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

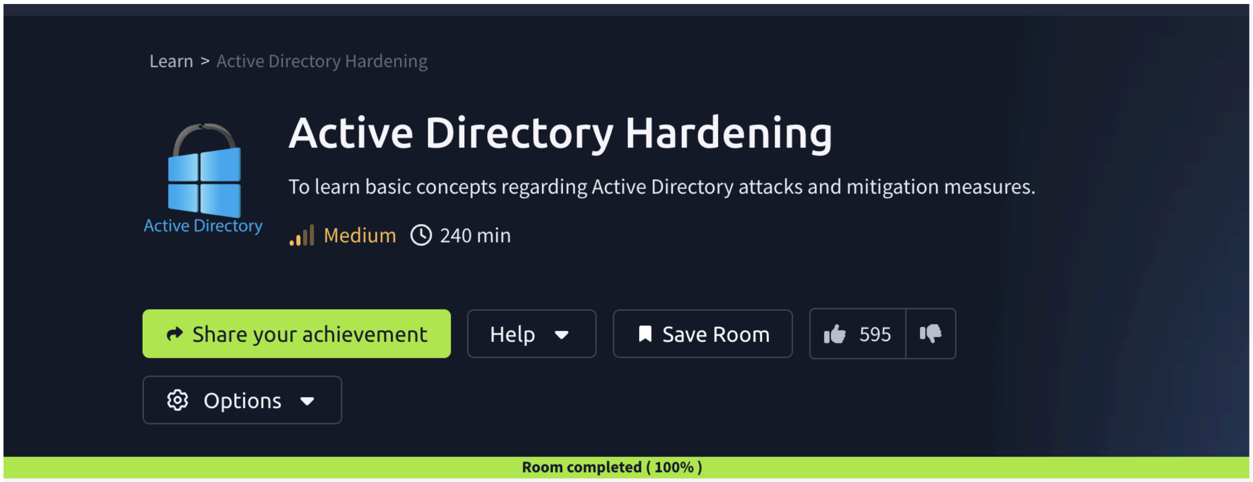
Masters in Cyber Security

Department of Computer Science and Engineering

Submission Date: 28-04-2025

Table of Contents:

Try Hackme: Active Directory Hardening

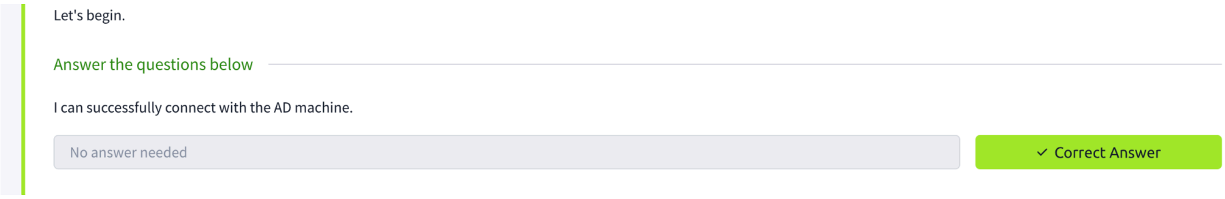


Learn > Active Directory Hardening

Active Directory Hardening

To learn basic concepts regarding Active Directory attacks and mitigation measures.

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



Let's begin.

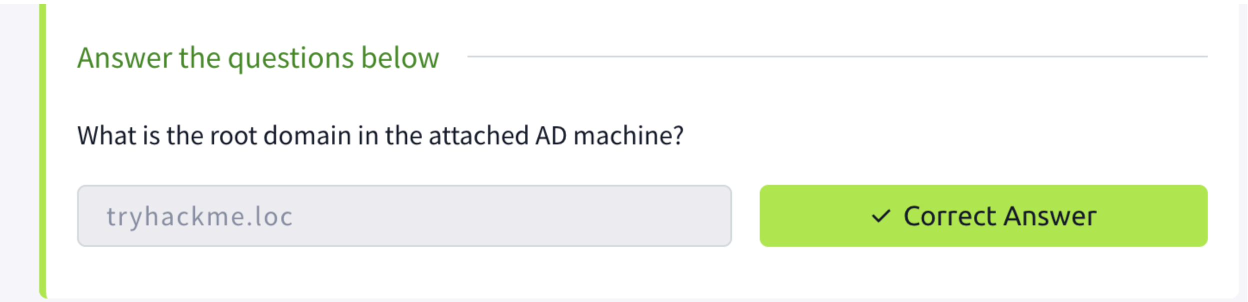
Answer the questions below

I can successfully connect with the AD machine.

