



**Exploitation and Post-Exploitation**

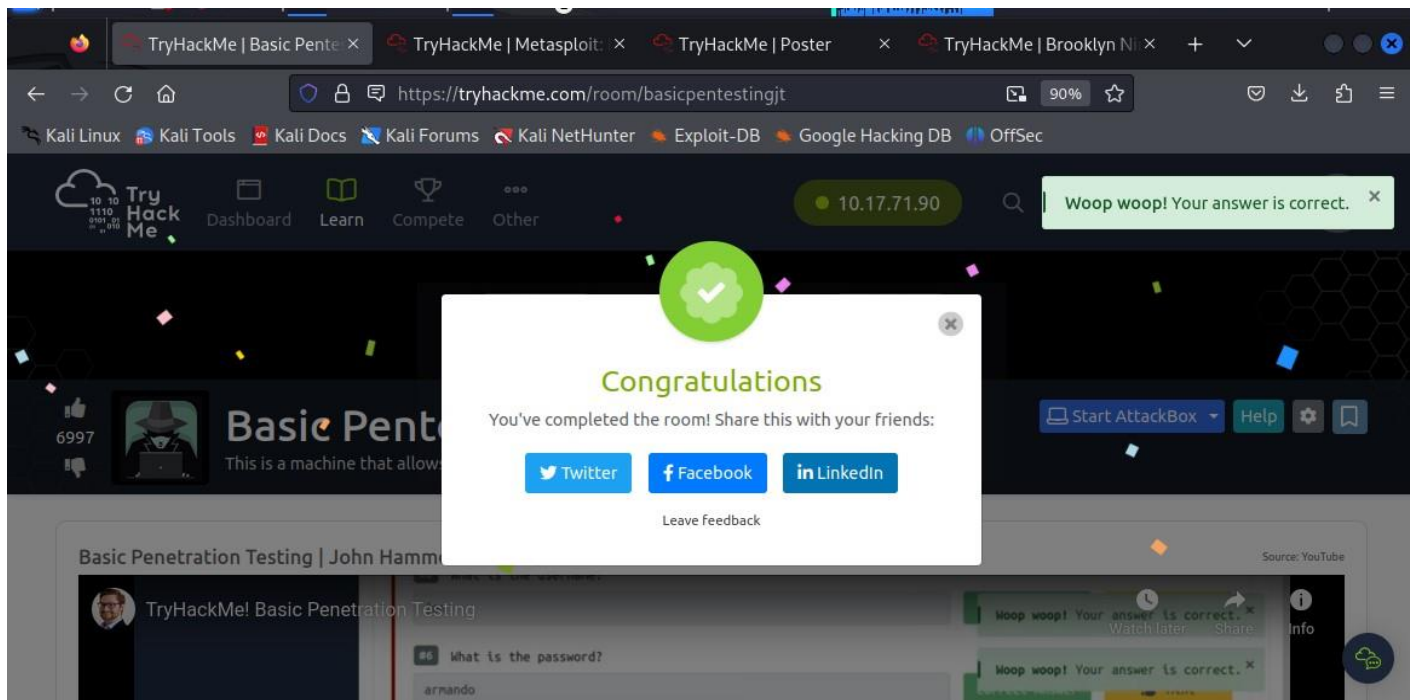
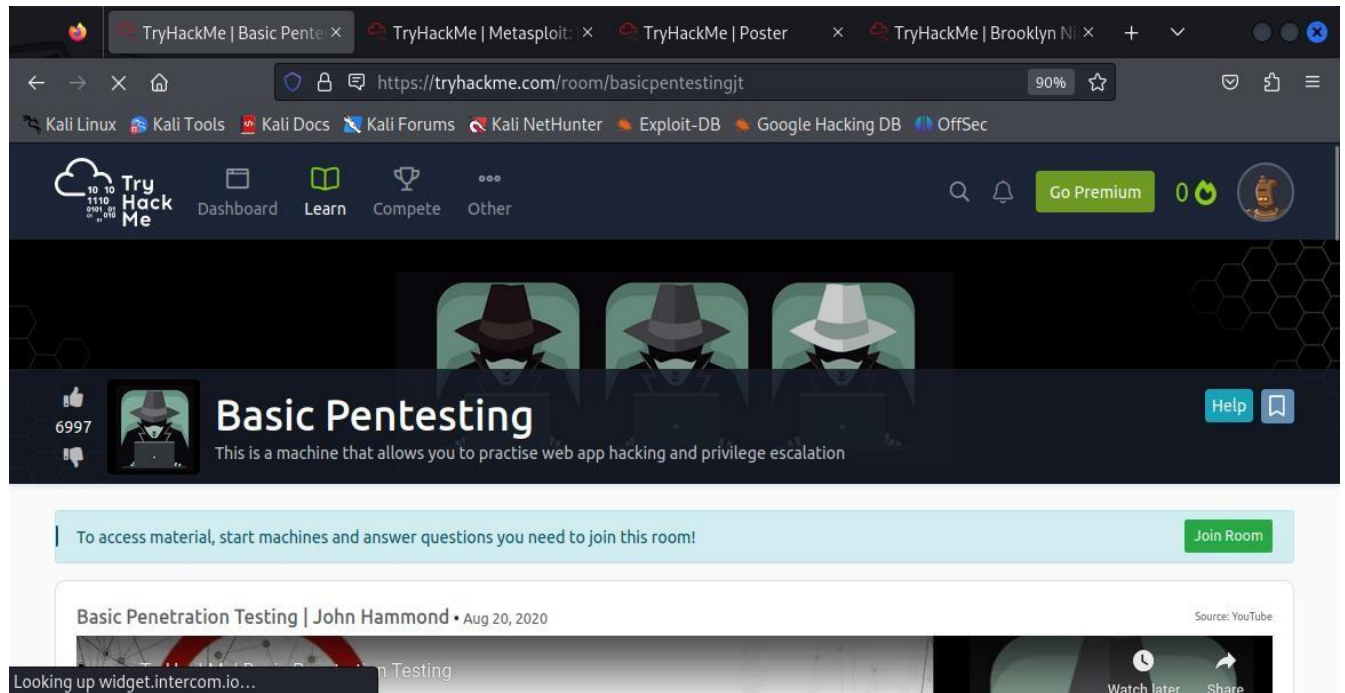
**Date: - 30/09/2023**

