IIK3100 – Etisk hacking og penetrasjonstesting

Practical Assignment

Kandidatnr: 10058

Contents

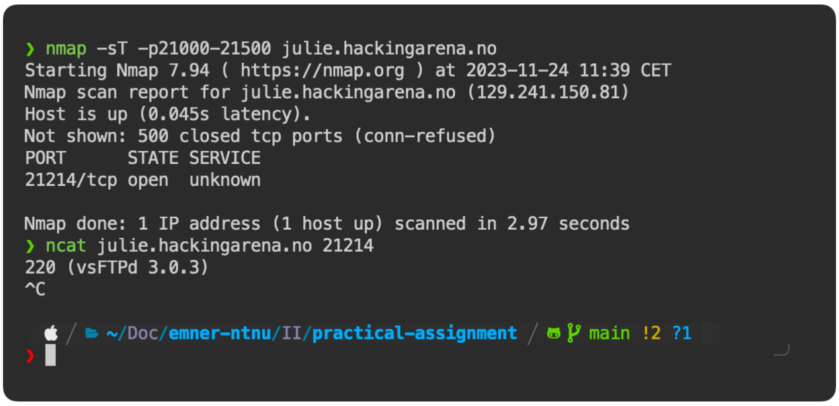
Total points: 360p

5 Get in touch with services

5.1 5th challenge (80p)

Ladies and gentlemen, this is the 5th challenge.
A little bit of everything...
julie.hackingarena.no port 21000-21500

Solution:
First I ran a nmap port scan on the ports 21000-21500, and found a service running on port 21214. I also connected to the service using netcat and found that it was an FTP server.

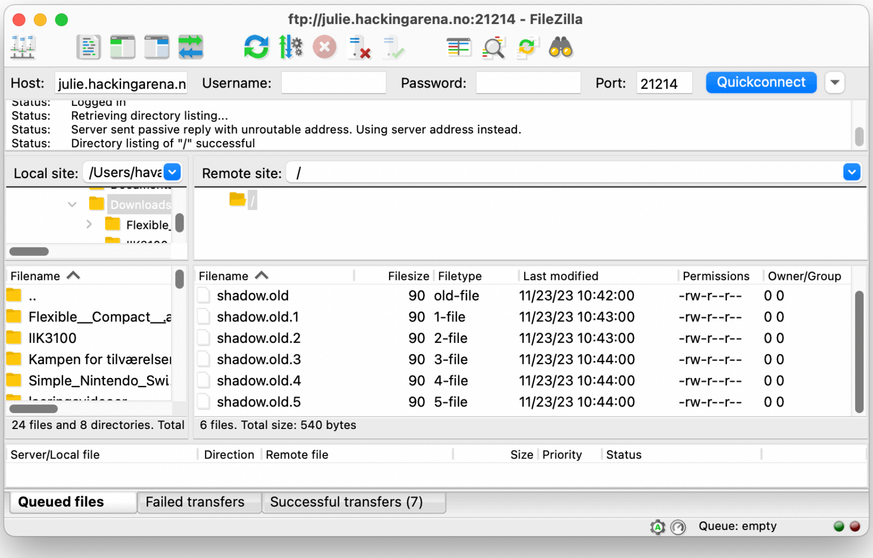


```
❯ nmap -sT -p21000-21500 julie.hackingarena.no
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-24 11:39 CET
Nmap scan report for julie.hackingarena.no (129.241.150.81)
Host is up (0.045s latency).
Not shown: 500 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21214/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.97 seconds
❯ ncat julie.hackingarena.no 21214
220 (vsFTPd 3.0.3)
^C

  / ~/Doc/emner-ntnu/II/practical-assignment /  main !2 ?1
❯
```

I then connected to the FTP server annonymously with filezilla and found six files named `shadow.old`.



ftp://julie.hackingarena.no:21214 - FileZilla

Host: julie.hackingarena.n Username: Password: Port: 21214 Quickconnect

```
Status:   Logged in
Status:   Retrieving directory listing...
Status:   Server sent passive reply with unroutable address. Using server address instead.
Status:   Directory listing of "/" successful
```

