IIK3100 – Etisk hacking og penetrasjonstesting
Home Exam

Håvard Solberg Nybøe

12. september 2023

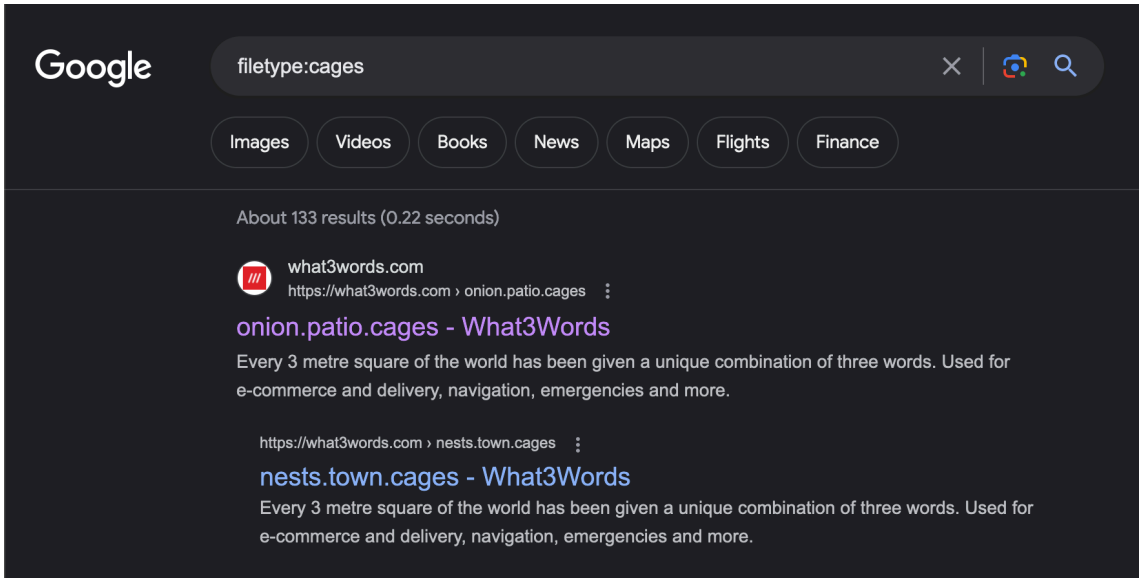
Innhold

1 OSINT

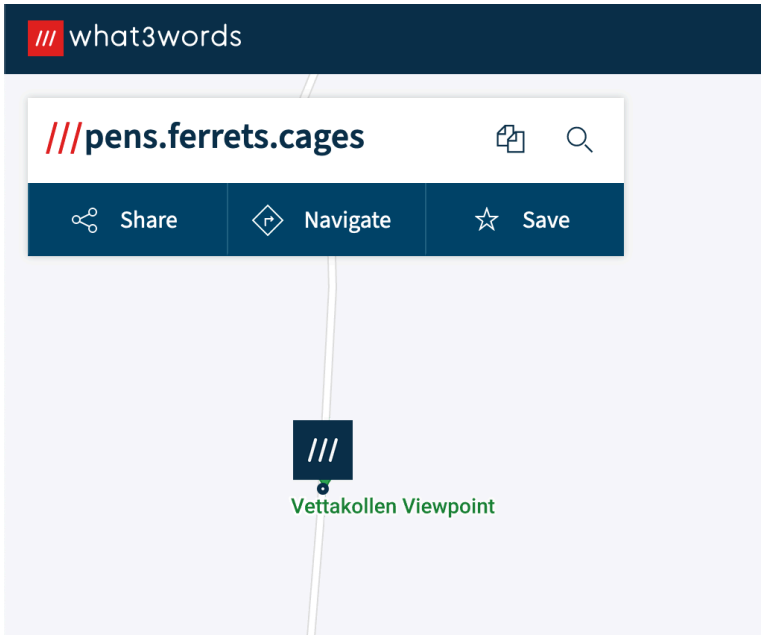
1.1 The meeting (40p)

The counter intelligence captured a message that is flagged as suspicious. “Let’s meet tomorrow at `///pens.ferrets.cages` at 10. I’ll give you all documents.” Can you help them to find out where the meeting takes place?

