

Passive Reconnaissance

Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.

In this room, after we define passive reconnaissance and active reconnaissance, we focus on essential tools related to passive reconnaissance. We will learn three command-line tools:

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

We will also learn the usage of two online services:

- DNSDumpster
- Shodan.io

These two online services allow us to collect information about our target without directly connecting to it.

Task 2

Passive Versus Active Recon

Before the dawn of computer systems and networks, in the Art of War, Sun Tzu taught, “If you know the enemy and know yourself, your victory will not stand in doubt.” If you are playing the role of an attacker, you need to gather information about your target systems. If

you are playing the role of a defender, you need to know what your adversary will discover about your systems and networks.

Reconnaissance (recon) can be defined as 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. We divide reconnaissance into:

1. Passive Reconnaissance
2. Active Reconnaissance

In passive reconnaissance, you rely on publicly available knowledge. It is the knowledge that you can access from publicly available resources without directly engaging with the target. Think of it like you are looking at target territory from afar without stepping foot on that territory.

Passive reconnaissance activities include many activities, for instance:

- 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.

Considering the invasive nature of active reconnaissance, one can quickly get into legal trouble unless one obtains proper legal authorisation.

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)**

ans: **passive reconnaissance**

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)**

ans: **active reconnaissance**

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?

ans: active reconnaissance

Task 3

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 it is leasing. The WHOIS server replies with various information related to the domain requested. Of particular interest, we can learn:

- 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 it last updated? And when does it need to be renewed?
- Name Server: Which server to ask to resolve the domain name?

To get this information, we need to use a `whois` client or an online service. Many online services provide `whois` information; however, it is generally faster and more convenient to use your local whois client. Using the AttackBox (or your local Linux machine, such as Parrot or Kali), you can easily access your whois client on the terminal. The syntax is `whois DOMAIN_NAME`, where `DOMAIN_NAME` is the domain about which you are trying to get more information. Consider the following example executing `whois tryhackme.com`.

```
root@kali: /home/kali
root@kali: /home/kali 157x36
root@kali) - [ /home/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
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-08-31T00:00:44Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
```

We can find the registrant's name and contact information unless they are using some privacy service. Although not displayed above, we get the admin and tech contacts for this domain. Finally, we see the domain name servers that we should query if we have any DNS records to look up.

1. **When was TryHackMe.com registered?**

ans: **20180705**

2. **What is the registrar of TryHackMe.com?**

ans: **namecheap.com**

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

ans: **cloudflare.com**

Task 4

nslookup and dig

Find the IP address of a domain name using `nslookup`, which stands for Name Server Look Up. You need to issue the command `nslookup DOMAIN_NAME`, for example, `nslookup tryhackme.com`. Or, more generally, you can use `nslookup OPTIONS DOMAIN_NAME SERVER`.

These three main parameters are:

- OPTIONS contains the query type as shown in the table below. For instance, you can use `A` for IPv4 addresses and `AAAA` for IPv6 addresses.
- DOMAIN_NAME is the domain name you are looking up.
- SERVER is the DNS server that you want to query. You can choose any local or public DNS server to query. Cloudflare offers `1.1.1.1` and `1.0.0.1`, Google offers `8.8.8.8` and `8.8.4.4`, and Quad9 offers `9.9.9.9` and `149.112.112.112`. There are many more public DNS servers that you can choose from if you want alternatives to your ISP's DNS servers.

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

For instance, `nslookup -type=A tryhackme.com 1.1.1.1` (or `nslookup -type=a tryhackme.com 1.1.1.1` as it is case-insensitive) can be used to return all the IPv4 addresses used by tryhackme.com.

```
root@kali: /home/kali
root@kali: /home/kali
root@kali: /home/kali 94x23

(root@kali)-[/home/kali]
# nslookup -type=A sathyabama.ac.com
Server:      A 192.168.220.2 Addresses
Address:     192.168.220.2#53

Non-authoritative answer:
Name:   sathyabama.ac.com Canonical Name
Address: 199.59.243.224 Mail Servers

SOA Start of Authority

XT Records

For instance, the following command can be used to return all the IPv4 addresses used by tryhackme.com.
```

The A and AAAA records are used to return IPv4 and IPv6 addresses, respectively.

