

# 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.

The screenshot displays the tryhackme.com interface for the 'sweettoothinc' room. At the top, a red header bar contains the text 'Active Machine Information'. Below this, a table lists machine details: Title 'sweettoothincv03', IP Address 'Shown in 39s', and Expires '59m 39s'. To the right of the table are buttons for '?', 'Add 1 hour', and 'Terminate'. A progress bar shows '0%'. Below the progress bar, a task card for 'Task 1: Deploy the machine!' is visible. It includes a 'Start Machine' button and instructions: 'Answer the questions below' and 'Start the machine and wait 5 minutes for it to startup.' A text input field contains 'No answer needed', and a 'Completed' button is present. Below Task 1, Task 2 'Enumeration' and Task 3 'Database exploration and user flag' are listed. The bottom of the screen shows a Windows taskbar with various application icons and a system tray displaying '17°C' and '11:37 AM 11/6/2023'.

## Task 2: Enumeration

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

The screenshot displays the TryHackMe interface for Task 2: Enumeration. The 'Active Machine Information' section shows the machine 'sweettoothincv03' with IP 10.10.114.113. The task instructions ask for the name of the database software running on one of the ports. The user has entered 'InfluxDB' and the system has marked it as the 'Correct Answer'. A terminal window on the right shows the output of a rustscan command, confirming the discovery of an InfluxDB service on port 8086.

