**Passive Recon**

**Introduction**

The learner is going dive deep into Network Security and cover areas in: Passive reconnaissance, Active reconnaissance, Nmap Live Host Discovery, Nmap Basic Port Scans, Nmap Post Port Scans, Protocols and Servers, Protocols and Servers 2 and Network Security Challenge.

***Activities***

***Task 1: Introduction***

***Task 2: Passive Versus Active Recon***

Reconnaissance can be put into the following classifications:

1. **Passive Recon**: can be carried out by watching passively
2. **Active Recon**: requires interacting with the target to provoke it in order to observe its response.

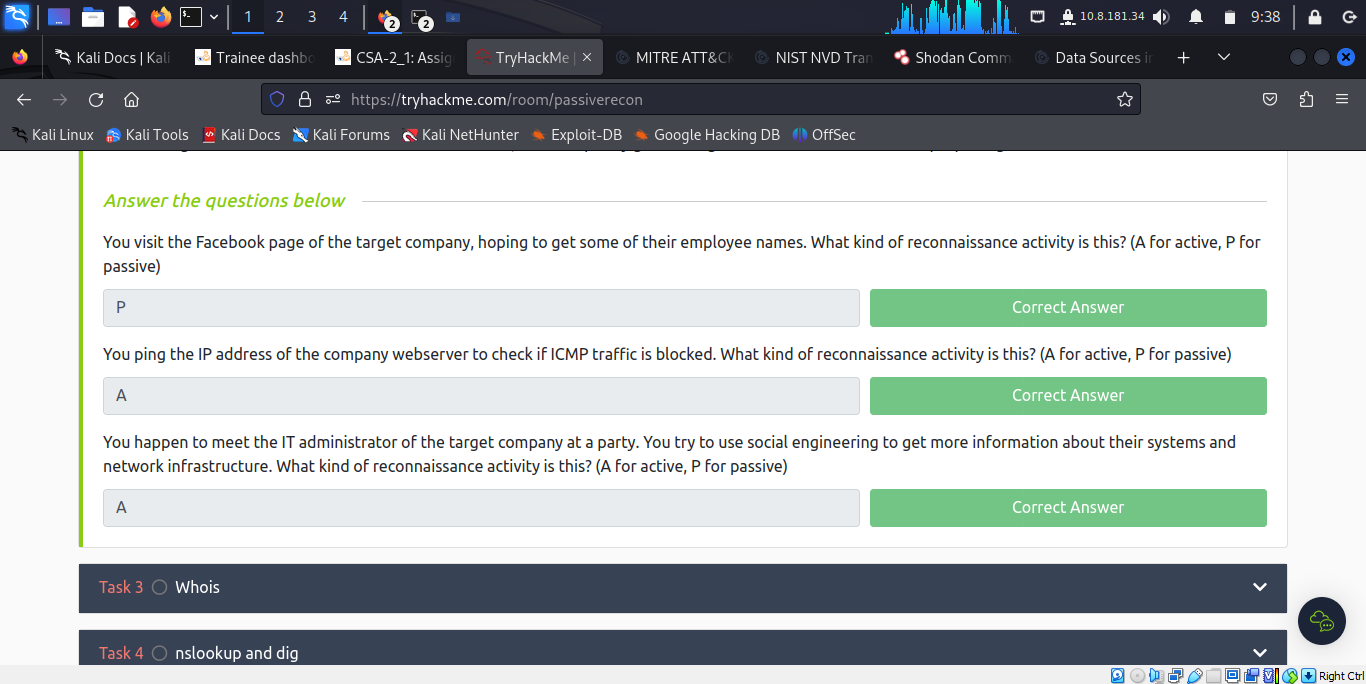
Passive recon doesn't require interacting with the target and relies on publicly available information that is collected and maintained by a third party.

Active recon requires interacting with the target by sending requests and packets and observing if and how it responds. An example of active reconnaissance is using Nmap to scan target subnets and live hosts.

