

IHK3100 – Etisk hacking og penetrasjonstesting

Home Exam

Håvard Solberg Nybøe

12. september 2023

Innhold

1 OSINT	2
1.1 The meeting (40p)	2
1.2 Cherchez la femme (50p)	3
1.3 Quality software (50p)	4
2 Technical Information Gathering	5
2.1 Vipps backoffice (30p)	5
2.2 Vy (30p)	6
3 Network Mapping	8

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 meant. So I searched for the cages suffix assuming it was a file extension, and stumbled upon what3words.com.

A screenshot of a Google search results page. The search query is "filetype:cages". The results section shows "About 133 results (0.22 seconds)". Two links are listed:

- what3words.com**
https://what3words.com › onion.patio.cages :
onion.patio.cages - What3Words
Every 3 metre square of the world has been given a unique combination of three words. Used for e-commerce and delivery, navigation, emergencies and more.
- nests.town.cages - What3Words**
https://what3words.com › nests.town.cages :
Every 3 metre square of the world has been given a unique combination of three words. Used for e-commerce and delivery, navigation, emergencies and more.

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

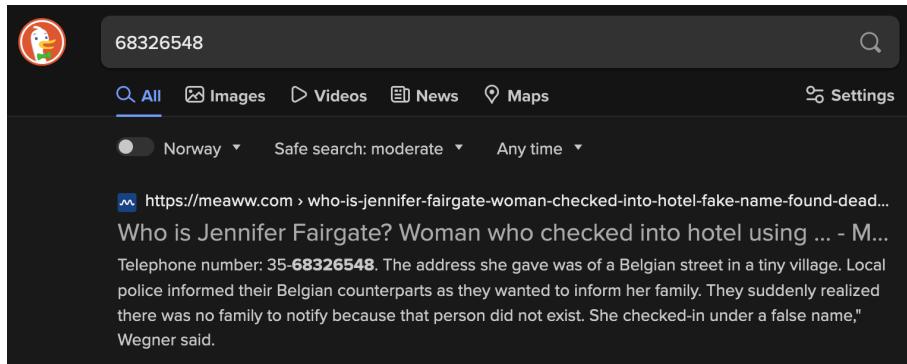
A screenshot of the what3words website. The URL in the address bar is `///pens.ferrets.cages`. The main content area displays the location "Vettakollen Viewpoint" with a small map icon and the three slashes logo.

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...

MEAWW.COM / NEWS / CRIME & JUSTICE

Who is Jennifer Fairgate? Woman who checked into hotel using fake name found dead 25 years ago still a mystery

By Divya Kishore

Published on : 23:01 PST, Oct 18, 2020

FOLLOW GETTY



(Getty Images)



In the early summer of 1995, a death happened in Oslo, Norway, that is still a mystery after 25 years. On May 31, 1995, a woman checked into the Oslo Plaza Hotel, which at the time was the top luxury hotel in the capital city. She was given room number 2805. Everything was fine till June 3, when the hotel manager noticed that the woman, who checked in as Jennifer Fairgate, did not give her credit card for her stay since it was an expensive hotel. It was then found that for two days the "do not disturb" sign had hung on the door of the room.

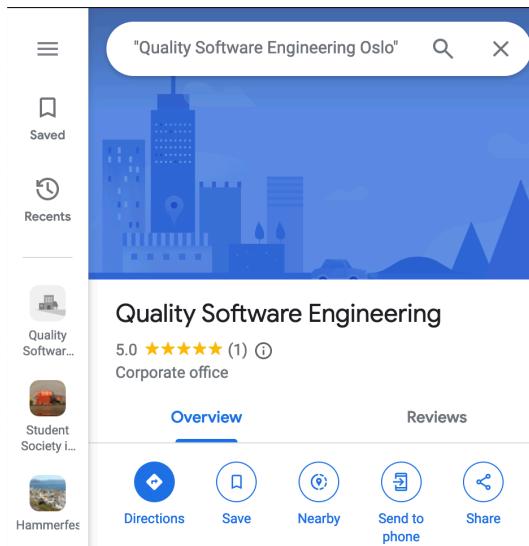
...to find the name.