Let's say you want to learn about the email servers and configurations for a particular domain. You can issue `nslookup -type=MX tryhackme.com`

```
root@kali: /home/kali
root@kali: /home/kali
root@kali: /home/kali 94x23

(root@kali)-[/home/kali]
# nslookup -type=MX sathyabama.ac.in
Server:      192.168.220.2
Address:     192.168.220.2#53

Non-authoritative answer:
sathyabama.ac.in mail exchanger = 1 aspmx.l.google.com.
sathyabama.ac.in mail exchanger = 10 aspmx2.googlemail.com.
sathyabama.ac.in mail exchanger = 5 alt2.aspmx.l.google.com.
sathyabama.ac.in mail exchanger = 5 alt1.aspmx.l.google.com.
sathyabama.ac.in mail exchanger = 10 aspmx3.googlemail.com.

Authoritative answers can be found from:

(root@kali)-[/home/kali]
#
```

```
Terminal

user@TryHackMe$ nslookup -type=MX tryhackme.com
Server:      127.0.0.53
Address:     127.0.0.53#53

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

We can see that tryhackme.com's current email configuration uses Google. Since MX is looking up the Mail Exchange servers, we notice that when a mail server tries to deliver email `@tryhackme.com`, it will try to connect to the `aspmx.l.google.com`, which has order 1. 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`.

You can repeat similar queries for other domain names and try different types, such as `-type=txt`. Who knows what kind of information you might discover along your way!

`dig`, the acronym for “Domain Information Groper,” if you are curious. Let’s use `dig` to look up the MX records and compare them to `nslookup`. We can use `dig DOMAIN_NAME`, but to specify the record type, we would use `dig DOMAIN_NAME TYPE`. Optionally, we can select the server we want to query using `dig @SERVER DOMAIN_NAME TYPE`

- SERVER is the DNS server that you want to query.
- DOMAIN_NAME is the domain name you are looking up.
- TYPE contains the DNS record type, as shown in the table provided earlier.

```
(root@kali)~/home/kali
# dig sathyabama.ac.in MX

;<>> DiG 9.18.16-1-Debian <>> sathyabama.ac.in MX
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 12033
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: MBZ: 0x0005, udp: 4096
;; COOKIE: c66d402ce86f8c83378ecd1564efdd54abd7292996a2dca5 (good)
;; QUESTION SECTION:
;sathyabama.ac.in.                IN      MX

;; ANSWER SECTION:
sathyabama.ac.in.                5       IN      MX      5 alt2.aspmx.l.google.com.
sathyabama.ac.in.                5       IN      MX      1 aspmx.l.google.com.
sathyabama.ac.in.                5       IN      MX      10 aspmx2.googlemail.com.
sathyabama.ac.in.                5       IN      MX      10 aspmx3.googlemail.com.
sathyabama.ac.in.                5       IN      MX      5 alt1.aspmx.l.google.com.

