Seth Ayers

02/13/2018

IT 430 – 02

Lab 3

SAyers\_Lab3.docx

**Digital Reconnaissance of USAA.com Domain and Hosts**

**Target:** [**www.USAA.com**](http://www.USAA.com)

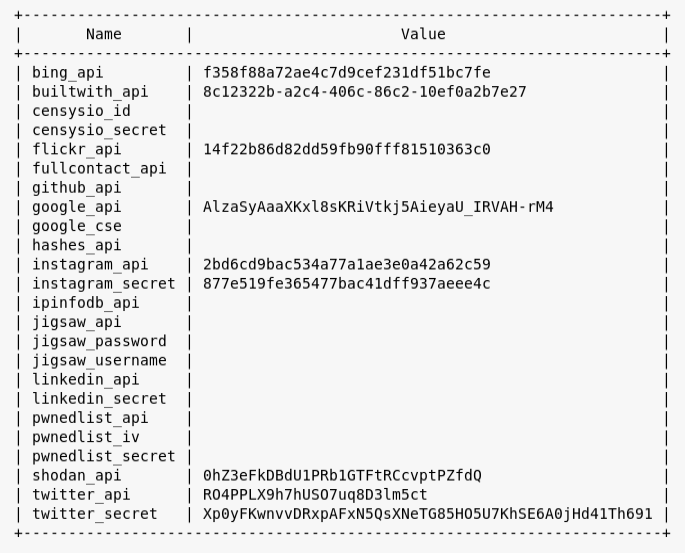
**Nature of Target:**

USAA, or originally known as The United Service Automobile Association, is a financial services company the specifically assists and provides United States military members with an assortment of banking options. Product services include: Mortgages solutions, banking options (Checking/Savings), automotive loans, and financial investing solutions. USAA has a member base of 11.9 million individuals, employs 28 thousand people, and has total assets in the range of 128 billion dollars USD.

**Reasoning:**

USAA, at it’s core, is a financial institution. Cybercriminals and social engineers tend gravitate to obtaining information that could potentially lead to monetary gain. This makes USAA’s digital infrastructure a prime target as obtaining sensitive information of customer assets or collecting sensitive internal information could lead to successful theft. Additionally, there’s another external threat vector; cyberterrorism and hacktivist. The fact that USAA provides services to only military members and their families makes it a prime target for the mentioned subgroups of hackers/crackers. With the high concentration of military members, disrupting operations of the company, obtaining sensitive information of customers, or stealing assets would not only have detrimental and damaging effects of the members, but possibly hinder effectiveness of the countries national defense.

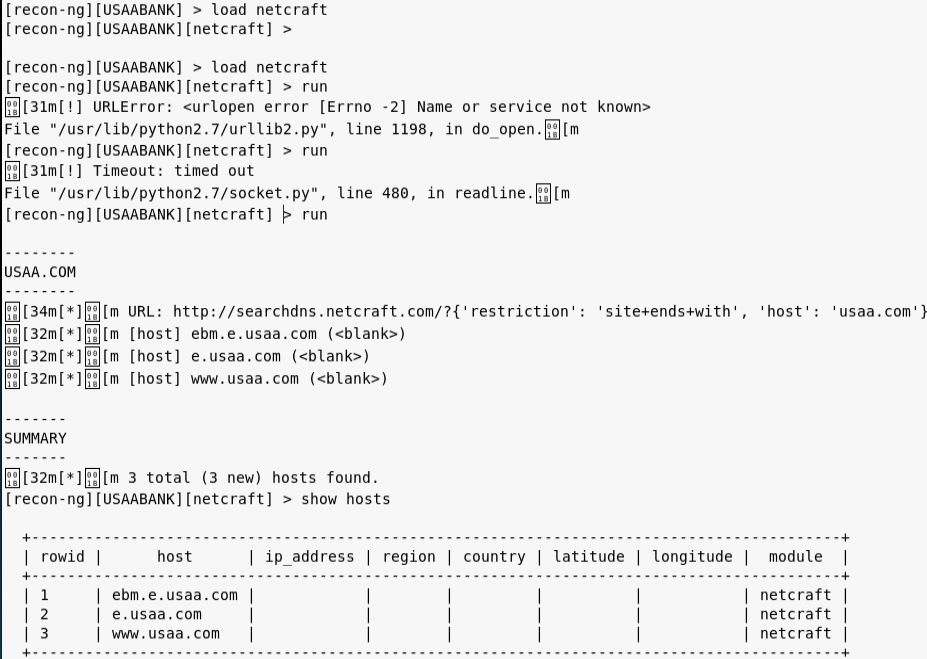
**API keys used:**



**Commands used and results:**

**Netcraft**

Result: Searches to provide related hosts of the target domain.



