THM-Subdomain Enumeration(子域名枚举)-学习

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

H2 简介

子域名枚举是为一个域查找有效子域的过程，在本节中我们将学习发现子域的各种方法，我们这样做是为了扩大我们的攻击面，试图发现更多潜在的漏洞点。

我们将探讨三种不同的子域枚举方法: Brute Force、 OSINT (开放来源情报)和 Virtual Host（虚拟主机）

答题

H2 OSINT - SSL/TLS证书

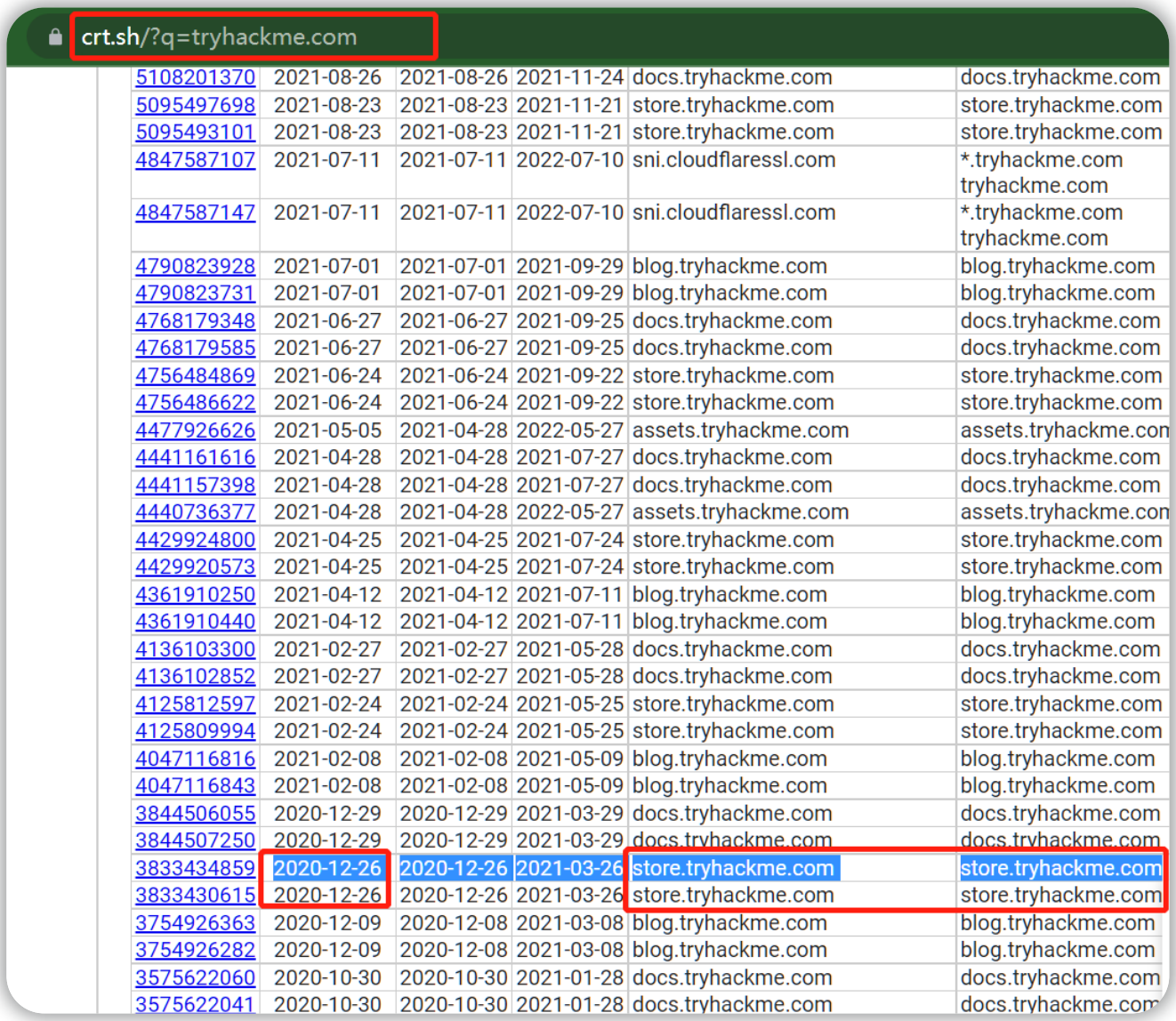
SSL/TLS 证书

当 SSL/TLS（Secure Sockets Layer/Transport Layer Security）证书 由 CA（Certificate Authority 数字证书认证机构）颁发给某个域名时，CA 会参与所谓的“证书透明度(CT)日志”。这些日志是 被颁发给一些域名的每个 SSL/TLS 证书 的公共访问日志。

证书透明度日志存在的目的 是为了阻止恶意和意外创建的证书被使用，我们可以利用这项服务 来发现属于一个域名的子域名,我们可以通过在线网站 http://crt.sh/ 以及 https://ui.ctsearch.entrust.com/ui/ctsearchui 所提供的一个可搜索的证书数据库，来查找某个证书的当前和历史记录。

答题

使用 http://crt.sh/ 搜索域名 tryhackme.com ，找到2020-12-26的记录并查看登记的子域名。



5108201370	2021-08-26	2021-08-26	2021-11-24	docs.tryhackme.com	docs.tryhackme.com
5095497698	2021-08-23	2021-08-23	2021-11-21	store.tryhackme.com	store.tryhackme.com
5095493101	2021-08-23	2021-08-23	2021-11-21	store.tryhackme.com	store.tryhackme.com
4847587107	2021-07-11	2021-07-11	2022-07-10	sni.cloudflaressl.com	*.tryhackme.com tryhackme.com
4847587147	2021-07-11	2021-07-11	2022-07-10	sni.cloudflaressl.com	*.tryhackme.com tryhackme.com
4790823928	2021-07-01	2021-07-01	2021-09-29	blog.tryhackme.com	blog.tryhackme.com
4790823731	2021-07-01	2021-07-01	2021-09-29	blog.tryhackme.com	blog.tryhackme.com
4768179348	2021-06-27	2021-06-27	2021-09-25	docs.tryhackme.com	docs.tryhackme.com
4768179585	2021-06-27	2021-06-27	2021-09-25	docs.tryhackme.com	docs.tryhackme.com
4756484869	2021-06-24	2021-06-24	2021-09-22	store.tryhackme.com	store.tryhackme.com
4756486622	2021-06-24	2021-06-24	2021-09-22	store.tryhackme.com	store.tryhackme.com
4477926626	2021-05-05	2021-04-28	2022-05-27	assets.tryhackme.com	assets.tryhackme.com