**Name: - Onkar vikas mhaskar**

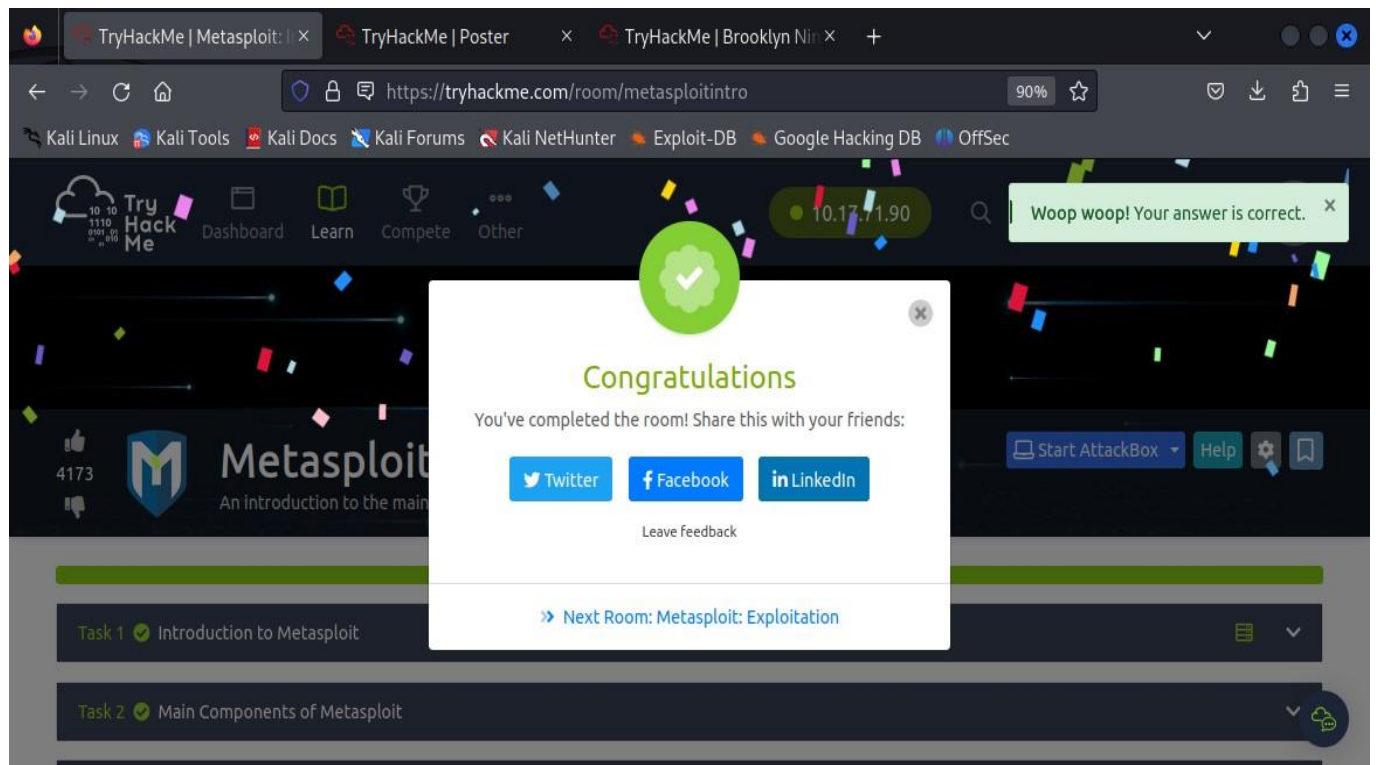
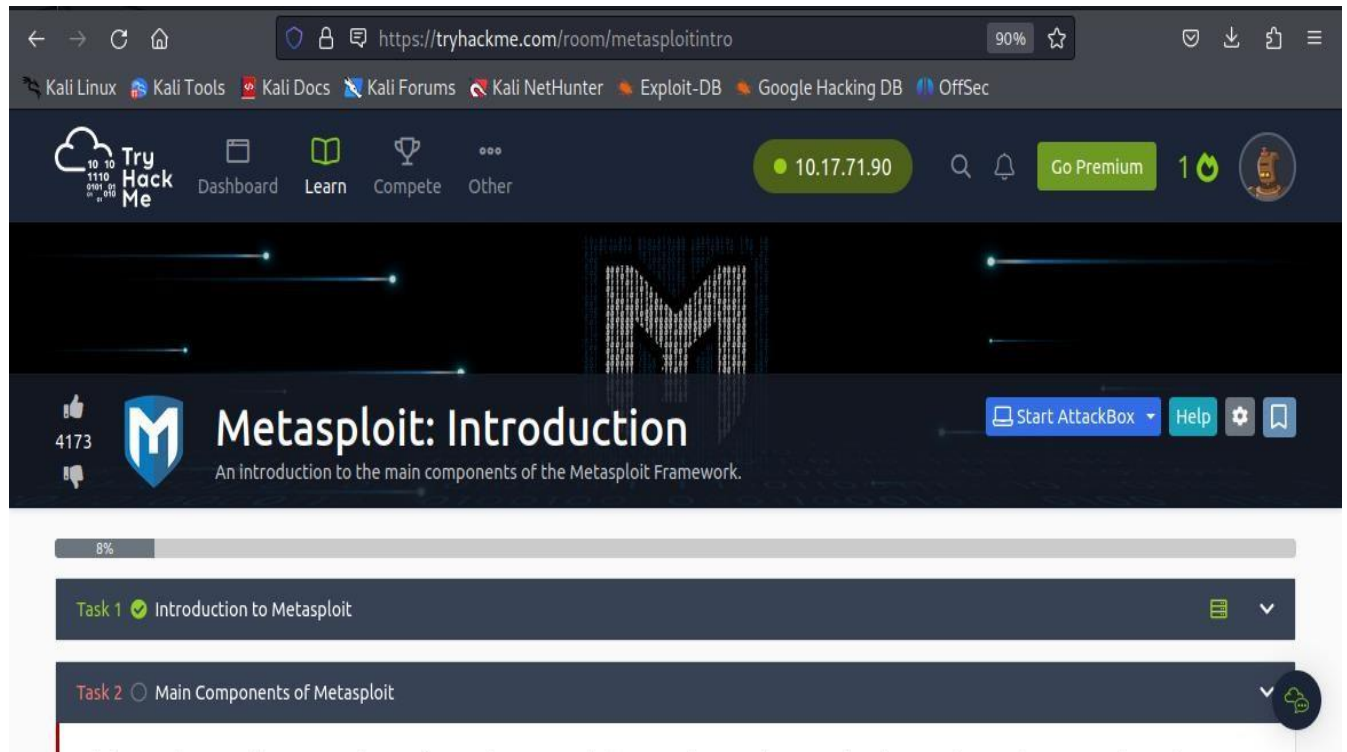
**Role: - Penetration testing Intern**

