Passive Recon

Introduction

The learner is going dive deep into Network Security and cover areas in: Passive reconnaissance, Active reconnaissance, Nmap Live Host Discovery, Nmap Basic Port Scans, Nmap Post Port Scans, Protocols and Servers, Protocols and Servers 2 and Network Security Challenge.

Activities

Task 1: Introduction

Task 2: Passive Versus Active Recon

Reconnaissance can be put into the following classifications:

1. **Passive Recon**: can be carried out by watching passively
2. **Active Recon**: requires interacting with the target to provoke it in order to observe its response.

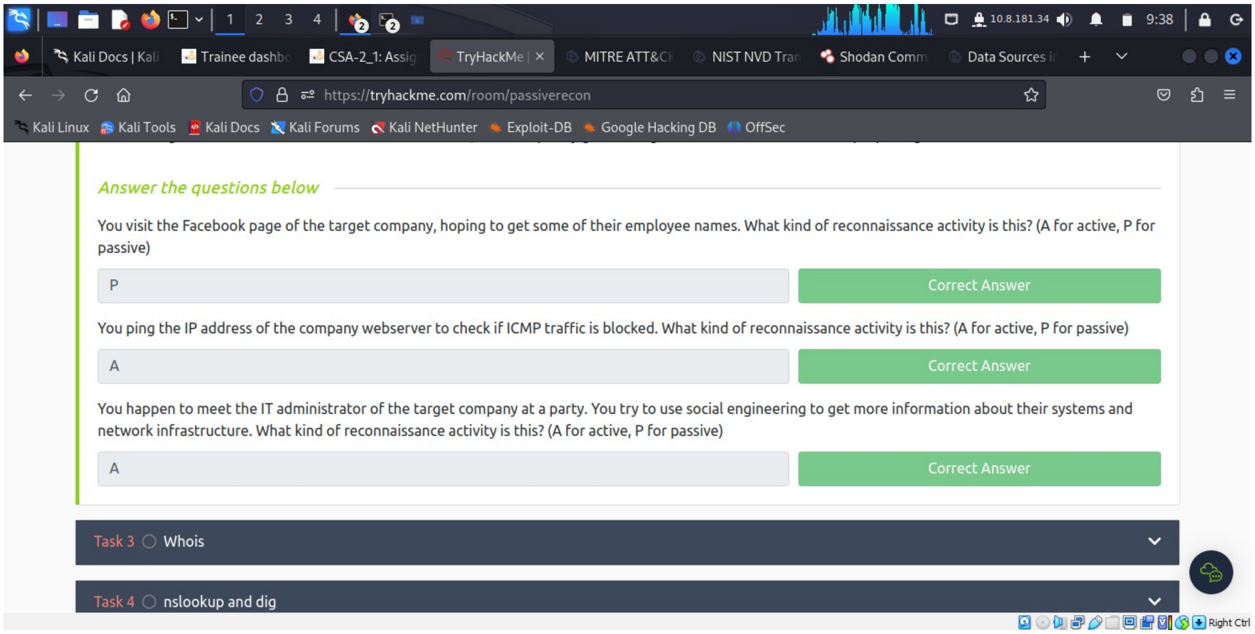
Passive recon doesn't require interacting with the target and relies on publicly available information that is collected and maintained by a third party.

Active recon requires interacting with the target by sending requests and packets and observing if and how it responds. An example of active reconnaissance is using Nmap to scan target subnets and live hosts.

Active recon can be classified as:

External Recon: Conducted outside the target's network and focuses on the externally facing assets assessable from the Internet. One example is running Nikto from outside the company network.

Internal Recon: Conducted from within the target company's network. In other words, the pentester or red teamer might be physically located inside the company building. In this scenario, they might be using an exploited host on the target's network. An example would be using Nessus to scan the internal network using one of the target’s computers.



Answer the questions below

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 — Correct Answer

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 — Correct Answer

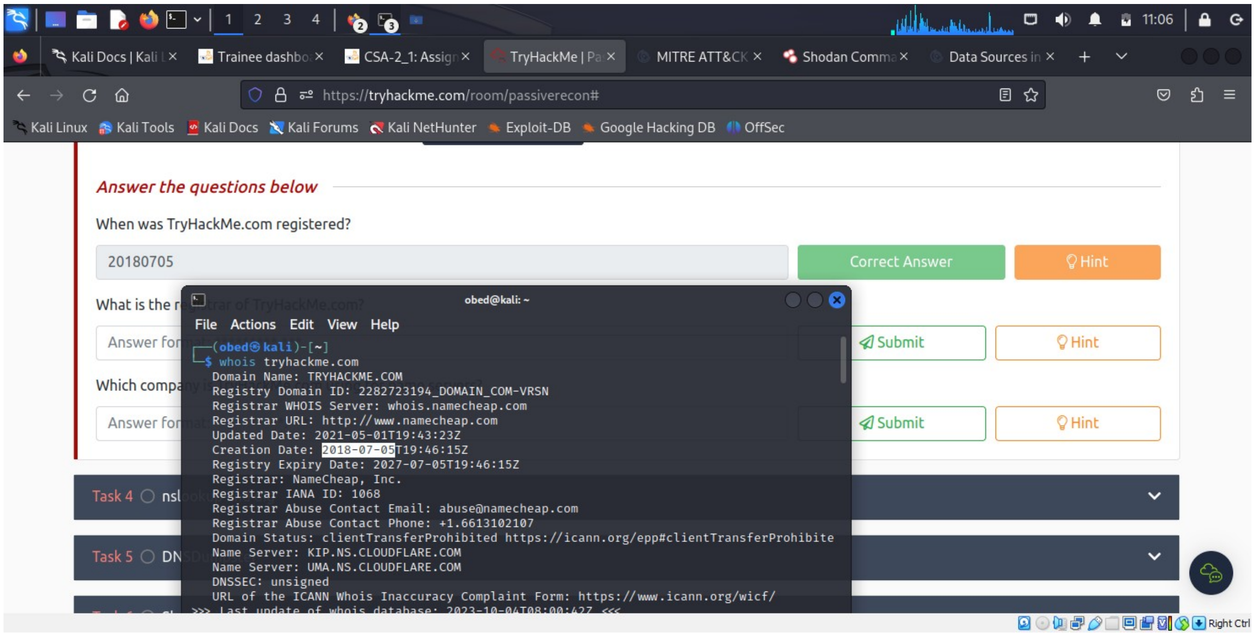
You happen to meet the IT administrator of the target company at a party. You try to use social engineering to get more information about their systems and network infrastructure. What kind of reconnaissance activity is this? (A for active, P for passive)

