**THM Sweettooth Inc**

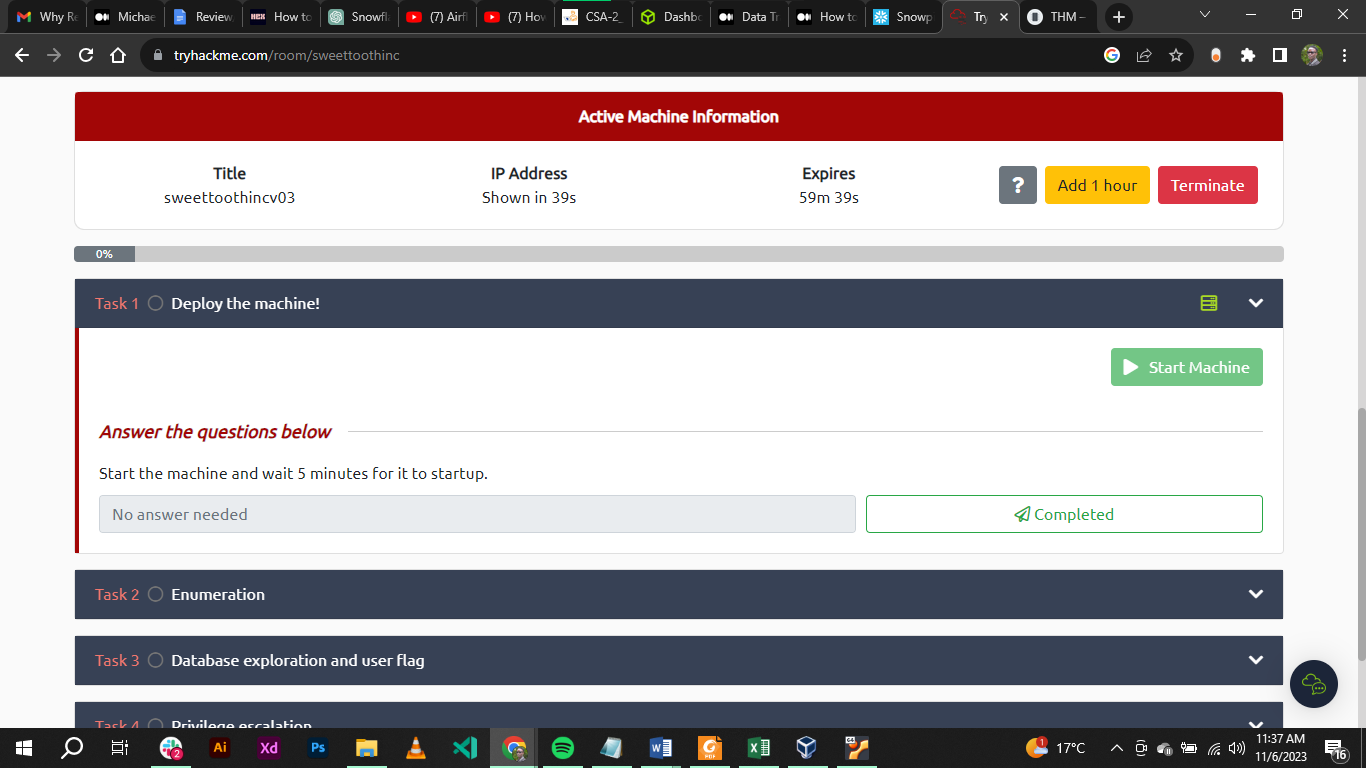
**Introduction**

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***

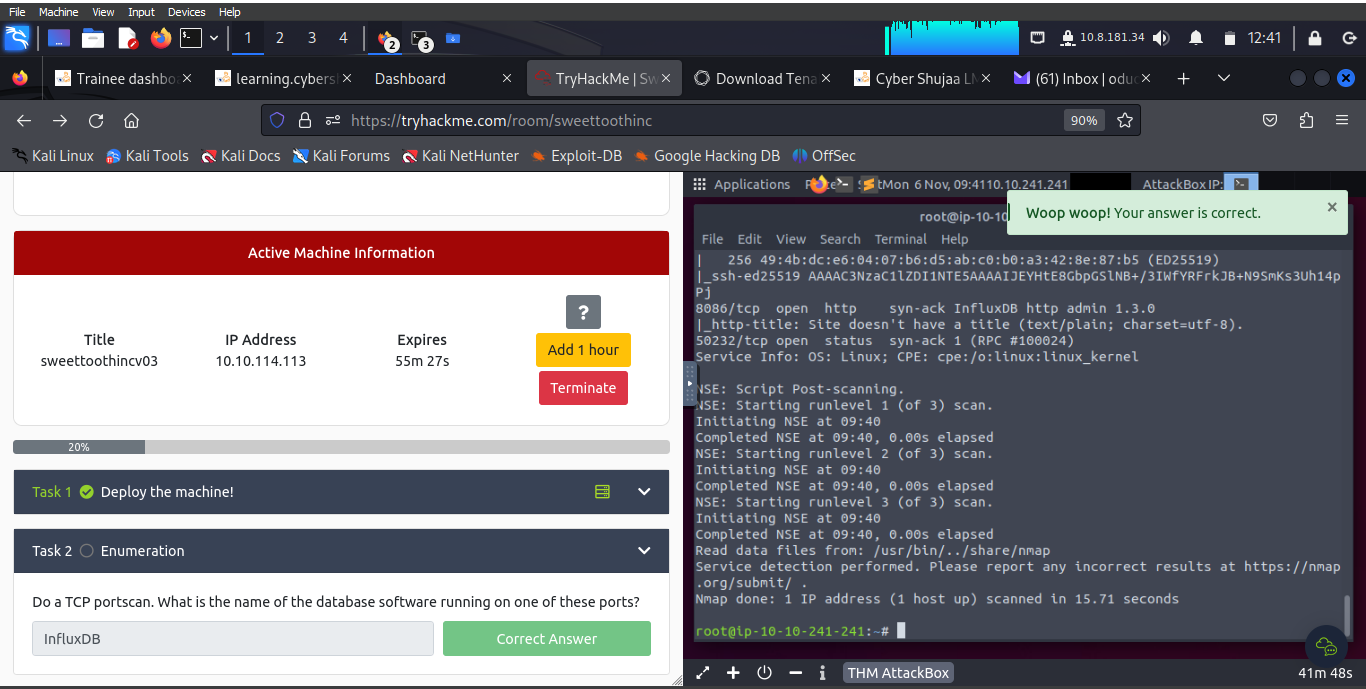