4441161616	2021-04-28	2021-04-28	2021-07-27	docs.tryhackme.com	docs.tryhackme.com
4441157398	2021-04-28	2021-04-28	2021-07-27	docs.tryhackme.com	docs.tryhackme.com
4440736377	2021-04-28	2021-04-28	2022-05-27	assets.tryhackme.com	assets.tryhackme.com
4429924800	2021-04-25	2021-04-25	2021-07-24	store.tryhackme.com	store.tryhackme.com
4429920573	2021-04-25	2021-04-25	2021-07-24	store.tryhackme.com	store.tryhackme.com
4361910250	2021-04-12	2021-04-12	2021-07-11	blog.tryhackme.com	blog.tryhackme.com
4361910440	2021-04-12	2021-04-12	2021-07-11	blog.tryhackme.com	blog.tryhackme.com
4136103300	2021-02-27	2021-02-27	2021-05-28	docs.tryhackme.com	docs.tryhackme.com
4136102852	2021-02-27	2021-02-27	2021-05-28	docs.tryhackme.com	docs.tryhackme.com
4125812597	2021-02-24	2021-02-24	2021-05-25	store.tryhackme.com	store.tryhackme.com
4125809994	2021-02-24	2021-02-24	2021-05-25	store.tryhackme.com	store.tryhackme.com
4047116816	2021-02-08	2021-02-08	2021-05-09	blog.tryhackme.com	blog.tryhackme.com
4047116843	2021-02-08	2021-02-08	2021-05-09	blog.tryhackme.com	blog.tryhackme.com
3844506055	2020-12-29	2020-12-29	2021-03-29	docs.tryhackme.com	docs.tryhackme.com
3844507250	2020-12-29	2020-12-29	2021-03-29	docs.tryhackme.com	docs.tryhackme.com
3833434859	2020-12-26	2020-12-26	2021-03-26	store.tryhackme.com	store.tryhackme.com
3833430615	2020-12-26	2020-12-26	2021-03-26	store.tryhackme.com	store.tryhackme.com
3754926363	2020-12-09	2020-12-08	2021-03-08	blog.tryhackme.com	blog.tryhackme.com
3754926282	2020-12-09	2020-12-08	2021-03-08	blog.tryhackme.com	blog.tryhackme.com
3575622060	2020-10-30	2020-10-30	2021-01-28	docs.tryhackme.com	docs.tryhackme.com
3575622041	2020-10-30	2020-10-30	2021-01-28	docs.tryhackme.com	docs.tryhackme.com

