Passive Reconnaissance

Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.

Task 1: Introduction

we will explore command-line tools like whois, nslookup, and dig for querying WHOIS and DNS servers, as well as online services like DNSDumpster and Shodan.io for gathering target information without direct connections.

Task 2: Passive Versus Active Recon

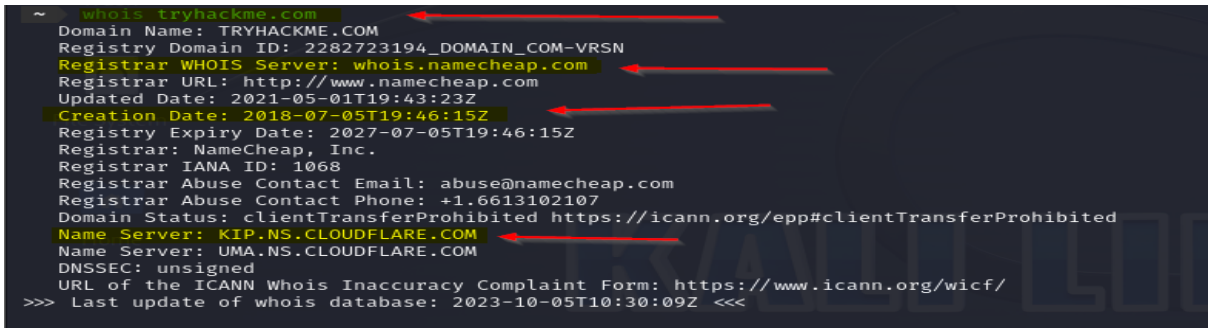
Passive reconnaissance lets you access publicly available resources without directly engaging with the target while Active reconnaissance requires direct engagement with the target.

Question	Answer
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)	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)	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)	A

Task 3: Whois

Whois function is a tool used to retrieve information about domain names, IP addresses, and other entities registered with a domain registrar.

- Syntax is **whois [DOMAIN_NAME]**
- To get answers to the questions, type **"whois tryhackme.com"**



Question	Answer
When was TryHackMe.com registered?	20180705
What is the registrar of TryHackMe.com?	NameCheap.com
Which company is TryHackMe.com using for name servers?	CLOUDFLARE.COM

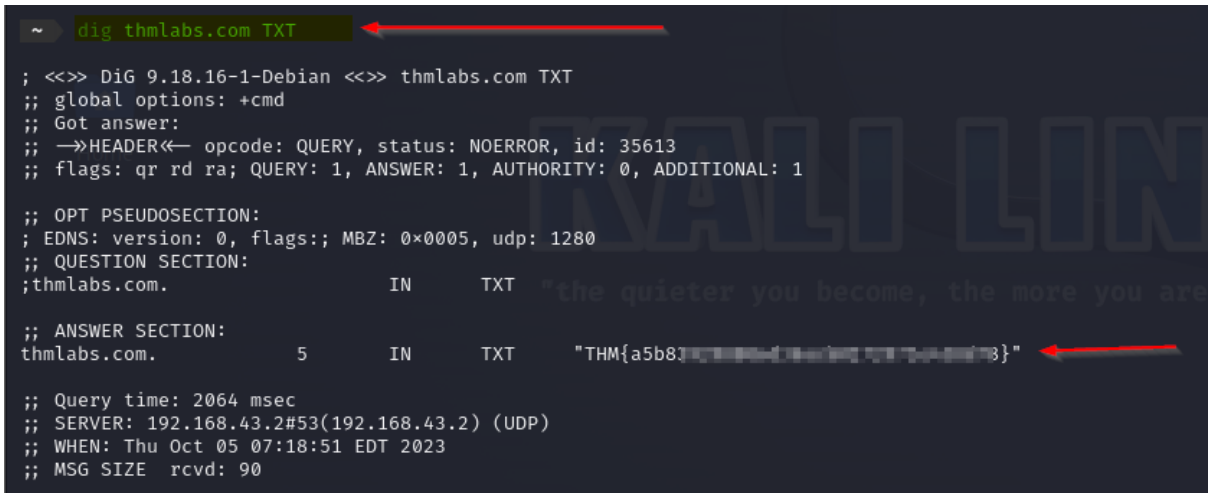
Task 4: nslookup and dig

Nslookup is a tool used to find the IP address of a domain name, syntax is **"nslookup DOMAIN_NAME"**

- You can also use the syntax **"nslookup OPTIONS DOMAIN_NAME SERVER"** where options is the query type and the server is the DNS server you want to query.
- Example: to query the mail server of tryhackme.com is **"nslookup -type=MX tryhackme 1.1.1.1".**

Domain Information Groper(dig) is a tool used for more advanced DNS queries and additional functionality.

