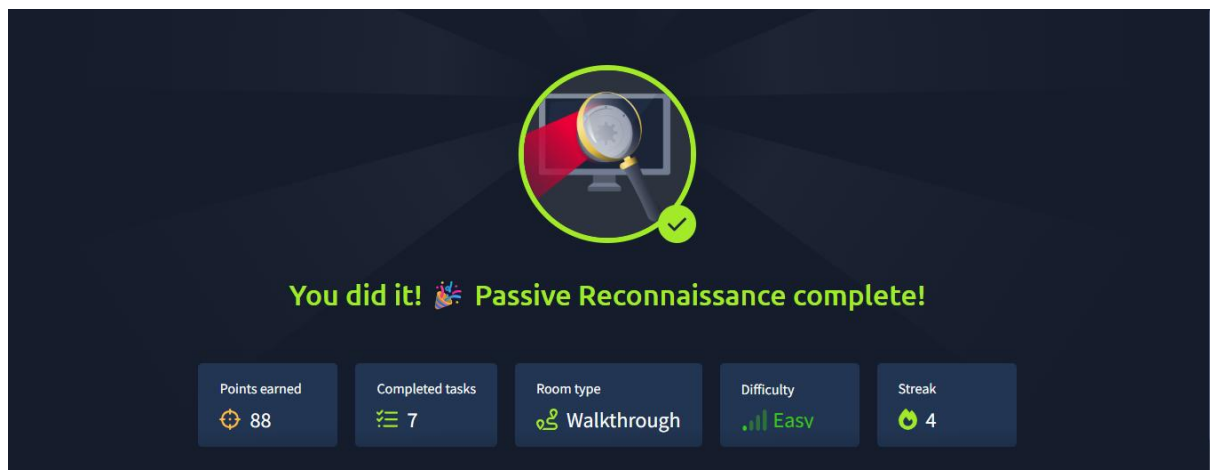


**NAME: Diana Wanjiru**

**ADMISSION NUMBER: CS-EH02-24103**

**LINK (Completed Module):**

<https://tryhackme.com/room/passiverecon?shareId=6606f1847d6a4dfe0cae29a5>



## **PASSIVE RECONNAISSANCE (TRY HACK ME)**

### **Introduction**

Reconnaissance is the information-gathering phase of an attack, where attackers research a target to identify vulnerabilities and plan an exploit. This room takes me deeper into understanding about how to do reconnaissance as an ethical hacker or penetration tester.

### **Passive VS Active Recon**

I got to understand the difference between passive and active recon where passive recon involves you relying on publicly available knowledge. It is the knowledge that you can access from publicly available resources without directly engaging with the target. On the other hand, active recon requires direct engagement with the target.

I answered the questions that followed based on the knowledge gained in this room. Here is the screenshot.

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

## Whois

Looking at this room, I learned that Whois is a request and response protocol that follows the [RFC 3912](#) specification. It listens on TCP port 43 for incoming requests. The WHOIS server replies with various information related to the domain requested.

I did some questions that followed which needed me to use **whois tryhackme.com** where I got the answers from the output. Below are the screenshots.