A — Correct Answer

Task 3 ○ Whois

Task 4 ○ nslookup and dig

Task 3: Whois



Answer the questions below

When was TryHackMe.com registered?

20180705 — Correct Answer

What is the r

Answer for

Which compa

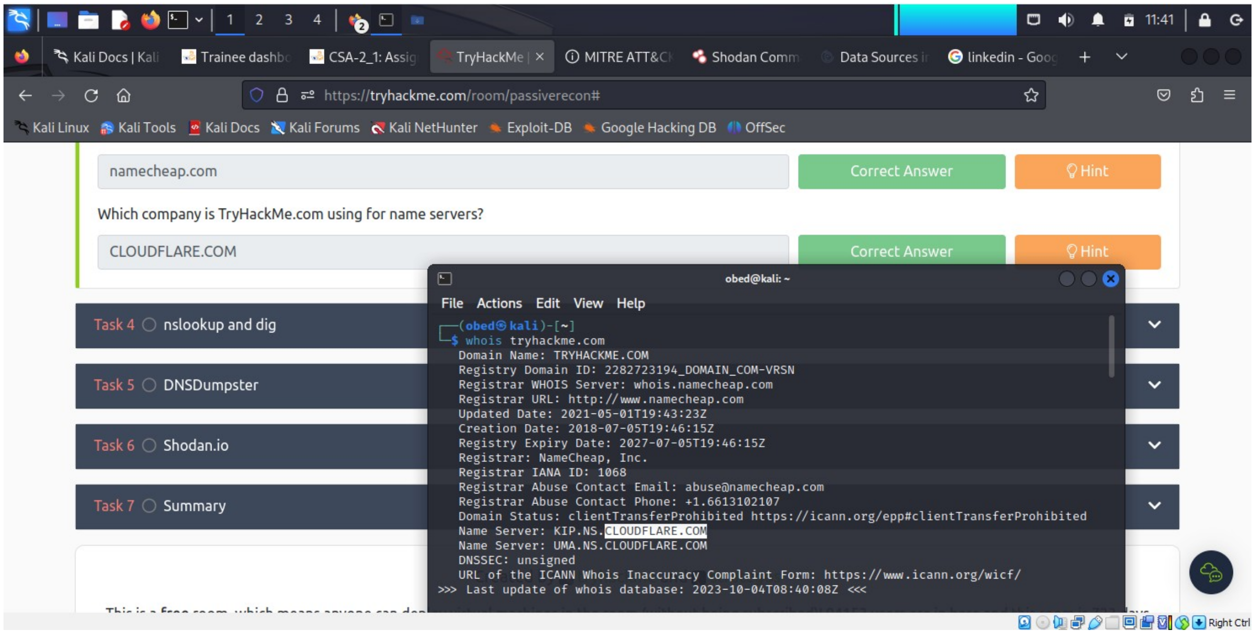
Answer for

Task 4 ○ nsl

Task 5 ○ DN

```
┌──(obed㉿kali)-[~]
└─$ 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#clientTransferProhibite
   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: 2023-10-04T08:00:42Z <<<
```

The company that TryHackMe.com is using for name servers is **cloudfare.com**



https://tryhackme.com/room/passiverecon#

namecheap.com

Which company is TryHackMe.com using for name servers?

