



PASSIVE RECONNAISSANCE REPORT

Tryhackme.com



JUNE 6, 2023

YUNIS MOHAMED

Contents

| | |
|---|----------|
| Table of Figures..... | 1 |
| Introduction..... | 2 |
| Passive and Active Reconnaissance..... | 2 |
| Whois Tool..... | 3 |
| DNSDumpster | 3 |
| Nslookup and Dig..... | 4 |
| Shodan.io..... | 5 |
| Module Completion Badge..... | 6 |
| Conclusion..... | 7 |

Table of Figures

| | |
|--|----------|
| FIGURE 1 PASSIVE AND ACTIVE RECONNAISSANCE. QUIZ..... | 2 |
| FIGURE 2 WHOIS TOOL. QUIZ | 3 |
| FIGURE 3 DNSDUMPSTER. QUIZ | 4 |
| FIGURE 4 NSLOOKUP. QUIZ..... | 5 |
| FIGURE 5 SHODAN.IO. QUIZ A..... | 5 |
| FIGURE 6 SHODAN.IO. QUIZ B | 6 |
| FIGURE 7 MODULE BADGE | 6 |

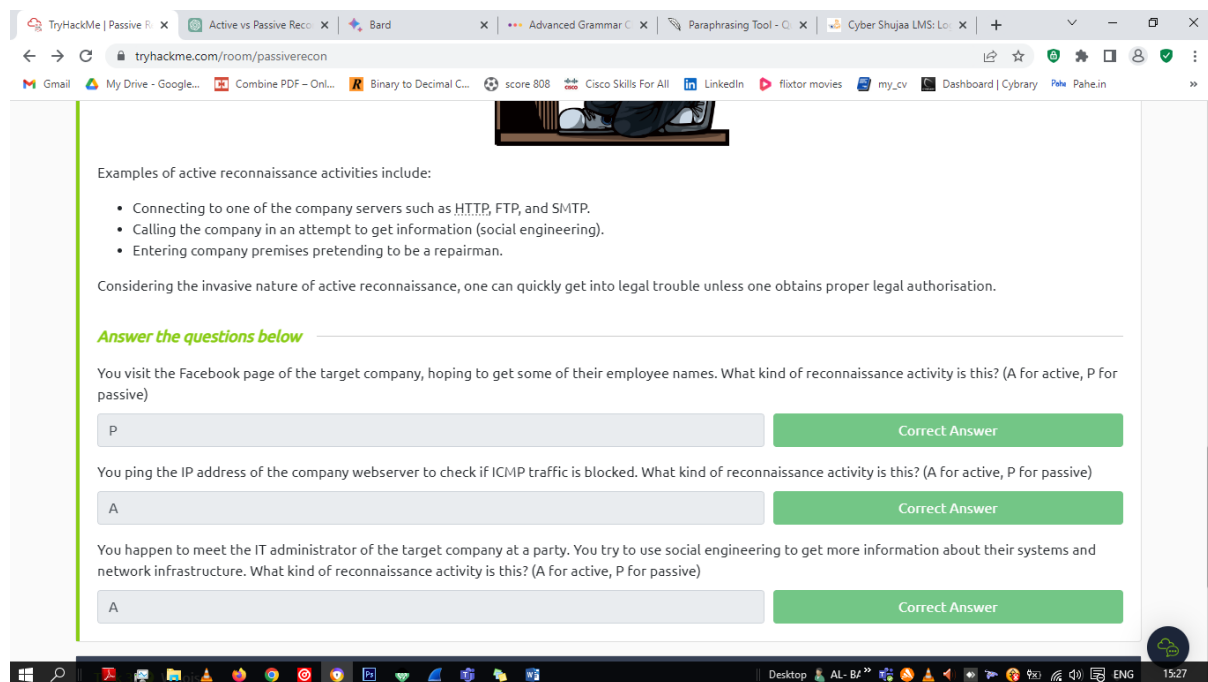
Introduction

In this module from tryhackme.com I was able to get an introduction to passive and active reconnaissance, processes involved when performing them and various tools used to perform the active and passive reconnaissance. Tools discussed include; whois tool, dnsdumpster, nslookup and dig and shodan.io.