;; Query time: 24 msec
;; SERVER: 192.168.220.2#53(192.168.220.2) (UDP)
;; WHEN: Thu Aug 31 05:52:43 IST 2023
;; MSG SIZE rcvd: 209
```

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


ans: `THM{a5b83929888ed36acb0272971e438d78}`

Task 5

DNSDumpster

DNSdumpster.com - dns recon and research, find and lookup dns records

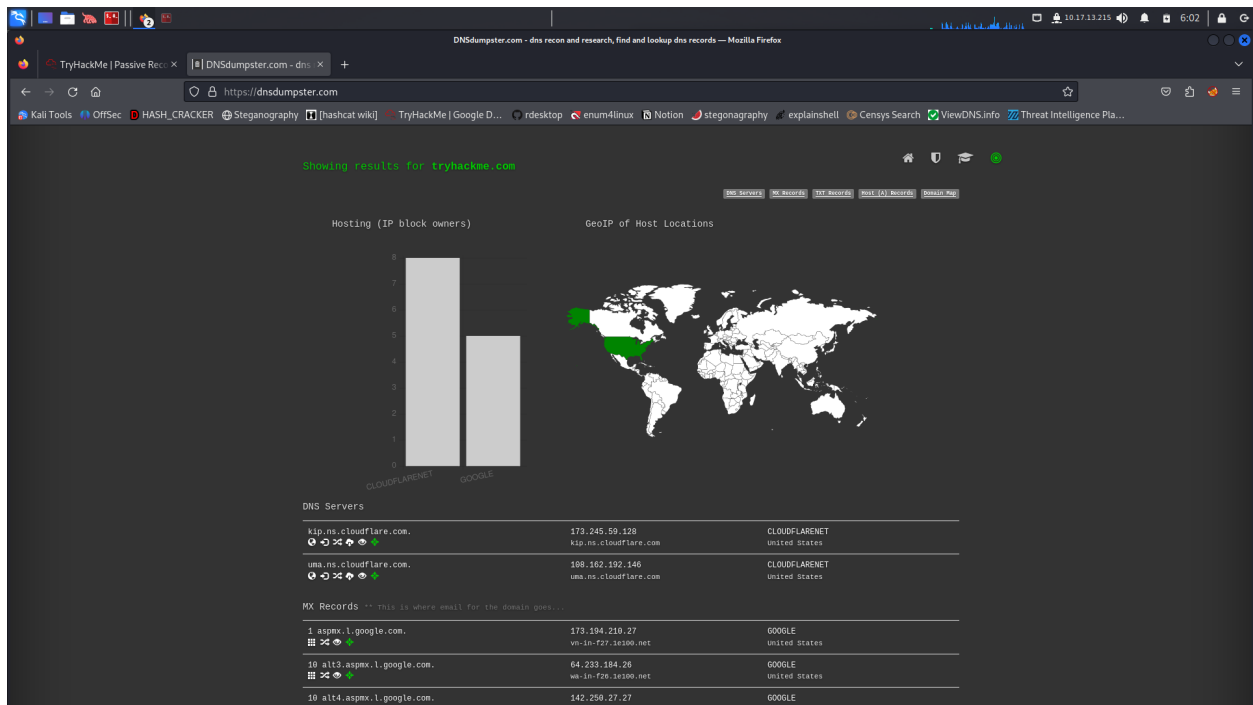
Find dns records in order to identify the Internet footprint of an organization. Recon that enables deeper security assessments and discovery of the attack surface.

 <https://dnsdumpster.com/>

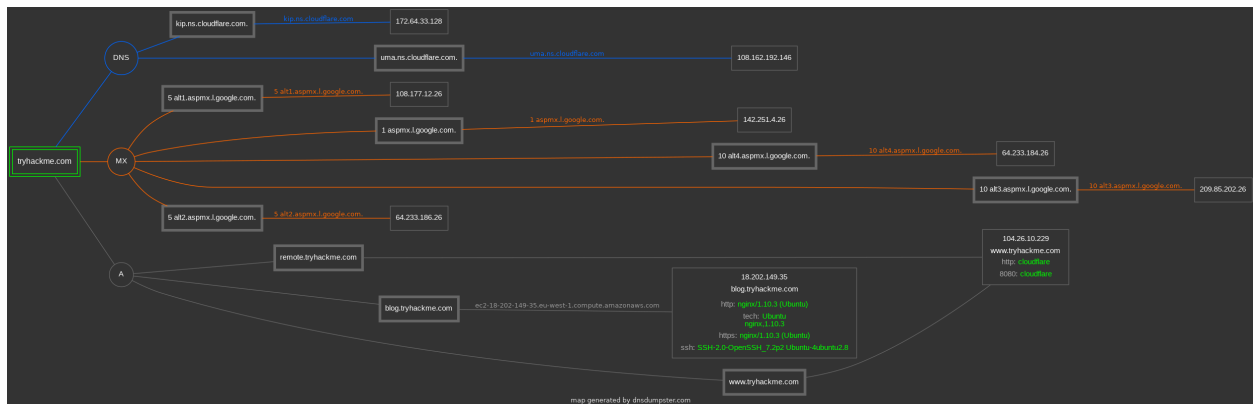
DNS lookup tools, such as nslookup and dig, cannot find subdomains on their own. The domain you are inspecting might include a different subdomain that can reveal much information about the target. For instance, if tryhackme.com has the subdomains wiki.tryhackme.com and webmail.tryhackme.com, you want to learn more about these two as they can hold a trove of information about your target.

We can consider using multiple search engines to compile a list of publicly known subdomains. One search engine won't be enough; moreover, we should expect to go through at least tens of results to find interesting data. After all, you are looking for subdomains that are not explicitly advertised, and hence it is not necessary to make it to the first page of search results. Another approach to discover such subdomains would be to rely on brute-forcing queries to find which subdomains have DNS records.

