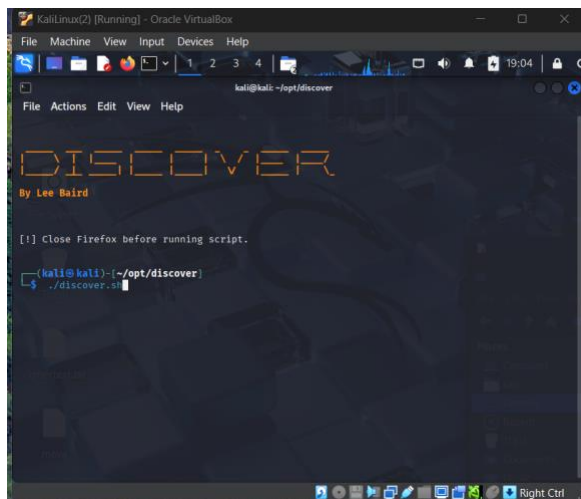


Introduction

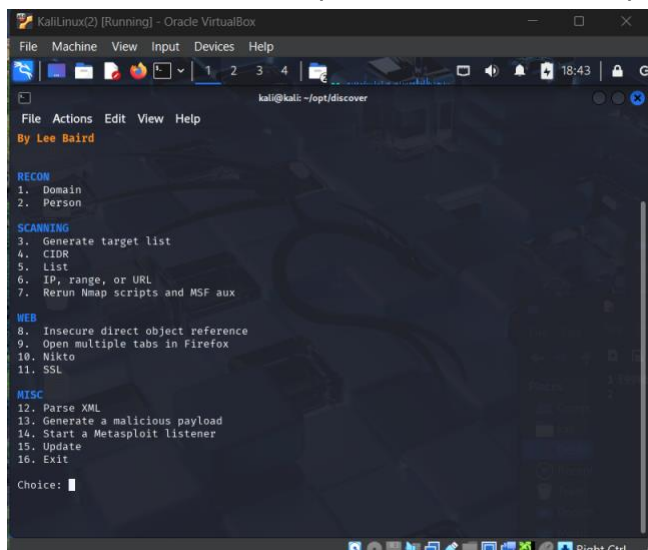
Through this project I will gain a better understanding of the importance of reconnaissance and footprinting for ethical hacking and penetration testing. I will learn multiple Open-Source Intelligence (OSINT) tools and apply them to complete both passive and active reconnaissance and footprinting. With 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 REPUBLICOFFKOFFEE.COM domain.

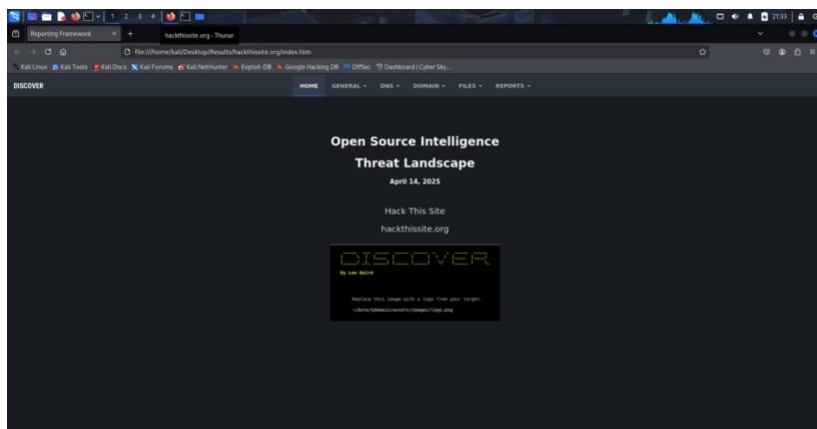
Exercise 1: Utilizing Discover

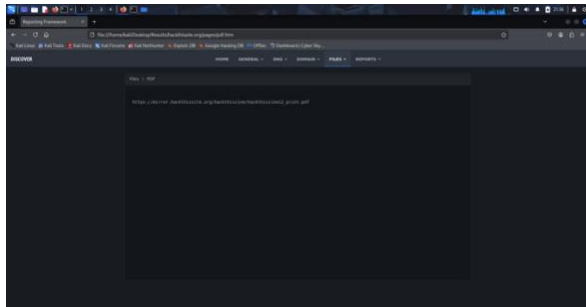
Passive Scan



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.