***Task 1: Deploy the machine!***

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



***Task 2: Enumeration***

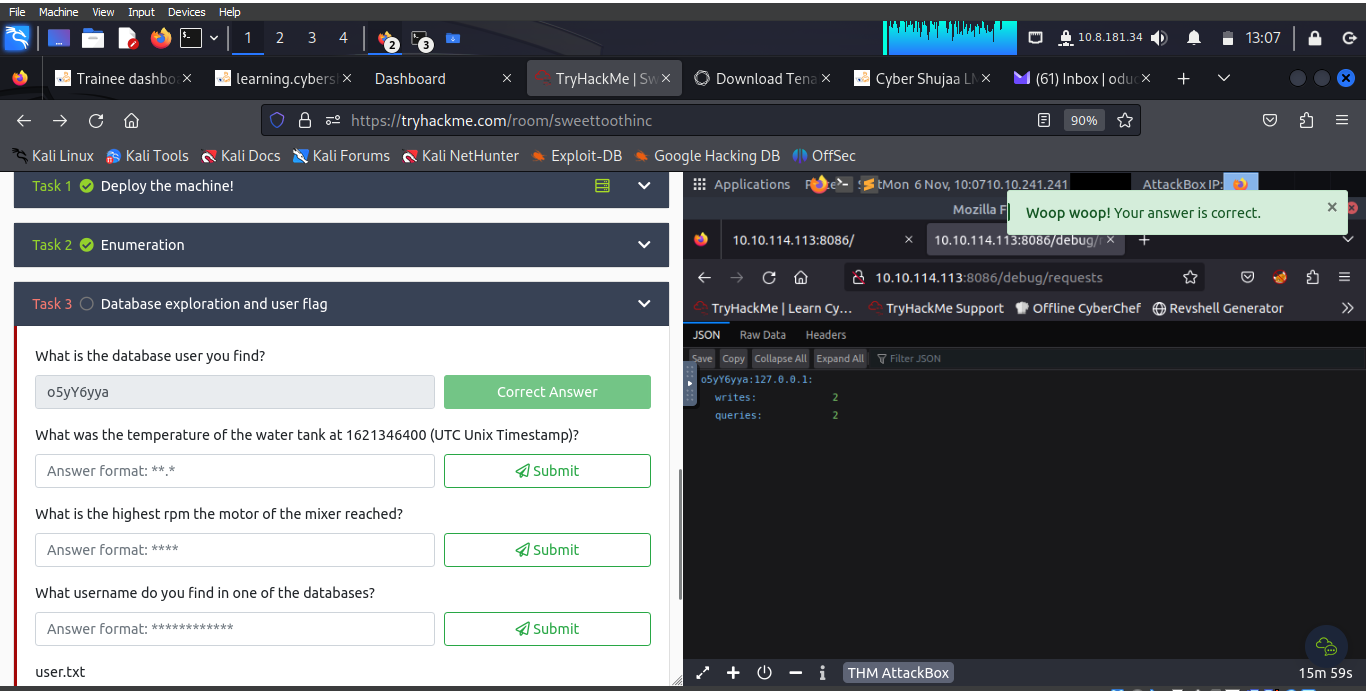