Passive and Active Reconnaissance

Passive reconnaissance refers to the collection of information without directly engaging with the target system or network. It involves analysing publicly available data, such as website information, social media profiles, and DNS records, to gather intelligence about potential vulnerabilities and weaknesses. **Active reconnaissance**, on the other hand, involves actively probing and scanning the target system or network to identify open ports, services, and potential entry points. It typically includes techniques like port scanning, vulnerability scanning, and network mapping. Both passive and active reconnaissance play crucial roles in the preliminary stages of a security assessment or hacking attempt, allowing attackers or security professionals to gather valuable information and assess the target's security posture.

Below is the topic quiz:



The screenshot shows a web browser window with the URL tryhackme.com/room/passiverecon. The page content includes:

Examples of active reconnaissance activities include:

- Connecting to one of the company servers such as HTTP, FTP, and SMTP.
- Calling the company in an attempt to get information (social engineering).
- Entering company premises pretending to be a repairman.

Considering the invasive nature of active reconnaissance, one can quickly get into legal trouble unless one obtains proper legal authorisation.

Answer the questions below

You visit the Facebook page of the target company, hoping to get some of their employee names. What kind of reconnaissance activity is this? (A for active, P for passive)

You ping the IP address of the company webserver to check if ICMP traffic is blocked. What kind of reconnaissance activity is this? (A for active, P for passive)

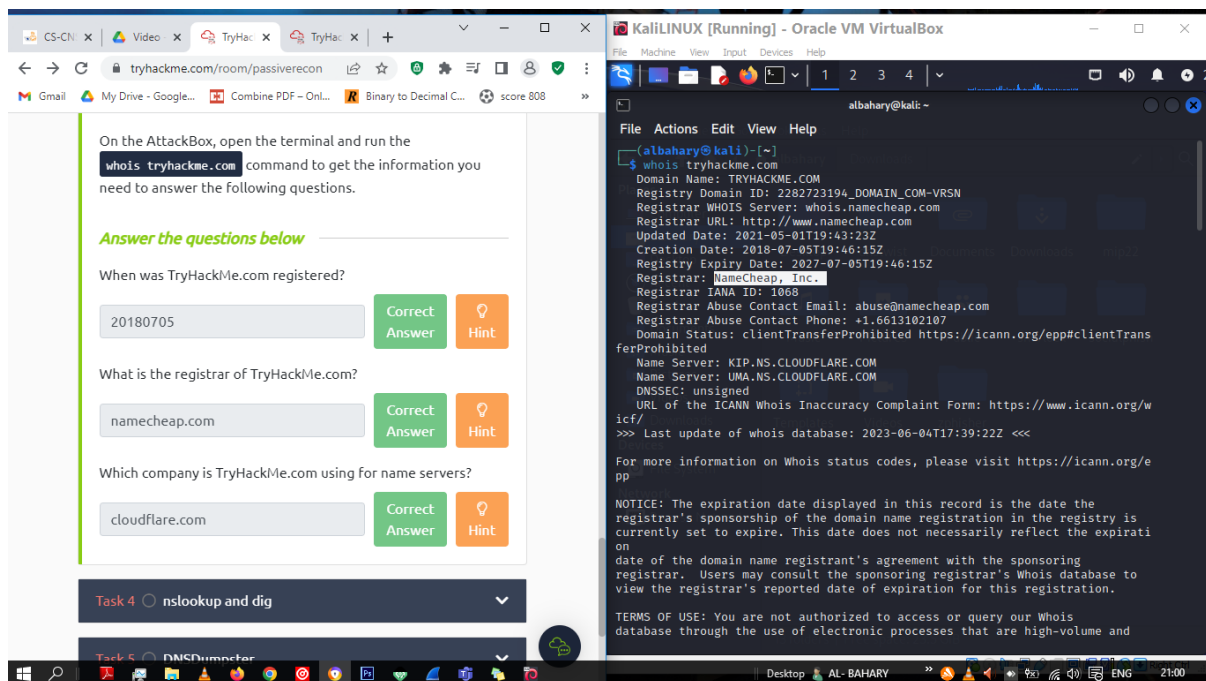
You happen to meet the IT administrator of the target company at a party. You try to use social engineering to get more information about their systems and network infrastructure. What kind of reconnaissance activity is this? (A for active, P for passive)

Figure 1 passive and active reconnaissance. quiz

Whois Tool

The WHOIS protocol, based on RFC 3912, is a request and response mechanism used to obtain domain information. Operating on TCP port 43, a WHOIS server is responsible for maintaining records for leased domain names. When queried, the server provides details such as the registrar responsible for the domain, contact information of the registrant (unless privacy services are utilized), dates of creation, updates, and expiration, and the name server for resolving the domain. Accessing this information requires a **whois** client or online service, with local clients being faster and more convenient. Example can be **whois google.com**.

