✦ Member-only story

Subdomain Enumeration | TryHackMe

Aircon Follow 4 min read · Feb 14, 2022

162 5

WWW
Subdomain Enumeration
Learn the various ways of discovering subdomains to expand yo

Lab Access: https://tryhackme.com/room/subdomainenumeration

Task 1 ○ Brief

Subdomain Enumeration —the process of identifying valid subdomains for a domain.

[Question 1.1] What is a subdomain enumeration method beginning with B?

Answer: Brute Force

[Question 1.2] What is a subdomain enumeration method beginning with O?

Answer: OSINT

[Question 1.3] What is a subdomain enumeration method beginning with V?

Answer: Virtual Host

Task 2 ○ OSINT - SSL/TLS Certificates

SSL/TLS (Secure Sockets Layer/Transport Layer Security) Certificate

- **Created for a domain** by a CA (Certificate Authority)

CA (Certificate Authority)

- Take part in what's called "**Certificate Transparency (CT) logs**"

Purpose of Certificate Transparency (CT) logs

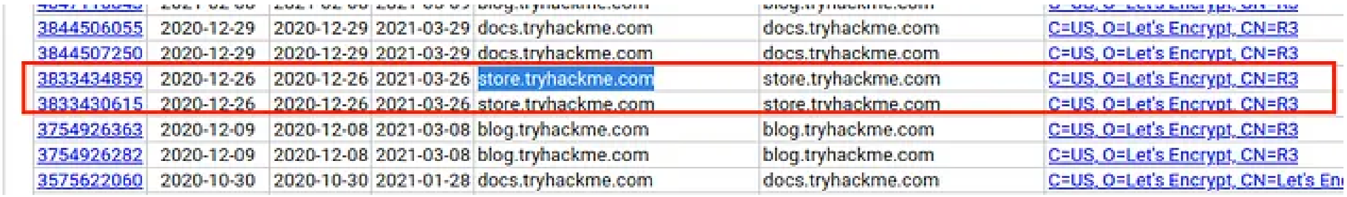
- **Stop malicious and accidentally made certificates** from being used

These two website provides a **certificate database that is searchable and displays current and historical results.**

http://crt.sh/
https://transparencyreport.google.com/https/certificates

[Question 2.1] What domain was logged on crt.sh at 2020–12–26?

1st - **crt.sh**
2nd - search "**tryhackme.com**"



[illegible]	[illegible]	[illegible]	[illegible]	blog.tryhackme.com	blog.tryhackme.com	[illegible]
3844506055	2020-12-29	2020-12-29	2021-03-29	docs.tryhackme.com	docs.tryhackme.com	C=US, O=Let's Encrypt, CN=R3
3844507250	2020-12-29	2020-12-29	2021-03-29	docs.tryhackme.com	docs.tryhackme.com	C=US, O=Let's Encrypt, CN=R3
3833434859	2020-12-26	2020-12-26	2021-03-26	store.tryhackme.com	store.tryhackme.com	C=US, O=Let's Encrypt, CN=R3
3833430615	2020-12-26	2020-12-26	2021-03-26	store.tryhackme.com	store.tryhackme.com	C=US, O=Let's Encrypt, CN=R3
3754926363	2020-12-09	2020-12-08	2021-03-08	blog.tryhackme.com	blog.tryhackme.com	C=US, O=Let's Encrypt, CN=R3
3754926282	2020-12-09	2020-12-08	2021-03-08	blog.tryhackme.com	blog.tryhackme.com	C=US, O=Let's Encrypt, CN=R3
3575622060	2020-10-30	2020-10-30	2021-01-28	docs.tryhackme.com	docs.tryhackme.com	C=US, O=Let's Encrypt, CN=Let's En