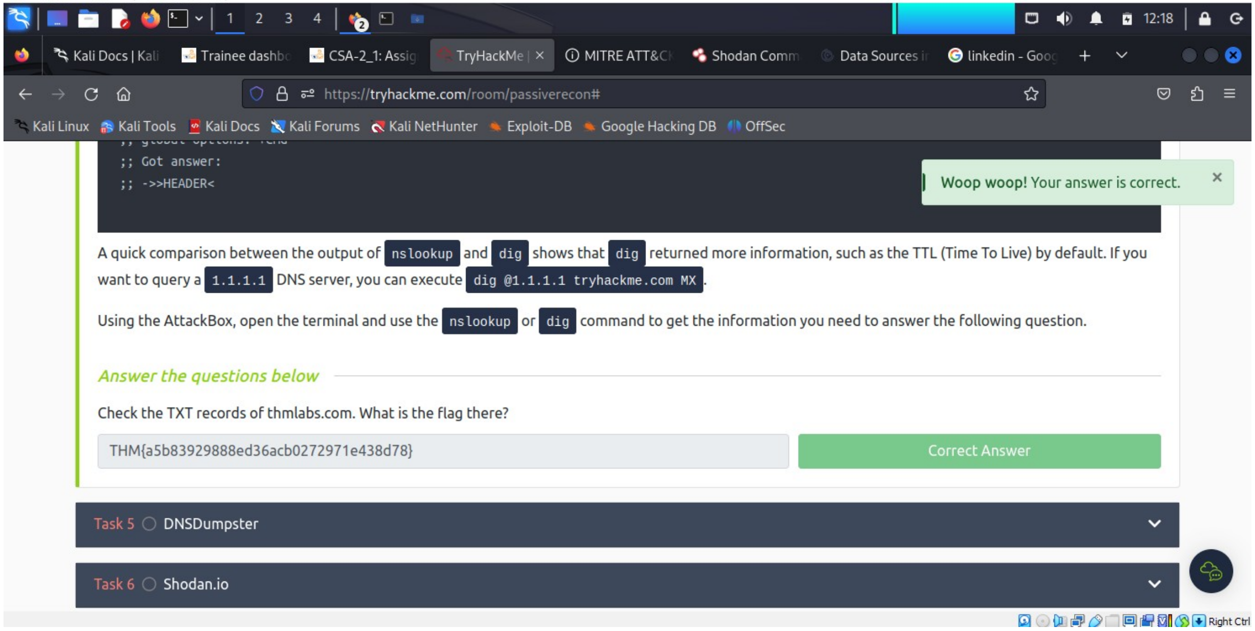
CLOUDFLARE.COM

```
┌──(obed㉿kali)-[~]
└─$ 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: 2023-10-04T08:40:08Z <<<
```

Task 4: nslookup and dig

The learner being familiar with **whois** command, now they use in this task – **nslookup (Name Server Look Up).** The command syntax is **nslookup DOMAIN_NAME SERVER. Server** refers to the DNS server that is to be queried.

Domain Information Groper (dig) – is an advanced DNS query with additional functionality. The syntax is **dig DOMAIN_NAME TYPE.** To select the server needed to be queried the syntax is **dig @SERVER DOMAIN_NAME TYPE.**



```
;; Got answer:
;; ->>HEADER<
```

Woop woop! Your answer is correct.

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.

