

# Passive Recon

## INTRODUCTION

This report show how I solved question in the tryhackme passiverecon room

# Passive recon basically is gathering as much information as possible of a target system or organisation using various tools such as dnsrecon, recon-ng, dnsdumpster,shodan.io e.t.c

# In this type of information gathering, an attacker does not directly interact with the target.

1 .

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

2.

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

3.

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

4.

When was TryHackMe.com registered?

20180705

✓ Correct Answer

🔍 Hint

```
(root@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
```

5.

What is the registrar of TryHackMe.com?

NameCheap.com

✓ Correct Answer

🔍 Hint

```
(root@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
```

6.

Which company is TryHackMe.com using for name servers?

CLOUDFLARE.COM

✓ Correct Answer

🔍 Hint

```
(root@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
```

7.

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

THM{a5b83929888ed36acb0272971e438d78}

✓ Correct Answer

```

(root@kali)-[~]
# nslookup -type=TXT thmlabs.com
;; communications error to 192.168.1.2#53: host unreachable
;; communications error to 192.168.1.2#53: host unreachable
;; communications error to 192.168.1.2#53: host unreachable
Server:         fde4:9f99:cc4a:10::1
Address:        fde4:9f99:cc4a:10::1#53

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

Authoritative answers can be found from:

(root@kali)-[~]
#

```

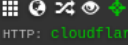
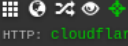
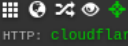
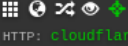
8.

Lookup tryhackme.com on DNSDumpster. What is one interesting subdomain that you would discover in addition to www and blog?

remote

✓ Correct Answer

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

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

9.

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

apache

Q

View Report

Browse Images

View on Map

Product Spotlight:

Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

302 Found

2024-0

64.136.53.71

my.vgs.netzero.net

[Juno Online Services, Inc.](#)

United States, Los Angeles

HTTP/1.1 302 Found

Date: Wed, 22 May 2024 22:14:11 GMT

Server: **Apache**

Location: <https://my.netzero.net/start/sp.do>

Content-Length: 218

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

Set-Cookie: NSC\_nz.wht=ffffff09bd146a45525d5f4f58455e445a4a42156a;expires=Wed, 22-May-2024 23:14:11 GMT

403 Forbidden

2024-0

167.235.102.250

imbabura.ecuahosting.net

[samaratex.com](#)

[Hetzner Online GmbH](#)

Germany, Falkenstein

SSL Certificate

Issued By:

- Common Name:

R3

- Organization:

Let's Encrypt

HTTP/1.1 403 Forbidden

Date: Wed, 22 May 2024 22:12:57 GMT

Server: **Apache**

Content-Length: 318

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

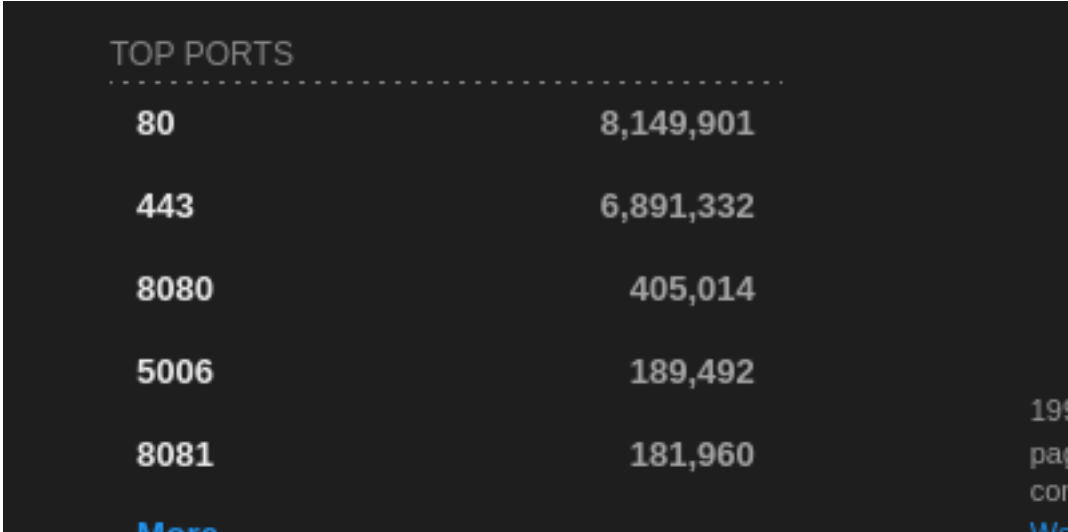
10.

