

Passive Recon

- This module covers:
- Passive Reconnaissance
- Active Reconnaissance
- Nmap Live Host Discovery
- Nmap Basic Port Scans
- Nmap Advanced Port Scans
- Nmap Post Port Scans
- Protocols and Servers
- Protocols and Servers 2
- Network Security Challenge

In this room, I have learned d passive reconnaissance and active reconnaissance, focusing on essential tools related to passive reconnaissance. I have learned three command-line tools:

- **whois** to query WHOIS servers
- **nslookup** to query DNS servers
- **dig** to query DNS servers

We use **whois** to query WHOIS records, while we use **nslookup** and **dig** to query DNS database records.

I have also learned the usage of two online services:

- DNSDumpster
- Shodan.io

Purpose	Commandline Example
Lookup WHOIS record	whois tryhackme.com
Lookup <u>DNS</u> A records	nslookup -type=A tryhackme.com
Lookup <u>DNS</u> MX records at <u>DNS</u> server	nslookup -type=MX tryhackme.com 1.1.1.1
Lookup <u>DNS</u> TXT records	nslookup -type=TXT tryhackme.com
Lookup <u>DNS</u> A records	dig tryhackme.com A
Lookup <u>DNS</u> MX records at <u>DNS</u> server	dig @1.1.1.1 tryhackme.com MX
Lookup <u>DNS</u> TXT records	dig tryhackme.com TXT

TryHackMe

DashboardLearnCompeteOther

Access Machines

Go Premium

1

- Connecting to one of the company servers such as HTTP, FTP, and SMTP.
- Calling the company in an attempt to get information (social engineering).
- Entering company premises pretending to be a repairman.

Considering the invasive nature of active reconnaissance, one can quickly get into legal trouble unless one obtains proper legal authorisation.

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

TryHackMe

DashboardLearnCompeteOther

Access Machines

Go Premium

1

These two online services allow us to collect information about our target without directly connecting to it.

Pre-requisites: This room requires basic networking knowledge along with basic familiarity with the command line. The modules [Network Fundamentals](#) and [Linux Fundamentals](#) provide the required knowledge if necessary.

Important Notice: Please note that if you're not subscribed, the AttackBox won't have Internet access, so you will need to use the VPN to complete the questions that require Internet access.

Answer the questions below

This room does not use a target virtual machine (VM) to demonstrate the discussed topics. Instead, we will query public WHOIS servers and DNS servers for domains owned by TryHackMe. Start the AttackBox and make sure it is ready. You will use the AttackBox to answer the questions in later tasks, especially tasks 3 and 4.

No answer needed

✓ Correct Answer

Task 2

Passive Versus Active Recon

Task 3

Whois

Task 4

nslookup and dig

Task 5

DNSDumpster

Task 6

Shodan.io

John_Mbithi_Mutave

might consider an attack against the email server of the admin user or the DNS servers, assuming they are owned by your client and fall within the scope of the attack.

It is important to note that due to automated tools abusing WHOIS queries to harvest email addresses, many WHOIS services take measures against the addresses, for instance. Moreover, many registrants subscribe to privacy services to avoid their email addresses being harvested by spammers and keep their information private.

On the AttackBox, open the terminal and run the `whois tryhackme.com` command to get the information you need to answer the following questions.

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

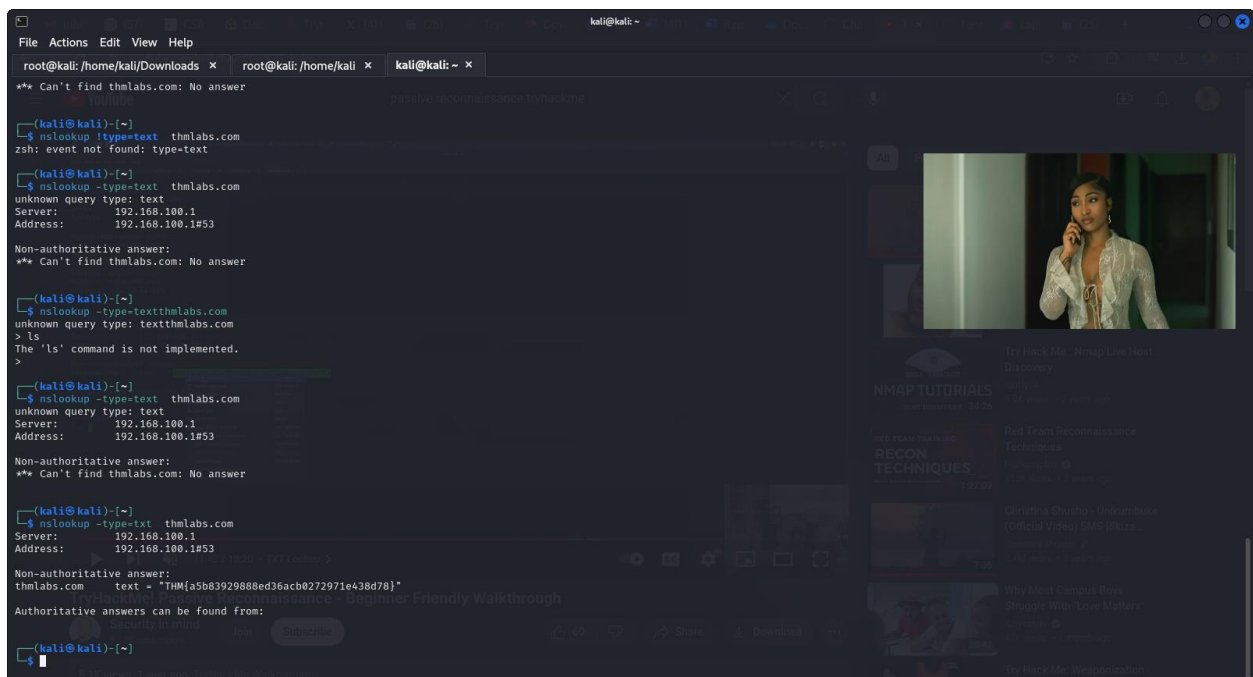
Which company is TryHackMe.com using for name servers?

