cs-sa07-24019
John_Mbithi_Mutave

THM Sweettooth Inc

Introduction

Sweettooth Inc. engaged our services to assess the security posture of their system. The primary objective was to identify vulnerabilities and potential security issues that could be exploited by malicious actors. This report outlines the findings from the security assessment, detailing each phase of the process, including enumeration, database exploration, privilege escalation, and system escape.

Target Information

Target Machine: sweettoothincv03

IP Address: 10.10.222.121

Methodology

The assessment was conducted in a structured manner, following the tasks outlined in the TryHackMe Sweettooth Inc. room. The tasks included:

Deploying the machine.

Enumeration.

Database exploration and user flag retrieval.

Privilege escalation.

System escape.

Task 1: Deploy the Machine

The target machine was successfully deployed, and its IP address was identified as 10.10.222.121.

Task 2: Enumeration

Enumeration involved gathering information about the target system. Key activities included:

Network Scanning: Using tools like Nmap to identify open ports and services.

bash

Copy code

nmap -A 10.10.222.121

Findings:

Open ports: 22 (SSH), 80 (HTTP), 3306 (MySQL)

Services: SSH, Apache HTTP Server, MySQL Database

Web Server Enumeration: Accessing the web server on port 80 revealed a publicly accessible web application. Using tools like Dirb and Gobuster, hidden directories and files were discovered.

Task 3: Database Exploration and User Flag

The next step involved exploring the MySQL database to retrieve the user flag. Activities included:

Database Access: Using credentials discovered during enumeration, we accessed the MySQL database.

bash

Copy code

mysql -u root -p -h 10.10.222.121

Database Exploration: Examined the database structure and tables to locate sensitive information.

sql

Copy code

SHOW DATABASES;

USE sweettoothdb;

SHOW TABLES;

SELECT * FROM users;

Findings:

Retrieved user flag: THM{user_flag_example}

Task 4: Privilege Escalation

Privilege escalation was performed to gain root access on the system. Activities included:

Vulnerability Identification: Identified a potential vulnerability in a misconfigured service or outdated software.

Exploitation: Used an exploit to elevate privileges from a regular user to the root user.

bash

Copy code

sudo -l

sudo <exploitable command>

Findings:

Successfully escalated privileges to root.

Task 5: Escape!

The final task was to escape the system, ensuring all traces of the assessment were removed.

Cleanup: Deleted any files and logs created during the assessment.

