Subdomain Enumeration

Brief

Subdomain enumeration is the process of finding valid subdomains for a domain, but why do we do this? We do this to expand our attack surface to try and discover more potential points of vulnerability.

We will explore three different subdomain enumeration methods: Brute Force, OSINT (Open-Source Intelligence) and Virtual Host.

Start the machine and then move onto the next task.
****

Answer the questions below:

What is a subdomain enumeration method beginning with B?
Answer: Brute Force

What is a subdomain enumeration method beginning with O?
Answer: OSINT

What is a subdomain enumeration method beginning with V?
Answer: Virtual Host
****

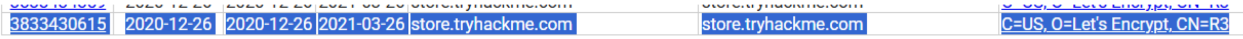
OSINT - SSL/TLS Certificates

When an SSL/TLS (Secure Sockets Layer/Transport Layer Security) certificate is created for a domain by a CA (Certificate Authority), CA's take part in what's called "Certificate Transparency (CT) logs". These are publicly accessible logs of every SSL/TLS certificate created for a domain name. The purpose of Certificate Transparency logs is to stop malicious and accidentally made certificates from being used. We can use this service to our advantage to discover subdomains belonging to a domain, sites like https://crt.sh offer a searchable database of certificates that shows current and historical results.

Go to crt.sh and search for the domain name tryhackme.com, find the entry that was logged at 2020-12-26 and enter the domain below to answer the question.
****

Answer the questions below:

What domain was logged on crt.sh at 2020-12-26?



3833430615	2020-12-26	2020-12-26	2021-03-26	store.tryhackme.com	store.tryhackme.com	C=US, O=Let's Encrypt, CN=R3

Answer: store.tryhackme.com
****

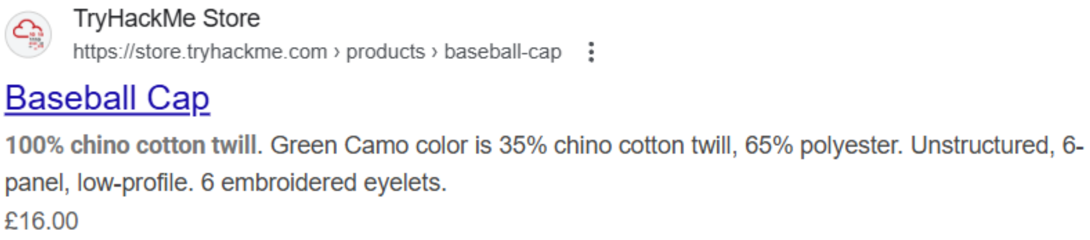
OSINT - Search Engines

Search engines contain trillions of links to more than a billion websites, which can be an excellent resource for finding new subdomains. Using advanced search methods on websites like Google, such as the site: filter, can narrow the search results. For example, site:*.domain.com -site:www.domain.com would only contain results leading to the domain name domain.com but exclude any links to www.domain.com; therefore, it shows us only subdomain names belonging to domain.com.

Go to Google and use the search term site:*.tryhackme.com -site:www.tryhackme.com, which should reveal a subdomain for tryhackme.com; use that subdomain to answer the question below.
****

Answer the questions below:

What is the TryHackMe subdomain beginning with S discovered using the above Google search?



TryHackMe Store
https://store.tryhackme.com › products › baseball-cap

Baseball Cap

100% chino cotton twill. Green Camo color is 35% chino cotton twill, 65% polyester. Unstructured, 6-panel, low-profile. 6 embroidered eyelets.