H2 OSINT - 搜索引擎

搜索引擎

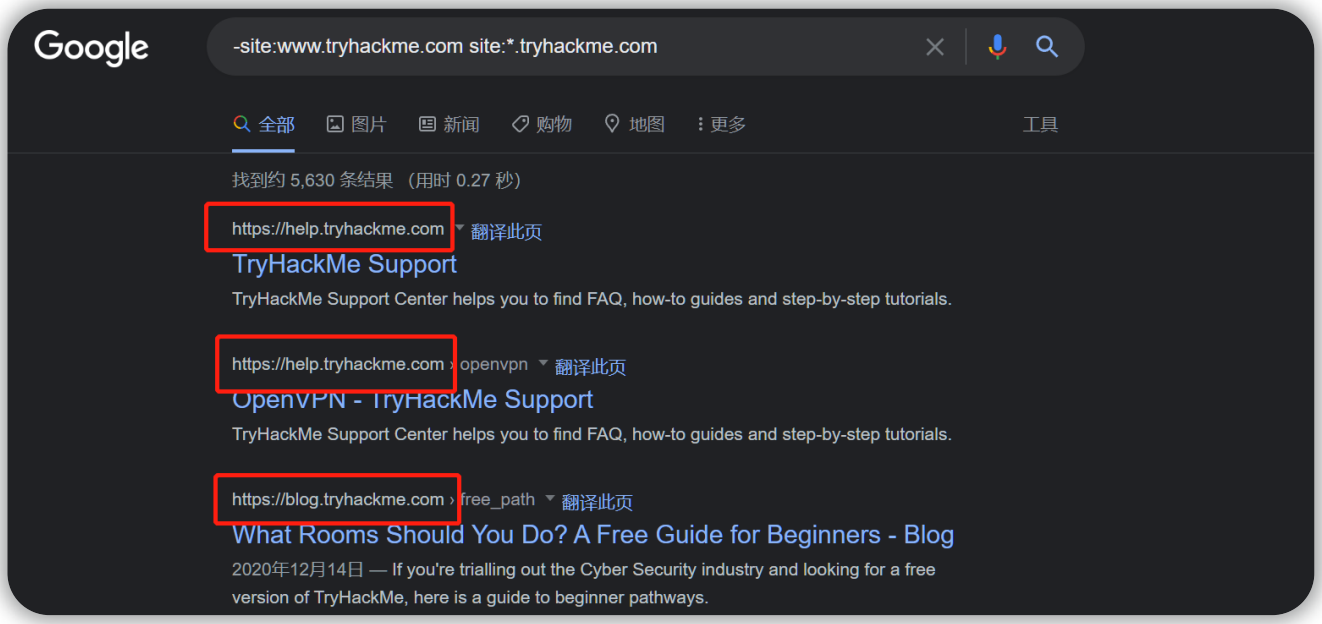
搜索引擎包含数万亿个链接，指向超过 10 亿个网站，是寻找子域名的绝佳途径。在 Google 等网站上使用高级搜索方法，如site:filter，可以缩小搜索结果。

