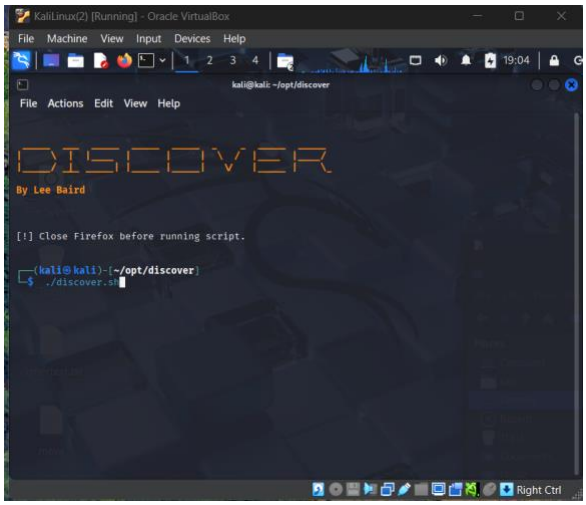
Introduction

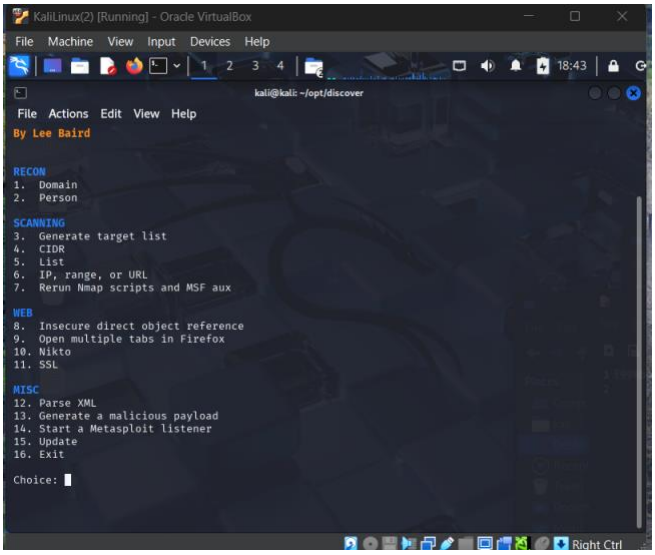
Through this project I will gain a better understanding of the importance of reconnaissance and footprinting for ethical hacking and penetration testing. I will learn multiple Open-Source Intelligence (OSINT) tools and apply them to complete both passive and active reconnaissance and footprinting. With this background knowledge of information gathering and OSINT tools I will apply what I've learned to two exercises involving scanning a domain using Discover and using other OSINT tools and techniques to gather information about the REPUBLICOFKOFFEE.COM domain.

