and important business matters.

Finding Domain Points of Contact with whois_pocs

The `whois_pocs` module enumerates all known points of contact for a given domain. It's more robust for this feature than the `whois_miner` module and works even against targets with domain privacy. Here is an example of running this module against Walmart:

```
[recon-ng][default][whois_pocs] > modules load whois_pocs
[recon-ng][default][whois_pocs] > options set SOURCE walmart.com
SOURCE => nostarch.com
[recon-ng][default][whois_pocs] > info
      Name: Whois POC Harvester
      Path: modules/recon/domains-contacts/whois_pocs.py
    Author: Tim Tomes (@LaNMaSteR53)
Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given
domain. Updates the 'contacts' table with the results.
Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  walmart.com    yes       source of input (see 'show 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][whois_pocs] > run
-----------
WALMART.COM
-----------
[*] URL: http://whois.arin.net/rest/pocs;domain=walmart.com
[*] URL: http://whois.arin.net/rest/poc/ABUSE327-ARIN
[*] Country: United States
[*] Email: abuse@walmart.com
[*] First_Name: None
[*] Last_Name: Abuse
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Brisbane, CA
[*] Title: Whois contact
[*] ------------------------------------------------
```

Keep in mind that some organizations don't publish their WHOIS information.

Using mx_spf_ip to Learn About a Domain's Email Policies

The `mx_sfp_ip` module retrieves the DNS mail exchanger (MX) record for a domain. The *MX record* defines how the domain processes email. It shows the mail servers used and any *Sender Policy Framework (SPF) records* that restrict IP ranges from which the domain can receive mail, as well as domains that can email the organization without scrutiny.

Using the MX record, an attacker can leverage the information it contains to craft a successful email spoofing attack. For example, the attacker can enumerate the IP ranges listed in the record and their associated domains. This may provide clues into business relationships, vendors, or technologies used.

The following command retrieves the MX record for *nostarch.com*. The output confirms that the site uses Google mail servers, but the lack of an SPF record indicates that No Starch hasn't implemented SPF:

```
[recon-ng][book][mx_spf_ip] > options set SOURCE nostarch.com
SOURCE => nostarch.com
[recon-ng][book][mx_spf_ip] > run
[*] Retrieving MX records for nostarch.com.
[*] [host] alt1.aspmx.l.google.com (<blank>)
[*] [host] aspmx.l.google.com (<blank>)
[*] [host] alt3.aspmx.l.google.com (<blank>)
[*] [host] alt2.aspmx.l.google.com (<blank>)
[*] [host] alt4.aspmx.l.google.com (<blank>)
[*] Retrieving SPF records for nostarch.com.
[*] nostarch.com => No record found.
```

On the other hand, the following output shows us that Walmart uses SPF:

```
[recon-ng][book][mx_spf_ip] > options set SOURCE walmart.com
SOURCE => walmart.com
[recon-ng][book][mx_spf_ip] > run
[*] Retrieving MX records for walmart.com.
[*] ❶[host] mxb-000c7201.gslb.pphosted.com (<blank>)
[*] [host] mxa-000c7201.gslb.pphosted.com (<blank>)
[*] Retrieving SPF records for walmart.com.
[*] TXT record: "dtOeNuIs42WbSVe3Zf2qizxLw9LSQpFd6bWqCr166oTRIuJ9yKS+etPsGGNOvaiasQk2C6GVO/5Pj
T9CI2nNAg=="
[*] TXT record: "google-site-verification=ZZYRwyiI6QKgOjVwmdIha68vuiZlNtfAJ9OmsPo1i7E"
[*] TXT record: "adobe-idp-site-verification=7f3fb527466337ac0ac0752c569ca2ac48926dc6c6dad3636d
581aa131a1cf3e"
[*] TXT record: "v=spf1 ip4:161.170.248.0/24 ip4:161.170.244.0/24 ip4:161.170.236.31
ip4:161.170.238.31 ip4:161.170.241.16/30 ip4:161.170.245.0/24 ip4:161.170.249.0/24
include:Walmart.com include:_netblocks.walmart.com include:_vspf1.walmart.com include:_vspf2.
walmart.co" "m include:_vspf3.walmart.com ~all"
[*] ❷[netblock] 161.170.248.0/24
[*] [netblock] 161.170.244.0/24
[*] [host] <blank> (161.170.236.31)
[*] [host] <blank> (161.170.238.31)
```

```
[*] [netblock] 161.170.241.16/30
[*] [netblock] 161.170.245.0/24
[*][netblock] 161.170.249.0/24
[*] ❸TXT record: "facebook-domain-verification=ximom3azpca8zph4n8lu200sos1nrk"
[*] ❹TXT record: "adobe-idp-site-verification=5800a1970527e7cc2f5394a2bfe99bcda4e5938e132c0a19
139fda9bf6e30704"
[*] ❺TXT record: "docusign=5bdc0eb1-5fb2-471c-99a0-d0d9cc5fdac8"
[*] ❻TXT record: "MS=E4F53D5B1A485B7BA06E0D36A9D38654A16609F3"
```

