Passive Reconnaissance

Introduction

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

Note: These are all publicly available records and hence do not alert the target.

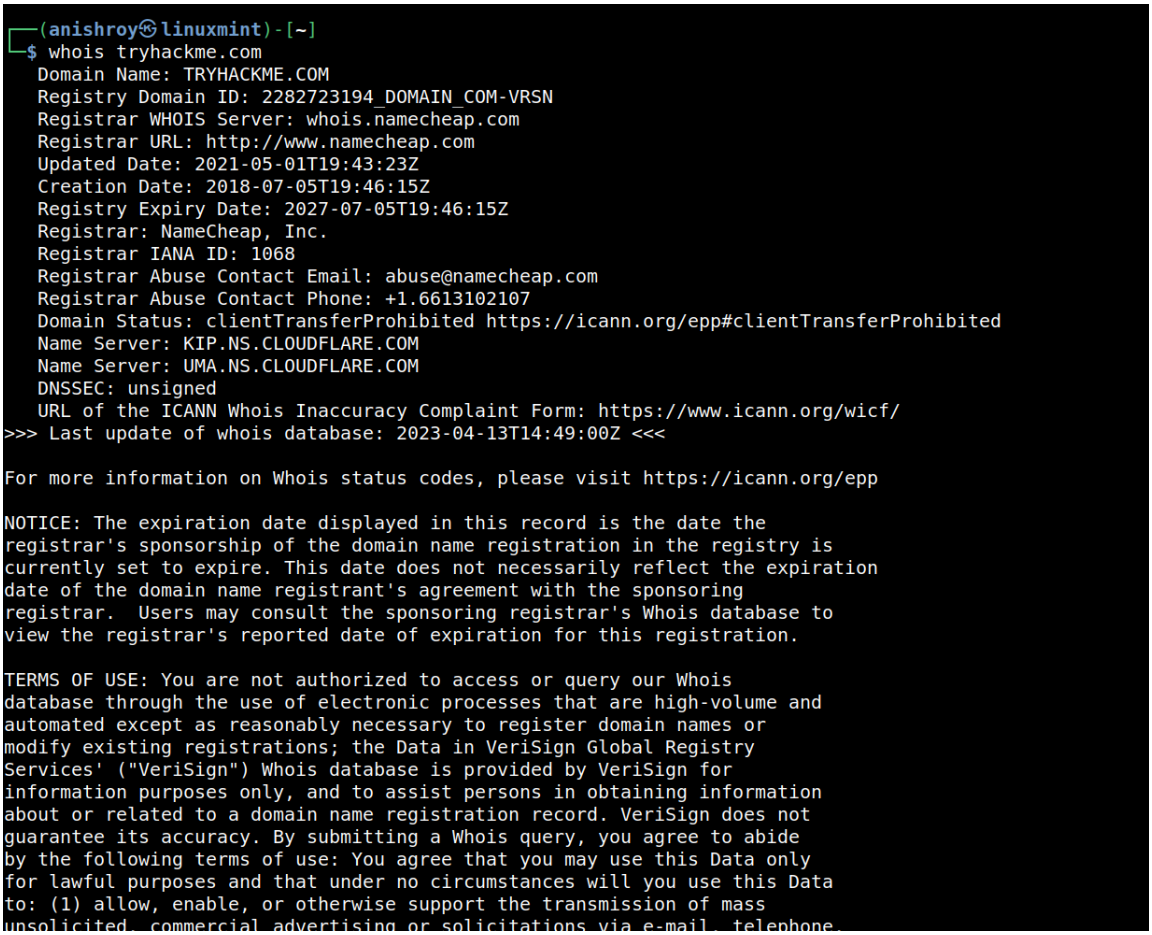
Passive Versus Active Recon

- **Reconnaissance -**
  - It is a preliminary survey to gather information about a target.
  - It is the first step in The Unified Kill Chain to gain an initial foothold on a system.
  - It can be divided into:
    - Passive Reconnaissance
    - Active Reconnaissance
  - **Passive Reconnaissance-**
    - We rely on publicly available knowledge.
    - It is the knowledge that we can access from publicly available resources without directly engaging with the target.
    - It includes many activities like-
      - Looking up DNS records of a domain from a public DNS server.
      - Checking job ads related to the target website.
      - Reading news articles about the target company.
  - **Active Reconnaissance-**

- It cannot be achieved so discreetly.
- It requires direct engagement with the target.
- Examples of active recon include-
    - 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.

