

## Reconocimiento pasivo

### Tarea 1: Introduccion

En esta sala, tras definir el reconocimiento pasivo y el reconocimiento activo, nos centraremos en las herramientas esenciales relacionadas con el reconocimiento pasivo. Aprenderemos tres herramientas de línea de comandos:

- `whois` para consultar servidores WHOIS
- `nslookup` para consultar servidores DNS
- `dig` para consultar servidores DNS

Utilizamos `whois` para consultar registros WHOIS, mientras que utilizamos `nslookup` y `dig` para consultar registros de bases de datos DNS. Estos registros son públicos y, por lo tanto, no alertan al objetivo.

También aprenderemos el uso de dos servicios en línea:

- Contenedor de basura DNS
- Shodan.io

Estos dos servicios en línea nos permiten recopilar información sobre nuestro objetivo sin conectarnos directamente con él.

Prerrequisitos: Esta sala requiere conocimientos básicos de redes y familiaridad con la línea de comandos. Los módulos Fundamentos de Red y Fundamentos de Linux proporcionan los conocimientos necesarios, si es necesario.

P: Esta sala no utiliza una máquina virtual (VM) de destino para demostrar los temas tratados. En su lugar, consultaremos los servidores públicos WHOIS y DNS de los dominios propiedad de TryHackMe. Inicie AttackBox y asegúrese de que esté listo. Utilizará AttackBox para responder las preguntas en tareas posteriores, especialmente las tareas 3 y 4.

R: No se necesita respuesta

### Tarea 2: Reconocimiento pasivo versus activo

P1: Visitas la página de Facebook de la empresa objetivo con la esperanza de obtener los nombres de algunos de sus empleados. ¿Qué tipo de actividad de reconocimiento es esta? (A de activa, P de pasiva).

R1: P

P2: Haces ping a la dirección IP del servidor web de la empresa para comprobar si el tráfico ICMP está bloqueado. ¿Qué tipo de actividad de reconocimiento es esta? (A para activa, P para pasiva)

R2: A

P3: Te encuentras con el administrador de TI de la empresa objetivo en una fiesta. Intentas usar ingeniería social para obtener más información sobre sus sistemas e infraestructura de red. ¿Qué tipo de actividad de reconocimiento es esta? (A de activa, P de pasiva).

R3: A

### Tarea 3: Quién es

P1: ¿Cuándo se registró TryHackMe.com?

R1: 20180705

P2: ¿Quién es el registrador de TryHackMe.com?

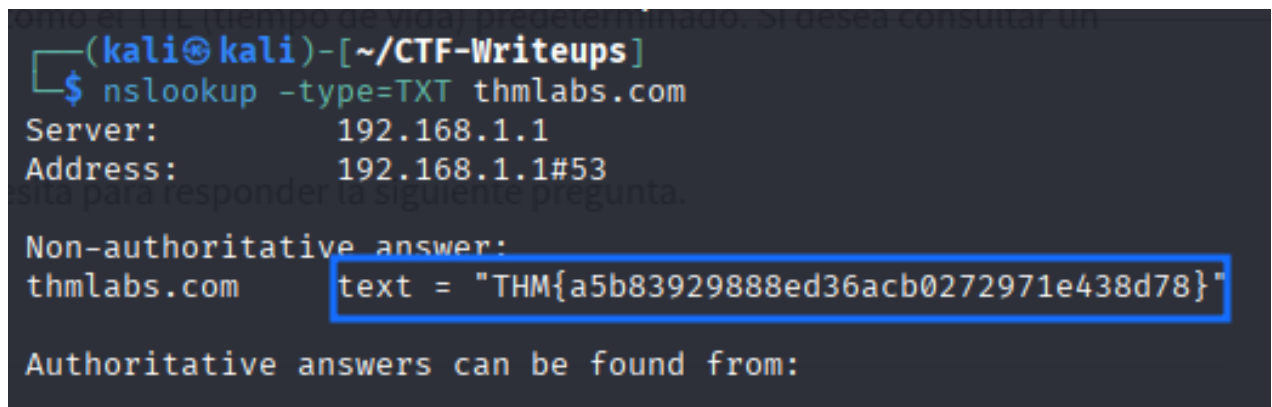
R2: namecheap.com

P3: ¿Qué empresa utiliza TryHackMe.com para los servidores de nombres?

R3: cloudflare.com

### Tarea 4: nslookup y dig

P: Revisa los registros TXT de thmlabs.com. ¿Qué es la bandera?



```
(kali㉿kali)-[~/CTF-Writeups]
$ nslookup -type=TXT thmlabs.com
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
thmlabs.com      text = "THM{a5b83929888ed36acb0272971e438d78}"

Authoritative answers can be found from:
```

R: THM{a5b83929888ed36acb0272971e438d78}

### Tarea 5: Contenedor de basura DNS

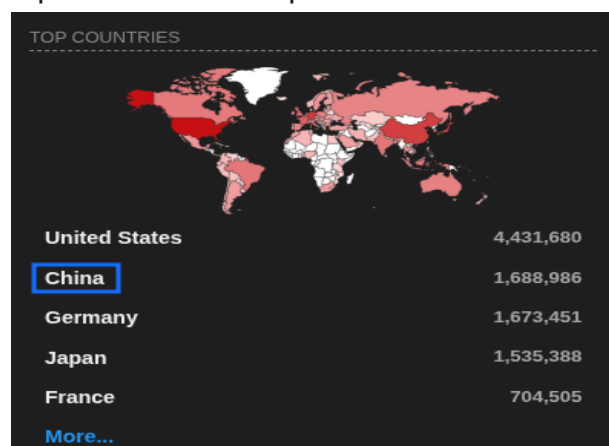
P: Busca tryhackme.com en DNSDumpster. ¿Qué subdominio interesante descubrirías además de "www" y "blog"?