Solution:
I found this task a bit difficult mostly because i didn’t understand what the three slashes ment. So I searched for the cages suffix assuming it was a file extension, and stumbled upon what3words.com.



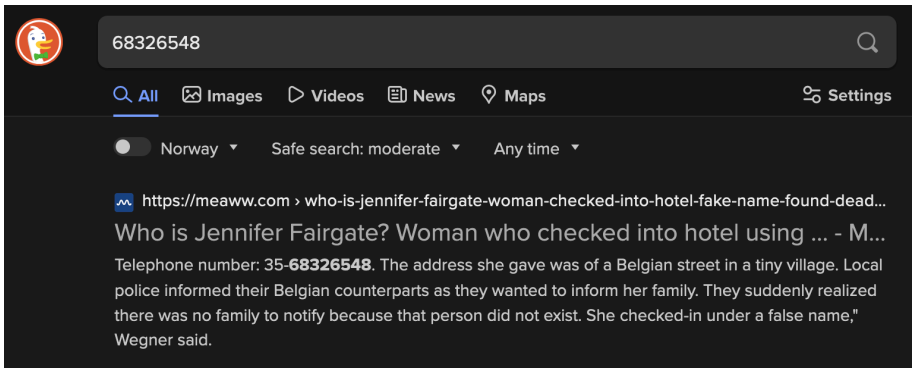
After that i just followed the link and found the location of the meeting.



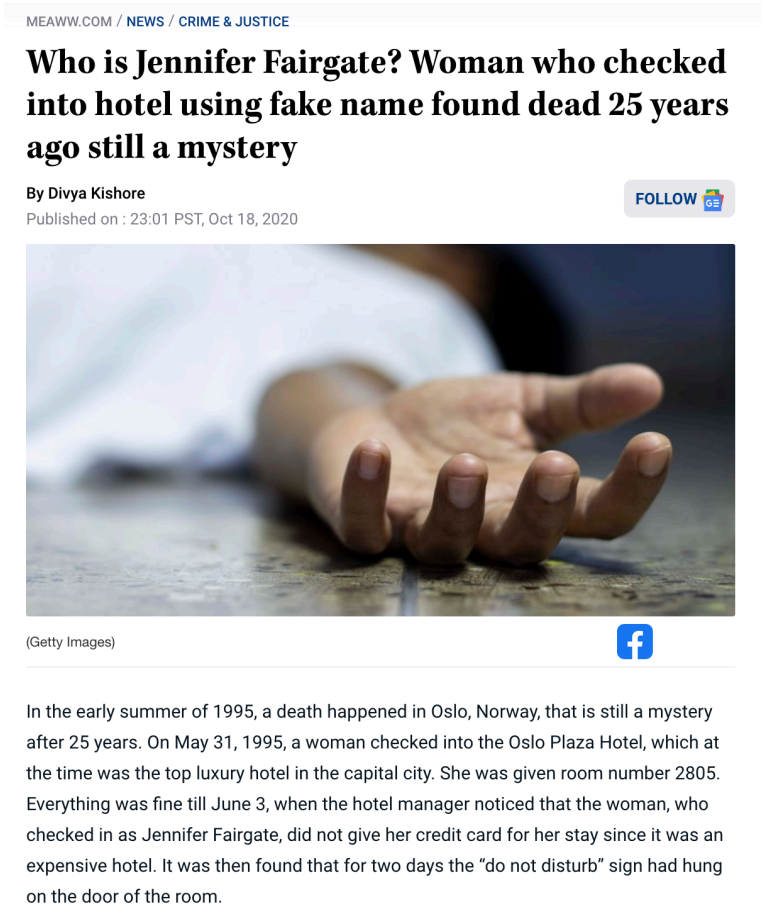
1.2 Cherchez la femme (50p)

I met this girl many years ago in Oslo. She was kind but very mysterious. She told me she lived in a hotel and wrote down her phone number on a piece of paper. She didn't even tell me her name and of course the phone number was fake. The same happens to me every time with girls with blue eyes :) After all these years can you help me to find her name at least?

Solution:
This task was pretty simple, all i did was to search the phone number from the image...



...and follow the link the the article...