Whois

- WHOIS is a request and response protocol that follows the RFC 3912 specification.
- A WHOIS server listens on TCP port 43 for incoming requests.
- The domain registrar is responsible for maintaining the WHOIS records for the domain names.
- he WHOIS server replies with various information related to the domain requested, for example-
    - Registrar: Via which registrar was the domain name registered
    - Contact info of registrant: Name, organization, address, phone, among other things. (unless made hidden via a privacy service)
    - Creation, update, and expiration dates: When was the domain name first registered, when was the domain last updated, and when does it needs to be renewed.
    - Name Server: Which server to ask to resolve the domain name



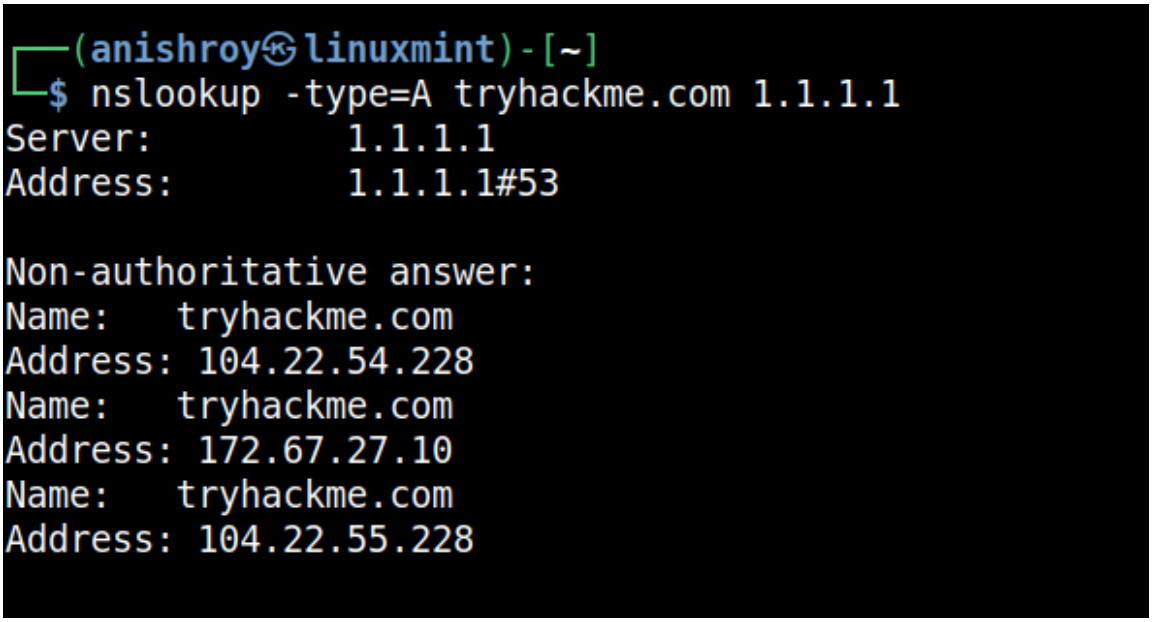
nslookup and dig

- We can find the IP address of a domain name using **nslookup.**
- **nslookup** stands for Name Server Lookup.
- We need to issue the command- `nslookup DOMAIN_NAME`, for example - `nslookup tryhackme.com`.
- We can also use - `nslookup OPTIONS DOMAIN_NAME SERVER`
- The three main parameters are:-
  - OPTIONS- It contains the query type. For example - We can use **A** for IPv4 addresses and **AAAA** for IPv6 addresses.

Query type	Result
A	IPv4 Addresses
AAAA	IPv6 Addresses
CNAME	Canonical Name

MX	Mail Servers
SOA	Start of Authority
TXT	TXT Records

  - DOMAIN_NAME- It is the domain name we are looking up.
  - SERVER- It is the DNS server that we want to query. We can choose any public DNS server to query. Cloudflare offers `1.1.1.1` and `1.0.0.1`. Similarly Google offers `8.8.8.8` and `8.8.4.4`.
  - There are many more public DNS servers that we can choose.
- Example syntax- `nslookup -type=A tryhackme.com 1.1.1.1` can be used to return all the IPv4 addresses used by tryhackme.com.



