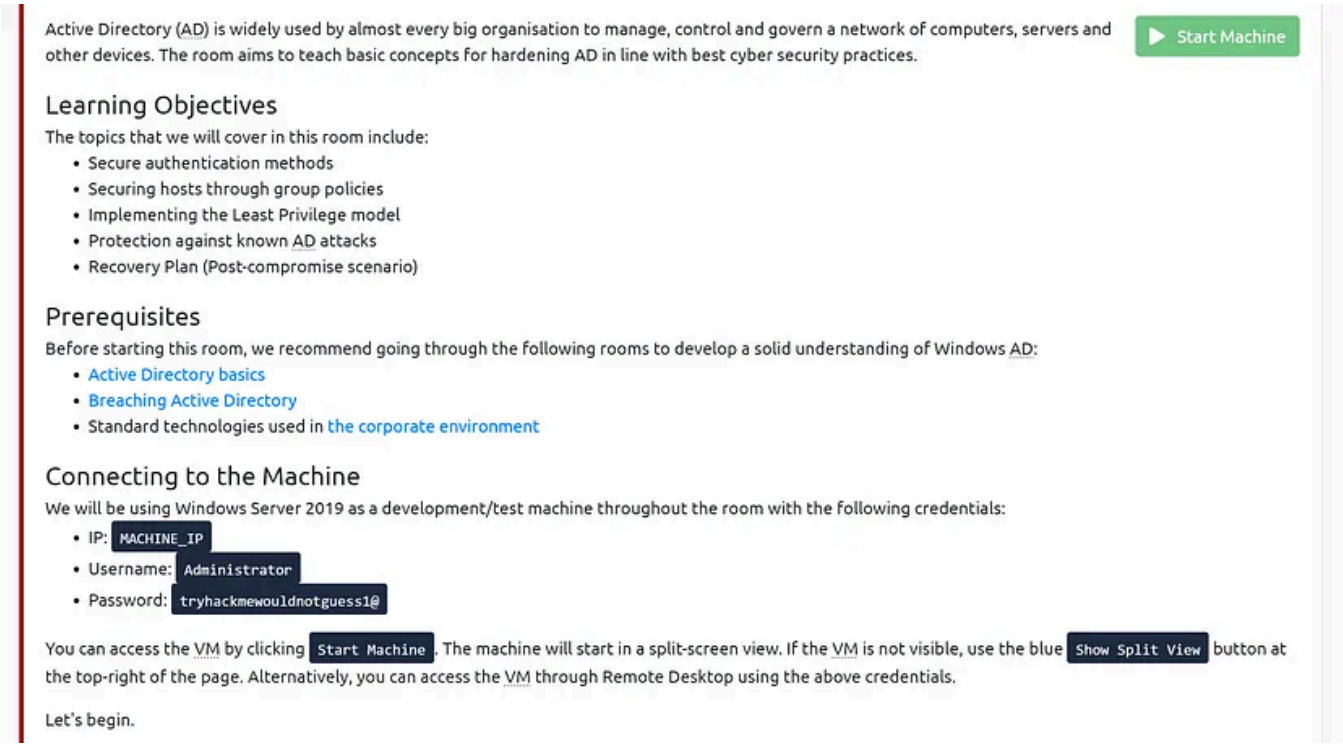
Tryhackme: Active Directory Hardening

Daniel Schwarzentraub · Follow
3 min read · Sep 28, 2023

Task 1: **Introduction**



Active Directory (AD) is widely used by almost every big organisation to manage, control and govern a network of computers, servers and other devices. The room aims to teach basic concepts for hardening AD in line with best cyber security practices.

Start Machine

Learning Objectives

The topics that we will cover in this room include:

- Secure authentication methods
- Securing hosts through group policies
- Implementing the Least Privilege model
- Protection against known AD attacks
- Recovery Plan (Post-compromise scenario)

Prerequisites

Before starting this room, we recommend going through the following rooms to develop a solid understanding of Windows AD:

- Active Directory basics
- Breaching Active Directory
- Standard technologies used in the corporate environment

Connecting to the Machine

We will be using Windows Server 2019 as a development/test machine throughout the room with the following credentials:

- IP: `MACHINE_IP`
- Username: `Administrator`
- Password: `tryhackmewouldnotguess1@`

You can access the VM by clicking `Start Machine`. The machine will start in a split-screen view. If the VM is not visible, use the blue `Show Split View` button at the top-right of the page. Alternatively, you can access the VM through Remote Desktop using the above credentials.