**recon/domains-hosts/google\_site\_web**

Result: Uses the google search engine to find hosts related to the target domain.



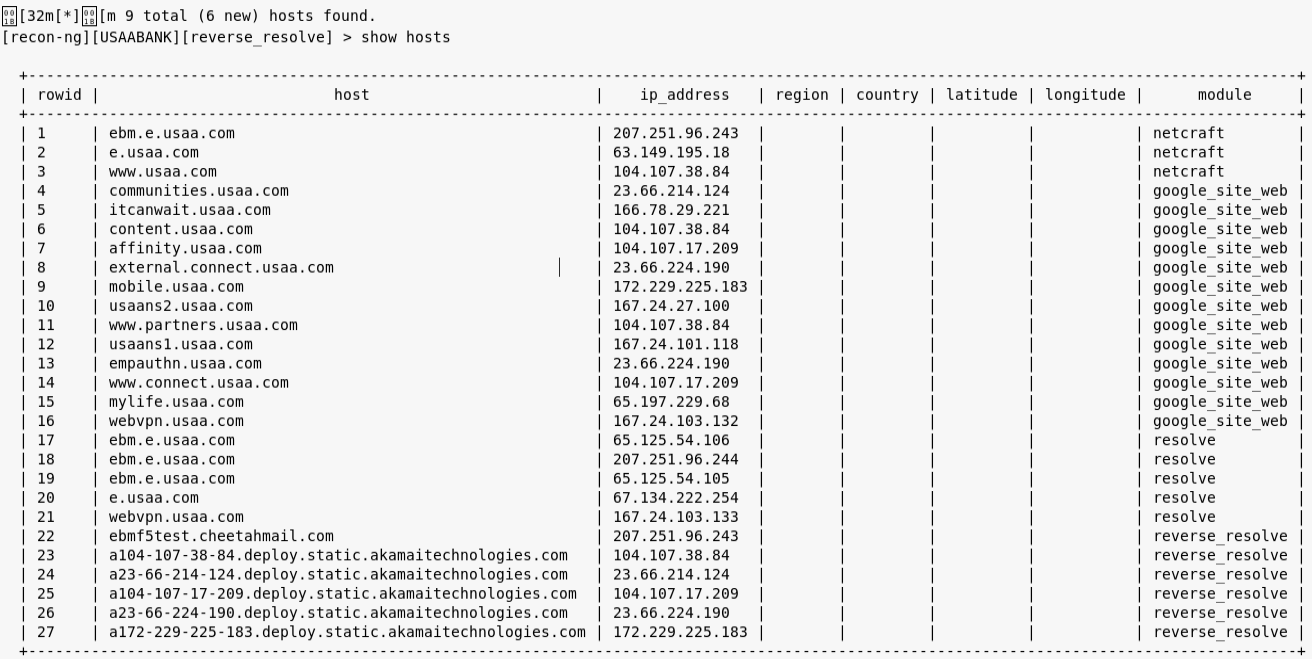
**recon/hosts-hosts/resolve**

Result: Resolves host names to an IP address. In this case resolve found 5 new hosts that weren’t picked up by the previous searches.