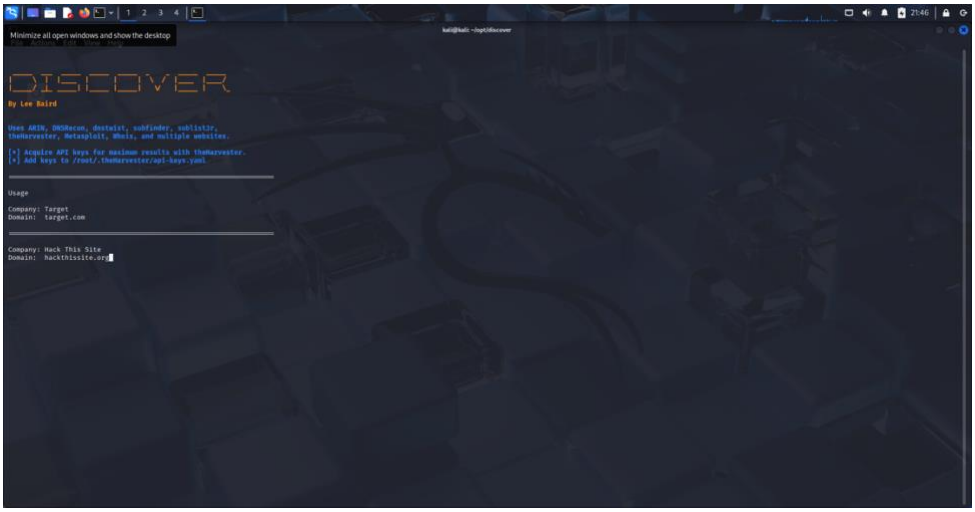
Exercise 1: Utilizing Discover

Passive Scan

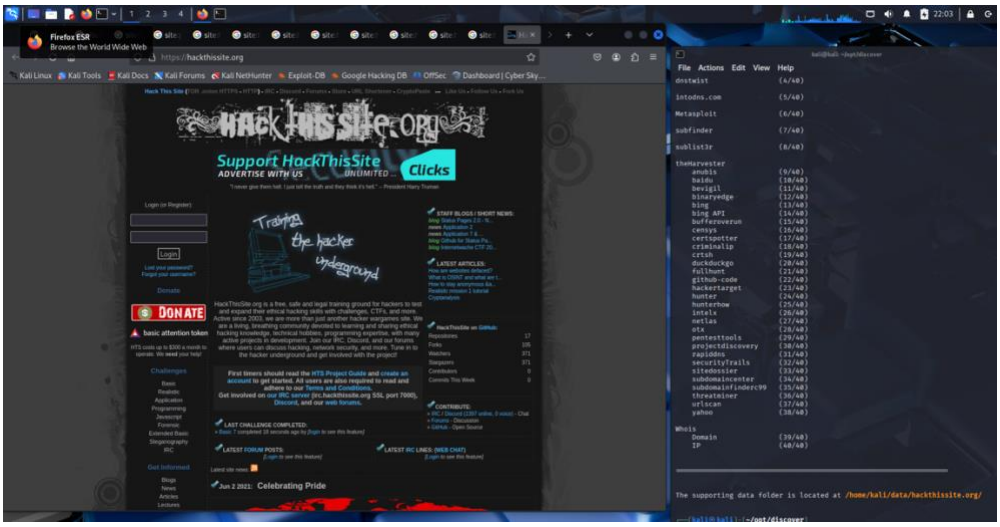


After installing and updating discover ensure firefox is closed, you are running it as the home Kali user and all permissions/ownership belong to the correct user.