Let's begin.

Task 2: **Understanding General Active Directory Concepts**

Domain

The domain acts as a core unit regarding the logical structure of the Active Directory. It initially stores all the critical information about the objects that belong to the domain only.

Domain Controller

A Domain Controller is an Active Directory server that acts as the brain for a Windows server domain; it supervises the entire network. Within the domain, it acts as a gatekeeper for users' authentication and IT resources authorisation.

Trees and Forests

Trees and Forests are the two most critical concepts of the Active Directory.

Trees

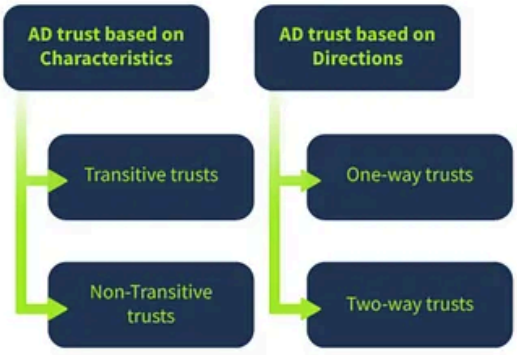
Trees are responsible for sharing resources between the domains. The communication between the domains inside a tree is possible by either one-way or two-way trust. When a domain is added to the Tree, it becomes the Offspring domain of that particular domain to which it is added – now a Parent domain.

Forests

When the sharing of the standard global catalogue, directory schema, logical structure, and directory configuration between the collections of trees is made successfully, it is called a Forest. Communication between two forests becomes possible once a forest-level trust is created.

Trust in Active Directory

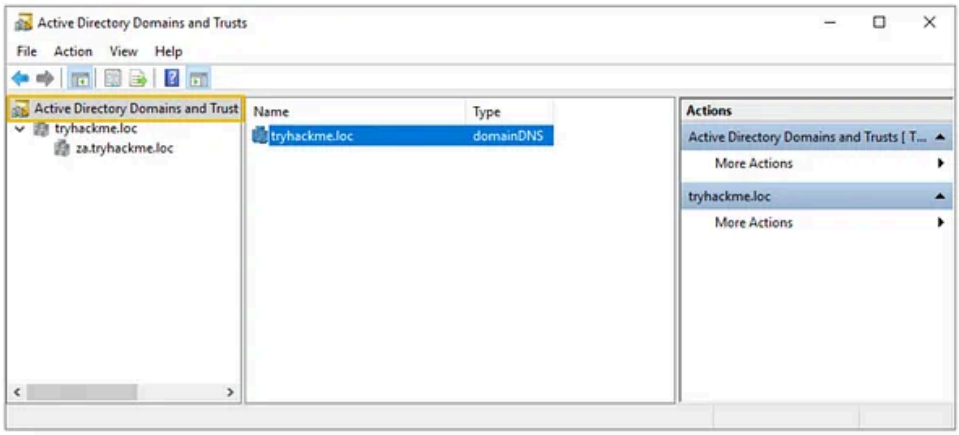
AD trust is the established communication bridge between the domains in Active Directory. When we say one domain trusts another in the AD network, it means its resources can be shared with another domain. However, one domain's resources are not directly available to every other domain, as it is not safe. Thus, the resource sharing availability is governed by Trusts in AD. The AD trusts are of two categories, which are classified based on their characteristics or the current direction.



AD trusts categorised based on characteristics are known as Transitive and non-Transitive trusts. Transitive trust reflects a two-way relationship between domains. If there are three domains, domain A trusts domain B and domain B has a transitive trust with domain C. Consequently, domain A will automatically trust domain C for sharing resources.

