cs-sa07-24019
John_Mbithi_Mutave

Attactive Directory

Introduction: Attacktive Directory is a simulated environment designed to replicate a corporate Active Directory infrastructure for educational and testing purposes. This environment presents various vulnerabilities and misconfigurations commonly found in real-world Active Directory deployments. This report aims to provide a comprehensive overview of the Attacktive Directory environment, focusing on enumeration, exploitation, and privilege escalation techniques.

Task 1: Deploy The Machine The initial task involves deploying the Attacktive Directory environment, which provides a controlled setting for conducting security assessments and learning about Active Directory vulnerabilities.

Task 2: Setup This task involves setting up the environment for exploration and exploitation. It may include configuring network settings, establishing connections, and preparing tools for enumeration and exploitation.

Task 3: Enumeration Welcome to Attacktive Directory Enumeration is a crucial phase in any security assessment. In this task, the focus is on gathering information about the Active Directory environment, including domain structure, domain controllers, user accounts, group memberships, and other relevant entities.

Task 4: Enumeration Enumerating Users via Kerberos Kerberos is the primary authentication protocol used in Active Directory environments. By enumerating users via Kerberos, attackers can identify valid user accounts and potentially exploit weak credentials or misconfigurations.

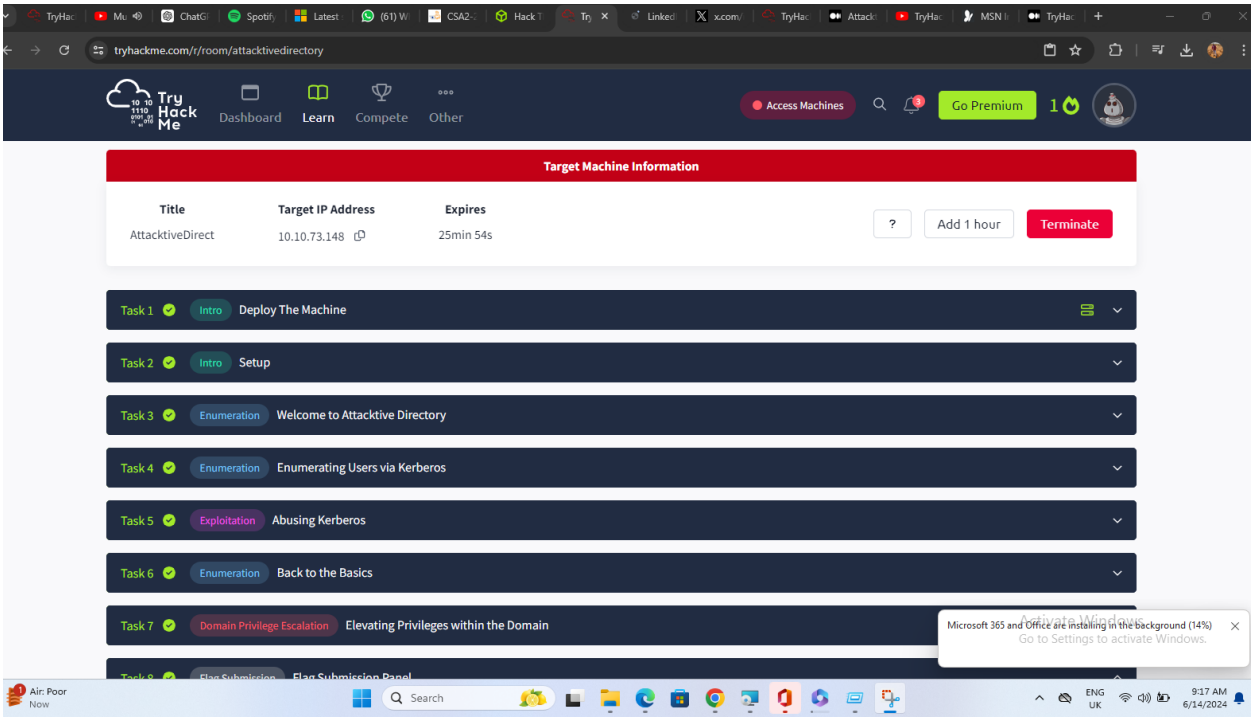
Task 5: Exploitation Abusing Kerberos Building upon the information gathered during enumeration, attackers can exploit vulnerabilities in the Kerberos authentication system to gain unauthorized access to resources within the Active Directory environment. Common exploitation techniques include Kerberoasting, Pass-the-Ticket attacks, and Golden Ticket attacks.