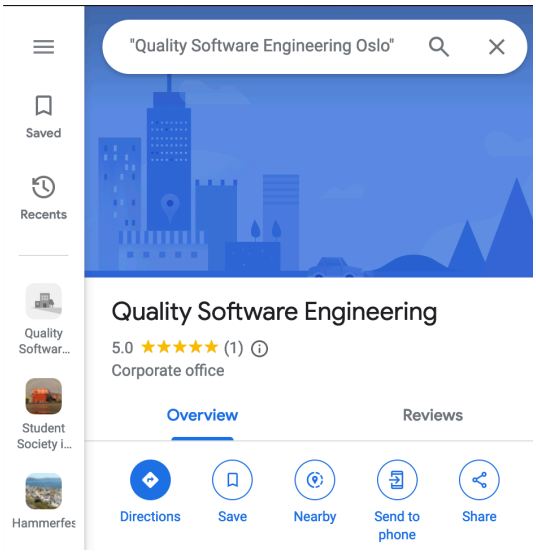


...to find the name.

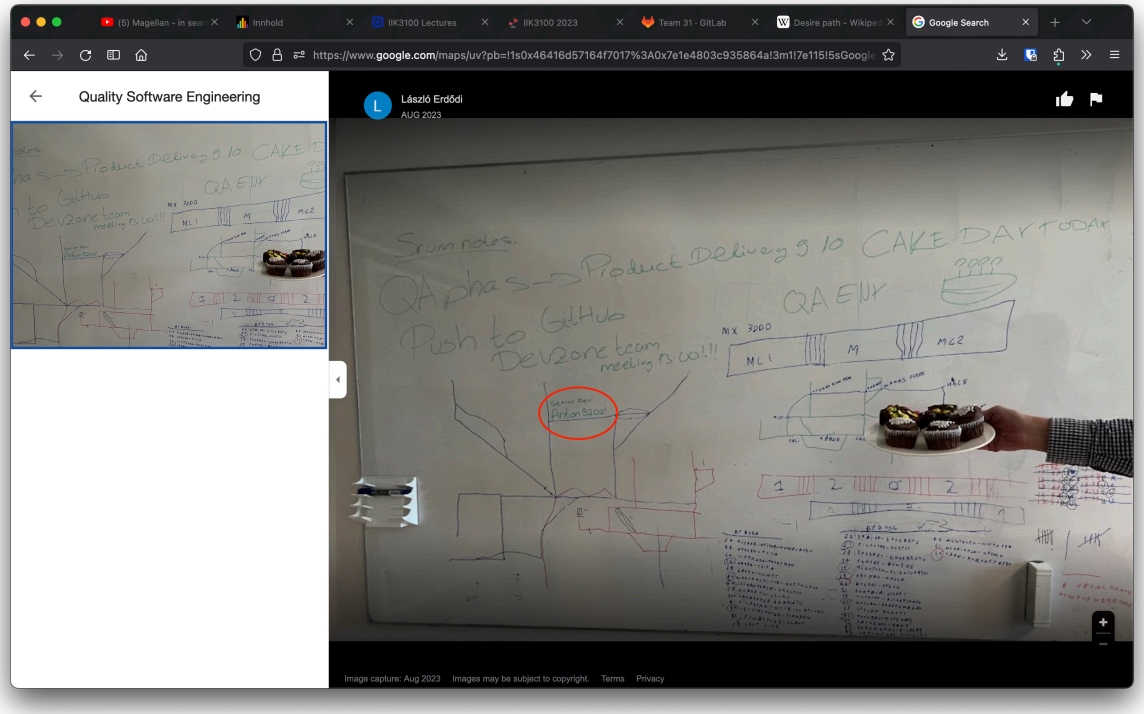
1.3 Quality software (50p)

There's this software developer company the Quality Software Engineering Oslo. I think they stole our product code, so I need their Github password :)

Solution:
This task was a bit more difficult, mostly because I overlooked the results in the sidebar on Google. Regardless I managed to find the company on Google Maps.



And found a review with an image.