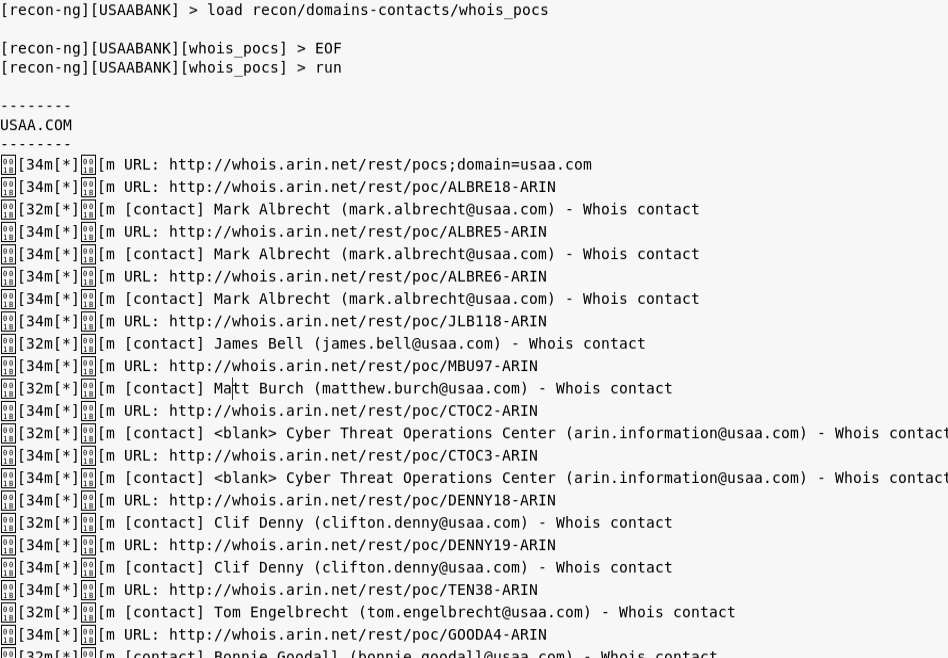
**recon/hosts-hosts/reverse\_resolve**

Result: Preforms a reverse resolve of IP addresses to the host name. As with the resolve command, the reverse\_resolve found 6 new hosts. However, these hosts seem to not relate to the target and can be dismissed.



**recon/domains-contacts/whois\_pocs**

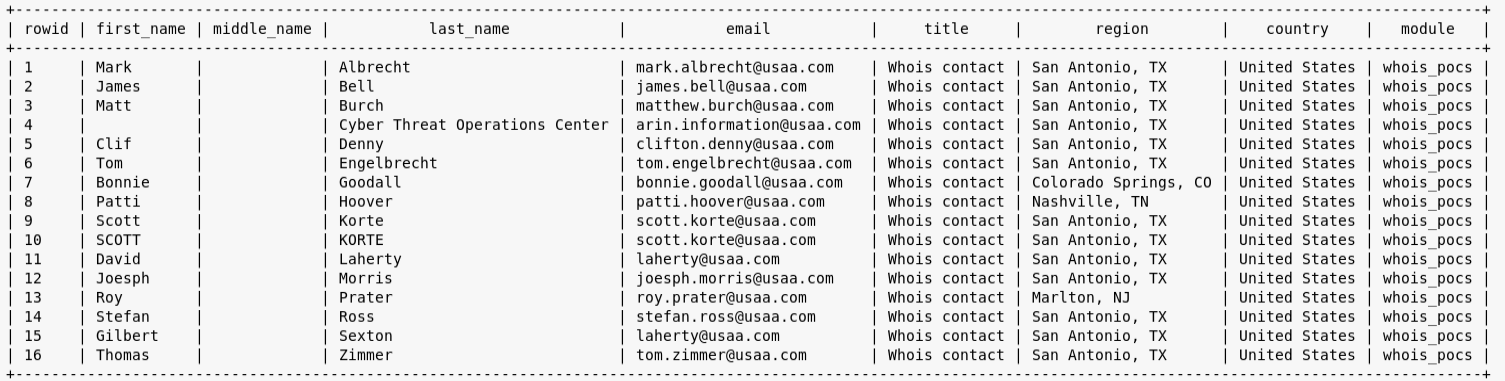
Result: Searches point of contact information for the target domain. The command found 16 names and contact emails associated with the target.



**recon/contacts-credentials/hibp\_breach**

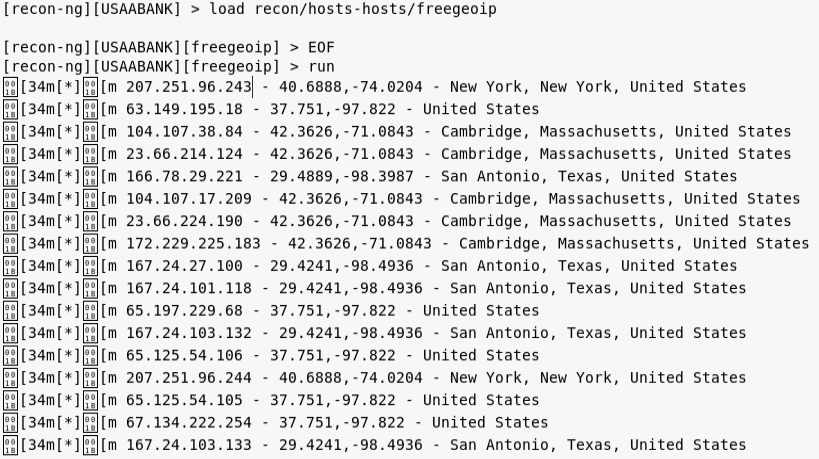
Result: Uses the populated POC data and searches for any known breaches of credentials.

