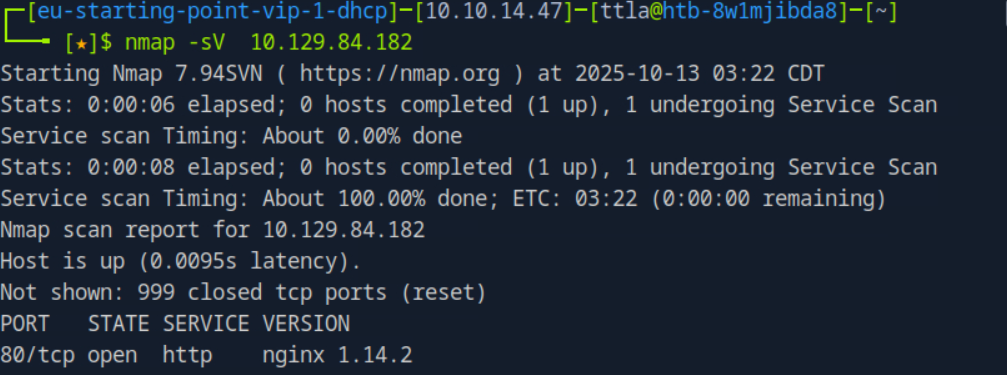
Ignition

First I always use nmap to scan for version and what port is opening by using

Nmap -sV 10.129.84.182



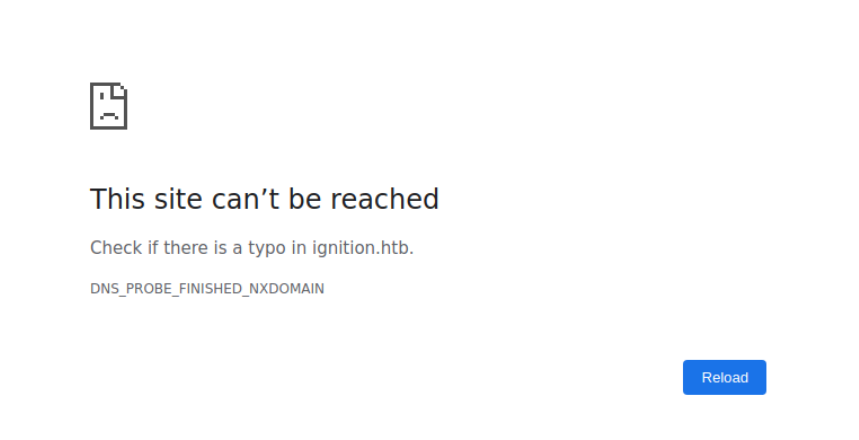
To get more information

I use -sC instead



Ok now we have <http://ignition.htb>

I try go on firefox but the website is unreacheable



This is a problem , I went on google and search that many webstire can use the same IP , this means to identify the one we are looking for we need hostname, we just found above that did not follow redirect to <http://ignition.htb/> . I try to go on Firefox and Test it , but it didn’t work. This does mean that the hostname and IP address is not mapped. Therefore , I need to map it on localhost /ect/host

Sudo nano /ect/hosts

Then add

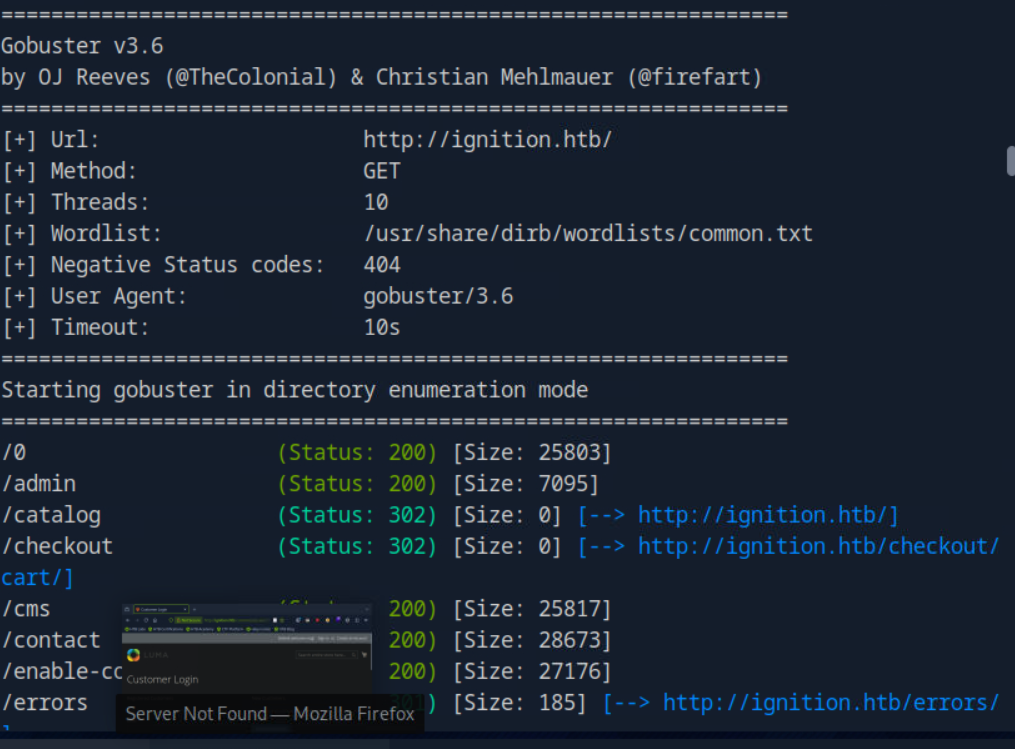
10.129.84.182 ignition.htb

Save It

Now I go on firefox to check : <http://ignition.htb/> and yes the website is now appearing

However this isnt what we looking for. Since it is http we can brute-force the directory to find any hidden sites that is accessable. In this case I use Gobuster

gobuster dir --url http://ignition.htb/ -w /usr/share/dirb/wordlists/common.txt



As we seen the results here, admin site is open

I try to go to <http://ignition.htb/admin>

I see a login page:

Username:

Password

As the Task said that this is multilayer sessions protection , it is quite difficult to brute-force it with any brute-force tools. In this case guessing is the option since the username is admin then I go on google and search for most used password for admin:

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

I try each one with admin as username , and qwerty123 is the password. I then type in and obtain the flag.