Task 6: Enumeration Back to the Basics In this task, the focus returns to enumeration, emphasizing the importance of thorough reconnaissance in identifying potential attack vectors and weaknesses within the Active Directory infrastructure.

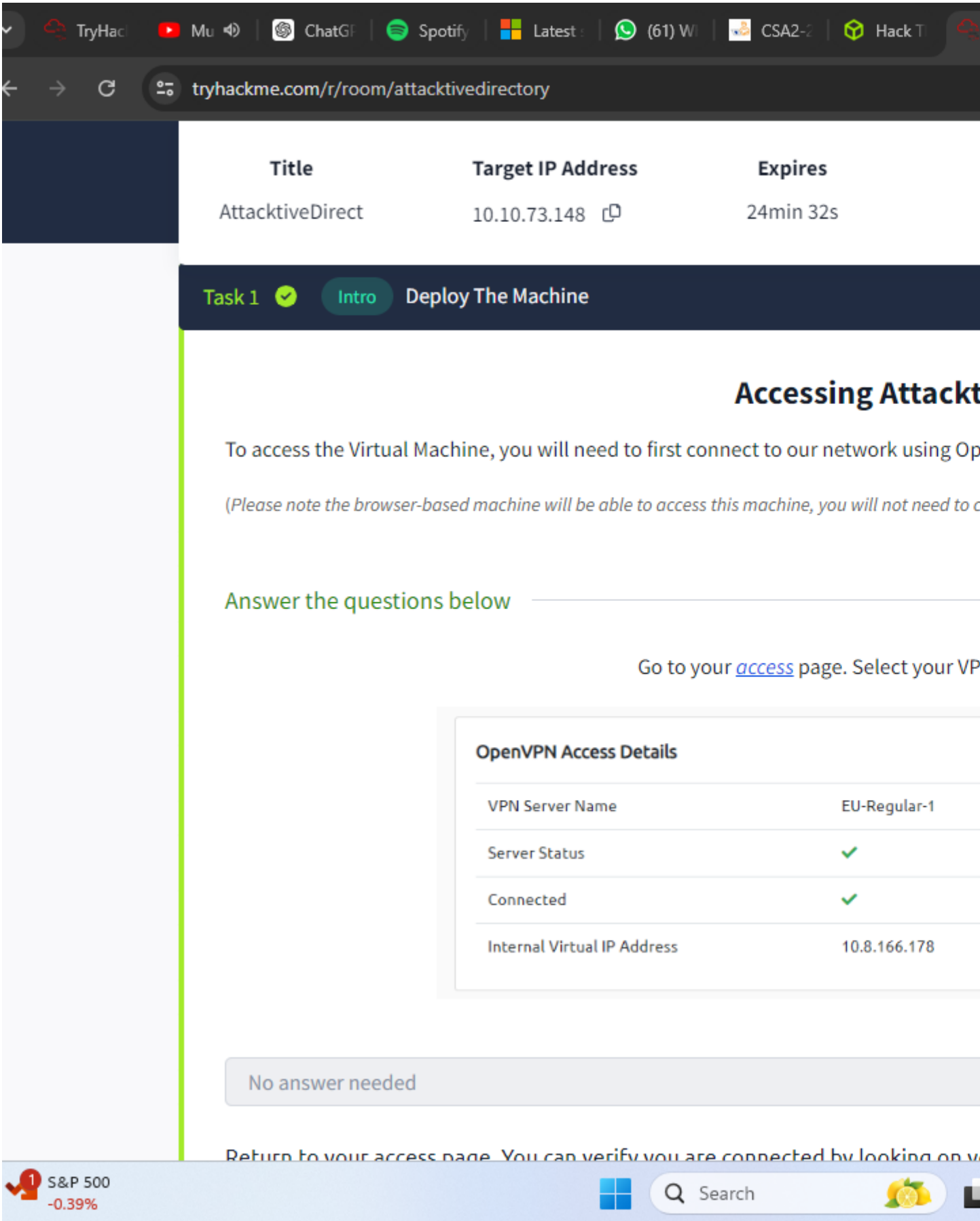
Task 7: Domain Privilege Escalation Elevating Privileges within the Domain Privilege escalation is the process of obtaining higher levels of access within the Active Directory domain than initially granted. Attackers leverage misconfigurations, vulnerabilities, and weaknesses to escalate privileges and gain control over critical systems and data.