1.3 Quality software (50p)

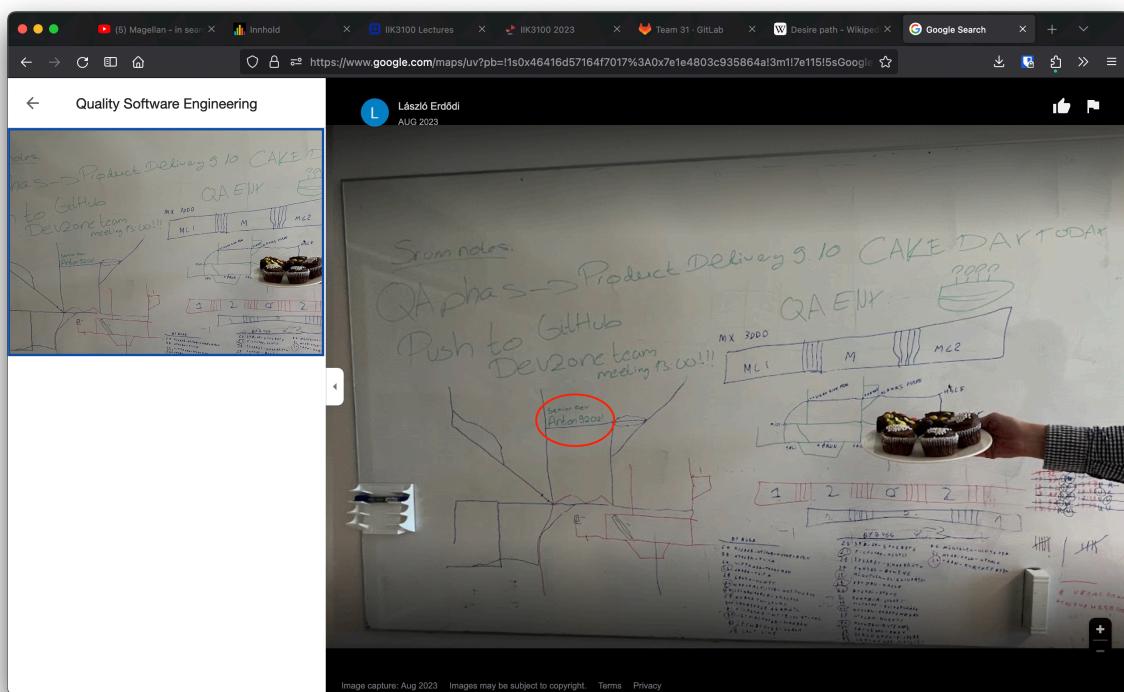
There's this software developer company the Quality Software Engineering Oslo. I think they stole our product code, so I need their Github password :)

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.

REPORT	
Subdomain Finder (Light)	
ASSET	vipps.no
Scan summary	
Subdomains 3	Scan status Finished
Start time 07/09/2023, 16:39:27	Finish time 07/09/2023, 16:39:36
Scan duration 9 seconds	Tests performed 1/1

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

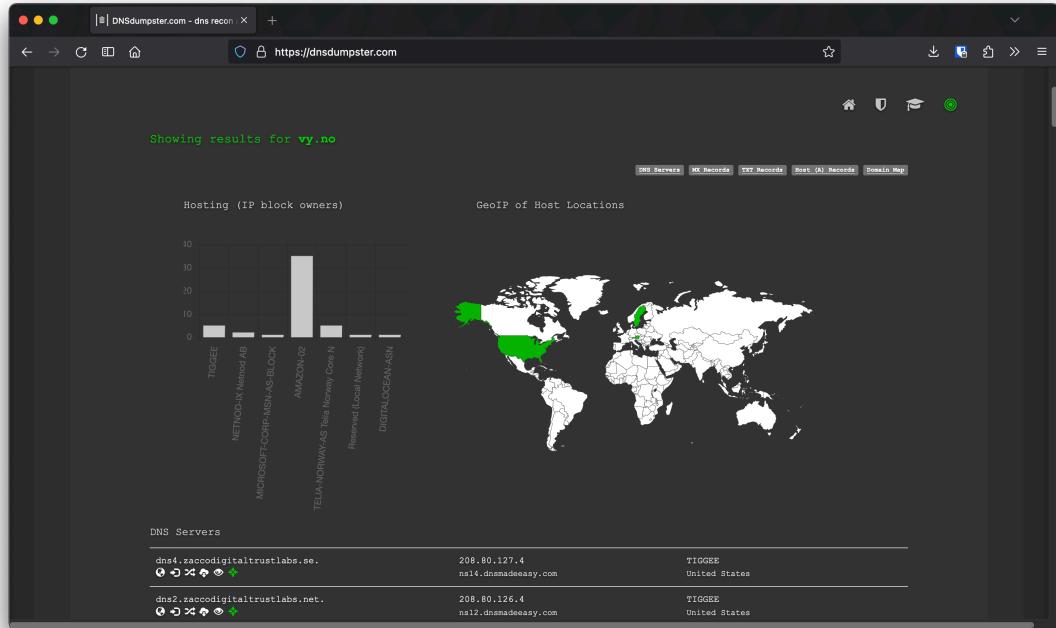
Subdomains								<input type="text"/> Search subdomains...
Hostname	IP Address	OS	Server	Technology	Web Platform	Page Title	Whois Netname	W
vipps.no	13.107.213.44	N/A	N/A	N/A	N/A	N/A	N/A	N/A
www.vipps.no	13.107.246.45	N/A	N/A	N/A	N/A	N/A	N/A	N/A
backoffice-test.vipps.no	13.107.246.64	N/A	N/A	N/A	N/A	N/A	N/A	N/A

