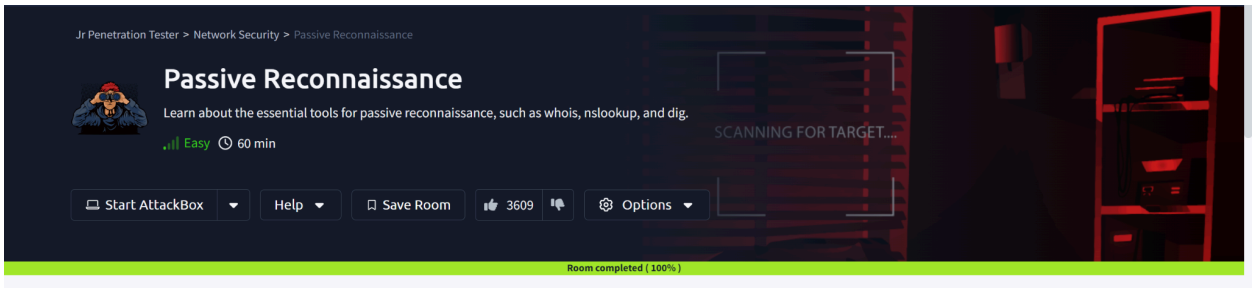
PASSIVE RECONNAISSANCE

ASSIGNMENT REPORT



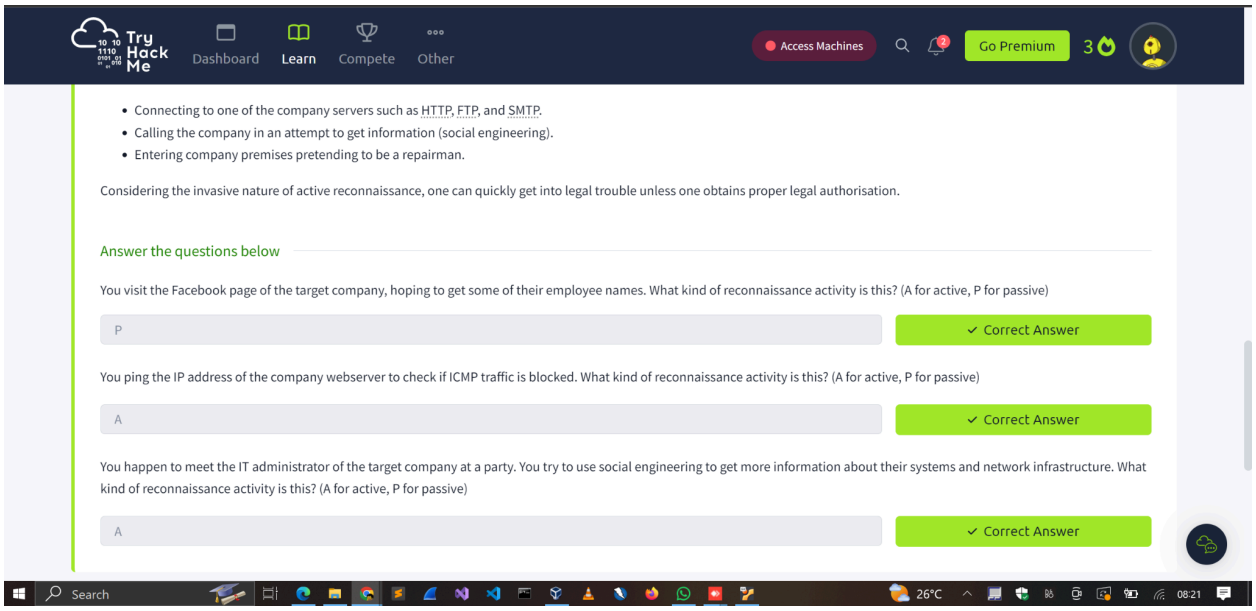
Peter Kinyumu,
cs-sa07-24067,
May 22nd, 2024.

1. INTRODUCTION

This room focused on the essentials of passive reconnaissance, which simply means gathering publicly accessible information about a target without engaging with it. This involves looking for DNS records, Job Ads related to the target, news articles, etc. It teaches using tools like **whois**, **dig**, **nslookup**, **DNSdumpster** and **Shodan.io**.