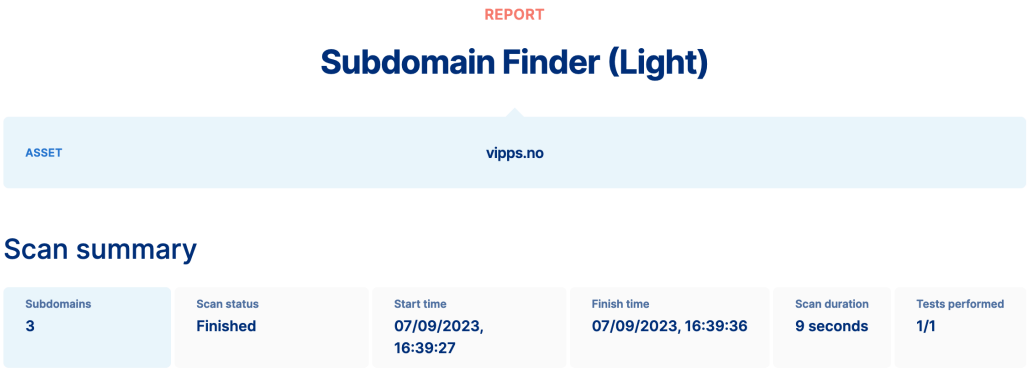
And after looking for a while I found a senior developer followed by a phrase that looked like a password.

2 Technical Information Gathering

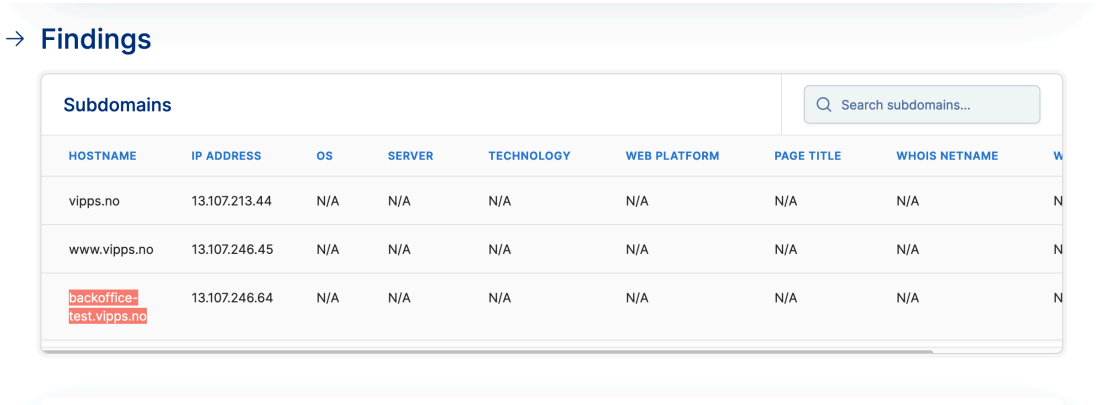
2.1 Vipps backoffice (30p)

Can you find the backoffice website of Vipps? Send the domain as a flag!

Solution:
The difficulty in this task was mostly finding a website that could look for and display subdomains without a paywall, since my manual attempts at finding the subdomain failed. I found a website called pentest-tools.com that could do this for me.



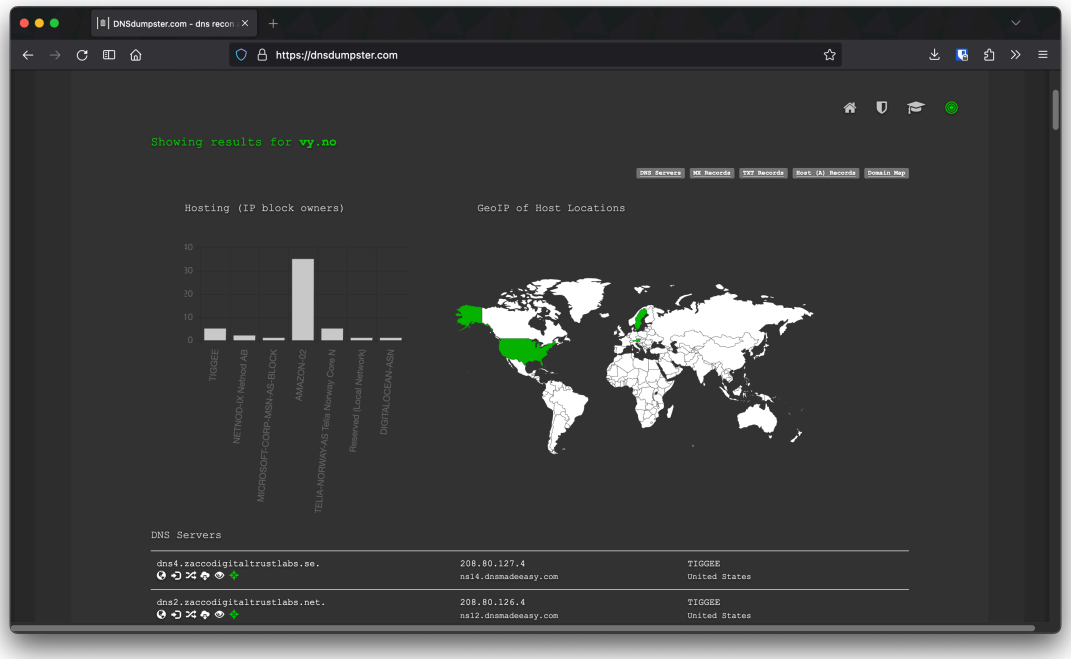
After the scan three subdomains were found, and the one that looked most promising was backoffice-test.vipps.no.