In this activity the learner used rustscan to scan the TCP port and got the following:



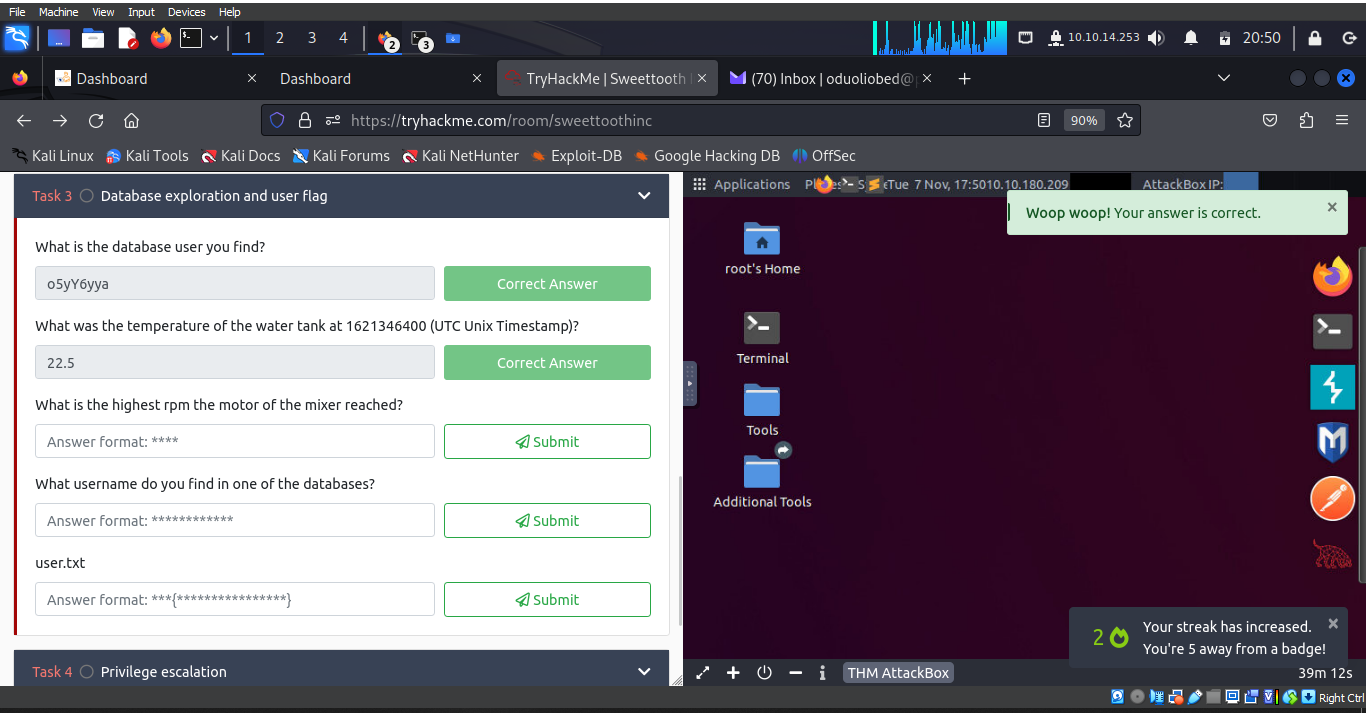
The syntax for the scan is: ***rustscan –a ‘machine-ip’ -- -sC –sV***

