THM Sweettooth Inc

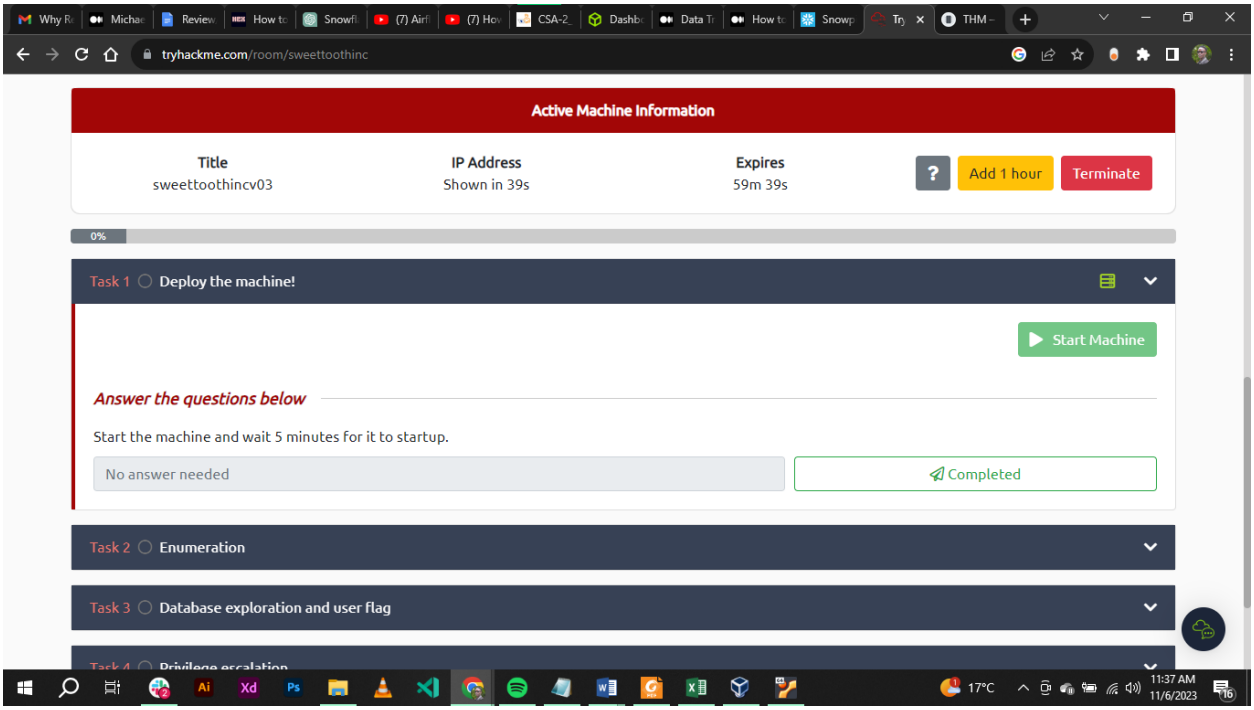
Introduction

This sub task introduces the learner to the practical knowledge of **Sweettooth Inc.** a tool for database inspection and exploration. The learner as a Security Analyst needs to understand how Sweettooth works. In part of learning this module, the objectives and tasks will be deploying the machine, enumeration, database exploration and user flag, privilege escalation, escape! and Credits.