- Syntax is **"dig DOMAIN_NAME"**, **"dig DOMAIN_NAME TYPE"** is syntax to specify the record type. If you want to select the server we want to query **"dig @SERVER DOMAIN_NAME TYPE"**



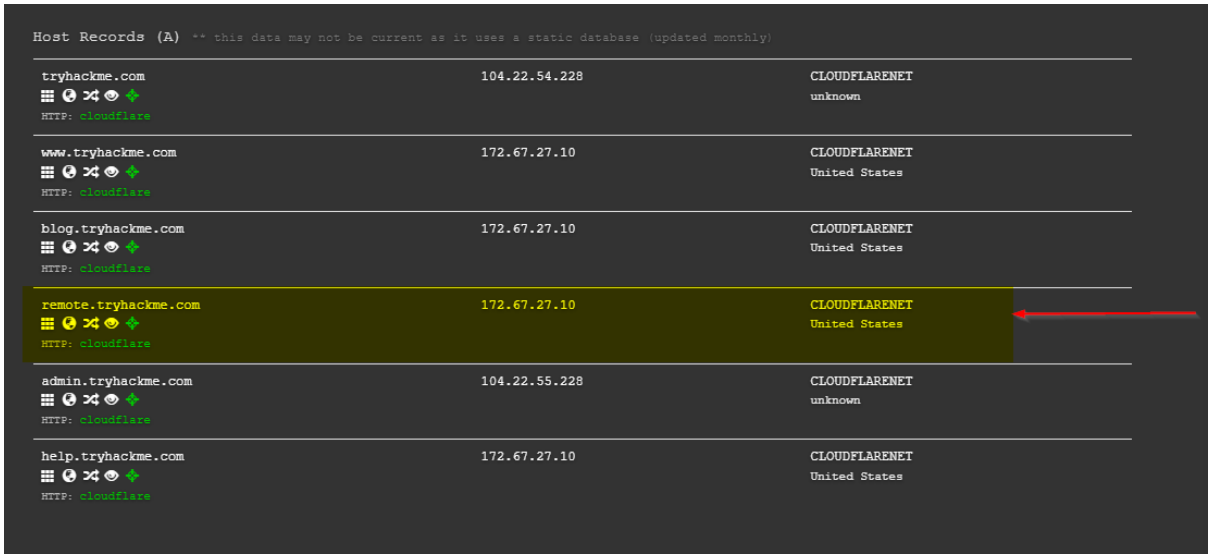
Question	Answer
Check the TXT records of thmlabs.com. What is the flag there?	THM{a5b8**********}