**Intern ID: - HPTI-SEP23-168**

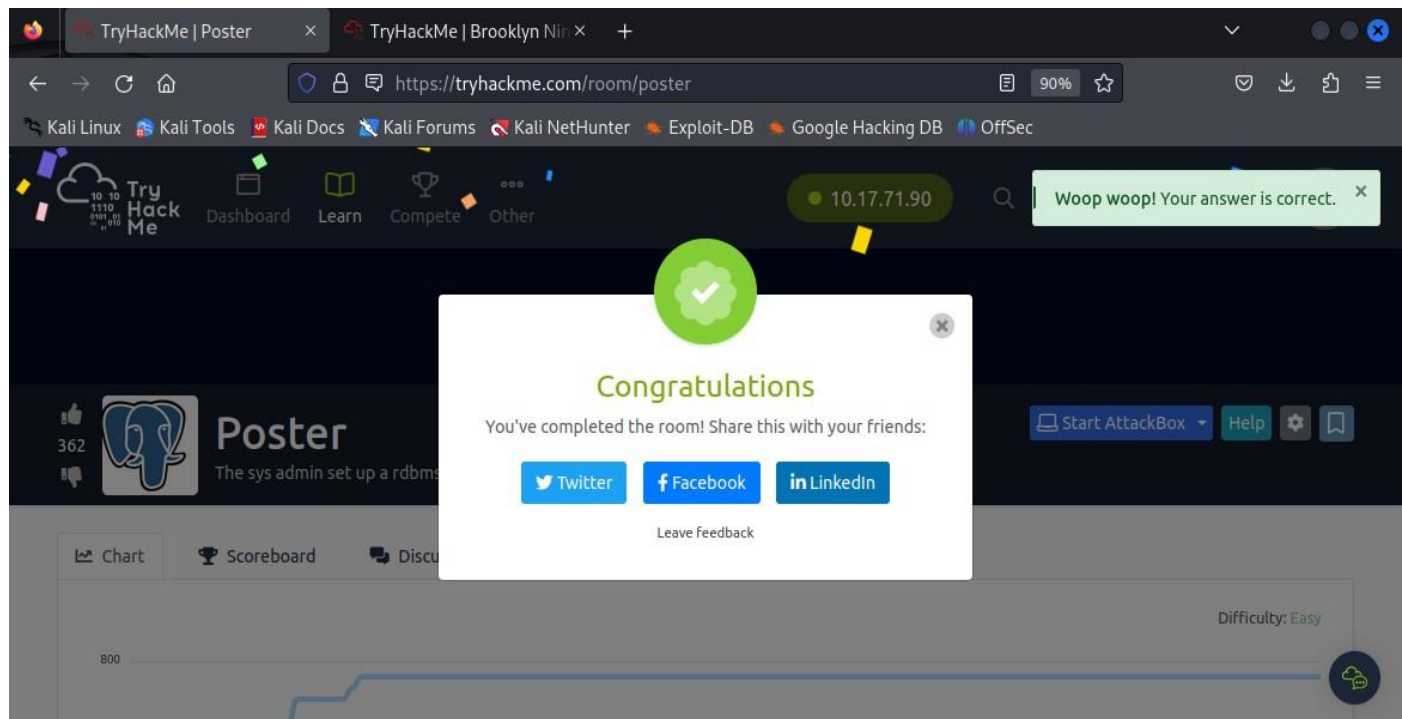
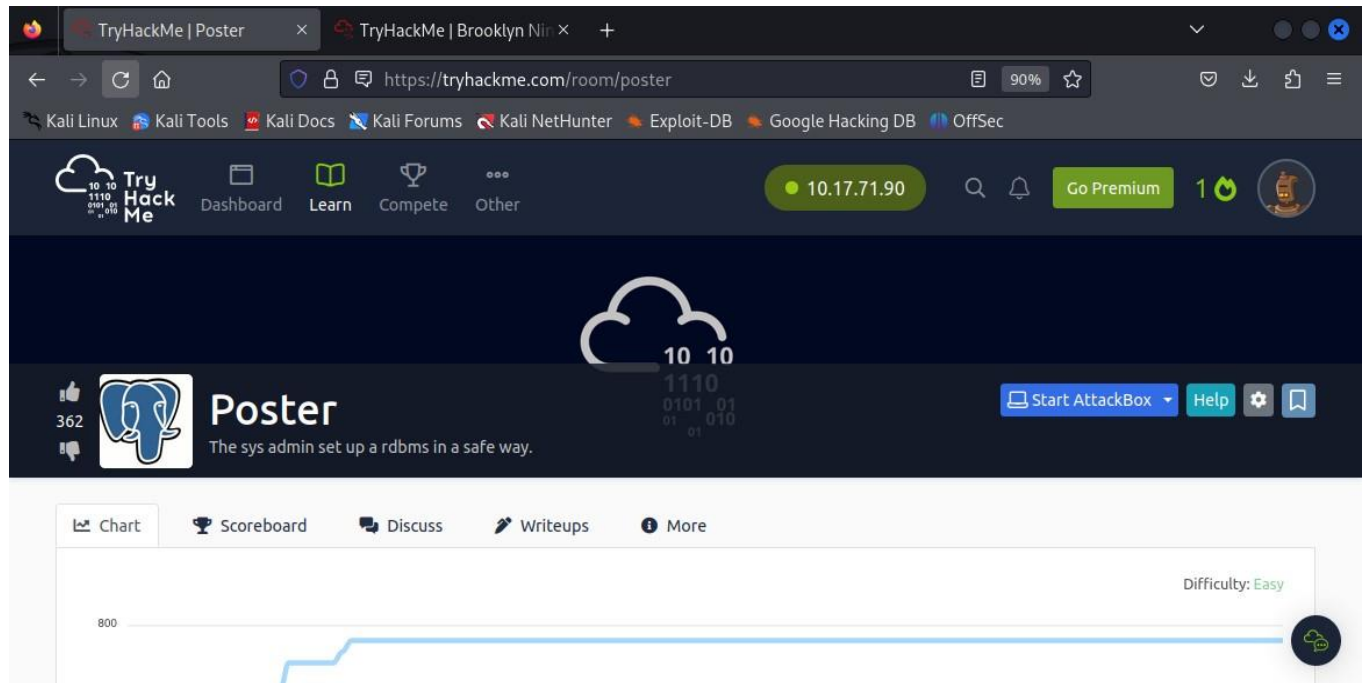
## Room1: - Basic Pentesting



## Room2: - Metasploit: Introduction



### Room3: - Poster



## Room4: - Brooklyn Nine Nine

The screenshot shows the TryHackMe interface for the 'Brooklyn Nine Nine' room. The browser address bar displays 'https://tryhackme.com/room/brooklynnine'. The top navigation bar includes links to 'Dashboard', 'Learn', 'Compete', and 'Other', along with a user profile icon and a 'Go Premium' button. The room title 'Brooklyn Nine Nine' is prominently displayed, accompanied by a 'Start AttackBox' button and a 'Help' button. Below the title, a description states: 'This room is aimed for beginner level hackers but anyone can try to hack this box. There are two main intended ways to root the box.' The main content area features a 'Chart' tab, a 'Scoreboard' tab, and a 'Discuss' tab. A progress bar is visible, indicating the user's progress through the room. The difficulty level is marked as 'Easy'.

This screenshot shows the same TryHackMe room page, but with a completion notification overlay. A green checkmark icon is displayed above the word 'Congratulations'. The notification text reads: 'You've completed the room! Share this with your friends:'. Below this text are three buttons for social media sharing: 'Twitter', 'Facebook', and 'LinkedIn'. A 'Leave feedback' link is also present. The background of the page remains the same, showing the room title and description.



## Room5: - Intro PoC Scripting

The screenshot shows the TryHackMe interface for the 'Intro PoC Scripting' room. The browser address bar displays `https://tryhackme.com/room/intropocscripting`. The navigation bar includes links to 'Dashboard', 'Learn', 'Compete', and 'Other', along with a user profile icon and a 'Go Premium' button. The room title 'Intro PoC Scripting' is prominently displayed, accompanied by a cloud icon and the IP address '10.17.71.90'. Below the title, a description reads: 'Learn the importance and beginner skills of crafting custom proof of concept (PoC) exploit scripts from many different sources.' A 'Start AttackBox' button is visible. The task list shows 'Task 1 Introduction - What are PoC scripts?' with a 'Greetings!' message and a 'Start Machine' button. A progress bar at the top indicates 0% completion.

This screenshot shows the same TryHackMe room page after completion. A green notification bubble at the top right states 'Woop woop! Your answer is correct.' A large 'Congratulations' modal is centered on the screen, featuring a green checkmark icon and the text: 'You've completed the room! Share this with your friends:'. Below this, there are buttons for 'Twitter', 'Facebook', and 'LinkedIn', along with a 'Leave Feedback' link. The task list now shows 'Task 1 Introduction - What are PoC scripts?' and 'Task 2 Example - The starting point', both marked with green checkmarks. The progress bar at the bottom is now filled green, indicating 100% completion.

## Room6: - Linux PrivEsc Arena

The screenshot shows the TryHackMe interface for the 'Linux PrivEsc Arena' room. The browser address bar displays 'https://tryhackme.com/room/linuxprivescarena'. The room title 'Linux PrivEsc Arena' is prominently displayed with a rating of 922. Below the title, a description states: 'Students will learn how to escalate privileges using a very vulnerable Linux VM. SSH is open. Your credentials are TCM:Hacker123'. A progress bar at the top indicates 100% completion. The task section, titled 'Task 1 [Optional] Connecting to the TryHackMe network', provides instructions on how to connect to the network via OpenVPN or directly through SSH. The interface includes a navigation bar with links to 'Dashboard', 'Learn', 'Compete', and 'Other', along with a search bar and a 'Go Premium' button.

TryHackMe | Linux PrivEsc Arena

https://tryhackme.com/room/linuxprivescarena

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

TryHackMe Dashboard Learn Compete Other 10.17.71.90 Go Premium 1

### Linux PrivEsc Arena

922

Students will learn how to escalate privileges using a very vulnerable Linux VM. SSH is open. Your credentials are TCM:Hacker123

100%

Task 1 [Optional] Connecting to the TryHackMe network

You can either use the browser-based terminal (which appears when you deploy the machine), or you can connect to TryHackMe's network (via OpenVPN) and SSH in directly. If you've not done this before, first complete the [OpenVPN room](#) and learn how to connect.

