Information Gathering (Reconnaissance)

Passive Recon

Physical

- Satellite images
- Drone Recon
- Building Layout(badge readers, break areas, security, fencing)

Social

- Employees (Names, Job Title, Phine Number, Manager, etc.)
- Pictures Badge photos, desk photos, computer photos, etc.

Web / Host

- **Target Validation** - WHOIS, nslookup, dnsrecon
- **Finding Subdomains** - Google Fu, dig, Nmap, Sublist3r, Bluto, crt.sh, etc.
- **Fingerprinting** - Nmap, Wappalyzer, WhatWeb, BuiltWith, Netcat
- **Data Breaches** - HaveIBeenPwned, Breach-Parse, WeLeakInfo

Identifying our target

Finding a client to "attack". Find a client using BugCrowd. He goes over Tesla in his video, I will be going over Humble Bundle. No matter the target, be sure to stay in scope on any type of engagement.

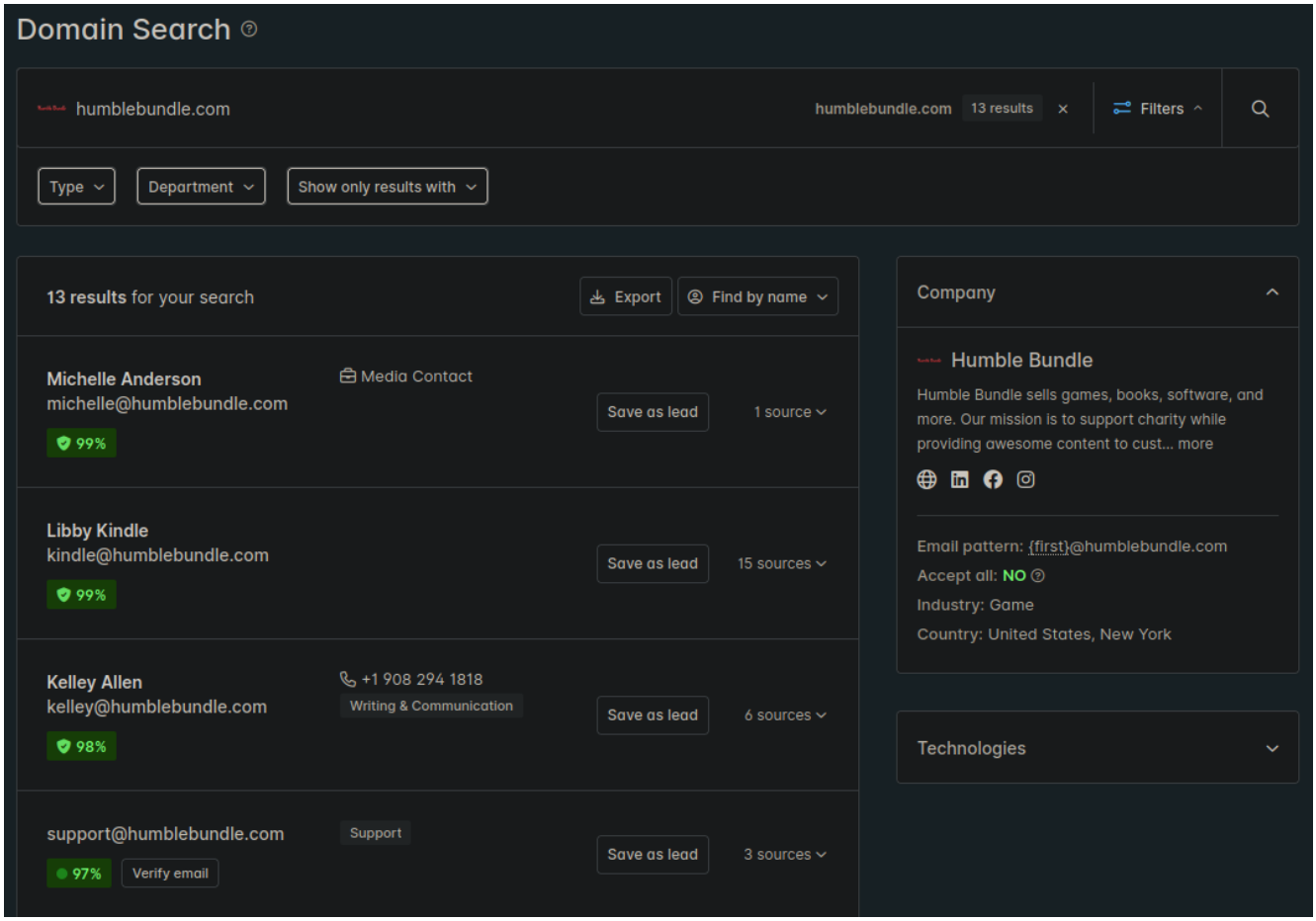
Discovering Email Addresses

Helpful Tools

I have my on list of various helpful tools on email OSINT here. Most of these tools were already added there.

Finding emails/username is very helpful for later on in the engagement as you can gather them for credential stuffing and other various types of attacks.

- Hunter.io - Discover email addresses by company name. This requires you to sign up with an email or Gmail)



We see various people with their job title and the source of where they found the email address. They have plugins/add-ons.

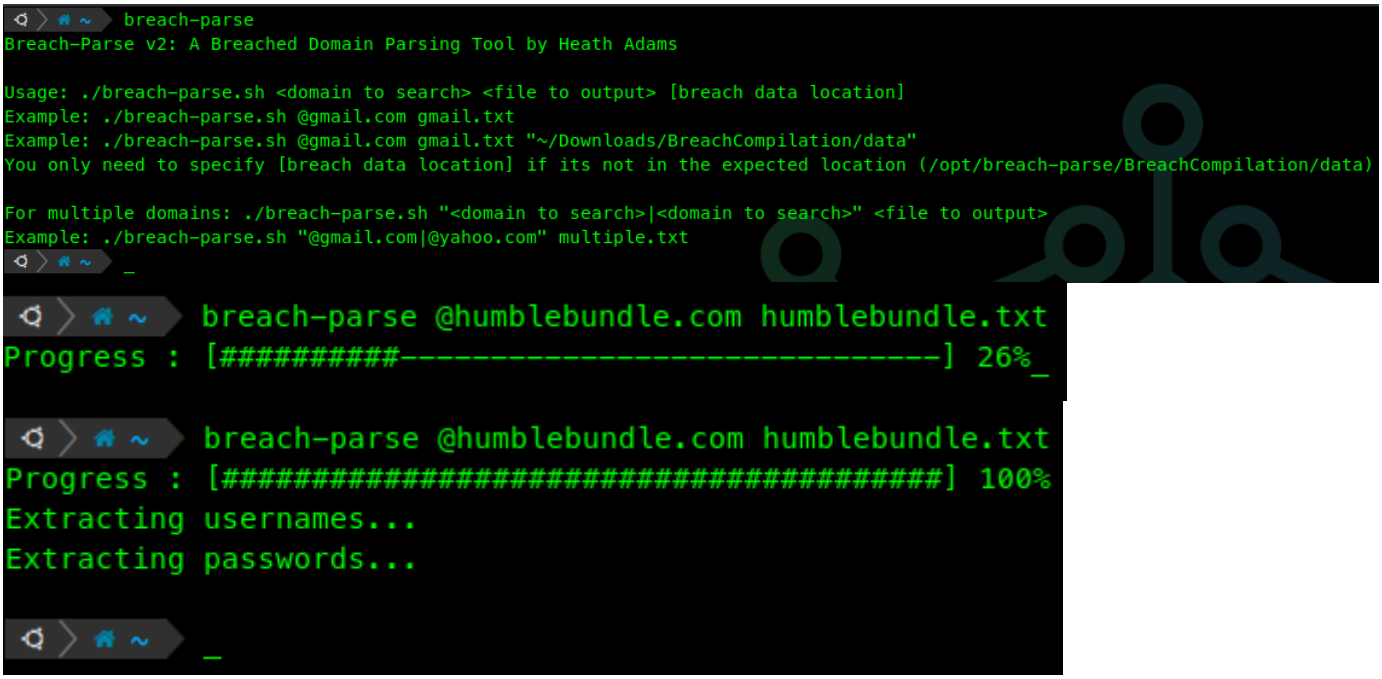
- Phonebook.cz - Lists all domains, email addresses, or URLs for the given input domain. This requires you to login with a intelx.io account.