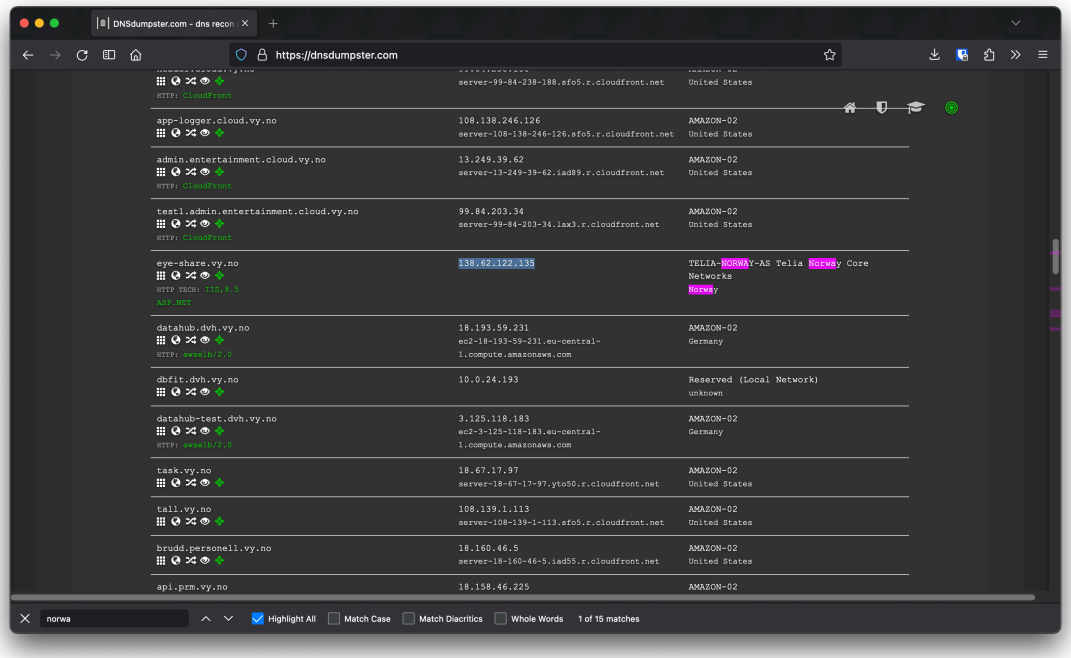
2.2 Vy (30p)

Find the network range of Vy in Norway! Write it in CIDR format!