## Room7: - Linux PrivEsc

The screenshot shows the TryHackMe interface for the 'Linux PrivEsc' room. The browser address bar displays 'https://tryhackme.com/room/linuxprivesc'. The room title 'Linux PrivEsc' is prominently displayed with a rating of 3567. Below the title, a description states: 'Practice your Linux Privilege Escalation skills on an intentionally misconfigured Debian VM with multiple ways to get root! SSH is available. Credentials: user:password321'. A progress bar at the top indicates 0% completion. The task section, titled 'Task 1 Deploy the Vulnerable Debian VM', provides instructions on how to deploy the machine. A 'Start Machine' button is visible. The interface includes a navigation bar with links to 'Dashboard', 'Learn', 'Compete', and 'Other', along with a search bar and a 'Go Premium' button.

TryHackMe | Linux PrivEsc

https://tryhackme.com/room/linuxprivesc

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

TryHackMe Dashboard Learn Compete Other 10.17.71.90 Go Premium 1

### Linux PrivEsc

3567

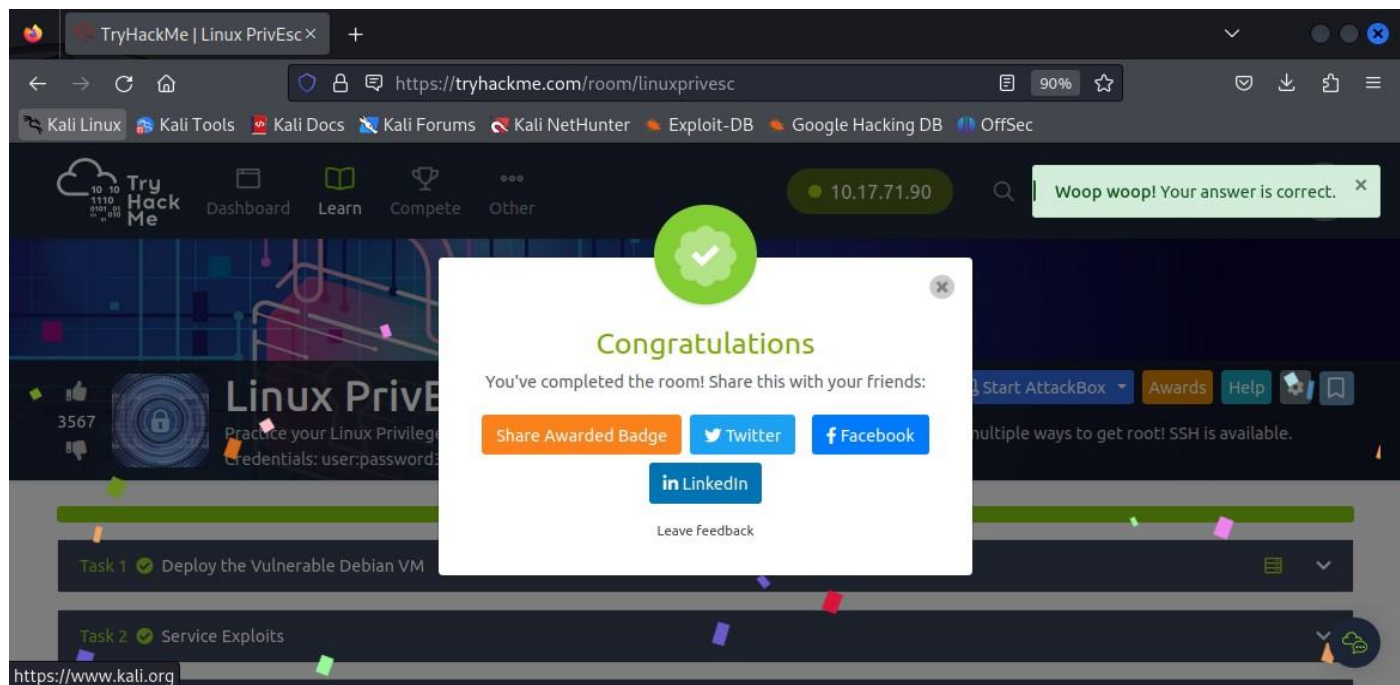
Practice your Linux Privilege Escalation skills on an intentionally misconfigured Debian VM with multiple ways to get root! SSH is available. Credentials: user:password321

0%

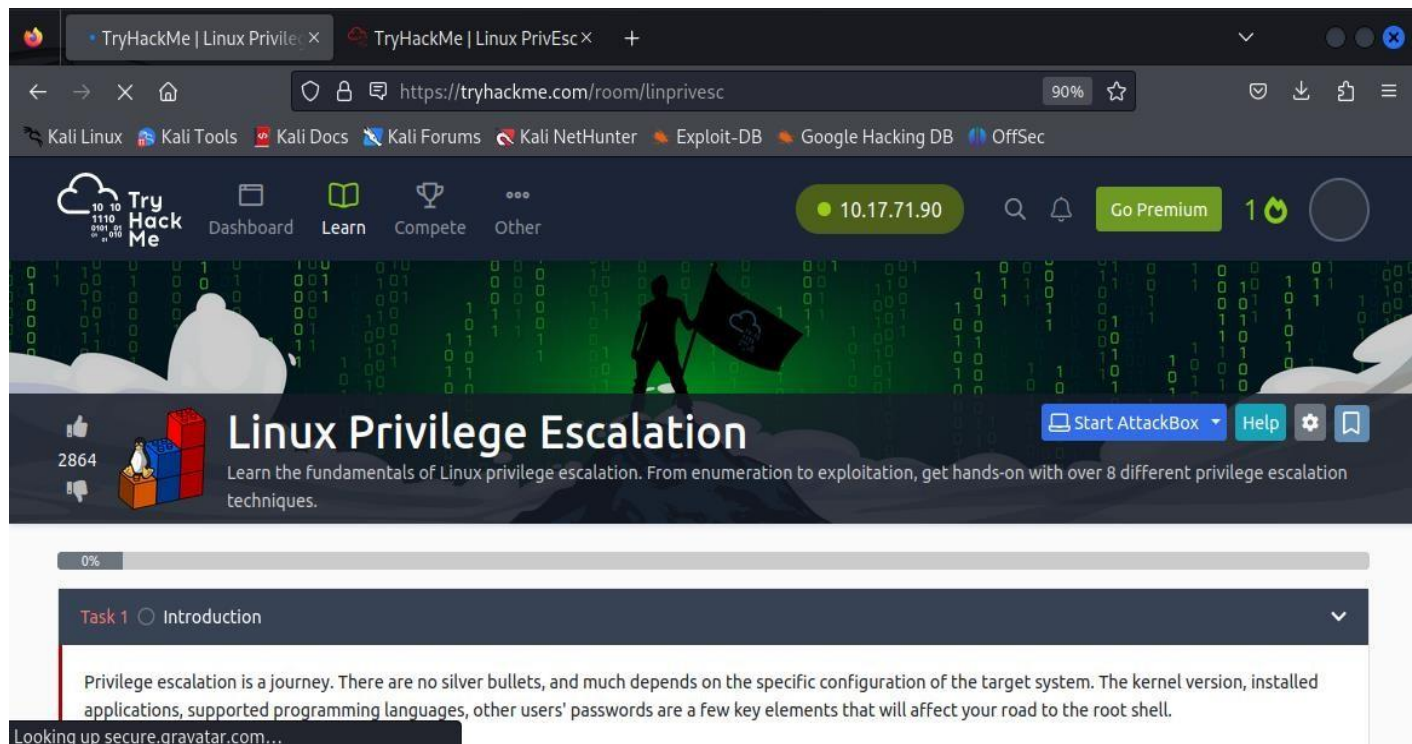
Task 1 Deploy the Vulnerable Debian VM

This room is aimed at walking you through a variety of [Linux Privilege Escalation](#) techniques. To do this, you must first deploy an intentionally vulnerable Debian VM. This VM was created by Sagi Shahar as part of his [local privilege escalation workshop](#) but has been updated by Tib3rius as part of his [Linux Privilege Escalation for OSCP and Beyond!](#) course on Udemy. Full explanations of the various