The SPF record lists domain verifications for Adobe, Facebook, DocuSign, Microsoft, and Google. The text (TXT) record that begins with `MS=` indicates that Walmart uses Microsoft Office 365 ❻. It also uses `adobe-idp-site-verification` to validate domains for Adobe Enterprise products like Creative Cloud ❹. The `facebook-domain-verification` TXT record restricts the domains that edit the official Facebook page for the domain ❸. The TXT record that begins with `docusign=` indicates that the site uses DocuSign to sign official documents ❺.

Notice *pphosted.com* ❶ listed as a host. This indicates the use of Proofpoint, an anti-spoofing technology that adds a custom message, often the string `[EXTERNAL]`, to the subject line of received emails, making phishes or attempts at business email compromise easier to spot.

Some network ranges are also listed ❷. These are the target's public IP addresses, and the two hosts listed are the main mail servers. You can confirm this by using other tools.

Using Other Tools: theHarvester and OSINT Framework

Like Recon-ng, *theHarvester* is a Linux-based command line OSINT tool freely available as part of Kali and Buscador. You can also find it on GitHub. Written by Christian Martorella, theHarvester requires API keys for Shodan and Google Custom Search Engine (CSE). You can enter these keys in the following files:

```
theHarvester path/discovery/googleCSE.py
```

and

```
theHarvester path/discovery/shodansearch.py
```

On theHarvester, you can use switches to direct the tool to perform tasks. The decision to use theHarvester instead of Recon-ng is a matter of preference. Even if you use Recon-ng as your primary tool, you may want to get a second opinion using theHarvester to see if Recon-ng missed any additional information.

OSINT Framework (*https://osintframework.com*) is a GUI-based collection of tools. Curated by Justin Nordine, OSINT Framework groups resources based on what you're looking for (Figure 4-8).

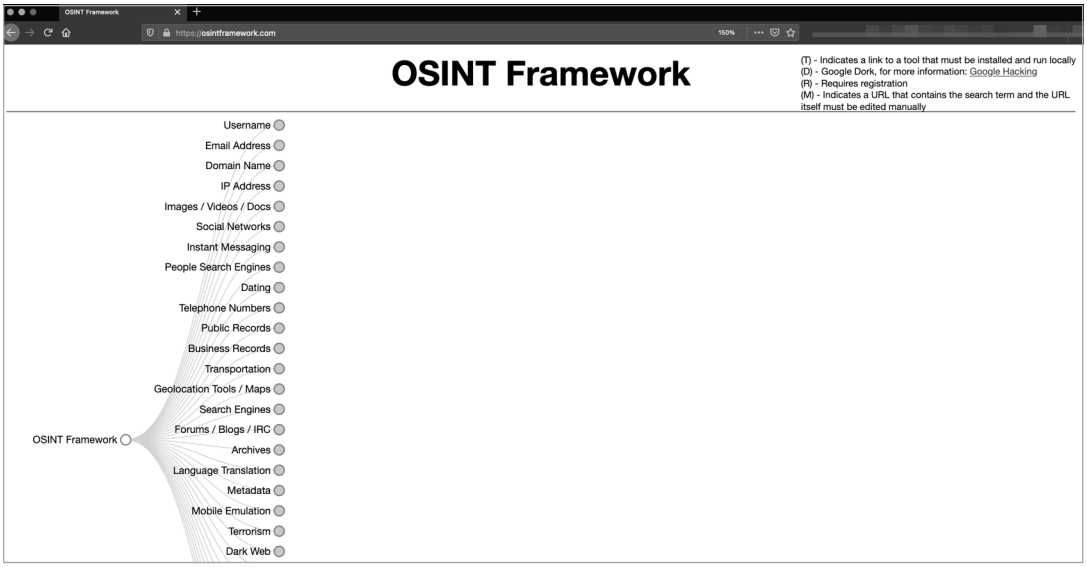

Figure 4-8: OSINT Framework

Finding Email Addresses with Hunter

You'll often need to find email addresses and a company's *email address syntax* (the format the company uses for its employees' email addresses). *Hunter* is an excellent tool to help enumerate these. Without logging in, you can get the basic email address syntax used at the company. Once you create an account and log in, you can get the most common email address syntaxes, full company email addresses, and occasionally, a person's title.