Again, AD trusts are of two types when classified based on their direction: One-way and Two-way trusts. You can access the AD trust through the following:

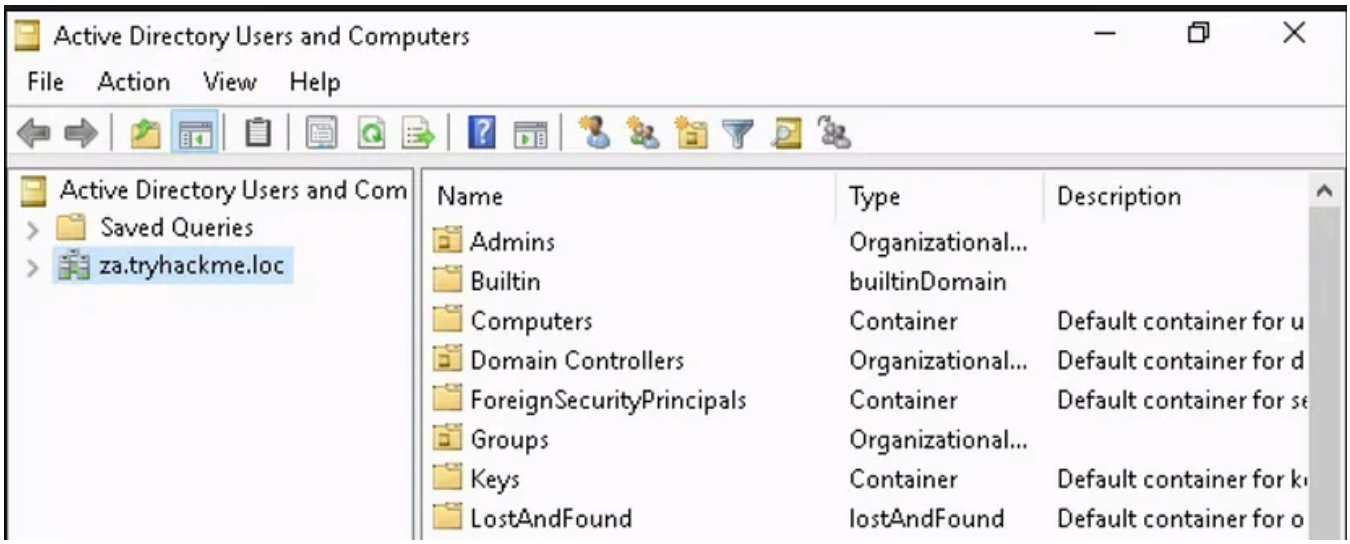
```
Server Manager > Tools > Active Directory Domains and Trust
```



Container and Leaves

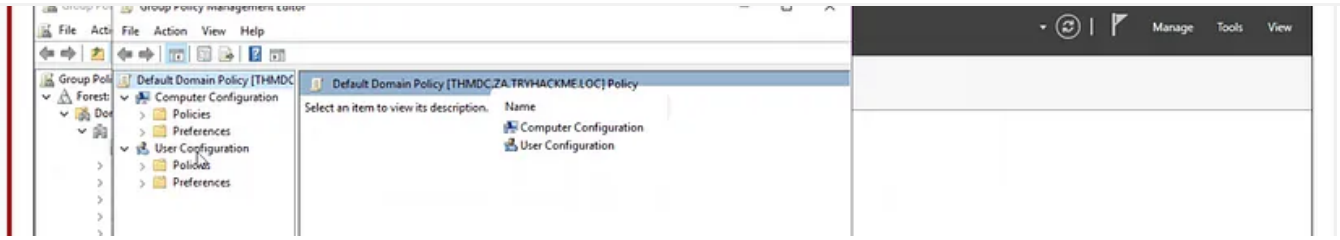
For those familiar, each network part is treated as an object in AD. Anything from resources, users, services, or part of the network can be an object. The hierarchical structure of AD defines that an object may or may not contain other objects based on the scenario. When an object holds another object, it is termed a container; otherwise, it is called the leaf object.

What is the root domain in the attached AD machine?