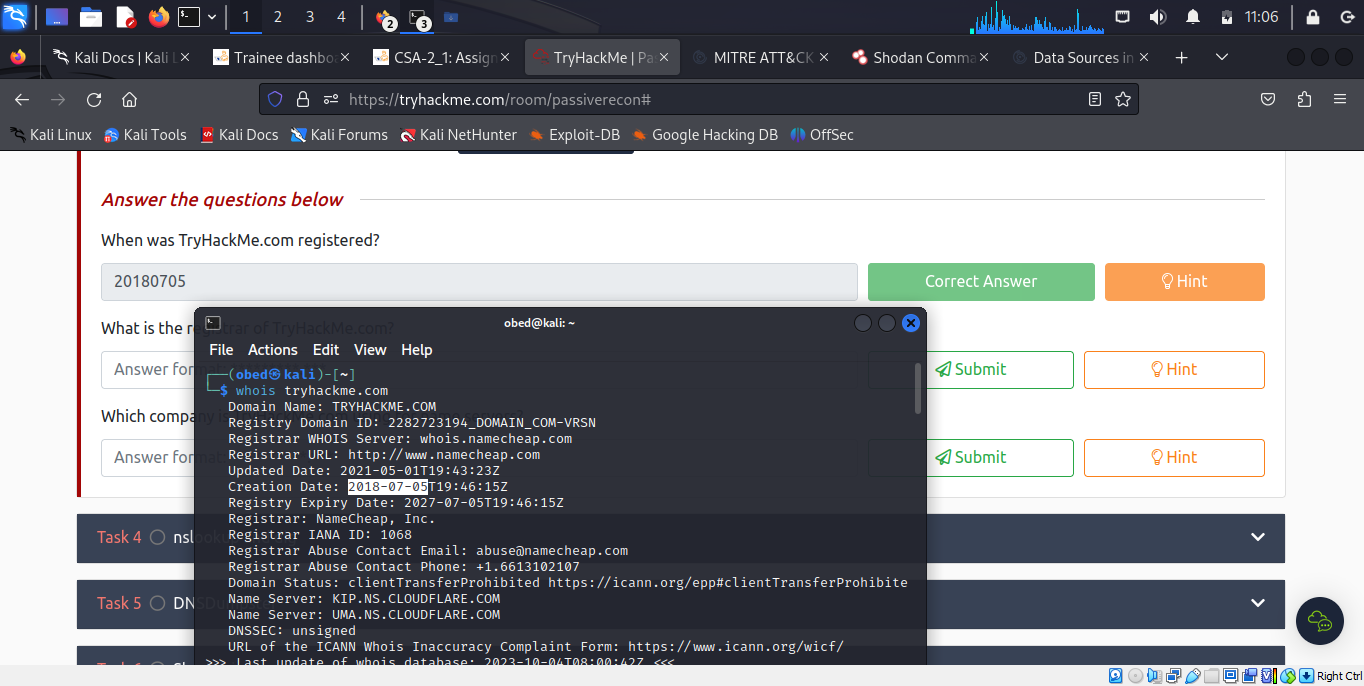
Active recon can be classified as:

External Recon: Conducted outside the target's network and focuses on the externally facing assets assessable from the Internet. One example is running Nikto from outside the company network.

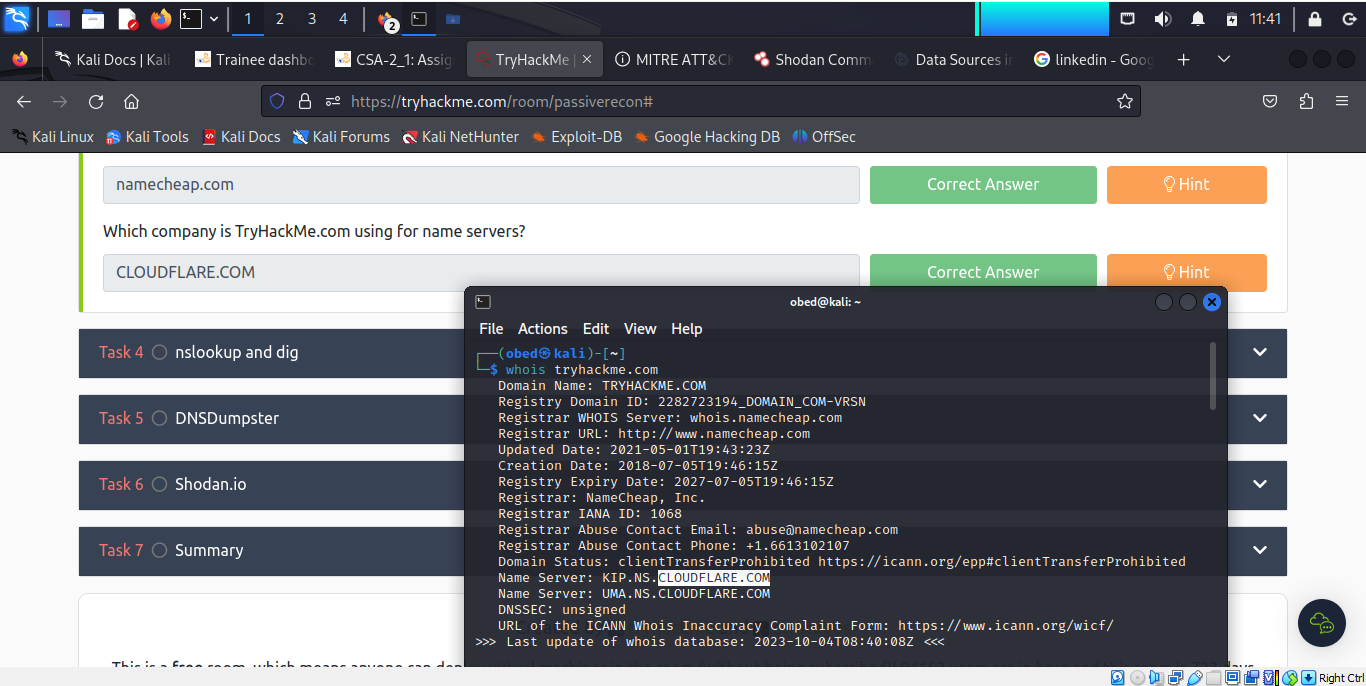
Internal Recon: Conducted from within the target company's network. In other words, the pentester or red teamer might be physically located inside the company building. In this scenario, they might be using an exploited host on the target's network. An example would be using Nessus to scan the internal network using one of the target’s computers.