Answer: store.tryhackme.com

Task 3 ○ OSINT - Search Engines

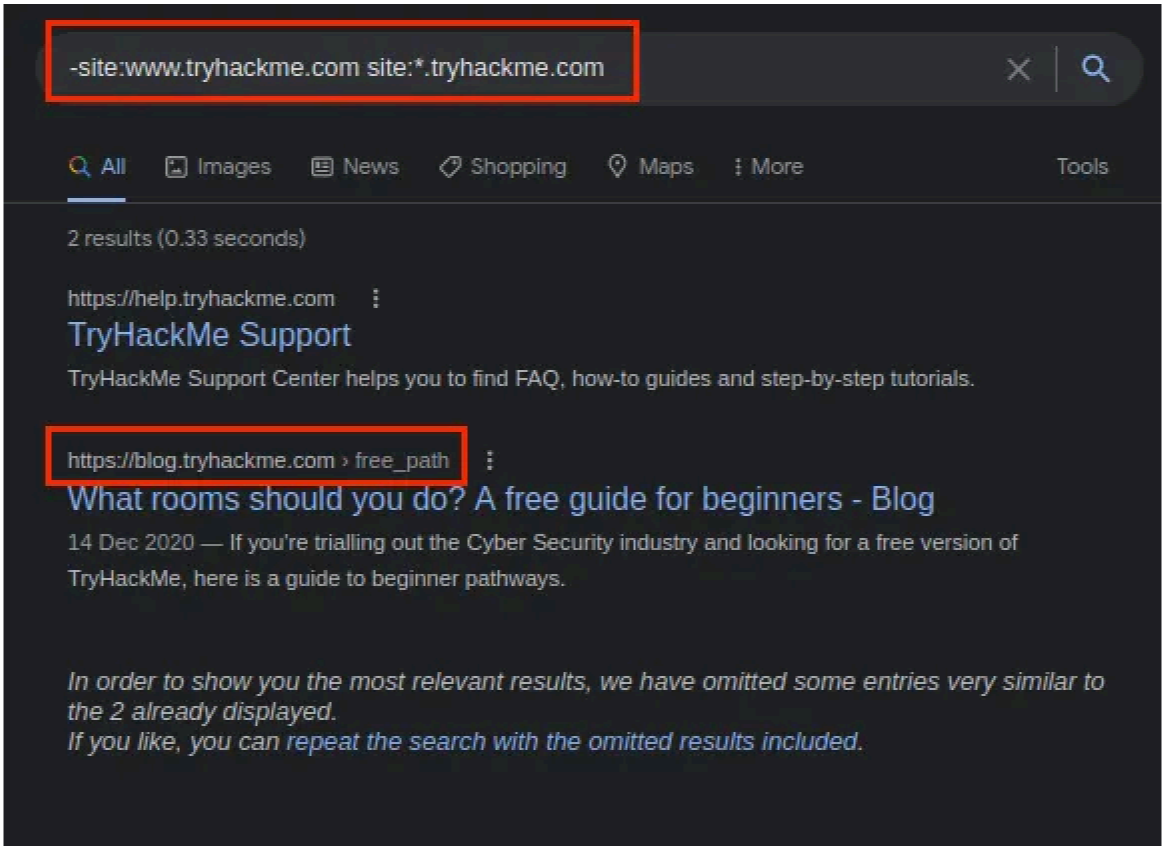
Search Engines — A fantastic resource for discovering new subdomains.

- By utilizing advanced search strategies on websites such as Google

```
Method:
• site:filter > can narrow the search results
• -site:www.domain.com site:*.domain.com

Example:
•  -site:www.tryhackme.com site:*.tryhackme.com
```

[Question 3.1] What is the TryHackMe subdomain beginning with B discovered using the above Google search?


-site:www.tryhackme.com site:*.tryhackme.com

2 results (0.33 seconds)

https://help.tryhackme.com
TryHackMe Support
TryHackMe Support Center helps you to find FAQ, how-to guides and step-by-step tutorials.

https://blog.tryhackme.com › free_path
What rooms should you do? A free guide for beginners - Blog
14 Dec 2020 — If you're trialling out the Cyber Security industry and looking for a free version of TryHackMe, here is a guide to beginner pathways.

In order to show you the most relevant results, we have omitted some entries very similar to the 2 already displayed.
If you like, you can repeat the search with the omitted results included.

