Lab 01 Template – Ethan Roepke

1. **WHOIS query Screenshot**

(15 points)

A screenshot of a contact page

Description automatically generated

1. Domain owner and contact info
   1. No given info on Domain information but the registrar is Network Solutions, LLC
   2. Perfect Privacy, LLC
   3. Phone - +1.5707088622
   4. Email - email@networksolutionsprivateregistration.com
2. Domain administrator and contact info
   1. Perfect Privacy, LLC
   2. Phone - +1.5707088622
   3. Email - email@networksolutionsprivateregistration.com
3. The IP ranges that the domain has registered to it (include the CIDR)
   1. IP - 13.89.172.22
   2. IP range – 13.64.0.0 - 13.95.255.255
   3. CIDR – 13.64.0.0/11
4. **DNS Interrogation screenshot**

(15 points)

1. Mail server

A close-up of a logo

Description automatically generated

The mail server is shown in above image -> figopetinsurance-com.mail.protection.outlook.com

This lets us know that they work through Microsoft

1. DNS server

A close-up of a computer code

Description automatically generated

Figo Pet Insurance uses worldnic for their domain name host

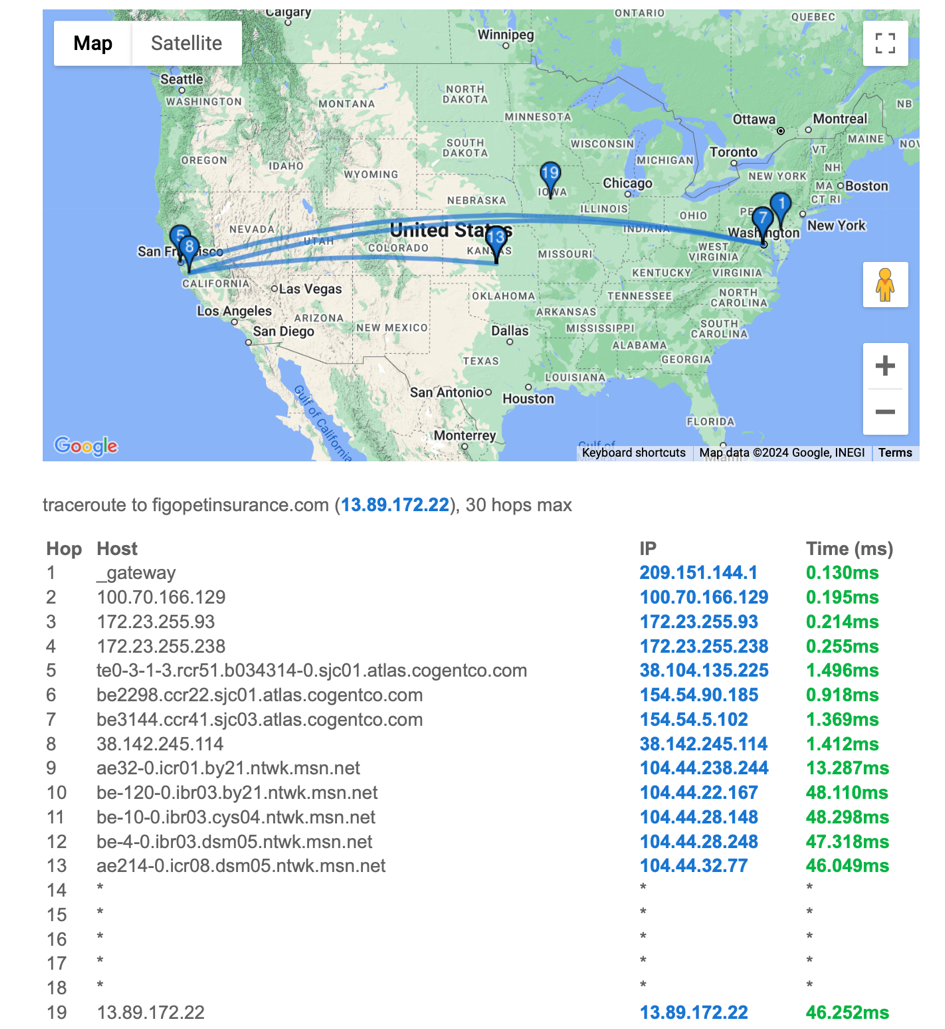
1. Find one other server

A close-up of a business card

Description automatically generated

1. **Screenshot of traceroutes - include both a visual and textual**

(10 points)



