# TryHackMe Reconnaissance Assignment

## Course: CEH

## Date Assigned: 12-10-2025

## Due Date: 13-10-2025

**Student Name:** Praveen Kumar

**Batch/Section:** Super30 Batch

**Instructor:** Nitish kumar

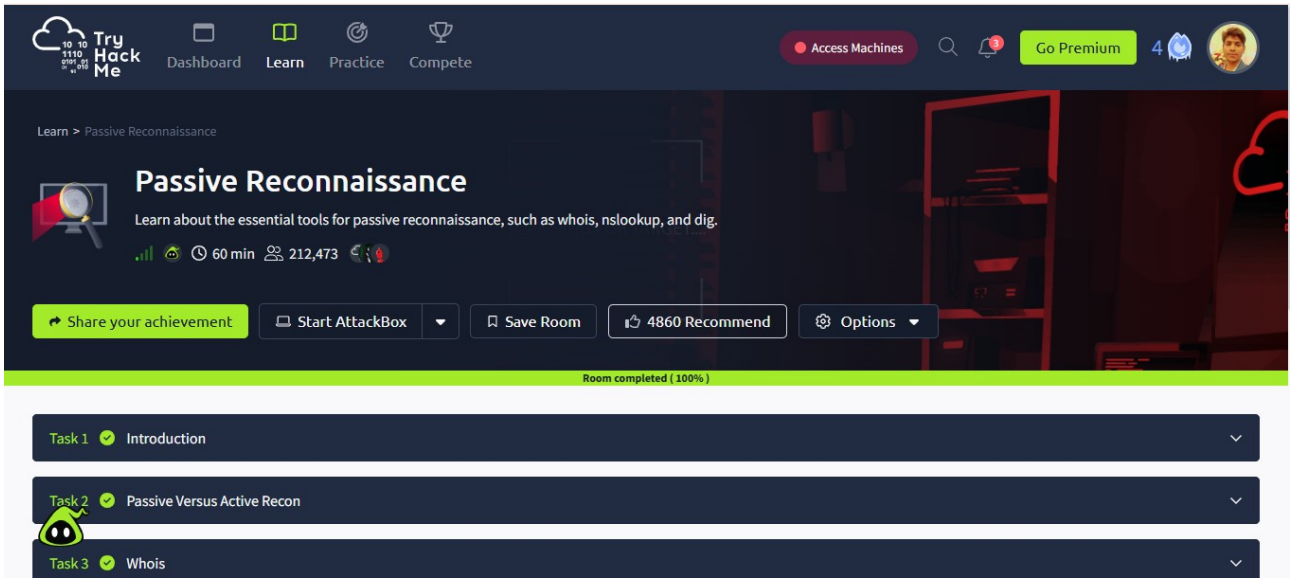
## Summary

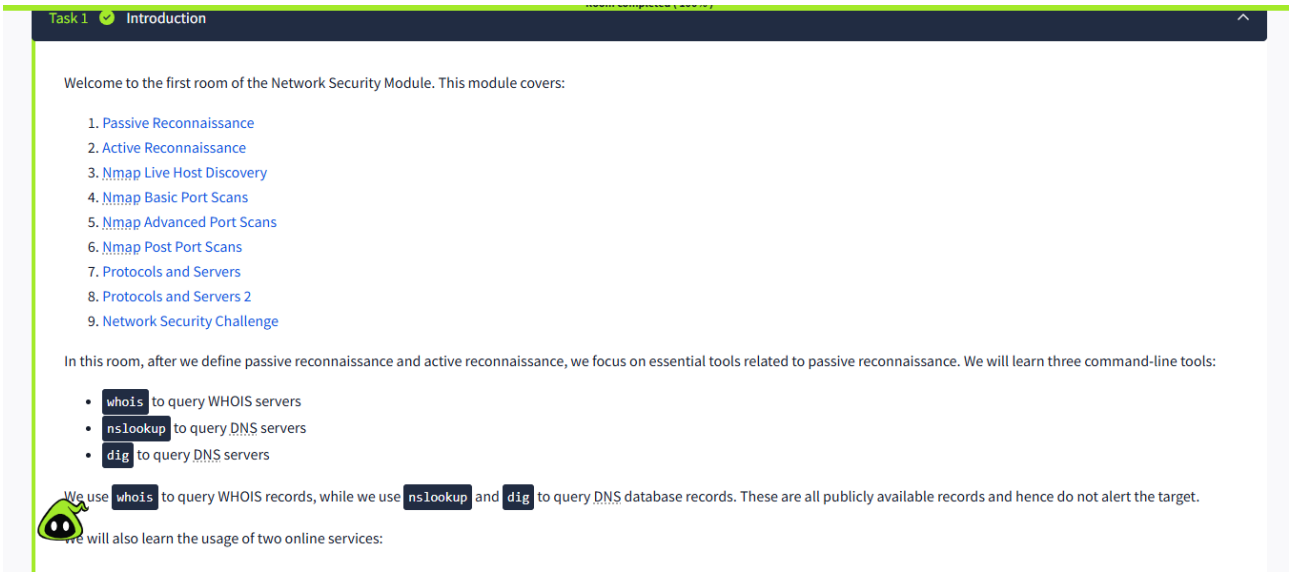
## 2. Executive Summary

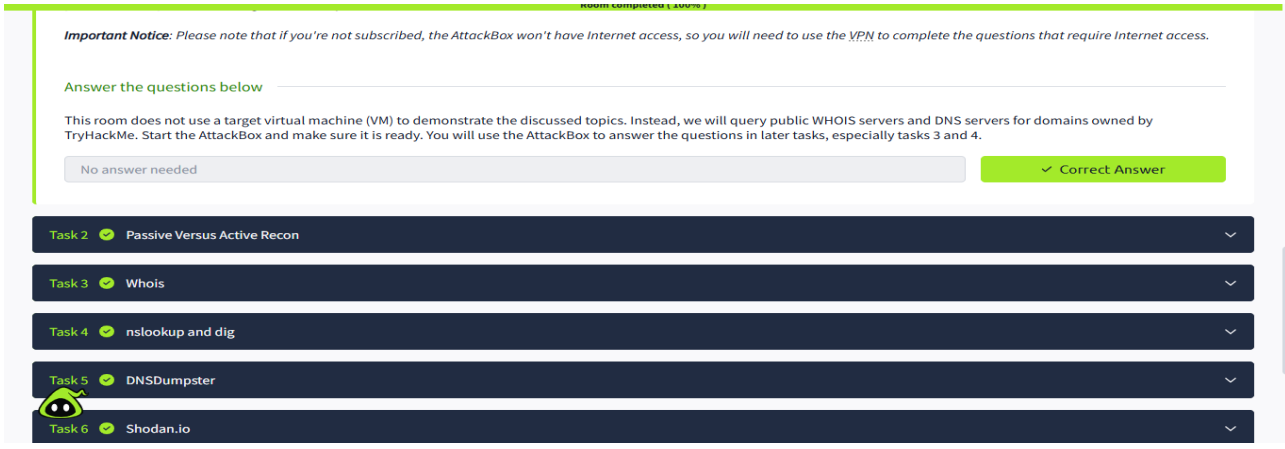
In this assignment, I worked through two TryHackMe rooms related to reconnaissance: Passive Reconnaissance and Active Reconnaissance. The reconnaissance phase is the first phase of ethical hacking, wherein an ethical hacker derives information about a target in order to understand its structure and potential vulnerabilities. The passive phase involved the collection of data that could be found in a public forum without ever interacting with the target systems. The active phase, referred to as "active" reconnaissance, required active interaction with the target in order to collect dynamic network data. I used a variety of tools along the way including WHOIS, nslookup, dig, ping, traceroute and nmap in order to obtain a practical understanding of data gathering techniques. Overall, the assignment was instrumental in deepening my understanding of the ways in which an attacker performs reconnaissance, while simultaneously offering an understanding of how key this phase is to a cybersecurity assessment.

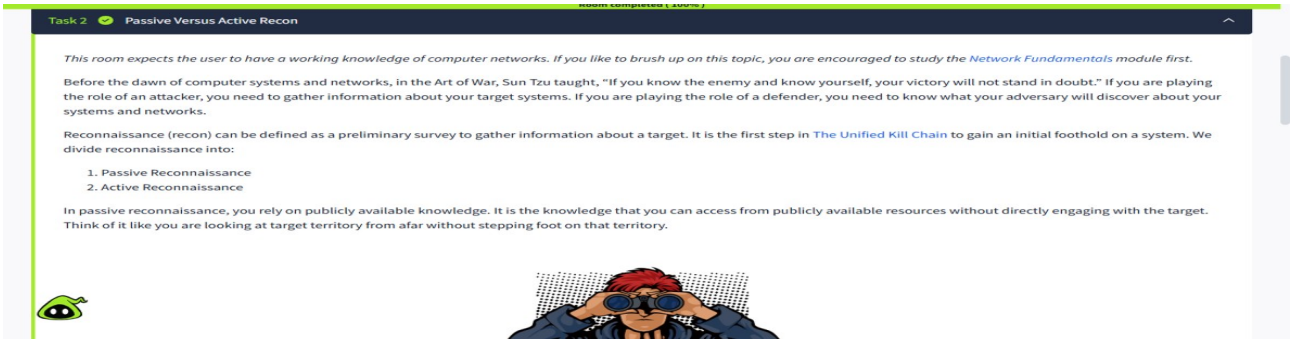
---

## Passive Reconnaissance


Try Hack Me
Dashboard
Learn
Practice
Compete
Access Machines
Go Premium
Learn > Passive Reconnaissance
Passive Reconnaissance
Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.
60 min
212,473
Share your achievement
Start AttackBox
Save Room
4860 Recommend
Options
Room completed ( 100% )
Task 1 Introduction
Task 2 Passive Versus Active Recon