£16.00

Answer: store.tryhackme.com
****

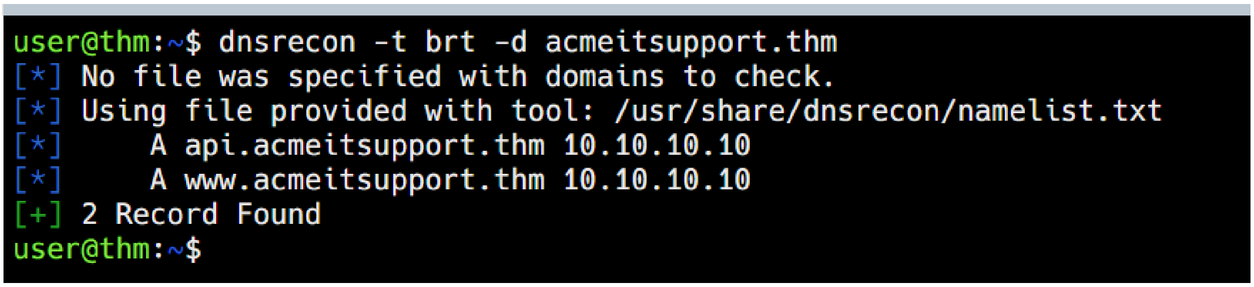
DNS Brute Force

Bruteforce DNS (Domain Name System) enumeration is the method of trying tens, hundreds, thousands or even millions of different possible subdomains from a pre-defined list of commonly used subdomains. Because this method requires many requests, we automate it with tools to make the process quicker. In this instance, we are using a tool called dnsrecon to perform this. Click the "View Site" button to open the static site, press the "Run DNSrecon Request" button to start the simulation, and then answer the question below.

****

Answer the questions below:

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

****

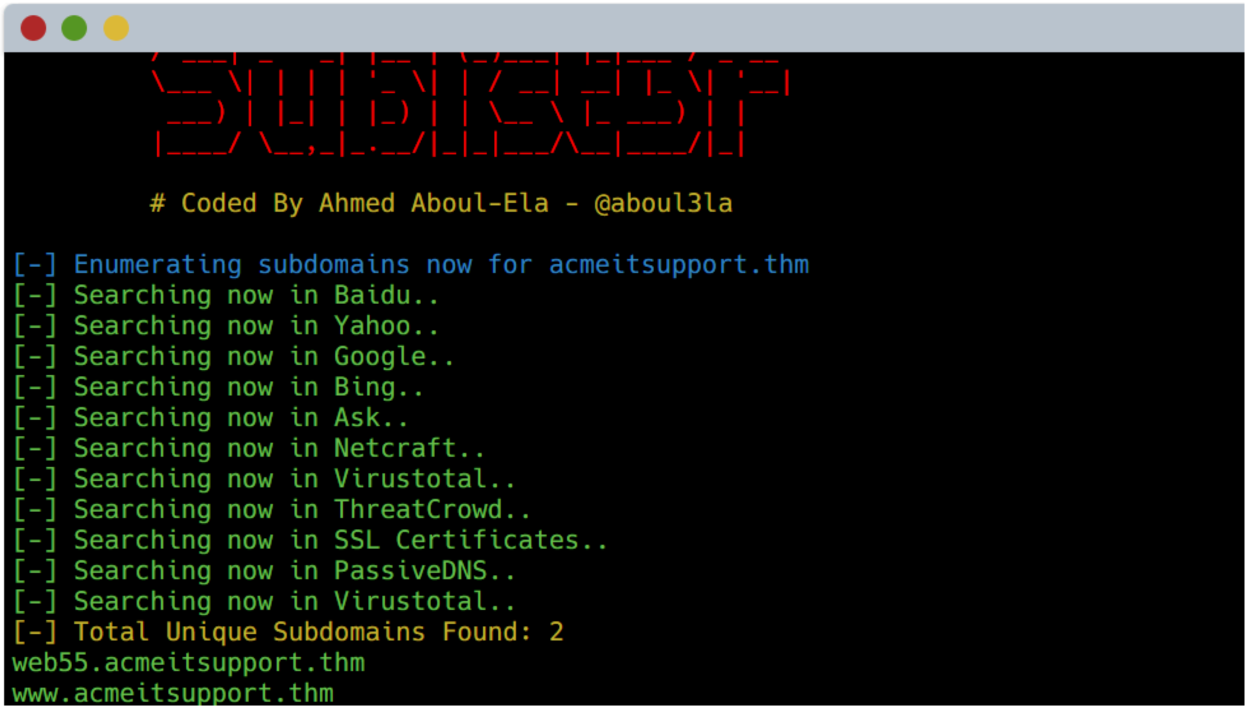
OSINT - Sublist3r

To speed up the process of OSINT subdomain discovery, we can automate the above methods with the help of tools like Sublist3r, click the "View Site" button to open up the static site and run the sublist3r simulation to discover a new subdomain that will help answer the question below.