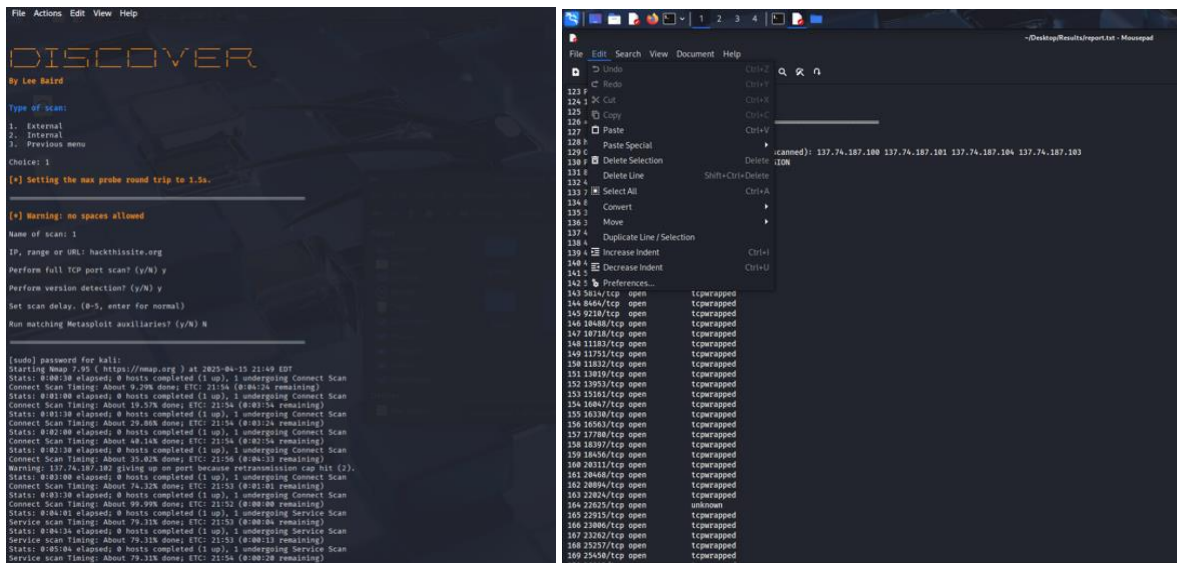




A myriad of information about the domain was gathered. Including IP information, source code, user logs, individual .pdf files, and much more.

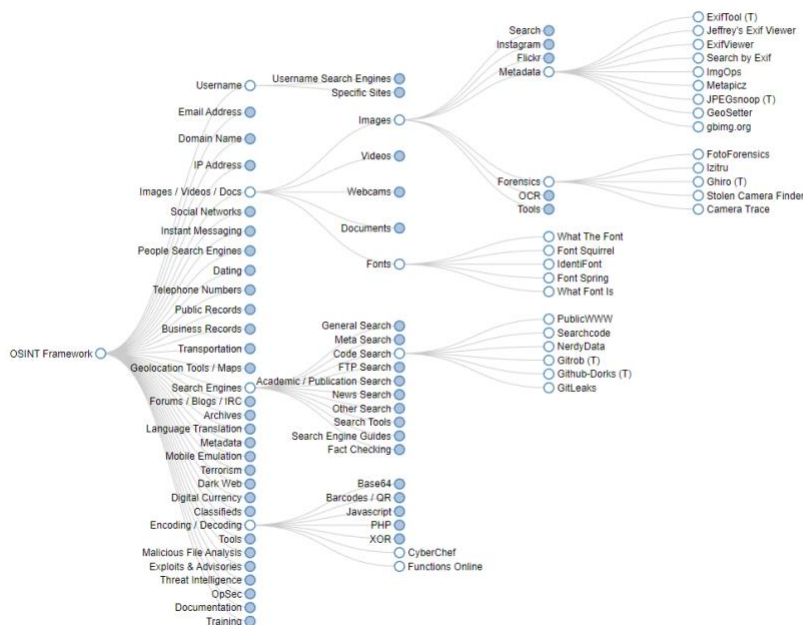
Active Scan

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 hacker 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: **REPUBLICOFFKOFFEE.COM**

1. Who owns the domain?

who.is Premium Domains Transfer Features Login Sign Up Search domains or IPs

republicoffkoffee.com

whois information

Whois RDAP DNS Records Uptime Diagnostics

Registrar Info		Site Status	
Name	NameCheap, Inc.	Status	Active
Whois Server	whois.namecheap.com	Server Type	
Referral URL	http://www.namecheap.com	Suggested Domains for republicoffkoffee.com	
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited	<input type="checkbox"/> republic-of-k-of-fee.live	\$3.99
Important Dates		<input type="checkbox"/> firstrepublicoffkoffee.live	\$3.99
Expires On	2026-01-01	<input type="checkbox"/> republicoffkoffeeonline.live	\$3.99
Registered On	2021-01-01	<input type="checkbox"/> republicoffkoffee.live	\$3.99
Updated On	2025-01-21	<input type="checkbox"/> republicoffkoffeecompany.live	\$3.99
Name Servers		Purchase Selected Domains	
ns1.brainydns.com	207.244.71.177		
ns2.brainydns.com	185.107.56.191		

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?