Task 3 Whois


Task 1 Introduction
Welcome to the first room of the Network Security Module. This module covers:
1. Passive Reconnaissance
2. Active Reconnaissance
3. Nmap Live Host Discovery
4. Nmap Basic Port Scans
5. Nmap Advanced Port Scans
6. Nmap Post Port Scans
7. Protocols and Servers
8. Protocols and Servers 2
9. Network Security Challenge
In this room, after we define passive reconnaissance and active reconnaissance, we focus on essential tools related to passive reconnaissance. We will learn three command-line tools:
whois to query WHOIS servers
nslookup to query DNS servers
dig to query DNS servers
We use whois to query WHOIS records, while we use nslookup and dig to query DNS database records. These are all publicly available records and hence do not alert the target.
We will also learn the usage of two online services:


Important Notice: Please note that if you're not subscribed, the AttackBox won't have Internet access, so you will need to use the VPN to complete the questions that require Internet access.
Answer the questions below
This room does not use a target virtual machine (VM) to demonstrate the discussed topics. Instead, we will query public WHOIS servers and DNS servers for domains owned by TryHackMe. Start the AttackBox and make sure it is ready. You will use the AttackBox to answer the questions in later tasks, especially tasks 3 and 4.
No answer needed
Correct Answer
Task 2 Passive Versus Active Recon
Task 3 Whois
Task 4 nslookup and dig
Task 5 DNSDumpster
Task 6 Shodan.io


## Objective

The goal of passive reconnaissance is to gather as much information as possible about a target without making direct contact with its systems. This ensures that the target remains unaware of the information gathering, reducing the risk of detection.