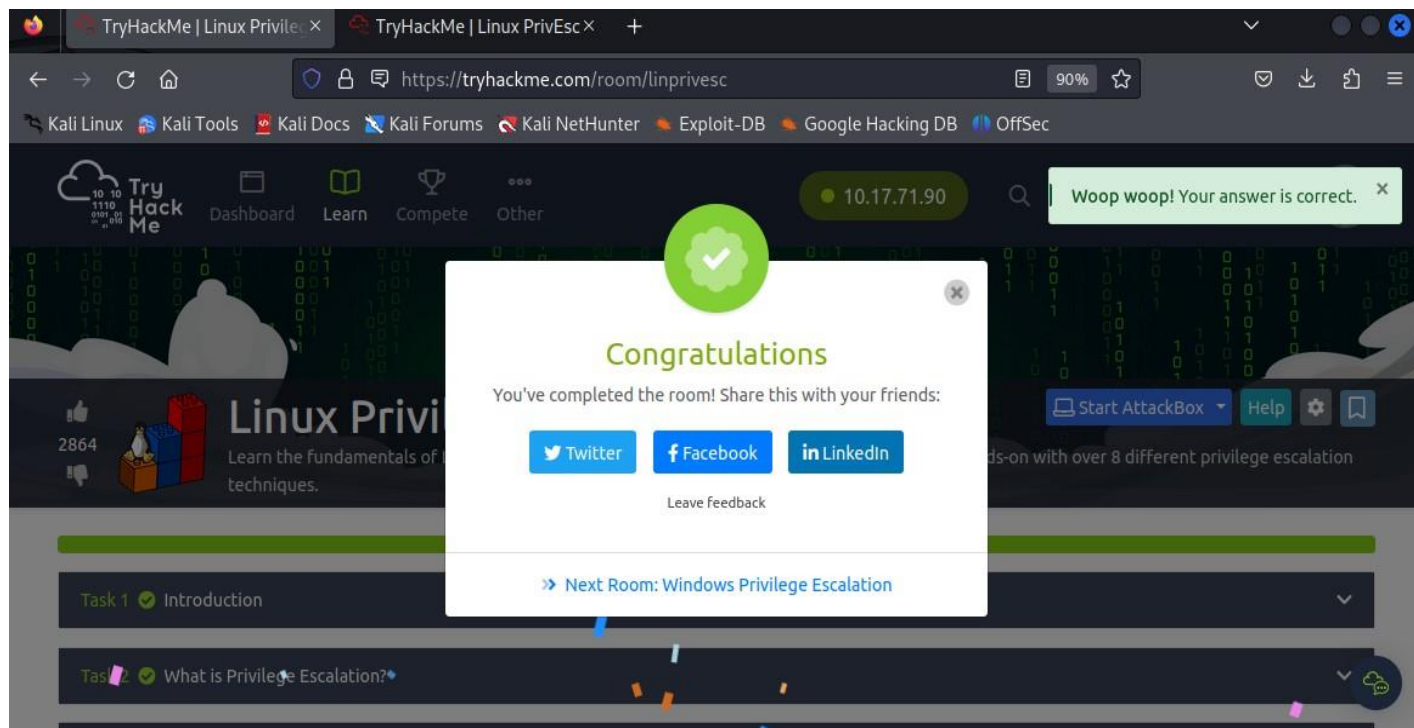
Start Machine



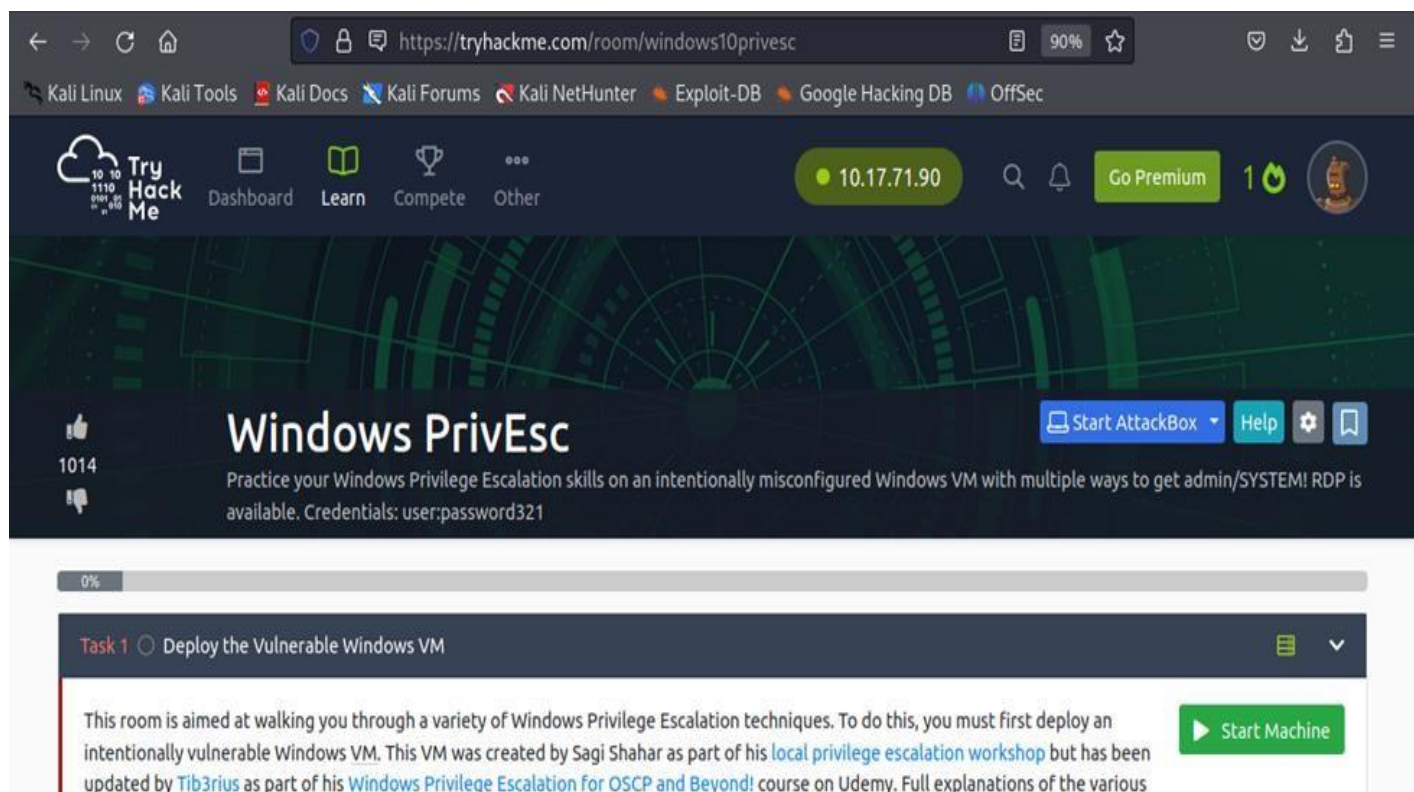
## Room8: - Linux Privilege Escalation