Figure 4-9 shows the output of an unauthenticated search.

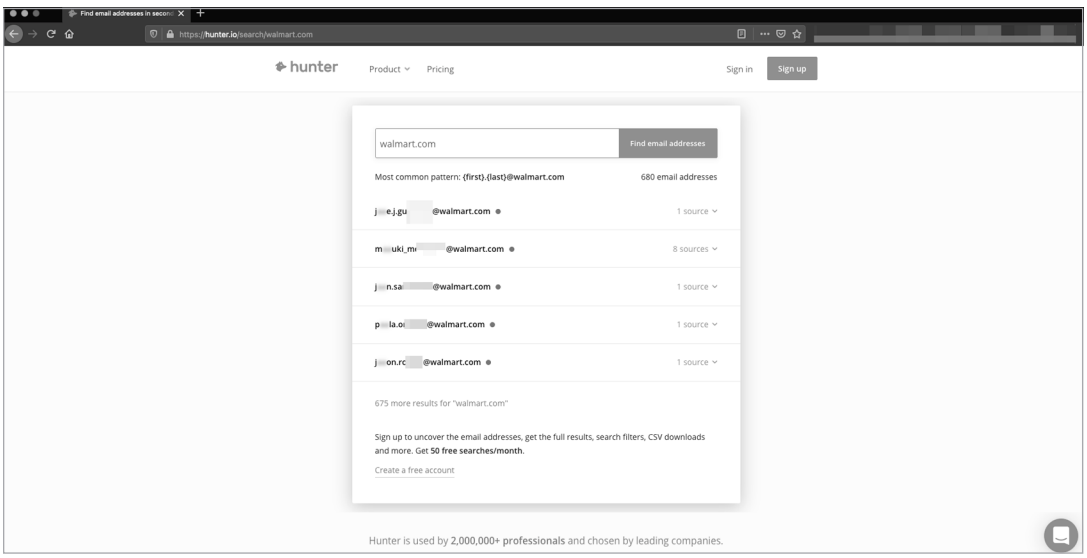

Figure 4-9: Hunter search results for an unauthenticated user (Note: Hunter censored these results.)

Figure 4-10 shows an authenticated search that returns valid email addresses for our target domain, as well as where they were found.

Figure 4-10: Hunter results for an authenticated user. (Note: The author censored these results.)

By looking at these results, you can deduce the syntax of the company's email addresses. You can then pivot to LinkedIn and the corporate website to get more names, and then put more email addresses together yourself should you want to phish those people.

Hunter provides varying levels of service; at the time of this writing, these range from free (100 requests per month and no CSV export) all the way to $399 per month, which includes 50,000 requests and allows CSV exports.

Exploiting Mapping and Geolocation Tools

You've probably used Google Maps or Bing Maps to orient yourself using map views, satellite views, and views taken from the street. When it comes to collecting OSINT, the satellite and street view modes are usually the most valuable.

The satellite view can show gates, dumpsters, satellite dishes, entrances and exits, parking schemas, and adjacent facilities. You can zoom in fairly close to some sites to help you determine hiding places, entrances, and smoking areas.

The street view allows you to see the building and facilities as you would if you walked or drove up. From this view, you can identify the following:

- Dumpster vendor (useful information for onsite pretexting that could help you gain access to the building or dumpster dive)

- Gates, doors, and fences, and whether they're routinely left open (and, sometimes, the presence of security guards)
- Delivery companies whose trucks are parked outside
- The specific names of buildings, such as the Walmart Innovation Center, Walmart People Center, or Walmart Home Office, which can help you blend into the organization better (a quick way to be outed is to call Disney or Walmart employees *employees* instead of *cast members* or *associates*, respectively);
- Other tenants

During the DerbyCon SECTF I mentioned at the beginning of this chapter, I used Google Maps to determine the shipping vendors for my target company by checking whose trucks were within the confines of the gates. I could have used this information to gain physical access, maybe by finding a uniform at a thrift shop, or as a vishing pretext to call about a shipment.

Using both Google Maps and Bing Maps can give you better information, as the source of the apps' data is different. Furthermore, the images are collected on different days, so you might, for example, find a delivery truck in one app but not in another, a new dumpster in a more recent photo, or poorly censored vendor names.

Conclusion

You can take many avenues for collecting OSINT. This chapter only scratches the surface of these tools' capabilities, and it's meant as a starting point that will help you apply OSINT techniques to social engineering, penetration testing, or any other ethical application. Through the exercises in this chapter, you've collected domains, IP addresses, email addresses, names, and technologies associated with businesses using open source tools.

The next chapter covers strategies for collecting OSINT without fancy tools. Chapter 6 covers OSINT operations against people.