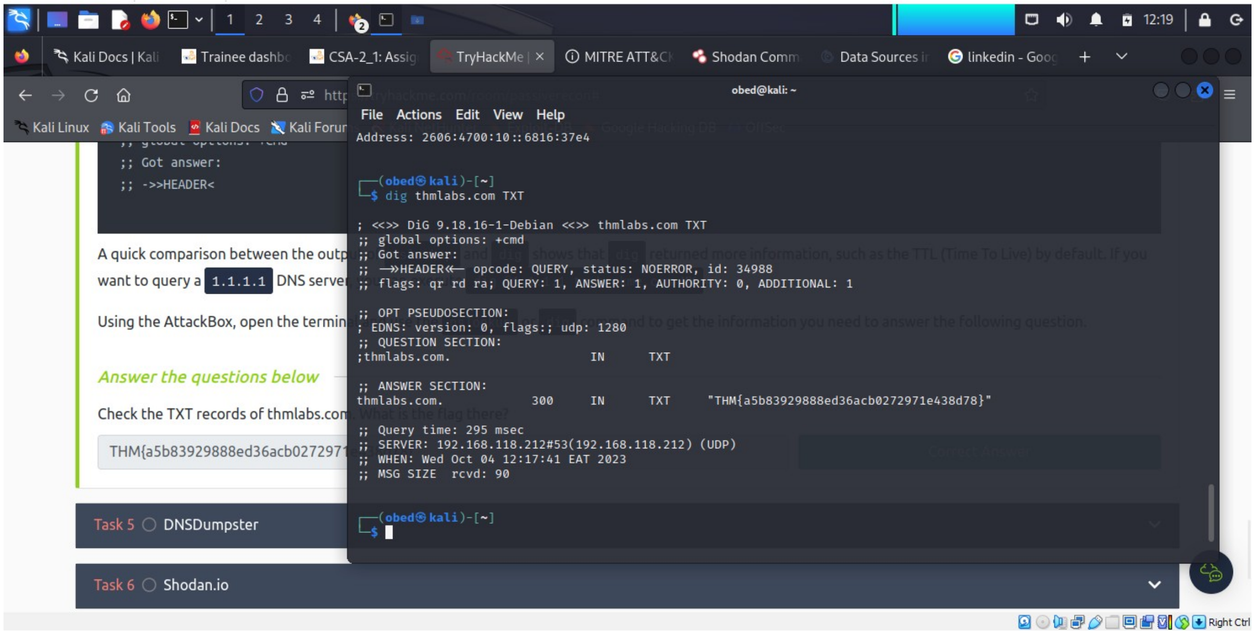
Answer the questions below

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

THM{a5b83929888ed36acb0272971e438d78} | Correct Answer

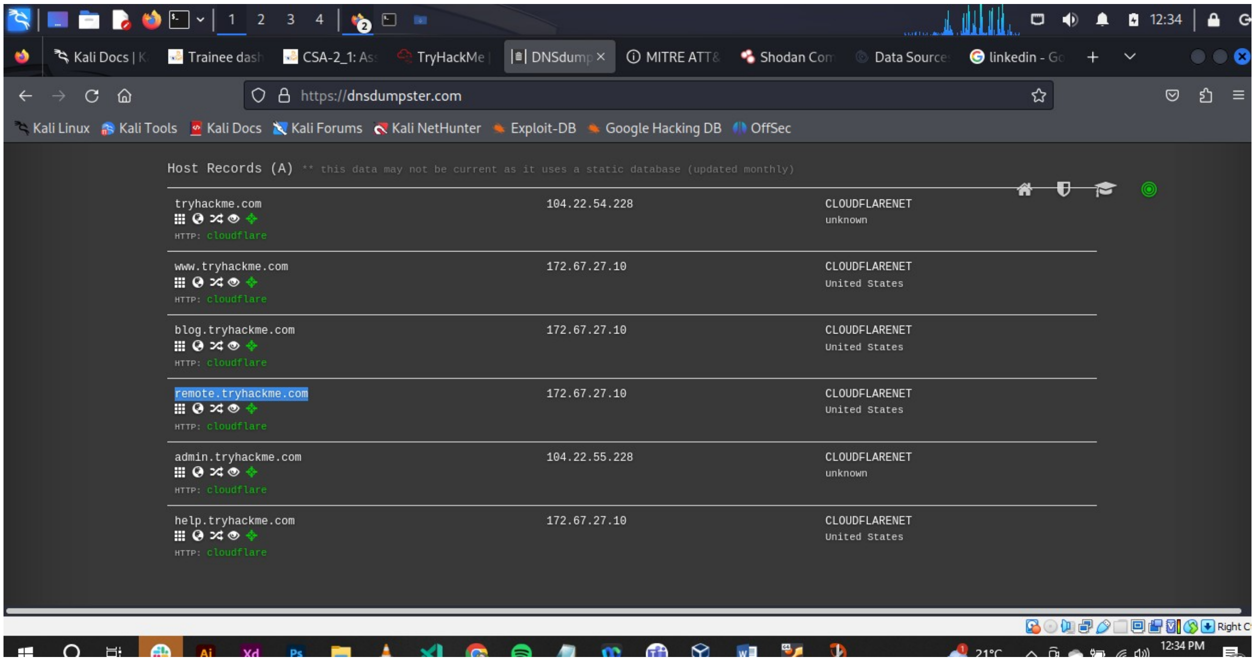
Task 5 ○ DNSDumpster

Task 6 ○ Shodan.io



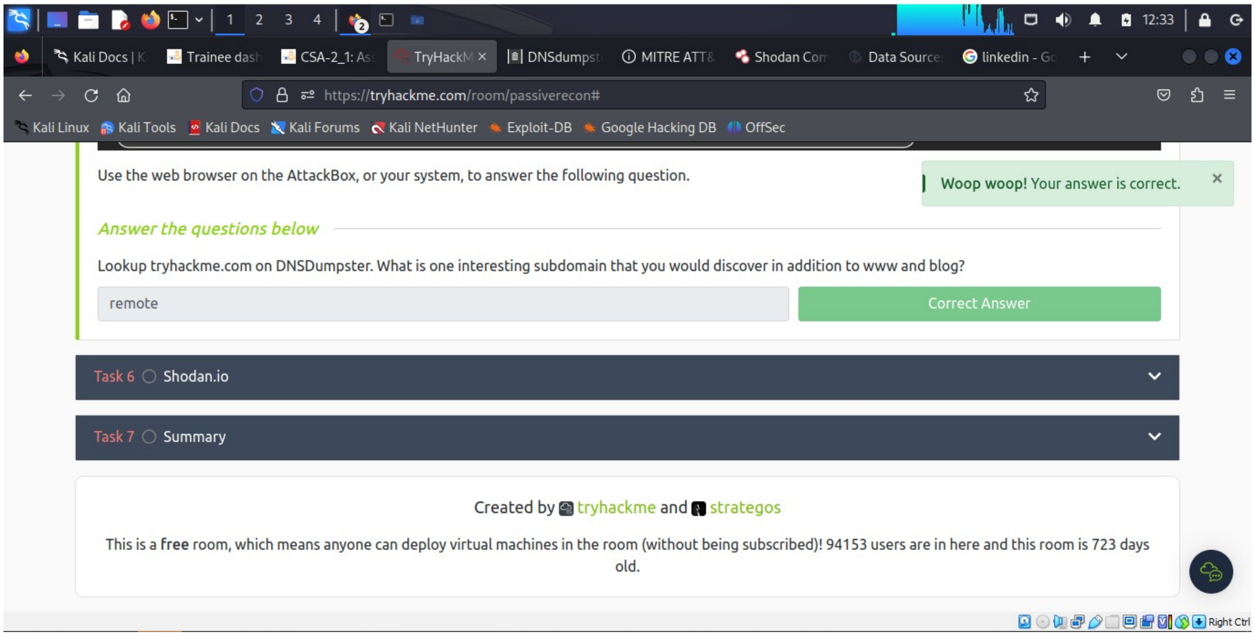
```
Address: 2606:4700:10::6816:37e4


┌──(obed㉿kali)-[~]
└─$ dig thmlabs.com TXT

; <<>> DiG 9.18.16-1-Debian <<>> thmlabs.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34988
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;thmlabs.com.                   IN      TXT

;; ANSWER SECTION:
thmlabs.com.            300     IN      TXT     "THM{a5b83929888ed36acb0272971e438d78}"

;; Query time: 295 msec
;; SERVER: 192.168.118.212#53(192.168.118.212) (UDP)
;; WHEN: Wed Oct 04 12:17:41 EAT 2023
;; MSG SIZE  rcvd: 90


┌──(obed㉿kali)-[~]
└─$ 
```