- In the above example, we started with one domain name, and we obtained three IPv4 addresses.
- Each of these IP address can further be checked for insecurities.
- To learn about the email servers and configurations for a particular domain, we can use- `nslookup -type=MX tryhackme.com` .

```
┌──(anishroy㉿linuxmint)-[~]
└─$ nslookup -type=MX tryhackme.com
;; communications error to 127.0.0.53#53: timed out
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
tryhackme.com   mail exchanger = 1 aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt3.aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt4.aspmx.l.google.com.
tryhackme.com   mail exchanger = 5 alt1.aspmx.l.google.com.
tryhackme.com   mail exchanger = 5 alt2.aspmx.l.google.com.

Authoritative answers can be found from:
```

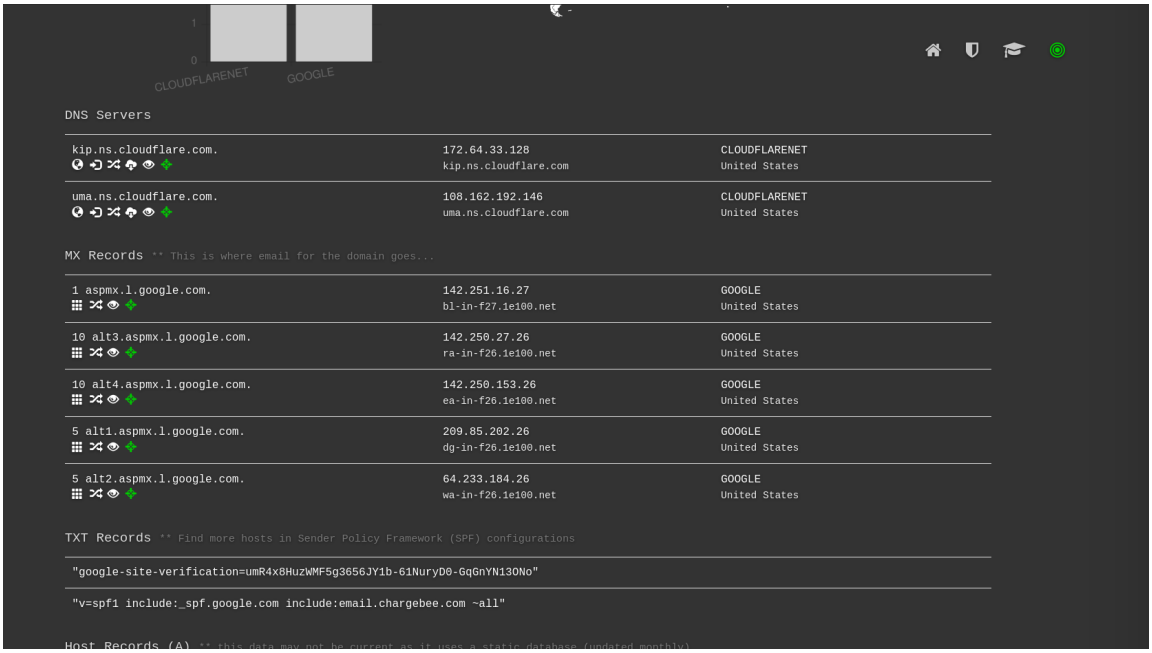
- We can see that tryhackme.com's current email configuration uses Google.
- When a mail server tries to deliver email **@tryhackme.com,** it will try to connect to **aspmx.l.google.com.**
- If it is busy or unavailable, the mail server will attempt to connect to the next in order mail exchange servers, **alt1.aspmx.l.google.com or alt2.aspmx.l.google.com**
- For more advance DNS queries and additional functionality, we can use `dig` which stands for "Domain Information Groper".
- To lookup for the MX records using **dig** we will use the command- `dig DOMAIN_NAME TYPE`.
- We can also select the server to query using - `dig @SERVER DOMAIN_NAME TYPE`
  - SERVER - It is the DNS server that we want to query.
  - DOMAIN_NAME- It is the domain name we are looking up.
  - TYPE- It contains the DNS record type.

