Report on Passive Reconnaissance in Network Security

Introduction

The first room of the Network Security Module emphasizes the importance of Passive Reconnaissance, a fundamental aspect of cybersecurity. This module covers various reconnaissance methods and introduces essential tools for gathering information discreetly.

https://tryhackme.com/p/Damiano254

Task 1: Overview of Passive Reconnaissance

Passive Reconnaissance is a critical initial step in cybersecurity, allowing one to gather information without alerting the target. This task introduces key tools for passive information gathering:

- **whois**: For querying WHOIS servers.
- **nslookup and dig**: For querying DNS servers.
- **DNSDumpster**: An online service for detailed DNS information.
- **Shodan.io**: A search engine for internet-connected devices.

These tools enable the collection of publicly available records, an essential aspect of passive reconnaissance.

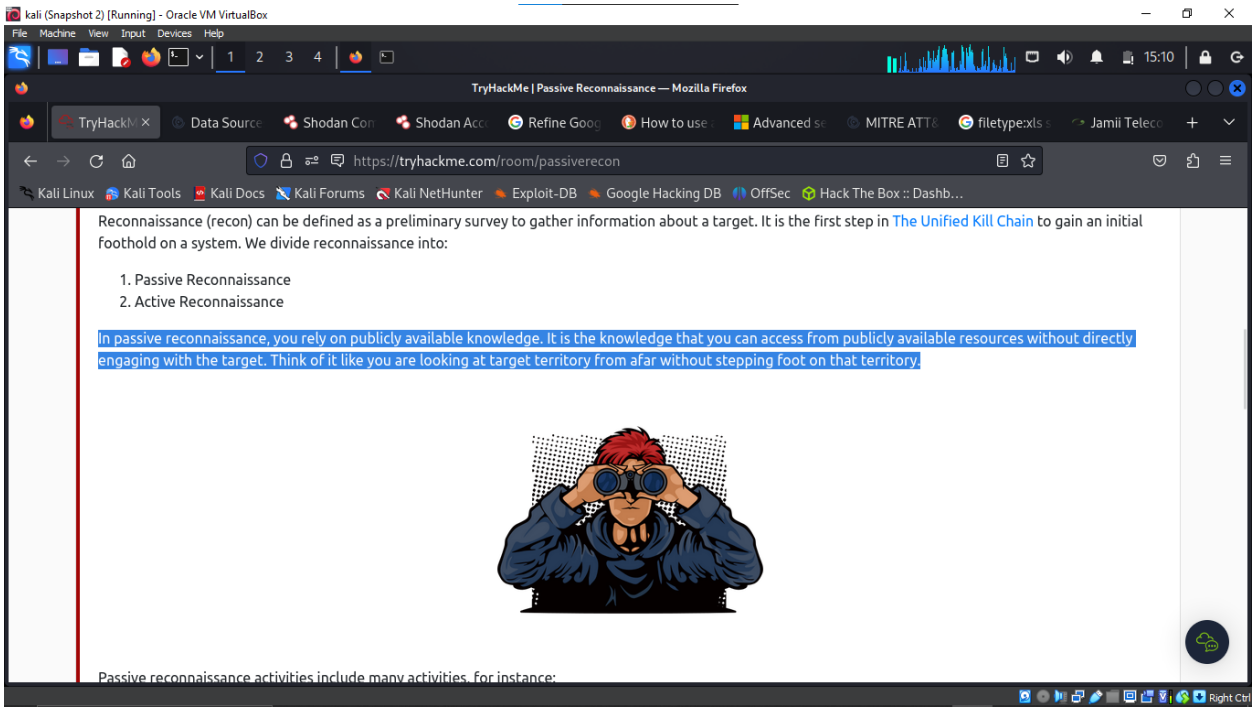
Task 2: Passive Versus Active Recon

Understanding the distinction between passive and active reconnaissance is crucial:

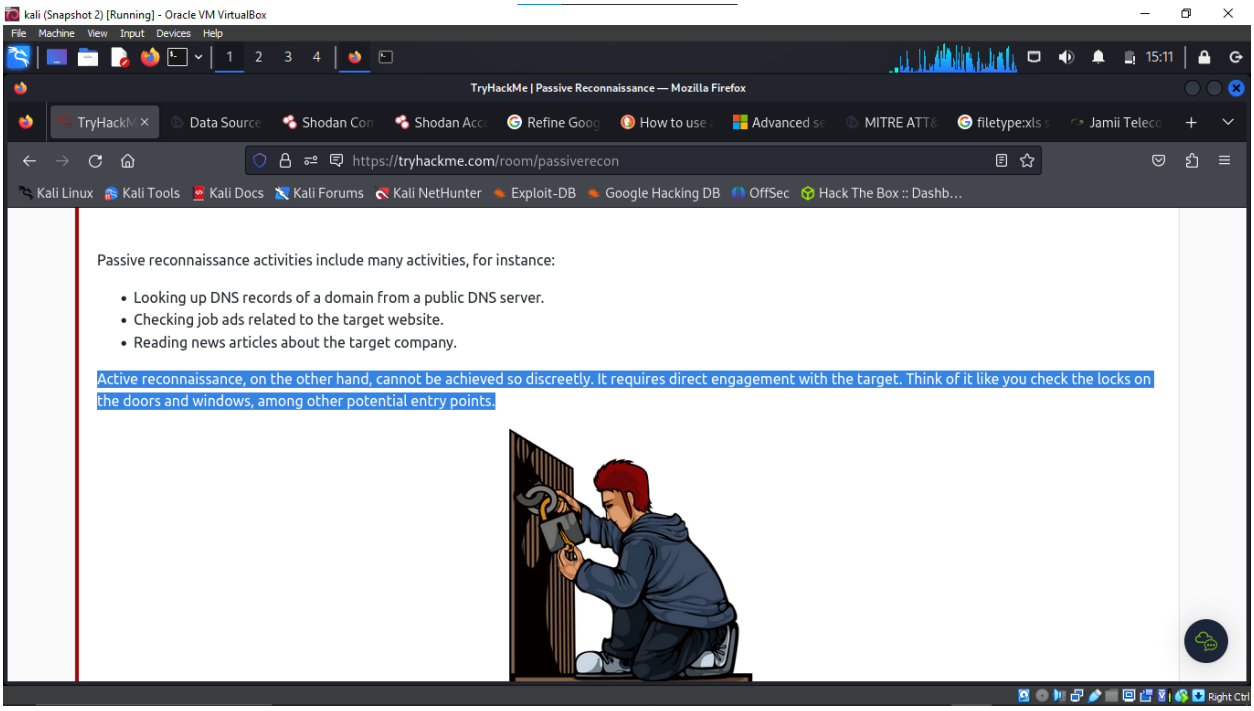
- **Passive Reconnaissance:** Involves gathering publicly available information without direct interaction with the target. Examples include looking up DNS records, checking job ads, and reading news articles.
- **Active Reconnaissance:** Requires direct engagement with the target, like connecting to company servers or employing social engineering techniques.

Questions and Answers

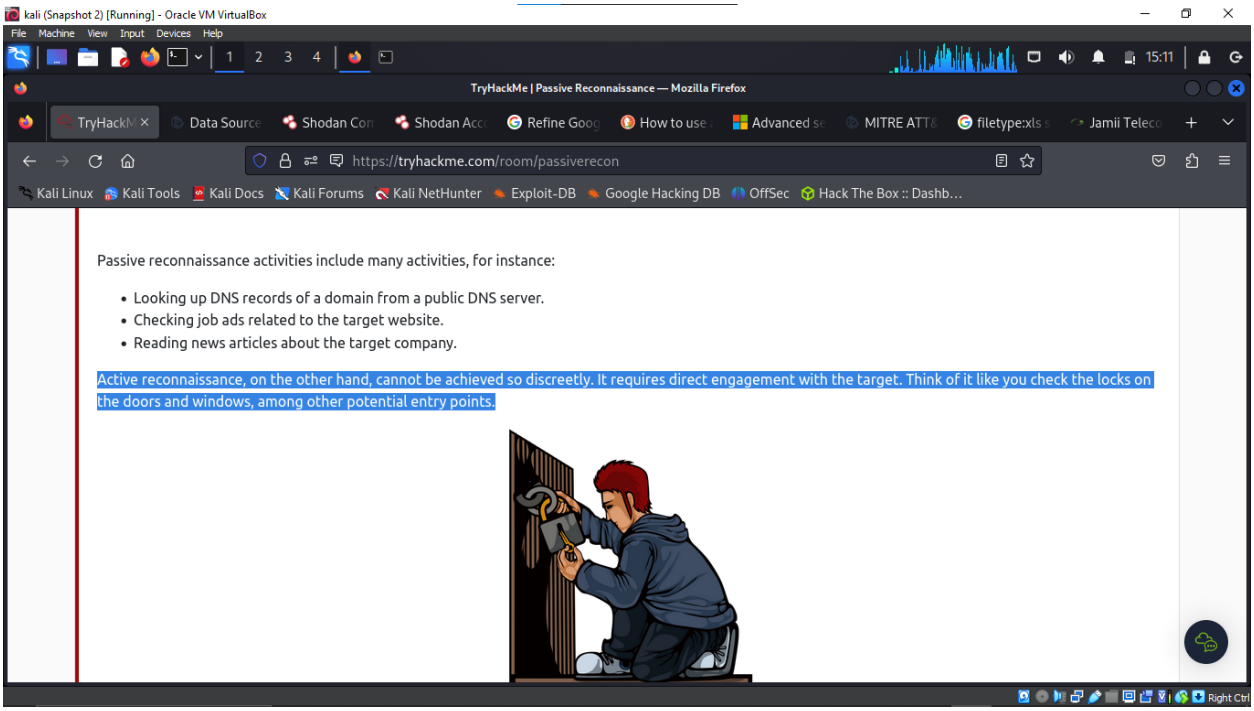
- Visiting a company's Facebook page for employee names is what type of reconnaissance?
    - **Answer:** P (Passive)



