Passive Reconnaissance

(part One) Introduction :

WHOIS : The command is a command-line utility used to retrieve information about domain names, IP addresses, and network devices registered with the Internet Corporation for Assigned Names and Numbers (ICANN). It is available on most Unix-like operating systems, including Linux, macOS, and FreeBSD.whois

nslookup : The nslookup command is a network administration command-line tool for querying the Domain Name System (DNS) to obtain the mapping between domain name and IP address, or other DNS records. It is available on most Unix-like operating systems, including Linux, macOS, and FreeBSD.

dig : The dig command can be used to query a variety of DNS records, including A records (IP addresses), MX records (mail exchanger records), NS records (name server records), and TXT records (text records). It can also be used to query the DNS servers that are authoritative for a particular domain name.

(The second part) Passive Versus Active Recon :

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 : **p**

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)

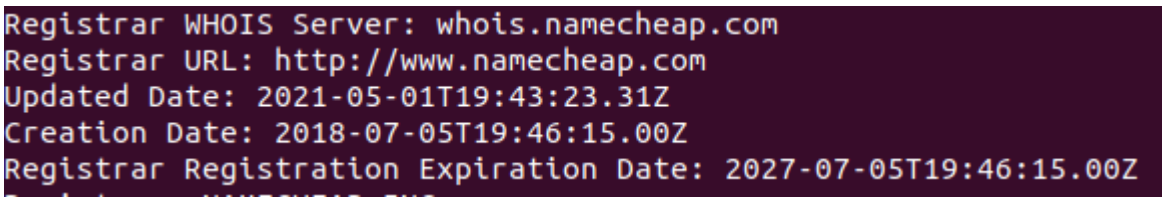
The answer : **a**

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 : **a**

(the third part) Whois :

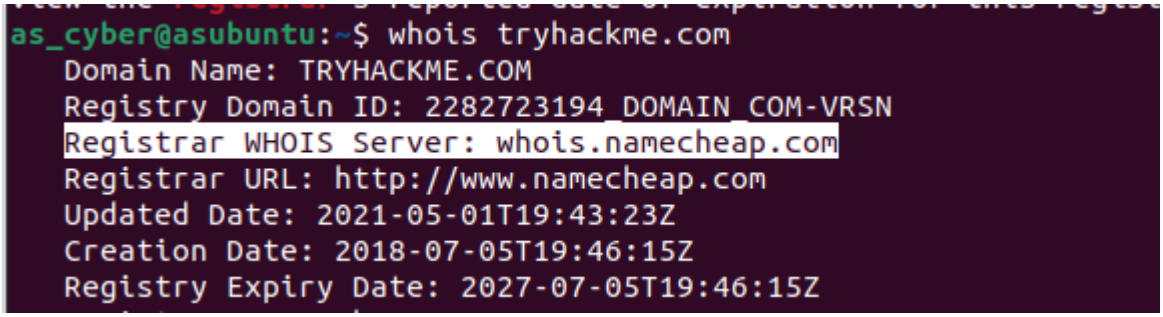
-When was TryHackMe.com registered?



Creation Date: 2018-07-05T19:46:15.00Z

The answer : **20180705**

What is the registrar of TryHackMe.com?



Registrar URL: http://www.namecheap.com

The answer : **namecheap.com**

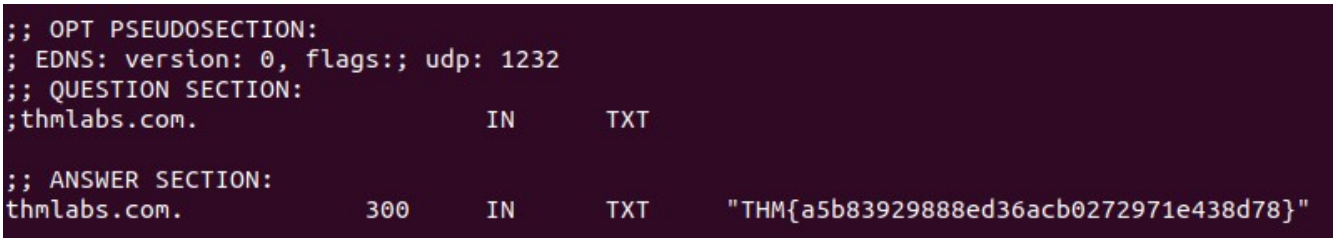
Which company is TryHackMe.com using for name servers?