Answer: **tryhackme.loc**

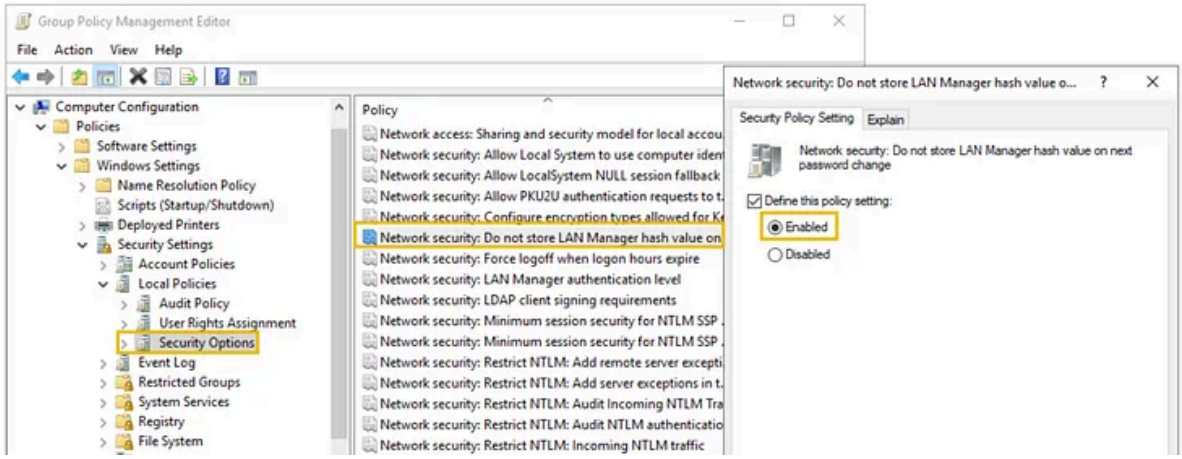
Task 3: **Securing Authentication Methods**



LAN Manager Hash

The user account password for Windows isn't stored in clear text; instead, it stores passwords with two types of hash representation. When the password for any user account is changed or set with fewer than 15 characters, both LM hash (LAN Manager hash) and NT hash (Windows NT hash) are generated by Windows and can be stored in AD. The LM hash is relatively weaker than the NT and is prone to a fast brute-force attack. The best recommendation is to prevent Windows from storing the password's LM hash. You can access it through the following:

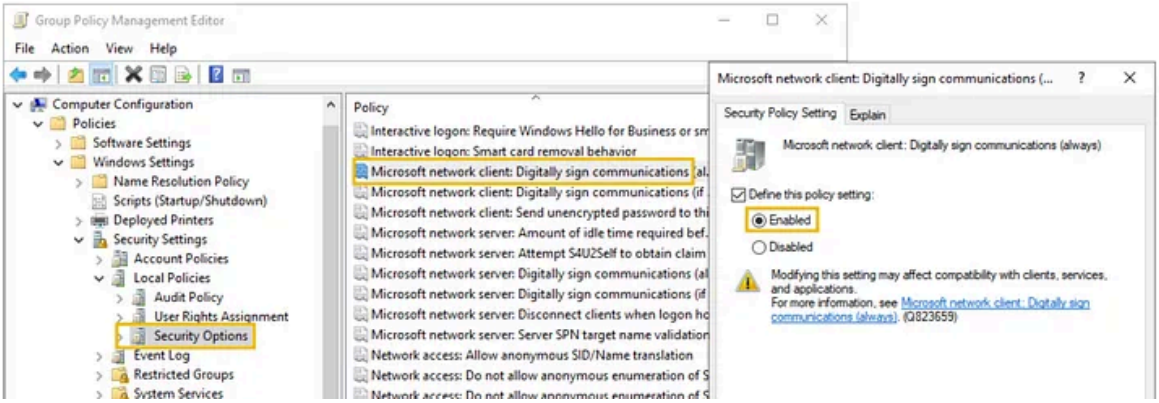
```
Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options >
double click Network security - Do not store LM hash value on next password change policy > select "Define policy setting"
```



SMB Signing

SMB stands for Server Message Block. Generally, Microsoft-based networks utilise this protocol for file and print communication. Moreover, it allows secure transmission over the network. Configuring SMB signing through group policy is crucial to detect Man in the Middle (MiTM) attacks that may result in modification of SMB traffic in transit. SMB signing ensures the integrity of data for both client and server. All supported Windows versions have an SMB packet signing option.