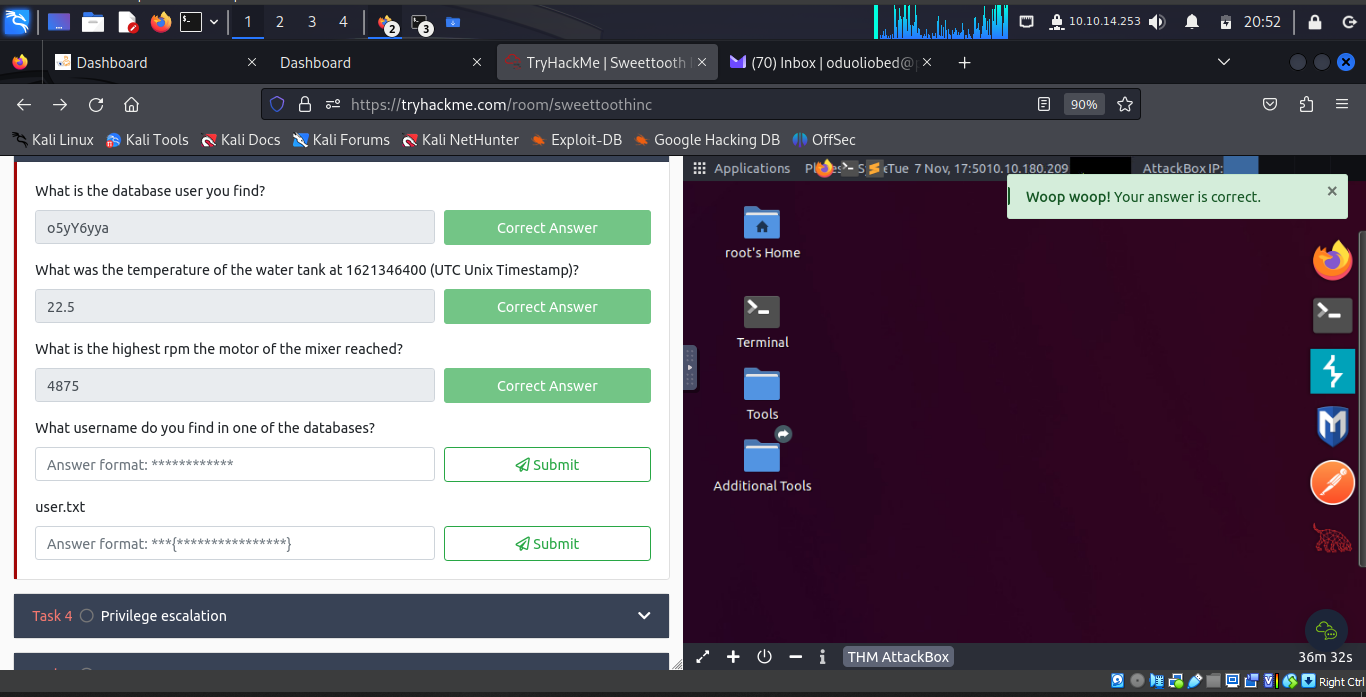
***Task 3: Database exploration and user flag***