## File Actions Edit View Help

```
2025-10-04 21:01:23 VERIFY OK: depth=1, CN=ChangeMe
2025-10-04 21:01:23 VERIFY KU OK
2025-10-04 21:01:23 Validating certificate extended key usage
2025-10-04 21:01:23 ++ Certificate has EKU (str) TLS Web Server Authentication,
2025-10-04 21:01:23 VERIFY EKU OK
2025-10-04 21:01:23 VERIFY OK: depth=0, CN=server
2025-10-04 21:01:24 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384
its X25519
2025-10-04 21:01:24 [server] Peer Connection Initiated with [AF_INET]18.202.129.19
2025-10-04 21:01:24 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-10-04 21:01:24 TLS: tls_multi_process: initial untrusted session promoted to
2025-10-04 21:01:24 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-10-04 21:01:24 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0/24
255.255.128.0,route-metric 1000,comp-lzo no,route-gateway 10.8.0.1,topology subnet
6-CBC'
2025-10-04 21:01:24 OPTIONS IMPORT: --ifconfig/up_options modified
```

```
File Actions Edit View Help

2025-10-04 21:01:23 VERIFY OK: depth=1, CN=ChangeMe
2025-10-04 21:01:23 VERIFY KU OK
2025-10-04 21:01:23 Validating certificate extended key usage
2025-10-04 21:01:23 ++ Certificate has EKU (str) TLS Web Server Authentication, ex
2025-10-04 21:01:23 VERIFY EKU OK
2025-10-04 21:01:23 VERIFY OK: depth=0, CN=server
2025-10-04 21:01:24 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384
its X25519
2025-10-04 21:01:24 [server] Peer Connection Initiated with [AF_INET]18.202.129.19
2025-10-04 21:01:24 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-10-04 21:01:24 TLS: tls_multi_process: initial untrusted session promoted to
2025-10-04 21:01:24 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-10-04 21:01:24 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0/24
255.255.128.0,route-metric 1000,comp-lzo no,route-gateway 10.8.0.1,topology subnet
6-CBC'
2025-10-04 21:01:24 OPTIONS IMPORT: --ifconfig/up_options modified
2025-10-04 21:01:24 OPTIONS IMPORT: route options modified
2025-10-04 21:01:24 OPTIONS IMPORT: route-related options modified
2025-10-04 21:01:24 net_route_v4_best_gw query: dst 0.0.0.0
2025-10-04 21:01:24 net_route_v4_best_gw result: via 10.0.2.2 dev eth0
2025-10-04 21:01:24 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFAACE=eth0 HWADDR=08:00:27:00:00:02
2025-10-04 21:01:24 TUN/TAP device tun0 opened
2025-10-04 21:01:24 net_iface_mtu_set: mtu 1500 for tun0
2025-10-04 21:01:24 net_iface_up: set tun0 up
2025-10-04 21:01:24 net_addr_v4_add: 10.8.108.154/16 dev tun0
2025-10-04 21:01:24 net_route_v4_add: 10.10.0.0/16 via 10.8.0.1 dev [NULL] table 0
2025-10-04 21:01:24 net_route_v4_add: 10.101.0.0/16 via 10.8.0.1 dev [NULL] table
2025-10-04 21:01:24 net_route_v4_add: 10.103.0.0/16 via 10.8.0.1 dev [NULL] table
2025-10-04 21:01:24 net_route_v4_add: 10.201.0.0/17 via 10.8.0.1 dev [NULL] table
2025-10-04 21:01:24 Initialization Sequence Completed
2025-10-04 21:01:24 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 45
2025-10-04 21:01:24 Timers: ping 5, ping-restart 120

64 bytes from 10.10.10.10: icmp_seq=7 ttl=63 time=167 ms
64 bytes from 10.10.10.10: icmp_seq=8 ttl=63 time=164 ms
64 bytes from 10.10.10.10: icmp_seq=9 ttl=63 time=167 ms