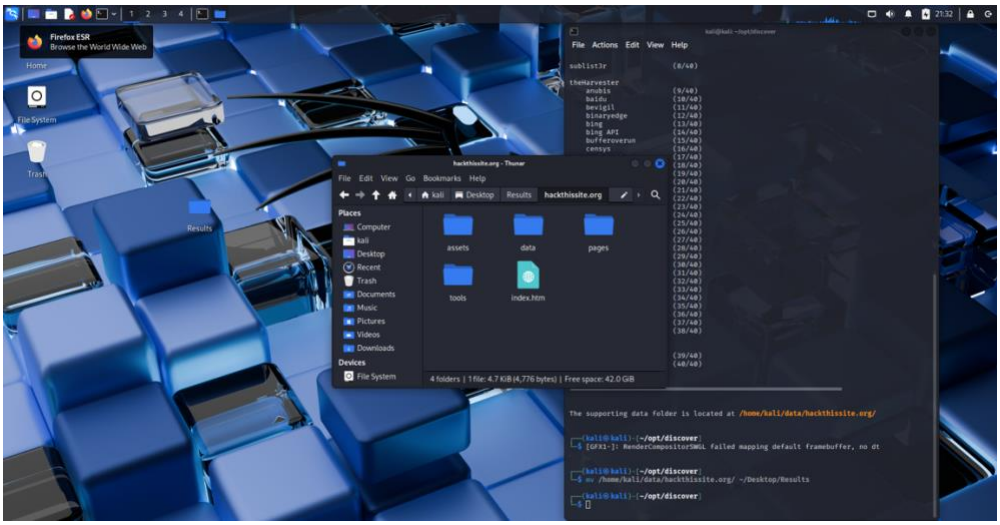


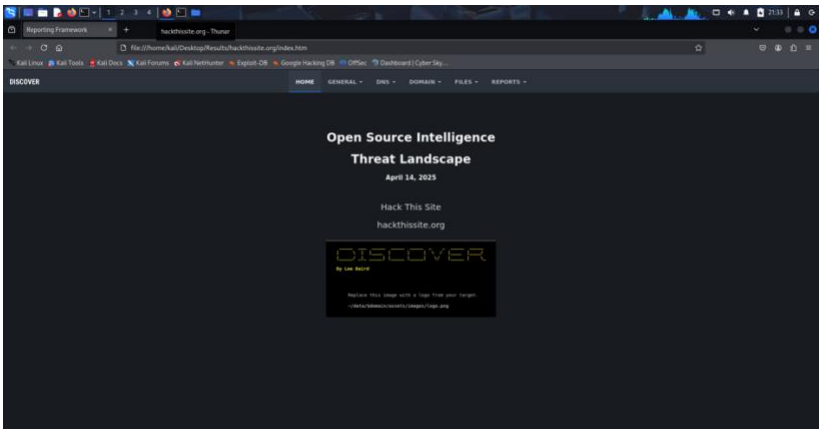


Choose Domain, then Passive scan, then input the target title and domain.

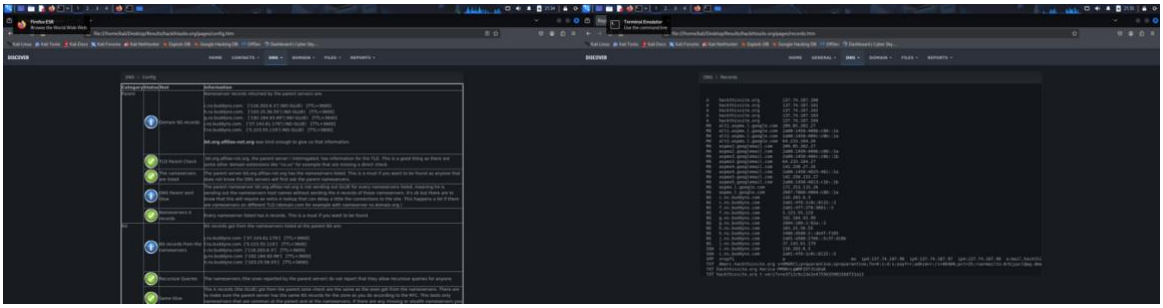


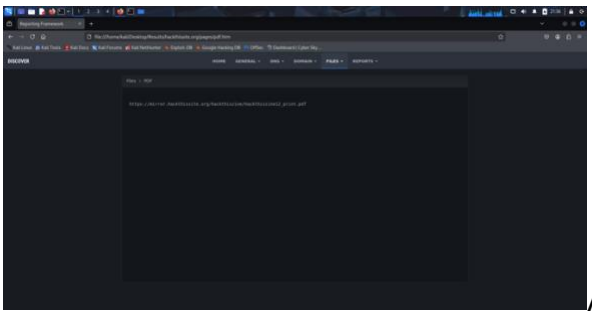
The Discover tool will run, executing a 40-step scan of the domain. After the scan is complete Firefox tabs aligning with each step of Recon open and an HTML document, index.htm is created which holds the entire summary of the scan. Also ran a command to move the scan results to an easy to access folder on the desktop.





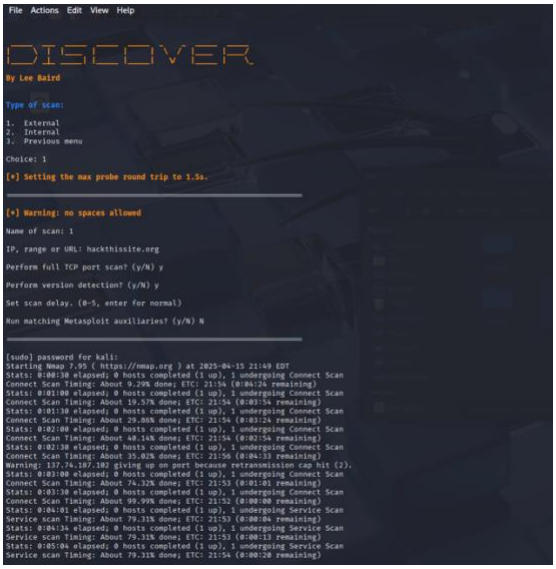
The summary site.