2. ANSWERS TO QUESTIONS

Passive vs Active recon

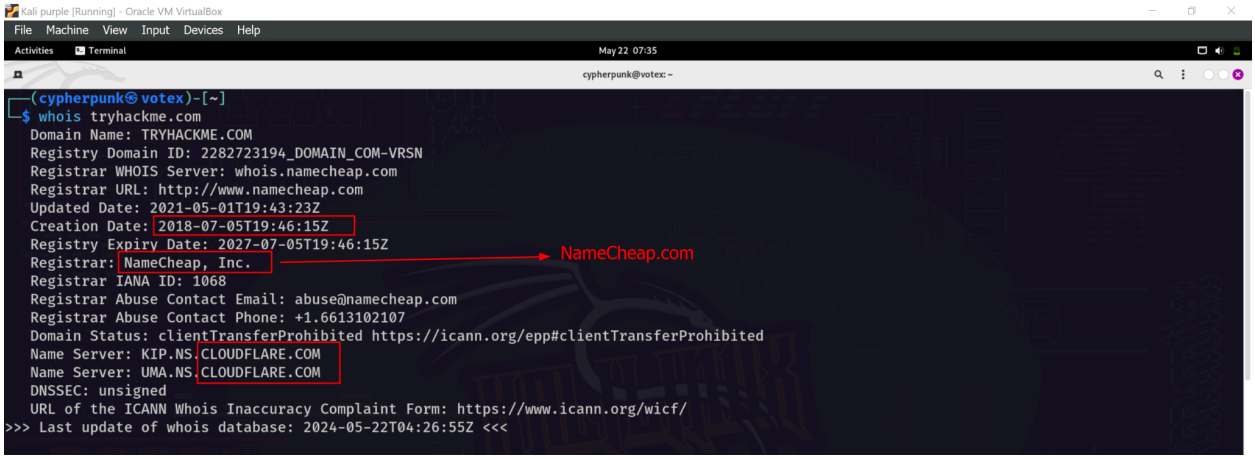


Whois

a. **When was TryHackMe.com registered?**
   20180705

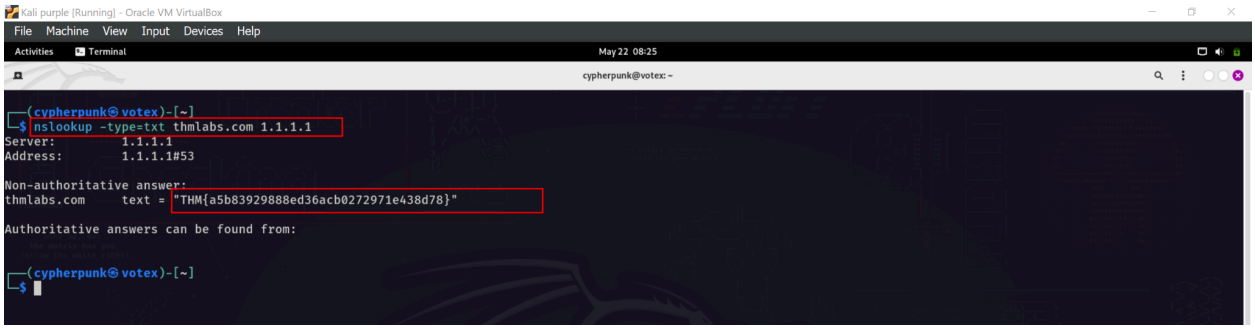
b. **What is the registrar of TryHackMe.com?**
   NameCheap.com