Activities

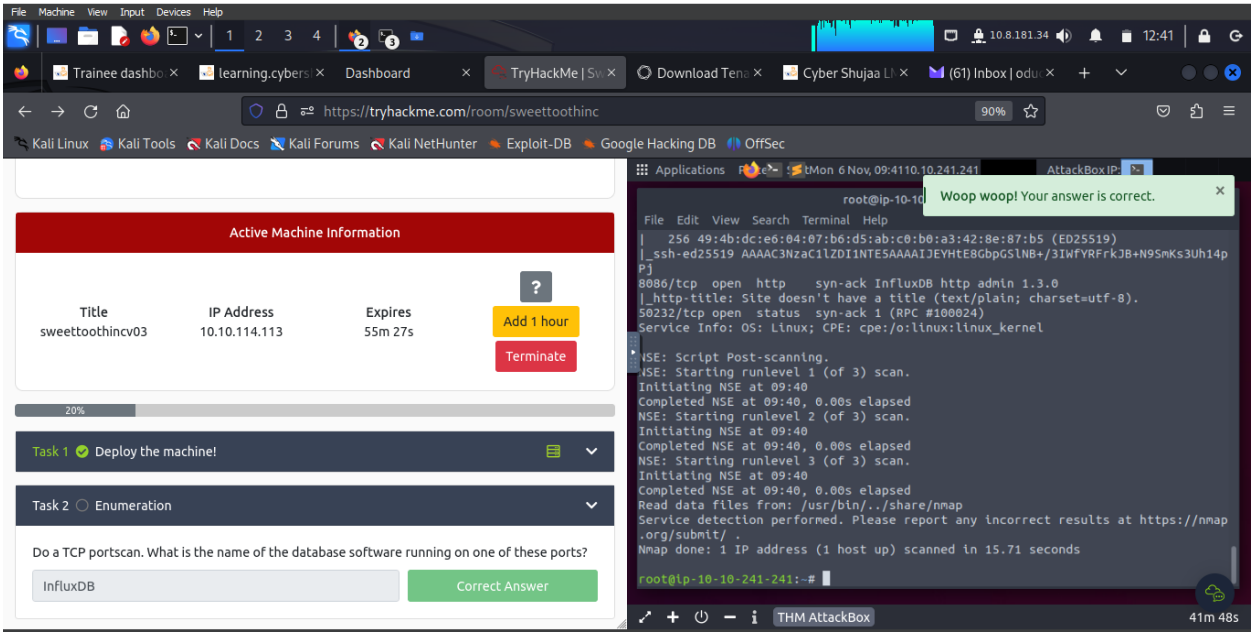
Task 1: Deploy the machine!

This section helps the learner to know the VM they will be working on.



Task 2: Enumeration

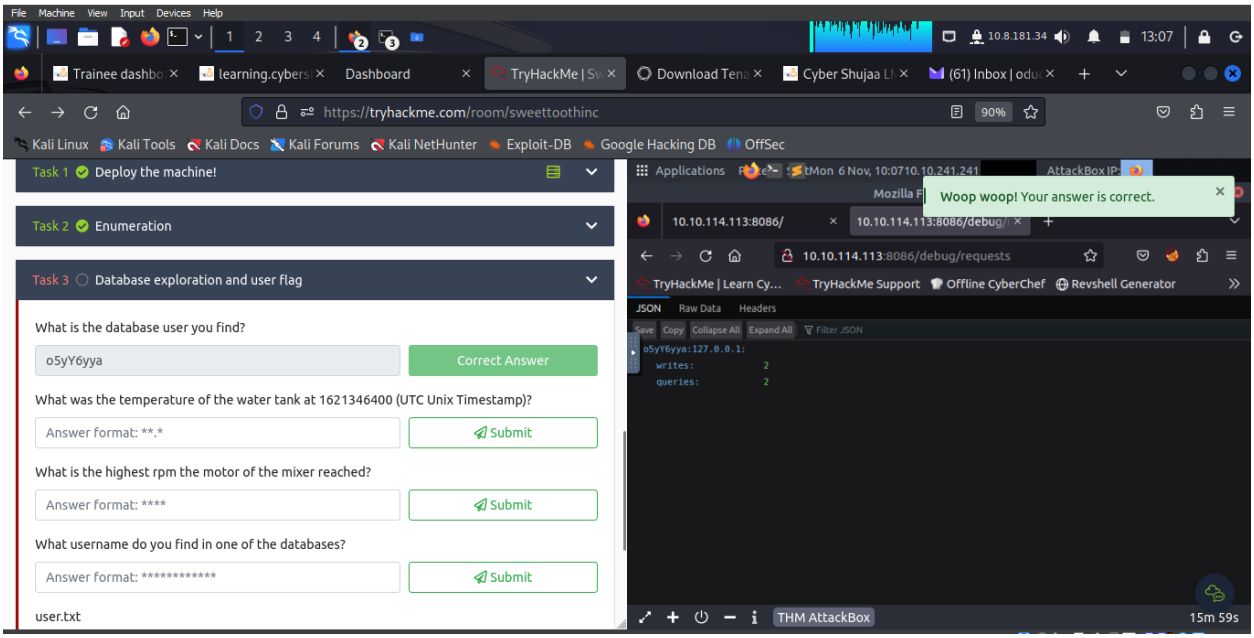
In this activity the learner used rustscan to scan the TCP port and got the following:



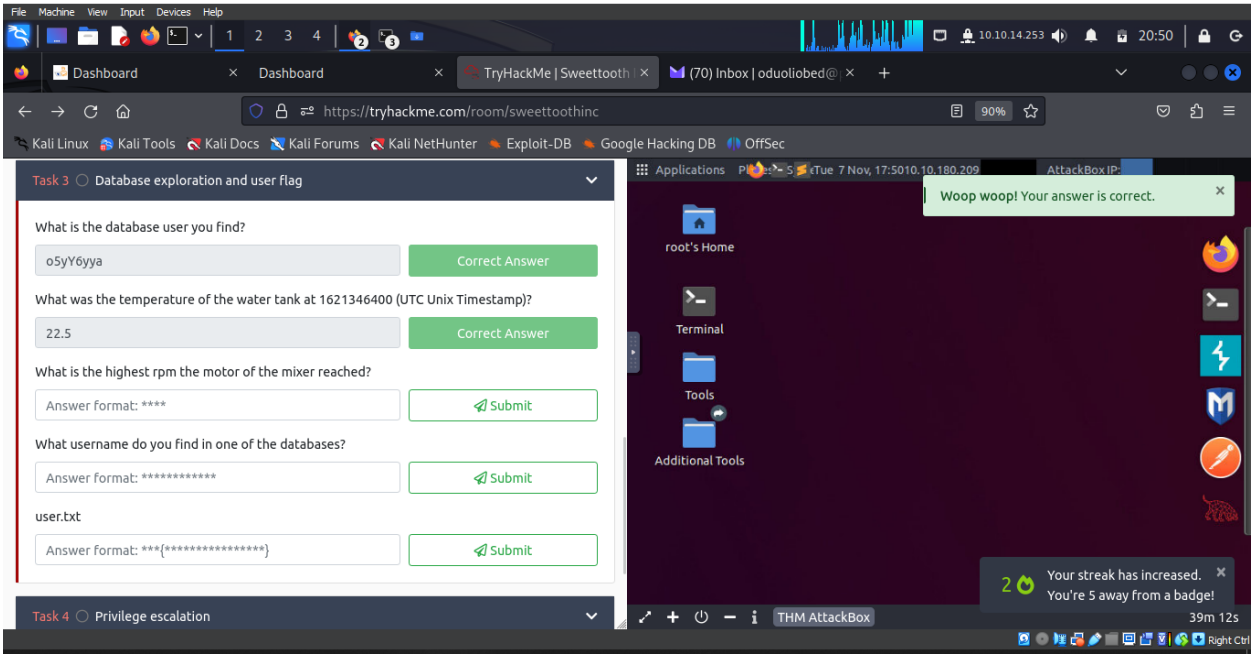
The syntax for the scan is: ***rustscan –a 'machine-ip' -- -sC –sV***