Answer: blog.tryhackme.com

Task 4 ○ DNS Bruteforce

Bruteforce DNS (Domain Name System) Enumeration

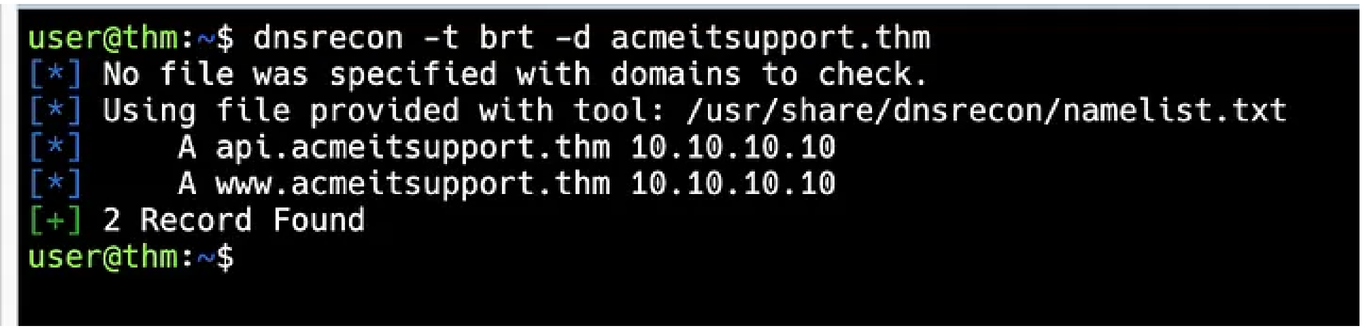
- By attempting tens, hundreds, thousands, or even millions of **unique subdomains from a pre-defined list** of frequently used subdomains, and it automates it with a tool to speed up the procedure.

Tool:

- **dnsrecon**

If you're running Kali Linux, it's already pre-installed, and you can go to the "terminal" and type "**dnsrecon**" to see how to use it.

[Question 4.1] What is the first subdomain found with the dnsrecon tool?



```
user@thm:~$ dnsrecon -t brt -d acmeitsupport.thm
[*] No file was specified with domains to check.
[*] Using file provided with tool: /usr/share/dnsrecon/namelist.txt
[*]     A api.acmeitsupport.thm 10.10.10.10
[*]     A www.acmeitsupport.thm 10.10.10.10
[+] 2 Record Found
user@thm:~$
```