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

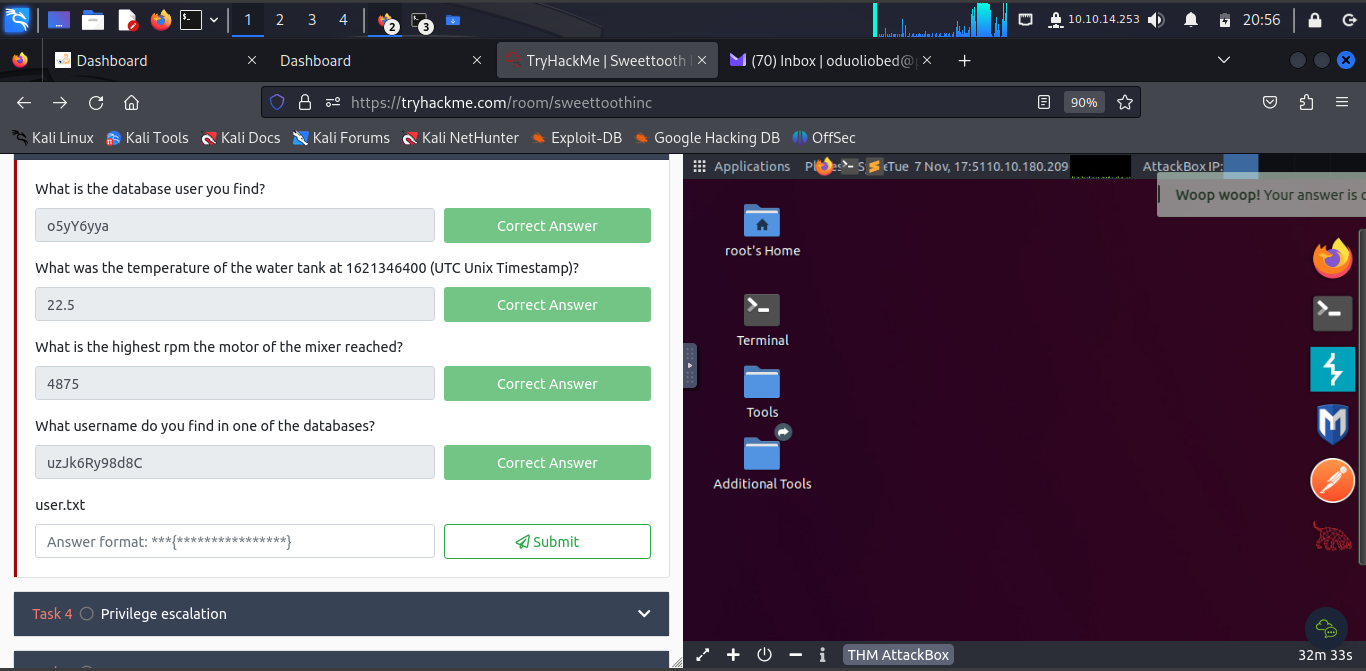