Task 8: Flag Submission Panel The final task involves submitting flags, which typically represent achievements or milestones reached during the assessment. Flags may include sensitive information extracted from compromised systems or evidence of successful exploitation.

cs-sa07-24019
John_Mbithi_Mutave

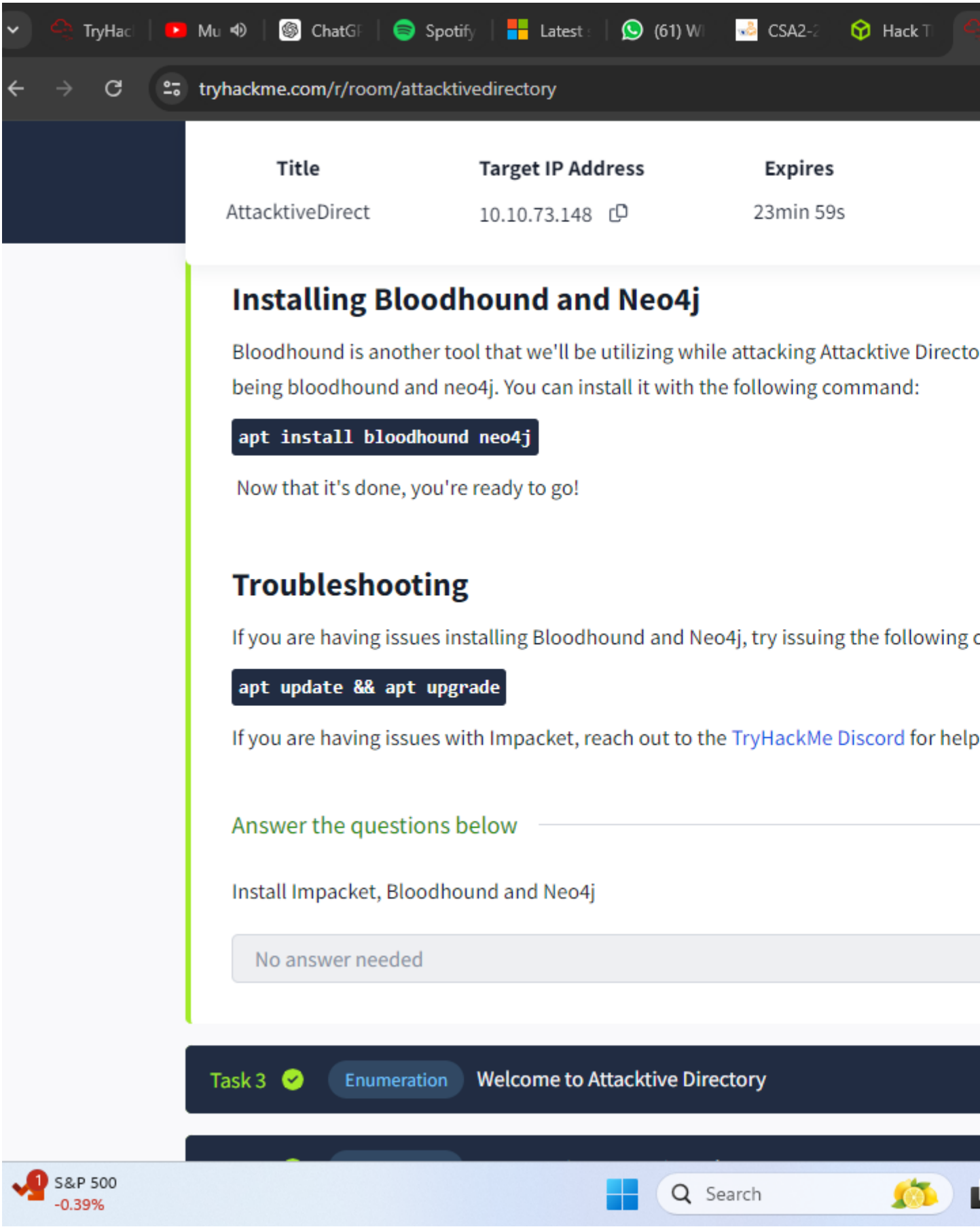


cs-sa07-24019
John_Mbithi_Mutave

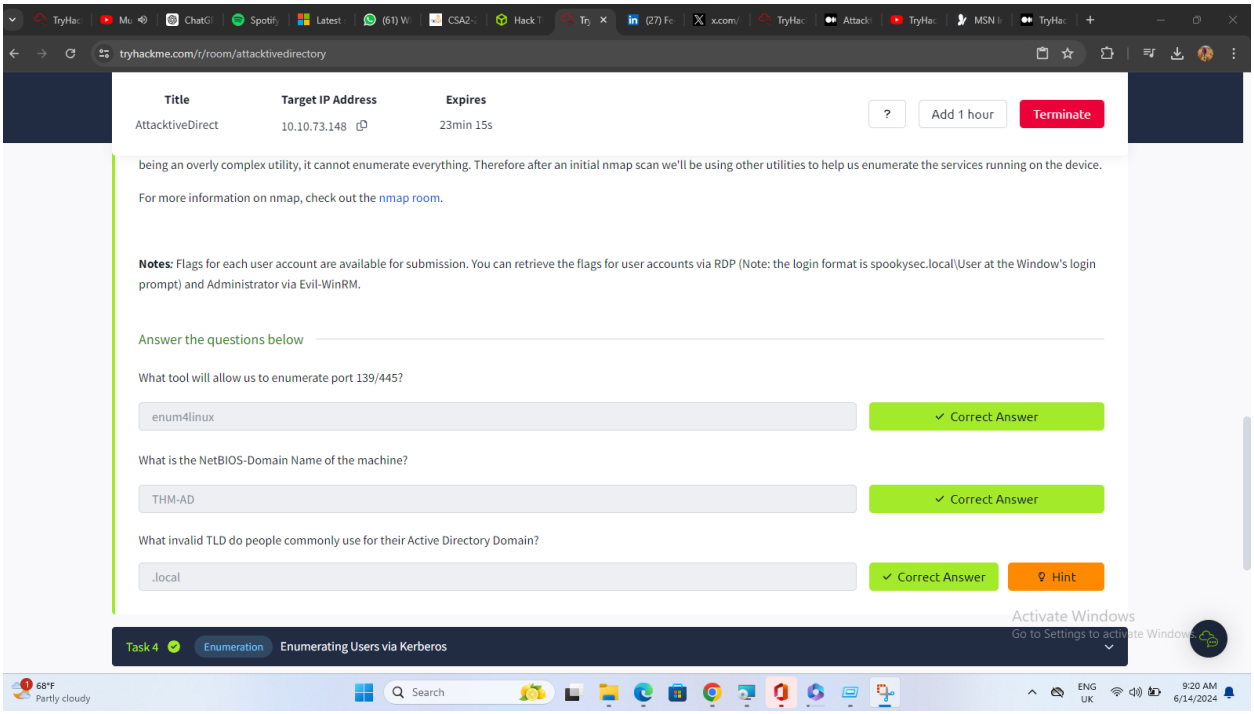


cs-sa07-24019
John_Mbithi_Mutave

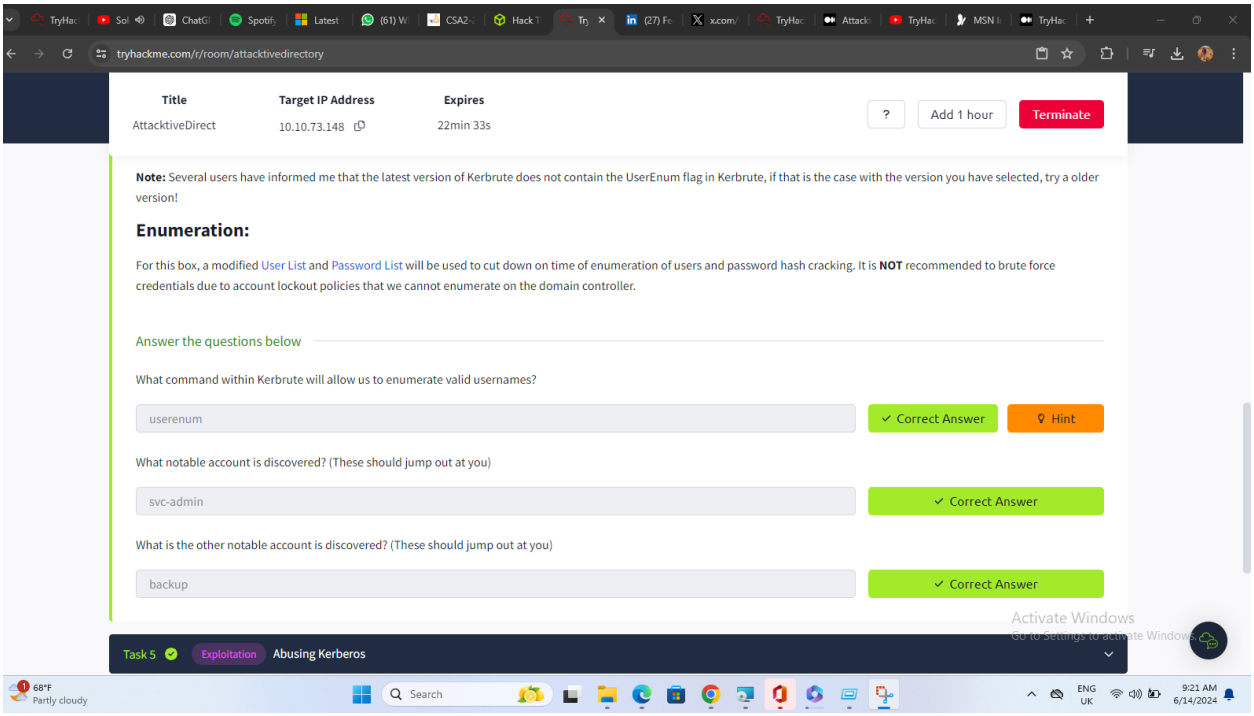
cs-sa07-24019