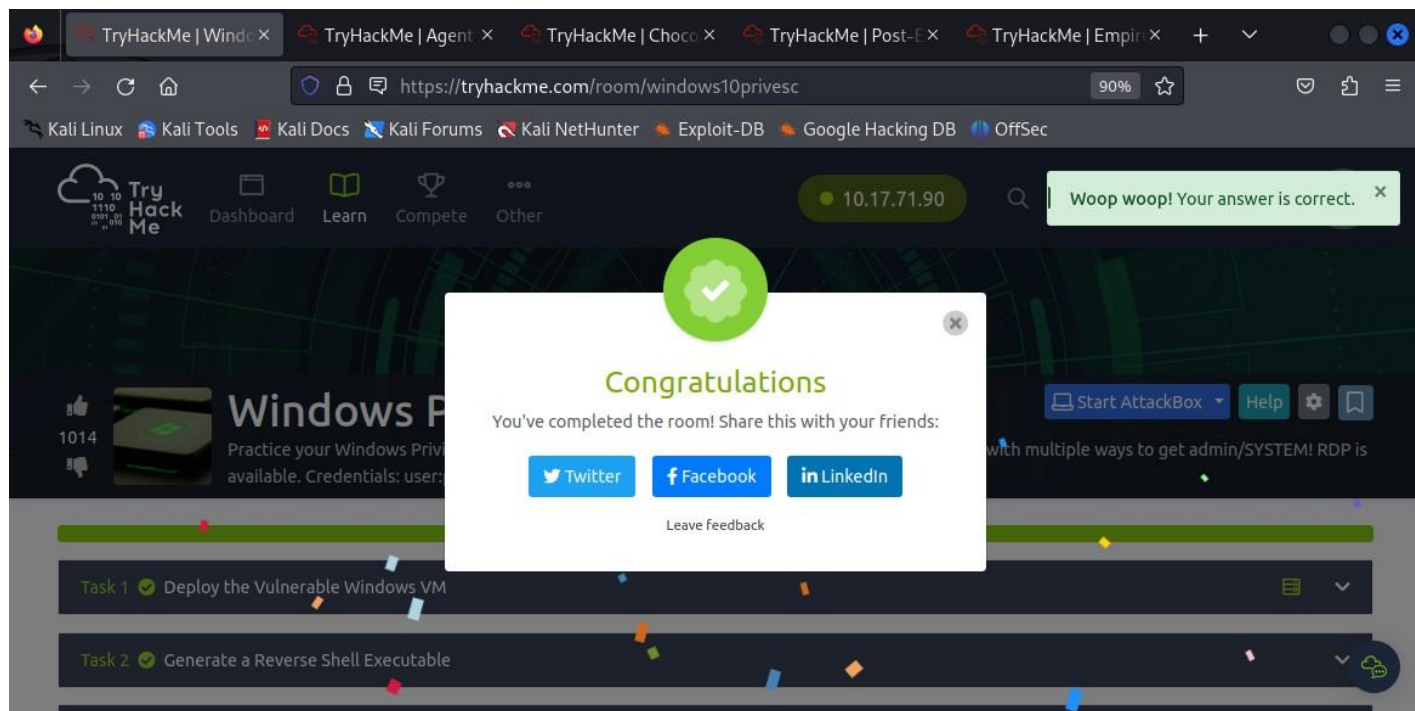




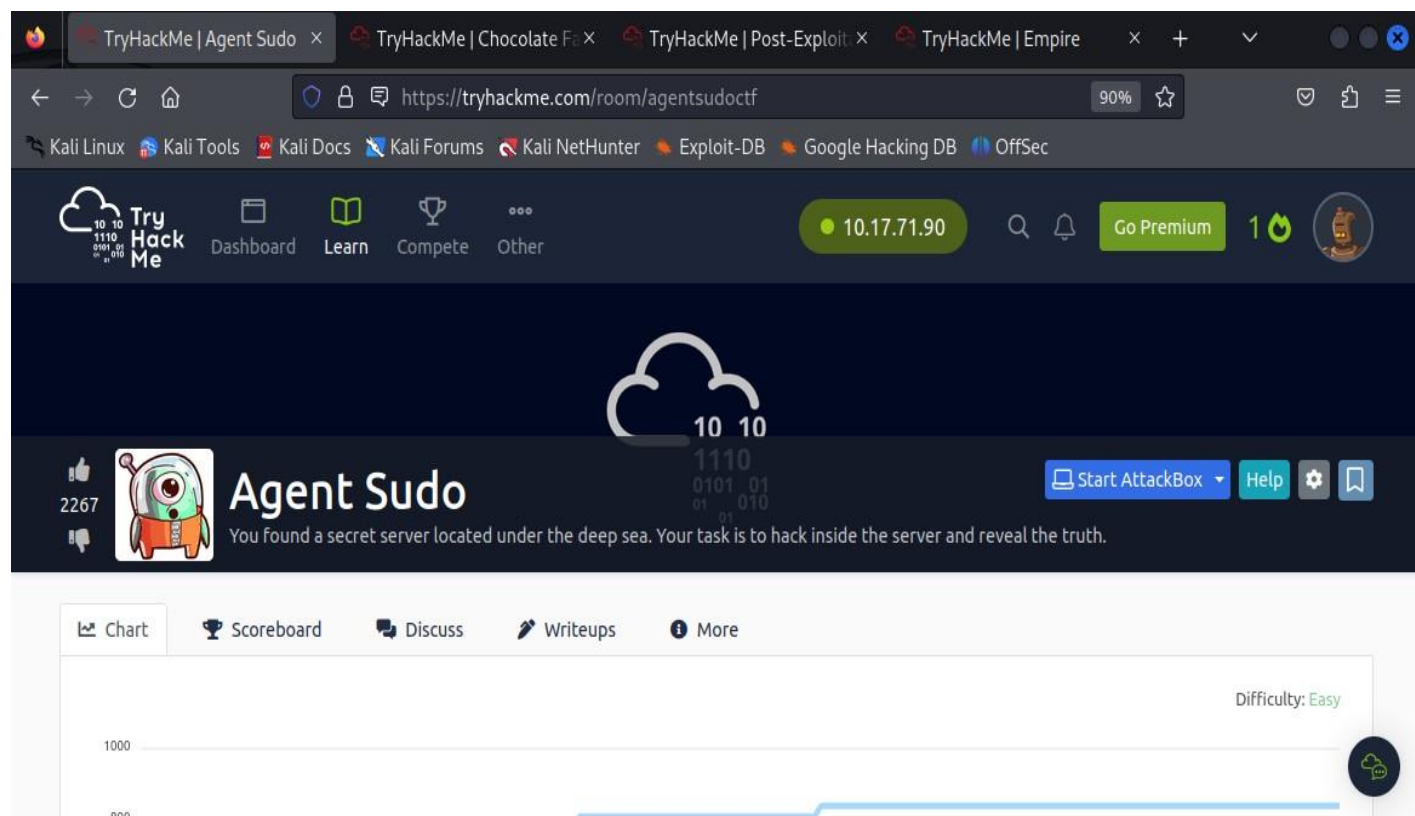


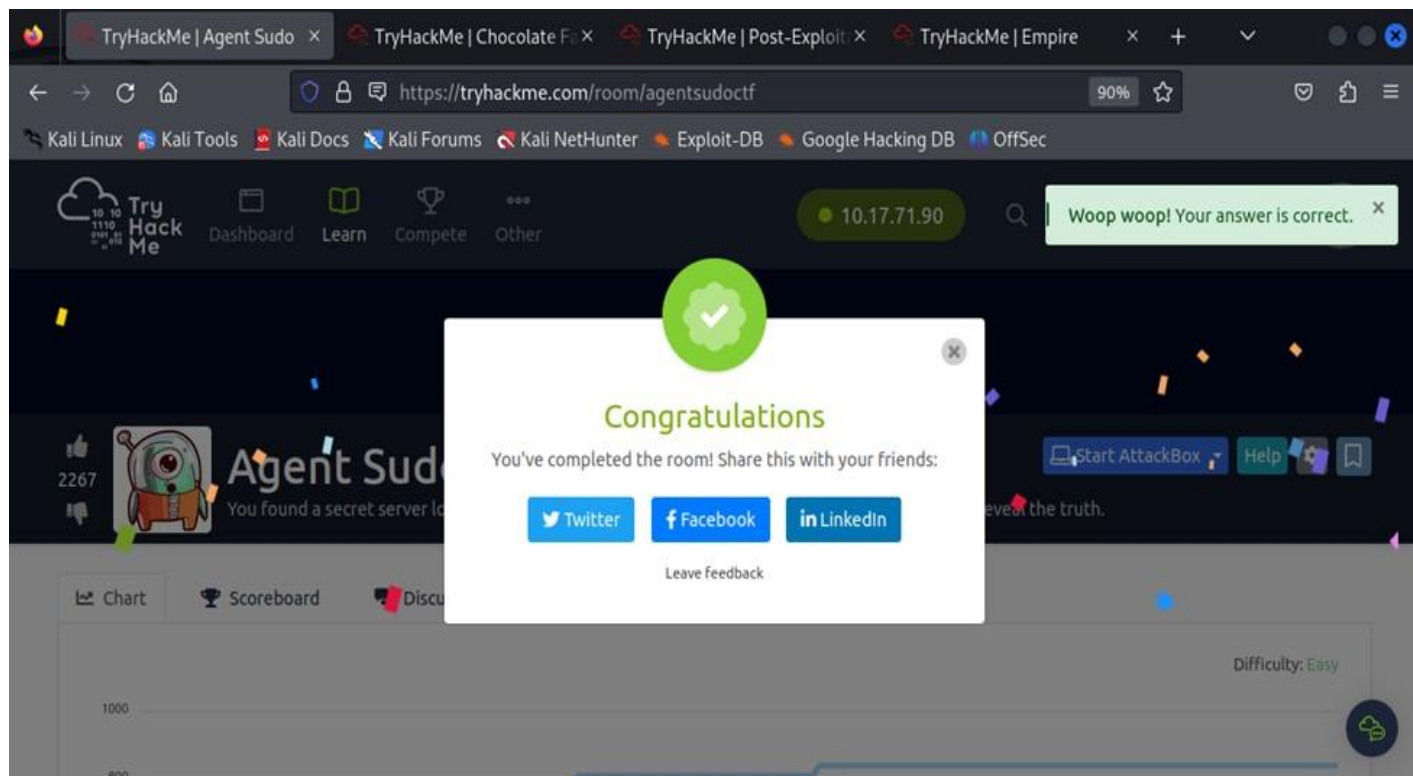
## Room9: - Windows PrivEsc