Task 5: DNSDumpster



Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

tryhackme.com HTTP: cloudflare	104.22.54.228	CLOUDFLARENET unknown
www.tryhackme.com HTTP: cloudflare	172.67.27.10	CLOUDFLARENET United States
blog.tryhackme.com HTTP: cloudflare	172.67.27.10	CLOUDFLARENET United States
remote.tryhackme.com HTTP: cloudflare	172.67.27.10	CLOUDFLARENET United States
admin.tryhackme.com HTTP: cloudflare	104.22.55.228	CLOUDFLARENET unknown
help.tryhackme.com HTTP: cloudflare	172.67.27.10	CLOUDFLARENET United States



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

Woop woop! Your answer is correct.

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

Task 6 ○ Shodan.io

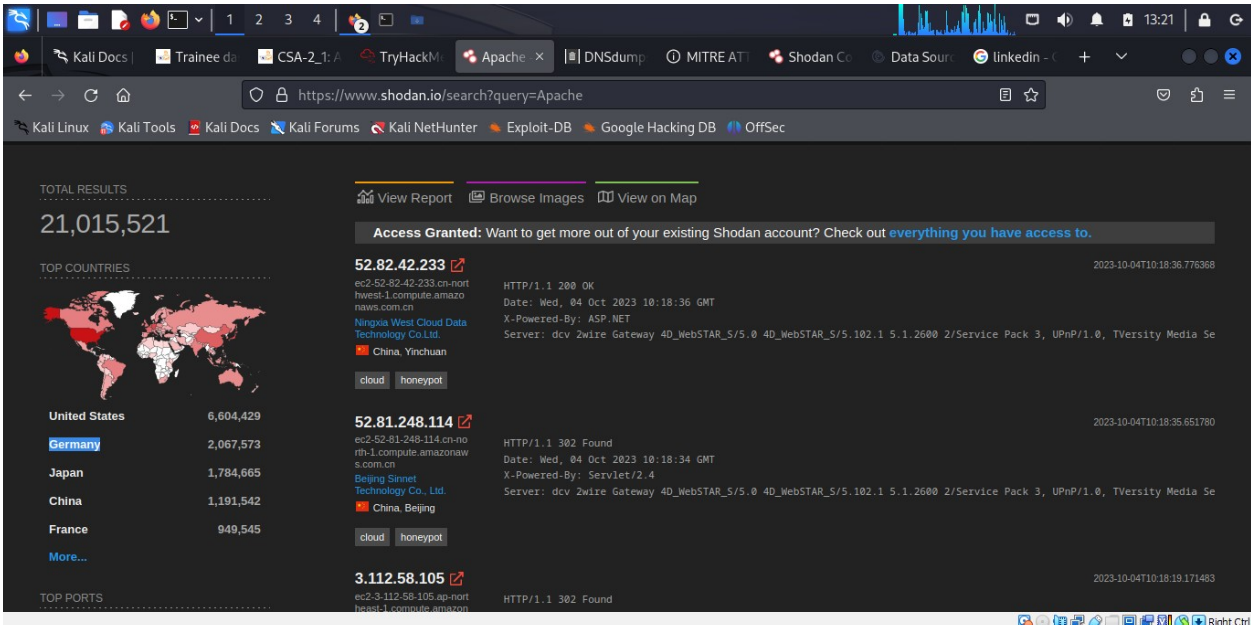
Task 7 ○ Summary

Created by tryhackme and strategos

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 94153 users are in here and this room is 723 days old.

Task 6: Shodan.io

The learner is equipped with s service like Shodan.io knowledge which is helpful to learn various pieces of information about the client’s network, without actively connecting to it.


1 2 3 4
13:21
Kali Docs | Trainee da CSA-2_1: A TryHackM Apache × DNSdump MITRE AT Shodan Co Data Sourc linkedin -
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
View Report
Browse Images
View on Map
cloud
honeypot
Right Ctrl

https://www.shodan.io/search?query=Apache

TOTAL RESULTS

21,015,521

TOP COUNTRIES

United States	6,604,429
Germany	2,067,573
Japan	1,784,665
China	1,191,542
France	949,545
More...	

