Vhost Fuzzing

As we saw in the previous section, we were able to fuzz public sub-domains using public DNS records. However, when it came to fuzzing sub-domains that do not have a public DNS record or sub-domains under websites that are not public, we could not use the same method. In this section, we will learn how to do that with Vhost Fuzzing.

Vhosts vs. Sub-domains

The key difference between VHosts and sub-domains is that a VHost is basically a 'sub-domain' served on the same server and has the same IP, such that a single IP could be serving two or more different websites.

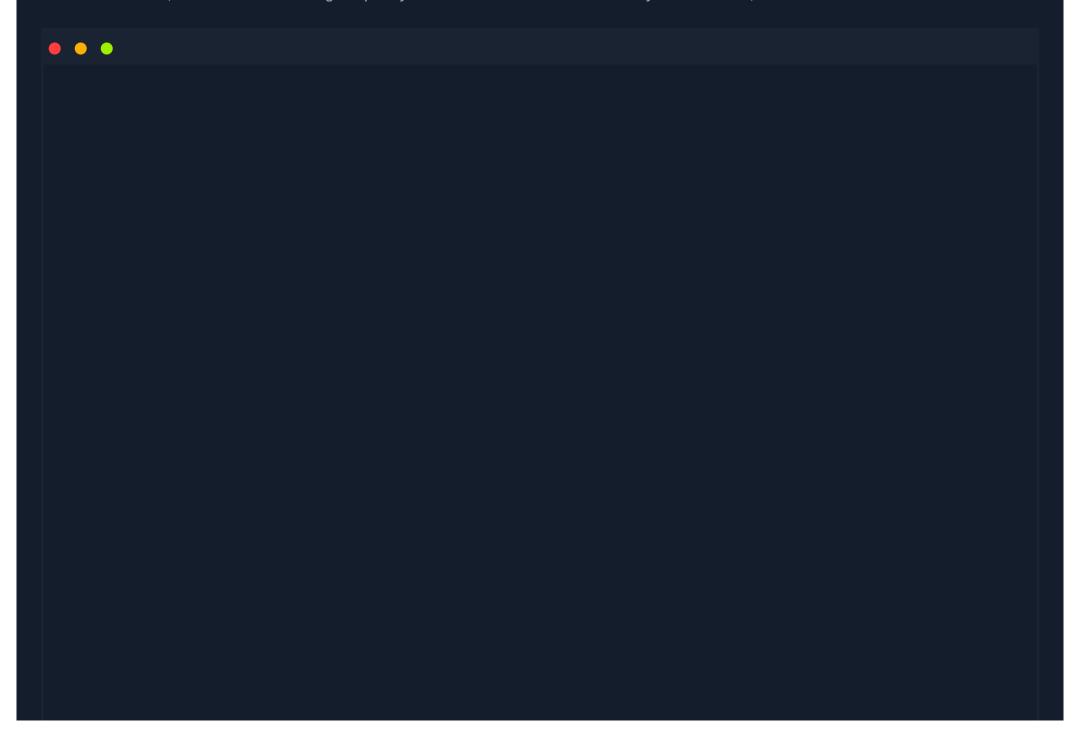
VHosts may or may not have public DNS records.

In many cases, many websites would actually have sub-domains that are not public and will not publish them in public DNS records, and hence if we visit them in a browser, we would fail to connect, as the public DNS would not know their IP. Once again, if we use the sub-domain fuzzing, we would only be able to identify public sub-domains but will not identify any sub-domains that are not public.

This is where we utilize VHosts Fuzzing on an IP we already have. We will run a scan and test for scans on the same IP, and then we will be able to identify both public and non-public sub-domains and VHosts.