## Tools Used

- WHOIS for domain registration data
- nslookup and dig for DNS interrogation
- Sublist3r and DNSDumpster for subdomain enumeration
- theHarvester for aggregating public data
- Shodan for website technology footprinting
- Google Dorking for uncovering indexed sensitive information

---

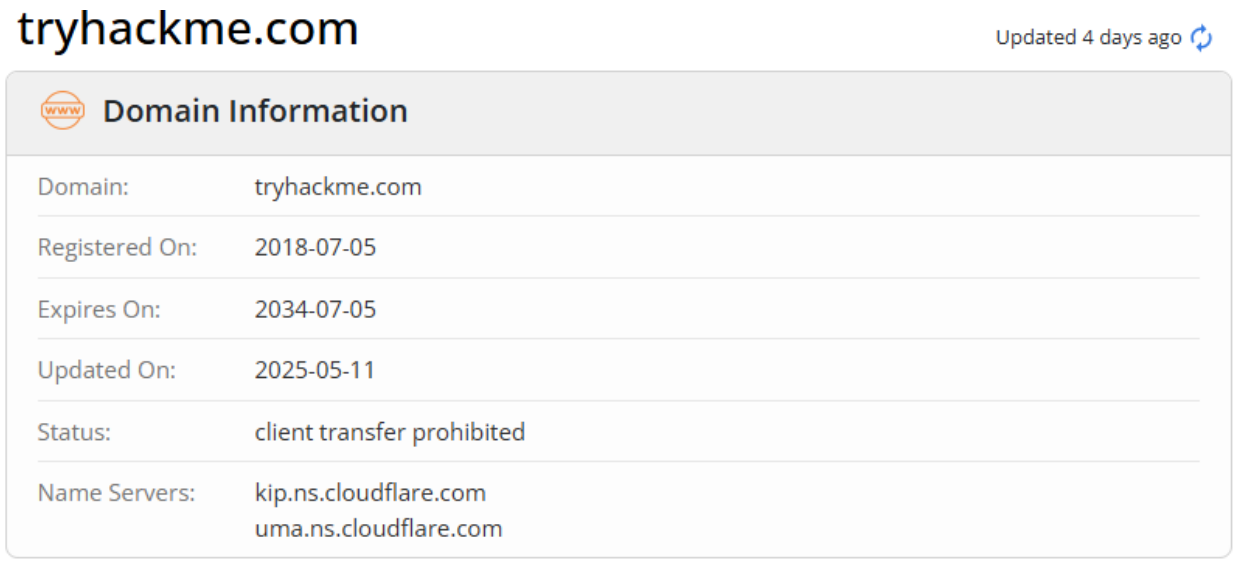
## Step-by-Step Walkthrough

### Step 1: WHOIS Lookup

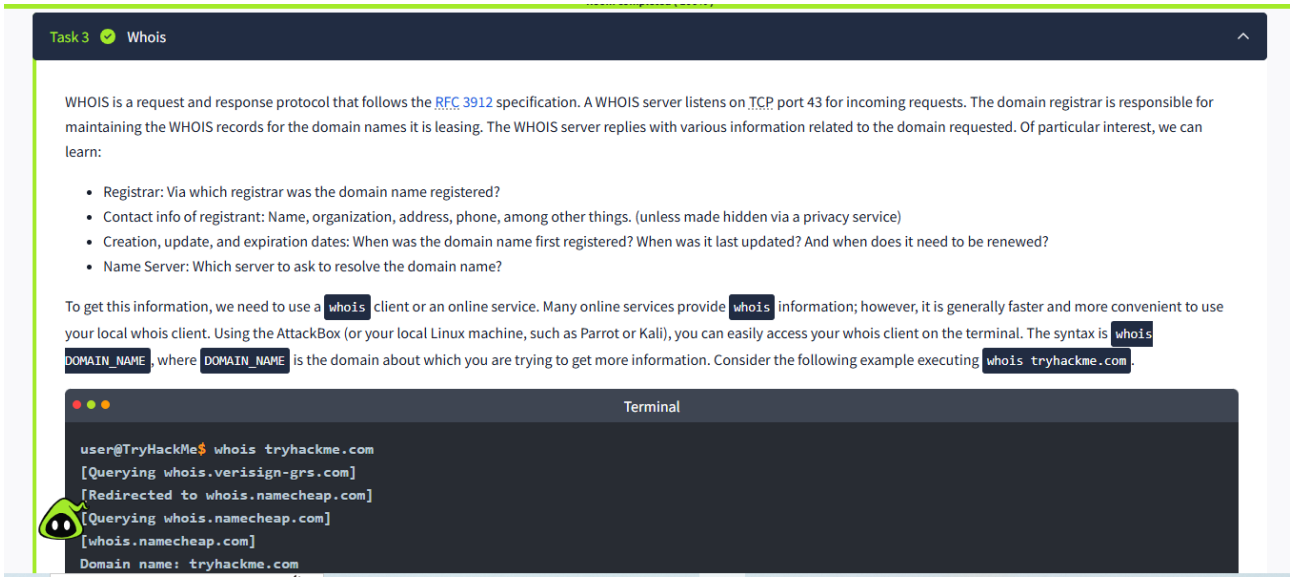
I started by querying WHOIS databases to obtain domain registration details. This step is crucial for identifying the domain owner, administrative contacts, registration and expiration dates, and hosting providers. Such details can often reveal organizational info or contact points useful for social engineering or further research.

Command Run:

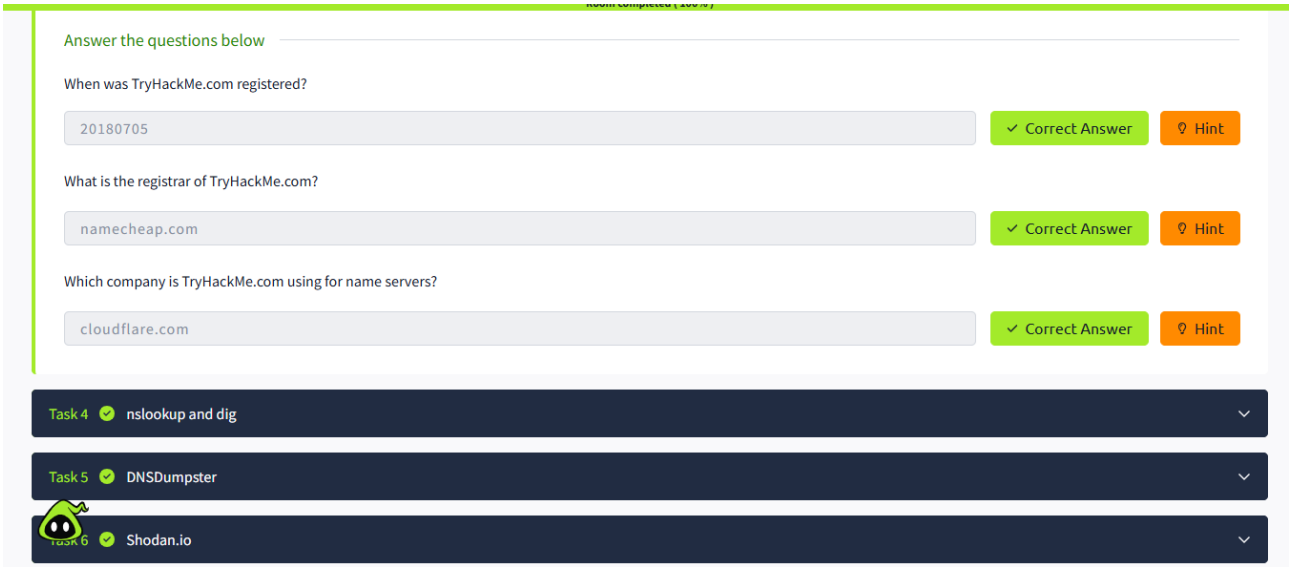
whois tryhackme.com
Analysis:
The WHOIS output showed the domain registrar’s name, registration timestamps, and the domain’s status. Notably, I could see the name servers assigned to the domain, which hinted at where DNS records might be managed.




---




---




**Step 2: DNS Information Gathering**

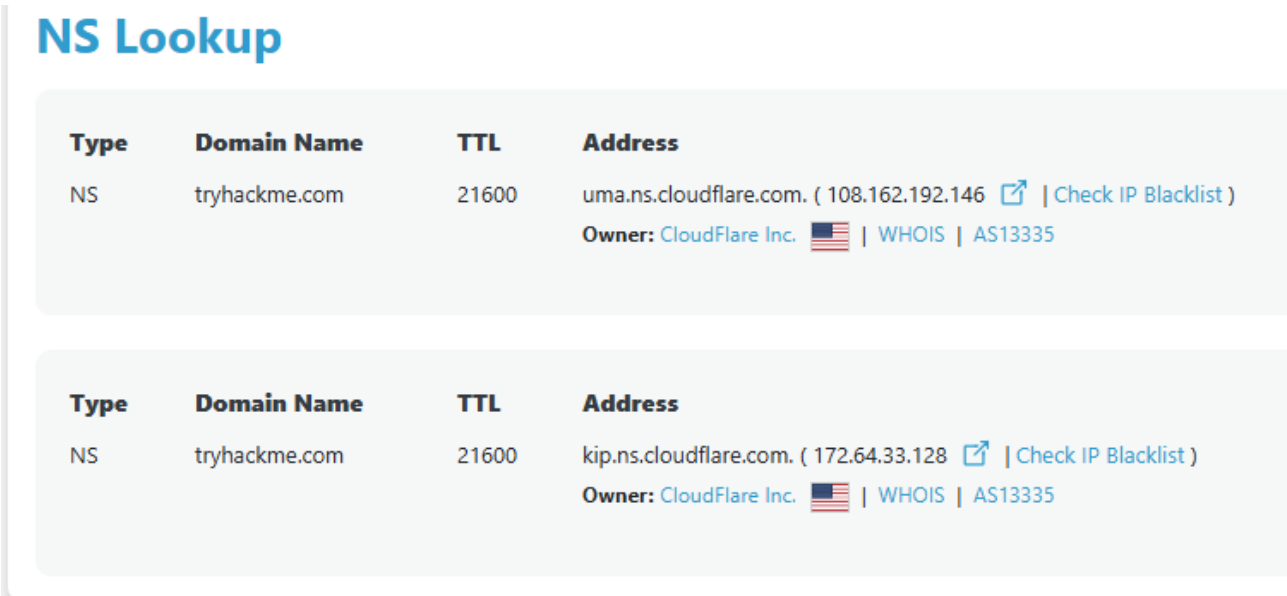
To understand the domain's DNS setup, I used nslookup and dig commands. These tools reveal mappings between domain names and IP addresses, mail servers, and authoritative name servers.

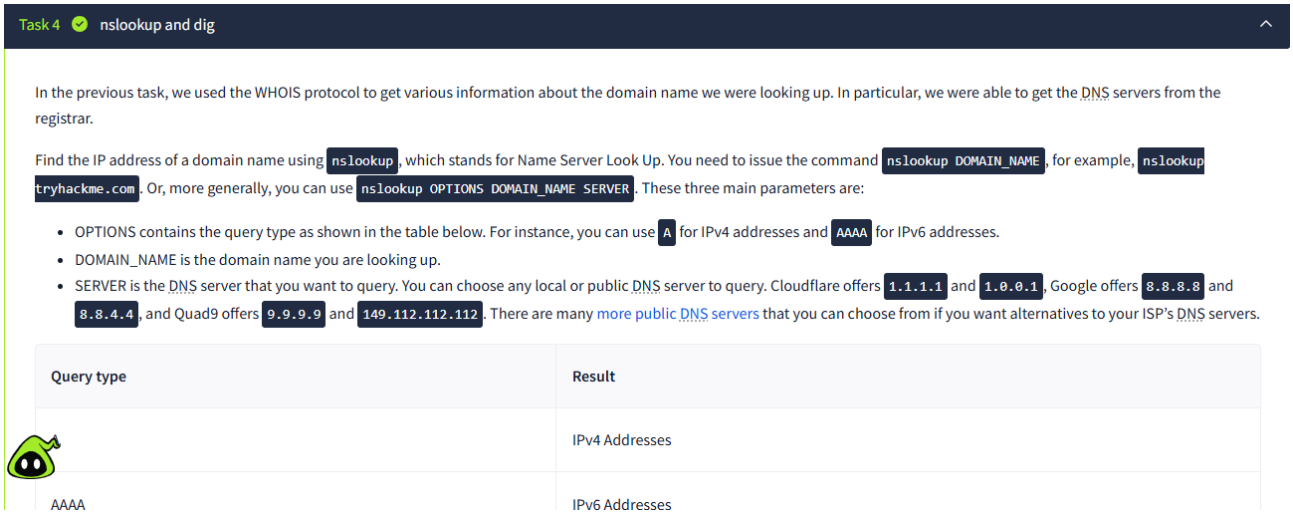
Commands Run:

nslookup tryhackme.com
dig tryhackme.com any

Analysis:

From nslookup, I extracted the primary IP address tied to the domain. The dig query returned a broader set of DNS records including MX (mail exchange) records and NS (name server) records. This information helps map out the email infrastructure and DNS hosting, which could be critical in phishing or spoofing attempts.





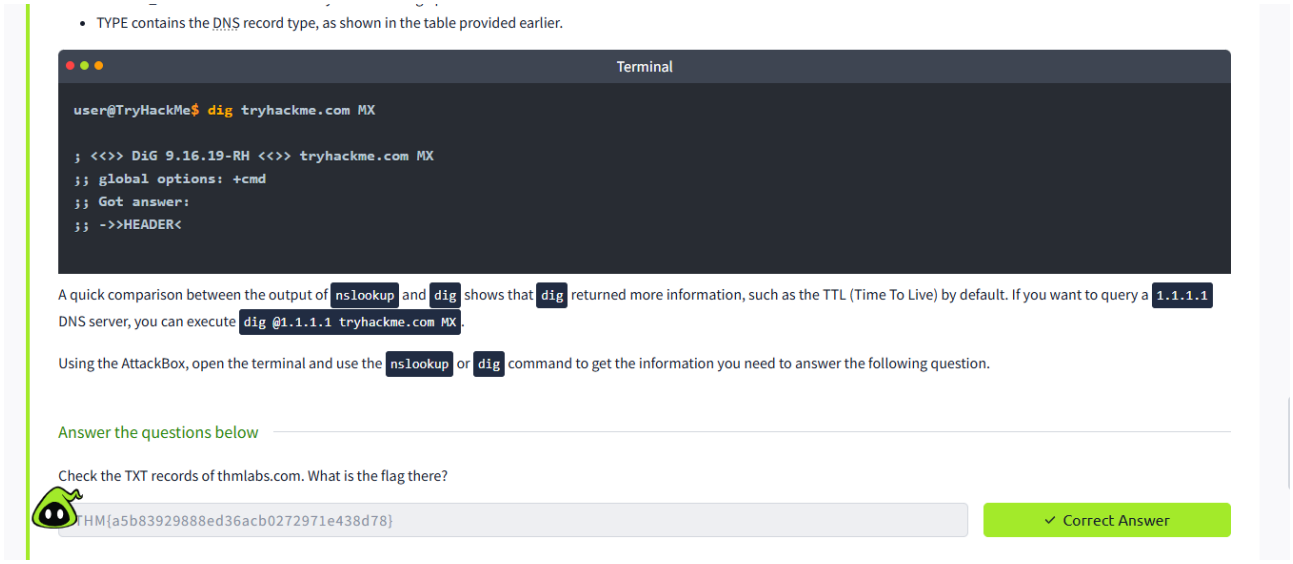
Task 4 nslookup and dig

In the previous task, we used the WHOIS protocol to get various information about the domain name we were looking up. In particular, we were able to get the DNS servers from the registrar.

Find the IP address of a domain name using `nslookup`, which stands for Name Server Look Up. You need to issue the command `nslookup DOMAIN_NAME`, for example, `nslookup tryhackme.com`. Or, more generally, you can use `nslookup OPTIONS DOMAIN_NAME SERVER`. These three main parameters are:

- OPTIONS contains the query type as shown in the table below. For instance, you can use `A` for IPv4 addresses and `AAAA` for IPv6 addresses.
- DOMAIN_NAME is the domain name you are looking up.
- SERVER is the DNS server that you want to query. You can choose any local or public DNS server to query. Cloudflare offers `1.1.1.1` and `1.0.0.1`, Google offers `8.8.8.8` and `8.8.4.4`, and Quad9 offers `9.9.9.9` and `149.112.112.112`. There are many more public DNS servers that you can choose from if you want alternatives to your ISP's DNS servers.

| Query type | Result |
|---|---|
| | IPv4 Addresses |
| AAAA | IPv6 Addresses |



- TYPE contains the DNS record type, as shown in the table provided earlier.

Terminal

```
user@TryHackMe$ dig tryhackme.com MX

; <<>> DiG 9.16.19-RH <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<
```

A quick comparison between the output of `nslookup` and `dig` shows that `dig` returned more information, such as the TTL (Time To Live) by default. If you want to query a `1.1.1.1` DNS server, you can execute `dig @1.1.1.1 tryhackme.com MX`.

Using the AttackBox, open the terminal and use the `nslookup` or `dig` command to get the information you need to answer the following question.

Answer the questions below

Check the TXT records of thmlabs.com. What is the flag there?

THM{a5b83929888ed36acb0272971e438d78}

✓ Correct Answer

## Step 3: Subdomain Enumeration

Subdomains often host different services or environments (like dev, staging, or mail servers) that might have different vulnerabilities. Using Sublist3r, I enumerated subdomains tied to the target domain.

Command Run:

sublist3r -d example.com
Analysis:
The tool discovered multiple subdomains including mail.example.com, dev.example.com, and shop.example.com. Each subdomain represents an additional attack surface and may expose services or outdated applications.

I also cross-checked these findings with DNSDumpster, an online DNS mapping tool, which visually confirmed the subdomain structure and IP mappings.

