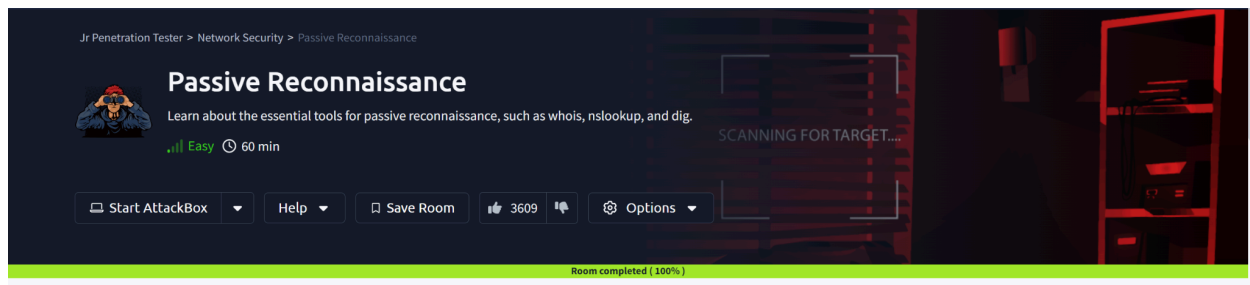


PASSIVE RECONNAISSANCE

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

The screenshot shows the TryHackMe interface for a room titled "Passive vs Active recon". The top navigation bar includes links for Dashboard, Learn, Compete, and Other. The room content lists three types of reconnaissance activities: connecting to company servers (HTTP, FTP, SMTP), calling the company (social engineering), and entering premises (pretending to be a repairman). It explains that active reconnaissance is invasive and can lead to legal trouble. Below this, three questions are presented with input fields and "Correct Answer" buttons:

- Question 1: "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)". The answer field contains "P".
- Question 2: "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)". The answer field contains "A".
- Question 3: "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)". The answer field contains "A".

The bottom of the screenshot shows a Windows taskbar with various application icons and a system tray displaying the temperature (26°C) and time (08:21).

Whois

- When was TryHackMe.com registered?**
20180705
- What is the registrar of TryHackMe.com?**
NameCheap.com
- Which company is TryHackMe.com using for name servers?**
CLOUDFARE.COM

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
May 22 07:35
cypherpunk@votex: ~
(cypherpunk@votex)~$ 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: 2021-05-01T19:43:23Z
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/wicf/
>>> Last update of whois database: 2024-05-22T04:26:55Z <<<
```

NSlookup

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

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
May 22 08:25
cypherpunk@votex: ~
(cypherpunk@votex)~$ nslookup -type=txt thmlabs.com 1.1.1.1
Server: 1.1.1.1
Address: 1.1.1.1#53

Non-authoritative answer:
thmlabs.com text = "THM{a5b83929888ed36acb0272971e438d78}"

Authoritative answers can be found from:

(cypherpunk@votex)~$
```

DNSDumpster

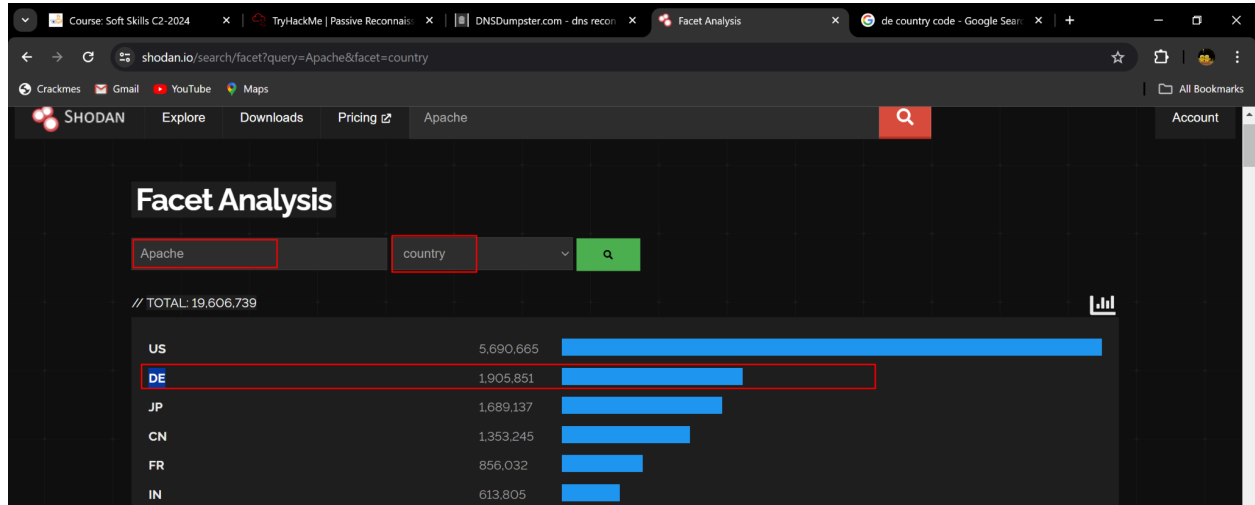
- a. Lookup tryhackme.com on DNSDumpster. What is one interesting subdomain that you would discover in addition to www and blog?