No answer needed

Task - 2: Understanding General Active Directory concepts -

Questions: What is the root domain in the attached AD machine?
Answers: tryhackme.loc



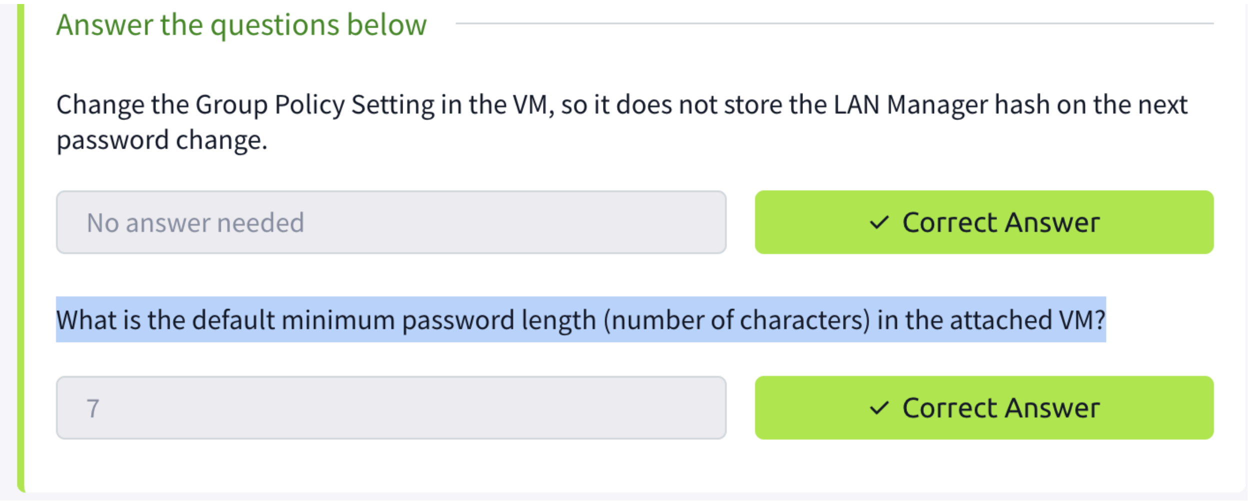
Answer the questions below

What is the root domain in the attached AD machine?

tryhackme.loc

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

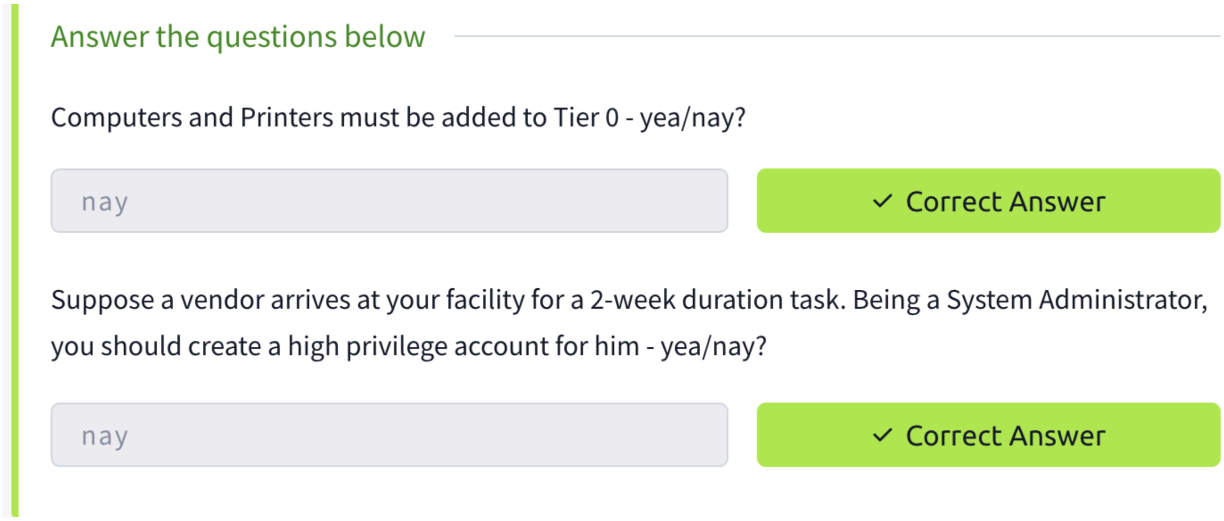
What is the default minimum password length (number of characters) in the attached VM?

7

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?