- Pinging a company's web server IP to check for ICMP traffic blockage is what type of reconnaissance?
    - **Answer:** A (Active)



- Using social engineering to get information from a company's IT administrator at a party is what type of reconnaissance?
    - **Answer:** A (Active)



Task 3: Whois

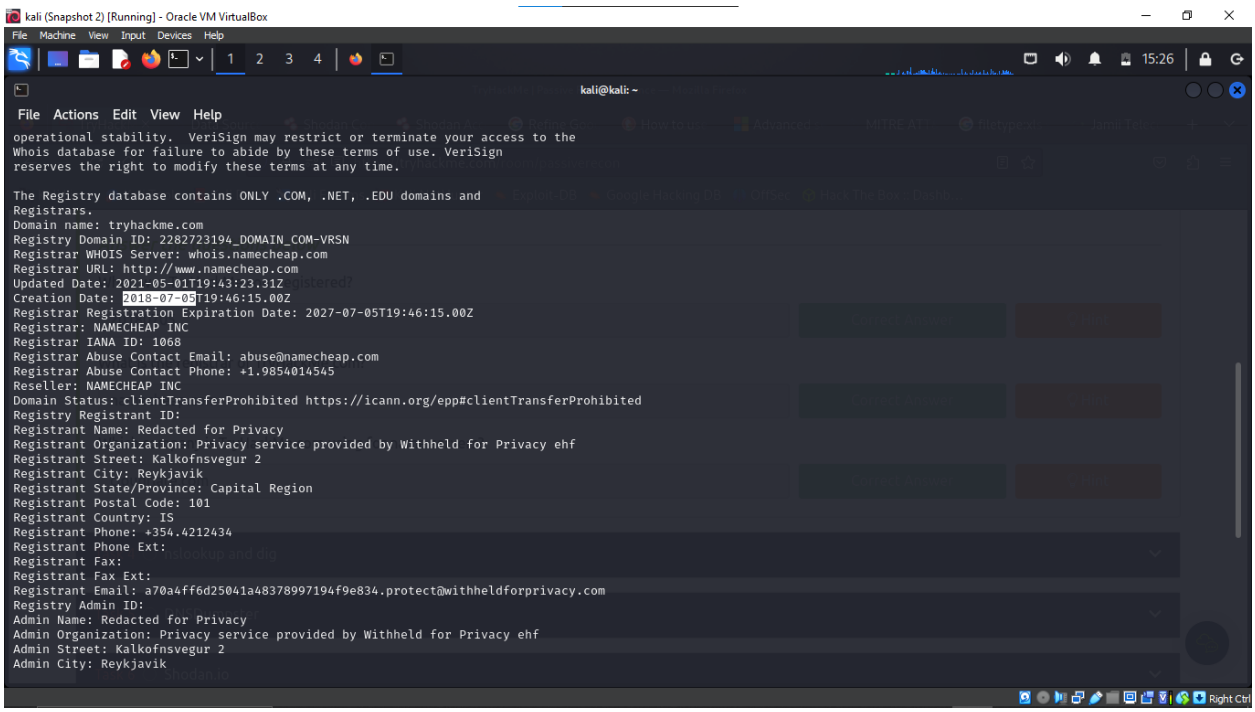
The WHOIS protocol provides detailed information about domain names, including:

- Registrar information.
- Registrant contact info (unless protected).
- Domain creation, update, and expiration dates.
- Name servers for the domain.

