

# THM-Passive Reconnaissance(被动侦察基础)-学习

---

本文相关的TryHackMe实验房间链接：<https://tryhackme.com/room/passiverecon>

## H2 简介

本文将阐述被动侦察和主动侦察的基本概念，然后重点介绍与被动侦察相关的一些必要工具，我们将学习以下三个用于被动侦察的命令行工具：

- whois: 查询 WHOIS 服务器（WHOIS的含义是域名查询服务）
- nslookup: 查询 DNS 服务器
- dig: 查询 DNS 服务器

我们可以使用whois工具来查询WHOIS记录，使用 nslookup 和 dig工具来查询 DNS 数据库记录，这些都是公开的记录，因此不会惊动你想要渗透的目标。

我们还会了解两个在线工具的使用：

- DNSDumpster
- Shodan.io

这两个在线网站服务工具允许我们收集关于目标的信息，并且无需直接连接到目标。在学习本文知识点之前，建议先了解网络基础知识以及关于linux命令行的基础知识。

## H2 被动侦察VS主动侦察

在计算机系统和网络出现之前，孙子在《孙子兵法》中教导说：“知己知彼，百战不殆”，在网络攻防中：如果你扮演的是攻击者的角色，你需要收集有关目标系统的信息；如果你扮演的是防御者的角色，你需要知道你的对手会发现哪些关于你的系统和网络的信息。

侦察(recon)可以定义为收集目标信息的初步调查，这是统一杀伤链中在系统上获得初步立足点的第一步--关于统一杀伤链：<https://www.unifiedkillchain.com/>

我们将侦察分为：

- 1.被动侦察（被动信息收集）；

- 2.主动侦察（主动信息收集）。

在被动侦察中，你将依赖于公开可用的知识，关于这些知识你无需直接与目标接触即可从公开可用的资源中进行获取，你可以把被动侦察想象成 你是从远处看着目标区域，而不是实际踏进目标区域。



被动侦察包括许多活动，例如：

- 从公共DNS服务器中查找目标域的 DNS 记录。
- 查看与目标网站相关的招聘广告。
- 阅读有关目标公司的新闻。

而在主动侦察中，无法像被动侦察一样谨慎地实现侦察目的，主动侦察需要与目标进行直接接触，你可以把主动侦察想象成你正在检查门窗上的锁，以及正在检查其他潜在的进入目标的入口点。



主动侦察活动的例子包括：

- 连接到目标公司的服务器，例如 HTTP、FTP 和 SMTP等。
- 致电目标公司以尝试获取信息（社会工程学）。
- 冒充修理工进入目标公司场所。

考虑到主动侦察的侵入性，你需要在获得适当的法律授权的情况下才能开展相关活动，否则你可能很快就会陷入法律纠纷中。

## 答题

### 回答以下问题

您访问目标公司的 Facebook 页面，希望获得他们的一些员工姓名。这是什么侦察活动？（A代表主动，P代表被动）

P

正确答案

您 ping 公司网络服务器的 IP 地址以检查 ICMP 流量是否被阻止。这是什么侦察活动？（A代表主动，P代表被动）

A

正确答案

你碰巧在聚会上遇到了目标公司的 IT 管理员。您尝试使用社会工程来获取有关他们的系统和网络基础设施的更多信息。这是什么侦察活动？（A代表主动，P代表被动）

A

正确答案

## H2 Whois工具

WHOIS是遵循RFC 3912规范的请求和响应协议，WHOIS 服务器在TCP端口43上侦听传入的请求。在现实场景中：域名注册商负责维护其租用域名的WHOIS记录，WHOIS服务器则负责回复与请求的域相关的各种信息。

通过WHOIS我们可以了解：

注册商：域名是通过哪个注册商注册的？

注册人的联系信息：姓名、组织、地址、电话等（如果使用了隐私服务隐藏，则注册人的联系信息将不可见）。

创建、更新和到期日期：域名首次注册的时间是什么时候？ 最后一次更新是什么时候？ 什么时候需要更新？

名称服务器：将请求哪个服务器来解析域名？

要获取以上信息，我们需要使用 whois 客户端或在线服务。虽然许多在线服务都能够提供whois信息，但是，使用本地 whois 客户端获取信息通常更快、更方便。