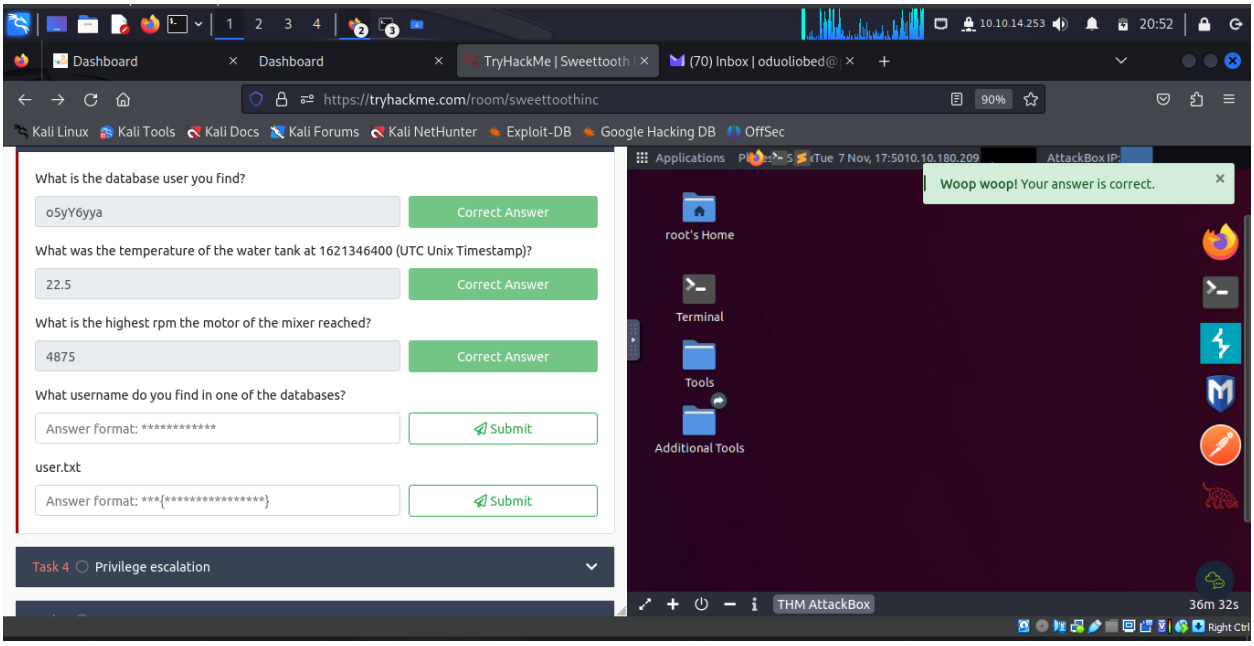
Task 3: Database exploration and user flag