Task 5: DNSDumpster

DNSDumpster is the tool used to find subdomains

- To solve the task, go to the dumpster link: https://dnsdumpster.com/

➢ Search /lookup tryhackme.com

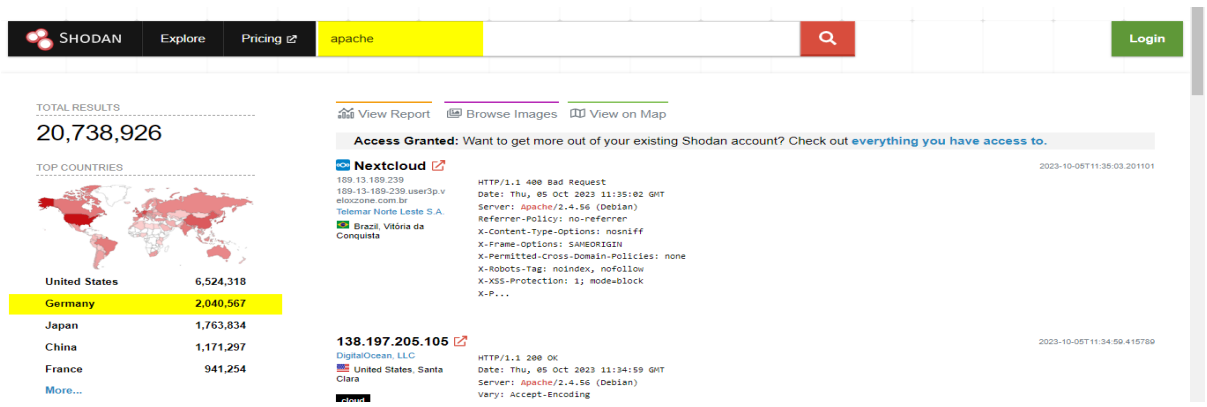


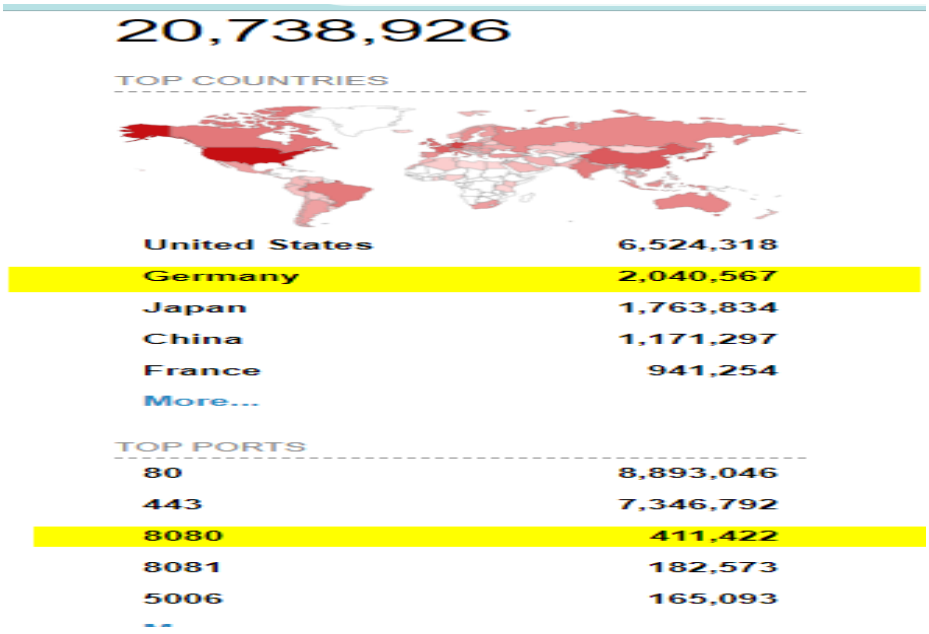
Question	Answer
Lookup tryhackme.com on DNSDumpster. What is one interesting subdomain that you would discover in addition to www and blog?	remote

Task 6: Shodan.io

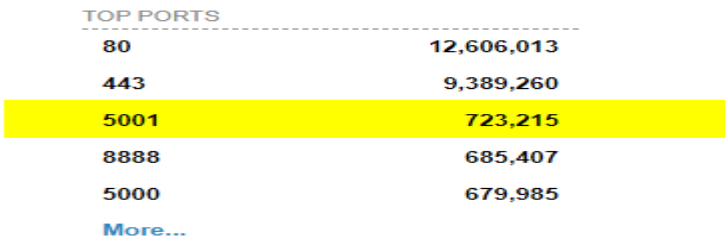
- Shodan.io is a unique search engine that discovers and indexes information about internet-connected devices and systems. It doesn't require active connections but collects data from devices it encounters online
- Shodan.io connects to online devices, retrieves information about their services, and stores it in a searchable database.

➢ To solve the task, go to shodan.io official website: https://www.shodan.io/
➢ Search for Apache





- Search for nginx too



Question	Answer
According to Shodan.io, what is the 2nd country in the world in terms of the number of publicly accessible Apache servers?	Germany
Based on Shodan.io, what is the 3rd most common port used for Apache?	8080
Based on Shodan.io, what is the 3rd most common port used for nginx?	5001

ADD TO YOUR PERSONAL TOOL LIST

Tools	Syntax
whois	whois [DOMAIN_NAME]
Nslookup	nslookup [DOMAIN_NAME]
Nslookup with options and server	nslookup [OPTIONS] [DOMAIN_NAME] [SERVER]
Dig	dig [DOMAIN_NAME]
Dig with type	dig DOMAIN_NAME TYPE
Dis with type and server	dig [@SERVER] [DOMAIN_NAME] [TYPE]