The answer : **CLOUDFLARE.COM**

(part Four)nslookup and dig

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

The answer : **"THM{a5b83929888ed36acb0272971e438d78}"**



(Fifth part) DNSDumpster

DNSDumpster is a free online tool that can be used to gather information about domain names, including:

-IP addresses
-Name servers
-MX records
-TXT records
-Reverse DNS lookups
-Subdomains

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

-You will go to https://dnsdumpster.com/
-Then you will search for (tryhackme.com)

The answer : **remote**

(The sixth part) Shodan.io

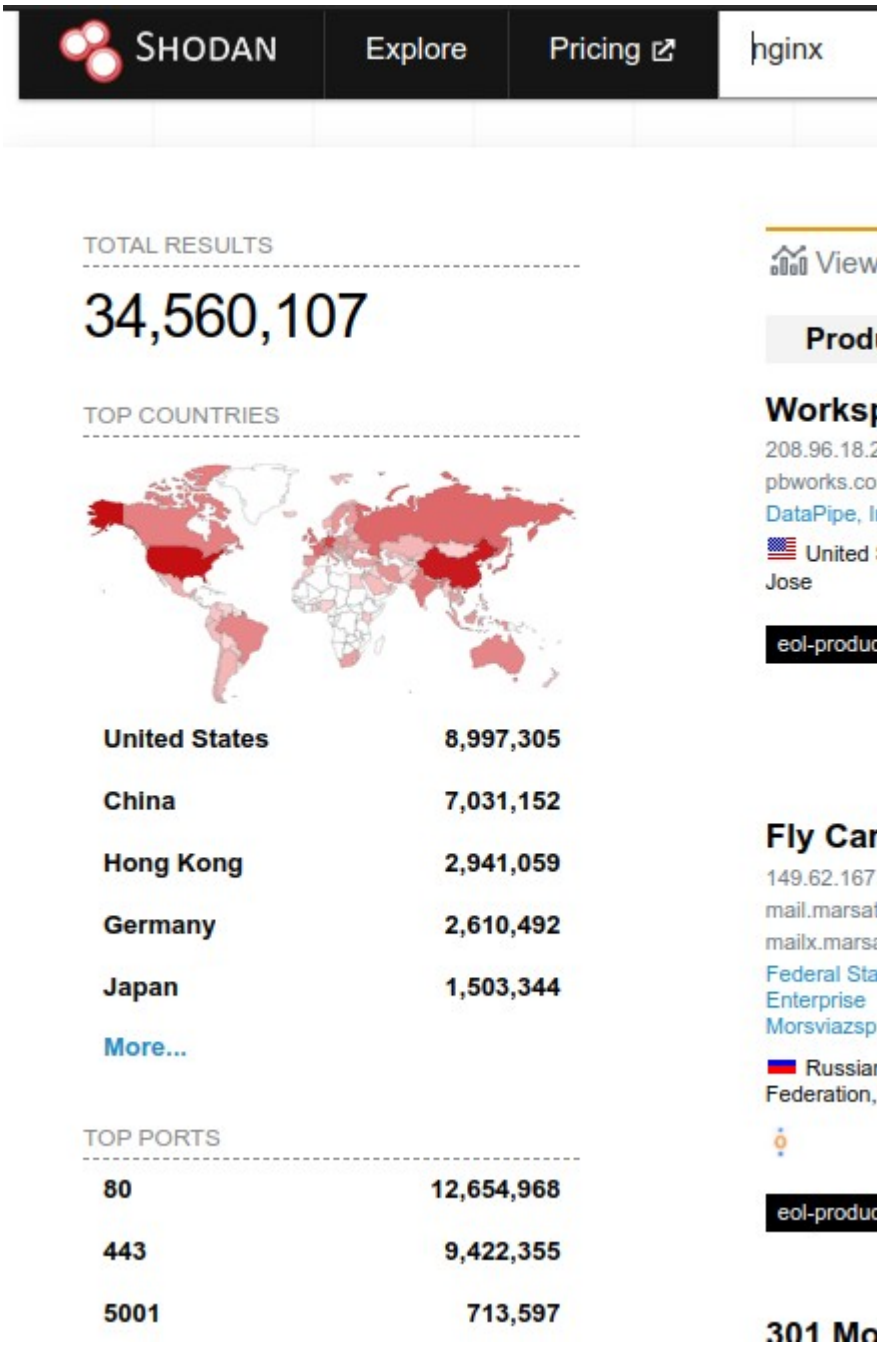
Shodan works by scanning the Internet and collecting information about devices and services, including servers, routers, webcams, industrial control systems, and more. This information is then indexed and made available to users through the Shodan search engine.