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

8080

✓ Correct Answer

🔗 Hint



11.

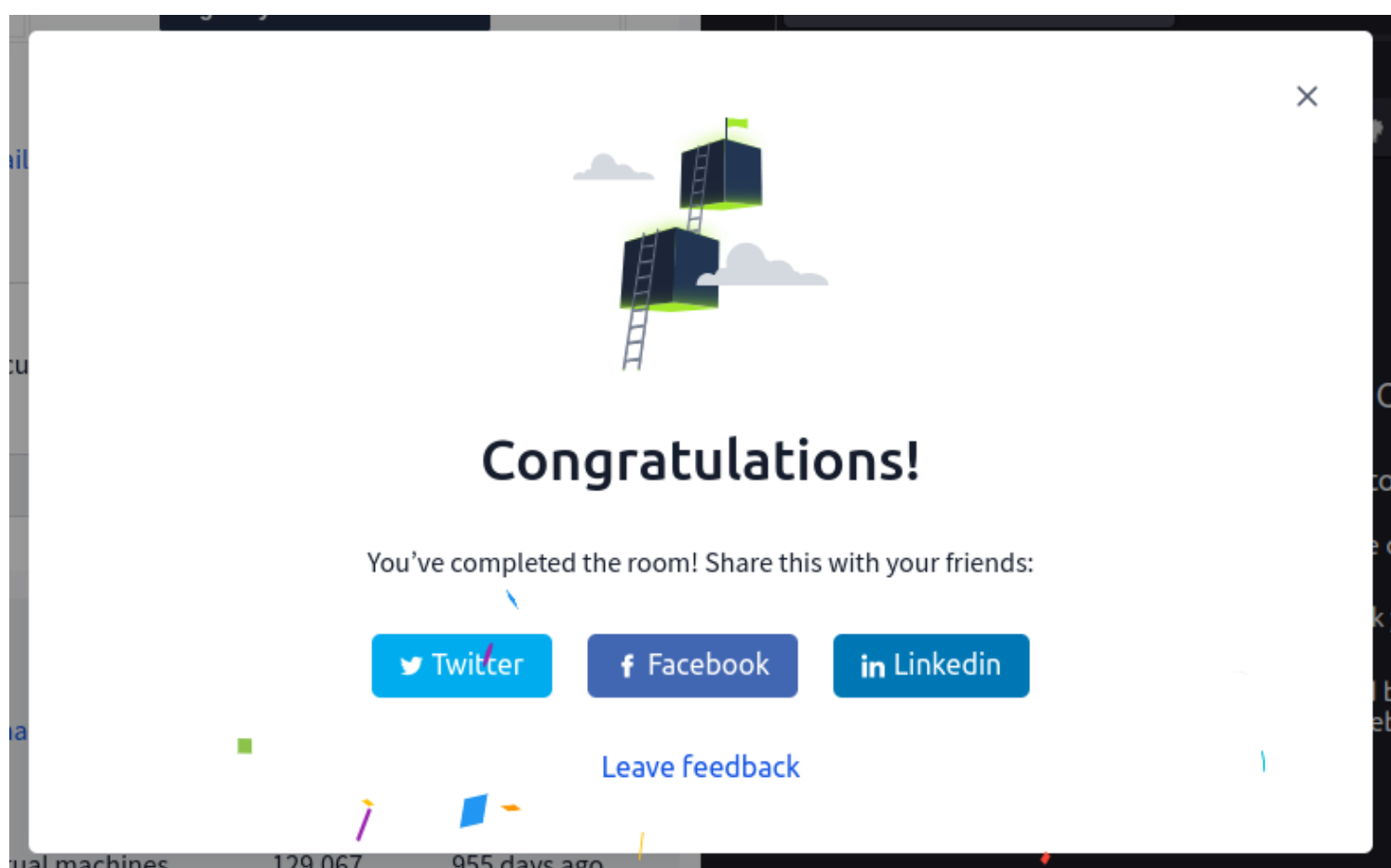
Based on Shodan.io, what is the 3rd most common port used for nginx?

5001

✓ Correct Answer

🔗 Hint

TOP PORTS	
80	206
443	160
5001	134
5000	126
7001	28



## CONCLUSION

# A thorough and intense information gathering during the passive recon stage should be conducted to increase our attack surface.

THE END !