John_Mbithi_Mutave



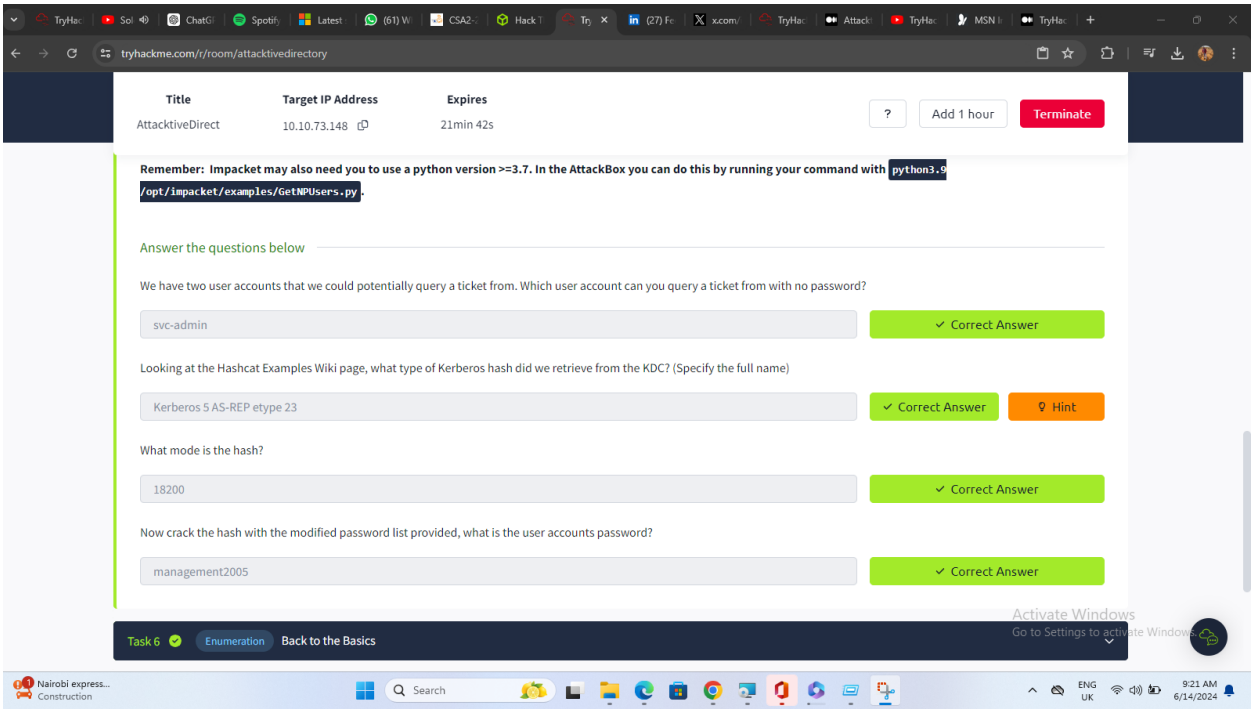
cs-sa07-24019
John_Mbithi_Mutave



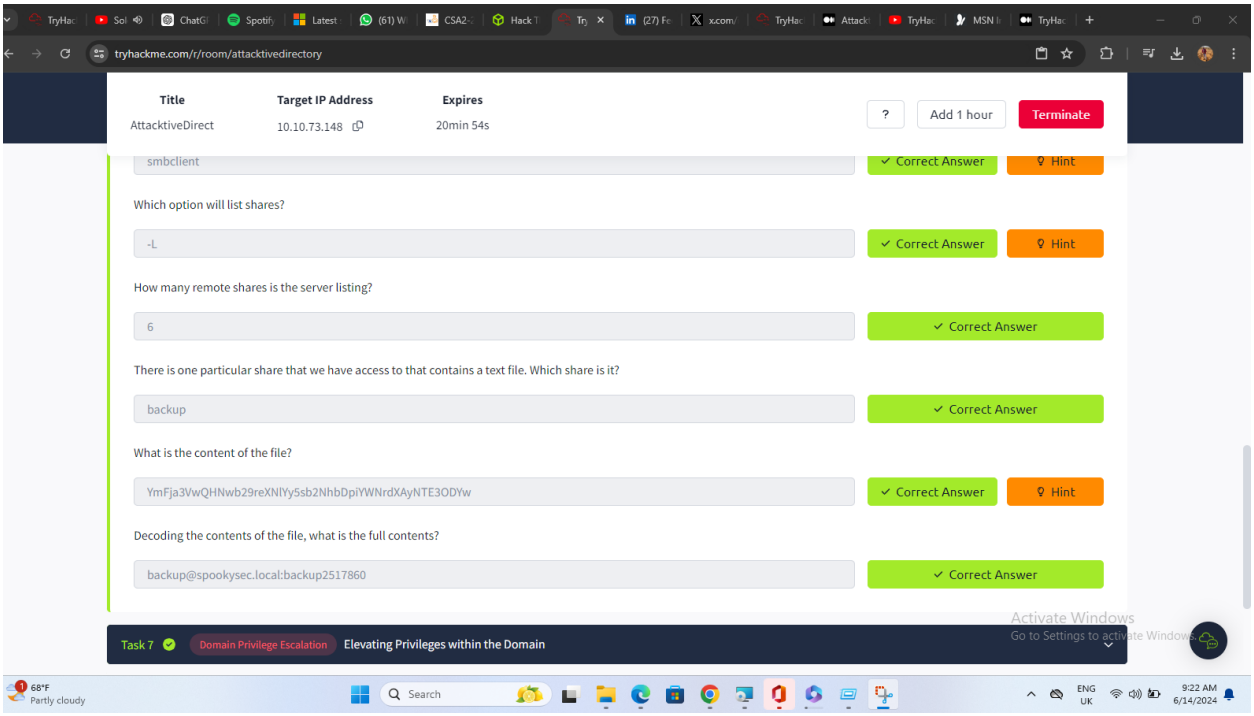
cs-sa07-24019
John_Mbithi_Mutave



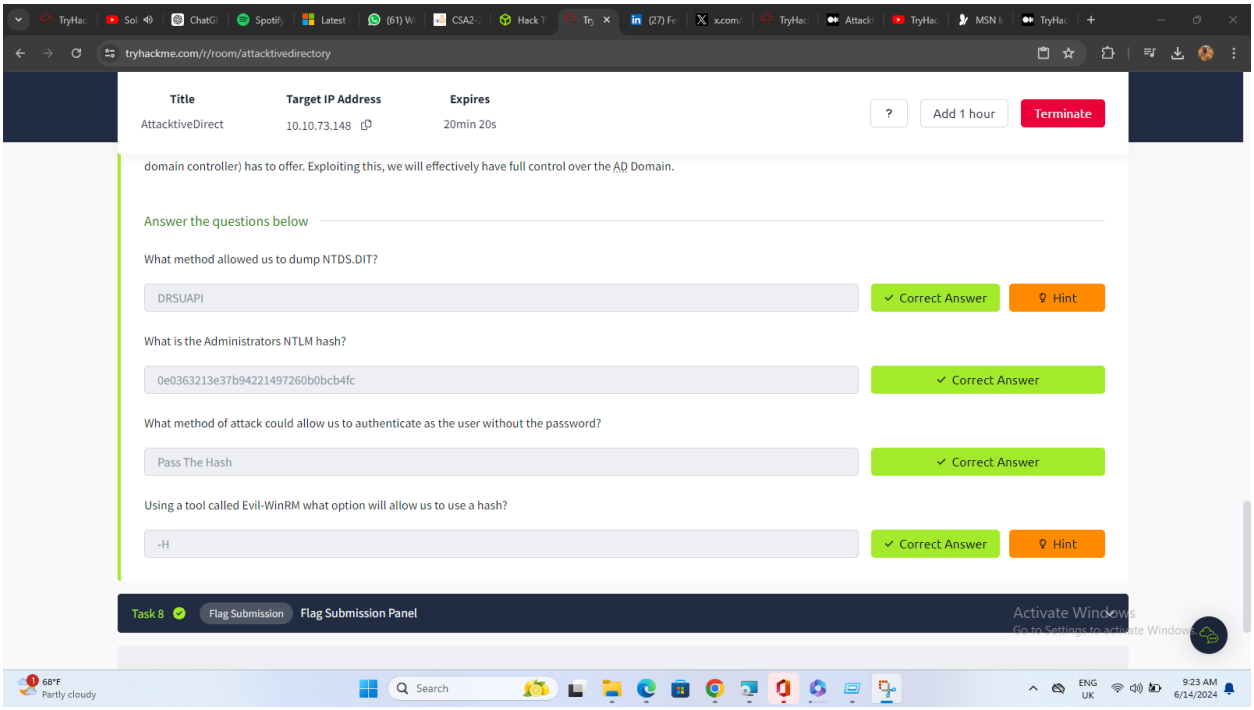
cs-sa07-24019
John_Mbithi_Mutave