c. **Which company is TryHackMe.com using for name servers?**
   CLOUDFARE.COM



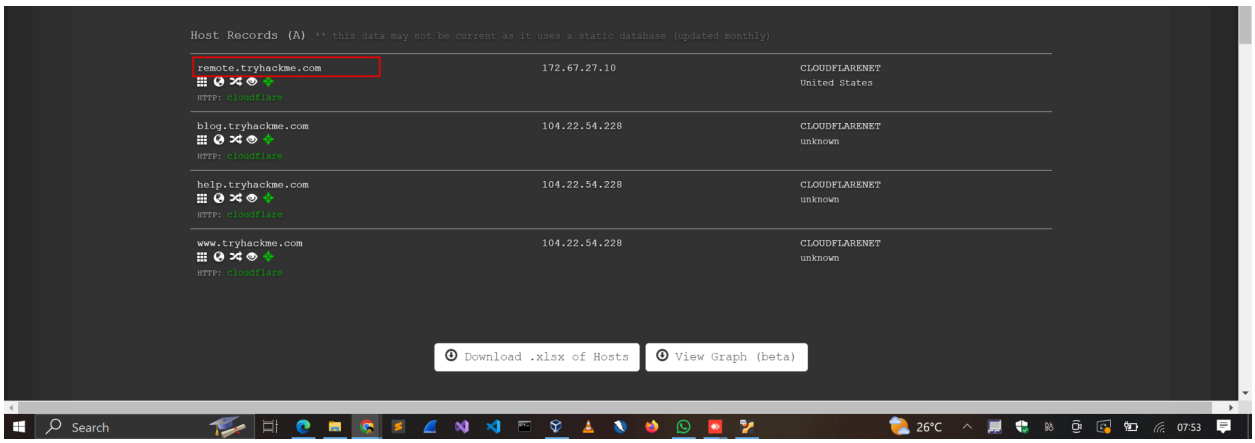
NSlookup

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



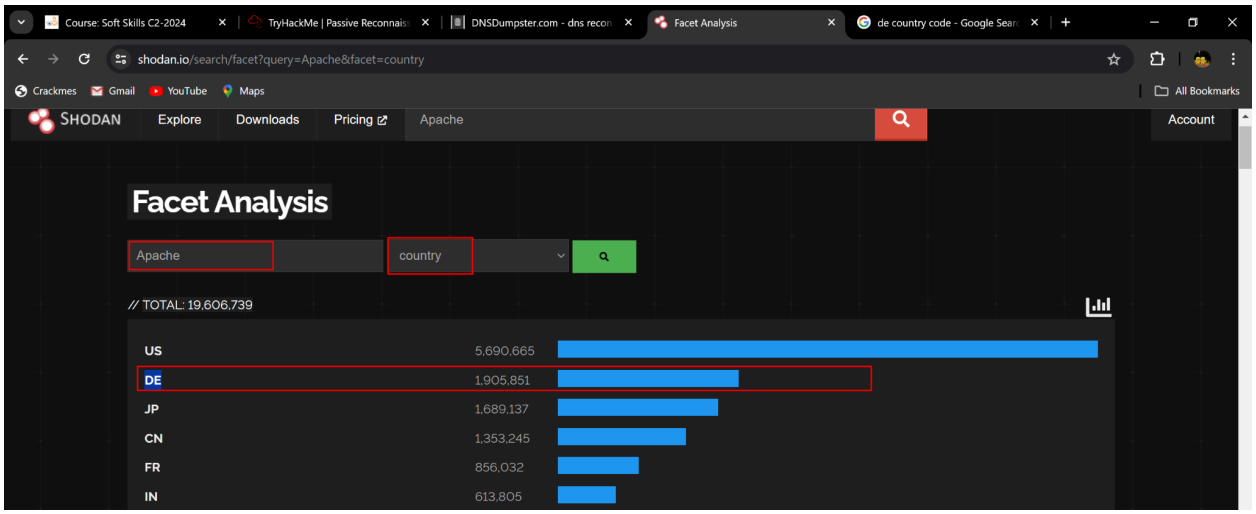
DNSDumpster