64 bytes from 10.10.10.10: icmp_seq=10 ttl=63 time=168 ms
^C
-- 10.10.10.10 ping statistics --
10 packets transmitted, 10 received, 0% packet loss, time 9240ms
rtt min/avg/max/mdev = 164.039/168.170/178.026/4.366 ms

(kali@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: 2025-05-11T14:06:02Z
Creation Date: 2018-07-05T19:46:15Z
Registry Expiry Date: 2034-07-05T19:46:15Z
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: 2025-10-05T01:03:16Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
```

```
File Actions Edit View Help

2025-10-04 21:01:23 VERIFY OK: depth=1, CN=ChangeMe
2025-10-04 21:01:23 VERIFY KU OK
2025-10-04 21:01:23 Validating certificate extended key usage
2025-10-04 21:01:23 ++ Certificate has EKU (str) TLS Web Server Authentication, ex
2025-10-04 21:01:23 VERIFY EKU OK
2025-10-04 21:01:23 VERIFY OK: depth=0, CN=server
2025-10-04 21:01:24 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384
its X25519
2025-10-04 21:01:24 [server] Peer Connection Initiated with [AF_INET]18.202.129.19
2025-10-04 21:01:24 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-10-04 21:01:24 TLS: tls_multi_process: initial untrusted session promoted to
2025-10-04 21:01:24 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-10-04 21:01:24 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0/24
255.255.128.0,route-metric 1000,comp-lzo no,route-gateway 10.8.0.1,topology subnet
6-CBC'
2025-10-04 21:01:24 OPTIONS IMPORT: --ifconfig/up_options modified
2025-10-04 21:01:24 OPTIONS IMPORT: route options modified
2025-10-04 21:01:24 OPTIONS IMPORT: route-related options modified
2025-10-04 21:01:24 net_route_v4_best_gw query: dst 0.0.0.0
2025-10-04 21:01:24 net_route_v4_best_gw result: via 10.0.2.2 dev eth0
2025-10-04 21:01:24 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFAACE=eth0 HWADDR=08:00:27:00:00:02
2025-10-04 21:01:24 TUN/TAP device tun0 opened
2025-10-04 21:01:24 net_iface_mtu_set: mtu 1500 for tun0
2025-10-04 21:01:24 net_iface_up: set tun0 up
2025-10-04 21:01:24 net_addr_v4_add: 10.8.108.154/16 dev tun0
2025-10-04 21:01:24 net_route_v4_add: 10.10.0.0/16 via 10.8.0.1 dev [NULL] table 0
2025-10-04 21:01:24 net_route_v4_add: 10.101.0.0/16 via 10.8.0.1 dev [NULL] table
2025-10-04 21:01:24 net_route_v4_add: 10.103.0.0/16 via 10.8.0.1 dev [NULL] table
2025-10-04 21:01:24 net_route_v4_add: 10.201.0.0/17 via 10.8.0.1 dev [NULL] table
2025-10-04 21:01:24 Initialization Sequence Completed
2025-10-04 21:01:24 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 45
2025-10-04 21:01:24 Timers: ping 5, ping-restart 120

64 bytes from 10.10.10.10: icmp_seq=7 ttl=63 time=167 ms
64 bytes from 10.10.10.10: icmp_seq=8 ttl=63 time=164 ms
64 bytes from 10.10.10.10: icmp_seq=9 ttl=63 time=167 ms
64 bytes from 10.10.10.10: icmp_seq=10 ttl=63 time=168 ms
^C
-- 10.10.10.10 ping statistics --
10 packets transmitted, 10 received, 0% packet loss, time 9240ms
rtt min/avg/max/mdev = 164.039/168.170/178.026/4.366 ms

(kali@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: 2025-05-11T14:06:02Z
Creation Date: 2018-07-05T19:46:15Z
Registry Expiry Date: 2034-07-05T19:46:15Z
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: 2025-10-05T01:03:16Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
```