cloudflare.com ✓ Correct Answer 🔍 Hint

Task 4 ☐ nslookup and dig

Task 5 ☐ DNSDumpster

John_Mbithi_Mutave



The screenshot shows a web browser window with the TryHackMe website. The browser's address bar shows the URL `tryhackme.com/r/room/passiverecon`. The TryHackMe header includes navigation links for Dashboard, Learn, Compete, and Other, along with buttons for Access Machines, Go Premium, and a user profile icon.

A terminal window is open, showing the command `dig 9.16.19-RH <>> tryhackme.com MX` and its output:

```
<>> Dig 9.16.19-RH <>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<
```

Below the terminal, a text block explains that `dig` returns more information than `nslookup` and provides the command `dig @1.1.1.1 tryhackme.com MX`. It then asks the user to use `nslookup` or `dig` to find a flag in the TXT records of `thmlabs.com`.

The question is: "Check the TXT records of thmlabs.com. What is the flag there?"

The answer input field contains the text `THM[a5b83929888ed36acb0272971e438d78]`, and a green button next to it says "Correct Answer".

At the bottom, there is a list of tasks:

- Task 5 ☐ DNSDumpster
- Task 6 ☐ Shodan.io
- Task 7 ☐ Summary

John_Mbithi_Mutave

Inbo(57)CSA(57)Dast xX (4)Fln (25)Try!DowWorMITRedDocChaTry!Newcapt(25)+

tryhackme.com/r/room/passiverecon

TryHackMe

DashboardLearnCompeteOther

Access Machines

Go Premium

1

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

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

strategos

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!

Users in Room

130,010

Created

961 days ago

Copyright TryHackMe 2018-2024

tryhackme.com/r/room/passiverecon

TryHackMe

DashboardLearnCompeteOther

Access Machines

Go Premium 1

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

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

tryhackmestrategos

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!

Users in Room

130,010

Created

961 days ago

Copyright TryHackMe 2018-2024

TwitterLinkedInDiscordFacebookYouTubeInstagramPinterest

tryhackme.com/r/room/passiverecon

TryHackMe

DashboardLearnCompeteOther

Access Machines

Go Premium 1

```
user@TryHackMe$ dig tryhackme.com MX
; <>> DiG 9.16.19-RH <>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<
```

Could not open "John_Mbithi_Mutave" Archive type not supported

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. To get the MX records for tryhackme.com, 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

Task 7

Summary

TryHackMe

DashboardLearnCompeteOther

Access Machines

Go Premium

1

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

🔍 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

Task 7

Summary

Created by

tryhackme

strategos

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!

Users In Room

130,010

Created

961 days ago

Copyright TryHackMe 2018-2024

shodan.io/search?query=nginx+

United States8,031,933

China7,746,115

Hong Kong3,322,398

Germany2,749,863

Japan1,386,689

More...

TOP PORTS

8012,462,904

4439,578,169

5001777,058

5000728,526

8888617,187

More...

TOP ORGANIZATIONS

Allyun Computing Co., LTD1,833,231

DigitalOcean, LLC1,336,187

Amazon Technologies Inc.1,203,696

Metaverse Limited.1,098,929

China Mobile Communications Cor...836,184

More...

151.101.193.75

www.ostandyspizza.com

Fastify, Inc.

