IIK3100 – Etisk hacking og penetrasjonstesting
Home Exam

Håvard Solberg Nybøe

October 30, 2023

Contents

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**
3.1 Detect the version (30p) 8
3.2 Padawan all ports (40p) 9
3.3 Censys (30p) 9

4 Get In Touch With Services **11**
4.1 Casanova (70p) 11
4.2 Minuteman (80p) 13

5 Web Hacking **15**
5.1 Beatles song catalogue (60p) 15
5.2 Web 5 (60p) 17
5.3 Redirect (60p) 19
5.4 Arenabook (80p) 20

Total points: 710p **23**

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.

REPORT

Subdomain Finder (Light)

ASSET	vipps.no

→ **Scan summary**

Subdomains	Scan status	Start time	Finish time	Scan duration	Tests performed
3	Finished	07/09/2023, 16:39:27	07/09/2023, 16:39:36	9 seconds	1/1

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

→ **Findings**

Subdomains 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
www.vipps.no	13.107.246.45	N/A	N/A	N/A	N/A	N/A	N/A	N
backoffice-test.vipps.no	13.107.246.64	N/A	N/A	N/A	N/A	N/A	N/A	N

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.

3.3 Censys (30p)

Use Censys to find a computer in Oslo that runs Ubuntu 20.04 and tcp port 2233 is open. What is the ip?

Solution:
Using Censys I searched for the following query:

`location.city:oslo and services.port:2233 and services.software.vendor:Ubuntu`

and got the following result:

The ip is: `185.101.34.119`

4 Get In Touch With Services

4.1 Casanova (70p)

My service is running on `kenobi.hackingarena.com`, port `9393`. My name is Casanova (username: `casanova`). I have a huge problem. One of my exgirlfriends somehow figured out my password and want to realese all details about my affairs. How she figured it out??? I was so cautios. Ok, I'm using the same password everywhere, but I never had any incident (except for this emberassing Ashley Madison case). I hope you cannot login.

Solution:
I started by connecting to the service with netcat, and got the following output:

That told me that an ssh service was running on the instance. I then figured the «Ashley Madison case» was a hint to a password breach, so i searched for it and found the top 100 passwords from the breach. I put the 100 passwords in a file called `passwrd.txt` and used hydra to brute force the password for the user `casanova` on the ssh service as such:

```
❯ hydra -l casanova -P passwrd.txt ssh://kenobi.hackingarena.com:9393
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** igno
re laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-26 15:58:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
 reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries
per task
[DATA] attacking ssh://kenobi.hackingarena.com:9393/
[9393][ssh] host: kenobi.hackingarena.com   login: casanova   password: kazuga
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-26 15:58:39

~/Doc/emner-ntnu/II/home-exam / main !1 ?6
❯
```

I then got one hit, and the password was `kazuga`. I then connected to the service with ssh and found the flag in the home directory.

```
❯ ssh -p 9393 casanova@kenobi.hackingarena.com
casanova@kenobi.hackingarena.com's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.10.0-25-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Oct 25 16:58:36 2023 from 46.15.83.82
Execute Order 66
$ ls
flag  hellofellowstudents.wedidit  test.txt  writeaccess.txt
$ cat flag
Hacking-Arena{I_am_much_more_Casan0va}
$
```

The flag is: `Hacking-Arena{I_am_much_more_Casan0va}`

4.2 Minuteman (80p)

A service is running on `kenobi.hackingarena.com` portrange: `7000-7500`. I hope you can find this very important flag :)

Solution:
I started by scanning the ports with nmap, and got the following output:

```
❯ nmap -sT -p7000-7500 kenobi.hackingarena.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 14:58 CEST
Nmap scan report for kenobi.hackingarena.com (158.39.48.133)
Host is up (0.015s latency).
Not shown: 496 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
7197/tcp filtered unknown
7211/tcp open     unknown
7339/tcp filtered swx
7434/tcp filtered unknown
7474/tcp filtered neo4j

Nmap done: 1 IP address (1 host up) scanned in 26.41 seconds
```

I then connected to the only open service on port 7211 with telnet, and got the following response:

```
❯ telnet kenobi.hackingarena.com 7211
Trying 158.39.48.133...
Connected to kenobi.hackingarena.com.
Escape character is '^]'.
Good day Mr. President!
It's Monday 7 November, 1983.
Welcome to Able Archer!
Enter the SILO 73C password:
```

After searching for what Able Archer was, i found that it was a NATO exercise in 1983. I then found the nuclear launch codes for the exercise, which was `00000000`. I then connected to the service again with telnet, gave it the launch codes, and got the following response:

The flag was `UiO-Hacking-Arena{C0ld_war_1s_0v4r}`.

5 Web Hacking

5.1 Beatles song catalogue (60p)

There must be something hidden here: http://r2d2.hackingarena.com:1811

Solution:
I first connected to the site with Burp Suite and explored the different sites. The parameter for switching sites was `songid`, and after finding the pattern with the albums that all ended with `53` i set up an intruder attack with the following payload:

When the attack was done I searched through the results that had a length other than 232 or 233 since these were empty pages. I found the following page:

The flag is: `UiO-Hacking-Arena{Lucy 1n the Sky w1th Flags}`

5.2 Web 5 (60p)

Can you find the flag here? http://padawan.hackingarena.com:820

Solution:
The trick I found to solving this task was exceeding the character limit of the input field. When I did this I got the following error message:

Assuming the site was located at `/var/www/` I followed the path `partnerprocess/process.php`

After that I jumped to the parent directory `partnerprocess/` and found the flag in the `flag.txt` file.

Opening the file revealed the flag:

The flag is: `UiO-Hacking-Arena{Err0r_m4ssag4_d1scl0sure}`

5.3 Redirect (60p)

Can you redirect `kenobi.hackingarena.com:821` to `kenobi.hackingarena.com:822`?

Solution:
This task was all about cross site scripting. I first tried to inject a script into the input field, but this did not work. I then tried to log to the console with the injected script, but I realized some anti tampering mechanism was in place as I got a lot of `***ANTIHACKER***` in my log. I then had the idea of replacing the `window.location` with the new url. This didn't work when injecting the script, so I tried again but this time in the console and it worked.

Before running the command in the console

After running the command in the console

5.4 Arenabook (80p)

Hi, Check out the latest social media platform: http://sidious.hackingarena.com:803 Sandra already tried it. :)

Solution:
The first step was to look for Sandra.

After getting her username I could use the forgot password function to get her password. I ended up at a page asking for the birthplace of her grandmother.

After putting this page into Burp Suite I found a field in the post request called where different place names could be tried. I then visited the Wikipedia page «List of villages in Telemark» and downloaded the list of villages to a text file. Then in Burp Suite I set up an intruder attack with the list of villages as the payload.

After the attack was done I searched through the results and found the following page:

Sandras grandmother was born in `Vinjastranda`, and her password was `MyDogNameIsSigurd`. Using the password I could log in to Sandras account and get the flag.

Total points: 710p