[repub.de](#) | [repub.ir](#) | [repub.info](#) | [repub.io](#) | [repub.it](#) |

Registrar Data

[Make Private Now](#)

We will display stored WHOIS data for up to 30 days.

Registrant Contact Information:

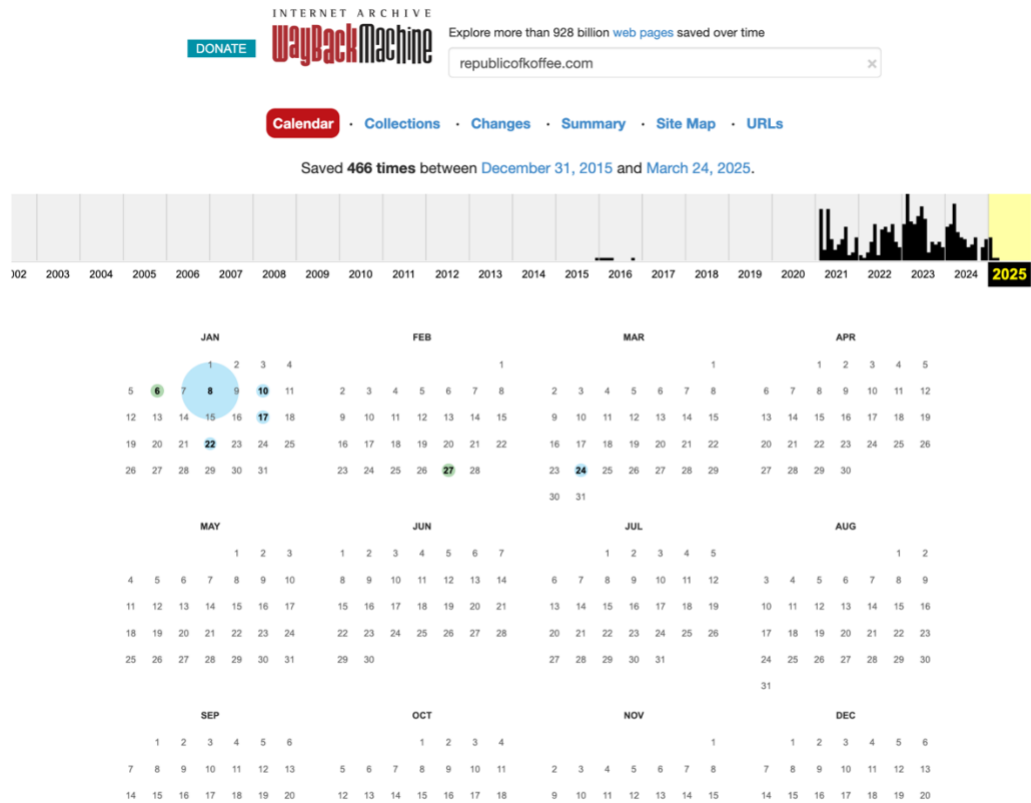
Name:	Redacted for Privacy
Organization:	Privacy service provided by Withheld for Privacy ehf
Address Line 1:	Kalkofnsvegur 2
Address Line 2:	
City:	Reykjavik
State/Province:	Capital Region
Postal Code:	101
Country:	IS
Phone:	+354.4212434
Fax:	
Email:	eabcfee13f0440cc8f3f9aeef8121917.protect@withheldforprivacy.com
Full Address:	Kalkofnsvegur 2, Reykjavik, Capital Region, 101, IS

Administrative Contact Information:

Name:	Redacted for Privacy
Organization:	Privacy service provided by Withheld for Privacy ehf

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.

INTERNET ARCHIVE
WayBack Machine
http://www.republicofkoffee.com/index.php/2015/03/14/bean-drugs/
4 captures
10 Apr 2018 - 11 Sep 2024

REPUBLIC OF KOFFEE CAFE REVIEW POLICY CONTACT KOREA COFFEE MAP

cd1

BEAN DRUGS; KDJ CONVENTION CENTER

March 14, 2015 Steve

I had a genuine "Come on, fellas, I'm up HERE!" moment yesterday upon walking into "Bean Drugs" coffee shop near the KDJ convention center in Sangmu, Gwangju.

As we entered, the place went quite and the dudes working behind the counter kept staring and whispering to each other. Based on the bits and pieces of conversation I picked up, it was a serious case of beard envy.

Also, it was in the top two or three espressos I've tried in Gwangju, and it was a huge beautiful place with it's own parking lot.

cd_foo id

Search field: type and press enter

RECENT POSTS

- Cafe Zorba, Chosun University area
- Caffe Bonito; Mujeungsan
- Link Roastery Cafe; Bongsodong
- Cafe Alamo; Jeju Island
- Bean Drugs; KDJ Convention Center

RECENT COMMENTS

ARCHIVES

June 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 more 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.