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)			
remote.tryhackme.com	172.67.27.10	CLOUDFLARENET	United States
blog.tryhackme.com	104.22.54.228	CLOUDFLARENET	unknown
help.tryhackme.com	104.22.54.228	CLOUDFLARENET	unknown
www.tryhackme.com	104.22.54.228	CLOUDFLARENET	unknown

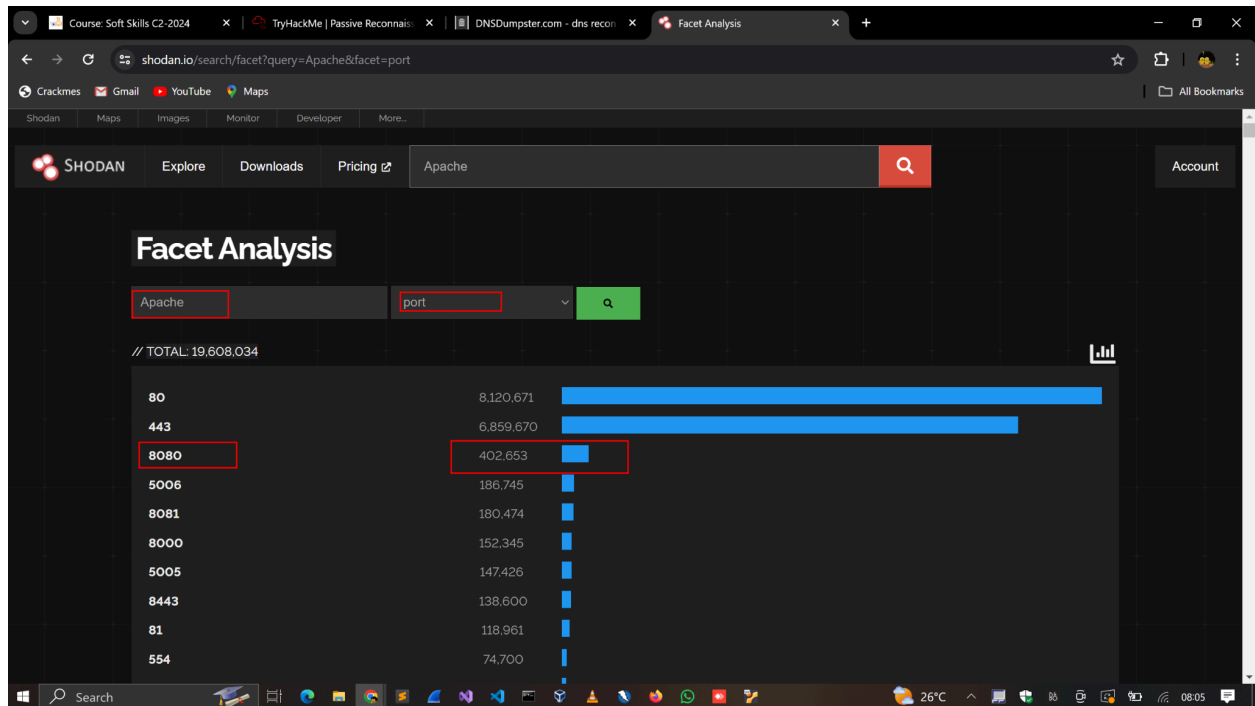
Download .xlsx of Hosts View Graph (beta)