通过使用你本地的Linux 机器，例如 Parrot 或 Kali，你可以轻松地到你的攻击机终端上访问whois 客户端。基础语法是 `whois DOMAIN_NAME`，其中DOMAIN\_NAME 是你尝试想获取更多信息的目标域。

以下是执行 `whois tryhackme.com` 命令的示例。



```
user@TryHackMe$ whois tryhackme.com
[Querying whois.verisign-grs.com]
[Redirected to whois.namecheap.com]
[Querying whois.namecheap.com]
```

```
[whois.namecheap.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: 2021-05-01T19:43:23.31Z
Creation Date: 2018-07-05T19:46:15.00Z
Registrar Registration Expiration Date: 2027-07-05T19:46:15.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Withheld for Privacy Purposes
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
[ ... ]
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-08-25T14:58:29.57Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

从上面的示例中，我们能够看到很多信息，现在按照显示的顺序查看这些信息：首先，我们注意到我们被重定向到 `whois.namecheap.com` 以获取WHOIS信息，正在维护目标域名的WHOIS记录的是 `namecheap.com`，此外，我们还可以看到域名的创建日期以及最后更新日期和到期日期等信息。

接下来，我们获取到有关注册商和注册人的信息，我们可以找到注册人的姓名和联系信息，除非他们使用了某些隐私服务（在现实环境下通常都会使用隐私服务）。

最后，我们可以看到能够被查询的域名服务器信息，此处的信息有助于我们之后查找DNS记录。

我们可以检查收集到的信息以发现新的攻击面，例如考虑社会工程学攻击或技术攻击。根据渗透测试的范围，你可以尝试对管理员用户的电子邮件服务器或 DNS 服务器进行攻击，假设它们归你的客户所有并且也在预定的渗透测试范围之内。

需要注意的是，由于自动化工具会滥用 WHOIS 查询来获取电子邮件地址，因此许多WHOIS服务器会对此采取相应的措施，例如：他们可能会重新编辑电子邮件地址，此外，许多注册人都会设置隐私服务，以保持他们的信息私密性并且能够在一定程度上避免他们的电子邮件地址被垃圾邮件发送者获取。

## 答题

### 回答以下问题

TryHackMe.com 是什么时候注册的？

正确答案

💡暗示

TryHackMe.com 的注册商是什么？

正确答案

💡暗示

TryHackMe.com 将哪家公司用于名称服务器？

正确答案

💡暗示

```
root@ip-10-10-186-241:~# 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: 2022-10-20T16:10:16Z <<<
```

## H2 nslookup以及dig工具

在上一小节中，我们使用了WHOIS协议来获取目标域名的各种信息。值得注意的是：在WHOIS信息中，我们还能够从域名注册商那里获得关于DNS服务器的信息。

### nslookup

我们可以使用nslookup (Name Server Look Up) 查找域名的IP地址，该命令的用法是 `nslookup DOMAIN_NAME`，例如 `nslookup tryhackme.com`。

nslookup完整的语法是 `nslookup OPTIONS DOMAIN_NAME SERVER`，这三个主要参数的含义是：

- OPTIONS (选项) -包含查询类型，例如：你可以使用参数 A 用于查询IPv4 地址，使用参数 AAAA 用于查询 IPv6 地址。
- DOMAIN\_NAME (域名) -你想要查询的目标域名。
- SERVER (服务器) -该参数代表你要查询的DNS服务器，你可以选择任何本地或公共 DNS 服务器进行查询：Cloudflare 提供的DNS是 1.1.1.1 和 1.0.0.1，Google 提供的DNS是 8.8.8.8 和 8.8.4.4，Quad9

提供的DNS是 9.9.9.9 和 149.112.112.112，你可以任意选择公共 DNS 服务器，以此替代ISP所分配的本地DNS服务器。

Query type	Result
A	IPv4 Addresses
AAAA	IPv6 Addresses
CNAME	Canonical Name 规范名称（别名）
MX	Mail Servers
SOA	Start of Authority 起始授权机构
TXT	TXT Records

例如，`nslookup -type=A tryhackme.com 1.1.1.1`（或者输入 `-type=a` 因为此参数不区分大小写）可用于返回tryhackme.com使用的所有 IPv4 地址。