## Task 5 DNSDumpster

DNS lookup tools, such as nslookup and dig, cannot find subdomains on their own. The domain you are inspecting might include a different subdomain that can reveal much information about the target. For instance, if tryhackme.com has the subdomains wiki.tryhackme.com and webmail.tryhackme.com, you want to learn more about these two as they can hold a trove of information about your target. There is a possibility that one of these subdomains has been set up and is not updated regularly. Lack of proper regular updates usually leads to vulnerable services. But how can we know that such subdomains exist?

We can consider using multiple search engines to compile a list of publicly known subdomains. One search engine won't be enough; moreover, we should expect to go through at least tens of results to find interesting data. After all, you are looking for subdomains that are not explicitly advertised, and hence it is not necessary to make it to the first page of search results. Another approach to discover such subdomains would be to rely on brute-forcing queries to find which subdomains have DNS records.

To avoid such a time-consuming search, one can use an online service that offers detailed answers to DNS queries, such as DNSDumpster. If we search DNSDumpster for `tryhackme.com`, we will discover the subdomain `blog.tryhackme.com`, which a typical DNS query cannot provide. In addition, DNSDumpster will return the collected DNS information in easy-to-read tables and a graph. DNSDumpster will also provide any collected information about listening servers.

We will search for `tryhackme.com` on DNSDumpster to give you a glimpse of the expected output. Among the results, we got a list of DNS servers for the domain we are looking up. DNSDumpster also resolved the domain names to IP addresses and even tried to geolocate them. We can also see the MX records; DNSDumpster resolved all five mail exchange servers to their respective IP addresses and provided more information about the owner and location. Finally, we can see TXT records. Practically a single query was enough to retrieve all this information.

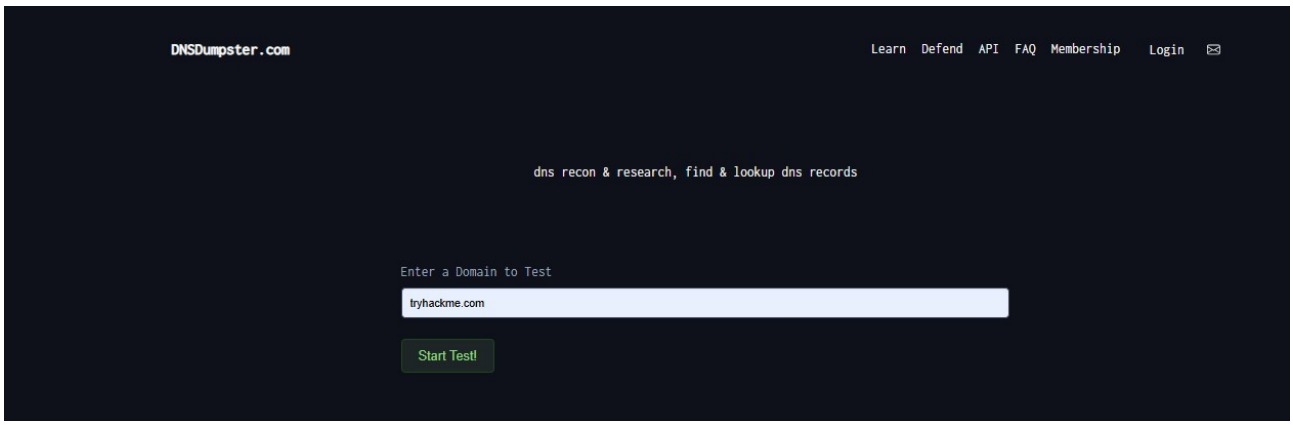
Use the web browser on the AttackBox, or your system, to answer the following question.

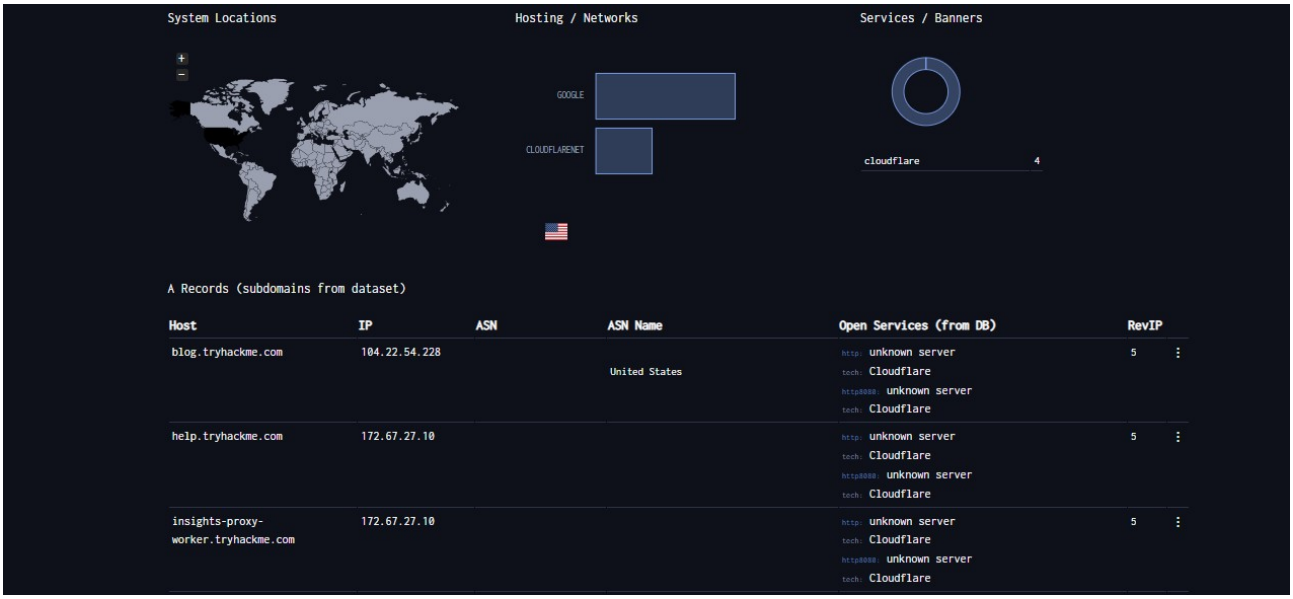
### Answer the questions below

Lookup tryhackme.com on DNSDumpster. What is one interesting subdomain that you would discover in addition to www and blog?

remote

✓ Correct Answer






---

**Step 4: Website Fingerprinting with Shodan**

To understand the underlying technology stack of the target's web presence, I used Shodan. This tool identifies content management systems, web servers, analytics tools, and other technologies.