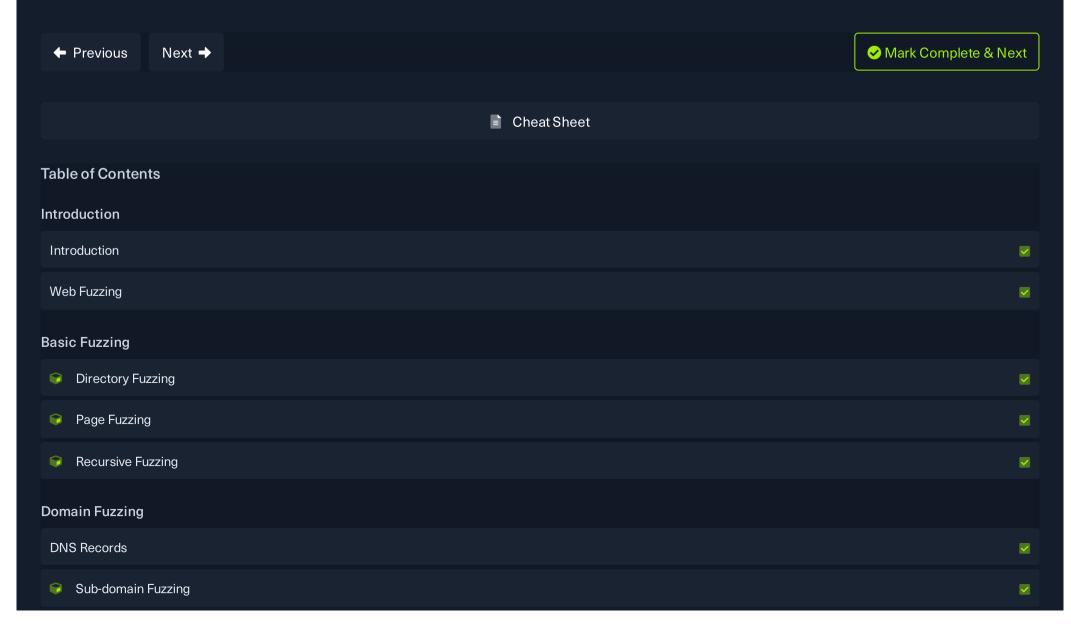
Vhosts Fuzzing

To scan for VHosts, without manually adding the entire wordlist to our /etc/hosts, we will be fuzzing HTTP headers, specifically the Host: header. To do that, we can use the -H flag to specify a header and will use the FUZZ keyword within it, as follows:



```
MichaelLuka@htb[/htb]$ ffuf -w /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.l
       /'___\
/\ \__/ /\ \__/ ___ __ /<u>\</u> \__/
       \\,__\\\,__\/\\\\\\,__\
        \ \ \_/ \ \ \_/\ \ \_\_\
        \\_\ \\_\ \\_\ \\__/ \\_\_/
       v1.1.0-git
                   : GET
 :: Method
 :: URL
                   : http://academy.htb:PORT/
 :: Wordlist
                   : FUZZ: /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header
                   : Host: FUZZ
 :: Follow redirects : false
 :: Calibration
                   : false
                    : 10
 :: Timeout
 :: Threads
                    : 40
 :: Matcher
                    : Response status: 200,204,301,302,307,401,403
                       [Status: 200, Size: 900, Words: 423, Lines: 56]
mail2
                       [Status: 200, Size: 900, Words: 423, Lines: 56]
dns2
ns3
                       [Status: 200, Size: 900, Words: 423, Lines: 56]
                       [Status: 200, Size: 900, Words: 423, Lines: 56]
dns1
                       [Status: 200, Size: 900, Words: 423, Lines: 56]
lists
                       [Status: 200, Size: 900, Words: 423, Lines: 56]
webmail
                       [Status: 200, Size: 900, Words: 423, Lines: 56]
static
                       [Status: 200, Size: 900, Words: 423, Lines: 56]
web
                       [Status: 200, Size: 900, Words: 423, Lines: 56]
www1
<...SNIP...>
```

We see that all words in the wordlist are returning 200 0K! This is expected, as we are simply changing the header while visiting http://academy.htb:PORT/. So, we know that we will always get 200 0K. However, if the VHost does exist and we send a correct one in the header, we should get a different response size, as in that case, we would be getting the page from that VHosts, which is likely to show a different page.



Vhost Fuzzing	
Filtering Results	
Parameter Fuzzing	
Parameter Fuzzing - GET	
Parameter Fuzzing - POST	
Solution Value Fuzzing	
Skills Assessment	
Skills Assessment - Web Fuzzing	
My Workstation	
iviy vvoi kstation	
	OFFLINE
	Start Instance
	1 / 1 spawns left