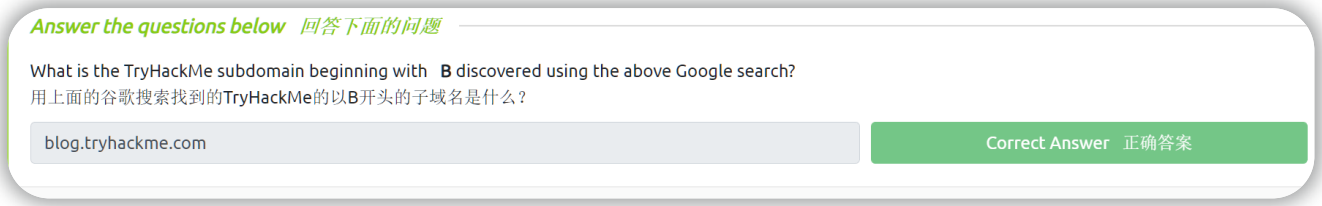
例子： “-site: www.domain.com site:*.domain.com” 只会包含指向域名 domain.com 的结果，但同时会排除任何指向 www.domain.com 的链接；所以，它只会向我们显示属于 domain.com 的子域名。

转到谷歌并使用搜索词 -site: www.tryhackme.com site:*.tryhackme.com ，搜索结果应该会显示 tryhackme.com 的子域名。