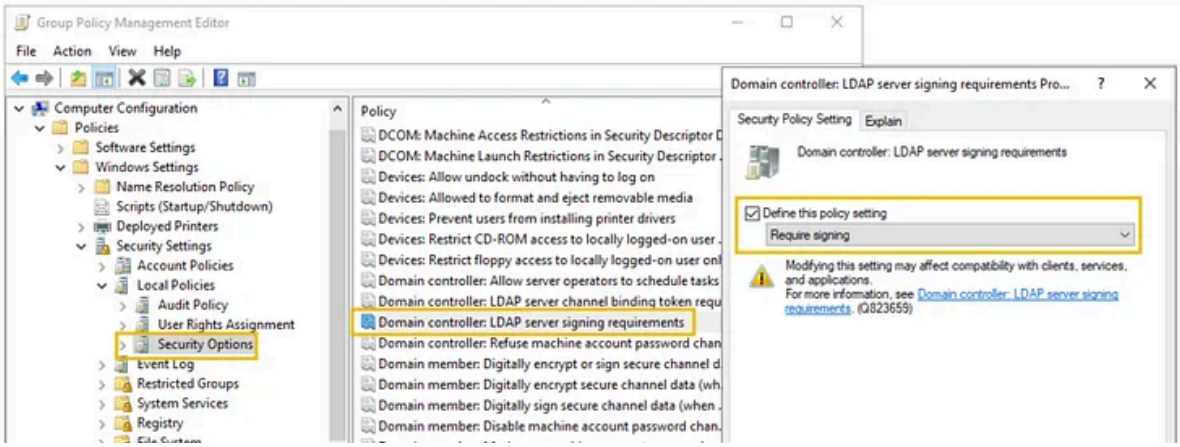
```
Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options >
double click Microsoft network server: Digitally sign communication (always) > select Enable Digitally Sign Communications
```



LDAP Signing

Light Weight Directory Access Protocol (LDAP) enables locating and authenticating resources on the network. Hackers may introduce replay or MiTM attacks to launch custom LDAP requests. Therefore, LDAP signing is a Simple Authentication and Security Layer (SASL) property that only accepts signed LDAP requests and ignores other requests (plain-text or non-SSL). We can enable LDAP signing through the following:

```
Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options >
Domain controller: LDAP server signing requirements > select Require signing from the dropdown
```



Password Rotation

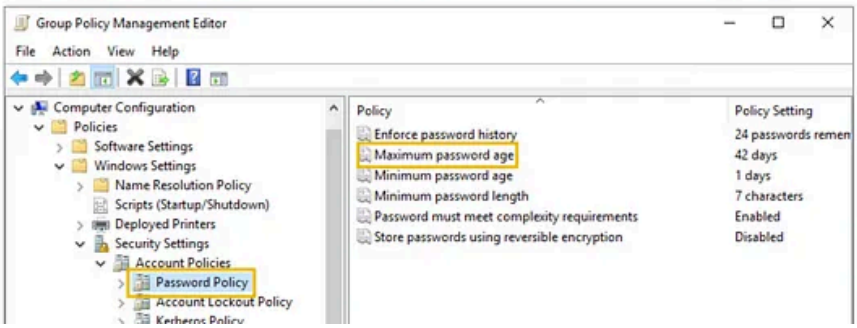
Active Directory password security is critical to address because of security breaches and password reuse. It becomes challenging for any organisation to reset account passwords or update them everywhere, so they prefer not to do it. This scenario could have a few alternate approaches, and each method has pros and cons.

- **First Technique:** Creating a script to update passwords automatically in the Scheduled Task with the help of PowerShell. This method does not require any additional overhead and removes all the manual efforts for password rotation, but it requires you to write and maintain your script – which could be challenging.
- **Second Technique:** Add a Multi-Factor Authentication (MFA) solution to AD and choose not to change the password often. It adds a security layer, and you will not need to change your password often. You can read more about implementing MFA here.
- **Third Technique:** Microsoft provides a solution for services account password rotation through Group Managed Services Accounts (gMSAs), which changes passwords after every 30 days. You can learn more about it here.