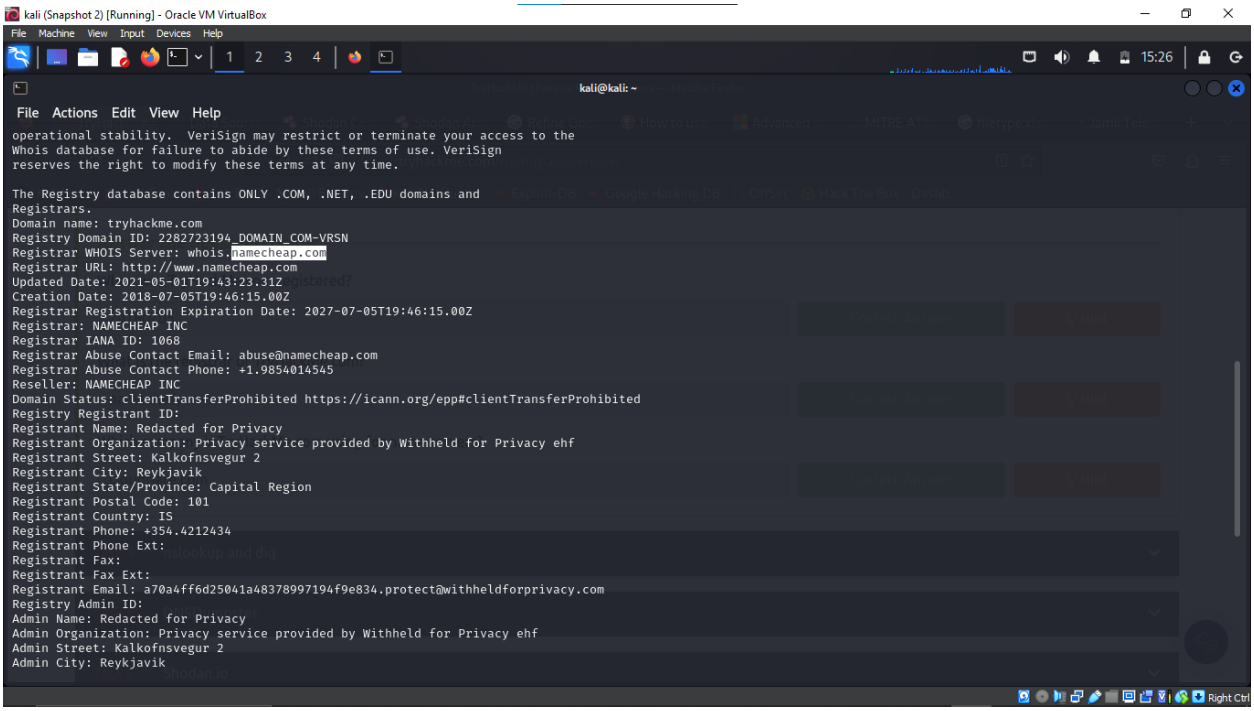
This information is crucial in understanding the target's domain infrastructure and potential vulnerabilities.

Questions and Answers

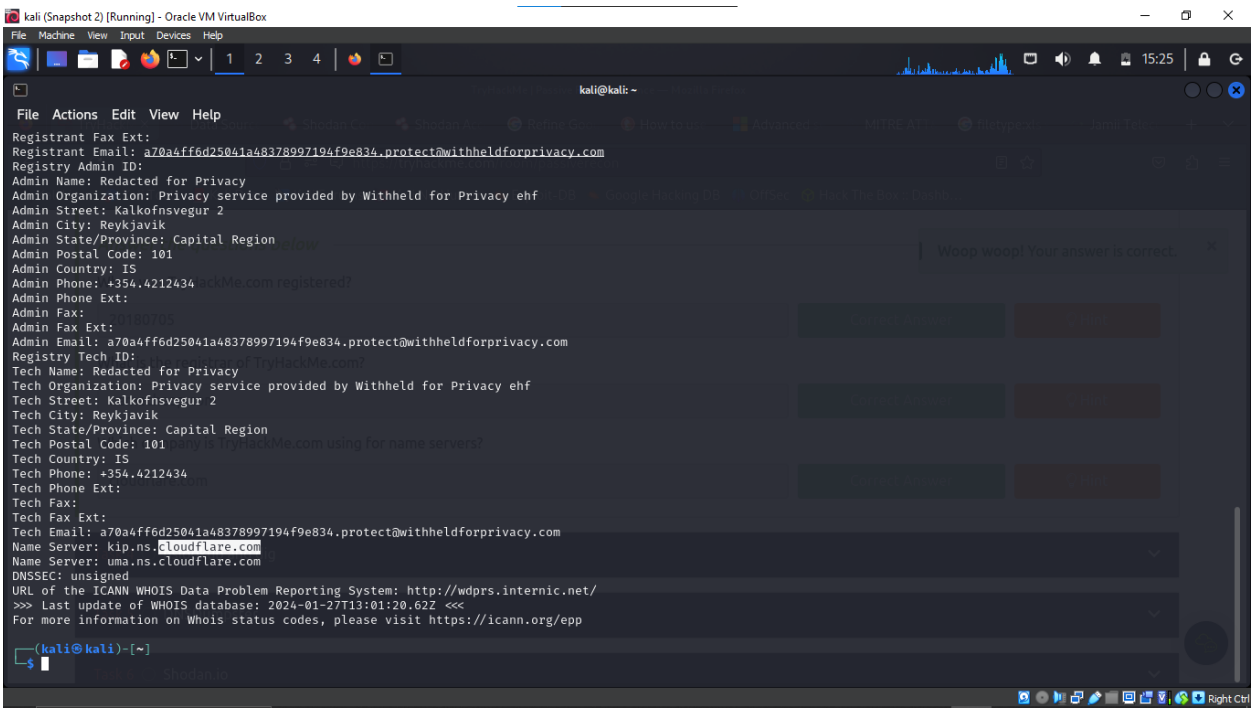
- When was TryHackMe.com registered?
  - **Answer:** 20180705