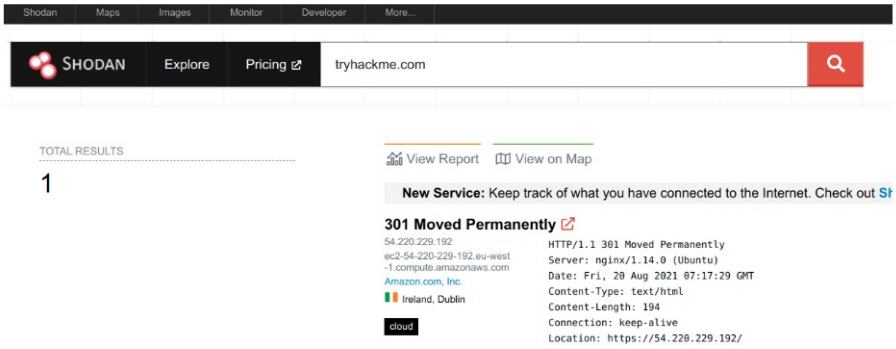
Observation:

Shodan indicated the website was built on WordPress, a popular CMS, and was served by an Apache web server. Knowing this helps in tailoring attacks or defenses, as certain CMS platforms have well-known vulnerabilities or plugin risks.

## Task 6 Shodan.io

When you are tasked to run a penetration test against specific targets, as part of the passive reconnaissance phase, a service like Shodan.io can be helpful to learn various pieces of information about the client's network, without actively connecting to it. Furthermore, on the defensive side, you can use different services from Shodan.io to learn about connected and exposed devices belonging to your organization.

Shodan.io tries to connect to every device reachable online to build a search engine of connected "things" in contrast with a search engine for web pages. Once it gets a response, it collects all the information related to the service and saves it in the database to make it searchable. Consider the saved record of one of tryhackme.com's servers.




### Answer the questions below

According to Shodan.io, what is the first country in the world in terms of the number of publicly accessible Apache servers?