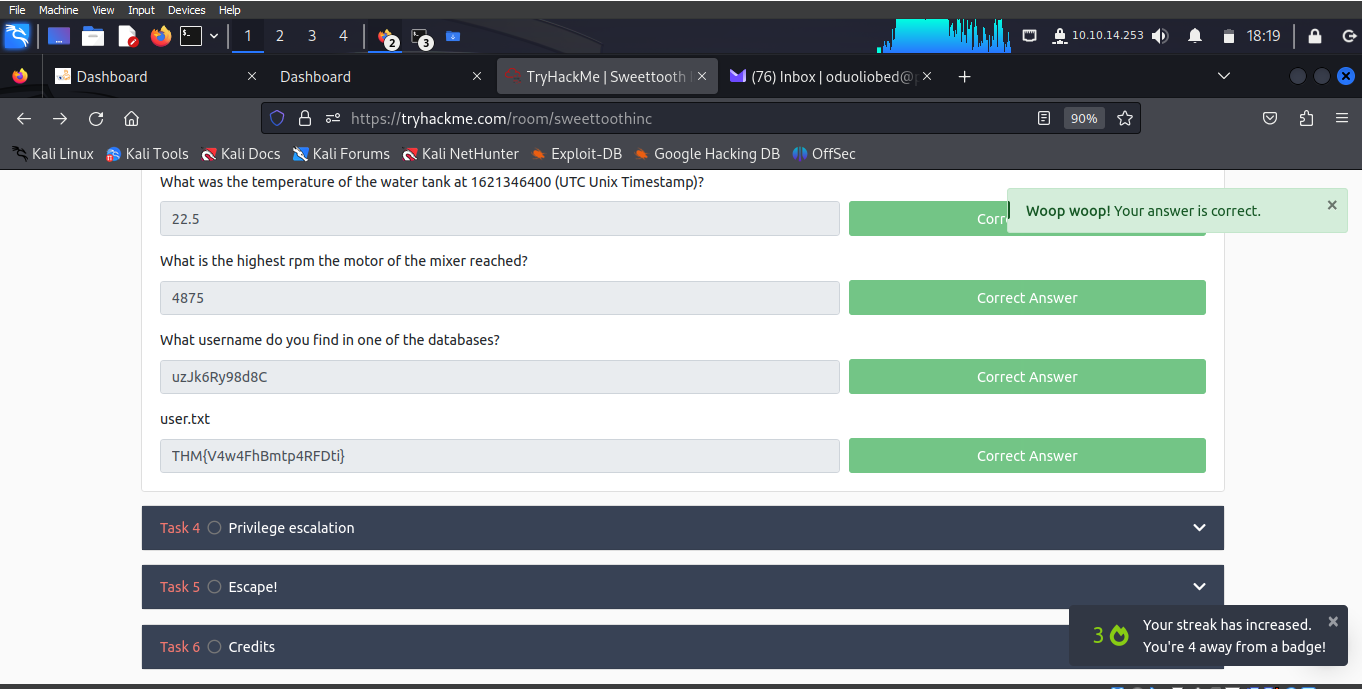
This happened after successfully running: ***https://10.10.114.113:8086/debug/requests***