To avoid such a time-consuming search, one can use an online service that offers detailed answers to DNS queries, such as DNSDumpster. If we search DNSDumpster for `tryhackme.com`, we will discover the subdomain `blog.tryhackme.com`, which a typical DNS query cannot provide. In addition, DNSDumpster will return the collected DNS information in easy-to-read tables and a graph. DNSDumpster will also provide any collected information about listening servers.



DNSDumpster will also represent the collected information graphically. DNSDumpster displayed the data from the table earlier as a graph. You can see the DNS and MX branching to their respective servers and also showing the IP addresses.



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

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)			🏠	🛡️	🎓
tryhackme.com 🔍 🔒 🔓 🔑 HTTP: cloudflare	104.22.54.228	CLOUDFLARENET unknown			
www.tryhackme.com 🔍 🔒 🔓 🔑 HTTP: cloudflare	172.67.27.10	CLOUDFLARENET United States			
blog.tryhackme.com 🔍 🔒 🔓 🔑 HTTP: cloudflare	172.67.27.10	CLOUDFLARENET United States			
remote.tryhackme.com 🔍 🔒 🔓 🔑 HTTP: cloudflare	172.67.27.10	CLOUDFLARENET United States			
admin.tryhackme.com 🔍 🔒 🔓 🔑 HTTP: cloudflare	104.22.55.228	CLOUDFLARENET unknown			
help.tryhackme.com 🔍 🔒 🔓 🔑 HTTP: cloudflare	172.67.27.10	CLOUDFLARENET United States			


ans: **remote**

Task 6

Shodan.io

Shodan

Search engine of Internet-connected devices. Create a free account to get started.

 <https://www.shodan.io/>

Shodan

// USAGE

- More than 4 million users
- Data on thousands of ports
- Globally distributed network of crawlers

// SERVICES

Search the Internet

Go beyond the web. Search the entire Internet for connected devices.

Monitor Networks

Know what you have exposed to the Internet and get notified when that changes.

Build Products

Leverage the Shodan API to give your products unprecedented insights about the Internet.