```
user@TryHackMe$ nslookup -type=A tryhackme.com 1.1.1.1
Server:      1.1.1.1
Address:     1.1.1.1#53

Non-authoritative answer:
Name:   tryhackme.com
Address: 172.67.69.208
Name:   tryhackme.com
Address: 104.26.11.229
Name:   tryhackme.com
Address: 104.26.10.229
```

A 和 AAAA 记录分别用于返回 IPv4 和 IPv6 地址，从渗透测试的角度了解此查找很有帮助。在上面的例子中，我们从一个域名开始，得到了三个 IPv4 地址，假设这些 IP 地址都在渗透测试的范围内，接下来则可以进一步检查每个 IP 地址的不安全性。

假设你了解特定域的电子邮件服务器和配置，你可以使用 `nslookup -type=MX tryhackme.com`，例子如下：



```
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.
```

我们可以看到 tryhackme.com 当前的电子邮件配置是使用Google邮件交换服务器。参数MX表示查找目标使用的 Mail Exchange 服务器，我们注意到当目标邮件服务器发送带@tryhackme.com的电子邮件时，它会先尝试连接到顺序为1的aspmx.l.google.com，如果它正忙或不可用，邮件服务器将尝试连接按顺序排列的下一个邮件交换服务器 alt1.aspmx.l.google.com 或 alt2.aspmx.l.google.com。

从以上信息可以得知：目标使用的是由Google 提供的邮件服务器；因此，我们不应期望目标邮件服务器使用的是易受攻击的服务器版本。但是，在其他情况下，我们也可能会发现目标邮件服务器并没有得到充分保护或漏洞修补。

## dig

如果需要更高级的 DNS 查询和附加功能，你可以使用dig工具，它是“Domain Information Groper”的首字母缩写词，我们可以使用 dig 查找 MX 记录并将它们与 nslookup得出的结果进行比较。

dig的一般语法是 `dig DOMAIN_NAME`，如果需要指定查询的记录类型，可以使用 `dig DOMAIN_NAME TYPE`，或者使用 `dig @SERVER DOMAIN_NAME TYPE` 以选择要查询的DNS服务器。

- SERVER 是你要查询的 DNS 服务器。
- DOMAIN\_NAME-是你要查找的域名。
- TYPE-是DNS记录类型，具体类型如前面提供的图表所示。



```
user@TryHackMe$ dig tryhackme.com MX

; <<>> DiG 9.16.19-RH <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->HEADER<
```

通过对nslookup 和 dig 的输出结果进行快速比较，可知dig返回了更多信息，例如默认情况下的 TTL（生存时间），如果要查询的DNS服务器为1.1.1.1，可以使用 `dig @1.1.1.1 tryhackme.com MX` 命令。



## 回答以下问题

检查 thmlabs.com 的 TXT 记录。那里的旗帜是什么？

THM{a5b83929888ed36acb0272971e438d78}

正确答案

```
root@ip-10-10-186-241:~# dig thmlabs.com TXT

; <<>> DiG 9.11.3-ubuntu1.13-Ubuntu <<>> thmlabs.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47236
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
thmlabs.com.                 300     IN      TXT      "THM{a5b83929888ed36acb0272971e438d78}"