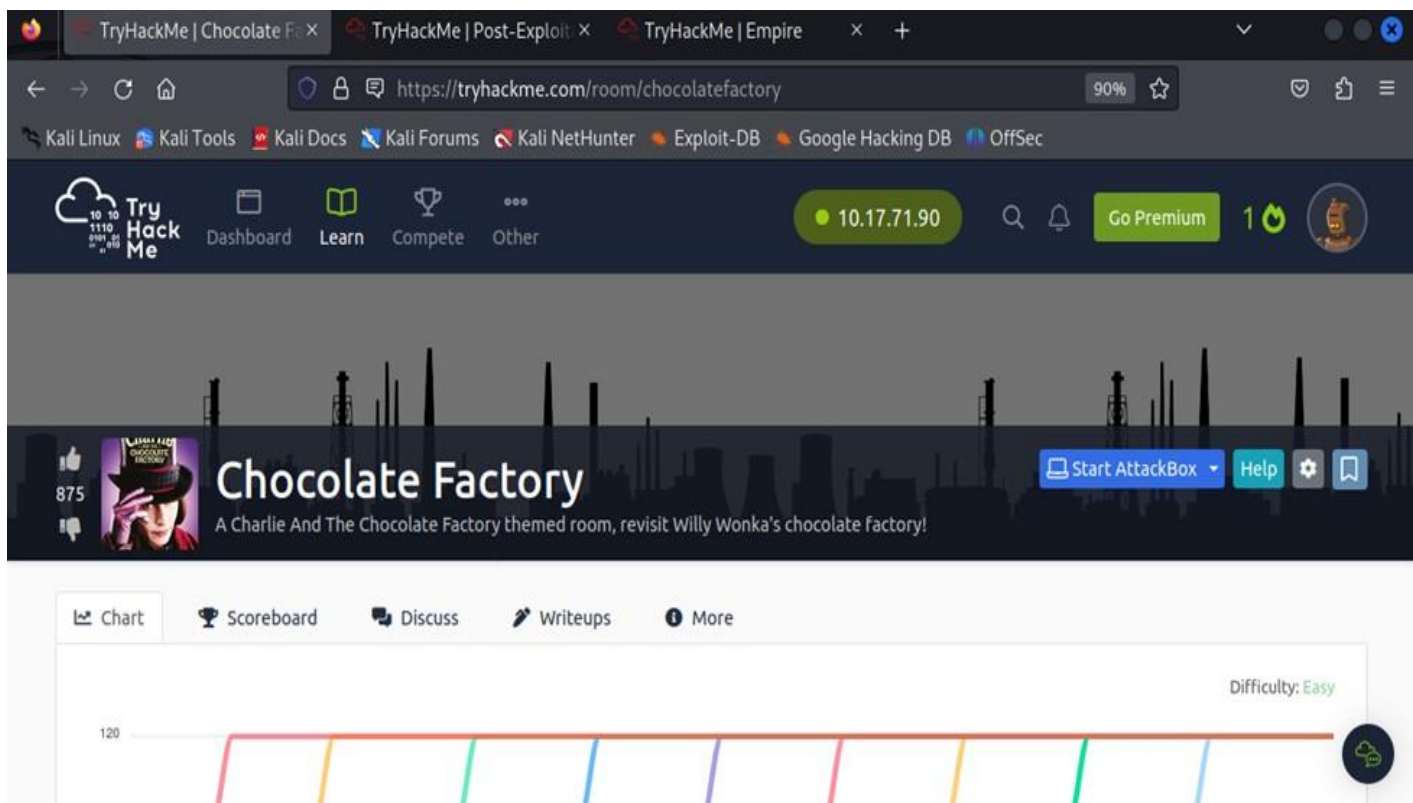


## Room10: - Agent Sudo

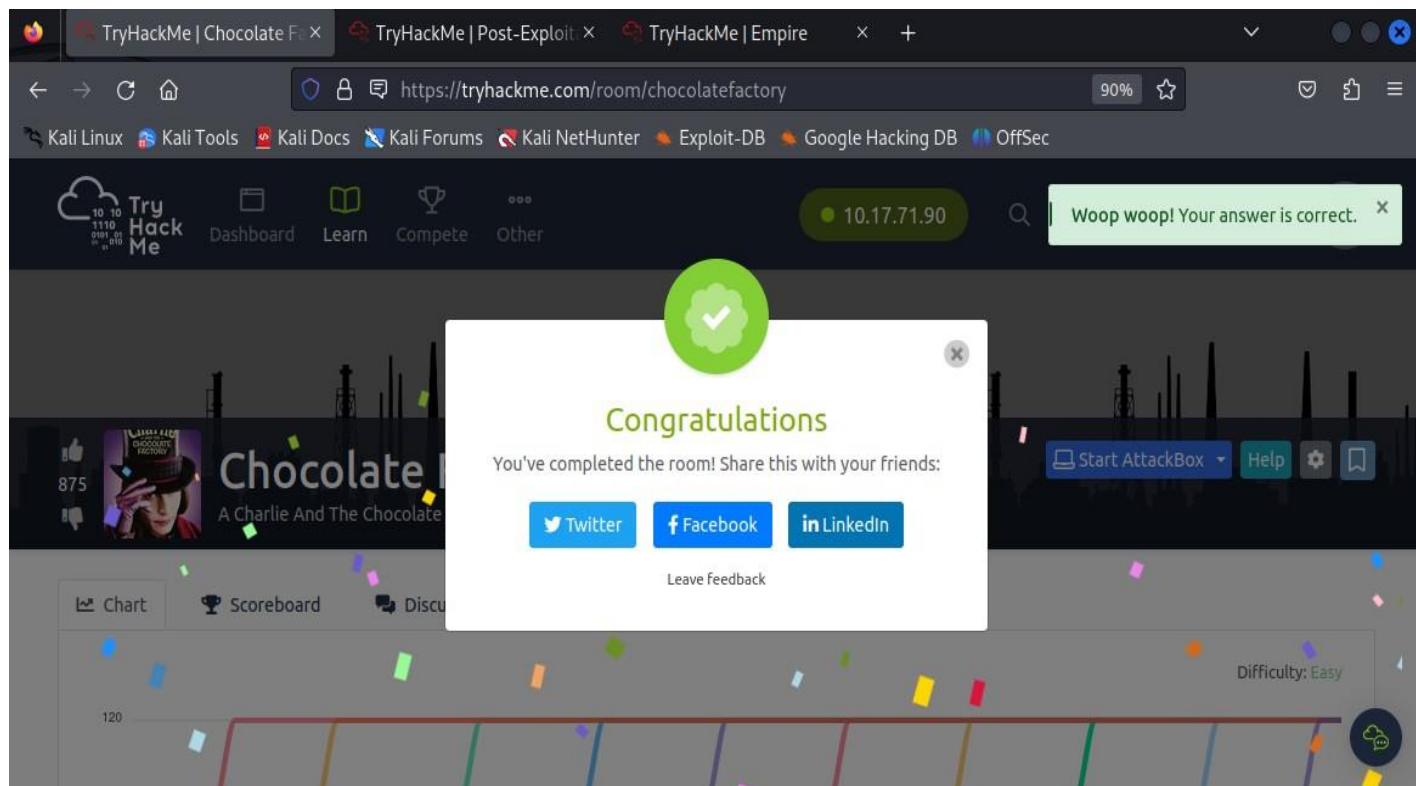




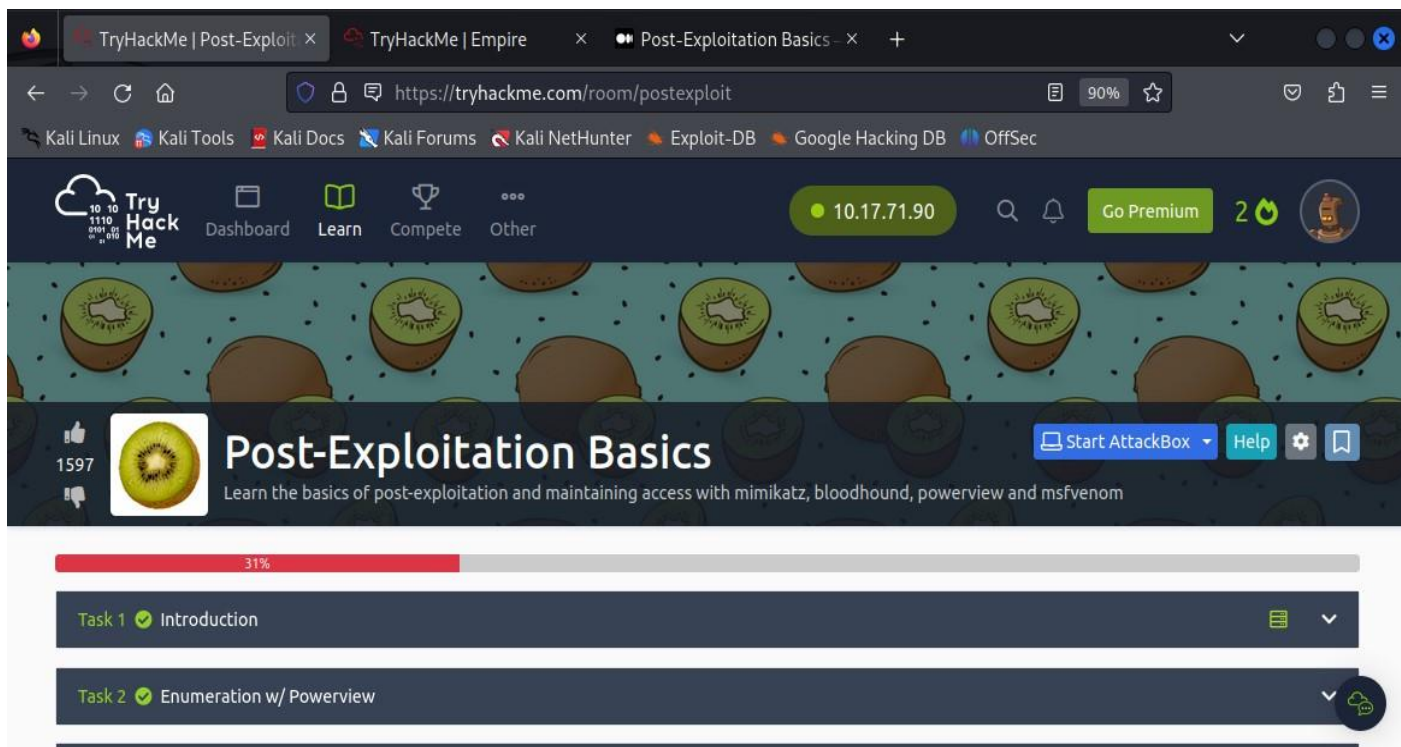