答题

在Google上使用高级语法，搜索tryhackme.com的子域名



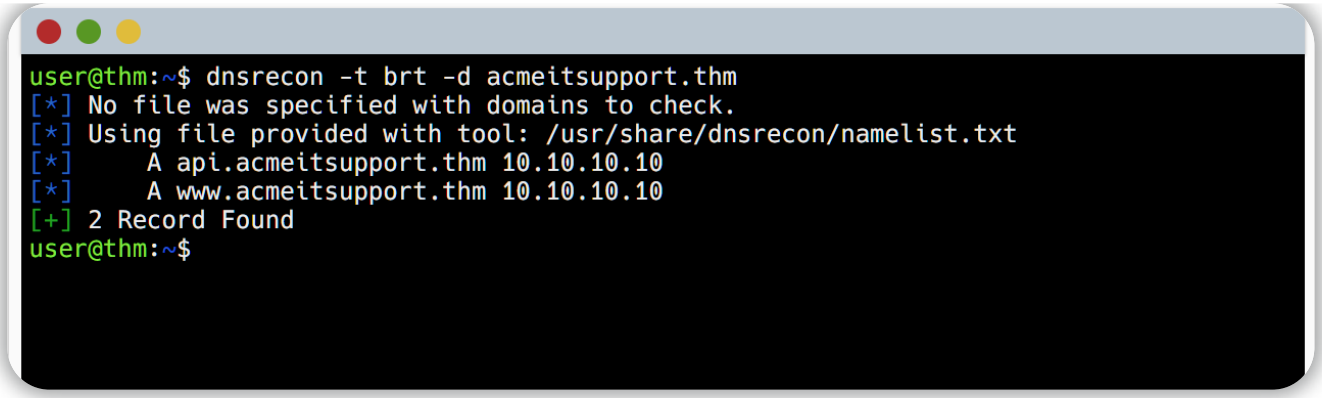


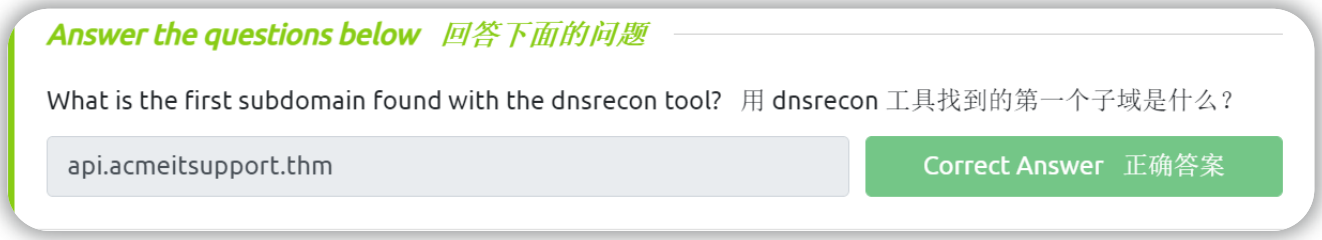
H2 DNS Bruteforce（DNS 暴力匹配）

Bruteforce DNS (域名系统)枚举是从预定义的常用子域名字典中，尝试向DNS请求数十个、数百个、数千个甚至数百万个不同可能的子域名的方法，因为这个方法需要很多请求，所以我们使用工具来自动化完成，以加快处理速度。