TOP PORTS

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

52.82.42.233
ec2-52-82-42-233.cn-northwest-1.compute.amazonaws.com.cn
Ningxia West Cloud Data Technology Co.Ltd.
China, Yinchuan
2023-10-04T10:18:36.776368

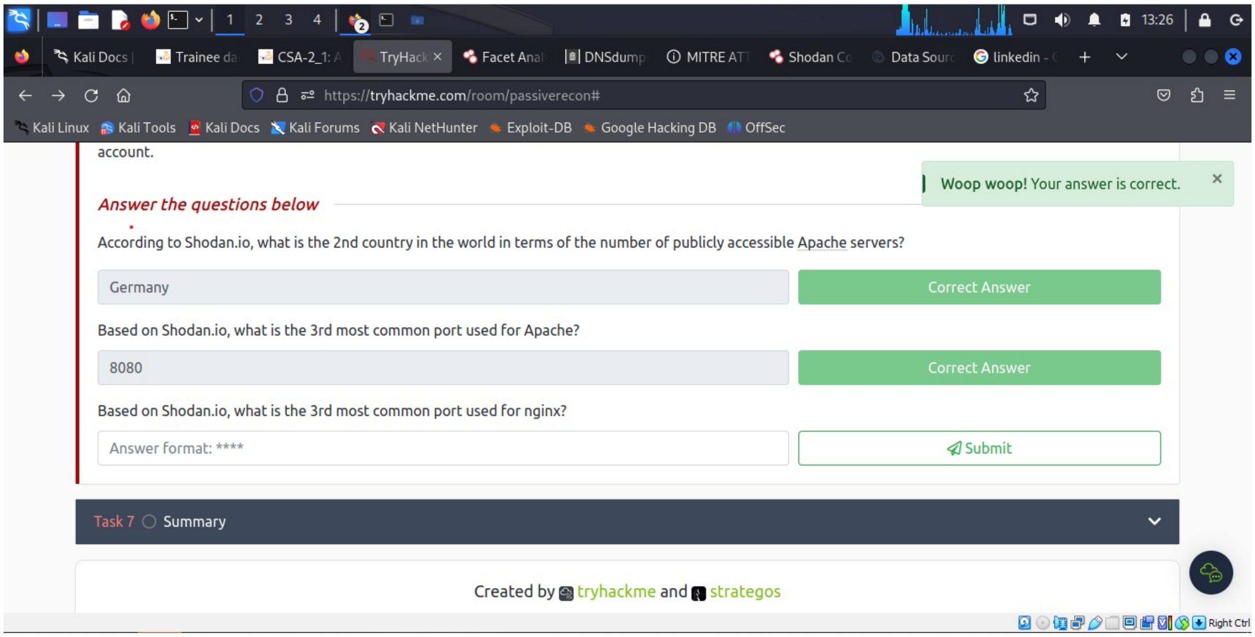
```
HTTP/1.1 200 OK
Date: Wed, 04 Oct 2023 10:18:36 GMT
X-Powered-By: ASP.NET
Server: dcv 2wire Gateway 4D_WebSTAR_S/5.0 4D_WebSTAR_S/5.102.1 5.1.2600 2/Service Pack 3, UPnP/1.0, TVersity Media Se
```

52.81.248.114
ec2-52-81-248-114.cn-north-1.compute.amazonaws.com.cn
Beijing Sinnet Technology Co., Ltd.
China, Beijing
2023-10-04T10:18:35.651780

```
HTTP/1.1 302 Found
Date: Wed, 04 Oct 2023 10:18:34 GMT
X-Powered-By: Servlet/2.4
Server: dcv 2wire Gateway 4D_WebSTAR_S/5.0 4D_WebSTAR_S/5.102.1 5.1.2600 2/Service Pack 3, UPnP/1.0, TVersity Media Se
```

3.112.58.105
ec2-3-112-58-105.ap-northeast-1.compute.amazon
2023-10-04T10:18:19.171483

```
HTTP/1.1 302 Found
```


1 2 3 4
13:26
Kali Docs | Trainee da CSA-2_1: A TryHack × Facet Anal DNSdump MITRE AT Shodan Co Data Sourc linkedin -
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Right Ctrl

https://tryhackme.com/room/passiverecon#

account.

Woop woop! Your answer is correct.