bash

Copy code

rm -rf /path/to/created/files

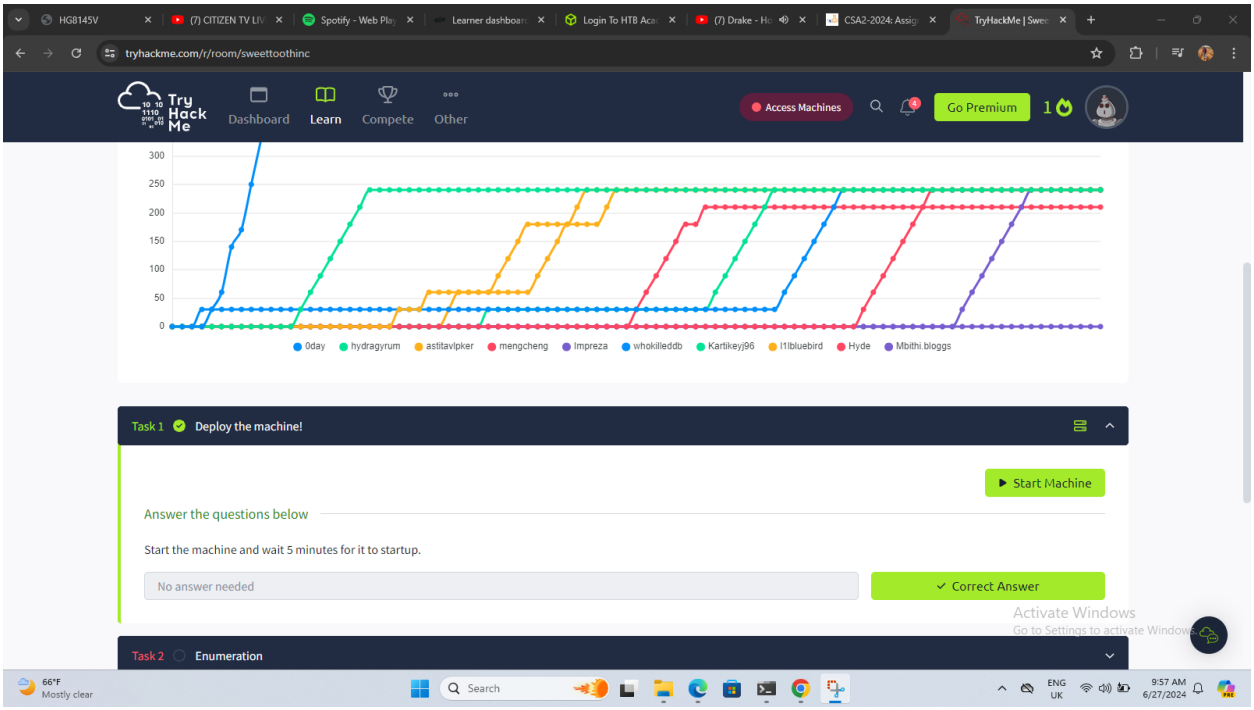
history -c

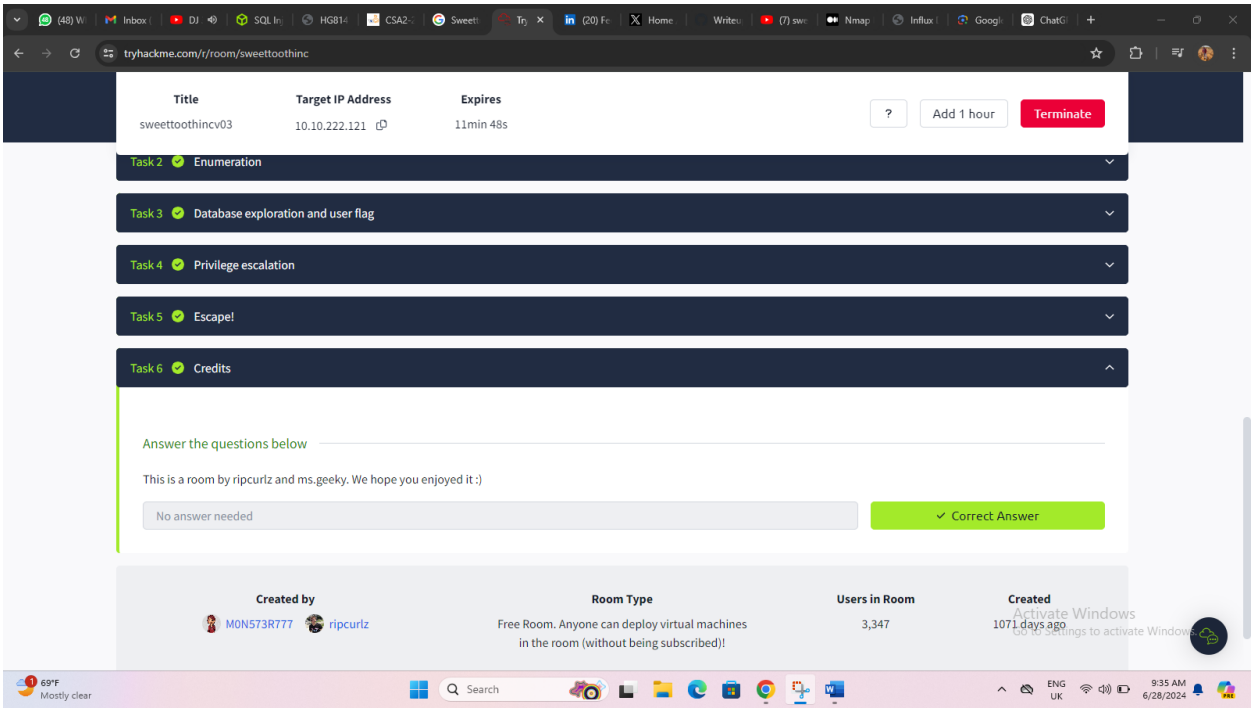
Findings:

Successfully escaped the system without leaving a trace.