***Task 3: Whois***



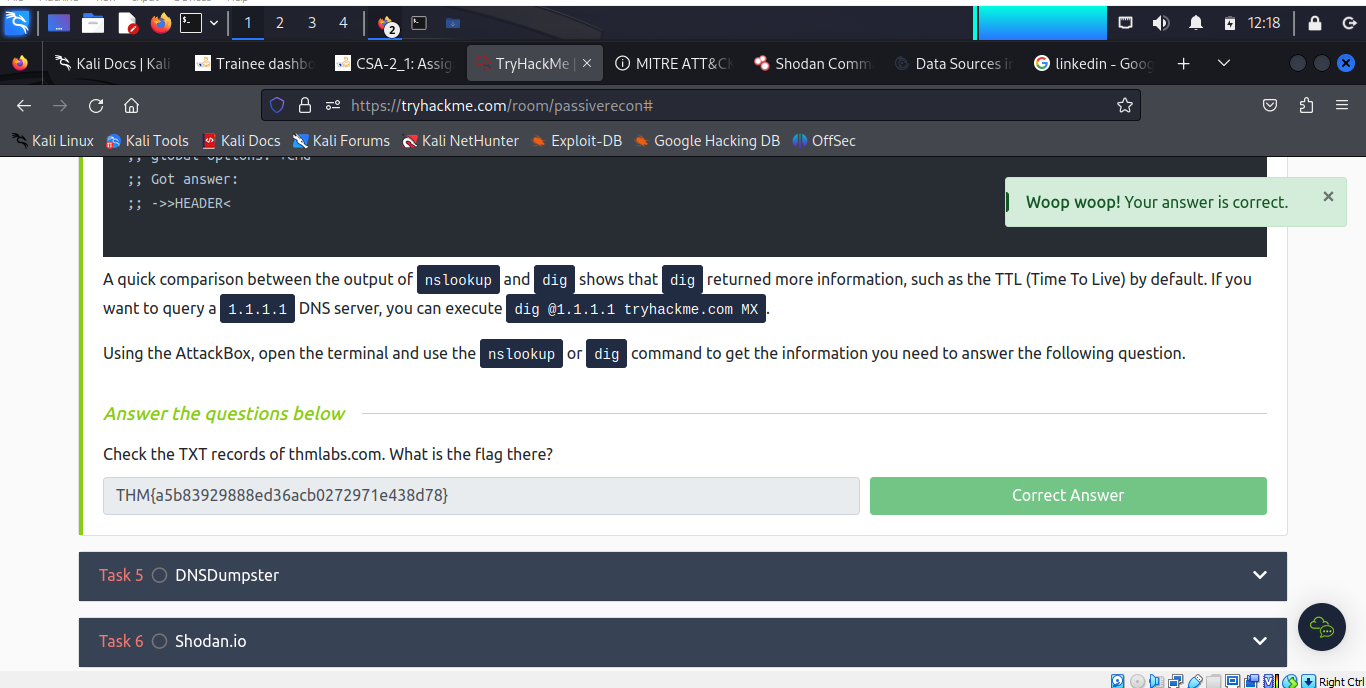
The company that TryHackMe.com is using for name servers is **cloudfare.com**