Host	IP	ASN	ASN Name
blog.tryhackme.com	104.22.54.228	ASN: 13335 104.22.48.0/20	CLOUDFLARENET
help.tryhackme.com	172.67.27.10	ASN: 13335 172.67.16.0/20	CLOUDFLARENET
insights-proxy- worker.tryhackme.com	172.67.27.10	ASN: 13335 172.67.16.0/20	CLOUDFLARENET
remote.tryhackme.com	104.22.54.228	ASN: 13335 104.22.48.0/20	CLOUDFLARENET
www.tryhackme.com	172.67.27.10	ASN: 13335 172.67.16.0/20	CLOUDFLARENET

R: remote

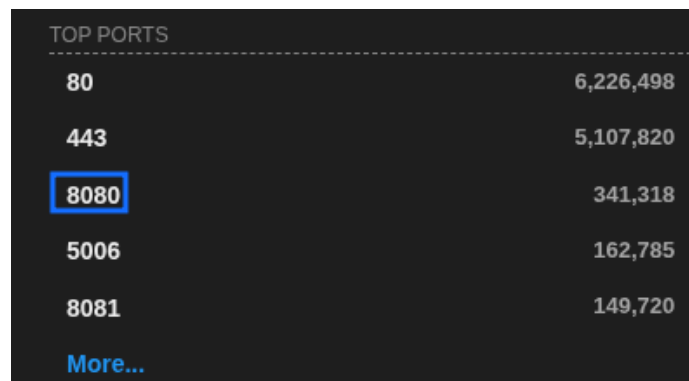
### Tarea 5: Shodan.io

P1: Según Shodan.io, ¿cuál es el segundo país del mundo en términos de cantidad de servidores Apache de acceso público?



R1: China

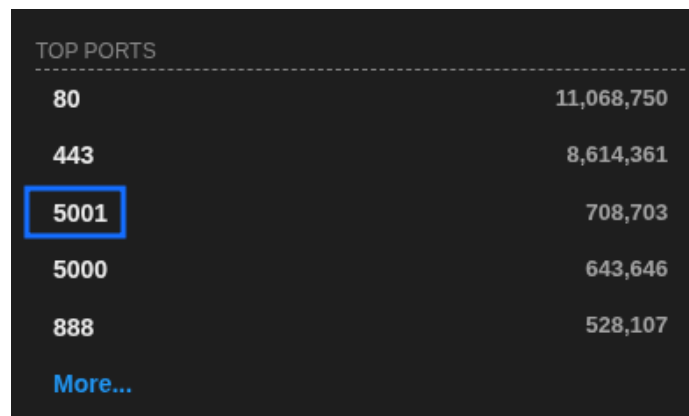
P2: Según Shodan.io, ¿cuál es el tercer puerto más común utilizado para Apache?

A screenshot of the Shodan.io 'TOP PORTS' section for Apache. The table lists the top 5 ports by frequency. The third port, 8080, is highlighted with a blue box. The background is dark with white text.

TOP PORTS	
80	6,226,498
443	5,107,820
8080	341,318
5006	162,785
8081	149,720
<a href="#">More...</a>	

R2: 8080

P3: Según Shodan.io, ¿cuál es el tercer puerto más común utilizado para nginx?

A screenshot of the Shodan.io 'TOP PORTS' section for nginx. The table lists the top 5 ports by frequency. The third port, 5001, is highlighted with a blue box. The background is dark with white text.

TOP PORTS	
80	11,068,750
443	8,614,361
5001	708,703
5000	643,646
888	528,107
<a href="#">More...</a>	

R3: 5001

## Tarea 7: Resumen

En esta sala, nos centramos en el reconocimiento pasivo. En particular, abordamos las herramientas de línea de comandos, [Nombre del sitio web] `whois`, [Nombre del sitio web] `nslookup` y [Nombre del sitio web] `dig`. También hablamos de dos servicios públicos: DNSDumpster y Shodan.io . La ventaja de estas herramientas radica en que permiten recopilar información sobre los objetivos sin necesidad de conectarse directamente a ellos. Además, la cantidad de información que se puede encontrar con estas herramientas puede ser enorme una vez que se dominen las opciones de búsqueda y se acostumbre a leer los resultados.

Objetivo	Ejemplo de línea de comandos
Buscar registro WHOIS	<code>whois tryhackme.com</code>
Buscar registros DNS A	<code>nslookup -type=A tryhackme.com</code>
Buscar registros MX de DNS en el servidor DNS	<code>nslookup -type=MX tryhackme.com 1.1.1.1</code>
Buscar registros TXT de DNS	<code>nslookup -type=TXT tryhackme.com</code>
Buscar registros DNS A	<code>dig tryhackme.com A</code>
Buscar registros MX de DNS en el servidor DNS	<code>dig @1.1.1.1 tryhackme.com MX</code>
Buscar registros TXT de DNS	<code>dig tryhackme.com TXT</code>

P: Asegúrese de tener en cuenta todos los puntos discutidos en esta sala, especialmente la sintaxis de las herramientas de la línea de comandos.

R: No se necesita respuesta

---

 **LinkedIn:** <https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/>

 **GitHub:** <https://github.com/MaateoSuar>