Answer the questions below

When was TryHackMe.com registered?

20180705

✓ Correct Answer

🔍 Hint

What is the registrar of TryHackMe.com?

namecheap.com

✓ Correct Answer

🔍 Hint

Which company is TryHackMe.com using for name servers?

cloudflare.com

✓ Correct Answer

🔍 Hint

## Nslookup and dig

I understood that Nslookup stands for Name Server Look Up and is used to find the ip address of a domain name. We can use the following command **nslookup DOMAIN\_NAME**, for example, **nslookup tryhackme.com**. Or, more generally, you can use **nslookup OPTIONS DOMAIN\_NAME SERVER** where.

- **OPTIONS** contains the query type. For instance, you can use A for IPv4 addresses and AAAA for IPv6 addresses.
- **DOMAIN\_NAME** is the domain name you are looking up.
- **SERVER** is the DNS server that you want to query.

**Dig** on the other hand stands for Domain Information Groper is used for more advanced DNS queries and additional functionality. The commands you can use are **dig DOMAIN\_NAME**, **dig DOMAIN\_NAME TYPE** or **dig @SERVER DOMAIN\_NAME TYPE**.

```
$ dig thmlabs.com TXT

; <<>> DiG 9.18.0-2-Debian <<>> thmlabs.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64210
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; MBZ: 0x0005, udp: 1280
;; QUESTION SECTION:
;thmlabs.com.                IN      TXT

;; ANSWER SECTION:
thmlabs.com.                5       IN      TXT      "THM{a5b83929888ed36acb0272971e438d78}"

;; Query time: 28 msec
;; SERVER: 192.168.85.2#53(192.168.85.2) (UDP)
;; WHEN: Fri May 20 00:36:23 EDT 2022
;; MSG SIZE  rcvd: 90
```

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

## DNSDumpster

The beauty of this tool is that it will assist in **extracting the target's "subdomains"** rather than going through search engines and hunting for it one by one, reducing the time-consuming search.

MX Records					
5	alt1.aspmx.l.google.com	172.253.116.27 dj-in-f27.1e100.net	ASN: 15169 172.253.116.0/24	GOOGLE United States	⋮
10	alt4.aspmx.l.google.com	192.178.213.26 yugrqs-in-f26.1e100.net	ASN: 15169 192.178.213.0/24	GOOGLE United States	⋮
10	alt3.aspmx.l.google.com	142.250.102.26 rb-in-f26.1e100.net	ASN: 15169 142.250.102.0/24	GOOGLE United States	⋮
1	aspmx.l.google.com	172.253.63.26 bi-in-f26.1e100.net	ASN: 15169 172.253.63.0/24	GOOGLE United States	⋮
5	alt2.aspmx.l.google.com	173.194.76.27 ws-in-f27.1e100.net	ASN: 15169 173.194.76.0/24	GOOGLE United States	⋮
NS Records					
kip.ns.cloudflare.com	173.245.59.128 kip.ns.cloudflare.com	ASN: 13335 173.245.59.0/24	CLOUDFLARENET	http: <b>cloudflare</b> title: Direct IP access not allowed tech: <b>Cloudflare</b> http8080: <b>cloudflare</b> title: Direct IP access not allowed tech: <b>Cloudflare</b>	⋮



The screenshot displays the Shodan.io web interface. At the top, there's a US flag icon. Below it, a section titled "A Records (subdomains from dataset)" shows a table of search results for the domain tryhackme.com. The table has columns for Host, IP, ASN, ASN Name, Open Services (from DB), and RevIP. The results show four subdomains: blog.tryhackme.com, help.tryhackme.com, insights-proxy-worker.tryhackme.com, and remote.tryhackme.com. Each entry lists its IP address, ASN (United States), and open services (http, http8080, and tech: Cloudflare). Below the table, there's a search bar with "tryhackme.com" entered and a "Start Test!" button. A message states: ">> Free users are limited to 50 results for a single domain. Get 12 months [Plus Access](#) - on Sale Now." At the bottom, there's a dashboard with three sections: "System Locations" (a world map), "Hosting / Networks" (a bar chart showing results for GOOGLE and CLOUDFLARENET), and "Services / Banners" (a donut chart showing results for cloudflare with a count of 4).

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
blog.tryhackme.com	104.22.54.228		United States	http: unknown server tech: Cloudflare http8080: unknown server tech: Cloudflare	5
help.tryhackme.com	172.67.27.10			http: unknown server tech: Cloudflare http8080: unknown server tech: Cloudflare	5
insights-proxy-worker.tryhackme.com	172.67.27.10			http: unknown server tech: Cloudflare http8080: unknown server tech: Cloudflare	5
remote.tryhackme.com	104.22.54.228		United States	http: unknown server tech: Cloudflare http8080: unknown server tech: Cloudflare	5

## Shodan.io

A tool such as this is notably useful for **learning various pieces of information about the client's network** during penetration testing (**without actively connecting to it**).