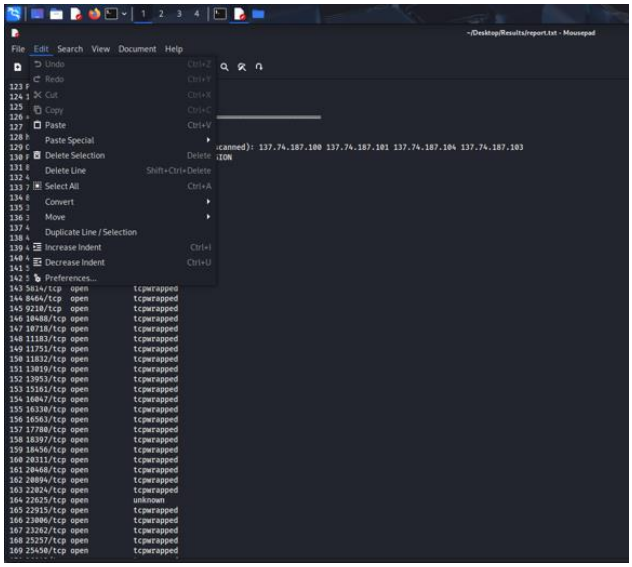



A myriad of information about the domain was gathered. Including IP information, source code, user logs, individual .pdf files, and much more.

Active Scan

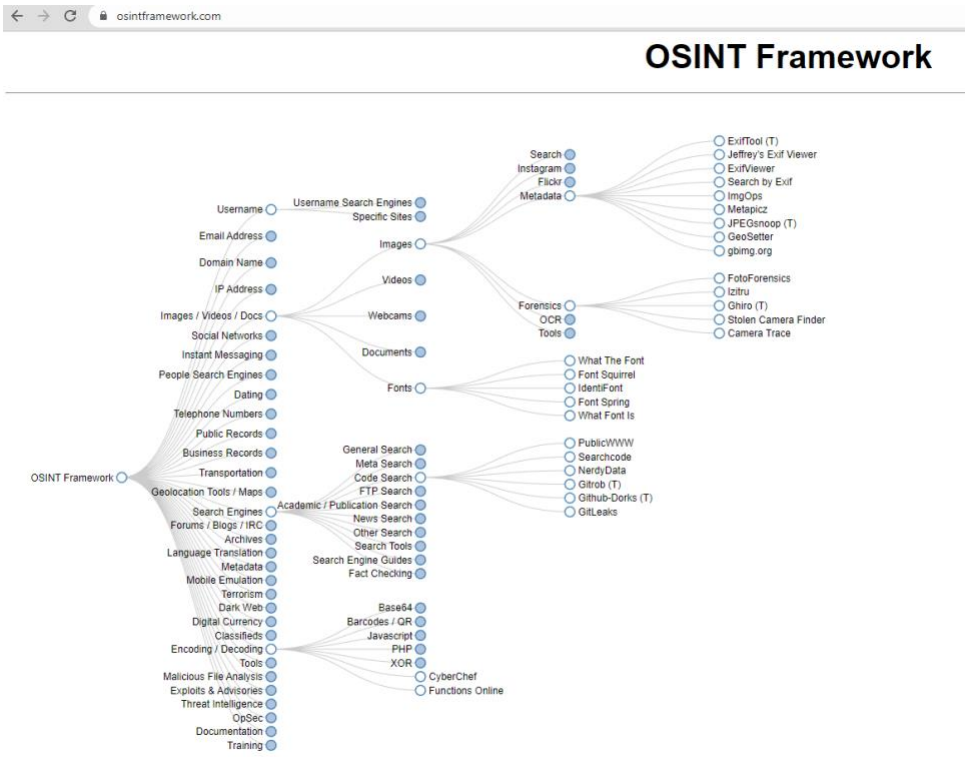
To gather more information about Hackthissite.org I played around with the active scanning options.