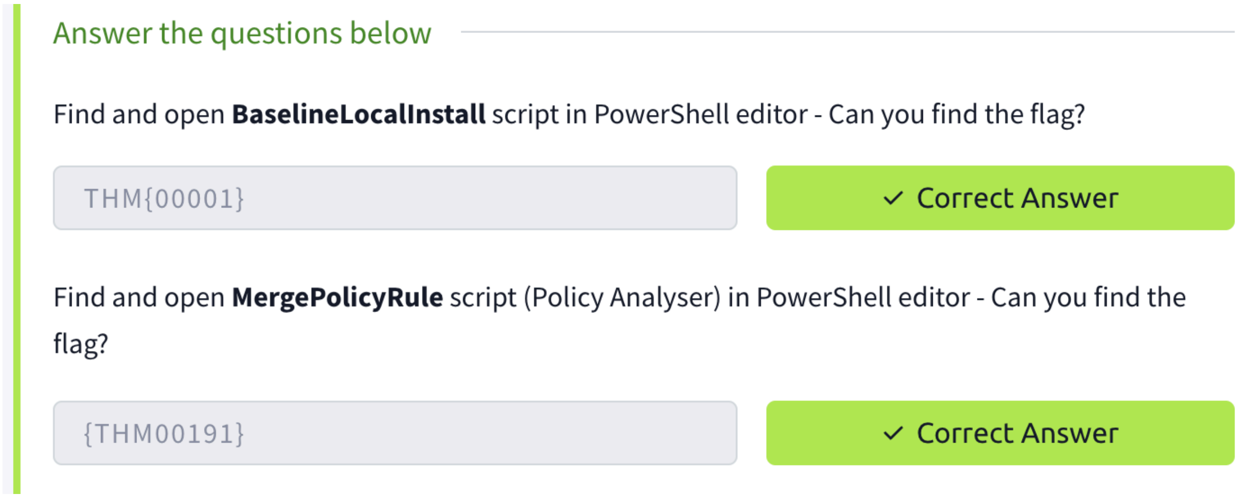
nay

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

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?

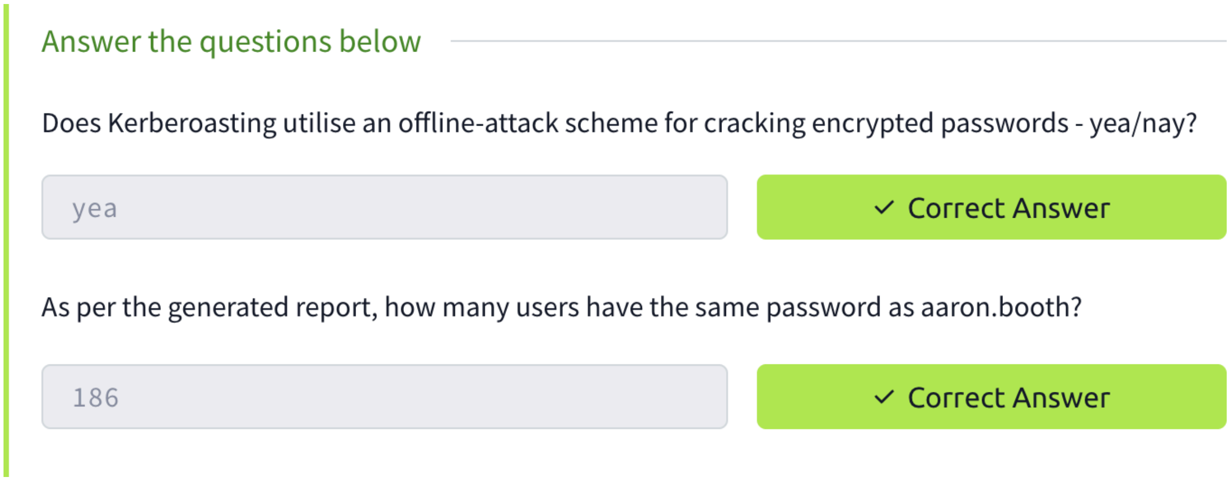
THM{00001}

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

{THM00191}

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

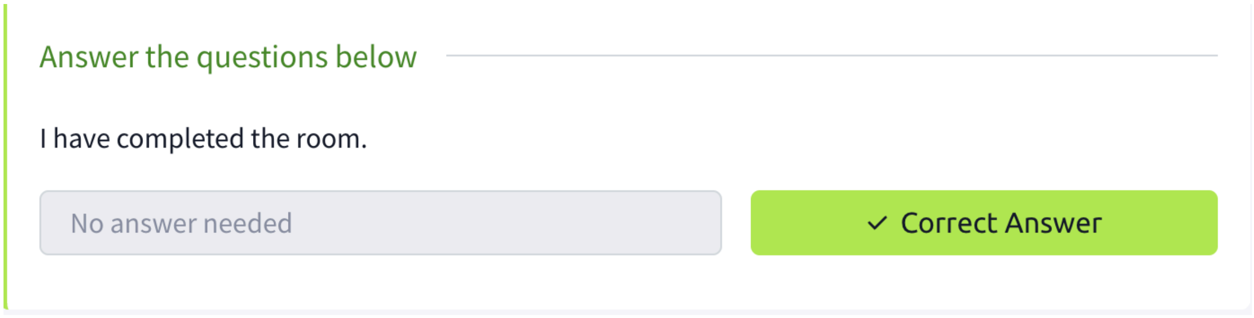
Does Kerberoasting utilise an offline-attack scheme for cracking encrypted passwords - yea/nay?

yea

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

186

Task - 7: Windows Active Directory Hardening Cheat Sheet
No Answers required



Answer the questions below

I have completed the room.

No answer needed