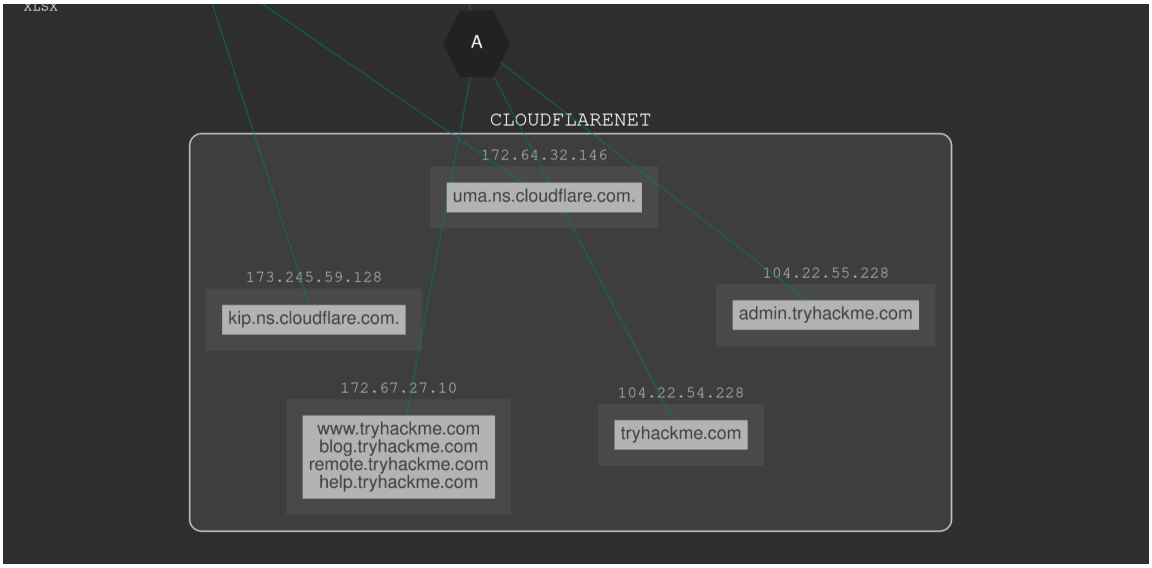
```
┌──(anishroy㉿linuxmint)-[~]
└─$ dig tryhackme.com MX

; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34869
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;tryhackme.com.                 IN      MX

;; ANSWER SECTION:
tryhackme.com.          300     IN      MX      1 aspmx.l.google.com.
tryhackme.com.          300     IN      MX      10 alt3.aspmx.l.google.com.
tryhackme.com.          300     IN      MX      10 alt4.aspmx.l.google.com.
tryhackme.com.          300     IN      MX      5 alt1.aspmx.l.google.com.
tryhackme.com.          300     IN      MX      5 alt2.aspmx.l.google.com.

;; Query time: 32 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Apr 13 20:54:35 IST 2023
;; MSG SIZE  rcvd: 157
```

- We can see that **dig** returned more information as compared to **nslookup**.
    - To query a **1.1.1.1** DNS server, we can execute - `dig @1.1.1.1 tryhackme.com MX`

DNSDumpster

- DNS lookup tools, such as nslookup and dig, cannot find subdomains on their own.
- We can use online services such as DNSDumpster to discover subdomains and many other info in a easy-to-read tables and graphs.
- When searching for tryhackme.com in DNSDumpster-

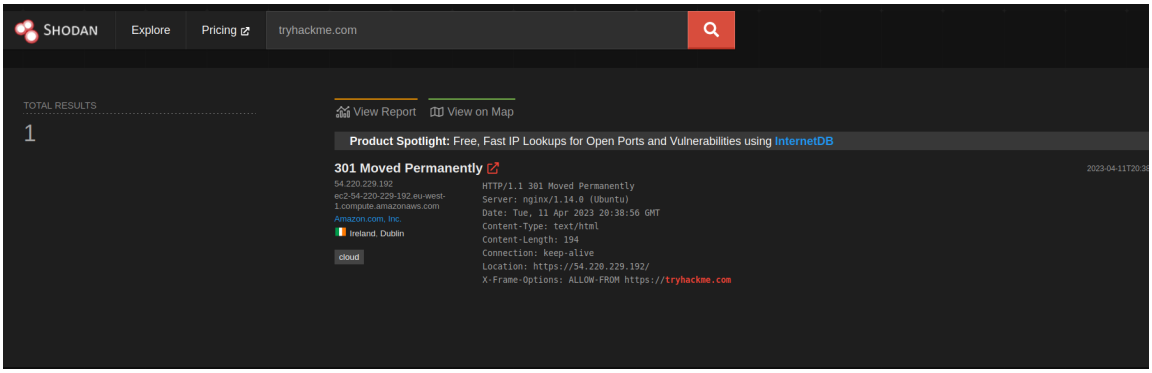




Shodan.io

- It tries to connect every device reachable online to build a search engine of connected “things”.
- Searching for tryhackme.com on shodan.io .
- We can learn several things such as:
  - IP address
  - hosting company
  - geographic location

- server type and version



Summary

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