;; Query time: 25 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Oct 20 17:04:43 BST 2022
;; MSG SIZE rcvd: 90
```

## H2 DNSDumpster--被动信息收集网站

DNS 查找工具（例如 nslookup 和 dig）无法自行查找子域，但是你现在正在检查的域可能包含一些不同的子域，这些子域可以揭示有关目标的更多信息。

例如，如果 tryhackme.com 有两个子域为 wiki.tryhackme.com 以及 webmail.tryhackme.com，你可能想了解更多关于这两个子域的信息，因为它们可能保存着关于目标的大量信息。可能这些子域之一已设置但是没有定期更新，缺乏适当的定期更新通常会导致子域上的服务易受攻击。

为了发现目标的子域，我们可以考虑使用多个搜索引擎来形成一个公开的子域列表。一个搜索引擎是不够的；此外，我们应该期望通过至少几十个结果来找到有用的数据，发现目标关键子域的另一种方法是依靠暴力查询来查找哪些子域具有 DNS 记录。

为了避免过于耗时的搜索工作，我们可以使用能够提供详细的 DNS 查询信息的一些在线服务，例如 DNSDumpster 网站。如果我们在 DNSDumpster 中搜索 tryhackme.com，我们会发现典型的 DNS 查询方式所无法提供的子域 blog.tryhackme.com；此外，DNSDumpster 将以易于阅读的表格和图表的形式返回收集到的 DNS 信息；DNSDumpster 还将提供任何收集到的有关监听服务器的信息。

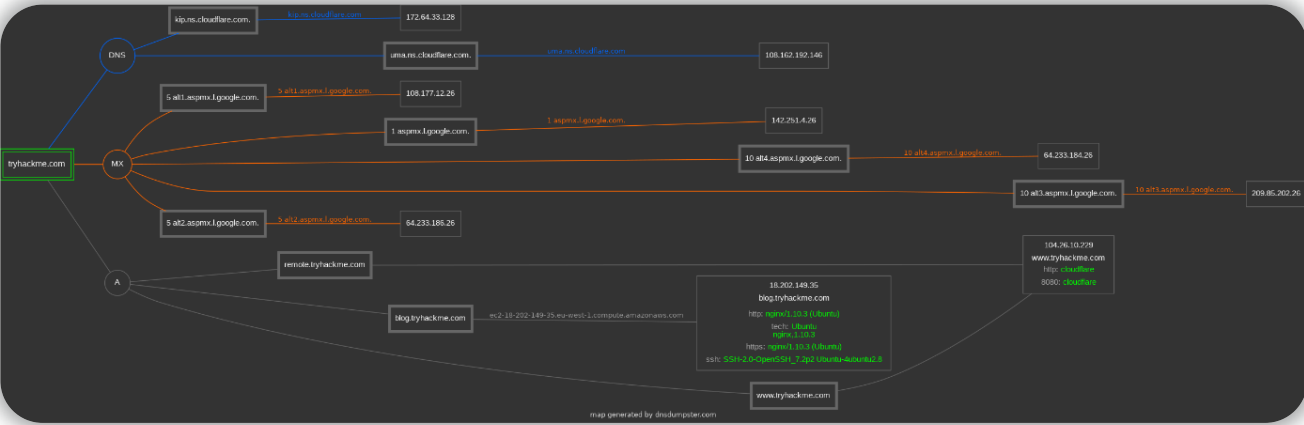
接下来，我们将在 DNSDumpster 上搜索 tryhackme.com，让你了解一下预期的输出结果。



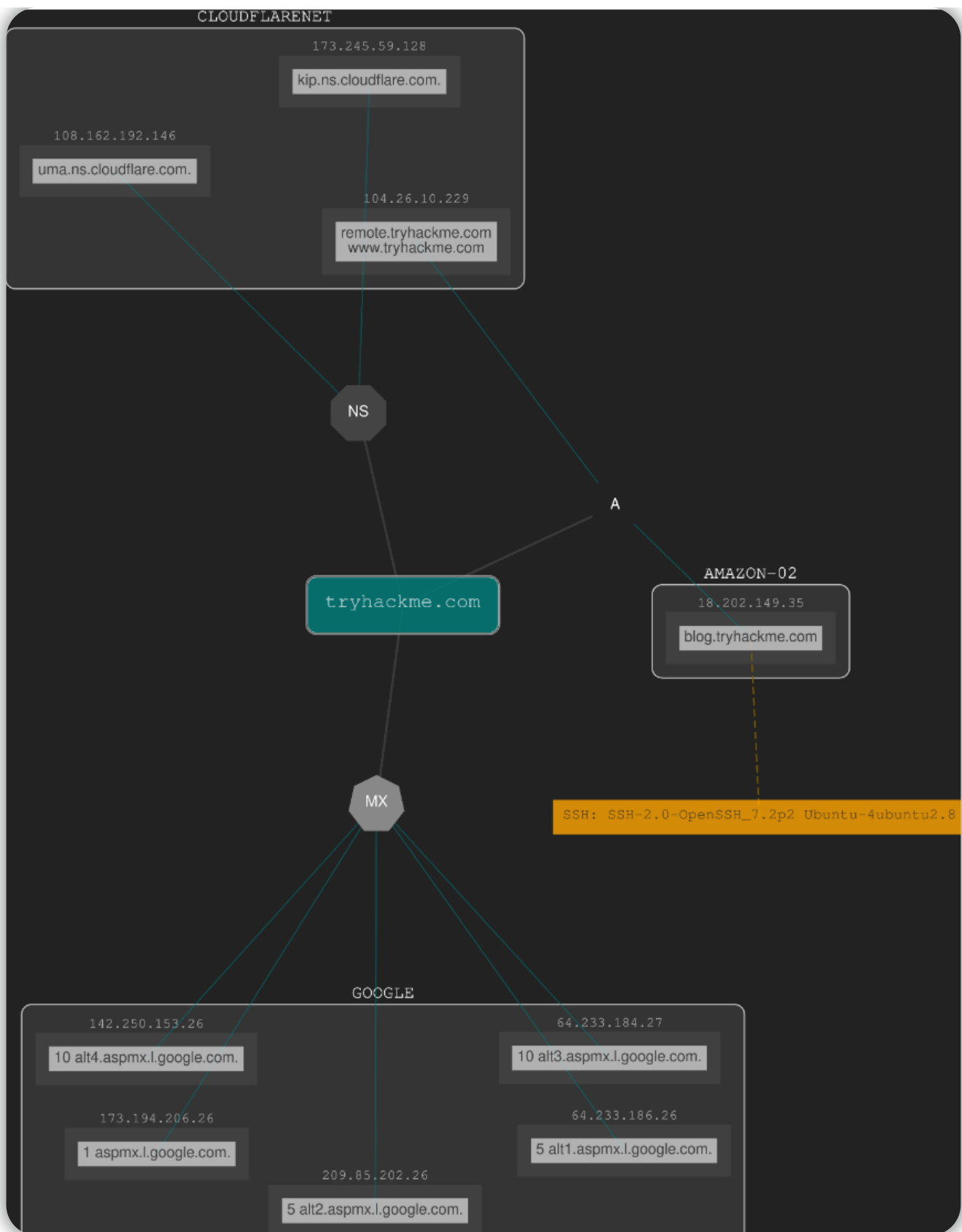
在下面示例的结果中，我们得到了我们正在查找的域的 DNS 服务器列表；DNSDumpster 会将域名解析为 IP 地址，甚至会尝试对其进行地理定位；我们还可以看到MX记录，DNSDumpster 将目标的所有五个邮件交换服务器解析为各自的 IP 地址，并提供有关所有者和位置的更多信息；最后，我们还可以看到 TXT 记录以及A记录。

DNS Servers		
kip.ns.cloudflare.com. 🌐 🔄 📶 📶 📶	108.162.193.128 kip.ns.cloudflare.com	CLOUDFLARENET United States
uma.ns.cloudflare.com. 🌐 🔄 📶 📶 📶	172.64.32.146 uma.ns.cloudflare.com	CLOUDFLARENET United States