- Clearbit.Connect - Email discovery tool, only works in chrome.

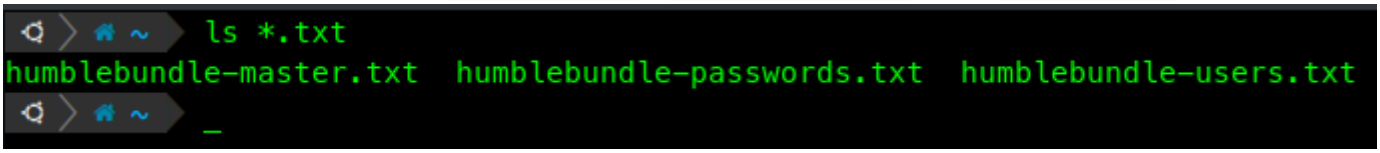
Gathering Breached Credentials with Breach-Parse

Breach-Parse is a tool created by Heath and is a tool for parsing breached usernames and passwords that have been dumped online. This pulls from a file under `/opt/breach-parse/BreachCompilation/data` under the `symbols file`. He does provide a password list located here. This is a magnet link so you will need some form of torrent software to download this. It is a larger

download(roughly 41GB).



Once done it is broken in 3 files: `*-master.txt`, `*-passwords.txt`, and `*-users.txt`.



The master.txt file will show user:password. Unfortunately this pulled no information for me from HumbleBundle, but this is what teslas looks like from Heaths video:

This is very helpful for credential stuffing by using the found users and passwords, but also by changing the passwords with upper/lower case strings, and appending numbers or symbols to the end.
We can also do a password spray by talking all the users and trying the same password against all the different users.

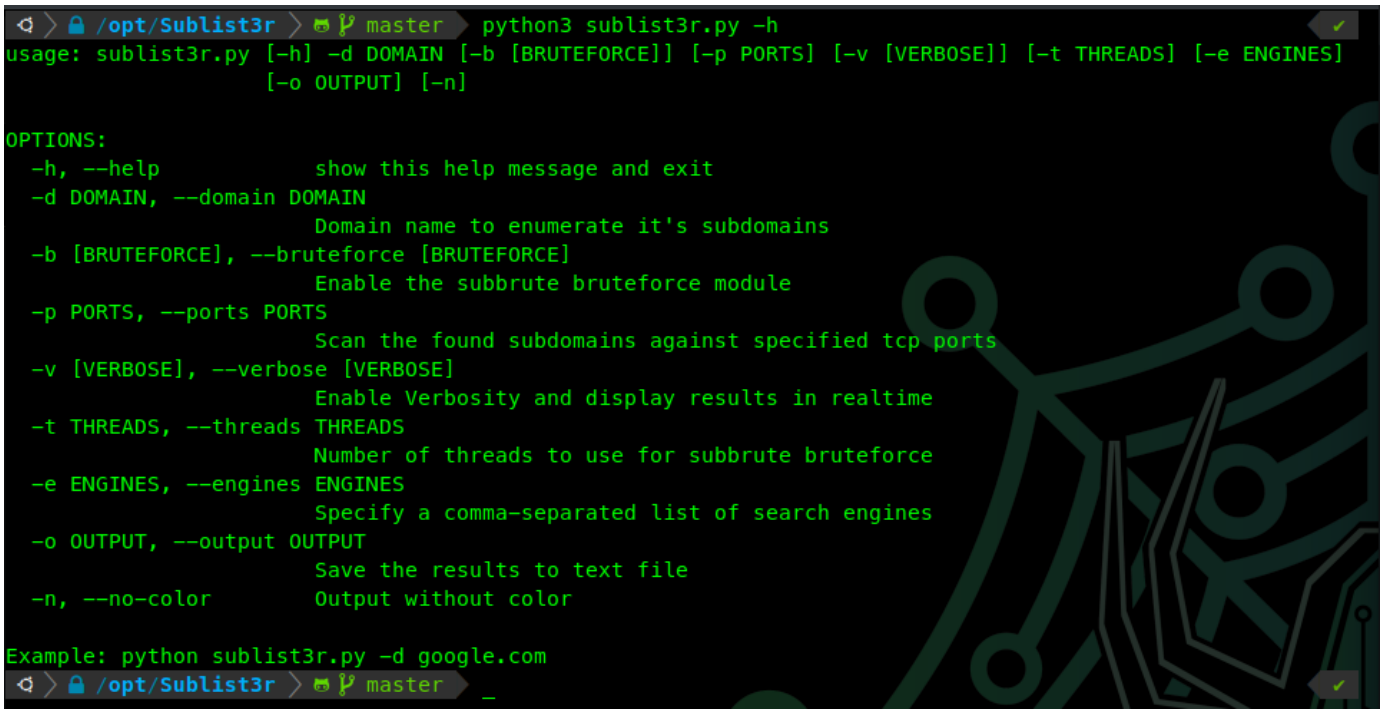
Hunting Breached Credentials with DeHashed