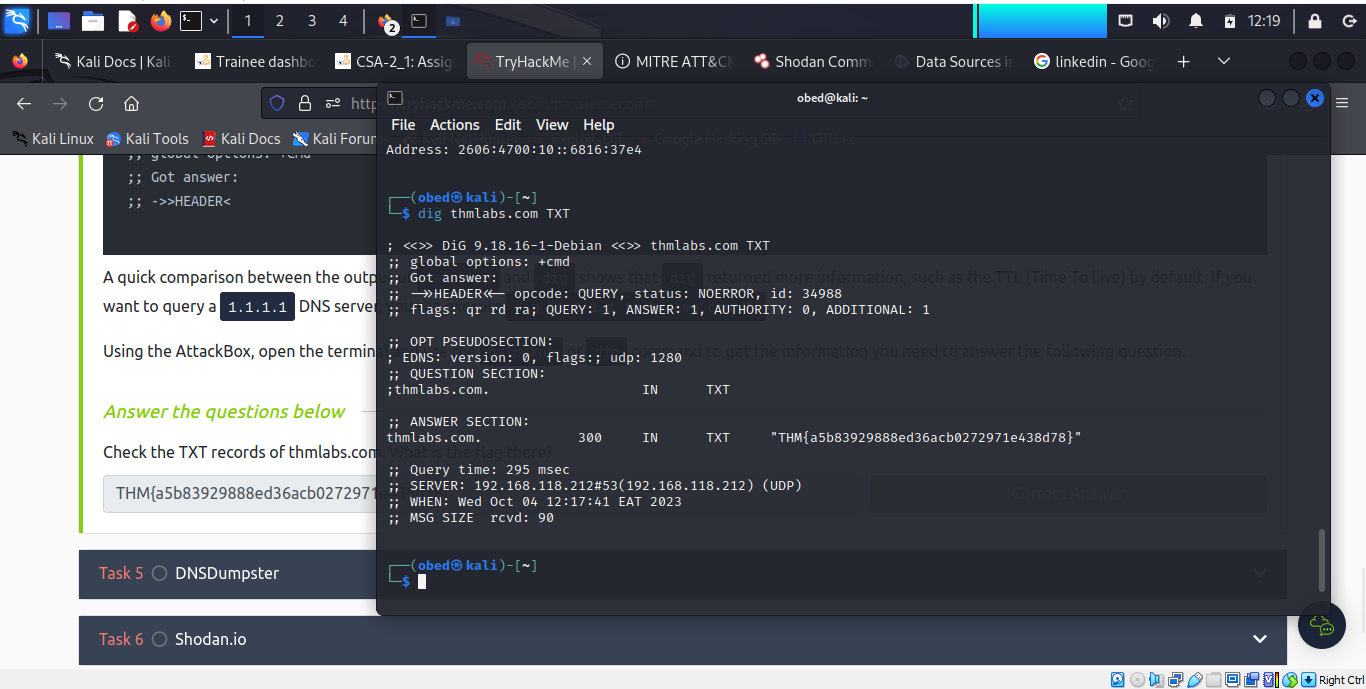


***Task 4: nslookup and dig***

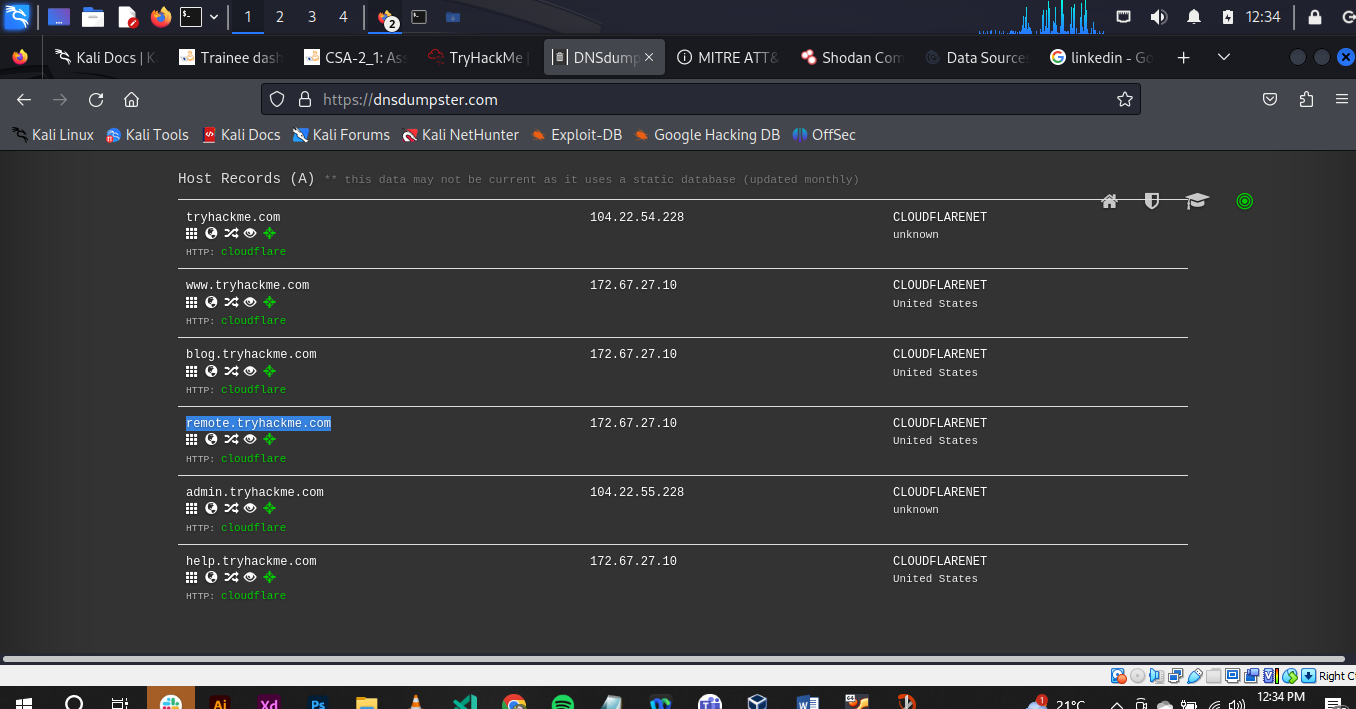
The learner being familiar with **whois** command, now they use in this task – **nslookup (Name Server Look Up).** The command syntax is  **nslookup DOMAIN\_NAME SERVER. Server** refers to the DNS server that is to be queried.