Password Policies

Attackers use various corporate password-compromise techniques, including brute force, dictionary, password spraying, credential attacks etc. All organisations must have a strict password policy to defend against all such attacks. Password policies mean different rules for creating passwords, including length, complexity, and changing frequency. For viewing and configuring the password policy, you can use the following:

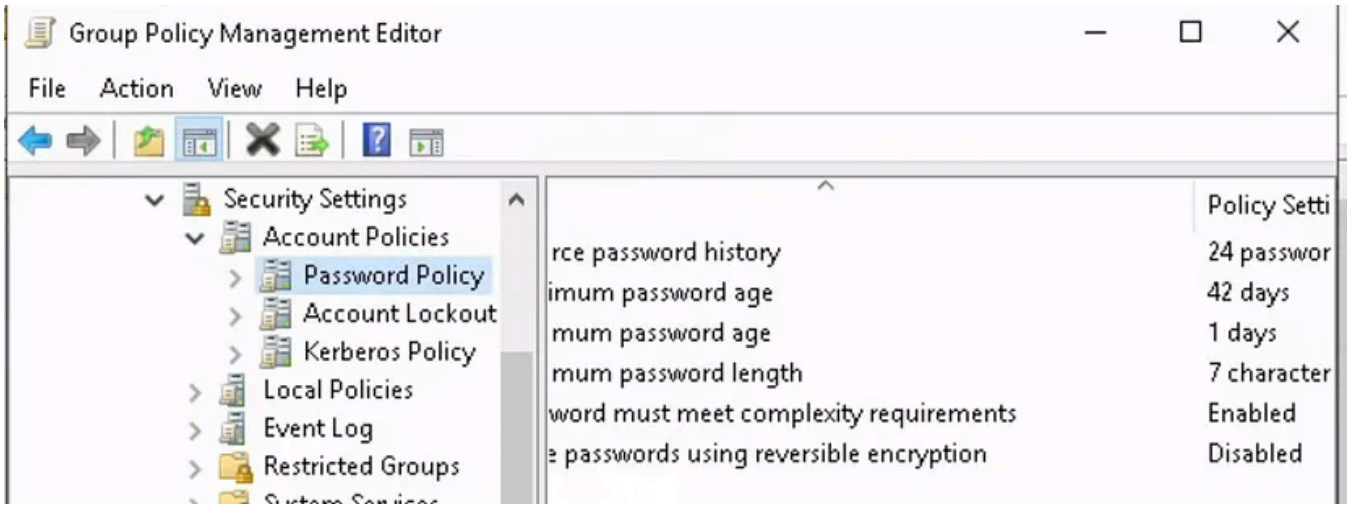
```
Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy
```



Understanding Password Policy Settings

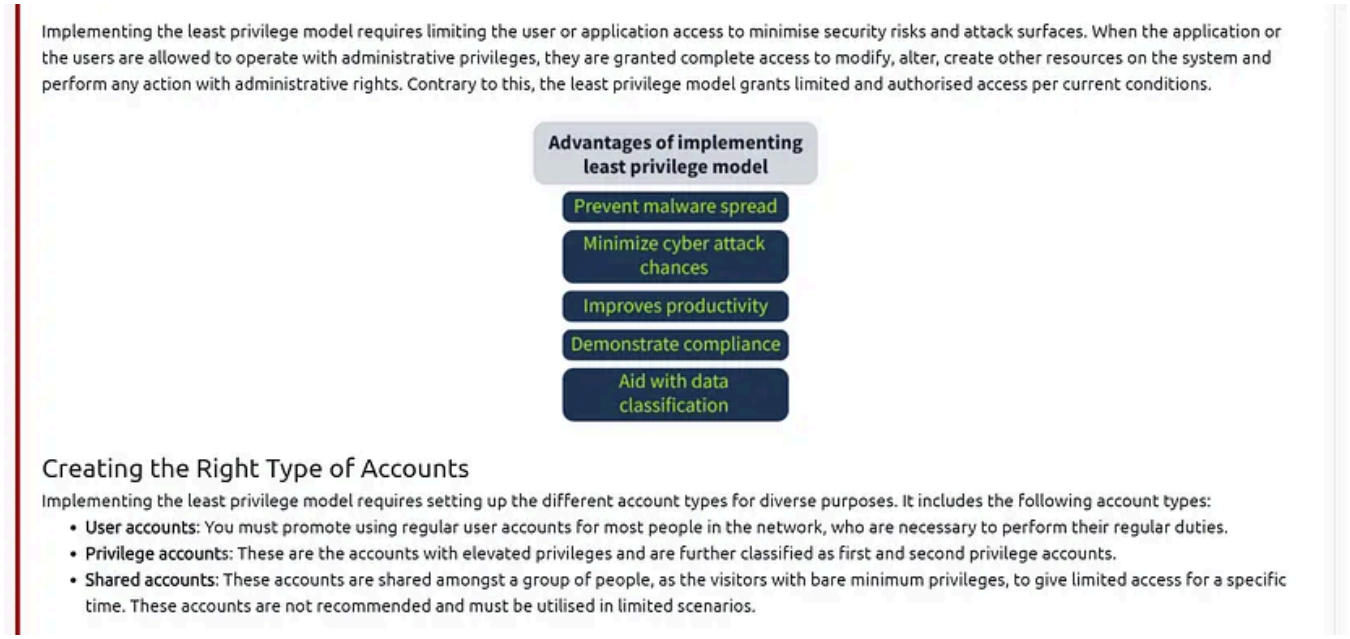
- **Enforce password history:** Prevent at least 10 to 15 old passwords from being set as new ones.
- **Minimum password length:** The minimum password length should be set between 10 to 14.
- **Complexity requirements:** Must not contain the name of the user account and ensure the password has uppercase letters, lowercase letters, digits, or special characters.