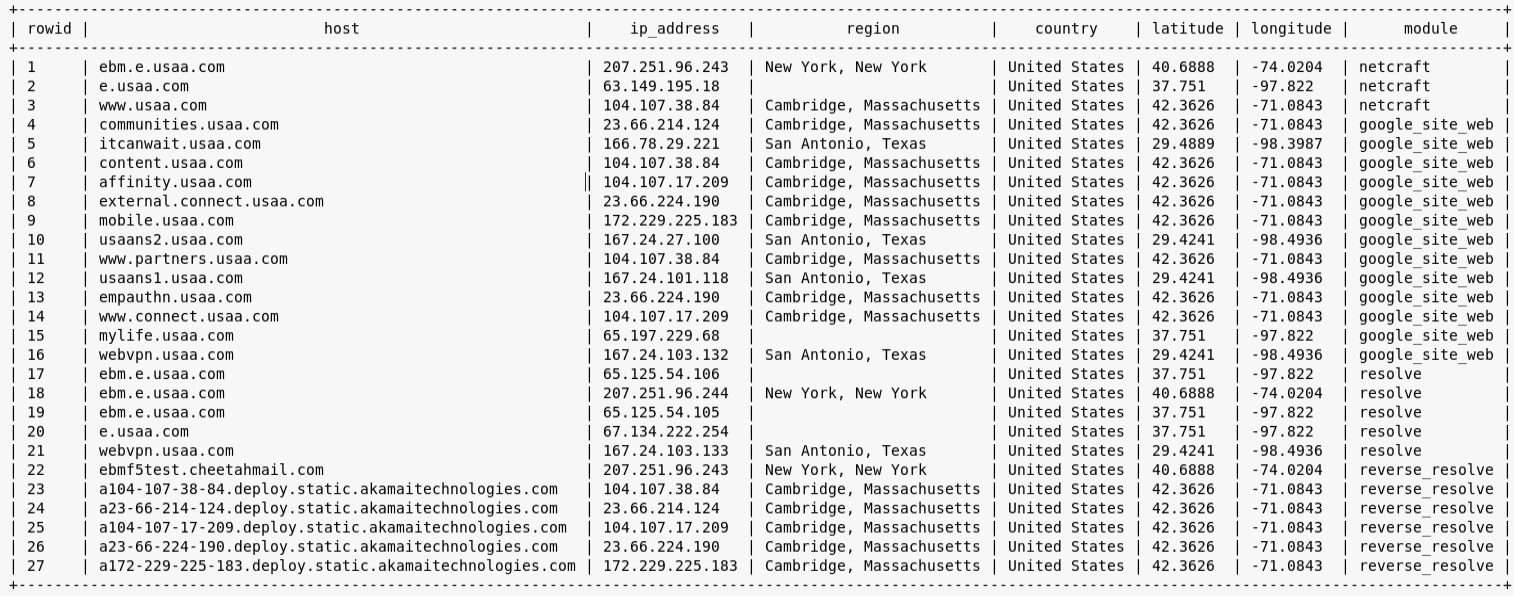




**recon/hosts-hosts/freegeoip**

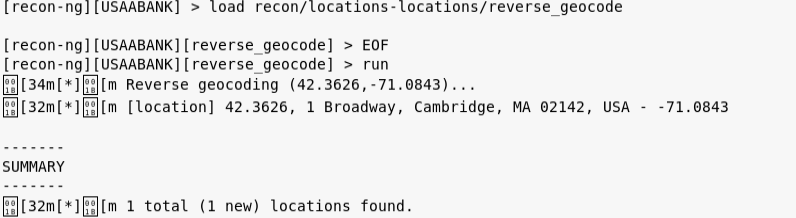
Result: Takes the list of host IP’s and searches for a geographical location for each host.