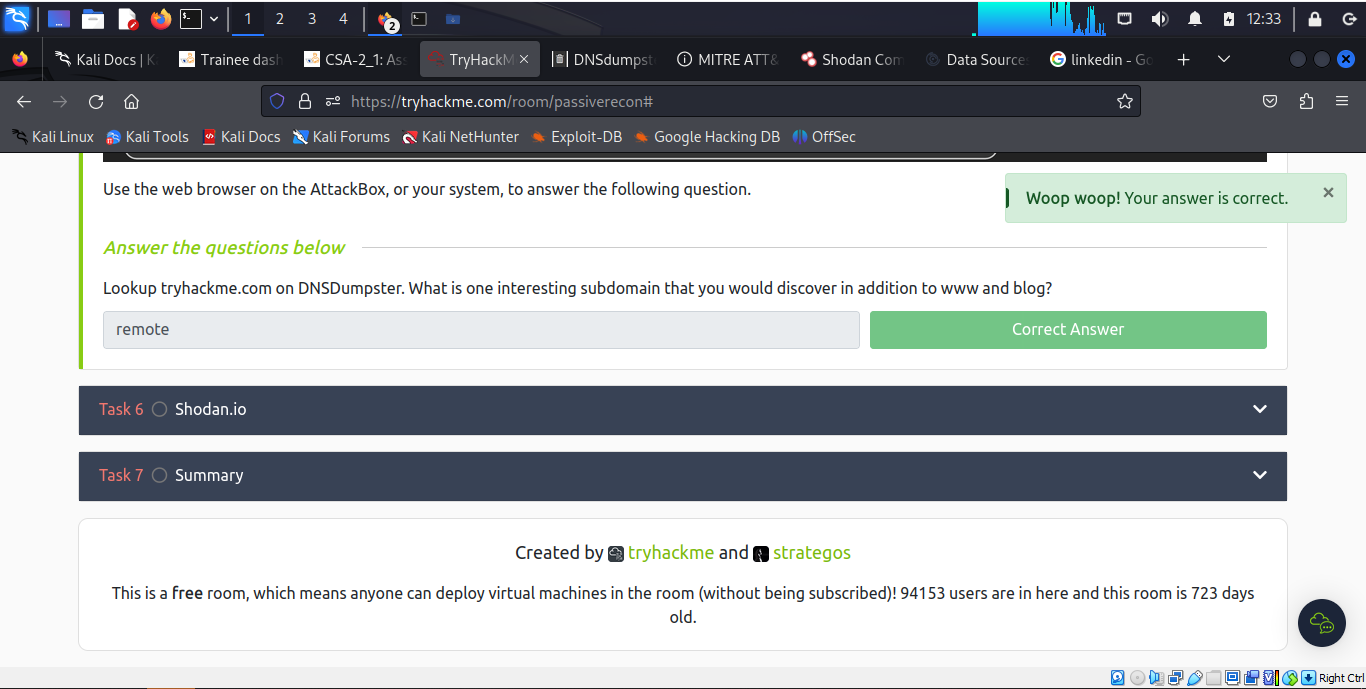
**Domain Information Groper (dig)** – is an advanced DNS query with additional functionality. The syntax is **dig DOMAIN\_NAME TYPE.** To select the server needed to be queried the syntax is **dig @SERVER DOMAIN\_NAME TYPE.**