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

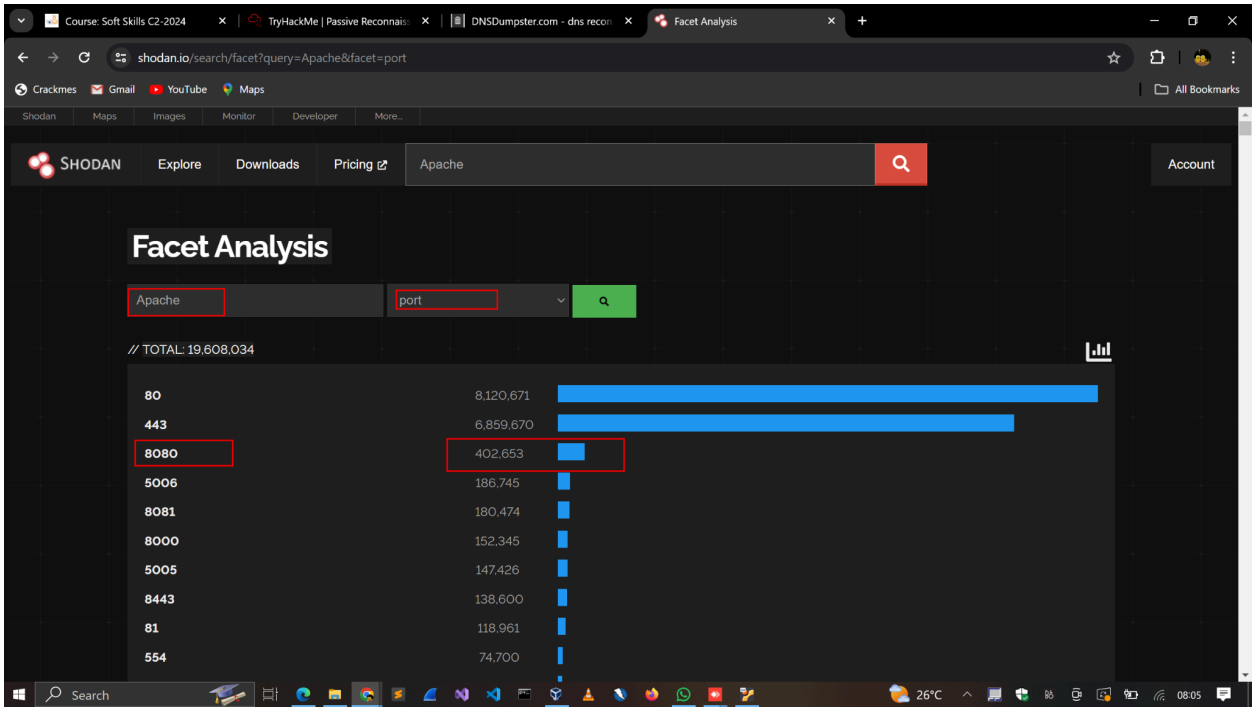


Shodan.io

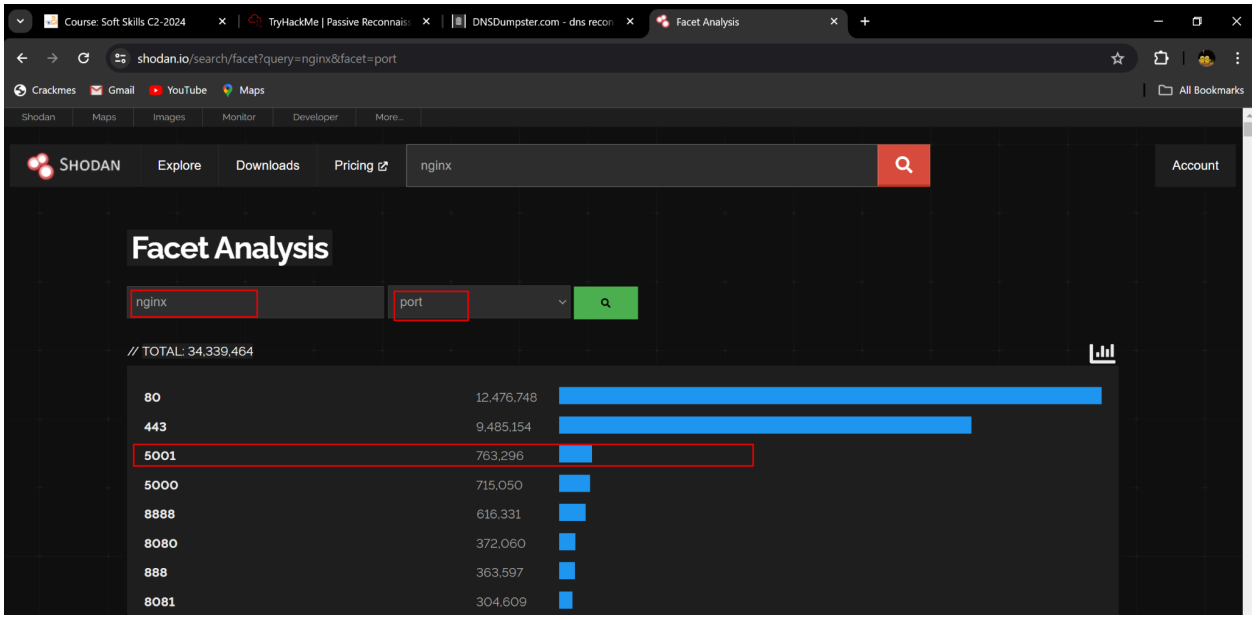
a. **According to Shodan.io, what is the 2nd country in the world in terms of the number of publicly accessible Apache servers?**