The learner found the database user as: ***o5yY6yya***

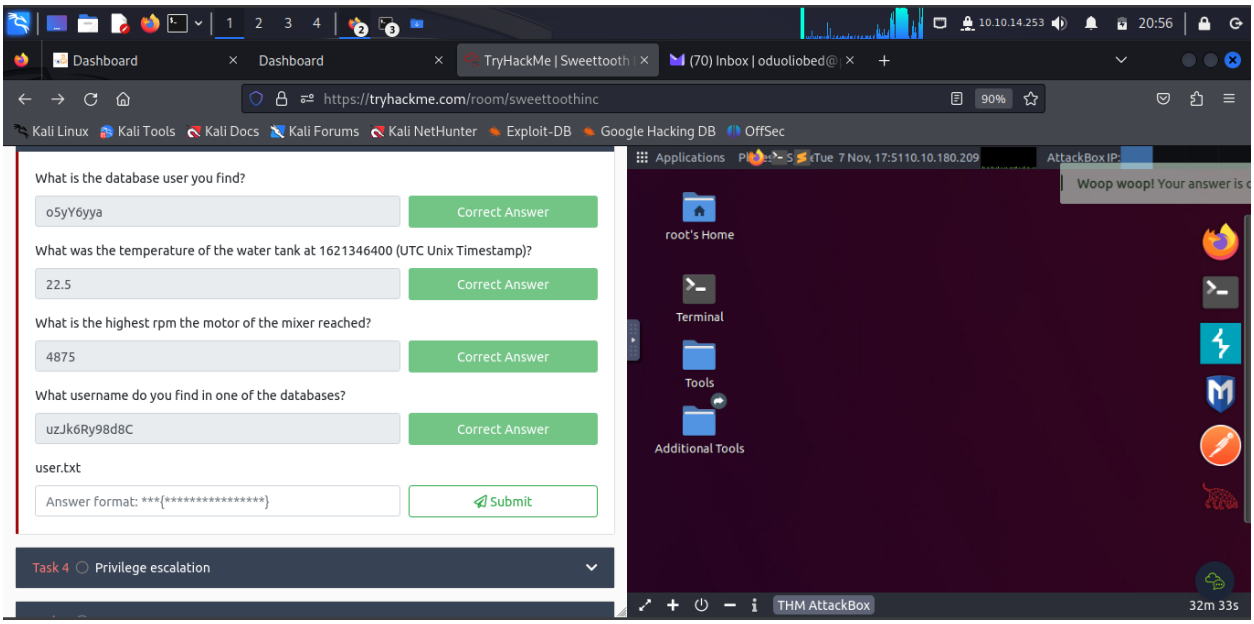


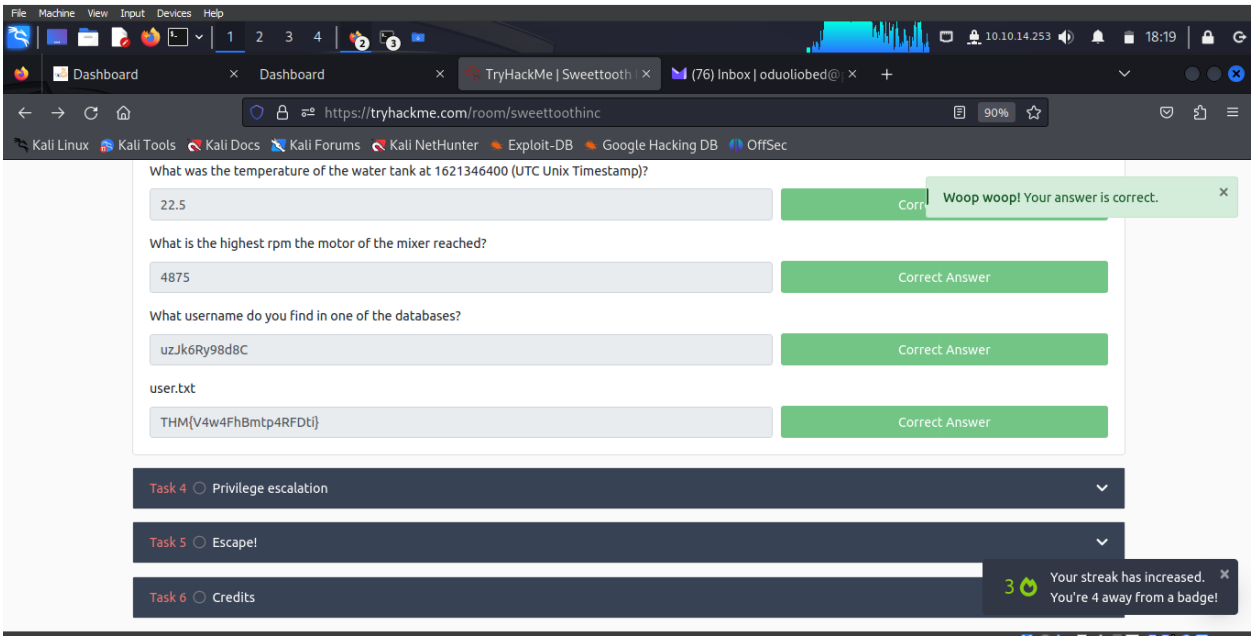
This happened after successfully running: ***https://10.10.114.113:8086/debug/requests***


Task 3 Database exploration and user flag
What is the database user you find?
o5yY6yya
Correct Answer
What was the temperature of the water tank at 1621346400 (UTC Unix Timestamp)?
22.5
Correct Answer
What is the highest rpm the motor of the mixer reached?
Answer format: ****
Submit
What username do you find in one of the databases?
Answer format: **********
Submit
user.txt
Answer format: ***{****************}
Submit
Task 4 Privilege escalation
Woop woop! Your answer is correct.
Your streak has increased.
You're 5 away from a badge!
THM AttackBox
39m 12s