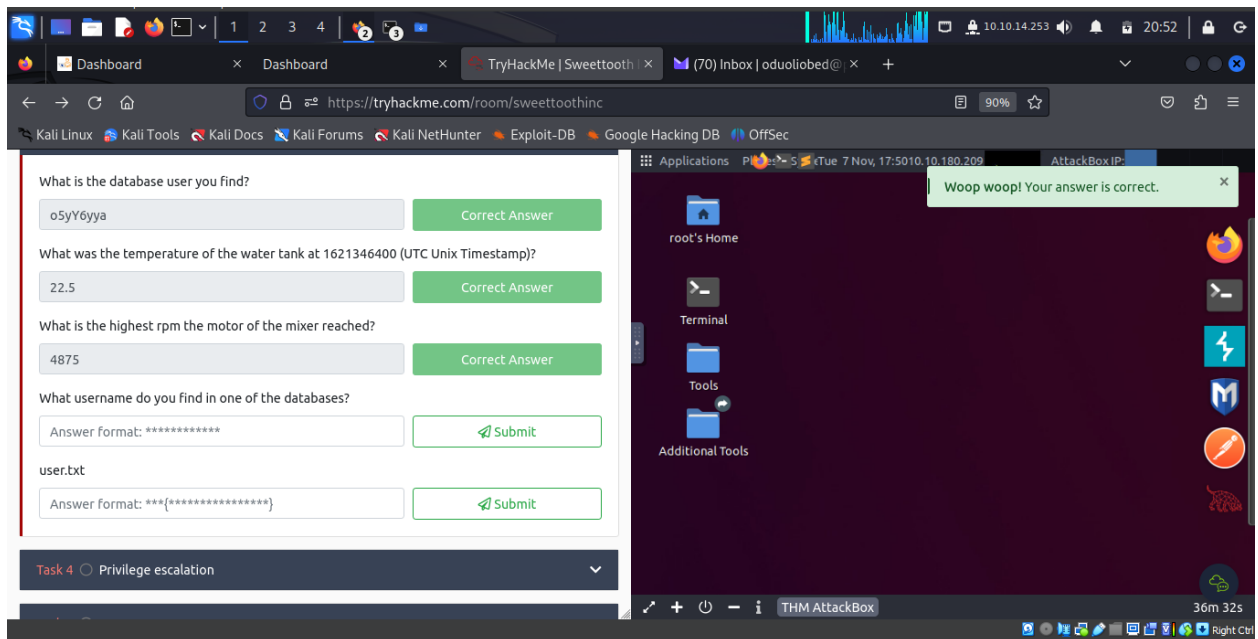
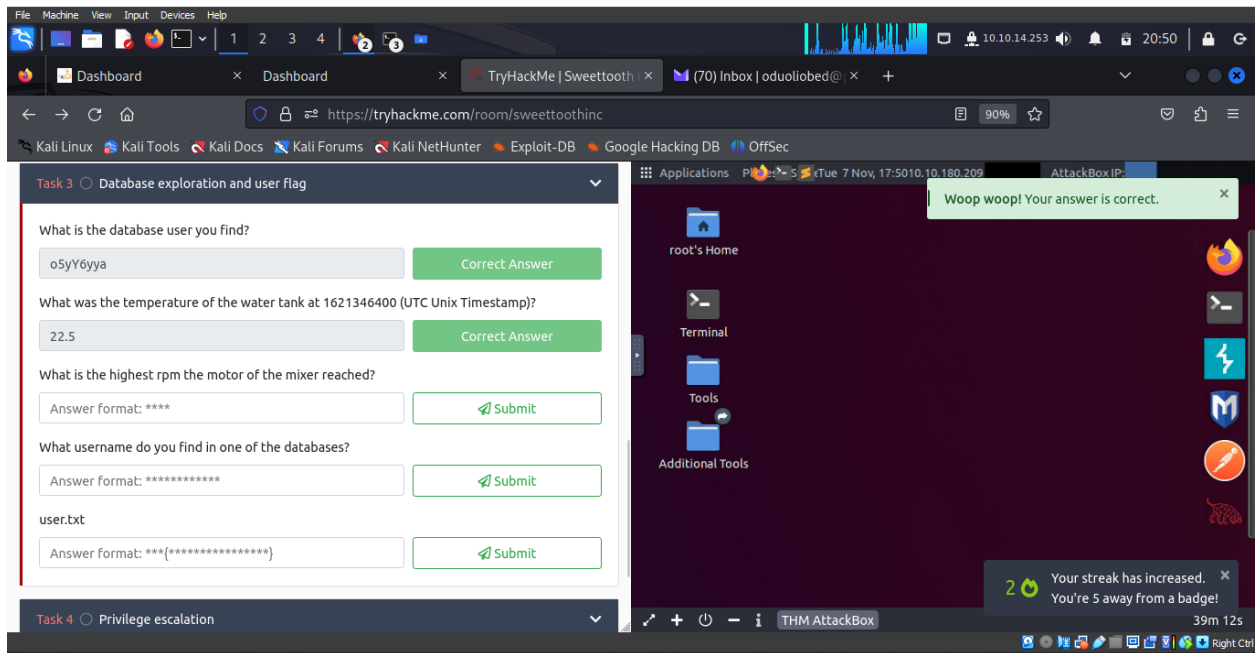
The syntax for the scan is: ***rustscan -a 'machine-ip' -- -sC -sV***