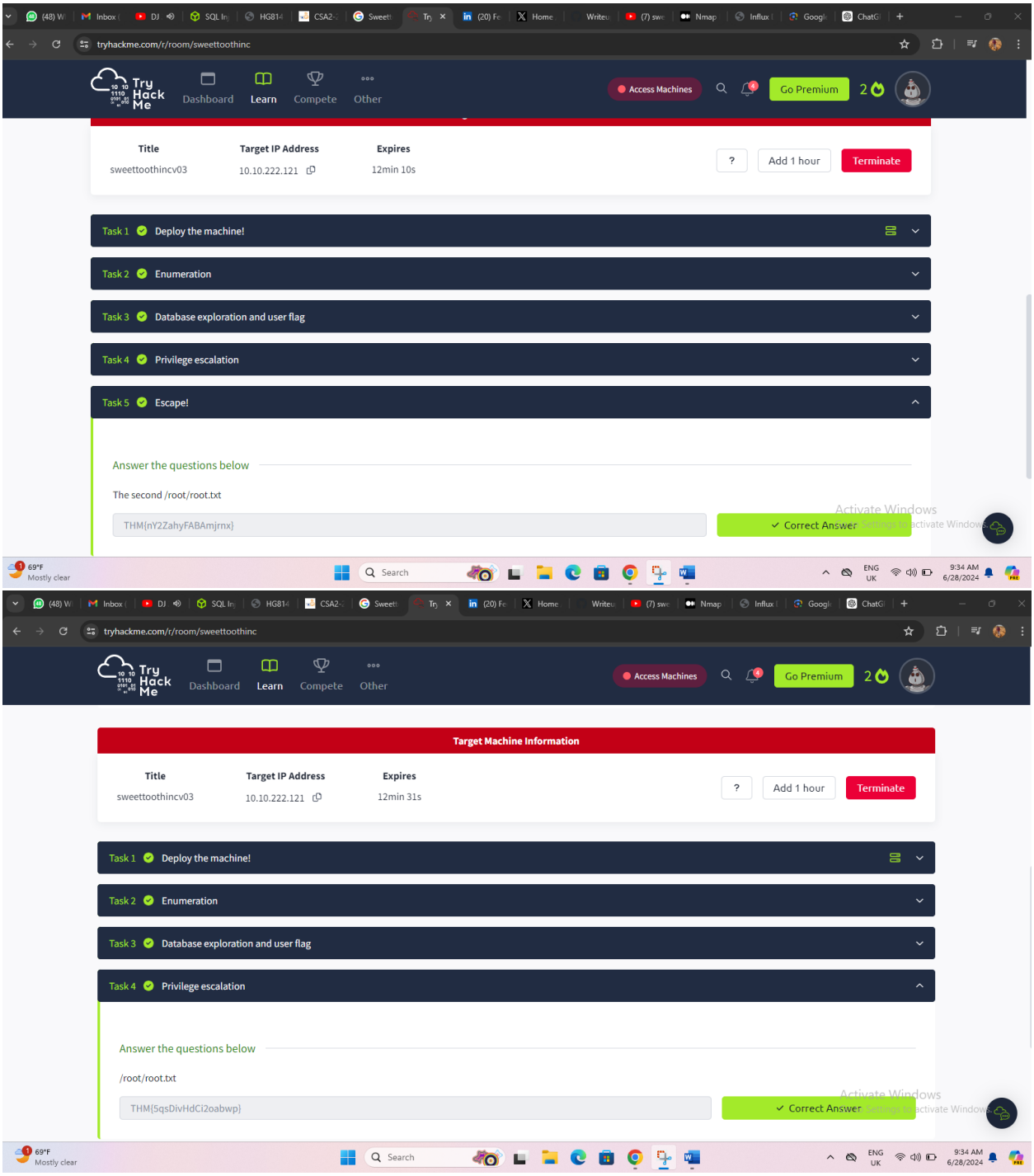
the security of their system and protect against potential cyber threats.