Local site: /Users/hava   Remote site: /

Filename
..
Flexible__Compact__a
IIK3100
Kampen for tilværelsei
Simple_Nintendo_Swi

24 files and 8 directories. Total

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group
shadow.old	90	old-file	11/23/23 10:42:00	-rw-r--r--	0 0
shadow.old.1	90	1-file	11/23/23 10:43:00	-rw-r--r--	0 0
shadow.old.2	90	2-file	11/23/23 10:43:00	-rw-r--r--	0 0
shadow.old.3	90	3-file	11/23/23 10:44:00	-rw-r--r--	0 0
shadow.old.4	90	4-file	11/23/23 10:44:00	-rw-r--r--	0 0
shadow.old.5	90	5-file	11/23/23 10:44:00	-rw-r--r--	0 0

6 files. Total size: 540 bytes

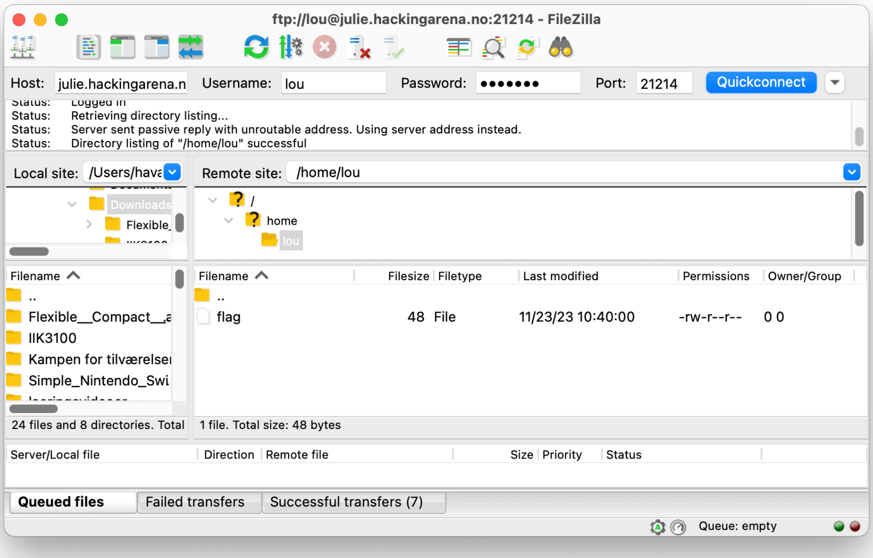
Opening the files revealed what looked like some hashed login credentials. I used https://www.dcode.fr/md5-hash to crack the hashes and found the following credentials:

```
> shadow.old
lou:Mary
> shadow.old.1
lou:Sandra
> shadow.old.2
lou:Tina
> shadow.old.3
lou:Rita
> shadow.old.4
lou:Monica
> shadow.old.5
lou:Mary
```

Given the six names and the intro text to the task I connected that this was a reference to the song *Mambo No. 5* by Lou Bega. Looking at the chorus of the song I found one of the names that was not used in the hashes, `Jessica`.

```
[Chorus]
A little bit of Monica in my life
A little bit of Erica by my side
A little bit of Rita's all I need
A little bit of Tina's what I see
A little bit of Sandra in the sun
A little bit of Mary all night long
A little bit of Jessica, here I am
A little bit of you makes me your man (Ha!)
```

I then logged in to the FTP server with the username `lou` and the password `Jessica` and found the flag file.



ftp://lou@julie.hackingarena.no:21214 - FileZilla

Host: julie.hackingarena.n Username: lou Password: ••••••• Port: 21214

```
Status:     Logged in
Status:     Retrieving directory listing...
Status:     Server sent passive reply with unroutable address. Using server address instead.
Status:     Directory listing of "/home/lou" successful
```

Local site: /Users/hava

Remote site: /home/lou

Filename
..
Flexible__Compact__a
IIK3100
Kampen for tilværelsen
Simple_Nintendo_Swi

24 files and 8 directories. Total

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group
..					
flag	48	File	11/23/23 10:40:00	-rw-r--r--	0 0

1 file. Total size: 48 bytes

Queue: empty

The flag was `Hacking-Arena{Everybody_in_come_on_let's_flag}`.

this page is intentionally left blank