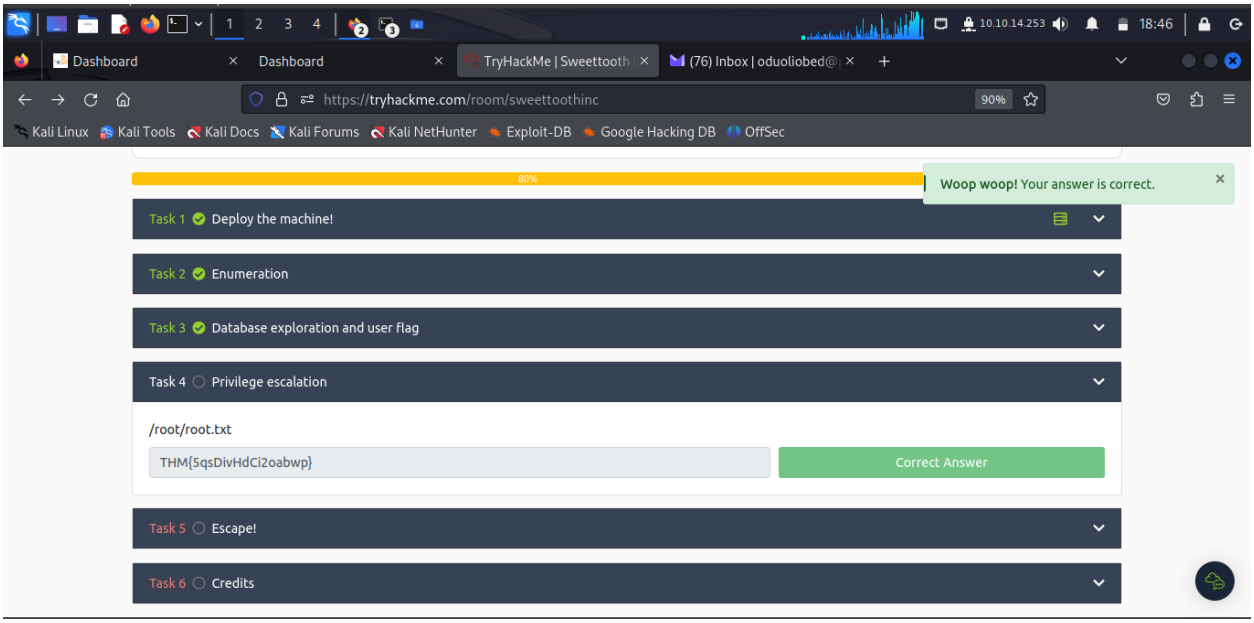

What is the database user you find?
o5yY6yya
Correct Answer
What was the temperature of the water tank at 1621346400 (UTC Unix Timestamp)?
22.5
Correct Answer
What is the highest rpm the motor of the mixer reached?
4875
Correct Answer
What username do you find in one of the databases?
Answer format: **********
Submit
user.txt
Answer format: ***{****************}
Submit
Task 4 Privilege escalation
Woop woop! Your answer is correct.
THM AttackBox
36m 32s