### Room11: - Chocolate Factory



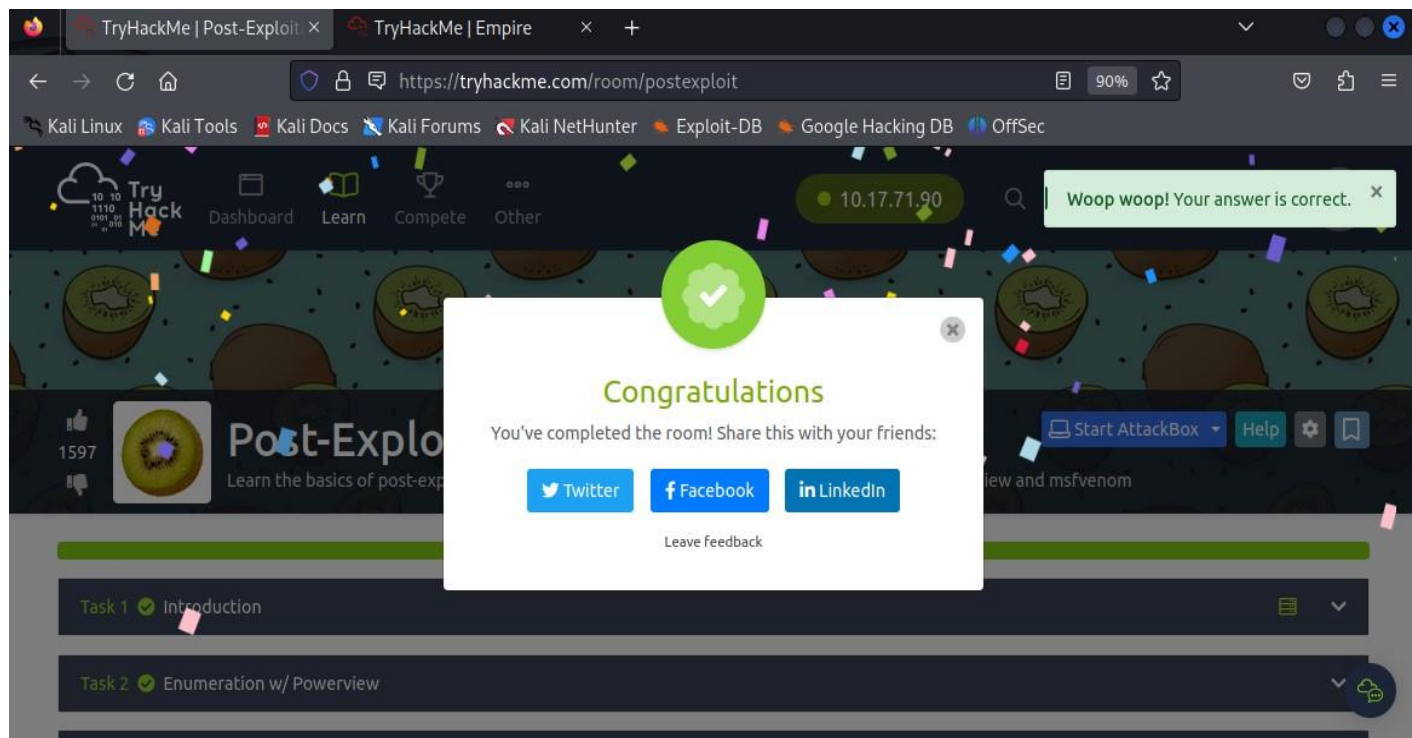




## Room12: - Post-Exploitation Basics







### Room13: - Empire