- Because, on the defensive side, it enables us to leverage various Shodan.io services to **learn about connected and exposed devices** belonging to the organization.
- In contrast to a search engine for web pages, **it attempts to connect to any device reachable online in order to develop a search engine of connected "things,"** and once connected, it collects all information linked to the service and saves it in the database to make it accessible.

It would be best to visit Shodan.io to answer the following questions; however, note that you can find the answers on Shodan.io

Woop woopl! Your answer is correct

Answer the questions below

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

United States

Correct Answer

Hint

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

8080

Correct Answer

Hint

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

5001

Correct Answer

Hint

China

13,252,046

United States

10,611,233

Hong Kong

4,892,065

Japan

3,691,211

Germany

3,060,281

More...

TOP PORTS

80

11,636,685

443

8,186,258

888

847,162

5001

682,762

5000

605,762

More...

400 Bad Request

14.225.200.127

static.vnpt.vn

Vietnam Posts and Telecommunications Group

Viet Nam, Ho Chi Minh City

400 Bad Request

111.62.90.59

China Mobile Communications Corporation

China, Beijing

400 Bad Request

14.0.124.102

CDNetworks

HTTP/1.1 400 Bad Request

Server: nginx

Date: Sun, 05 Oct 2025 14:00:22 GMT

Content-Type: text/html

Content-Length: 2415

Connection: close

X-WS-Request-Id: 68e279f6\_PS-SGN-043c038\_47940-58082

HTTP/1.1 400 Bad Request

Server: nginx

Date: Sun, 05 Oct 2025 14:00:19 GMT

Content-Type: text/html

Content-Length: 2410

Connection: close

X-WS-Request-Id: 68e279f3\_PShbsjzyd4lg48\_4361-51548

HTTP/1.1 400 Bad Request

Server: nginx

TOP PORTS

80

6,306,976

443

4,650,346

8080

340,195

5006

153,167

8081

144,940

More...

Apache Tomcat

46.252.34.7

4ALB shpk

Albania, Durrës

HTTP/1.1 200 OK

Server: Apache-Coyote/1.1

Accept-Ranges: bytes

ETag: W/"861-1526907641000"

Last-Modified: Mon, 21 May 2018 13:00:41 GMT

Content-Type: text/html

Content-Length: 861

Date: Sun, 05 Oct 2025 13:52:53 GMT

Shodan

Maps

Images

Monitor

Developer

More...

SHODAN

Explore

Pricing

Apache

Login

TOTAL RESULTS

16,351,023

TOP COUNTRIES

United States

4,344,558

Germany

1,561,662

Japan

1,513,752

China

913,010

France

685,835

More...

72.35.194.111

Zigly Fiber

United States, La Grande

14.241.245.146

static.vnpt.vn

Vietnam Posts and Telecommunications Group

Viet Nam, Quận Ba

View Report

Browse Images

View on Map

Advanced Search

Product Spotlight: Keep track of what you have connected to the Internet. Check out Shodan Monitor

HTTP/1.1 302 Found

Date: Sun, 05 Oct 2025 13:55:15 GMT

Server: Apache/2.4.29 (Ubuntu)

Location: https://72.35.194.111/

Content-Length: 285

Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

<html><head>

<title>302 Found</title>

</head><body>

<h1...</h1>

2025-10-05T13:55:14.533770

HTTP/1.1 302 Found

Server: Apache-Coyote/1.1

Cache-Control: private

Expires: Thu, 01 Jan 1970 07:00:00 GMT

2025-10-05T13:53:23.230265

## CONCLUSION



We focused on passive reconnaissance. We covered command-line tools, **whois**, **nslookup**, and **dig**. We also discussed two publicly available services [DNSDumpster](#) and [Shodan.io](#). The power of such tools is that you can collect information about your targets without directly connecting to them. This one was exciting to learn and explore.