The database username at "***https://10.10.114.113:8086/debug /vars".***



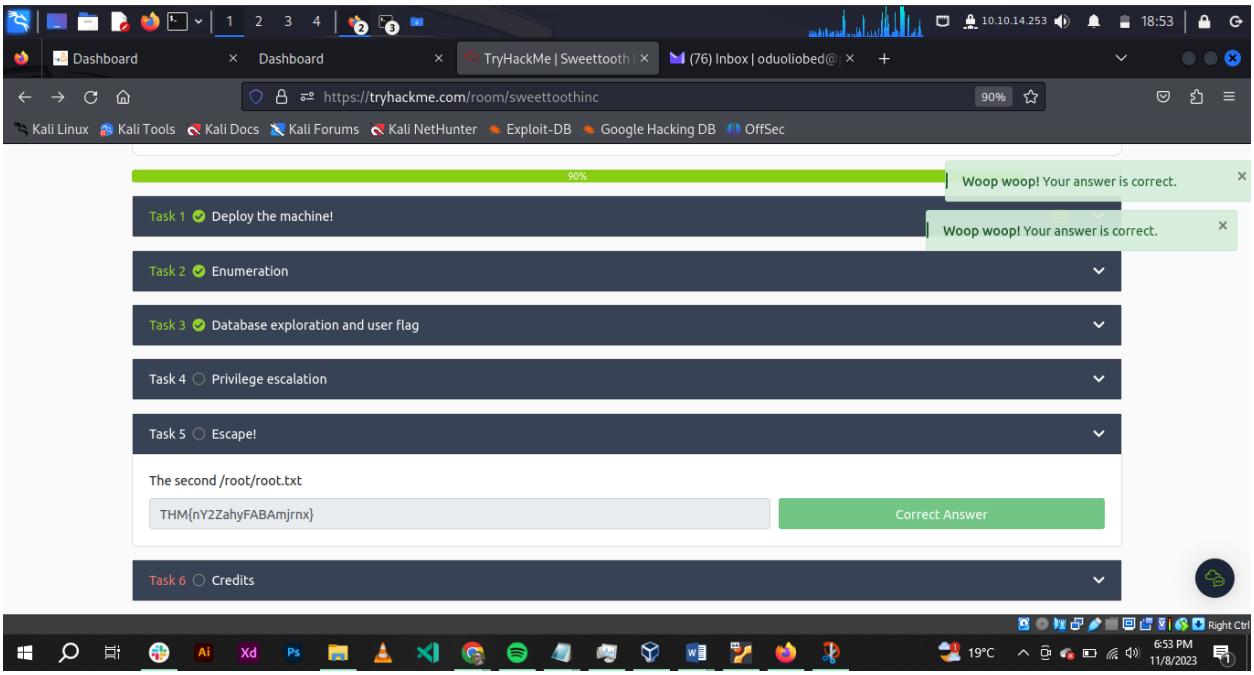


Task 4: Privilege escalation

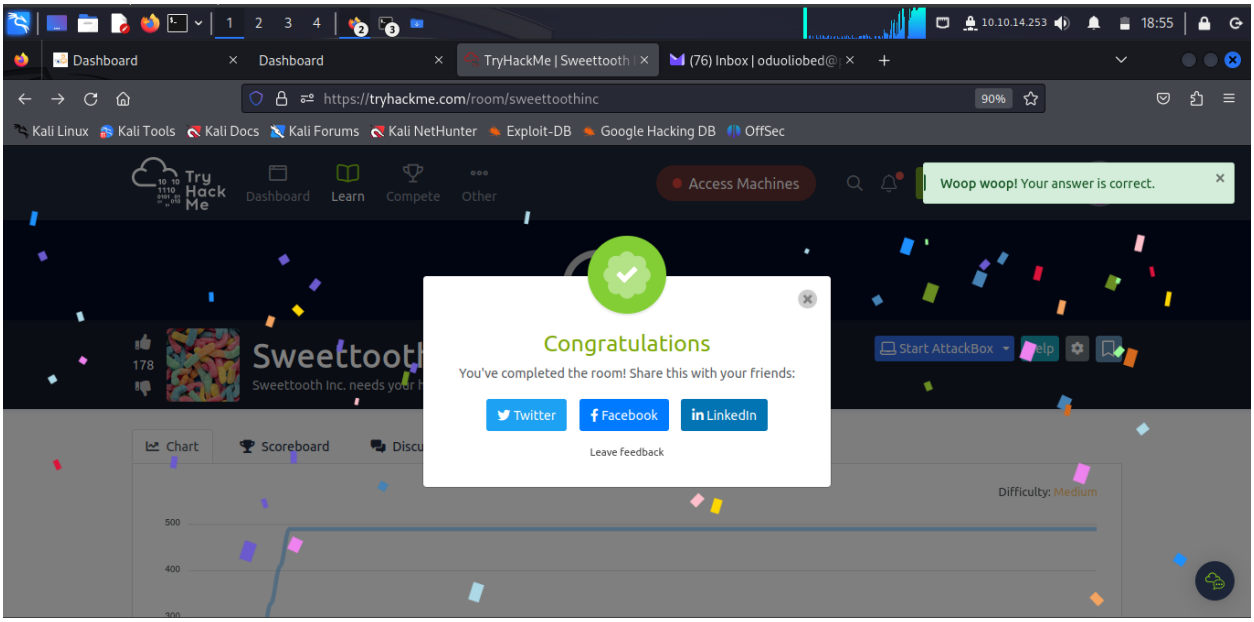


Task 5: Escape!

The learner run..



Task 6: Credits



Conclusion

This task took the learner penetrating InfluxDB or database exploits and enhanced knowledge in Cybersecurity.