Below is the topic quiz:



The image shows a quiz interface on the left and a terminal window on the right. The quiz is titled "On the AttackBox, open the terminal and run the `whois tryhackme.com` command to get the information you need to answer the following questions." It asks three questions: "When was TryHackMe.com registered?", "What is the registrar of TryHackMe.com?", and "Which company is TryHackMe.com using for name servers?". The answers are 20180705, namecheap.com, and cloudflare.com respectively. The terminal window shows the output of the `whois tryhackme.com` command, displaying domain information such as Domain Name, Registry Domain ID, Registrar, and Name Servers.

On the AttackBox, open the terminal and run the `whois tryhackme.com` command to get the information you need to answer the following questions.

Answer the questions below

When was TryHackMe.com registered?

20180705 Correct Answer Hint

What is the registrar of TryHackMe.com?

namecheap.com Correct Answer Hint

Which company is TryHackMe.com using for name servers?

cloudflare.com Correct Answer Hint

Task 4 nslookup and dig

Task 5 DNSDumpster

KaliLinux [Running] - Oracle VM VirtualBox

```
albahary@kali:~$ whois tryhackme.com
Domain Name: TRYHACKME.COM
Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-05-01T19:43:22Z
Creation Date: 2018-07-05T19:46:15Z
Registry Expiry Date: 2027-07-05T19:46:15Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: KIP.NS.CLOUDFLARE.COM
Name Server: UMA.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/whois-inaccuracy-complaint-form
>>> Last update of whois database: 2023-06-04T17:39:22Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and
```

Figure 2 whois tool. Quiz

DNSDumpster

DNSDumpster is a web-based tool that provides domain-related information and DNS reconnaissance. It allows users to gather details about a domain, such as DNS records, subdomains, IP addresses, and associated email servers. By utilizing DNSDumpster, users can perform reconnaissance and intelligence gathering on a specific domain, helping to identify potential vulnerabilities or gather information for security assessments. The tool provides a user-friendly interface for exploring and visualizing DNS-related data, making it a valuable resource for network administrators, security professionals, and researchers.

Below is the topic quiz: website used is **dnsdumpster.com**

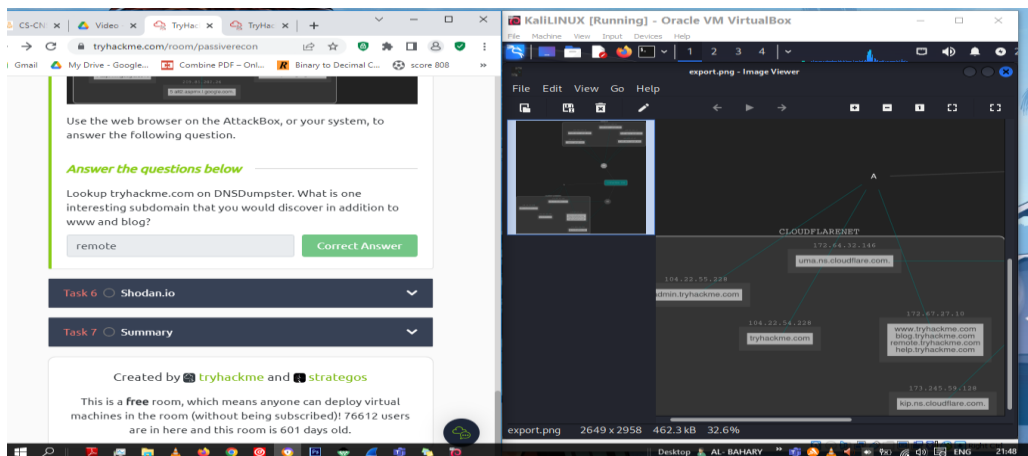


Figure 3 dnsdumpster. Quiz

Nslookup and Dig

DNS lookup and dig are both command-line tools used for querying DNS (Domain Name System) servers to retrieve information about domain names and IP addresses. DNS lookup, also known as nslookup, is a common utility that allows users to obtain DNS-related information, such as IP address resolution, mail server details, and DNS record types (such as A, MX, CNAME, etc.). It provides a straightforward way to directly query DNS servers and retrieve specific information related to a domain or IP address. On the other hand, dig (Domain Information Groper) is a more advanced DNS tool with additional features and flexibility. It supports more extensive querying options, provides detailed information about DNS responses, and can perform various types of DNS record lookups. Dig is widely used by network administrators, developers, and researchers to troubleshoot DNS issues, analyse DNS configurations, and gather detailed DNS data for a given domain. Below is the query type and its result.