A screenshot of a computer code

Description automatically generated

1. **Geolocation of host(s) screenshot**

(10 points)

A screenshot of a map

Description automatically generated

1. What country
   1. United States
2. Which ISP
   1. Microsoft Corporation
3. Who is providing the hosting of the website?
   1. worldNic is the hosting of website
4. Who is providing the target’s DNS?
   1. Microsoft Azure

1. **Sensitive information on public website - screenshots/description of why useful**

(10 points)

1. Employee rosters and email addresses

A screenshot of a phone number and address

Description automatically generated

After scrolling through the source code and website for quite some time, I have been unsuccessful in gathering employee roster and contacts. All that I could find in support phone numbers and email. Given that this is mostly a remote job, there personal information is hidden. All that I was able to find was images with some of the workers and their pets as well as their first name. Using that we could possibly use keywords in google and find personal information about them online.

A person and a dog

Description automatically generated

After doing this process of looking up a name and working at figo, it brought me to another website called “The org” which gives a branch of employers starting from CEO and all the subdivisions. This is a big progress to now finding contact information next.

A screenshot of a computer

Description automatically generated

1. Technical documents (how to use services/login/etc)

A screenshot of a medical records form

Description automatically generated

1. **Recent happenings in the news - screenshots/description of why useful**

(10 points)

1. Mergers

A screenshot of a website

Description automatically generated

1. Acquisitions

A screenshot of a computer

Description automatically generated

1. Where do you believe vulnerabilities may lie?
   1. I believe vulnerabilities may lie in between the JAB servers and Figo servers. If JAB has a flaw in their server that an attacker could gain access to, theoretically they would be able to get access to the Figo servers since they need some sort of connections between them.
   2. Costco partners with figo pet insurance so members at Costco can get a discount through figo and be able to get pet prescriptions as well at Costco for free. Between these two companies, a vulnerability is if an attacker wants to attack Costco and finds a hole in Figo’s server and gains access, then they are able to find a way to get inside Costco’s server since they need to have some connection to be able to know Costco memberships and information.

1. **Vulnerable web apps**

(15 points)

1. Can you find any vulnerable web apps using Google Dorks against your target?
   1. When using google dork against Figopetinsurance.com, for filetypes, I chose these options because maybe I would be able to find a file with usernames/passwords or possibly files claimed but, I mostly got in return “brochures” and “claim a file”.
   2. I next did a “intitle:login” that would give specific text in html titles and hoping would give me webs for login pages. All I got in return was a website that had multiple figo web pages directing you to a login page.
   3. Next I did a “inurl:admin” hoping to get something in return with “admin” or “login.php” in the URL, however after searching it pops up with nothing.
   4. Lastly I tried a “cache” which I am not familiar with so I did not know what I was completely looking for but when I entered it in, it sent me to their website. I do not know if I did something wrong or found nothing important.
2. Provide list of google queries you tried
   1. Filetype:pdf
   2. Filetype:doc
   3. Filetype:xls
   4. Filetype:log
   5. Intitle:login
   6. Inurl:admin
   7. Inutl:login.php
   8. Cache:figopetinsurance.com/login.php

1. **Similar Domains**

(15 points)

1. Can you find any domains similar to the target for sale?
   1. It looks like they only own figopetinsurance.com, however figopetinsurance.org(.net, and more that could be used) that were available. As well as this being a long domain name, an attacker could change a letter in the domain name (i -> l or a-> o) and most independent people would not recognize the difference and could be looking at a fake website. As well they could change the domain name to “figo-petinsurance.com” and would be very believable that it’s the real website.
2. Are there domains that might benefit an attacker, should they be purchased?
   1. There are many domain names available that would benefit attackers, especially in an insurance world if paying a monthly subscription, an attacker could set up the exact website and set up and gain valuable money with not many people realizing a difference between the fake and real domain.
   2. I do believe Figo should purchase these domain names so they are protected from attackers making copies of their website with a very familiar domain name. This would help customers to reach the correct website and not a fake website where Figo could be losing money from.