- What is the registrar of TryHackMe.com?
  - **Answer:** namecheap.com



- Which company provides name servers for TryHackMe.com?
  - **Answer:** cloudflare.com



Task 4: nslookup and dig

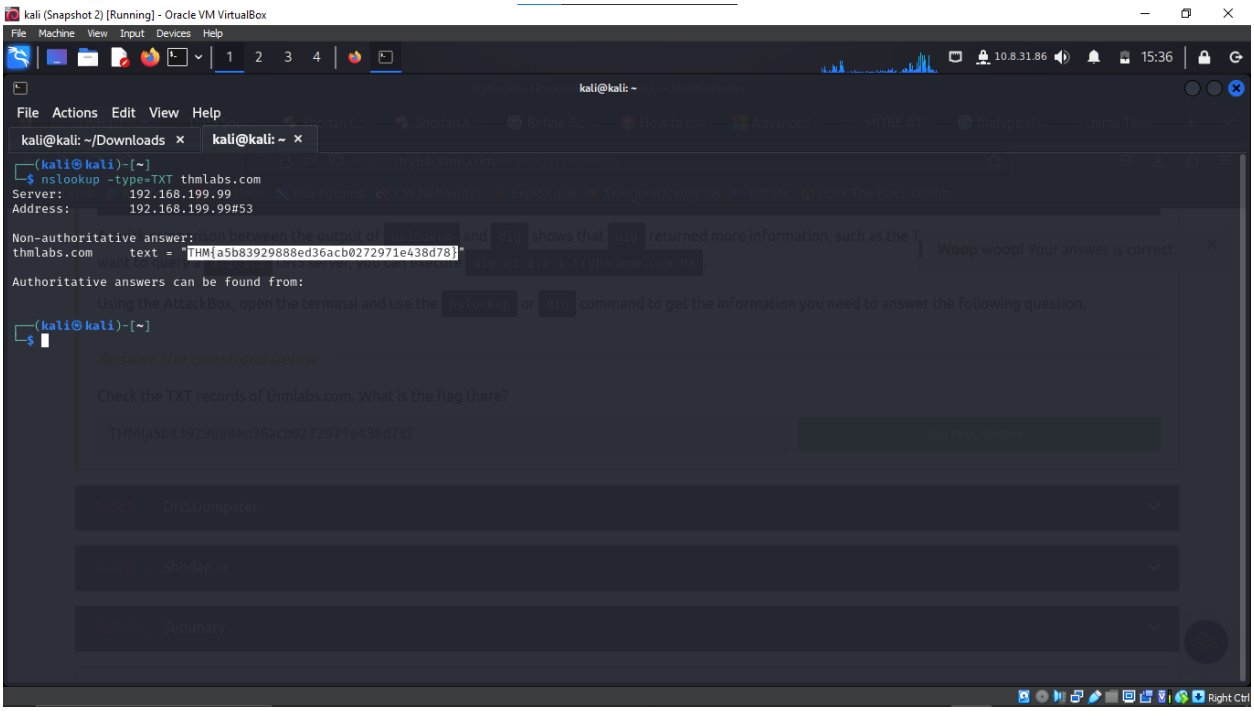
nslookup and dig are tools used to query DNS records, providing essential information such as:

- IP addresses (IPv4 and IPv6).
- Canonical names.
- Mail servers (MX records).
- Start of Authority (SOA).
- TXT records.