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 do was look up vy.no on dnsdumpster.com.



Then find an IP-address from Norway...

The screenshot shows the dnsdumpster.com search results for the query "norway". The results table includes columns for the host name, IP address, and location. The results are as follows:

Host Name	IP Address	Location
server-99-84-238-188.sfo5.r.cloudfront.net	108.138.246.126	AMAZON-02 United States
server-108-138-246-126.sfo5.r.cloudfront.net	108.138.246.126	AMAZON-02 United States
server-13-249-39-62.iad89.r.cloudfront.net	13.249.39.62	AMAZON-02 United States
server-99-84-203-34.lax3.r.cloudfront.net	99.84.203.34	AMAZON-02 United States
server-99-84-203-34.lax3.r.cloudfront.net	99.84.203.34	AMAZON-02 United States
138.62.122.135	138.62.122.135	TELIA-NORWAY-AS Relia Norway Core Networks Norway
ec2-18-193-59-231.eu-central-1.compute.amazonaws.com	18.193.59.231	AMAZON-02 Germany
eu2-3-125-118-183.eu-central-1.compute.amazonaws.com	3.125.118.183	AMAZON-02 Germany
server-18-67-17-97.yto50.r.cloudfront.net	18.67.17.97	AMAZON-02 United States
server-108-139-1-113.sfo5.r.cloudfront.net	108.139.1.113	AMAZON-02 United States
server-18-160-46-5.iad55.r.cloudfront.net	18.160.46.5	AMAZON-02 United States
18.158.46.225	18.158.46.225	AMAZON-02

...and look it up in the RIPE database.

The screenshot shows a web browser window displaying the RIPE Database search results for the IP address 138.62.0.0/16. The search query is: https://apps.db.ripe.net/db-web-ui/query?bflag=false&dflag=false&rflag=true&searchtext=138.62.122.135. The results are presented in three separate sections, each showing detailed information about the route object:

Route Object	Information
138.62.0.0/16 (AS25400)	mnt-by: GS17496-RIPE mnt-by: TJ01 mnt-routes: UTFORS-MNT mnt-routes: BANETELE-LIR created: 1970-01-01T00:00:00Z last-modified: 2019-12-04T13:04:05Z source: RIPE
138.62.0.0/16 (AS3292)	route: 138.62.0.0/16 origin: NSB-NET mnt-by: TELE1-NO-MNT created: 2020-05-11T16:00:22Z last-modified: 2020-05-11T16:00:22Z source: RIPE
138.62.0.0/16 (AS3292)	route: 138.62.0.0/16 descr: NSB-NET origin: AS3292 mnt-by: TELE1-NO-MNT created: 2015-09-18T20:12:49Z last-modified: 2015-09-18T20:12:49Z source: RIPE

The sidebar on the left includes links for Resources, RIPE Database (selected), Query Database, Full Text Search, Syncupdates, Create an Object, Documentation, and Feedback/Support. At the bottom, there is a cookie consent banner with options for REQUIRED ONLY or ALL COOKIES.

3 Network Mapping