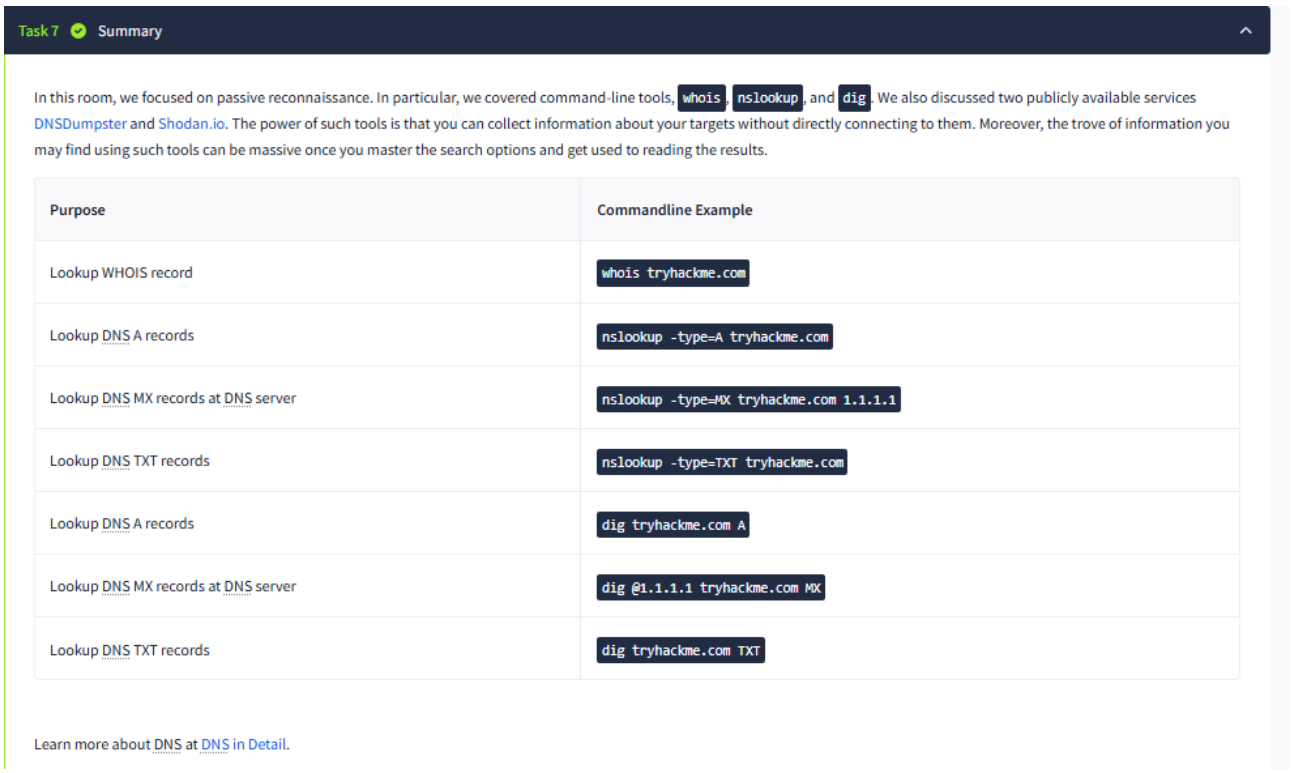
United States — ✓ Correct Answer — Hint

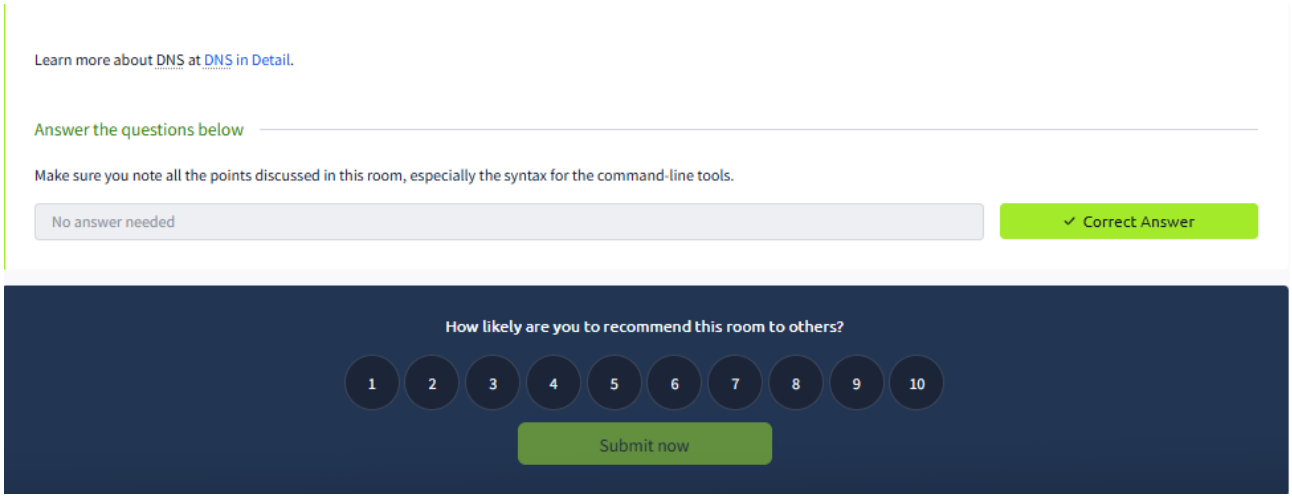
Based on Shodan.io, what is the 3rd most common port used for Apache?

8080 — ✓ Correct Answer — Hint

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

888 — ✓ Correct Answer — Hint







**Step 5: Google Dorking**

Google dorking leverages advanced search operators to find sensitive or hidden information indexed by Google, such as confidential documents or admin pages.

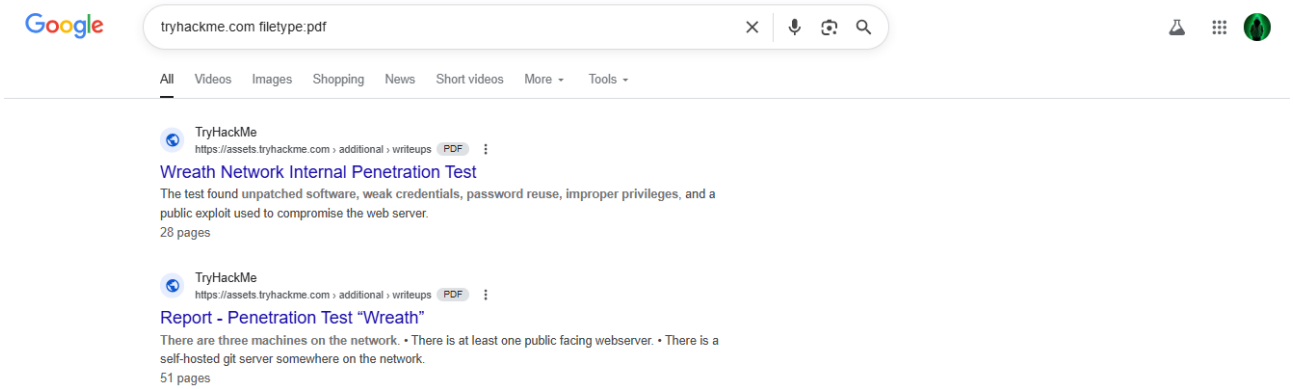
Examples Used:

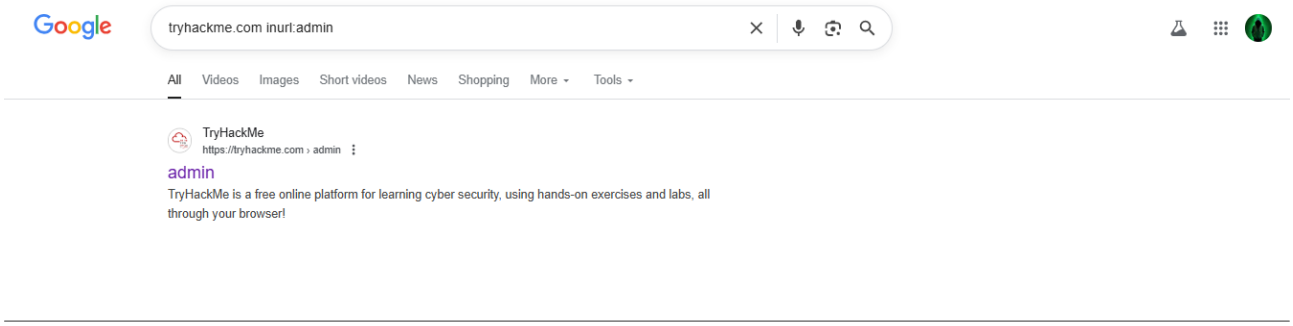
site:tryhackme.com filetype:pdf
site:tryhackme.com inurl:admin

Analysis:

These queries uncovered publicly accessible PDF documents and administrative pages exposed

unintentionally. This demonstrates how misconfigured web servers or careless publishing can leak critical information.




---

**Lessons Learned**
This room highlighted the power of passive reconnaissance in gathering comprehensive target intelligence without triggering alarms. Public databases and search engines can expose a wealth of actionable information. The key is thorough documentation and cross-verification of data to build a solid target profile for subsequent phases.

---

# Declaration

I declare that this work is my own and completed without unauthorized assistance.

Signature: Praveen Kumar

Date: 12-10-2025