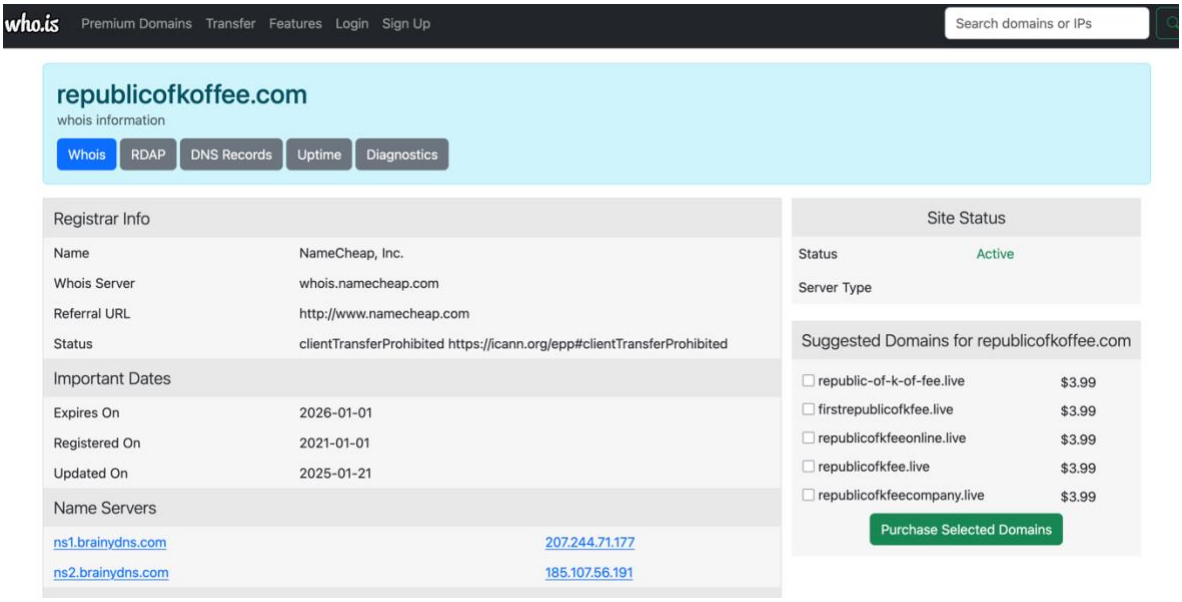
The scan I had the most success with was an NMAP report. After inputting the url of our target and configuring the settings the scan generated a report of potential targets, open ports, and tcp versions. A hacket could use this active scan to identify the ports within the network that are exploitable and available for access.

Exercise 2: Open Source Intelligence



I found this helpful framework (from osintframework.com) which provides resources for all different types of open source intelligence gathering. Utilizing this and the different tools brought forth in the prelude of the project I will put together information on the domain: REPUBLICOFKOFFEE.COM

1. Who owns the domain?



Using the who.is tool I found that the registrar of the domain is **NameCheap, Inc**.

2. When was it created (date and time)?

Also, according to the who.is database, the domain was registered on **January 1st, 2021**

3. What is the second name server associated with this domain?

The second name server associated with this domain is **ns2.brainydns.com**. The IP is 185.107.56.191

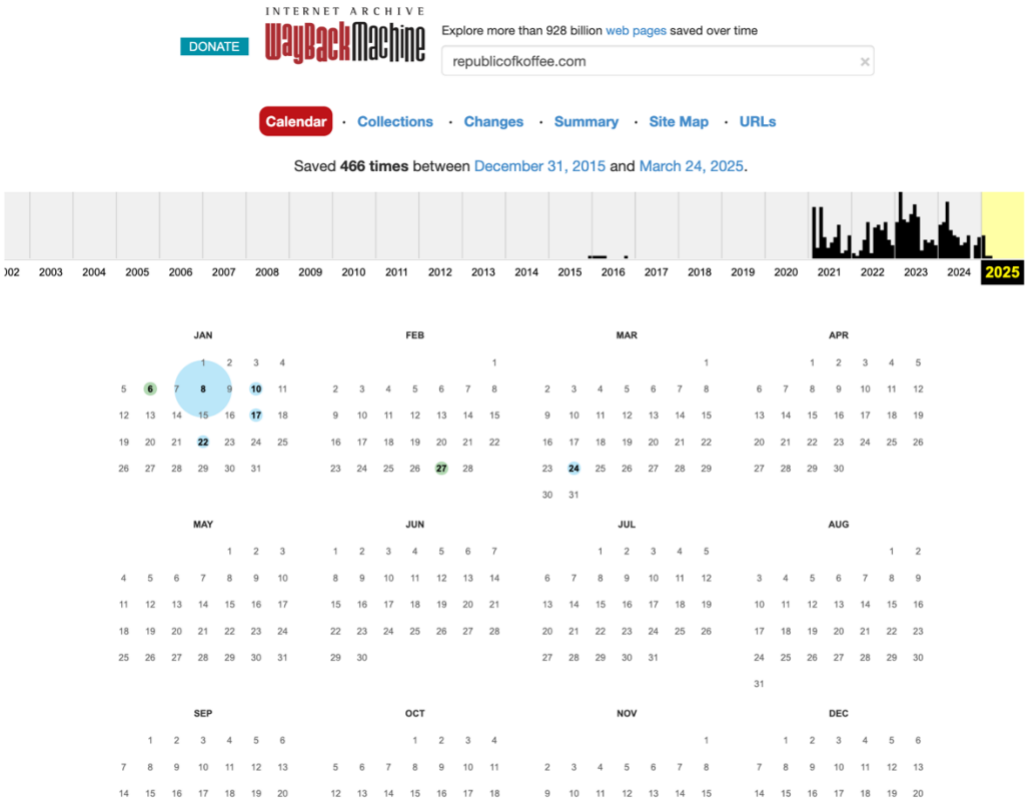
4. What is the name of registrant, if available?