MX Records ** This is where email for the domain goes...		
5 alt1.aspmx.l.google.com. 🌐 🔄 📶 📶 📶	108.177.12.26 ua-in-f26.1e100.net	GOOGLE United States
1 aspmx.l.google.com. 🌐 🔄 📶 📶 📶	142.250.123.26 gh-in-f26.1e100.net	GOOGLE United States
10 alt4.aspmx.l.google.com. 🌐 🔄 📶 📶 📶	64.233.184.26 wa-in-f26.1e100.net	GOOGLE United States
10 alt3.aspmx.l.google.com. 🌐 🔄 📶 📶 📶	209.85.202.26 dg-in-f26.1e100.net	GOOGLE United States
5 alt2.aspmx.l.google.com. 🌐 🔄 📶 📶 📶	64.233.186.26 cb-in-f26.1e100.net	GOOGLE United States
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations		
"google-site-verification=umR4x8HuzWMP5g3656JY1b-61NuryD0-GqGnYN130Ne"		
"v=spf1 include:_spf.google.com include:email.chargebee.com ~all"		
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
remote.tryhackme.com 🌐 🔄 📶 📶 📶 HTTP: <span>cloudflare</span> TCP8080: <span>cloudflare</span>	104.26.10.229	CLOUDFLARENET United States
blog.tryhackme.com 🌐 🔄 📶 📶 📶 HTTP: <span>nginx/1.10.3 (Ubuntu)</span> HTTPS: <span>nginx/1.10.3 (Ubuntu)</span> SSH: <span>SSH-2.0-OpenSSH_7.2p1 Ubuntu-4ubuntu0.6</span> HTTP TECH: <span>Ubuntu</span> nginx/1.10.3	18.202.149.35 ec2-18-202-149-35.eu-west-1.compute.amazonaws.com	AMAZON-02 Ireland