A: Returns the IPv4 addresses associated with the domain.

AAAA: Provides the IPv6 addresses associated with the domain.

CNAME: Returns the canonical name or alias for the domain.

MX: Provides the mail servers responsible for handling email for the domain.

SOA: Returns the Start of Authority record, which contains important information about the domain's authoritative DNS server.

TXT: Provides any text records associated with the domain, which can include various types of information, such as SPF (Sender Policy Framework) records for email authentication or general descriptive text.

Example of the nslookup syntax: ***nslookup -type=A tryhackme.com 1.1.1.1***

Below is the topic quiz:

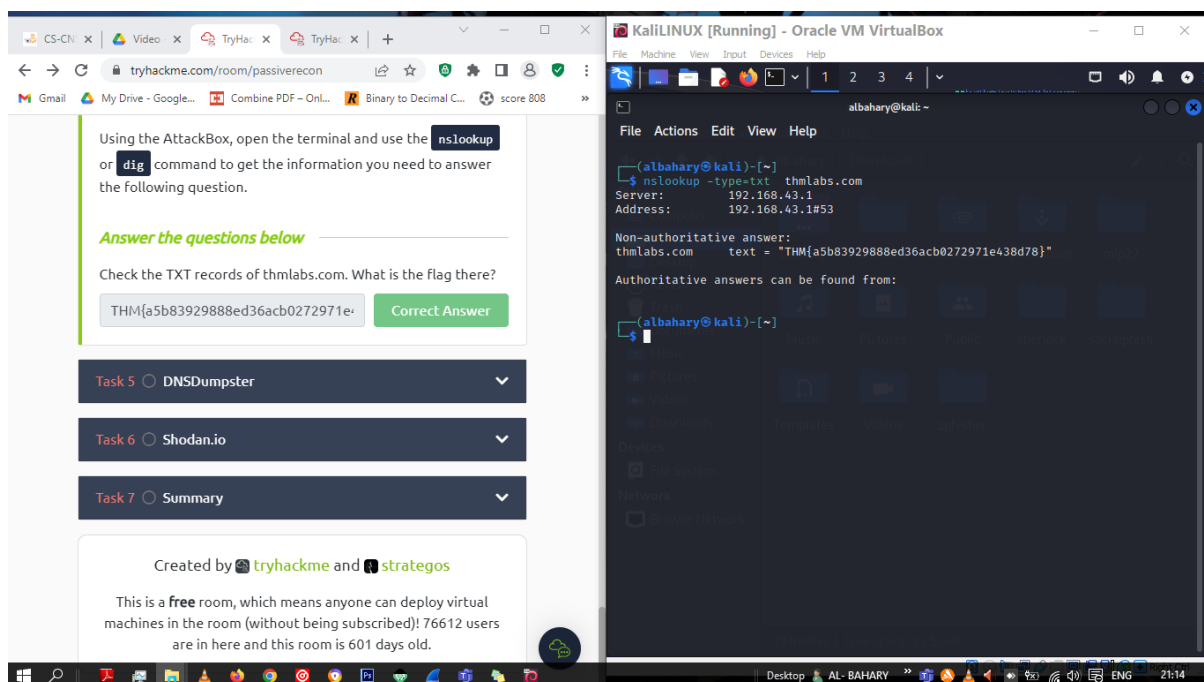


Figure 4 nslookup. Quiz

Shodan.io

Shodan.io is a search engine for internet-connected devices. It allows users to search for devices by their IP address, hostname, or operating system. Shodan.io also provides information about the devices, such as their open ports, services, and vulnerabilities. This tool is a specialized search engine that scans and indexes devices connected to the internet.

