Passive Reconnaissance

Introduction

This involves collecting information without directly interacting or connecting to the target. This can involve using command line tools like whois,nslookup and dig or online services like shodan.io and DNSDumpster. This module will concentrate on this tools to get the public accessible knowledge of the target.

Passive reconnaissance activities involves :

>Looking for DNS records of domain from public DNS server.

>Checking for jobs ads related to the target website.

>Reading news articles about the target company.

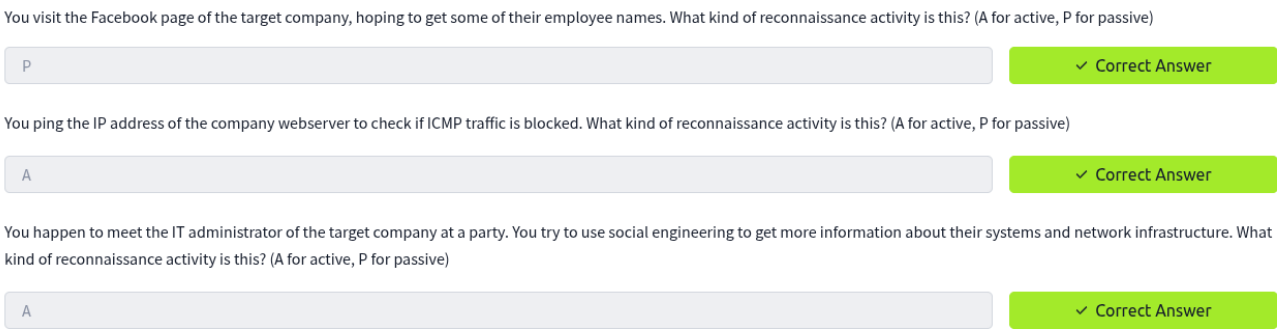
The opposite of this is active reconnaissance and include:

>Connecting to one of the company server 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.

Questions:



Whois

This is a request and response protocol that follows the RFC 3912 specifications and its server listens on TCP port 43 for incoming requests.

Whois gives information about the domain name.

Whois gives information such as the registrar,contact info of a registrant,creation,update,expiration date and name of the server.

Questions:

When was TryHackMe.com registered?

Answer 20180705

```
[kabangi@parrot ~ 21:37 :(]$ 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/
```

What is the registrar of TryHackMe.com?

Answer namecheap.com

```
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
```

Which company is TryHackMe.com using for name servers?

Answer cloudflare.com

```
Name Server: KIP.NS.CLOUDFLARE.COM
Name Server: UMA.NS.CLOUDFLARE.COM
```

Nslookup and dig

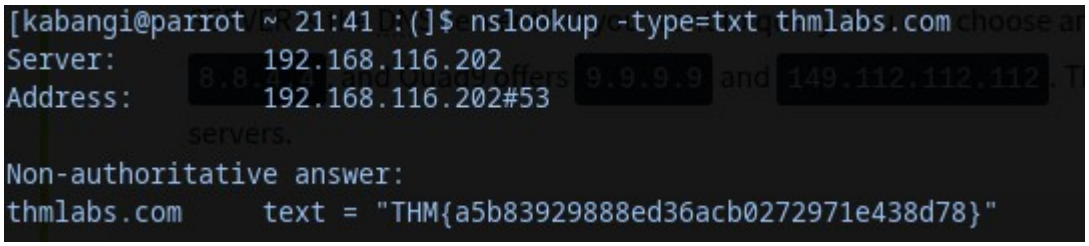
Nslookup looks for the ip address of a domain name either the ipv4 address using option A and ipv6 using option AAA.

Query type	Result
A	IPv4 Addresses
AAAA	IPv6 Addresses
CNAME	Canonical Name
MX	Mail Servers
SOA	Start of Authority
TXT	TXT Records

Question:

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

THM{a5b83929888ed36acb0272971e438d78}

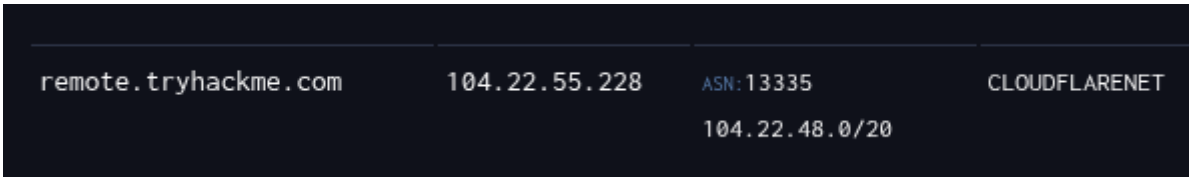


DNSDumpster

This is an online services that can help you find the subdomain which can reveal much information about the taarget and returns the collected DNS information in easy to read tables and grapgh.
Also it will provide any collected information about listening servers.

Question:

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



Shodan.io

Shodan.io tries to connect to every device reachable online to build a search engine of connected "things" in contrast with a search engine for web pages. Once it gets a response, it collects all the information related to the service and saves it in the database to make it searchable.

Questions:

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

China

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

8080

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

5001

Conclusion

Passive recon is the first step in ethical hacking, used to gather information about a target without direct interaction. Using tools like WHOIS, Shodan.io, DNSDumpster, dig, and nslookup, you can find details such as domain info, subdomains, IPs, and services. It's a stealthy and safe way to understand your target before active testing.