DNSDumpster还能以图形化的方式表示收集到的信息，将前面表格中的数据显示为图表：你可以看到DNS和MX到它们各自的服务器的分支，同时也能看到相关的ip地址。



DNSDumpster有一个功能允许你导出图表，你可以自由操纵图形界面并移动区块。

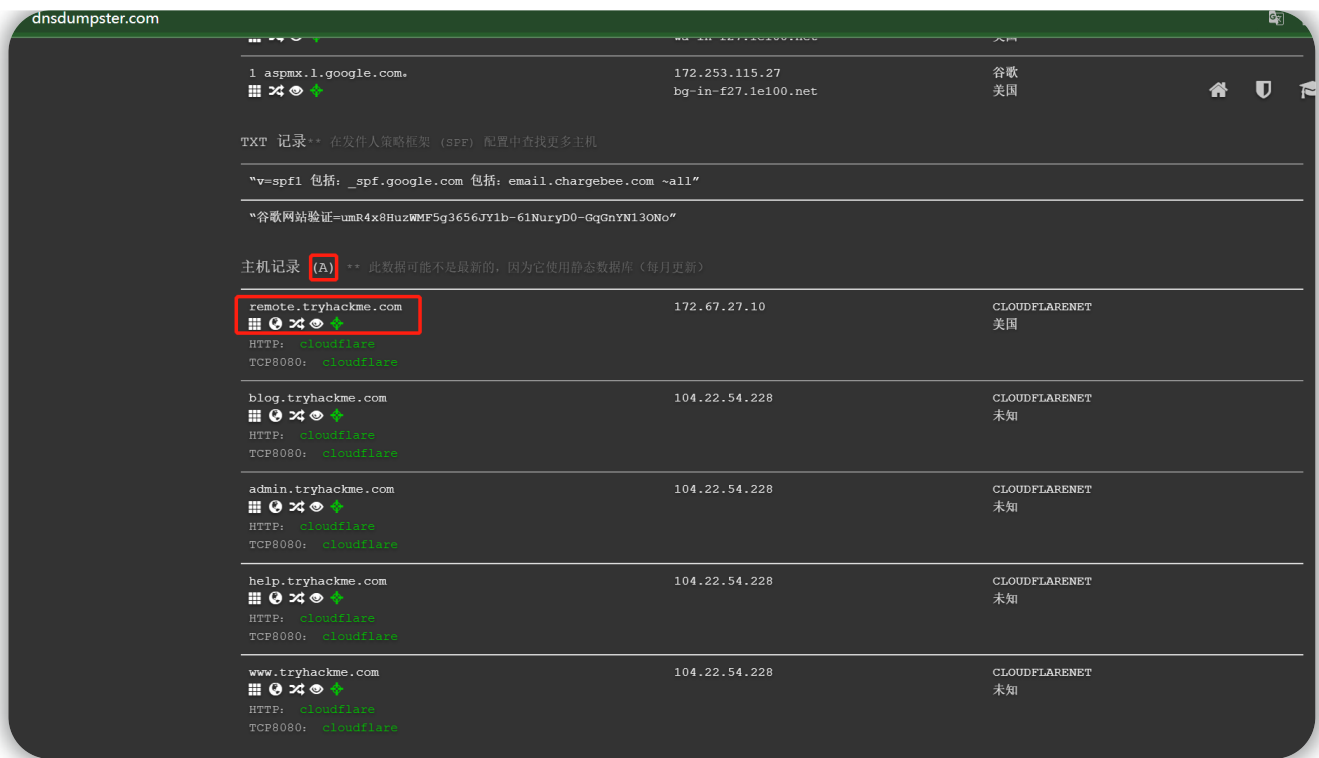


## 答题

### 回答以下问题

在 DNSDumpster 上查找 `tryhackme.com`。除了 `www` 和 `blog`，您还会发现什么有趣的子域？

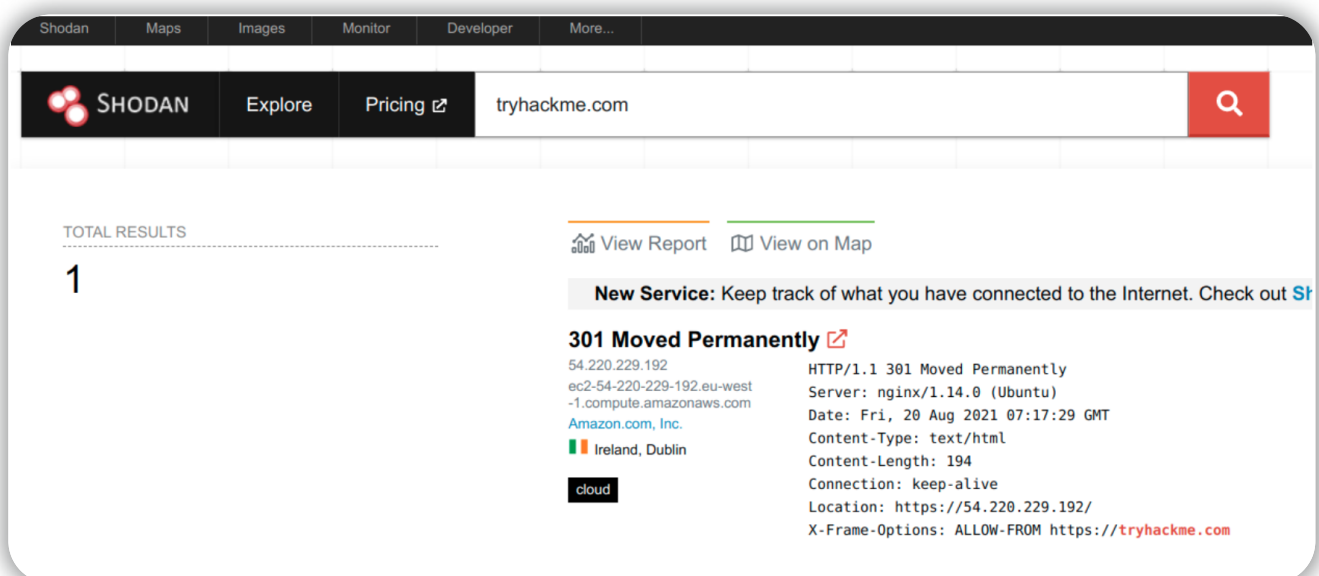
正确答案



## H2 Shodan.io--被动信息收集网站

当你的任务是针对特定目标进行渗透测试时, 作为被动侦察阶段的一部分, 像 Shodan.io 这样的网站服务可以帮助你了解有关客户端网络的各种信息, 而无需主动连接目标网络。此外, 在防御方面, 你也可以使用 Shodan.io 来了解属于你的组织的网络连接情况和暴露的网络设备情况。

Shodan.io 会尝试连接到所有可在线访问的网络设备, 以构建一个连接“物”的搜索引擎, 而不是简单的网页搜索引擎。Shodan 所发出的请求一旦得到响应, 它就会收集与服务相关的所有信息并将其保存在网站数据库中以便其内容变得可搜索。下图是 tryhackme.com 在 Shodan 中的一条信息记录。



该记录显示的是一个网络服务器，如前所述，Shodan.io 会收集与它可以在线找到的任何连接设备相关的信息，在 Shodan.io 上搜索 tryhackme.com 将至少显示上面截图中的记录。通过Shodan.io的搜索结果，我们可以了解到很多信息，例如：

- 服务器的IP地址
- 服务器的托管公司
- 服务器的地理位置
- 服务器类型和版本

你也可以尝试搜索从DNS查找中获得的 IP 地址，在Shodan的帮助页面上，你可以了解 Shodan.io 提供的所有搜索选项。

## 答题

### 回答以下问题

根据 Shodan.io 的说法，就可公开访问的Apache服务器的数量而言，世界上第二个国家是什么？

Germany

正确答案

根据 Shodan.io，Apache 使用的第三大常用端口是什么？

8080

正确答案

根据 Shodan.io，nginx 使用的第三个最常用的端口是什么？

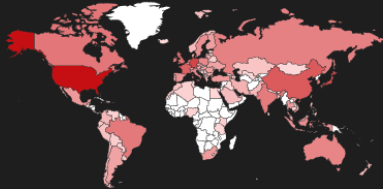
8888

正确答案

TOTAL RESULTS

25,476,161

TOP COUNTRIES



United States	8,000,349
Germany	2,427,760
Japan	2,036,787
China	1,399,251
France	1,207,681

[More...](#)

