Information Gathering

Iker M. Canut

July 10, 2020

1 TOOL: hunter.io

Hunter is a Domain Search. It gives a list of people that works in the organization: You get the first and last name and the most common pattern as far as email addresses are concerned. You can export all this information in a .csv. Maybe it tells you the department: Human Resources, IT/Engineering, Management, Executive, Legal, Sales, Support,...

This service may not list all the workers, but if you know that the email pattern is, for example, **{f}{last}@tesla.com**, and you know because of Linkedin, that "*Iker Canut*" works there, you can probably assume his email is *icanut@tesla.com.* This is crucial when we perform attacks (e.g password spraying in a login form).

2 TOOL: Breach Parse

In hmaverickadams' Github, we can find a breach-parse. It's quite heavy, but it has emails and password from breaches: credentials got dumped out and you can use them. The bash script is for searching more easily. To illustrate this, you can write: **./breach-parse.sh @tesla.com tesla.txt**. Then, the results are extracted to three files: A master, passwords and users. You can take advantage if people utilize their work credentials and they log into websites.

3 TOOL: theHarvester

You can use it to get emails and domains. It's fast, but it's not as powerful as other tools. Options in **theHarvester –help**.

4 Hunting subdomains

For example, if you need to analyze ***.tesla.com**, you can search for subdomains like *dev.tesla.com* or something that should have never been there, like logs. You shouldn't be limiting yourself to one website where there could be potenially tons of websites.

5 TOOL: sublist3r

To install it: **apt install sublist3r**. Options as usual in **sublist3r –help**. This is going to list a bunch of Unique Subdomains, because it uses Baidu, Yahoo, Google, Bing, Ask, Netcraft, DNSdumpster, Virustotal, ThreatCrowd, SSL Certificates, PassiveDNS, ... It will even find 4th level subdomains.

6 TOOL: crt.sh

You can use this for certificate fingerprinting: You look for certificates that have been registered; You can find a lot of information. For example, APIs, VPN, dev, SSO, QA, mail, ... The wildcard is %.

7 TOOL: owasp amass

This is THE go to tool for a lot of people. You can go to the Github and download it. You can configure it to do a lot of things and find a lot more subdomains.

- amass intel – Discover targets for enumerations
- amass enum – Perform enumerations and network mapping
- amass viz – Visualize enumeration results
- amass track – Track differences between enumerations
- amass db – Manipulate the Amass graph database

8 Narrowing the lists

You can use for example the thomnomnom's tool named httprobe to check a list of domains, to see which ones are alive.

9 TOOL: builtwith

You can go to builtwith.com and search a domain: You'll get information about:

- Analytics and Tracking
- **Widgets**
- Languages
- **Frameworks**
- Mobile
- **Content Delivery Network**
- **Payment**
- Audio / Video Media
- Content Management System
- JavaScript Libraries and Functions
- Advertising
- Email Hosting Providers
- Web Hosting Providers
- SSL Certificates
- Name Server
- Web Servers
- Verified CDN
- Web Master Registration
- Content Delivery Network

10 TOOL: wappalyzer

You can add this extension to your browser, and you get a little button that shows a little bit of information. It gives you an indication right away with what's going on. This is more of an active type of reconnaissance because we need to interact with the website: We're not doing any type of scanning, but we're just going after the website like a normal user would, so it's still passive.

This is important because if we know that's running PHP or Drupal, there may be a vulnerability within those. If we get the versions, that's a plus! The more information that we can gather on a client, the better.

11 TOOL: whatweb

You can use this tool to gather information. It's not as pretty as the other options, but it's built in in Kali. You can also get the version number.

12 TOOL: burpsuite

This is called a ”Web proxy”. This means that it has the capability of intercepting traffic for us. First, we need to set up our browser, so we open up firefox ¿ Preferences ¿ Network settings ¿ Manual proxy configuration:

- HTTP Proxy: 127.0.0.1:8080.
- And DO use this proxy server for all protocols.

Then, you should go to **https://burp** and accept this certificate exception. After that, click on **CA Certificate** and save the file.

Then, again in the browser's preferences, but under Privacy & Security ¿ View Certificates ¿ Import. Then you import the file you just downloaded and double check the boxes.

Now, if we go to *tesla.com*, it's gonna stall out.. But if we go to the burp app, we see that the Proxy tab is lit up. If you go there, you can see that is gathering some information. You can forward packages and also you can modify them.

If you go to the target tab, you can see all the libraries, themes. And also you can analyze packages, you can find CMSs with its version for example. While intercepting traffic you can get a lot of information in the headers.

13 How to Google

OR	This will return results related to X or Y, or both.	jobs OR gates
AND	This will return only results related to both X and Y.	jobs AND gates
-	Exclude a term or phrase.	jobs -apple
*	Acts as a wildcard and will match any word or phrase.	steve * apple
( )	Group multiple terms or search operators to control how the search is executed.	(ipad OR iphone) apple
$	Search for prices.	ipad $329
define:	The dictionary built into Google.	define:entrepreneur
cache:	Returns the most recent cached version of a web page.	cache:apple.com
filetype:	Restrict results to those of a certain filetype: PDF, DOCX, TXT, PPT.	apple filetype:pdf
site:	Limit results to those from a specific website.	site:apple.com
related:	Find sites related to a given domain.	related:apple.com
[all]intitle:	Find pages with certain words in the title.	intitle:apple
[all]inurl:	Find pages with certain words in the URL.	inurl:apple
[all]intext:	Find pages containing certain words in the content.	intext:apple
AROUND(X)	Find pages containing two words or phrases within X words of each other.	apple AROUND(4) iphone
in	Convert one unit to another	$329 in GBP
#..#	Search for a range of numbers.	wwdc video 2010..2014
+	Force an exact-match search on a single word or phrase. You can do the same thing by using double quotes	jobs +apple jobs ”apple”

Others quite intuitive are: **weather:**, **stocks:**, **map:**, **movie:**, **location:**

For example, you could google something like: **site:tesla.com filetype:csv**. You could potentially find sensitive files out there, maybe credentials, backup files...