在本例中，我们会使用一个名为 dnsrecon 的工具来执行此操作。

答题





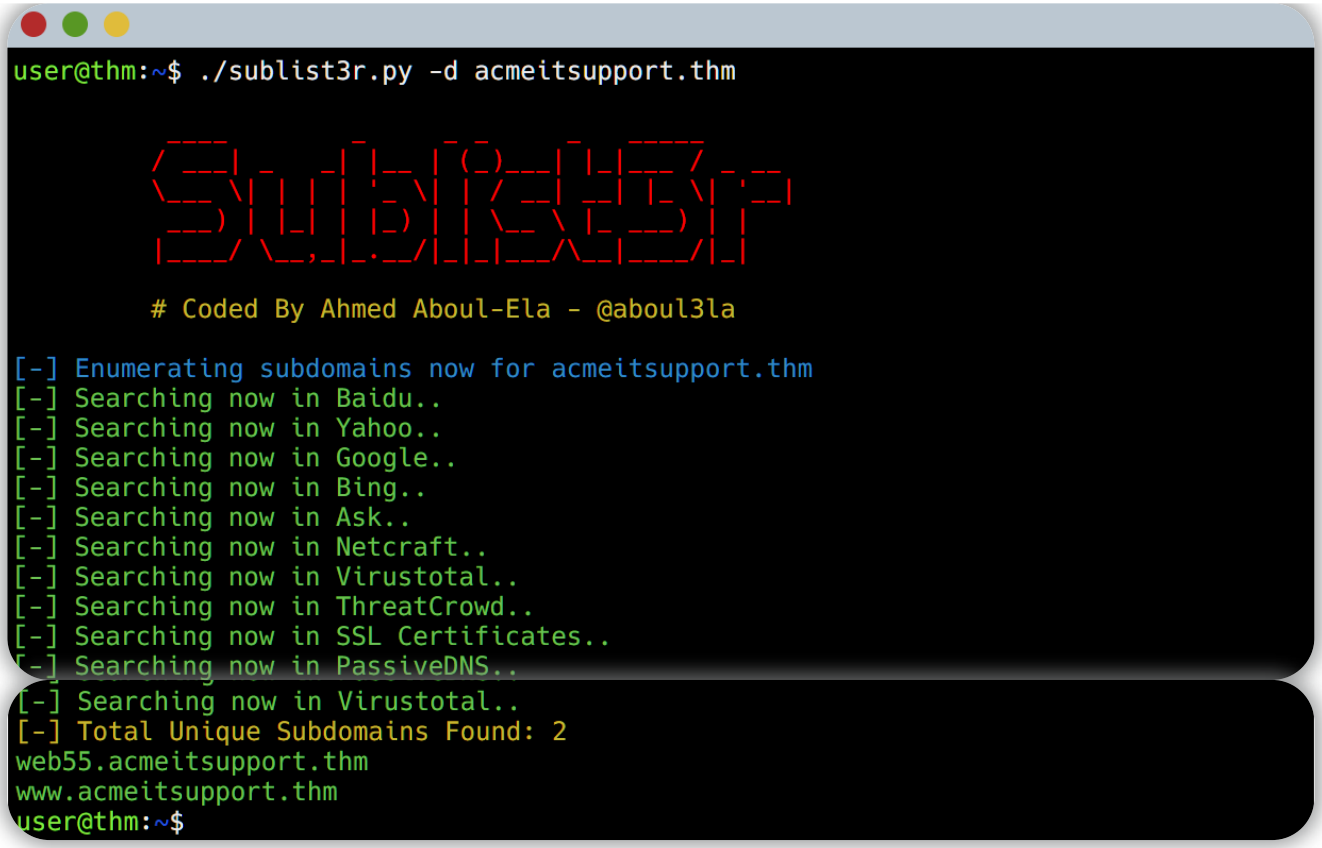
H2 OSINT-Sublist3r

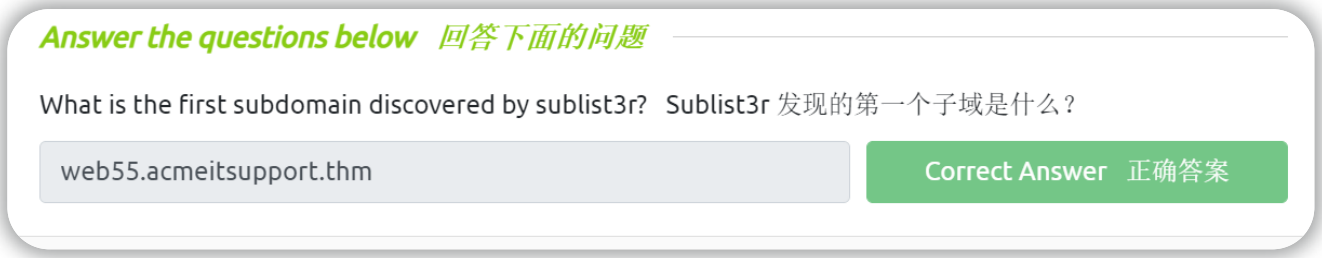
使用 Sublist3r 自动化工具

为了加快 OSINT 子域发现的进程，我们可以使用 Sublist3r 这样的工具来自动化查找子域。

Sublist3r项目地址： https://github.com/aboul3la/Sublist3r

答题





H2 Virtual Hosts 虚拟主机

有些子域名并不总是托管在公共可访问的 DNS 的结果中，例如 Web 应用程序的开发版本或一些管理门户。

DNS 记录也可以保存在一个私有的 DNS 服务器上，或者记录在开发者的机器上的 /etc/hosts 文件中(或者在c:\windows\system32\drivers\etc\hosts 文件中，Windows 用户可以使用这个文件)，hosts能将域名映射到 IP 地址。

Web 服务器可以在一台服务器上托管多个网站，当客户端请求网站时，服务器能从 Host 标头中知道客户端具体想要访问哪一个网站。我们可以通过更改Host信息来利用这个Host标头，并监控服务器的响应以查看我们是否发现了一个新网站。

与 DNS 的暴力匹配一样，我们可以通过使用包含常用子域名的字典来自动化请求过程。

启动TryHackMe网站提供的AttackBox，然后对 Acme IT Support 机器尝试以下命令，以尝试发现一个新的子域。

```
user@machine$ ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H
"Host: FUZZ.acmeitsupport.thm" -u http://10.10.91.202
```

上面的命令使用 -w 开关来指定我们要使用的字典，使用 -H 开关来添加/编辑标头（在本例中为 Host 标头），我们在子域名的url地址中能够插入一个FUZZ关键字，在这个位置，我们将尝试填充字典中的所有子项。

因为上面的命令总是会产生一个有效的结果，所以我们需要做过滤输出。我们可以使用-fs 开关 加上所得结果的"页面大小值" 来做过滤。

编辑并执行以下命令，将 {size} 替换为上一个命令的结果中出现次数最多的"页面大小值"。

```
user@machine$ ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H
"Host: FUZZ.acmeitsupport.thm" -u http://10.10.91.202 -fs {size}
```