Shodan.io

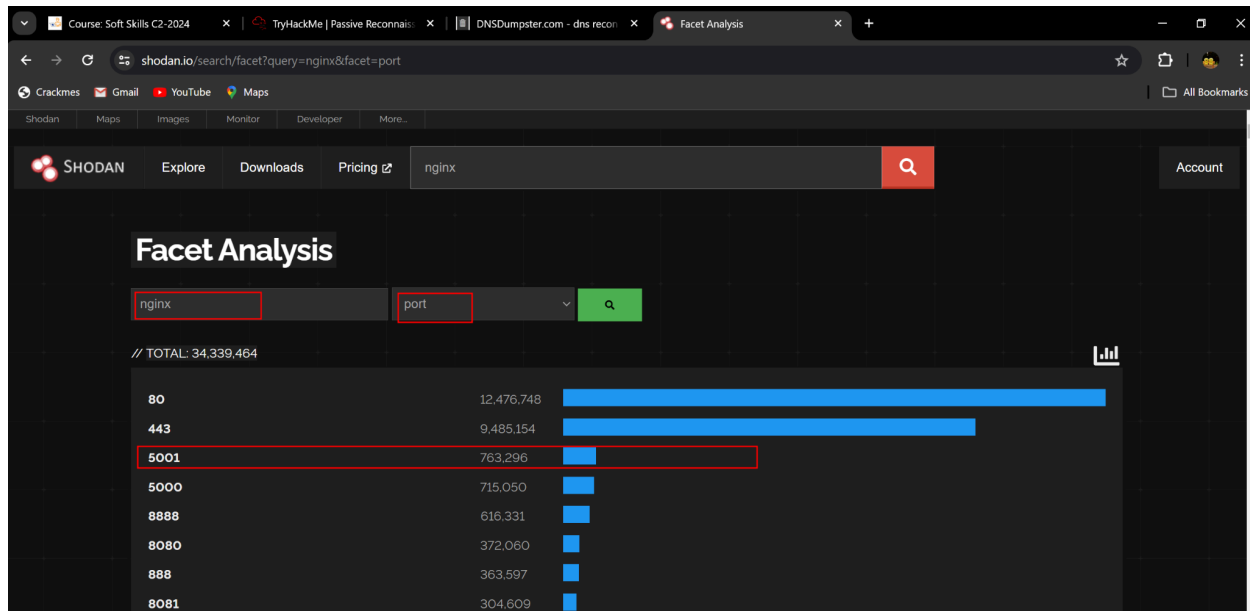
- a. According to Shodan.io, what is the 2nd country in the world in terms of the number of publicly accessible Apache servers?



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



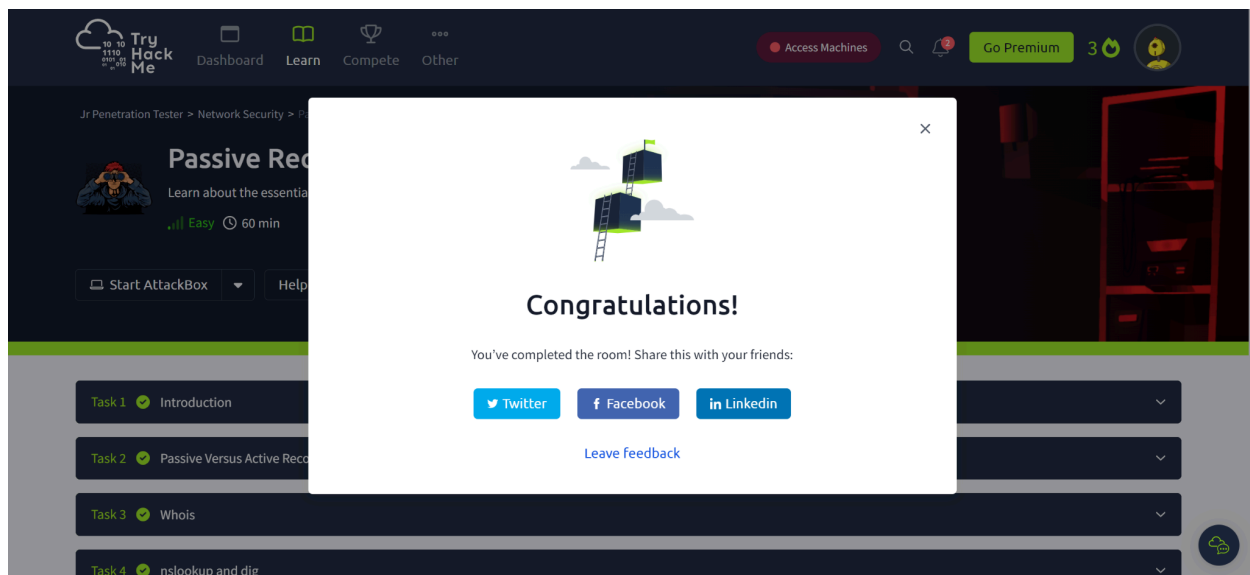
c. Based on Shodan.io, what is the 3rd most common port used for nginx?



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.