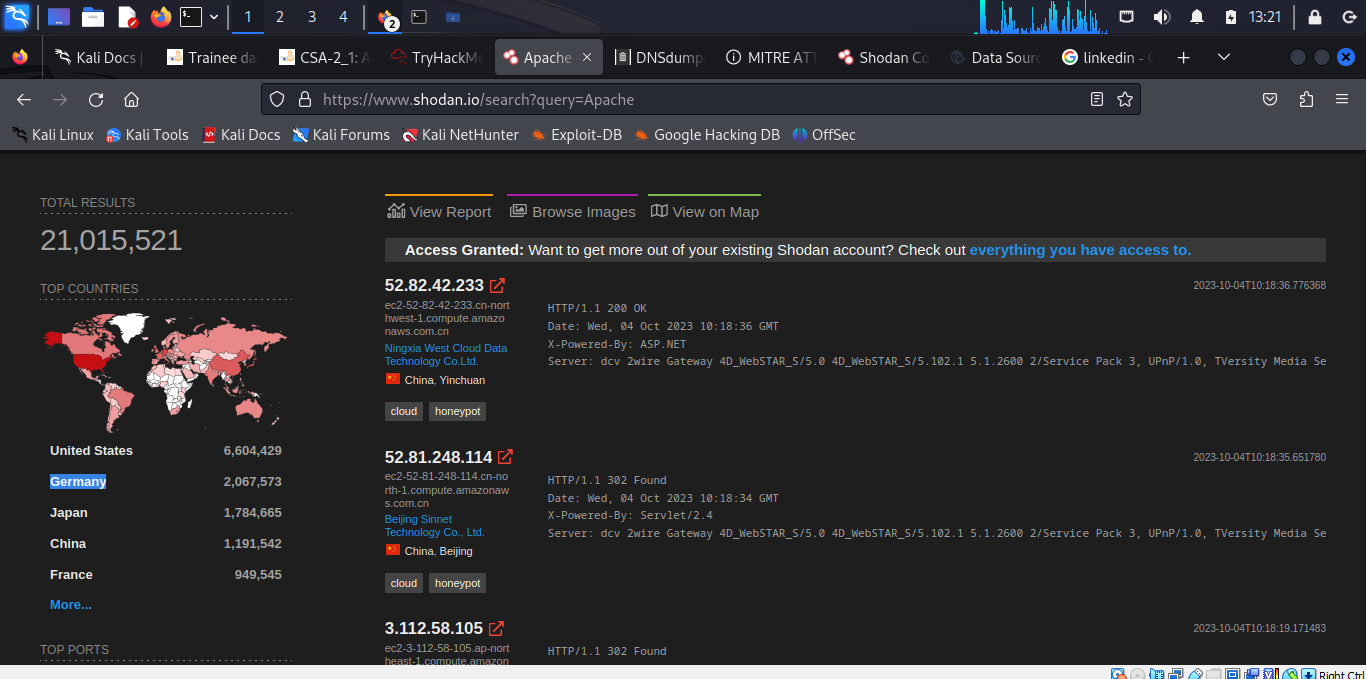
***Task 5: DNSDumpster***

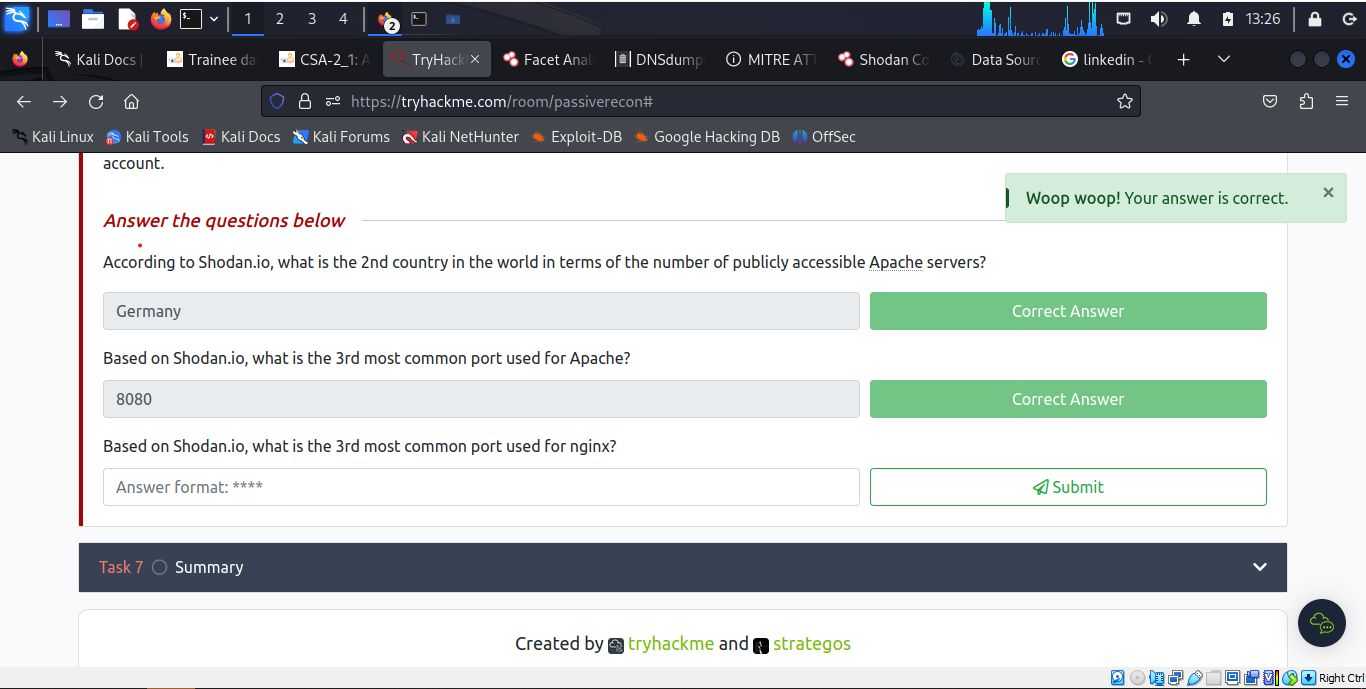




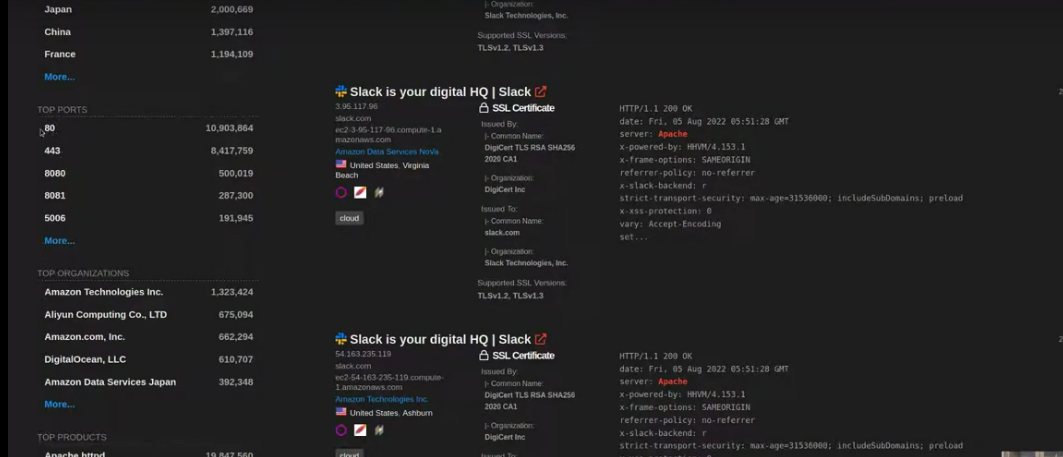
***Task 6: Shodan.io***

The learner is equipped with s service like [Shodan.io](https://www.shodan.io/) knowledge which is helpful to learn various pieces of information about the client’s network, without actively connecting to it.