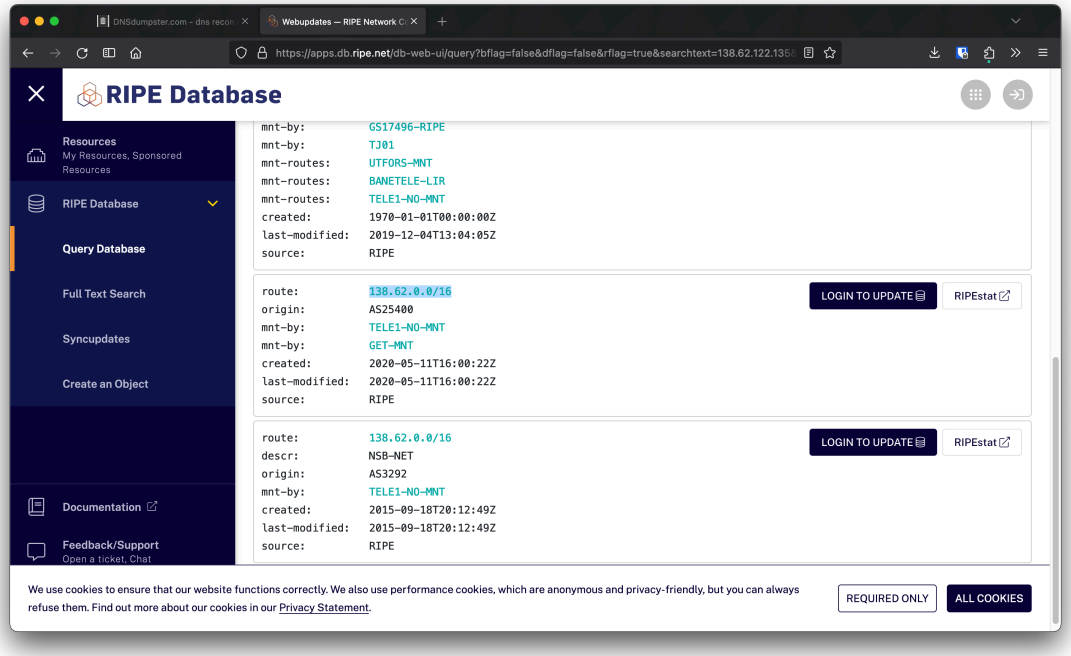
Solution:
This task was pretty straight forward, all I needed to di was look up vy.no on dnsdumpster.com.



Then find an IP-address from Norway...



…and look it up in the RIPE database.