Answer: api.acmeitsupport.thm

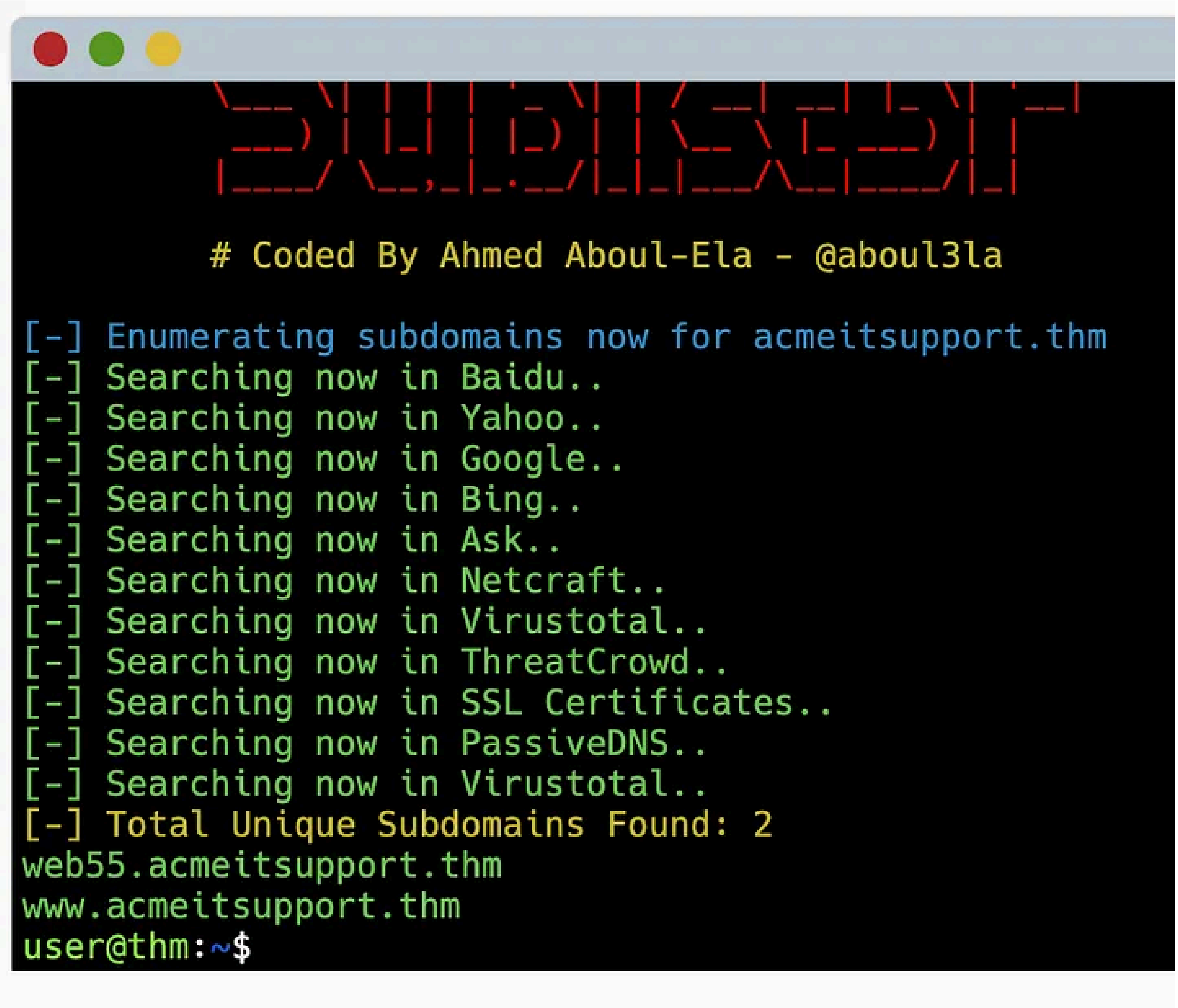
Task 5 ○ OSINT - Sublist3r

It expedites the process of discovering OSINT subdomains.

```
1st - Install sublist3r in Kali Linux
• sudo apt install sublist3r

2nd Run sublist3r
• type: sublist3r
```

[Question 5.1] What is the first subdomain discovered by sublist3r?



```
                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for acmeitsupport.thm
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Searching now in Virustotal..
[-] Total Unique Subdomains Found: 2
web55.acmeitsupport.thm
www.acmeitsupport.thm
user@thm:~$
```

Answer: web55.acmeitsupport.thm

Task 6 ○ Virtual Hosts

Subdomains aren't usually hosted in DNS results that are publicly accessible, such as:

- development versions of a web application
- administration portals

DNS records can be **stored on a private DNS server** or on the **developer's workstations** in the **/etc/hosts** file (or **c:\windows\system32\drivers\etc\hosts file for Windows users**), which translates domain names to IP addresses.

```
Web servers can host numerous websites from a single server.

• When a client requests a website, the server determines which
website the client wants based on the Host Header.
```

What we can do:

- Make use of this **host header by modifying it and checking the response** to see whether we've discovered a new website, and it's very similar to DNS Brute Force in that it uses a tool to seek it out and automates the process.