United States, San Francisco

cdn

SSL Certificate

Issued By: Let's Encrypt

Issued To: www.ostandyspizza.com

Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP/1.1 200 OK

Connection: keep-alive

Content-Length: 46241

strict-transport-security: max-age=300; includeSubDomains

content-type: text/html; charset=utf-8

via: 1.1 varnish, 1.1 varnish, 1.1 varnish

cross-origin-opener-policy: same-origin

x-frame-options: SAMEORIGIN

server: nginx

Accept...

99.86.102.54

server-99-86-102-54.lan50.r.cloudfront.net

academia.edu

Amazon.com, Inc.

United States, Houston

cloudcdn

SSL Certificate

Issued By: Amazon RSA 2048 M01

Issued To: *.academia.edu

Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP/1.1 200 OK

Content-Type: text/html; charset=utf-8

Transfer-Encoding: chunked

Connection: keep-alive

Date: Wed, 29 May 2024 18:43:50 GMT

Server: nginx

Vary: Accept-Encoding

Status: 200 OK

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

X-...

76.223.25.140

adefee0d7f5m02e.awsglobal.amazonaws.com

Amazon.com, Inc.

United States, Seattle

cloud

SSL Certificate

Issued By: Amazon RSA 2048 M02

Issued To: *.gingrapp.com

Supported SSL Versions:

HTTP/1.1 200 OK

Date: Wed, 29 May 2024 18:43:41 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

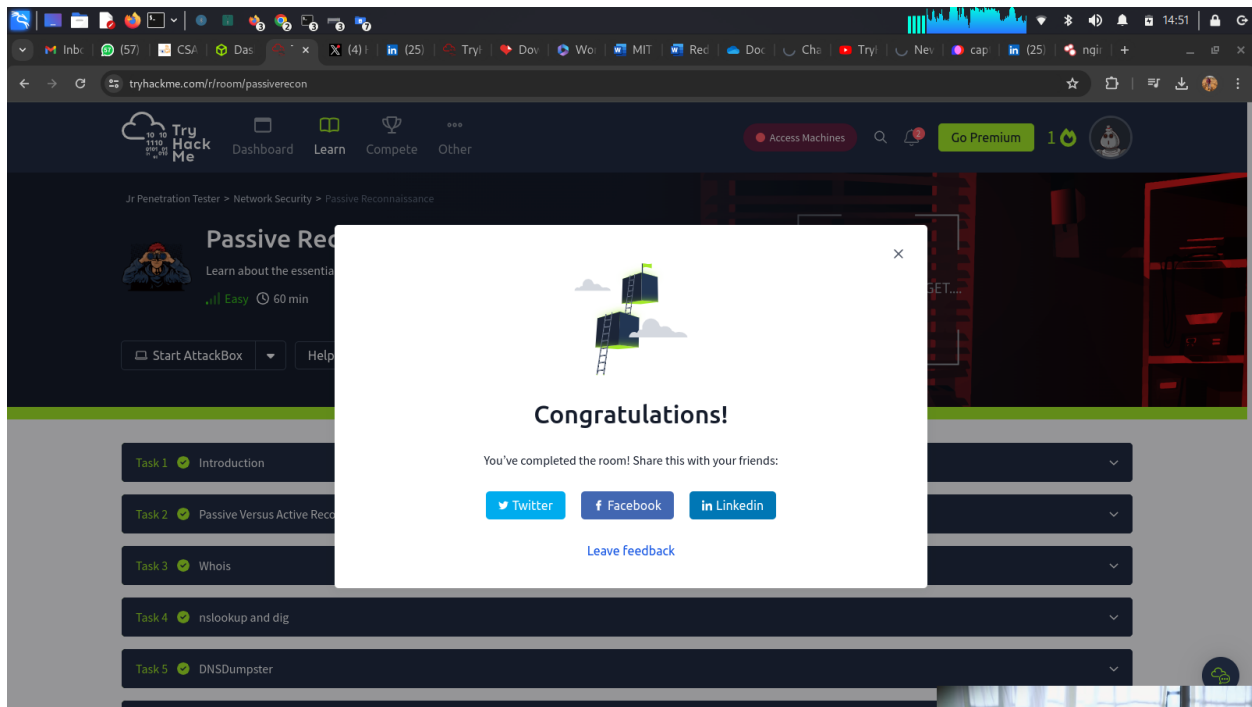
Connection: keep-alive

Server: nginx

Set-Cookie: gingr_csrf_cookie_name=049c489cf2395fcae46de9ebc390dbd8; expires=Sat, 01-Jun-2024 18:43:41 GMT; M...

cs-sa07-24019

John_Mbithi_Mutave



Shareable link - www.tryhackme.com/r/room/passiverecon

In this room, we focused on passive reconnaissance. In particular, 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. Moreover, the trove of information you may find using such tools can be massive once you master the search options and get used to reading the results.