These tools are indispensable for uncovering information about the domain's infrastructure.

Question and Answer

- What is the flag in the TXT records of thmlabs.com?
  - **Answer:** THM{a5b83929888ed36acb0272971e438d78}

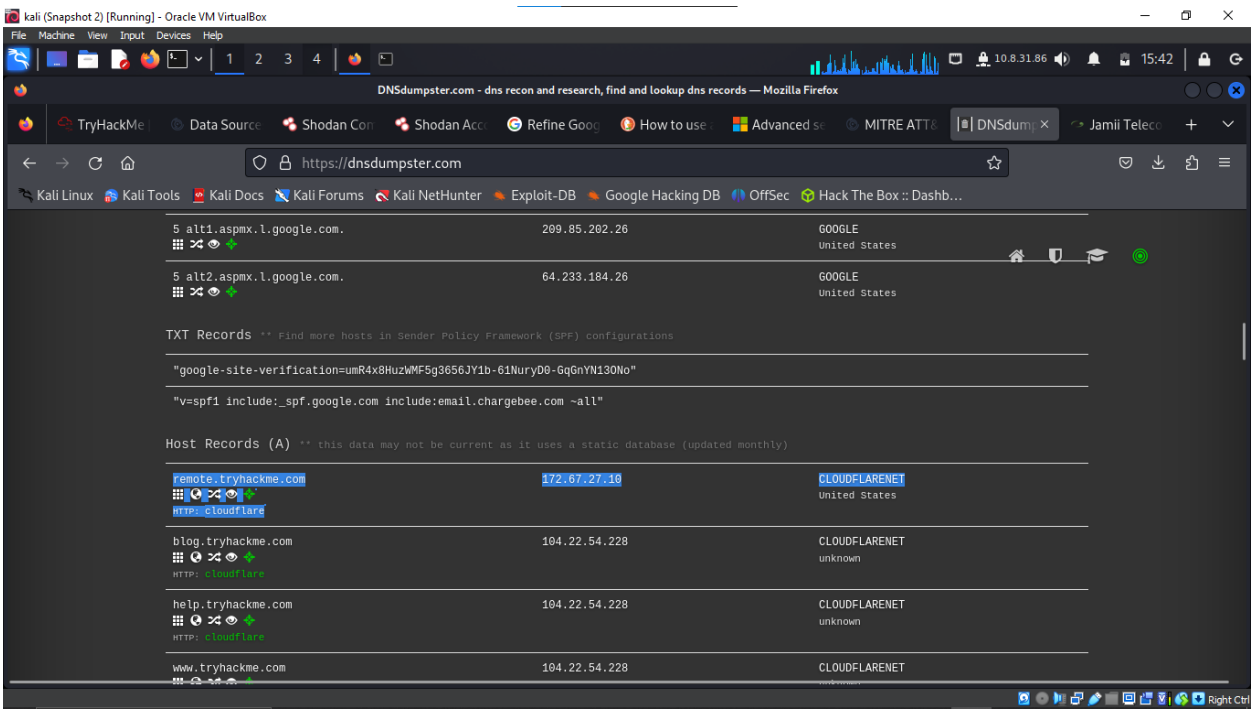


Task 5: DNSDumpster

DNSDumpster is an online service that reveals comprehensive DNS information, including subdomains that are not easily discoverable through standard DNS queries. It presents data in easy-to-read formats and graphical representations, making it a valuable tool for uncovering hidden aspects of a domain.

Question and Answer

- What is an interesting subdomain of tryhackme.com found on DNSDumpster besides www and blog?
    - **Answer:** remote



Task 6: Shodan.io

Shodan.io is a search engine for internet-connected devices, providing information such as:

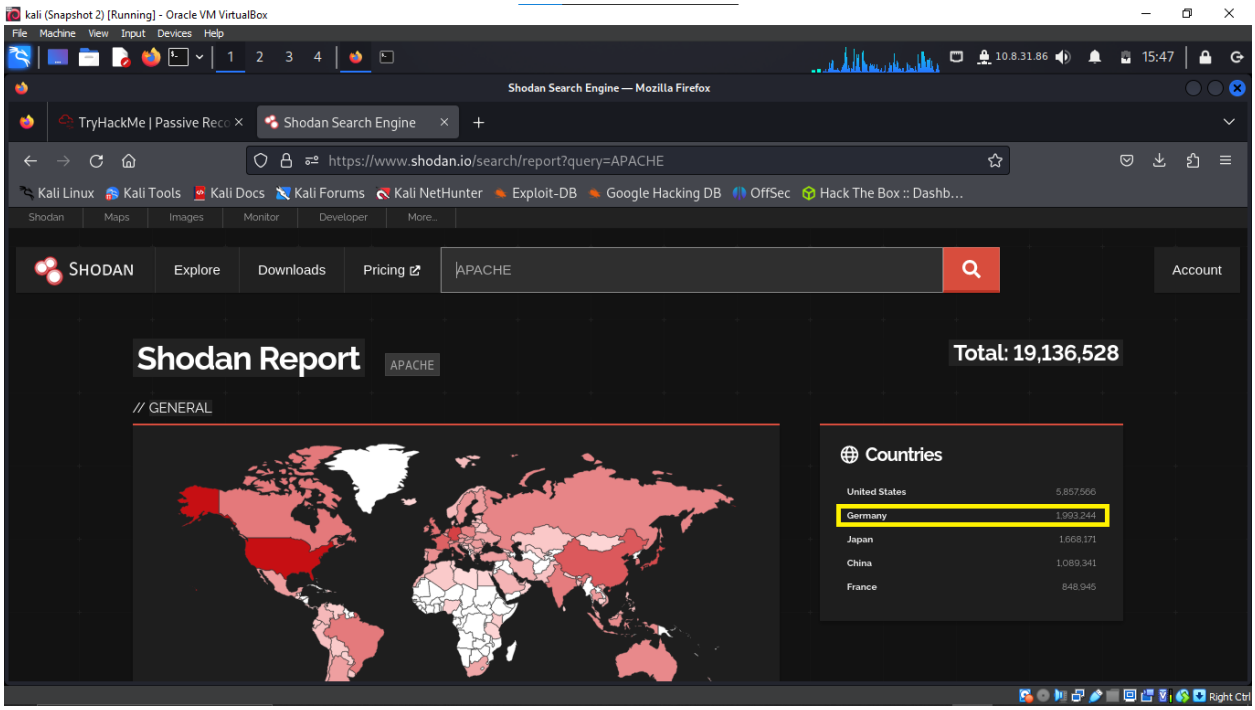
- IP addresses.
- Hosting companies.

- Geographic locations.
- Server types and versions.

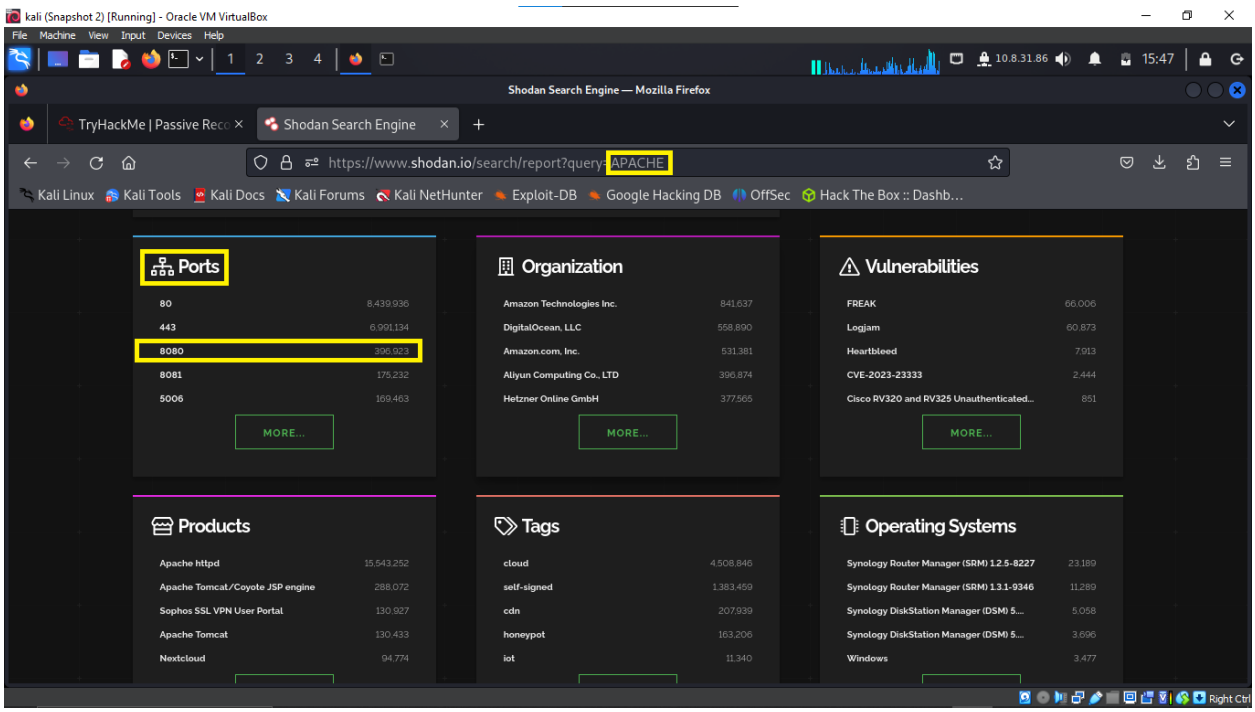
This tool is beneficial for both offensive and defensive cybersecurity strategies.