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



Answer: 7

Task 4: **Implementing Least Privilege Model**



Role-Based Access Control on Hosts

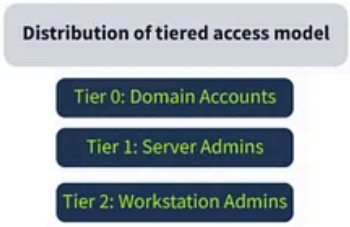
As a System Administrator, it is of utmost importance to grant rights to resources while keeping the principle of Least privilege in mind, which states that:
Per Wikipedia, "*The principle of minimal privilege or the principle of least authority, requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose*".

Role-based access control allows you to indicate access privileges at different levels. It includes DNS zone, server, or resource record levels and specifies who has access control over creating, editing, and deleting operations of various resources of Active Directory.

Tiered Access Model

The Active Directory Tiered Access Model (TAM) comprises plenty of technical controls that reduce the privilege escalation risks. It consists of a logical structure that separates Active Directory's assets by creating boundaries for security purposes. The primary goal is the protection of Active Directory's top-valued identities (Tier 0). At the same time, domain members and other users can perform routine tasks, such as email checking, surfing the internet, and using apps and other services (Tier 1, 2). It comprises three tiers, Tier 0, 1, and 2, which are as follows:

- **Tier 0**: Top level and includes all the admin accounts, Domain Controller, and groups.
- **Tier 1**: Domain member applications and servers.
- **Tier 2**: End-user devices like HR and sales staff (non-IT personnel).



Implementation of Tiered Access Model

The critical implementation of this model is based on the principle of *"Prevention of privileged credentials from crossing boundaries, either accidentally or intentionally"*. Implementing technical controls via Group Policy Objects is crucial to avoid such scenarios. These Group Policy Objects put together the security rights that can deny access or grant permission. You can read more about the Tiered and Enterprise Access Model (EAM) here.

Auditing Accounts

Accounts audit is a crucial task mainly carried out by setting up the correct account, assigning privileges, and applying restrictions. Three audit types related to accounts must be done periodically: usage, privilege, and change audits.

- Usage audits allow monitoring each account's specific tasks and validating their access rights.
- A privilege audit allows you to check if every account in the system has the least privilege.
- Change audits allow you to look for any improper changes to account permissions, passwords, or settings. Any unacceptable change to these may lead to a data breach.

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

Answer: **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?