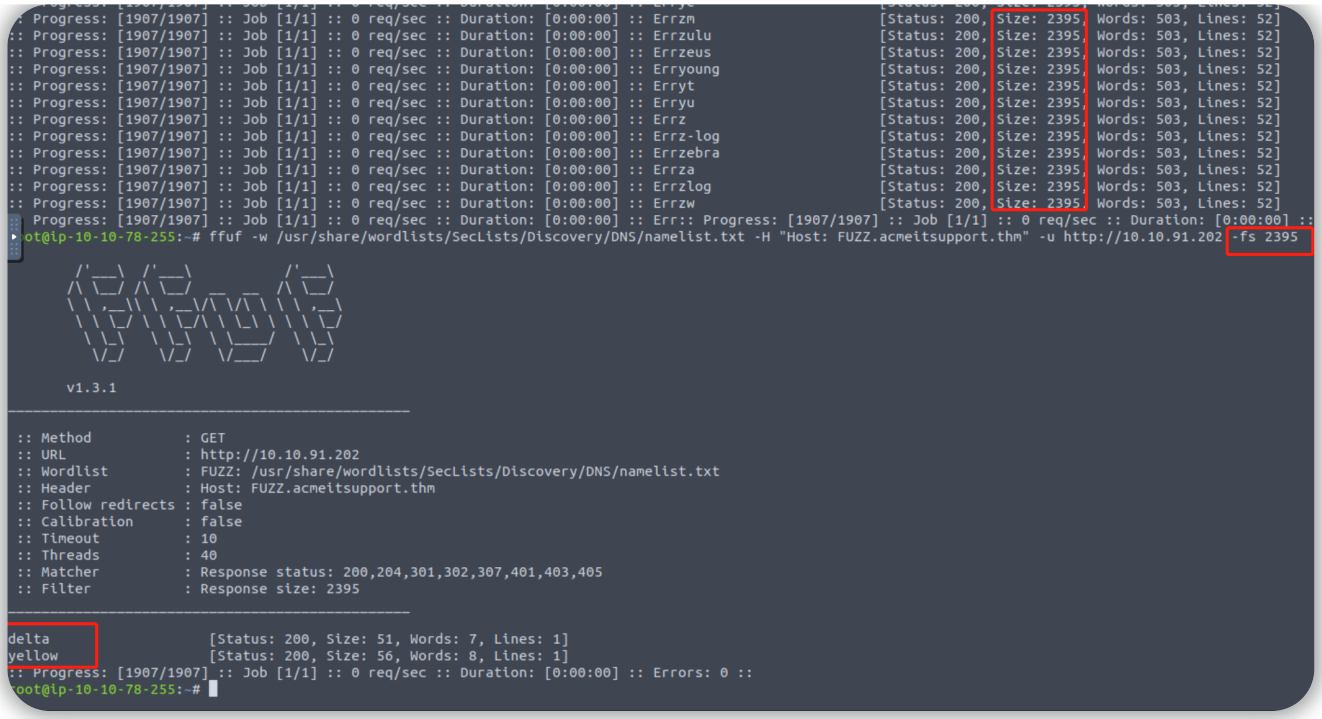
除了 -fs 开关之外，此命令的语法与第一个命令类似，使用-fs 将告诉 ffuf 忽略任何指定大小的结果。

答题

使用命令

```
ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H "Host:
FUZZ.acmeitsupport.thm" -u http://10.10.91.202

#对上一条命令的结果进行过滤 忽略出现次数最多的size值：2395
ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H "Host:
FUZZ.acmeitsupport.thm" -u http://10.10.91.202 -fs 2395
```



Answer the questions below *回答下面的问题*

What is the first subdomain discovered? 发现的第一个子域是什么？

delta — Correct Answer 正确答案

What is the second subdomain discovered? 发现的第二个子域是什么？

yellow — Correct Answer 正确答案