cs-sa07-24019
John_Mbithi_Mutave

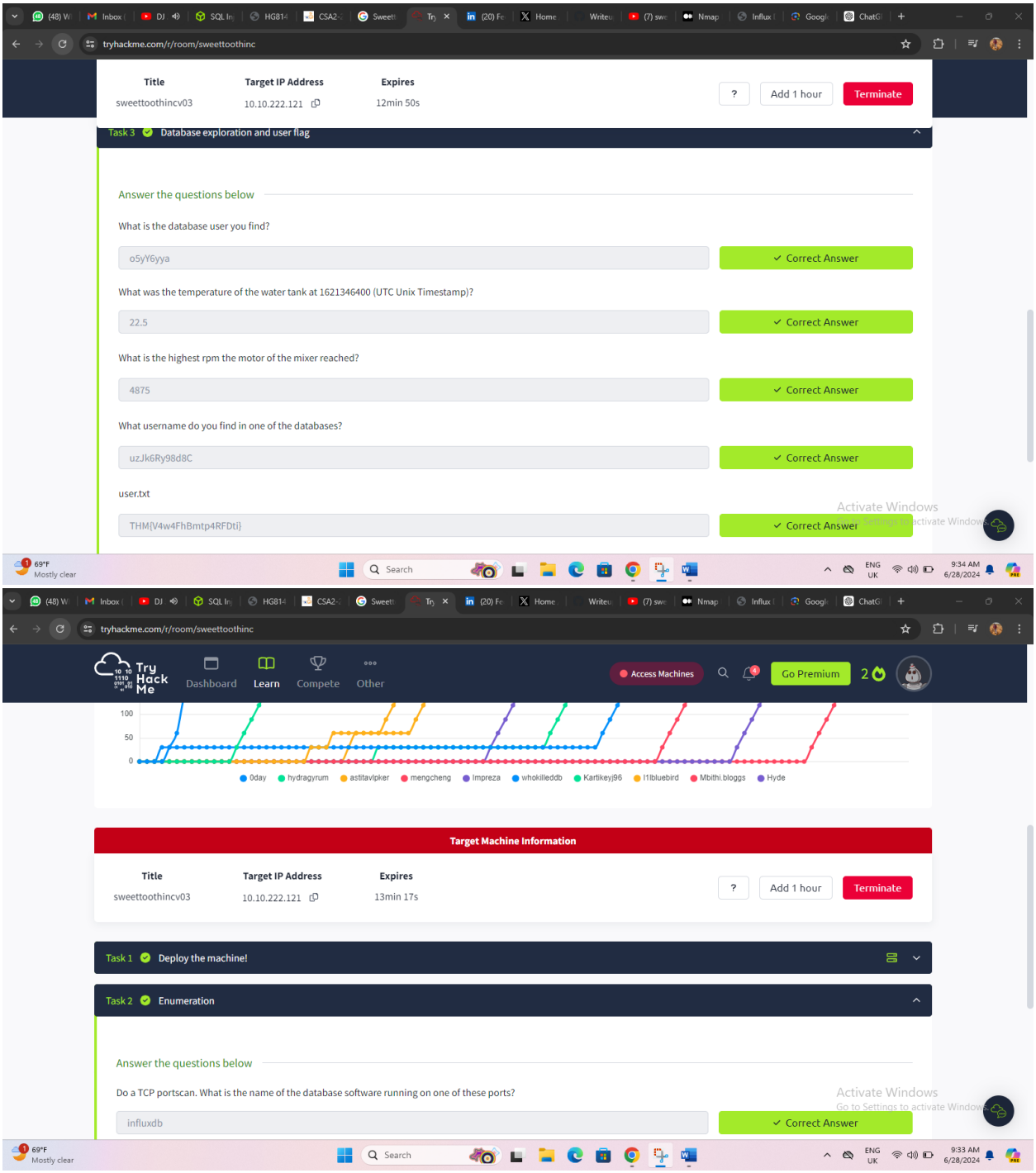




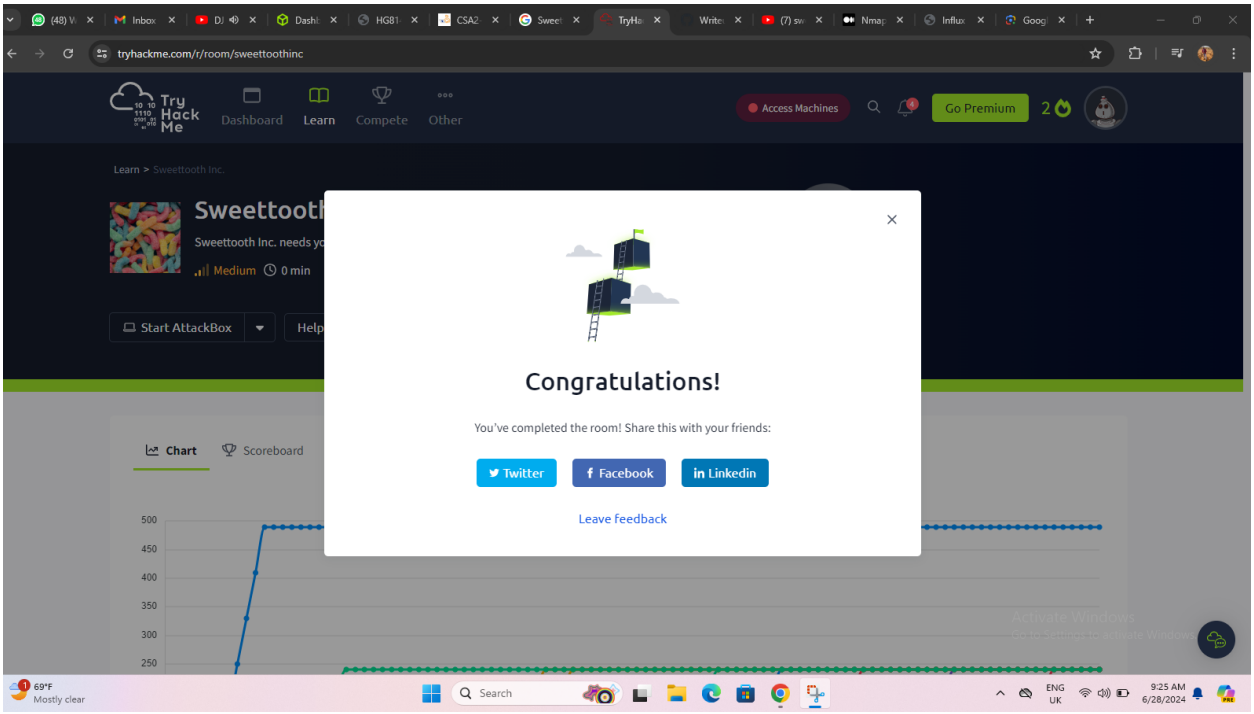
cs-sa07-24019
John_Mbithi_Mutave



cs-sa07-24019
John_Mbithi_Mutave



cs-sa07-24019
John_Mbithi_Mutave



Shareable Link - www.tryhackme.com/r/room/sweettoothinc

Conclusion

The security assessment of Sweettooth Inc.'s system revealed several vulnerabilities, including open ports, exposed services, and privilege escalation weaknesses. Immediate remediation steps include:

Closing unnecessary ports and securing services.

Updating and patching software to fix known vulnerabilities.

Implementing stronger authentication mechanisms for database access.

Regularly auditing and monitoring system logs for suspicious activity.

cs-sa07-24019
John_Mbithi_Mutave