TOP PORTS

80	11,390,230
443	8,846,111
8080	511,013
8081	254,795
5006	191,763

[More...](#)[View Report](#) [Browse Images](#) [View on Map](#)

New Service: Keep track of what you have connected

## Site not found &amp;middot; DreamHost ↗

67.205.51.35

dp-5de652f92b.dreamhostps.  
com[New Dream Network, LLC](#)

United States, Portland

HTTP/1.1 200 OK

Date: Thu, 20 Oct 2022 16:17

Server: **Apache**

Last-Modified: Tue, 27 Sep 20

ETag: "360-5e9a5545fe680"

Accept-Ranges: bytes

Content-Length: 864

Content-Type: text/html

## ✖ Ametys - Connexion ↗

37.187.225.101

101.ip-37-187-225.eu

[OVH SAS](#)

France, Strasbourg

HTTP/1.1 200

Date: Thu, 20 Oct 2022 16:17

Server: **Apache**

Content-Security-Policy: def

Referrer-Policy: strict-orig

X-Frame-Options: SAMEORIGI...

## SquirrelMail - Login ↗

170.81.228.3

mail.agilinet.com.ar

[FIBERNEXT SRL](#)

Argentina, Viedma



HTTP/1.1 200 OK

Date: Thu, 20 Oct 2022 16:17

Server: **Apache**

Set-Cookie: SQMSESSID=o28cfm

Expires: Sat, 1 Jan 2000 00:0

Cache-Control: no-cache, no-

Pragma: no-cache

SHODAN

Explore

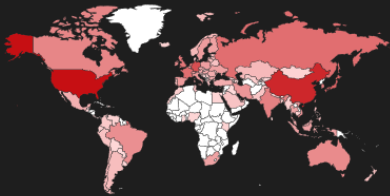
Pricing

nginx

TOTAL RESULTS

29,964,361

TOP COUNTRIES



United States	9,045,952
China	5,417,466