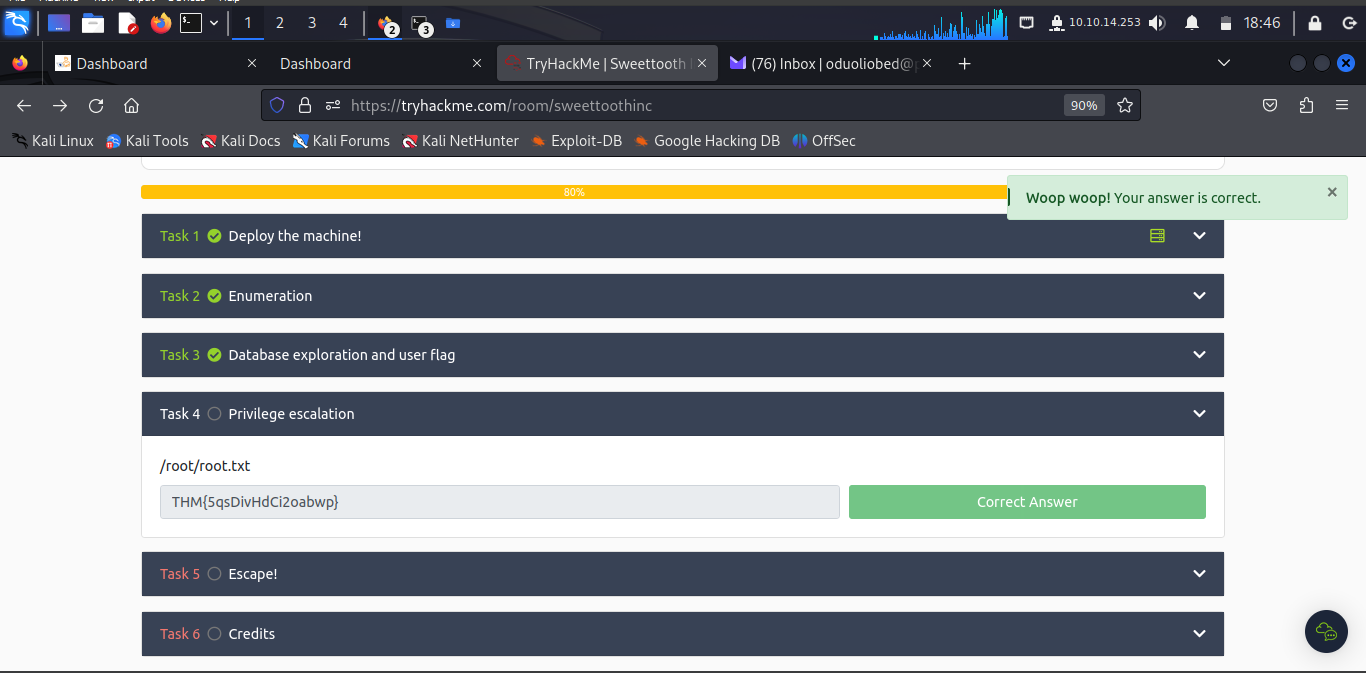


The database username at “***https://10.10.114.113:8086/debug /vars”.***



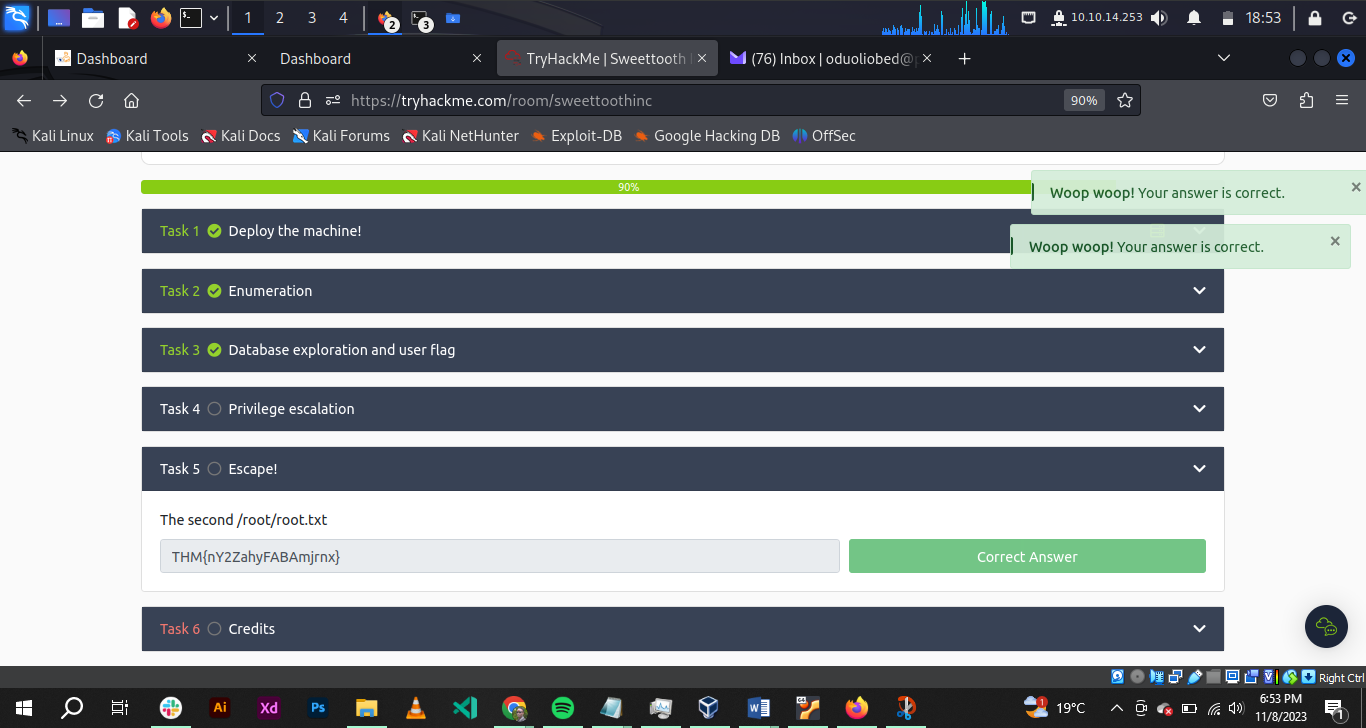