****

Answer the questions below:

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
```

Answer: web55.acmeitsupport.thm

****

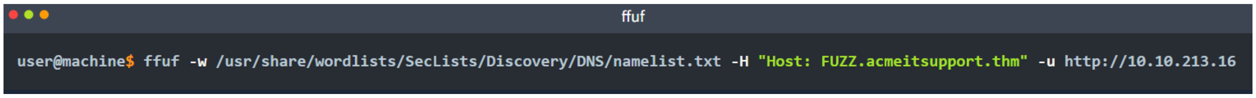
Virtual Hosts

Some subdomains aren't always hosted in publically accessible DNS results, such as development versions of a web application or administration portals. Instead, the DNS record could be kept on a private DNS server or recorded on the developer's machines in their /etc/hosts file (or c:\windows\system32\drivers\etc\hosts file for Windows users), which maps domain names to IP addresses.

Because web servers can host multiple websites from one server when a website is requested from a client, the server knows which website the client wants from the Host header. We can utilize this host header by making changes to it and monitoring the response to see if we've discovered a new website.

Like with DNS Bruteforce, we can automate this process by using a wordlist of commonly used subdomains.

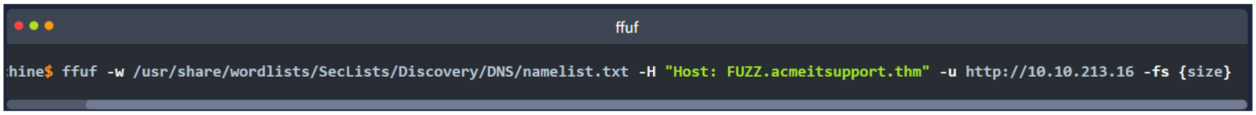
Start the AttackBox and then try the following command against the Acme IT Support machine to discover a new subdomain.



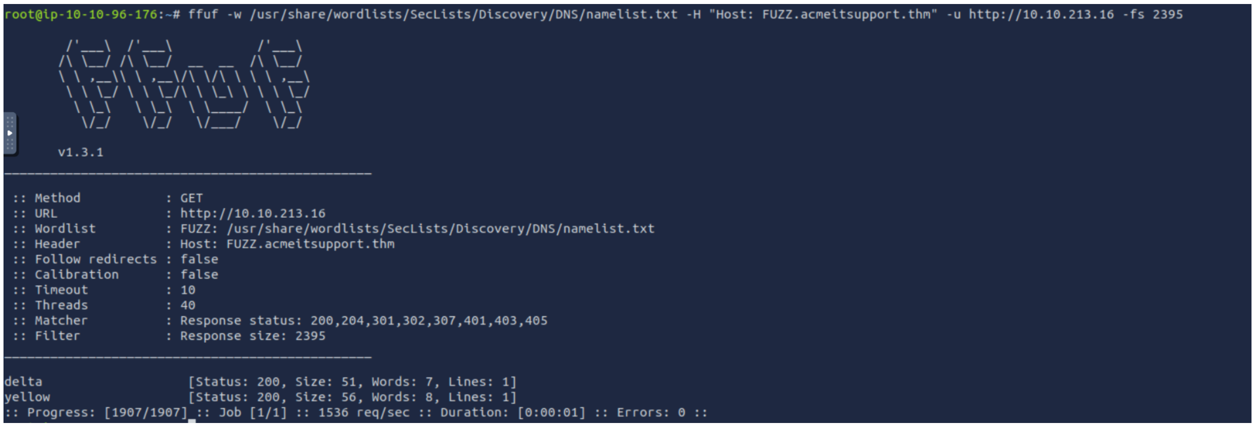
```
user@machine$ ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H "Host: FUZZ.acmeitsupport.thm" -u http://10.10.213.16
```

The above command uses the -w switch to specify the wordlist we are going to use. The -H switch adds/edits a header (in this instance, the Host header), we have the FUZZ keyword in the space where a subdomain would normally go, and this is where we will try all the options from the wordlist.

Because the above command will always produce a valid result, we need to filter the output. We can do this by using the page size result with the -fs switch. Edit the below command replacing {size} with the most occurring size value from the previous result and try it on the AttackBox.



```
hine$ ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H "Host: FUZZ.acmeitsupport.thm" -u http://10.10.213.16 -fs {size}
```



```
root@ip-10-10-96-176:~# ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H "Host: FUZZ.acmeitsupport.thm" -u http://10.10.213.16 -fs 2395

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

       v1.3.1
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.213.16
 :: Wordlist         : FUZZ: /usr/share/wordlists/SecLists/Discovery/DNS/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] :: 1536 req/sec :: Duration: [0:00:01] :: Errors: 0 ::
```

This command has a similar syntax to the first apart from the -fs switch, which tells ffuf to ignore any results that are of the specified size.

The above command should have revealed two positive results that we haven't come across before.
****

Answer the questions below:

What is the first subdomain discovered?
Answer: delta

What is the second subdomain discovered?
Answer: yellow