Answer the questions below

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

Germany

Correct Answer

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

8080

Correct Answer

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

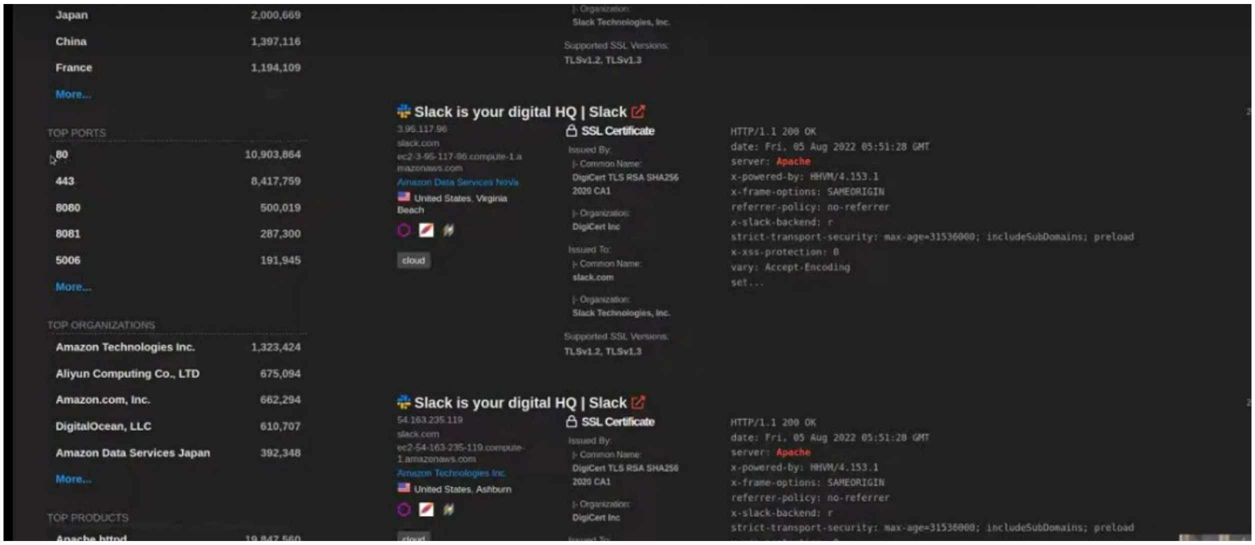
Answer format: ****

Submit

Task 7 ○ Summary

Created by tryhackme and strategos

From the Shodan.io website, the learner finds out that port **8080** is the 3rd most common port used for Apache.



Japan	2,000,669
China	1,397,116
France	1,194,109
More...	

TOP PORTS

80	10,903,864
443	8,417,759
8080	500,019
8081	287,300
5006	191,945
More...	

TOP ORGANIZATIONS

Amazon Technologies Inc.	1,323,424
Aliyun Computing Co., LTD	675,094
Amazon.com, Inc.	662,294
DigitalOcean, LLC	610,707
Amazon Data Services Japan	392,348
More...	

TOP PRODUCTS

Apache httpd	19,847,560

|- Organization:
Slack Technologies, Inc.

Supported SSL Versions:
TLSv1.2, TLSv1.3

Slack is your digital HQ | Slack

3.95.117.96
slack.com
ec2-3-95-117-96.compute-1.amazonaws.com
Amazon Data Services NoVa
United States, Virginia Beach

cloud

SSL Certificate

Issued By:
|- Common Name:
DigiCert TLS RSA SHA256 2020 CA1

|- Organization:
DigiCert Inc

Issued To:
|- Common Name:
slack.com

|- Organization:
Slack Technologies, Inc.

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
date: Fri, 05 Aug 2022 05:51:28 GMT
server: Apache
x-powered-by: HHVM/4.153.1
x-frame-options: SAMEORIGIN
referrer-policy: no-referrer
x-slack-backend: r
strict-transport-security: max-age=31536000; includeSubDomains; preload
x-xss-protection: 0
vary: Accept-Encoding
set...
```

Slack is your digital HQ | Slack

54.163.235.119
slack.com
ec2-54-163-235-119.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn

cloud

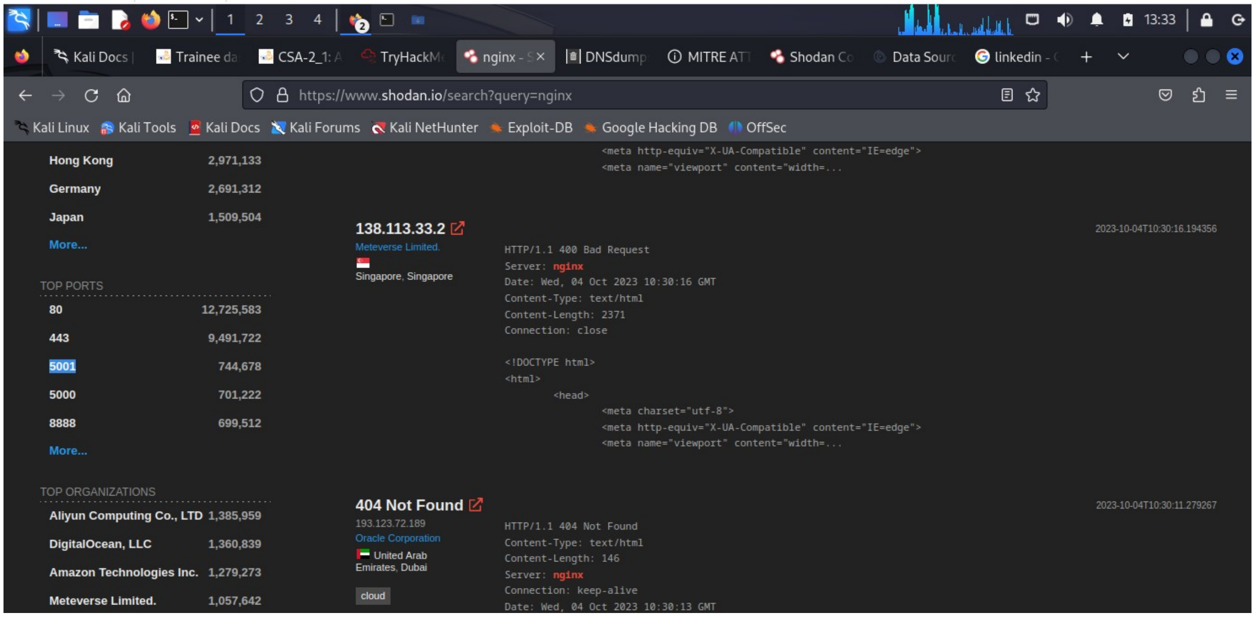
SSL Certificate

Issued By:
|- Common Name:
DigiCert TLS RSA SHA256 2020 CA1

|- Organization:
DigiCert Inc

```
HTTP/1.1 200 OK
date: Fri, 05 Aug 2022 05:51:28 GMT
server: Apache
x-powered-by: HHVM/4.153.1
x-frame-options: SAMEORIGIN
referrer-policy: no-referrer
x-slack-backend: r
strict-transport-security: max-age=31536000; includeSubDomains; preload
```

Based on Shodan.io, the 3rd most common port used for nginx is **5001**.