Below is the topic quiz: website used is **shodan.io**

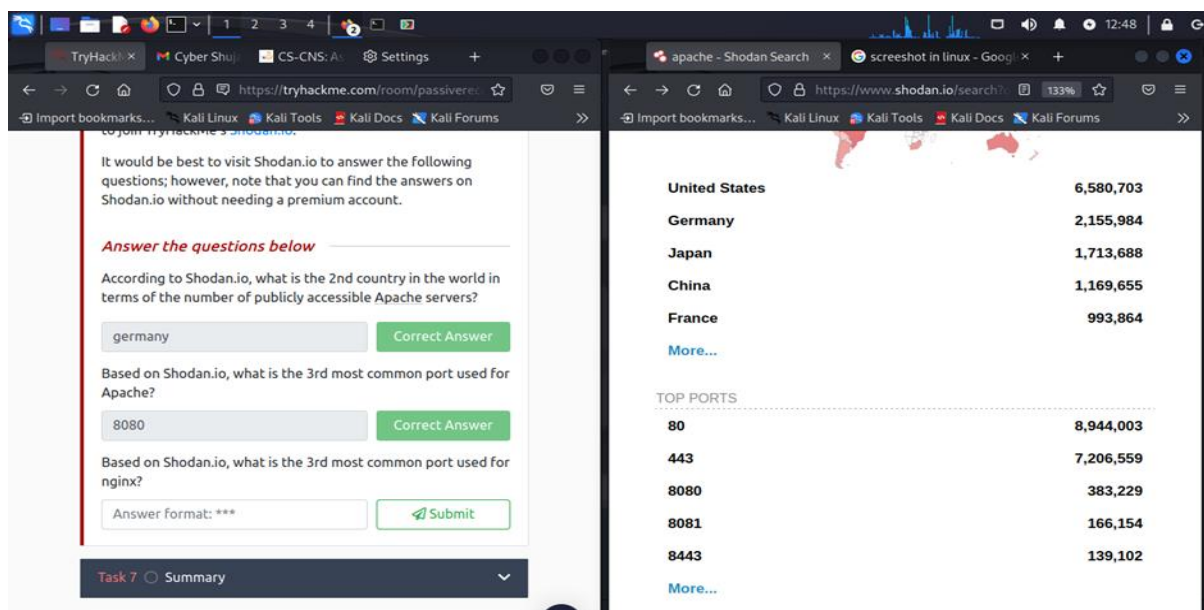


Figure 5 shodan.io. quiz a

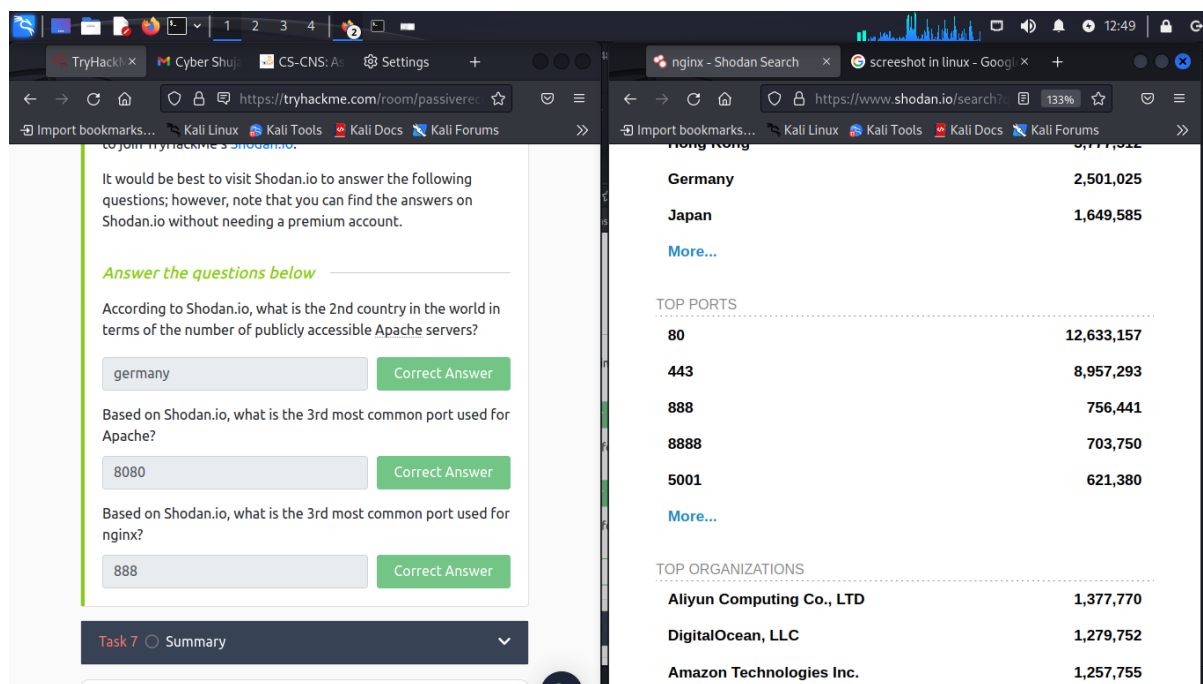


Figure 6 shodan.io.quiz b

Module Completion Badge

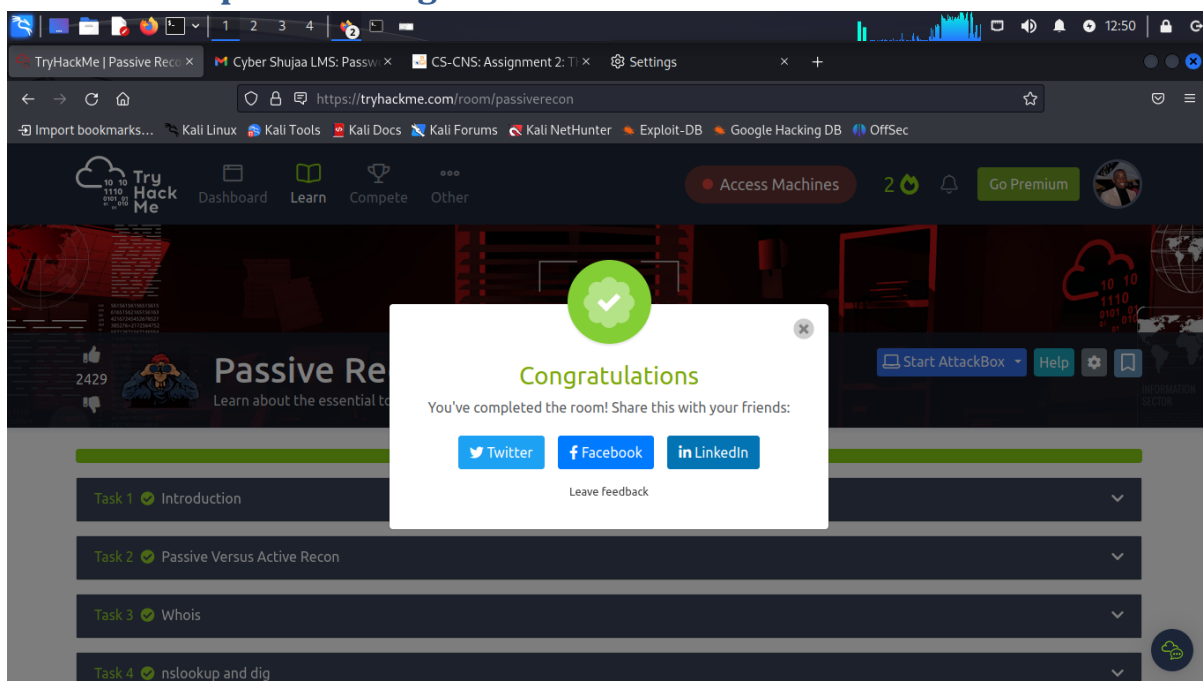


Figure 7 module badge

Conclusion

Passive and active reconnaissance are vital components of information gathering and vulnerability assessment in the field of cybersecurity. Passive reconnaissance involves collecting information without directly engaging with the target system, while active reconnaissance involves actively probing and scanning the target. Several tools play a significant role in these reconnaissance activities. The WHOIS tool provides domain-related information, including registrar details, contact information, and important dates. Shodan.io specializes in scanning and indexing internet-connected devices, providing insights into open ports and services. DNSDumpster enables the exploration of DNS records and subdomains, aiding in intelligence gathering. Nslookup and dig are command-line tools used for querying DNS servers to retrieve DNS-related information, offering flexibility and detailed analysis. By leveraging these tools effectively, security professionals can gain valuable insights, identify vulnerabilities, and enhance the overall security posture of their networks and systems. The module has introduced me to help tools such as whois tool, shodan.io which will assist me in performing reconnaissance in future. Overall the module is short, precise and easy to understand with practical activities to help practice the gained skills and knowledge.