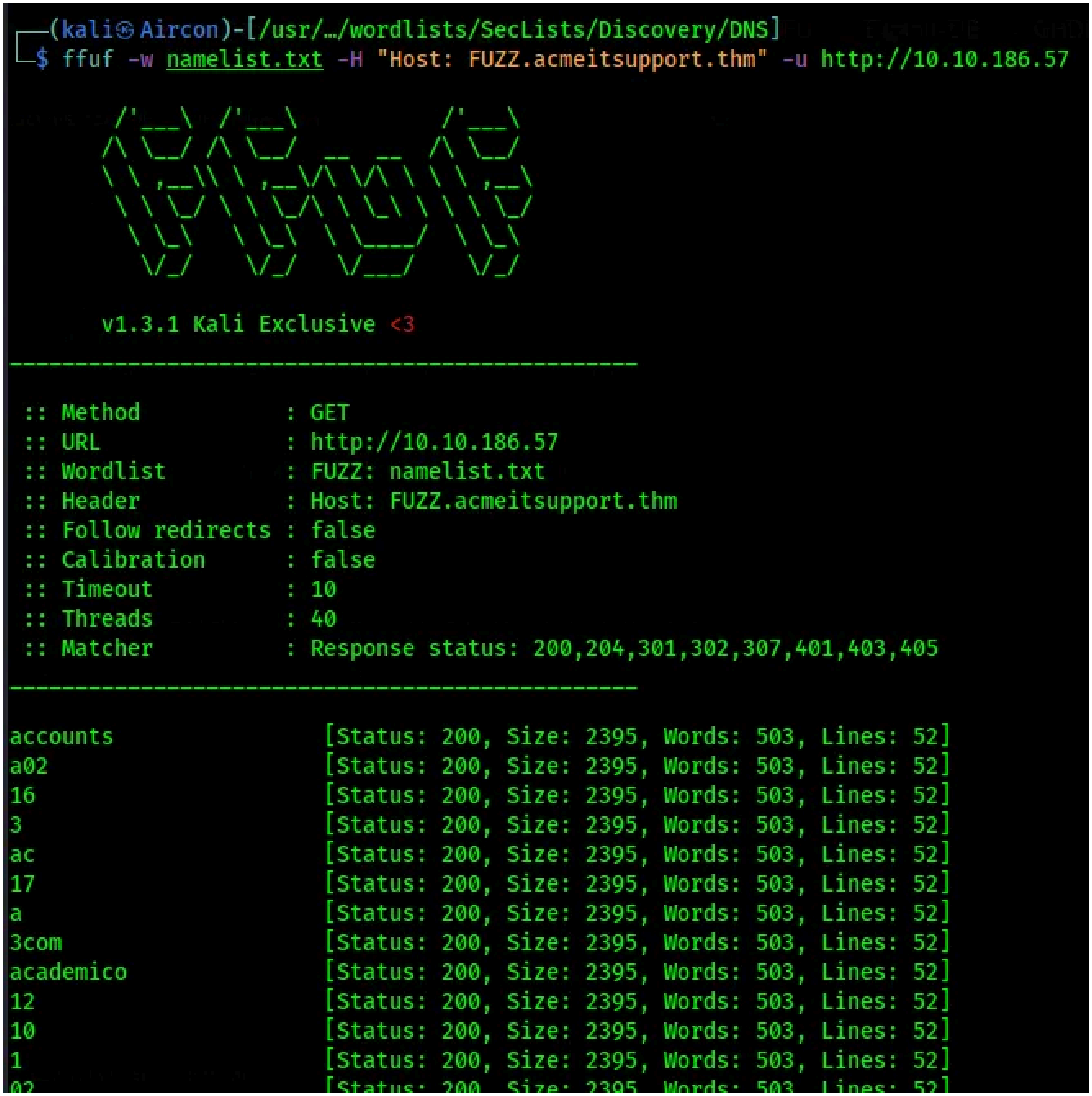
```
Tool:
• ffuf

It comes pre-installed with Kali Linux

Example:
• ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H
"Host: FUZZ.acmeitsupport.thm" -u http://<domain name/ip address>

Switches:
-w > wordlist
-H > adds/edits a header
-u > url
-fs > tells ffuf to ignore any results that are of the specified size
```

[Question 6.1] What is the first subdomain discovered?



```
┌──(kali㉿Aircon)-[/usr/…/wordlists/SecLists/Discovery/DNS]
└─$ ffuf -w namelist.txt -H "Host: FUZZ.acmeitsupport.thm" -u http://10.10.186.57

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.186.57
 :: Wordlist         : FUZZ: namelist.txt
 :: Header           : Host: FUZZ.acmeitsupport.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

accounts                [Status: 200, Size: 2395, Words: 503, Lines: 52]
a02                     [Status: 200, Size: 2395, Words: 503, Lines: 52]
16                      [Status: 200, Size: 2395, Words: 503, Lines: 52]
3                       [Status: 200, Size: 2395, Words: 503, Lines: 52]
ac                      [Status: 200, Size: 2395, Words: 503, Lines: 52]
17                      [Status: 200, Size: 2395, Words: 503, Lines: 52]
a                       [Status: 200, Size: 2395, Words: 503, Lines: 52]
3com                    [Status: 200, Size: 2395, Words: 503, Lines: 52]
academico               [Status: 200, Size: 2395, Words: 503, Lines: 52]
12                      [Status: 200, Size: 2395, Words: 503, Lines: 52]
10                      [Status: 200, Size: 2395, Words: 503, Lines: 52]
1                       [Status: 200, Size: 2395, Words: 503, Lines: 52]
02                      [Status: 200, Size: 2395, Words: 503, Lines: 52]
```