Hong Kong	3,471,750
Germany	2,040,133
Japan	1,121,612
More...	

TOP PORTS

80	10,684,090
443	6,919,940
8888	885,112
5001	558,844
5000	521,602

View Report

Browse Images

View on Map

New Service: Keep track of what you have connected

404 Not Found

172.82.182.198  
QuickPacket, LLC  
United States, Los Angeles

HTTP/1.1 200 OK  
Server: nginx  
Date: Thu, 20 Oct 2022 16:00:00 GMT  
Content-Type: text/html  
Content-Length: 138  
Last-Modified: Sat, 01 Oct 2022 16:00:00 GMT  
Connection: keep-alive  
ETag: "63383c2f-8a"  
Accept-Ranges: bytes

404 Not Found

210.16.99.239  
Asia Pacific Network Information Centre  
United States, Los Angeles

HTTP/1.1 404 Not Found  
Server: nginx  
Date: Thu, 20 Oct 2022 16:00:00 GMT  
Content-Type: text/html  
Content-Length: 566  
Connection: keep-alive

151.80.123.8

ip8.ip-151-80-123.eu  
OVH SAS  
France, Ermont

HTTP/1.1 403 Forbidden  
Server: nginx  
Date: Thu, 20 Oct 2022 16:00:00 GMT  
Content-Type: text/html  
Content-Length: 146

## H2 小结

在本文中，我们专注于被动侦察，主要介绍了三个命令行工具：whois、nslookup 和 dig；还介绍了两个公开可用的在线服务：DNSDumpster 和 Shodan.io。此类工具的强大之处在于你可以被动收集有关目标的信息，而无需直接连接到目标。

一旦你掌握了搜索选项并习惯了阅读查询的结果，使用此类工具可能会帮助你在渗透测试前期找到大量目标相关的信息。

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>