Sub-domain Fuzzing

In this section, we will learn how to use `ffuf` to identify sub-domains (i.e., `*.website.com`) for any website.

Sub-domains

A sub-domain is any website underlying another domain. For example, `https://photos.google.com` is the `photos` sub-domain of `google.com`.

In this case, we are simply checking different websites to see if they exist by checking if they have a public DNS record that would redirect us to a working server IP. So, let's run a scan and see if we get any hits. Before we can start our scan, we need two things:

- A `wordlist`
- A `target`

Luckily for us, in the `SecLists` repo, there is a specific section for sub-domain wordlists, consisting of common words usually used for sub-domains. We can find it in `/opt/useful/seclists/Discovery/DNS/`. In our case, we would be using a shorter wordlist, which is `subdomains-top1million-5000.txt`. If we want to extend our scan, we can pick a larger list.

As for our target, we will use `inlanefreight.com` as our target and run our scan on it. Let us use `ffuf` and place the `FUZZ` keyword in the place of sub-domains, and see if we get any hits:

Sub-domain Fuzzing

```
MisaelMacias@htb[/htb]$ ffuf -w /opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u https://FUZ


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

       v1.1.0-git
------------------------------------------------

 :: Method           : GET
 :: URL              : https://FUZZ.inlanefreight.com/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
------------------------------------------------

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 381ms]
    * FUZZ: support

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 385ms]
    * FUZZ: ns3

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 402ms]
    * FUZZ: blog

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 180ms]
    * FUZZ: my

[Status: 200, Size: 22266, Words: 2903, Lines: 316, Duration: 589ms]
    * FUZZ: www

<...SNIP...>
```

We see that we do get a few hits back. Now, we can try running the same thing on `academy.htb` and see if we get any hits back:

Sub-domain Fuzzing

```
MisaelMacias@htb[/htb]$ ffuf -w /opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://FUZZ


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

       v1.1.0-git
------------------------------------------------

 :: Method           : GET
 :: URL              : https://FUZZ.academy.htb/
 :: Wordlist         : FUZZ: /opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
------------------------------------------------

:: Progress: [4997/4997] :: Job [1/1] :: 131 req/sec :: Duration: [0:00:38] :: Errors: 4997 ::
```

We see that we do not get any hits back. Does this mean that there are no sub-domain under `academy.htb`? - No.

This means that there are no `public` sub-domains under `academy.htb`, as it does not have a public DNS record, as previously mentioned. Even though we did add `academy.htb` to our `/etc/hosts` file, we only added the main domain, so when `ffuf` is looking for other sub-domains, it will not find them in `/etc/hosts`, and will ask the public DNS, which obviously will not have them.

Cheat Sheet

Go to Questions

Table of Contents

Introduction
- Introduction
- Web Fuzzing

Basic Fuzzing
- Directory Fuzzing
- Page Fuzzing
- Recursive Fuzzing

Domain Fuzzing
- DNS Records
- Sub-domain Fuzzing
- Vhost Fuzzing
- Filtering Results

Parameter Fuzzing
- Parameter Fuzzing - GET
- Parameter Fuzzing - POST
- Value Fuzzing

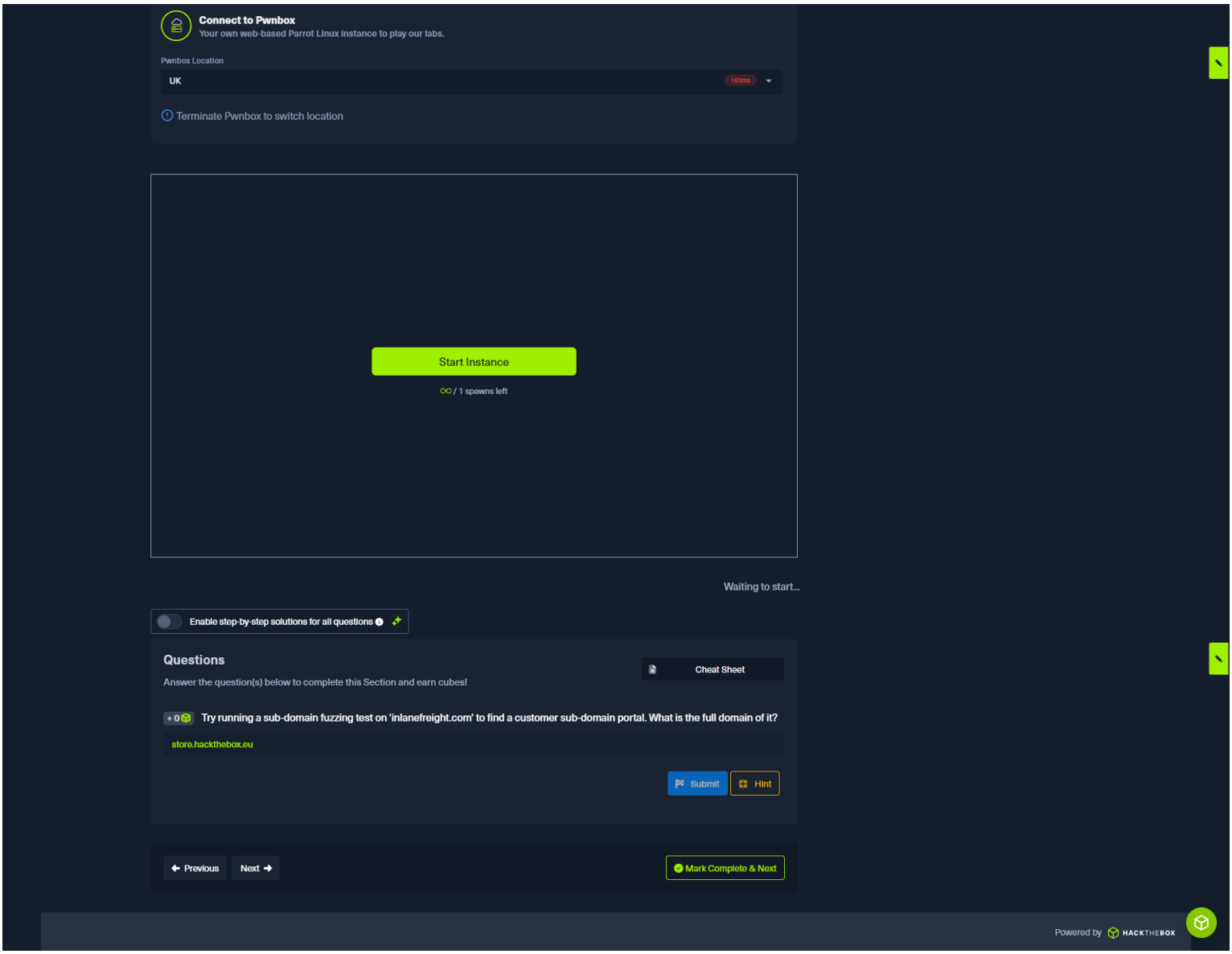
Skills Assessment
- Skills Assessment - Web Fuzzing

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left


Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.
Pwnbox Location
UK
163ms
Terminate Pwnbox to switch location
Start Instance
∞ / 1 spawns left
Waiting to start...
Enable step-by-step solutions for all questions
Questions
Answer the question(s) below to complete this Section and earn cubes!
Cheat Sheet
+ 0
Try running a sub-domain fuzzing test on 'inlanefreight.com' to find a customer sub-domain portal. What is the full domain of it?
store.hackthebox.eu
Submit
Hint
Previous
Next
Mark Complete & Next
Powered by HACKTHEBOX