DeHashed "DeHashed is a public data search-engine created for Security Analysts, Journalists, Security Companies, and everyday people to help secure accounts and provide insight on breaches and account leaks. DeHashed can also be used for investigations & fraud prevention." This does cost money to use with an active subscription.
We can search: email, username, IP address, address, name, Phone number, VIN. At the time of these notes, I do not have an active subscription.
Hashes.org

Hunting Subdomains

Sublist3r

Sublist3r is a tool designed to enumerate subdomains of websites using OSINT.



Note: As of lately, it won't return results, this issue on github show if we edit the sublist3r.py file, go to line 158 and replace the user agent from:

`'User-Agent': 'Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36'`

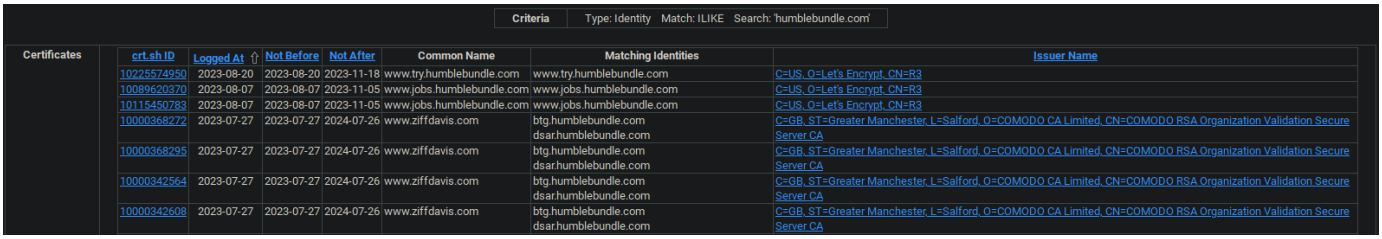
to:

`'User-Agent': 'Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:105.0) Gecko/20100101 Firefox/105.0'`


/opt/Sublist3r master !1 sudo python3 sublist3r.py -d humblebundle.com
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for humblebundle.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 26
www.humblebundle.com
andytest.humblebundle.com
blog.humblebundle.com
www.blog.humblebundle.com
btg.humblebundle.com
checkout.humblebundle.com
cn.humblebundle.com
de.humblebundle.com
developer.humblebundle.com
dsar.humblebundle.com
es.humblebundle.com
fr.humblebundle.com
it.humblebundle.com
jenkins.humblebundle.com
www.jobs.humblebundle.com
mailer.humblebundle.com
d.mailer.humblebundle.com
e.mailer.humblebundle.com
i.mailer.humblebundle.com
t.mailer.humblebundle.com
reviews.humblebundle.com
ru.humblebundle.com
support.humblebundle.com
try.humblebundle.com
www.try.humblebundle.com
zh.humblebundle.com
/opt/Sublist3r master !1

Crt.sh

Crt.sh is a tool to pull certificate fingerprints.