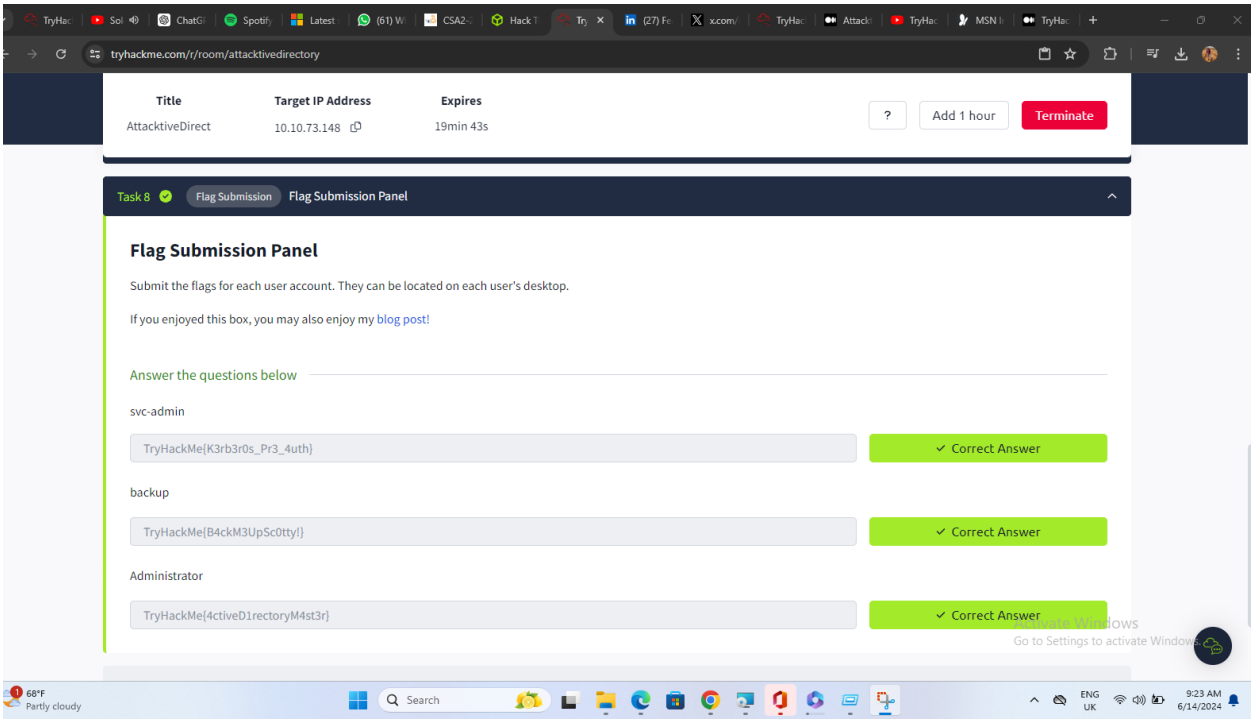
cs-sa07-24019
John_Mbithi_Mutave

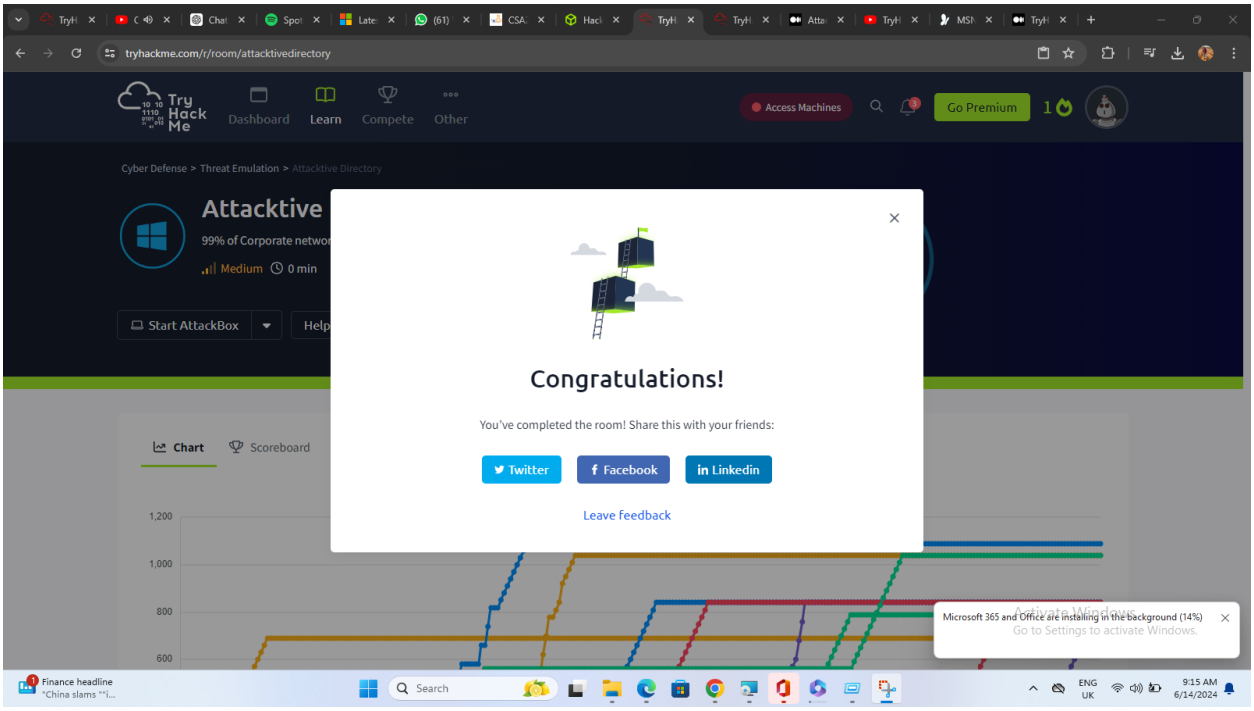


cs-sa07-24019
John_Mbithi_Mutave



cs-sa07-24019
John_Mbithi_Mutave





cs-sa07-24019
John_Mbithi_Mutave

Shareable link - https://tryhackme.com/r/room/attacktivedirectory

Conclusion: Attacktive Directory provides a valuable learning platform for understanding the complexities of Active Directory security and practicing techniques for identifying and mitigating common vulnerabilities. By following the tasks outlined in this report, security professionals can gain practical experience in reconnaissance, exploitation, and privilege escalation within Active Directory environments, ultimately enhancing their skills in defending against real-world threats.