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

The answer : **Germany**

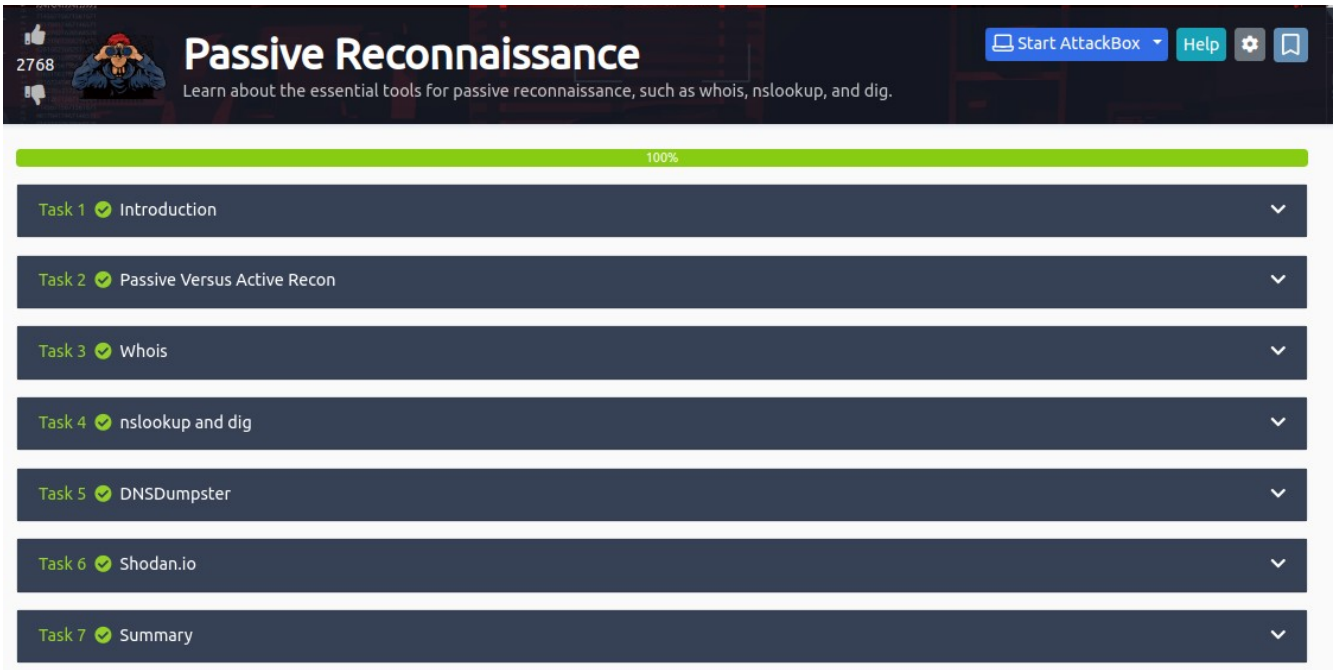
Based on Shodan.io, what is the 3rd most common port used for Apache?

The answer : **8080**



Summary

Purpose	Commandline Example
Lookup WHOIS record	Whois tryhackme.com
Lookup DNS A records	nslookup -type=A tryhackme.com
Lookup DNS MX records at DNS server	Nslookup tryhackme.com 1.1.1.1
Lookup DNS TXT records	nslookup -type=TXT tryhackme.com
Lookup DNS A records	dig tryhackme.com A
Lookup DNS MX records at DNS server	dig @1.1.1.1 tryhackme.com MX
Lookup DNS TXT records	dig tryhackme.com TXT



-Thanks for reading my report

BY : Abdelwahab Ahmed Shandy