## Task 3: Database exploration and user flag

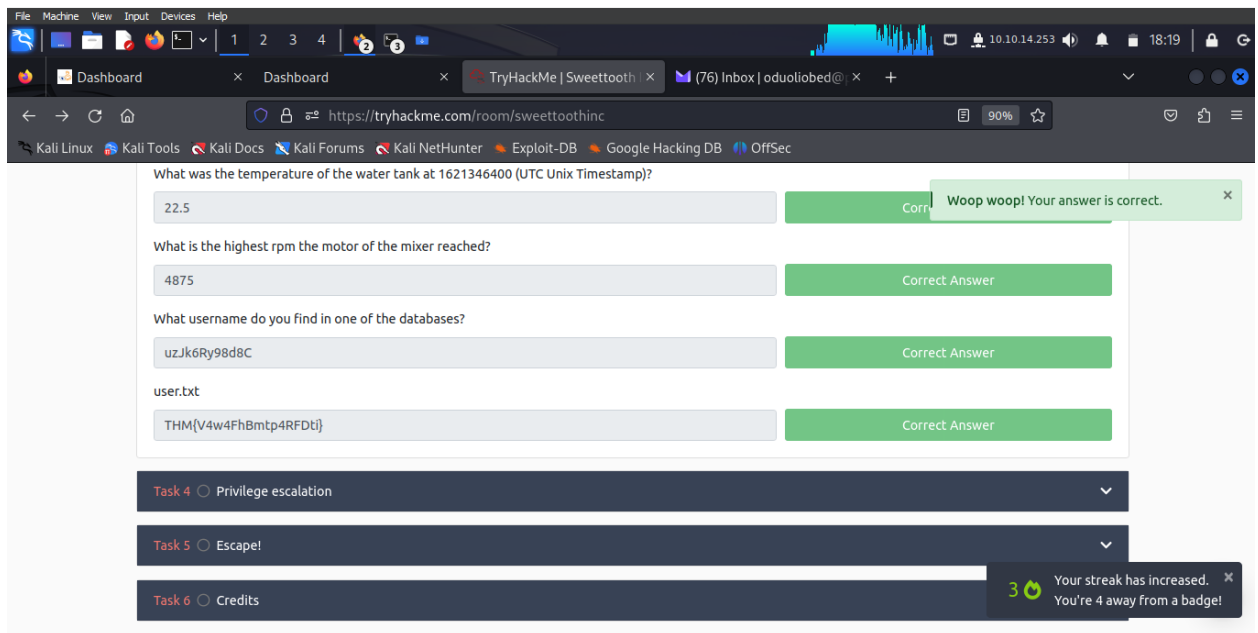
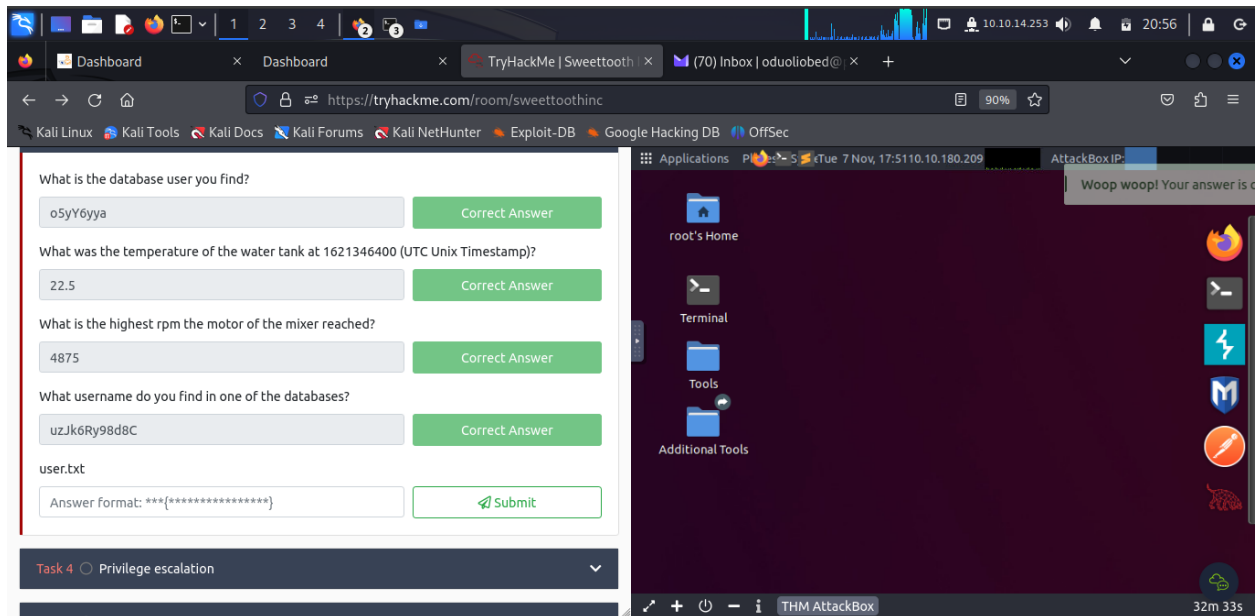
The learner found the database user as: ***o5yY6yya***

The screenshot displays the TryHackMe interface for Task 3: Database exploration and user flag. The task instructions ask for the database user found. The user has entered 'o5yY6yya' and the system has marked it as the 'Correct Answer'. The terminal window on the right shows the output of a curl command to the InfluxDB debug endpoint, displaying a JSON response with the user '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