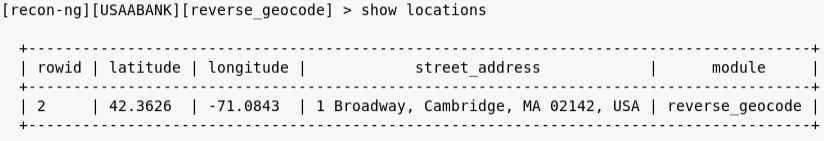




**recon/locations-locations/reverse\_geocode**

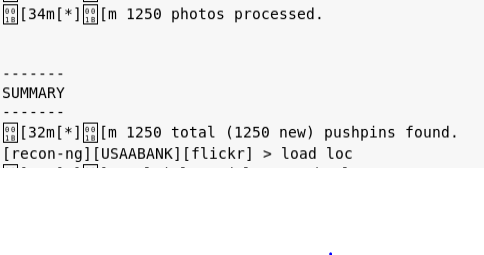
Result: Searches a specific latitude and longitude of an IP and adds the address of the findings to the locations SOURCE table. In this case, I chose the location of the target server [www.USAA.com](http://www.USAA.com).





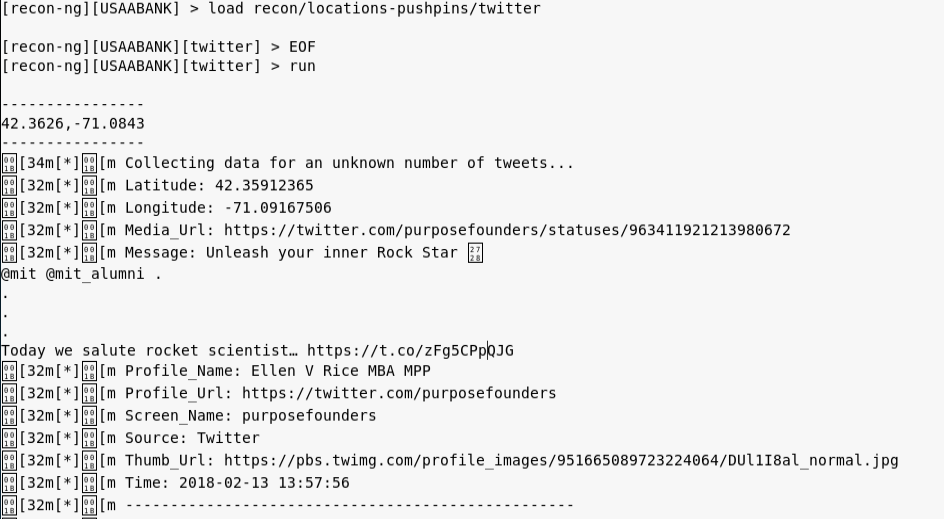
**recon/locations-pushpins/flickr**

Result: Uses the location in the table to find flickr pictures with metadata that match the location within 1 kilometer. The information is “pinned” to a map as well as an infograph of the search.



**recon/locations-pushpins/twitter**

Result: Uses the location in the table to find twitter tweets that have a location indicator within 1 kilometer. The information is “pinned” to a map as well as an infograph. The results are slim however, this is due to the twitter API having limitations to developers not associated with the company.

