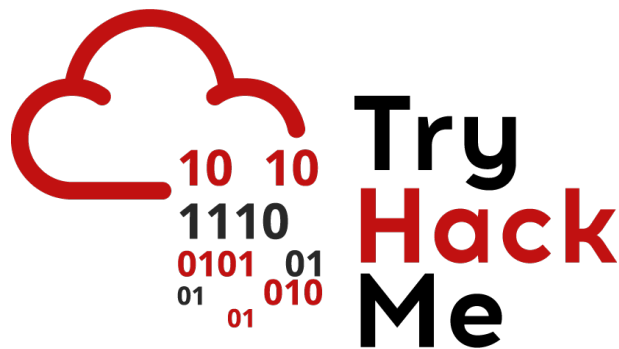


# Writeup: Sala *Passive Reconnaissance*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



## Índice

<b>1. Introducción</b>	<b>2</b>
<b>2. Sala</b>	<b>2</b>
2.1. Tarea 1 - Introducción . . . . .	2
2.2. Tarea 2 - Reconocimiento Pasivo vs Activo . . . . .	2
2.3. Tarea 3 - Whois . . . . .	3
2.4. Tarea 4 - nsLookup y Dig . . . . .	3
2.5. Tarea 5 - DNSDumpster . . . . .	4
2.6. Tarea 6 - Shodan.io . . . . .	5
2.7. Tarea 7 - Resumen . . . . .	8
<b>3. Conclusión sobre la Sala</b>	<b>8</b>

# 1. Introducción

En esta sala aprenderemos los fundamentos del **reconocimiento pasivo**, una técnica esencial dentro del proceso de recolección de información durante una auditoría de seguridad o una evaluación de penetración.

## 2. Sala

### 2.1. Tarea 1 - Introducción

En esta primera tarea se presenta el reconocimiento pasivo y se contextualiza frente a métodos activos y se adelantan algunas herramientas a utilizar.

**Respuesta:** **No requiere respuesta** (Hacemos clic en **Submit**).

### 2.2. Tarea 2 - Reconocimiento Pasivo vs Activo

Ahora, aprenderemos como el reconocimiento es una fase inicial para recopilar datos del objetivo. El reconocimiento pasivo explora fuentes públicas sin hacer contacto con el sistema, mientras que el activo implica interacción directa al sistema (ping, escaneos, etc), lo que puede alertar al objetivo e implicar riesgos legales.

Una vez que comprendemos ambas partes del reconocimiento, podemos pasar a responder las siguientes preguntas:

**Pregunta:** 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)

**Respuesta:** **P**

**Pregunta:** 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)

**Respuesta:** **A**

**Pregunta:** 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)

**Respuesta:** **A**

## 2.3. Tarea 3 - Whois

Aprenderemos a usar el protocolo **WHOIS** para obtener información del registro de dominio, algunos datos que logramos obtener son:

- **Responsable del registro**
- **Fechas de creación y expiración**
- **Nombres de servidores**
- **Datos de contacto**

Después de entender el funcionamiento de Whois, usaremos una terminal y ejecutaremos el siguiente comando:

**whois tryhackme.com**

Posterior a eso, pasaremos a responder las siguientes preguntas:

**Pregunta:** When was TryHackMe.com registered?

**Respuesta:** **20180705**

**Pregunta:** What is the registrar of TryHackMe.com?

**Respuesta:** **namecheap.com**

**Pregunta:** Which company is TryHackMe.com using for name servers?

**Respuesta:** **cloudflare.com**

## 2.4. Tarea 4 - nslookup y Dig

Vamos a introducirnos en el uso de **nslookup**, una herramienta para consultar registros DNS (A, AAAA, MX, CNAME, TXT, SOA) permitiendo usar servidores específicos; y **dig**, una alternativa más avanzada que ofrece respuestas detalladas, incluidos TTL, autoridades DNS y otras configuraciones, útil para evaluar infraestructuras de red de forma pasiva.

Para completar esta tarea, vamos a responder las siguientes preguntas.