On the who.is website, the name of the registrant was redacted. So unfortunately I was unable to find the name of the registrant.

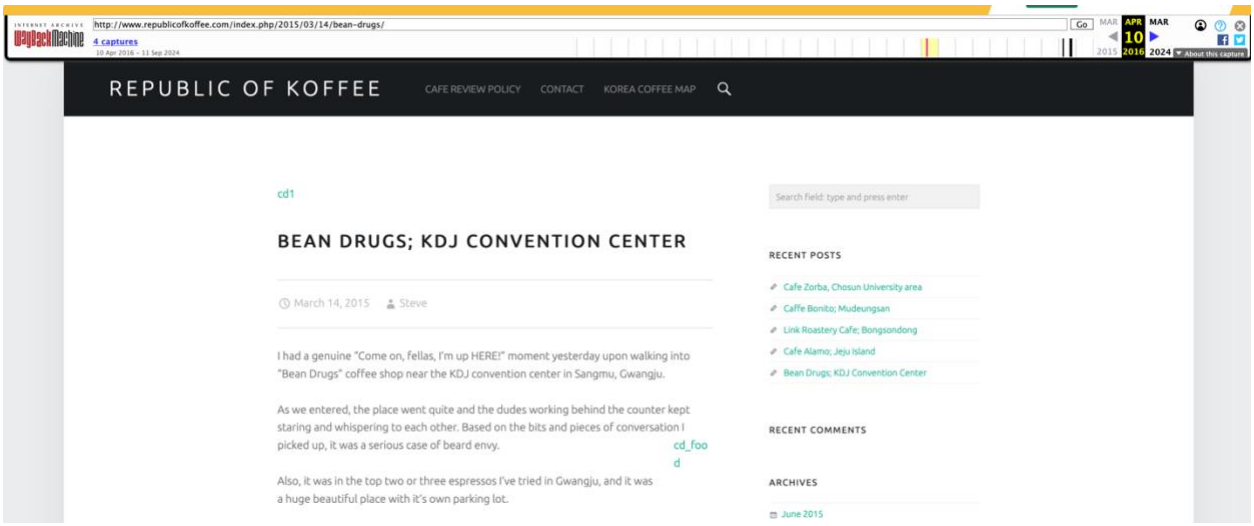
5. What is the country of the registrant?

Back within the registrar data I found that the city of the registrar is Reykjavik in the State/Province: Capital Region. After a google search I found that this city is in **Iceland**.

6. What was the name of the author of the very first blog on the website?



Using the Wayback Machine, I found that the earliest snapshot in their database for republicofkoffee.com was from *way back* in December, 2015.



After opening the snapshot there were 5 articles on the page with the oldest one being published March 14, 2015 by **Steve**. The article gives a review of "Bean Drugs" coffee shop.

Out of curiosity I looked a little emore into this coffee shop. It was in South Korea, but the most recent trip advisor report was from June 2015 and there was only one review. 5 out of 5 stars.

Conclusion

The main thing I learned from this project was how fast open-source intelligence is. I feel the phenomena of the more you know, the less you know after completing this project. It is very fascinating to see how much information is out there that you may believe is private and how many tools there are to recover it. Through the prelude I got an introduction to the different methods of information gathering and the tools that could be used with them. Overall throughout this project I have gained lots of insight into open source intelligence and my interest in the subject has grown.