***Task 4: Privilege escalation***

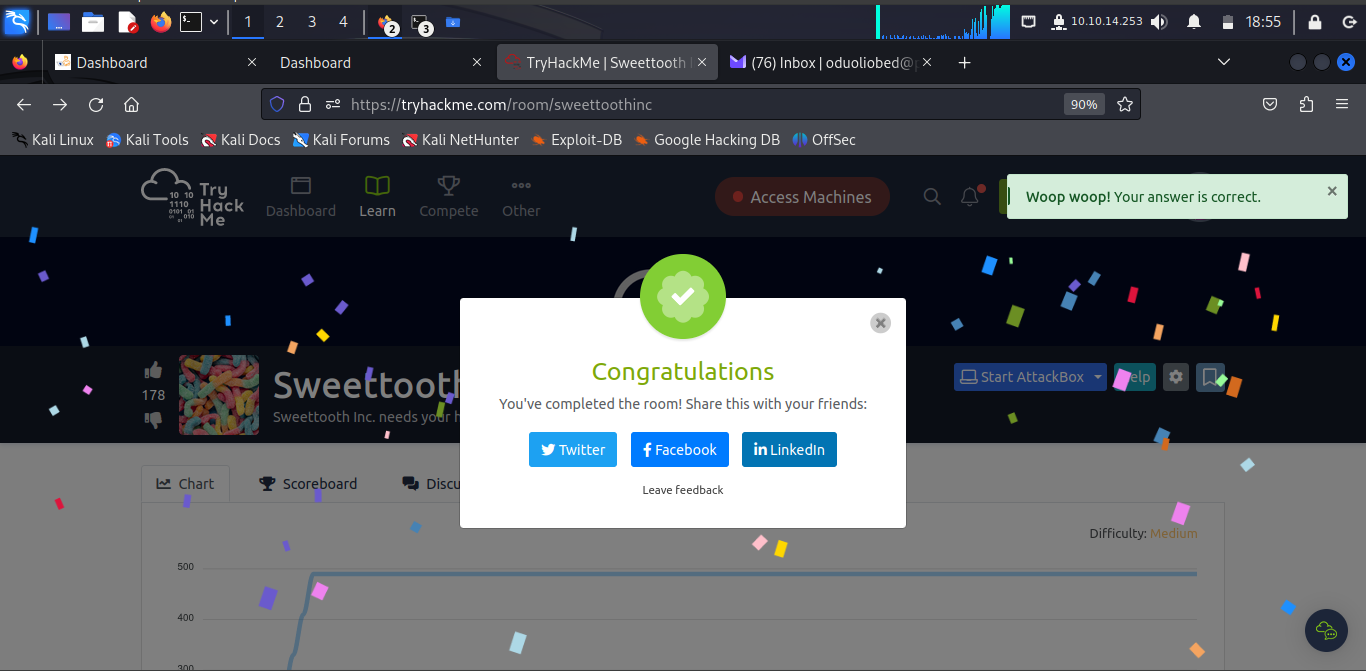


***Task 5: Escape!***

The learner run..



***Task 6: Credits***



**Conclusion**

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