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

Para conseguir la flag de respuesta, debemos dirigirnos a nuestra terminal y ejecutaremos el siguiente comando:

**dig TryHackMe.com TXT**

Después, nos saltarán los resultados de la búsqueda y lograremos encontrar la flag.

```
(kali@kali)-[~]
$ dig thmlabs.com TXT

; <<>> DiG 9.20.8-6-Debian <<>> thmlabs.com TXT
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 31850
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;thmlabs.com.                IN      TXT

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

;; Query time: 255 msec
;; SERVER: 192.168.188.2#53(192.168.188.2) (UDP)
;; WHEN: Fri Jun 06 12:23:37 EDT 2025
;; MSG SIZE rcvd: 90
```

Respuesta: **THM{a5b83929888ed36acb0272971e438d78}**

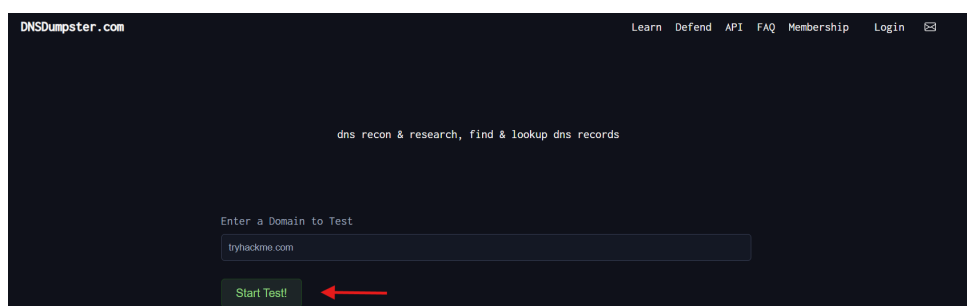
## 2.5. Tarea 5 - DNSDumpster

En esta tarea aprenderemos cómo **DNSDumpster** permite descubrir subdominios y almacenar información DNS automáticamente (servidores, IPs, MX, TXT) haciendo posible identificar infraestructuras ocultas o vulnerables, como subdominios poco mantenidos o mal configurados.

Una vez que comprendemos DNSDumpster, pasamos a responder las siguientes preguntas.

**Pregunta:** Lookup tryhackme.com on DNSDumpster. What is one interesting sub-domain that you would discover in addition to www and blog?

Para encontrar la respuesta, nos dirigiremos al sitio oficial de DNSDumpster y en el buscador vamos a escribir el dominio: **tryhackme.com**. Una vez hecho eso, nos saltará en la parte inferior los distintos subdominios y el que más nos llama la atención es remote.



A Records (subdomains from dataset)

Host	IP	ASN	ASN Name
blog.tryhackme.com	104.22.55.228	ASN: 13335 104.22.48.0/20	CLOUDFLARENET
insights-proxy- worker.tryhackme.com	104.22.55.228	ASN: 13335 104.22.48.0/20	CLOUDFLARENET
remote.tryhackme.com	104.22.55.228	ASN: 13335 104.22.48.0/20	CLOUDFLARENET
www.tryhackme.com	104.22.55.228	ASN: 13335 104.22.48.0/20	CLOUDFLARENET

Respuesta: **remote**

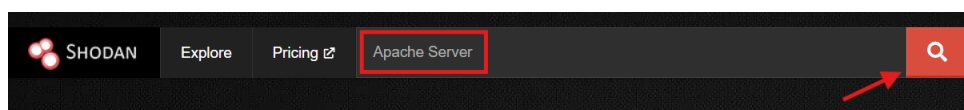
## 2.6. Tarea 6 - Shodan.io

Ahora, aprenderemos como **Shodan** es un buscador global el cual almacena datos de servicios (IP, puertos, geolocalización, compañía de hosting), y permite búsquedas pasivas sobre los objetivos sin interacción directa.

Una vez que entendemos como funciona Shodan y su uso, procederemos a dirigirnos a su **sitio oficial** para lograr responder las siguientes preguntas.