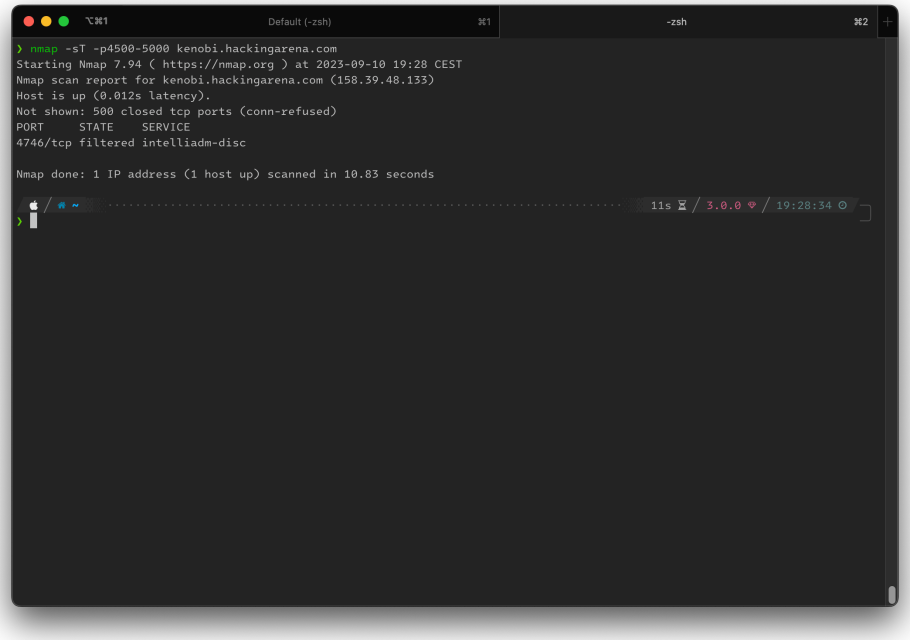


3 Network Mapping

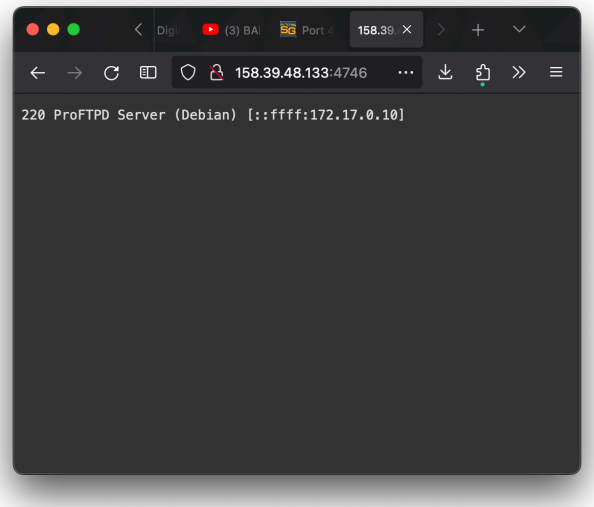
3.1 Detect the version (30p)

What type of service is running on kenobi.hackingarena.com in the port range 4500-5000?

Solution:
This task was quite straight forward, I used nmap to scan the ports in the range 4500-5000, and got one open port.



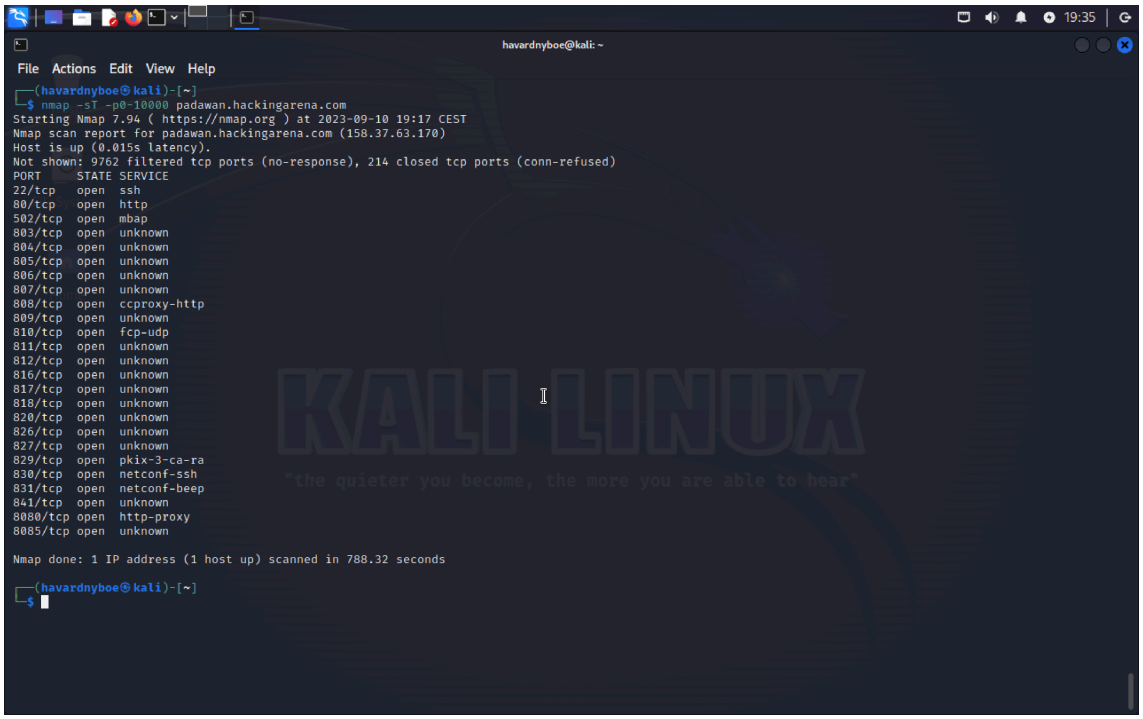
Then i connected to the address on the specified port with a browser, and got the following page with the answer being ProFTPD:



3.2 Padawan all ports (40p)

What is the sum of the all open ports at padawan.hackingarena.com? This time not only the regular ports has to be considered. E.g. if only tcp22, tcp80 and tcp443 is open then the answer is 545.

Solution:
When I first tried to solve this task i begun a full port scan with nmap using the `-p-` flag, but after 15 minutes i realised that this would take a long time. So i decided to use the `-p0-10000` flag to scan the first 10000 ports. This seemed to be enough, as i got the following output:



The sum of all the open ports was 33099.