Criteria: Type: Identity Match: ILIKE Search: 'humblebundle.com'

Certificates

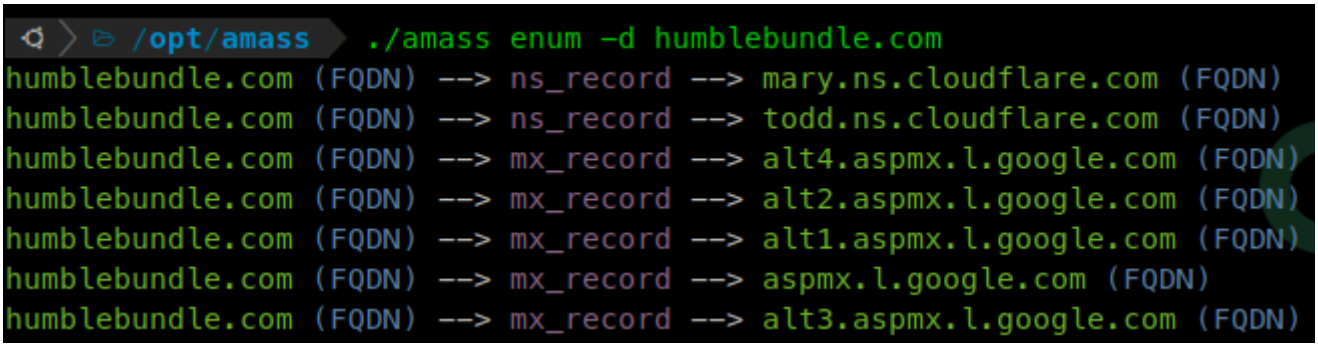
crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
10225574950	2023-08-20	2023-08-20	2023-11-18	www.try.humblebundle.com	www.try.humblebundle.com	C=US, O=Let's Encrypt, CN=R3
10089620370	2023-08-07	2023-08-07	2023-11-05	www.jobs.humblebundle.com	www.jobs.humblebundle.com	C=US, O=Let's Encrypt, CN=R3
10115450783	2023-08-07	2023-08-07	2023-11-05	www.jobs.humblebundle.com	www.jobs.humblebundle.com	C=US, O=Let's Encrypt, CN=R3
10000368272	2023-07-27	2023-07-27	2024-07-26	www.ziffdavis.com	btg.humblebundle.com dsar.humblebundle.com	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Organization Validation Secure Server CA
10000368295	2023-07-27	2023-07-27	2024-07-26	www.ziffdavis.com	btg.humblebundle.com dsar.humblebundle.com	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Organization Validation Secure Server CA
10000342564	2023-07-27	2023-07-27	2024-07-26	www.ziffdavis.com	btg.humblebundle.com dsar.humblebundle.com	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Organization Validation Secure Server CA
10000342608	2023-07-27	2023-07-27	2024-07-26	www.ziffdavis.com	btg.humblebundle.com dsar.humblebundle.com	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Organization Validation Secure Server CA

OWASP Amass

OWASP Amass "The OWASP Amass Project performs network mapping of attack surfaces and external asset discovery using open source information gathering and active reconnaissance

techniques."

A basic way to use amass is `amass enum -d example.com`, but as I am testing against HumbleBundle



Identifying Website Technologies

Tools we can use:
Builtwith
We can see various technologies the site is running, any widgets, languages, etc. What frameworks it's running. CDN(Content Delivery Network), etc.

Wappalyzer - Ad-on/Extention for Chrome/Firefox and again see what technologies the website is using.

WhatWeb - Simply analyzes websites.

Information Gathering with Burp Suite

I have my own notes and documentation on Burpsuite here.

Burpsuite

Google Fu

Simple enough, use Google. Using and understanding Google Search Syntax will be helpful. understanding how to use `site:`, remove results using subtract (`-www`), `filetype:` to find documents or PDFs,

Utilizing Social Media

Use Social Media like LinkedIn, Facebook, Twitter, etc.
Images hold a lot of information that have valuable OPSEC. Badge pictures, desks, etc. See the people and their email addresses and roles. Use their names for potential email addresses like `first.last@domain.com`.