

Bangladesh University of Professionals (BUP)



Assignment – 07

Title - TryHackMe - Active Directory Hardening

Course Name - Enterprise Security Architecture Design and Management

Course Code - MCS1103

Submitted To

Engr. Md. Mushfiqur Rahman

Submitted By

Jannatul Ferdous Katha

Masters in Cyber Security

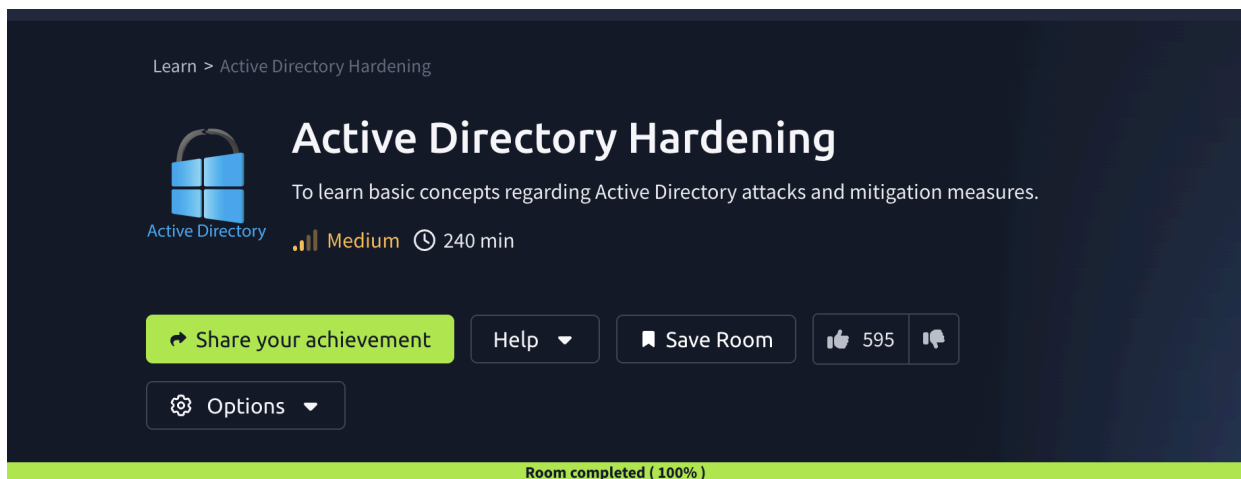
Department of Computer Science and Engineering

Submission Date: 28-04-2025

Table of Contents:

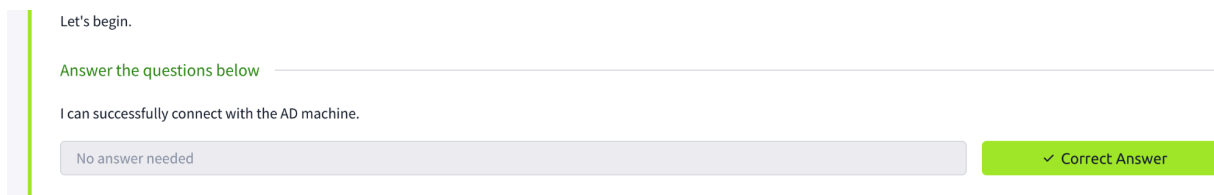
1. Task -1: introduction
2. Task - 2: Understanding General Active Directory concepts
3. Task - 3: securing Authentication Methods
4. Task - 4: Implementing least privilege model
5. Task -5: Microsoft security compliance toolkit'
6. Task - 6: protecting Against known Attacks .
7. Task - 7: Windows Active Directory Hardening Cheat Sheet

Try Hackme: Active Directory Hardening



The screenshot shows the 'Active Directory Hardening' room interface on TryHackMe. At the top, it says 'Learn > Active Directory Hardening'. Below this is the room title 'Active Directory Hardening' with a subtitle 'To learn basic concepts regarding Active Directory attacks and mitigation measures.' The room is marked as 'Medium' difficulty and '240 min' duration. There are buttons for 'Share your achievement', 'Help', 'Save Room', and a thumbs up icon with '595' likes. An 'Options' button is also present. At the bottom, a green bar indicates 'Room completed (100%)'.

Task - 1: Introduction - In this section no answer is needed. An Attachment is attached -



The screenshot shows the 'Task - 1: Introduction' section. It starts with 'Let's begin.' followed by 'Answer the questions below'. The question is 'I can successfully connect with the AD machine.' Below the question, there is a text input field containing 'No answer needed' and a green button labeled '✓ Correct Answer'.

Task - 2: Understanding General Active Directory concepts -

Questions: What is the root domain in the attached AD machine?

Answers: tryhackme.loc

Answer the questions below

What is the root domain in the attached AD machine?

tryhackme.loc

✓ Correct Answer

Task - 3: securing Authentication Methods

Questions: Change the Group Policy Setting in the VM, so it does not store the LAN Manager hash on the next password change.

Answer: No Answer Needed

Questions: What is the default minimum password length (number of characters) in the attached VM?

Answer: 7

Answer the questions below

Change the Group Policy Setting in the VM, so it does not store the LAN Manager hash on the next password change.

No answer needed

✓ Correct Answer

What is the default minimum password length (number of characters) in the attached VM?

7

✓ Correct Answer

Task - 4: Implementing least privilege model

Questions: Computers and Printers must be added to Tier 0 - yea/nay?

Answers: nay

Questions: Suppose a vendor arrives at your facility for a 2-week duration task. Being a System Administrator, you should create a high privilege account for him - yea/nay?

Answers: nay

Answer the questions below

Computers and Printers must be added to Tier 0 - yea/nay?

nay

✓ Correct Answer

Suppose a vendor arrives at your facility for a 2-week duration task. Being a System Administrator, you should create a high privilege account for him - yea/nay?

nay

✓ Correct Answer

Task -5: Microsoft security compliance toolkit

Questions: Find and open BaselineLocalInstall script in PowerShell editor - Can you find the flag?

Answers: THM{00001}

Questions: Find and open MergePolicyRule script (Policy Analyser) in PowerShell editor - Can you find the flag?

Answers: {THM00191}

Answer the questions below

Find and open **BaselineLocalInstall** script in PowerShell editor - Can you find the flag?

THM{00001}

✓ Correct Answer

Find and open **MergePolicyRule** script (Policy Analyser) in PowerShell editor - Can you find the flag?

{THM00191}

✓ Correct Answer

Task - 6: protecting Against known Attacks .

Questions: Does Kerberoasting utilise an offline-attack scheme for cracking encrypted passwords - yea/nay?

Answer: yea

Questions: As per the generated report, how many users have the same password as aaron.booth?

Answer: 186

Answer the questions below

Does Kerberoasting utilise an offline-attack scheme for cracking encrypted passwords - yea/nay?

yea

✓ Correct Answer

As per the generated report, how many users have the same password as aaron.booth?

186

✓ Correct Answer

Task - 7: Windows Active Directory Hardening Cheat Sheet

No Answers required

Answer the questions below

I have completed the room.

No answer needed

✓ Correct Answer