```
                <meta http-equiv="X-UA-Compatible" content="IE=edge">
                <meta name="viewport" content="width=...
```

Hong Kong	2,971,133
Germany	2,691,312
Japan	1,509,504
More...	

TOP PORTS

80	12,725,583
443	9,491,722
5001	744,678
5000	701,222
8888	699,512
More...	

TOP ORGANIZATIONS

Aliyun Computing Co., LTD	1,385,959
DigitalOcean, LLC	1,360,839
Amazon Technologies Inc.	1,279,273
Meteverse Limited.	1,057,642

138.113.33.2

Meteverse Limited.
Singapore, Singapore

2023-10-04T10:30:16.194356

```
HTTP/1.1 400 Bad Request
Server: nginx
Date: Wed, 04 Oct 2023 10:30:16 GMT
Content-Type: text/html
Content-Length: 2371
Connection: close

<!DOCTYPE html>
<html>
        <head>
                <meta charset="utf-8">
                <meta http-equiv="X-UA-Compatible" content="IE=edge">
                <meta name="viewport" content="width=...
```

404 Not Found

193.123.72.189
Oracle Corporation
United Arab Emirates, Dubai

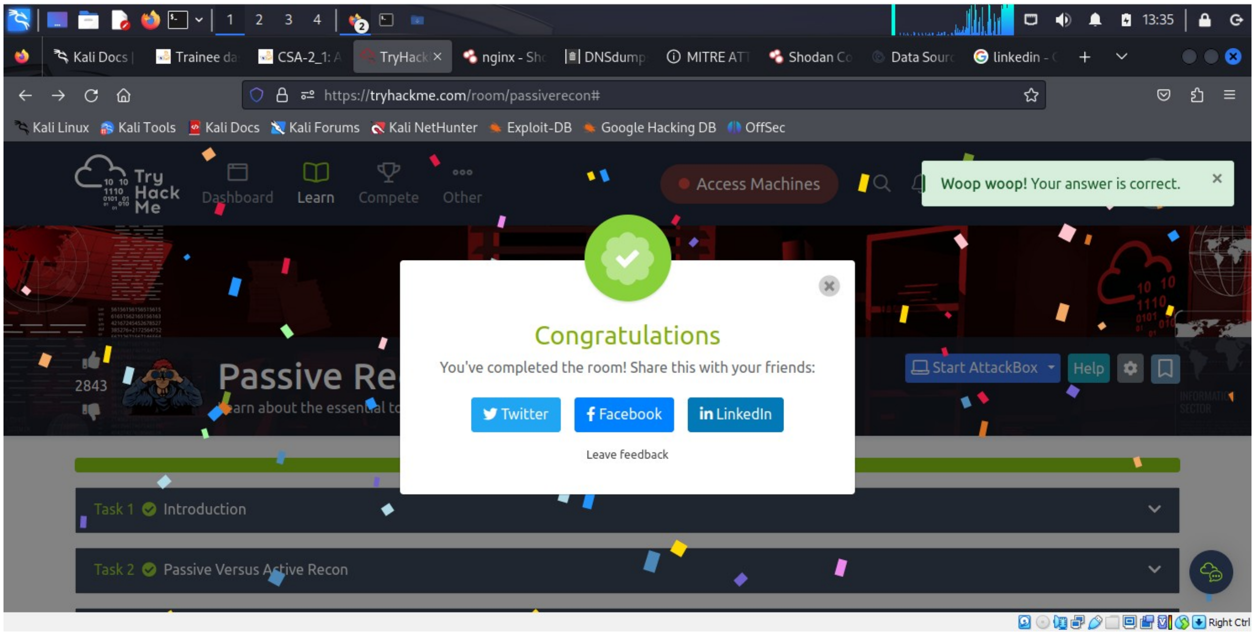
cloud

2023-10-04T10:30:11.279267

```
HTTP/1.1 404 Not Found
Content-Type: text/html
Content-Length: 146
Server: nginx
Connection: keep-alive
Date: Wed, 04 Oct 2023 10:30:13 GMT
```

Task 7: Summary

This task enabled the learner focus on passive reconnaissance. Particularly covering command-line tools, whois, nslookup, and dig. The learner also covered two publicly available services DNSDumpster and Shodan.io. The power of such tools is that it enables collection of information about the targets without directly connecting to them.



https://tryhackme.com/room/passiverecon#

Woop woop! Your answer is correct.

Passive Re

arn about the essential t

Congratulations

You've completed the room! Share this with your friends:

Task 1 Introduction

Task 2 Passive Versus Active Recon

Conclusion

This task enabled the learner focus on passive reconnaissance. Particularly covering command-line tools, whois, nslookup, and dig. The learner also covered two publicly available services DNSDumpster and Shodan.io. The power of such tools is that it enables collection of information about the targets without directly connecting to them.