Questions and Answers

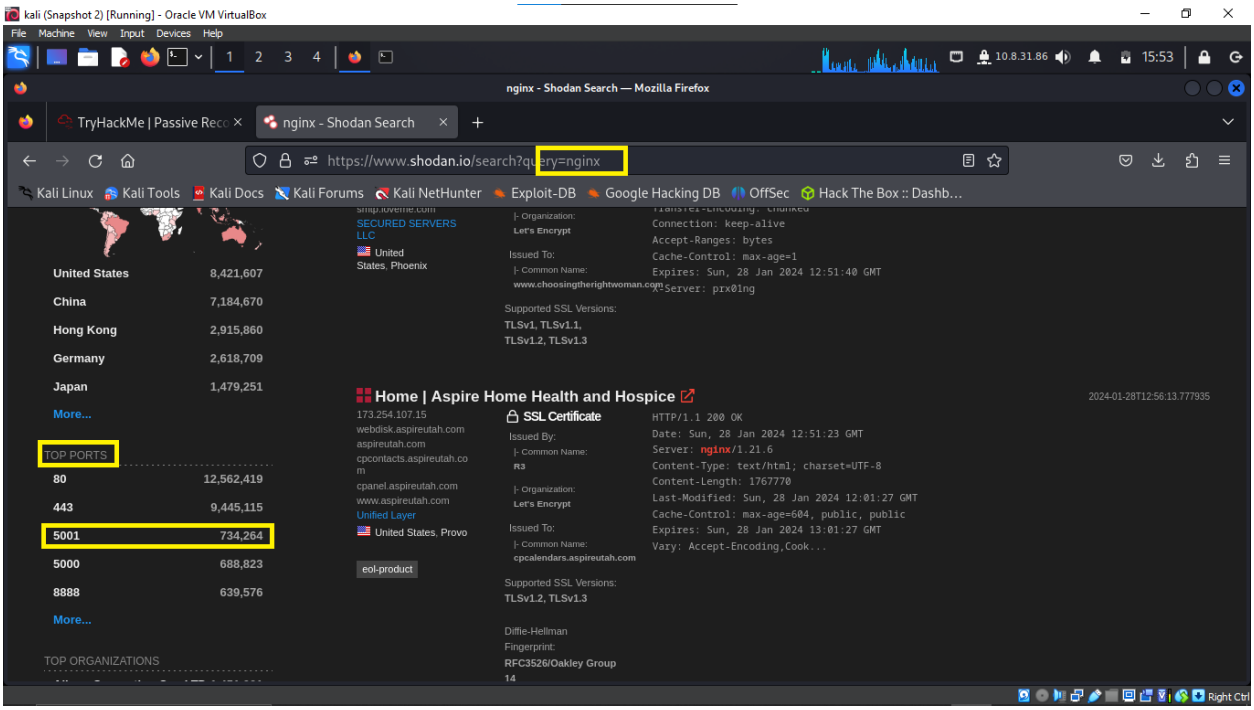
- According to Shodan.io, which country has the second-highest number of publicly accessible Apache servers?
    - **Answer:** Germany



- Based on Shodan.io, what is the third most common port used for Apache?
    - **Answer:** 8080



- According to Shodan.io, what is the third most common port used for nginx?
    - **Answer:** 5001



Task 7: Summary

Passive reconnaissance plays a vital role in cybersecurity. It allows gathering a wealth of information without direct engagement with the target. The tools discussed, including whois, nslookup, dig, DNSDumpster, and Shodan.io, are essential in collecting this information efficiently and discreetly.

Conclusion

Passive reconnaissance is an indispensable phase in cybersecurity operations. The ability to gather detailed information about a target discreetly lays the groundwork for effective cyber strategies, whether for defensive purposes or in preparation for a more active engagement.