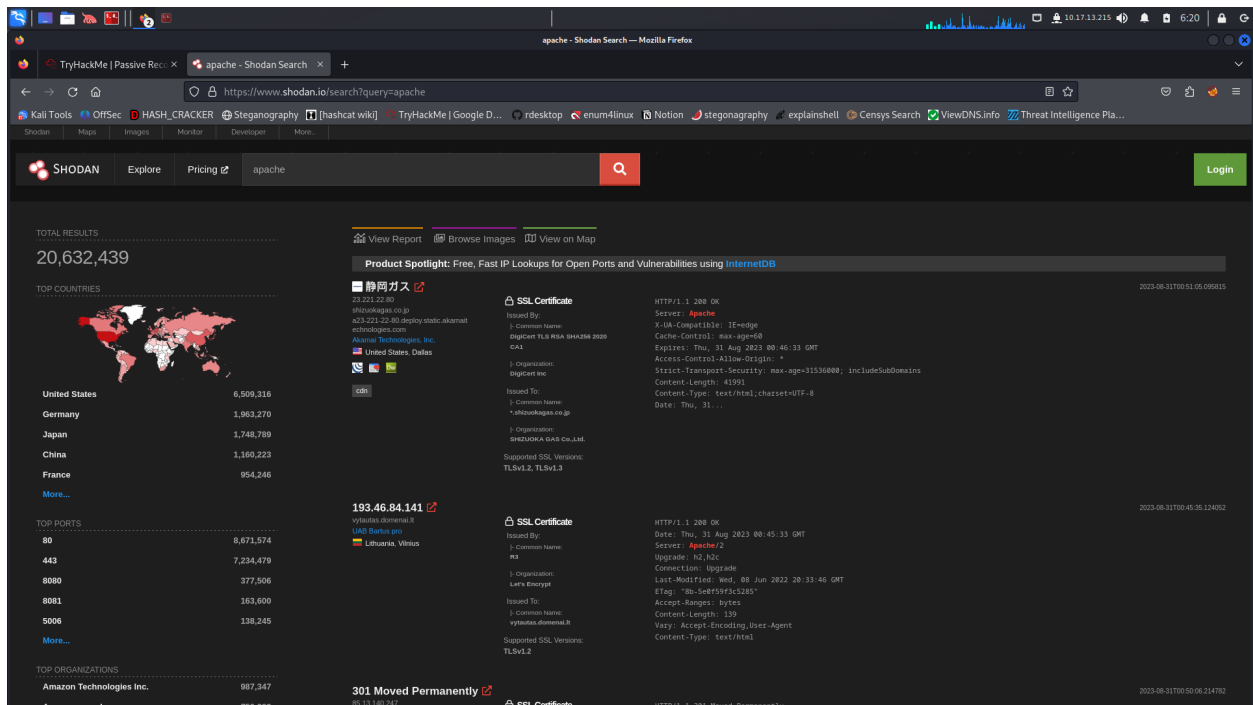
When you are tasked to run a penetration test against specific targets, as part of the passive reconnaissance phase, a service like Shodan.io can be helpful to learn various pieces of information about the client's network, without actively connecting to it.

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. Consider the saved record of one of tryhackme.com's servers.

This record shows a web server; however, as mentioned already, Shodan.io collects information related to any device it can find connected online. Searching for `tryhackme.com` on Shodan.io will display at least the record shown in the screenshot above. Via this Shodan.io search result, we can learn several things related to our search, such as:

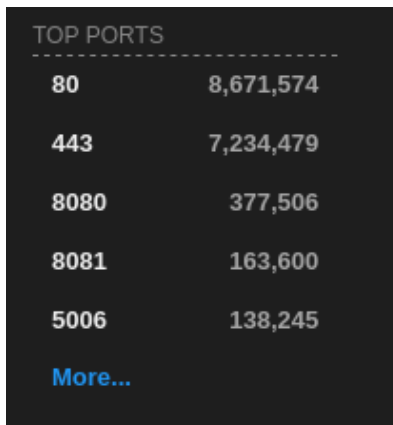
- IP address
- hosting company
- geographic location
- server type and version

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



ans: **germany**

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



ans: **8080**

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

ans: **888**

Task 7

Summary

In this room, we focused on passive reconnaissance. In particular, we covered command-line tools, `whois`, `nslookup`, and `dig`. We also discussed two publicly available services [DNSDumpster](#) and [Shodan.io](#).

The power of such tools is that you can collect information about your targets without directly connecting to them. Moreover, the trove of information you may find using such tools can be massive once you master the search options and get used to reading the results.

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

Learn more about DNS at [DNS in Detail](#).