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

Para resolver esta primera pregunta, en el buscador de shodan vamos a escribir **Apache Server** y nos buscará toda la información necesaria. En el lado izquierdo podremos visualizar los países con más servidores Apache.





Respuesta: **China**

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

Si bajamos un poco más, en el lado izquierdo también nos aparecerá los puertos más comunes usados para Apache.

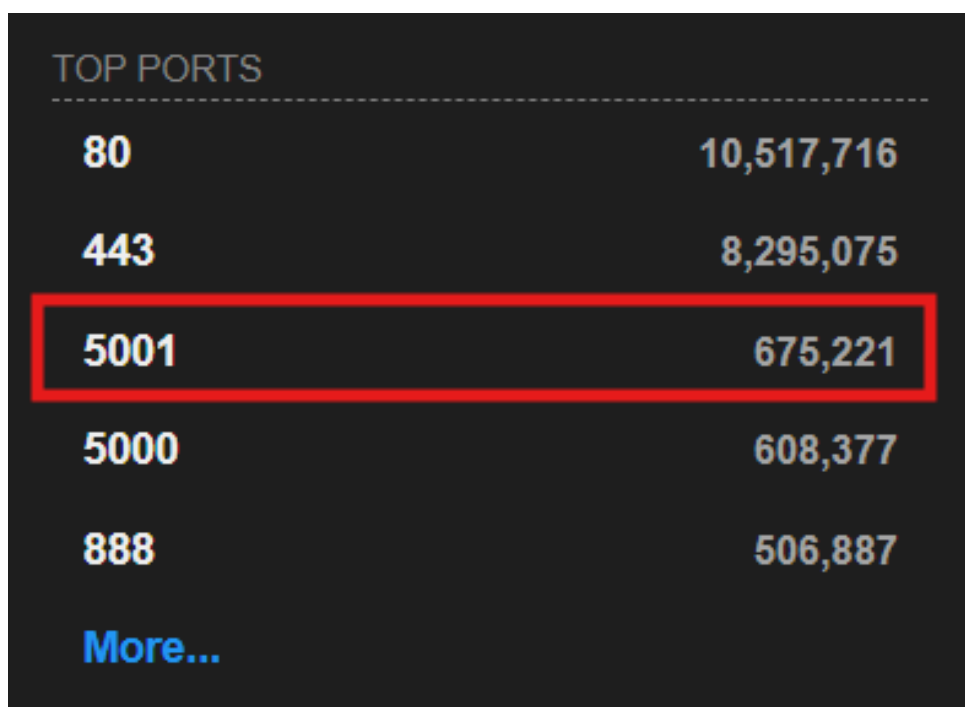
TOP PORTS	
80	6,160,001
443	5,121,182
8080	335,824
5006	152,660
8081	142,130
<a href="#">More...</a>	

**Respuesta:** 8080

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

Ahora, cambiaremos la consulta en el buscador de shodan y buscaremos **Nginx**. Al finalizar la búsqueda nos aparecerá toda la información necesaria y si bajamos un poco, en el lado izquierdo aparecerán los puertos más comunes.





A screenshot of a terminal window showing a list of top ports. The title 'TOP PORTS' is at the top, followed by a dashed line. The table has two columns: the first column lists port numbers and the second column lists their corresponding counts. The row for port 5001 is highlighted with a red rectangular box. Below the table, there is a blue link that says 'More...'.

TOP PORTS	
80	10,517,716
443	8,295,075
5001	675,221
5000	608,377
888	506,887
<a href="#">More...</a>	

Respuesta: 5001

## 2.7. Tarea 7 - Resumen

En esta tarea final, vamos a reforzar el conocimiento de que mediante estas herramientas pasivas se puede recolectar información valiosa a gran escala sin alertar al objetivo.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

## 3. Conclusión sobre la Sala

Al finalizar la sala, hemos comprendido la importancia del reconocimiento pasivo como primera fase en el análisis de un objetivo. Aprendimos a utilizar herramientas y servicios que permiten recolectar datos públicos sobre dominios, infraestructura de red y dispositivos conectados sin levantar alertas.