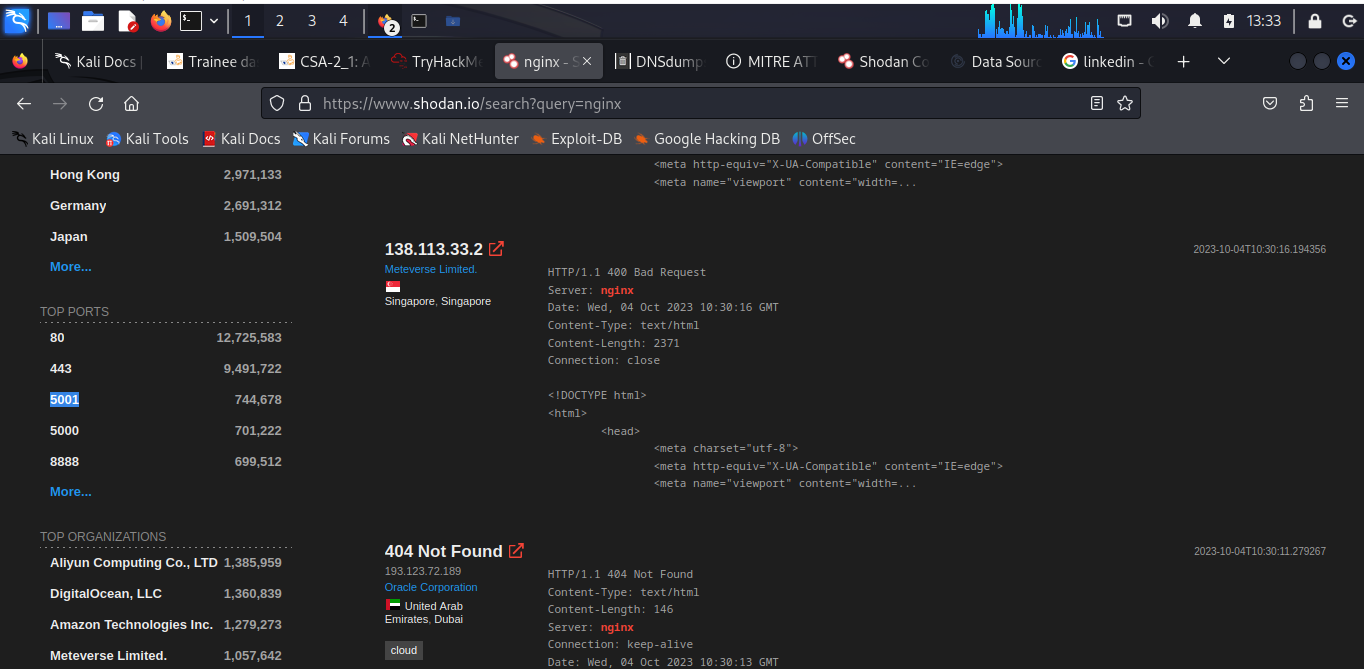




From the Shodan.io website, the learner finds out that port **8080** is the 3rd most common port used for Apache.

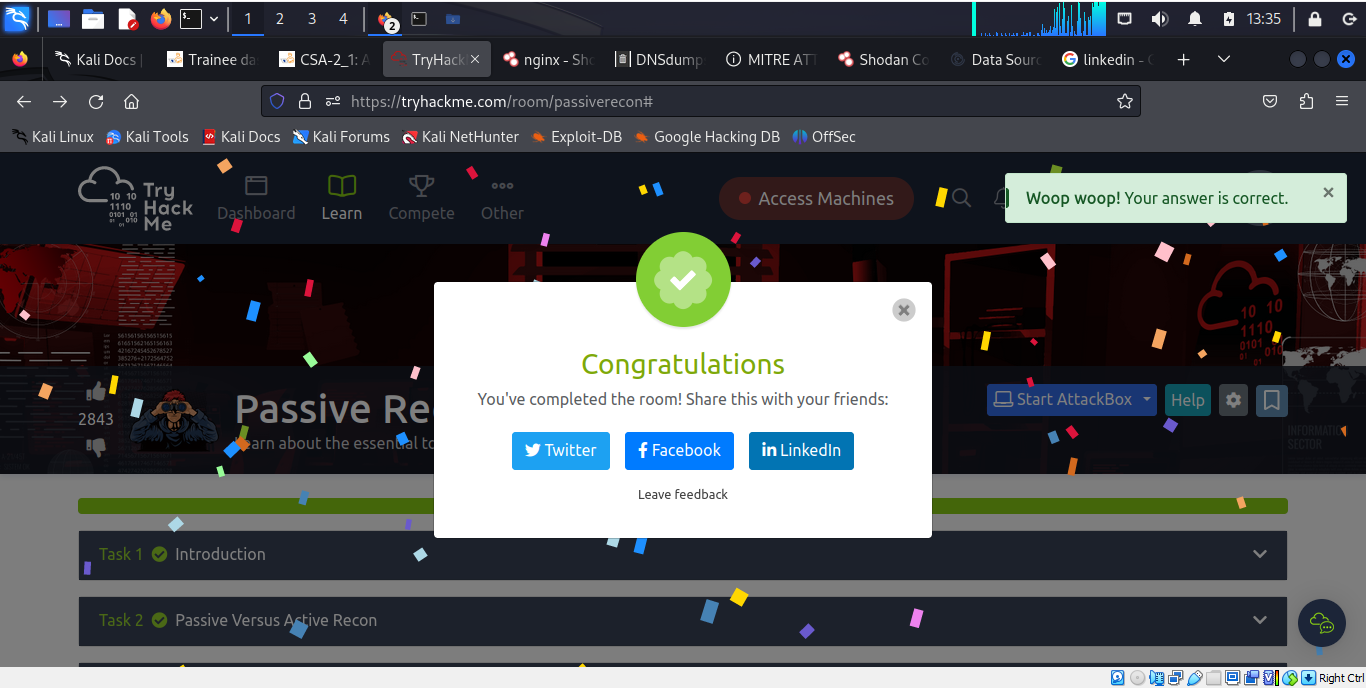


Based on Shodan.io, the 3rd most common port used for nginx is **5001**.



***Task 7: Summary***

This task enabled the learner focus on passive reconnaissance. Particularly covering command-line tools, whois, nslookup, and dig. The learner also covered two publicly available services [DNSDumpster](https://dnsdumpster.com/) and [Shodan.io](https://www.shodan.io/). The power of such tools is that it enables collection of information about the targets without directly connecting to them.



**Conclusion**

This task enabled the learner focus on passive reconnaissance. Particularly covering command-line tools, whois, nslookup, and dig. The learner also covered two publicly available services [DNSDumpster](https://dnsdumpster.com/) and [Shodan.io](https://www.shodan.io/). The power of such tools is that it enables collection of information about the targets without directly connecting to them.