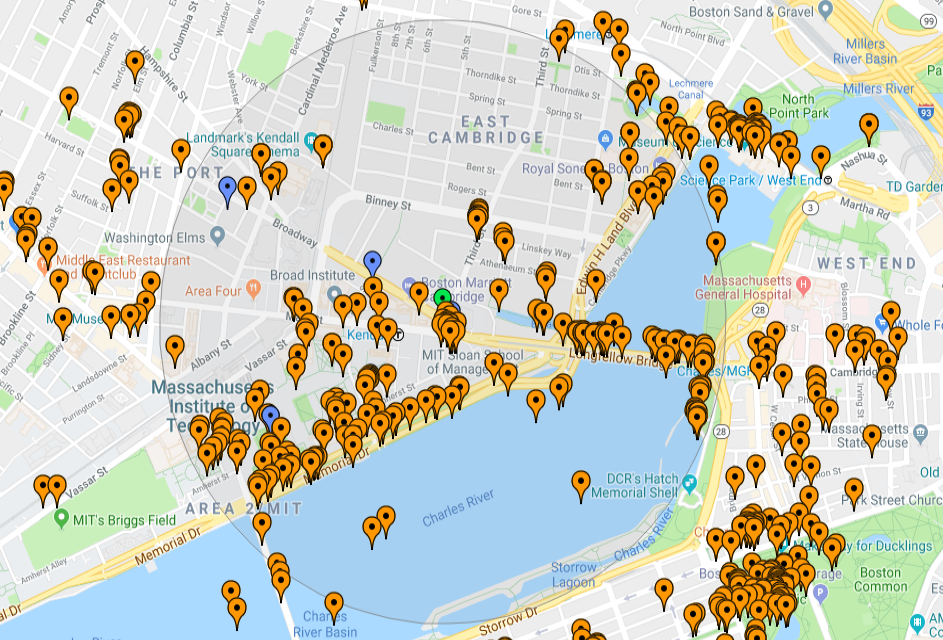


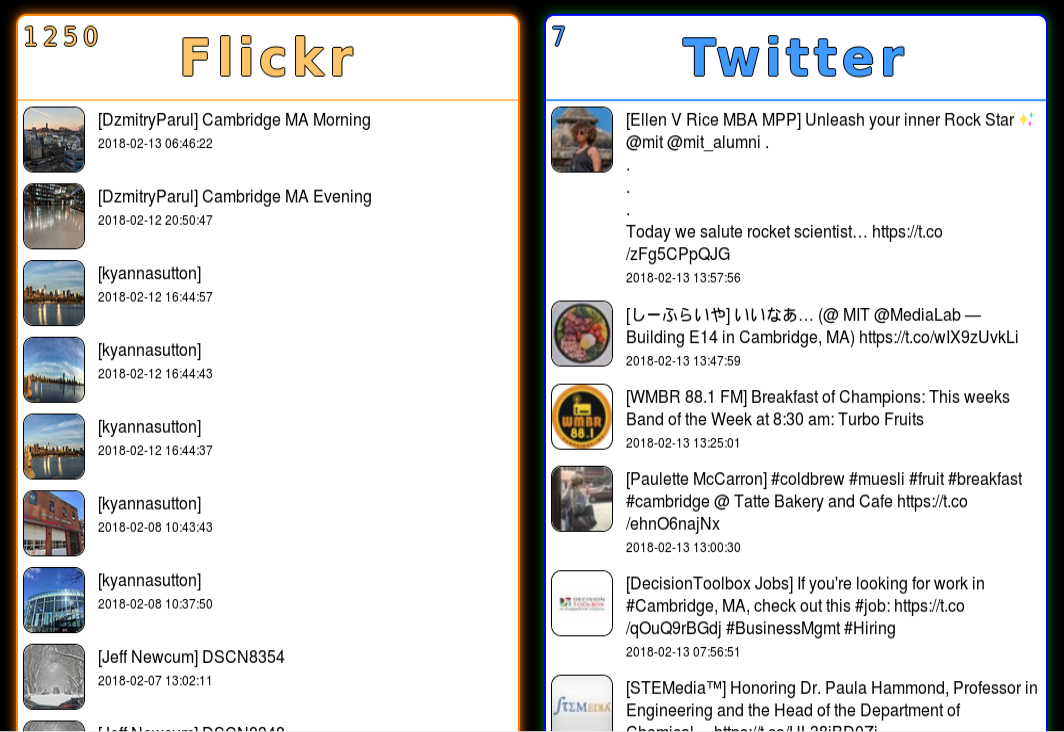
Additional actions for pushpin:

The following is to write the data collected from the pushpin results from above.



Map and infograph of the data:





**Result impressions and observations:**

Overall, Recon-ng has the protentional to provide large amounts of valuable data about a pentest target, or multiple pentest targets. Domain and host information, IP addresses, and locations gives the pentester or hacker a starting point in which port scanning and OS checks can be performed, as well as vulnerability checks. Point of contact information can be used for social engineering, and if used with the pushpin social media commands, can be used to target individuals specifically and obtain personal information. This information might be utilized to gain access to systems or impersonate the individual. In addition to the in-depth POC contact information, recon-ng can also scan for known leaks of credentials. Depending on the nature of the leak, a pentester or hacker could possibly get vital information from the leak, depending on the type and nature of it. Lastly, having a geographical location of hosts can provide some dumpster diving opportunities, possibly finding sensitive information about the hardware and software.

In terms of the target I selected, USAA, their footprint is surprisingly small in comparison to other similar institutions. I did refrain from preforming a brute force scan of the domain and just used my google, resolve/reverse\_resolve , and netcraft api’s to scan for relevant hosts.