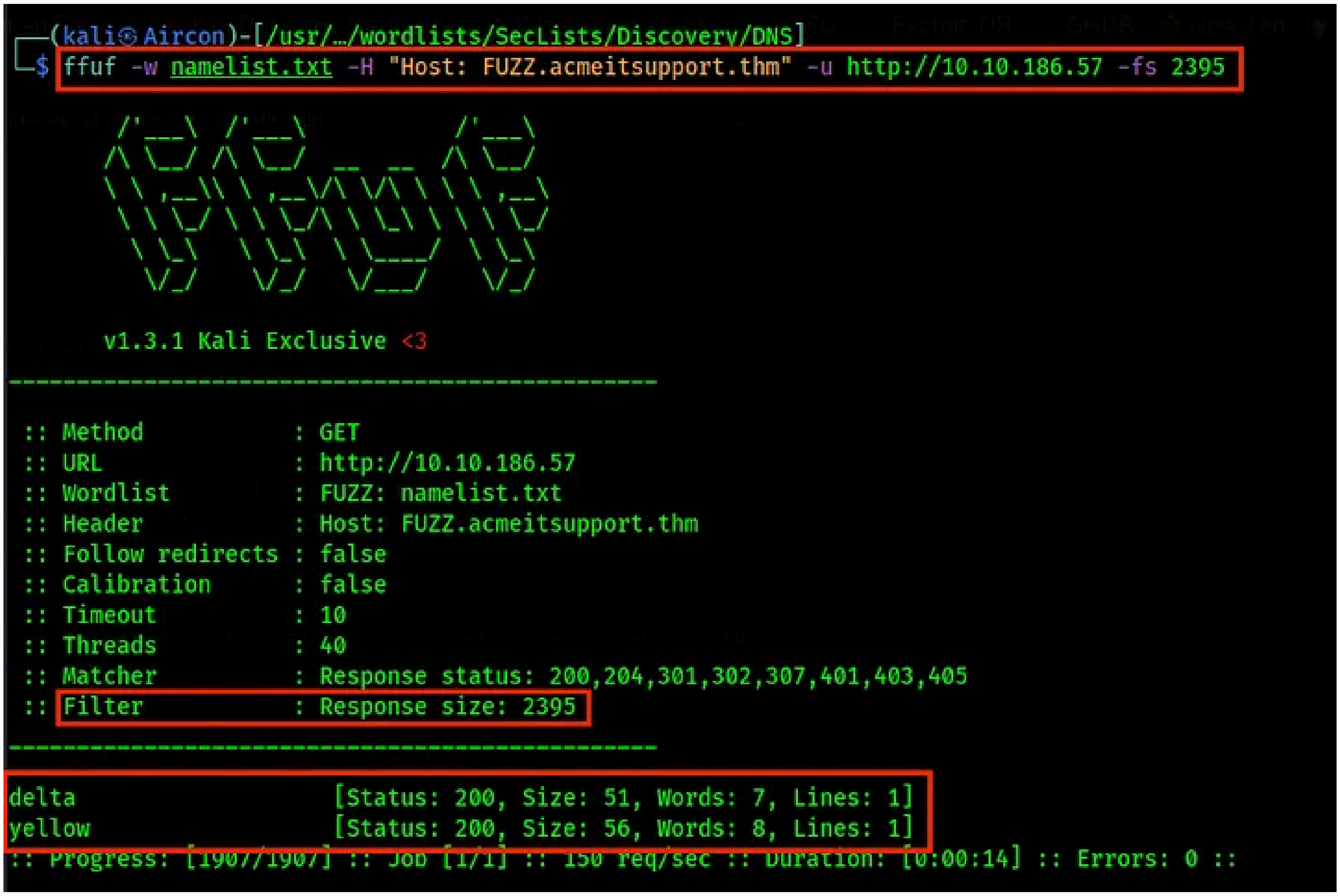
ffuf -w namelist.txt -H “Host: FUZZ.acmeitsupport.thm” -u http://<IP address>

Notice that there are numerous reports with the “Size” of “2395” and that you

```
Method:
```

- `ffuf -w namelist.txt -H "Host: FUZZ.acmeitsupport.thm" -u http://10.10.186.57` **`-fs 2395`**

By including the switch "-fs" and the value "2395," it will filter and eliminate all of the "2395"



```
┌──(kali㉿Aircon)-[/usr/…/wordlists/SecLists/Discovery/DNS]
└─$ ffuf -w namelist.txt -H "Host: FUZZ.acmeitsupport.thm" -u http://10.10.186.57 -fs 2395

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.186.57
 :: Wordlist         : FUZZ: namelist.txt
 :: Header           : Host: FUZZ.acmeitsupport.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response size: 2395
________________________________________________

delta                   [Status: 200, Size: 51, Words: 7, Lines: 1]
yellow                  [Status: 200, Size: 56, Words: 8, Lines: 1]
:: Progress: [1907/1907] :: Job [1/1] :: 150 req/sec :: Duration: [0:00:14] :: Errors: 0 ::
```

Answer: delta

[Question 6.2] What is the second subdomain discovered?

Answer: yellow