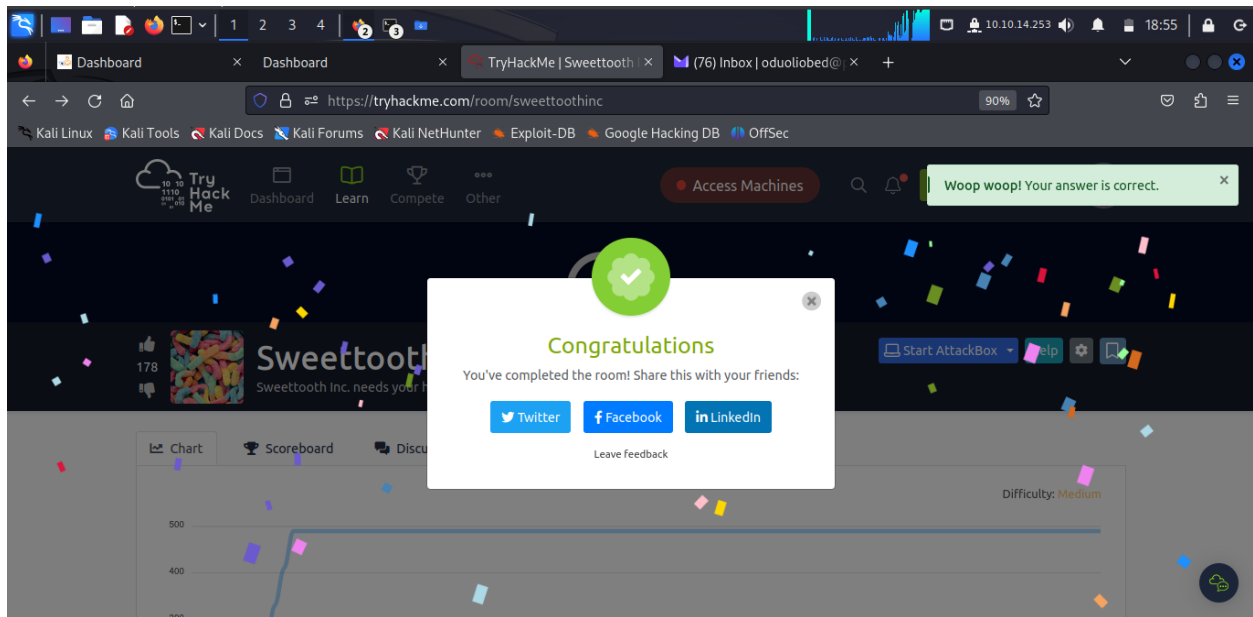
The screenshot shows the TryHackMe Sweettooth room interface. At the top, a progress bar indicates 80% completion. A green notification box says "Woop woop! Your answer is correct." Below this, a list of tasks is shown: Task 1 (Deploy the machine!), Task 2 (Enumeration), Task 3 (Database exploration and user flag), Task 4 (Privilege escalation), Task 5 (Escape!), and Task 6 (Credits). Task 4 is currently selected. The task description for Task 4 is "/root/root.txt". The answer input field contains "THM{5qsDivHdCi2oabwp}" and a green "Correct Answer" button is visible.

## Task 5: Escape!

The learner run..

The screenshot shows the TryHackMe Sweettooth room interface. At the top, a progress bar indicates 90% completion. Two green notification boxes say "Woop woop! Your answer is correct." Below this, a list of tasks is shown: Task 1 (Deploy the machine!), Task 2 (Enumeration), Task 3 (Database exploration and user flag), Task 4 (Privilege escalation), Task 5 (Escape!), and Task 6 (Credits). Task 5 is currently selected. The task description for Task 5 is "The second /root/root.txt". The answer input field contains "THM{nY2ZahyFABAmjrnxi}" and a green "Correct Answer" button is visible. The Windows taskbar is visible at the bottom of the screen.

## Task 6: Credits



## Conclusion

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