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



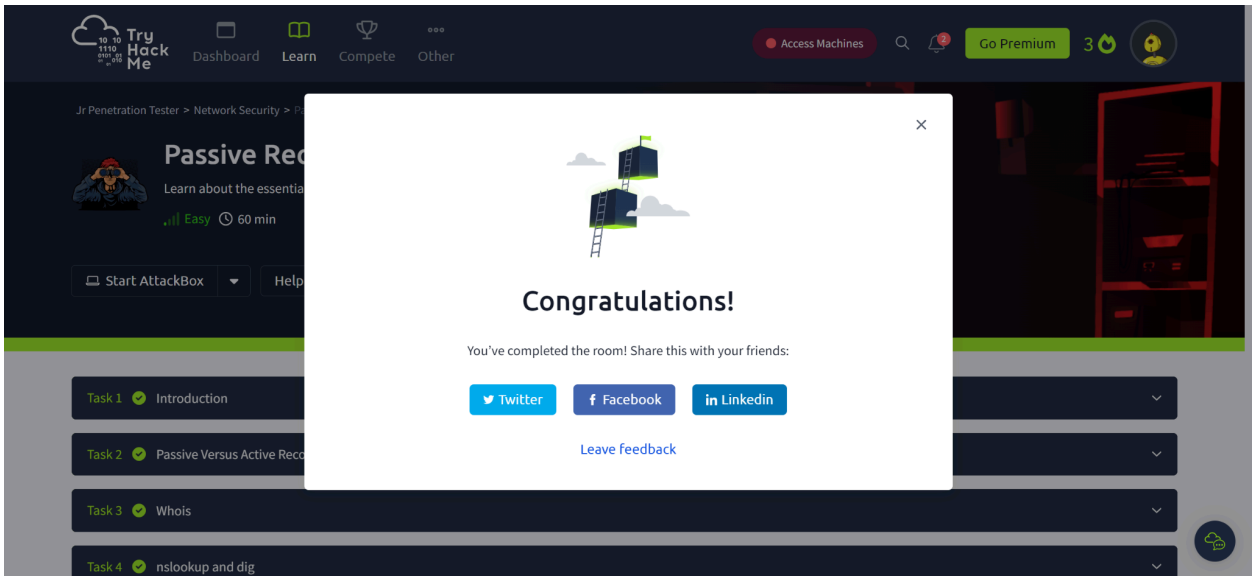
c. Based on Shodan.io, what is the 3rd most common port used for nginx?



3. MODULE COMPLETION

Below is the link to my THM profile, which displays completed rooms, including this room, Passive Reconnaissance.

https://tryhackme.com/p/c1ph3rbnuk



4. CONCLUSION

This room relates so much to the previous room I completed on Red Team Recon. It was easy to go through this after going through the previous one.

However, I learned two more things from this assignment. First, I learned how to use the DNSDumpster tool, which collectively gives you all DNS information about a domain, from MX records to TX records and Host records, from just a single query. It also visualizes domain mappings and geolocation information, which is very insightful. Second, I learned how to use Shodan.io to learn about connected and exposed devices.