Answer: **Nay**

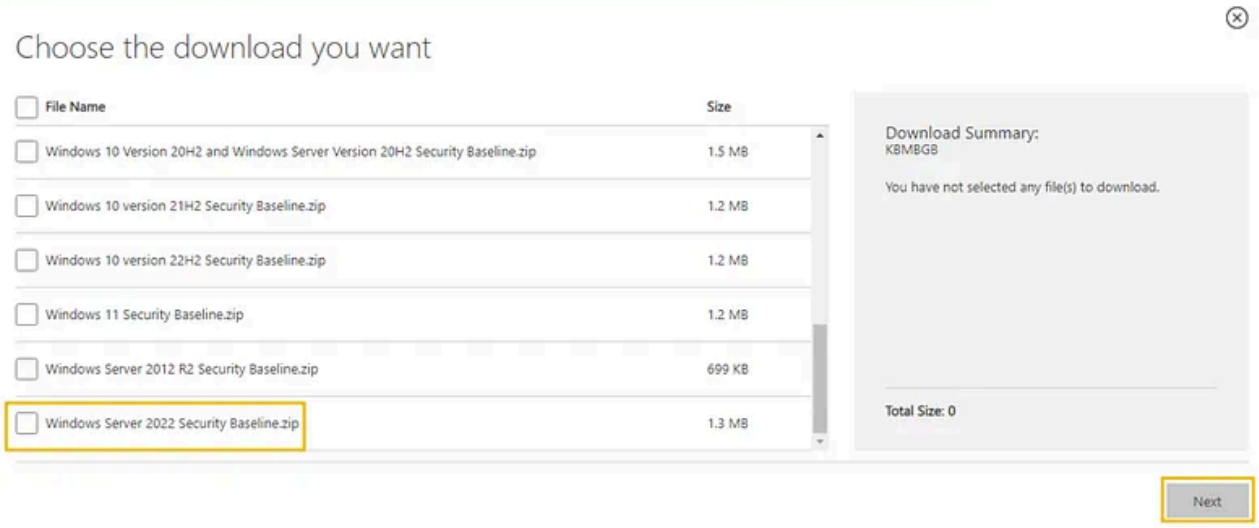
Task 5: **Microsoft Security Compliance Toolkit**

Microsoft Security Compliance Toolkit (MSCT) is an official toolkit provided by Microsoft to implement and manage local and domain-level policies. You don't have to worry about complex policy syntaxes and scripts, as Microsoft will provide pre-developed security baselines per the end user environment. You can download MSCT from the official Microsoft website link. You can find all the baselines and policy analyser software on `Desktop > Scripts` of the attached VM.

Installing Security Baselines

Microsoft offers its customers security baselines readily available in consumable formats, like, Group Policy Objects Backups. You can easily download it as zip files and extract the content. Here is how you can download and install the security baselines for Windows Server in a simple way:

```
Open Microsoft Security Compliance Website > click Download > click Windows Servers Security Baseline.zip > Download
```

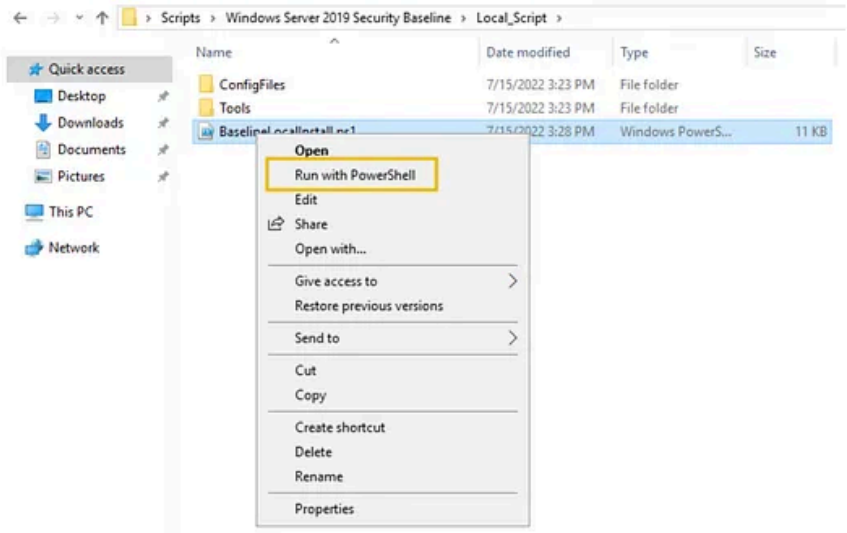


Download Security Compliance Toolkit and Baselines from Official Microsoft Download Center

This set of tools allows enterprise security administrators to download, analyze, test, edit and store...

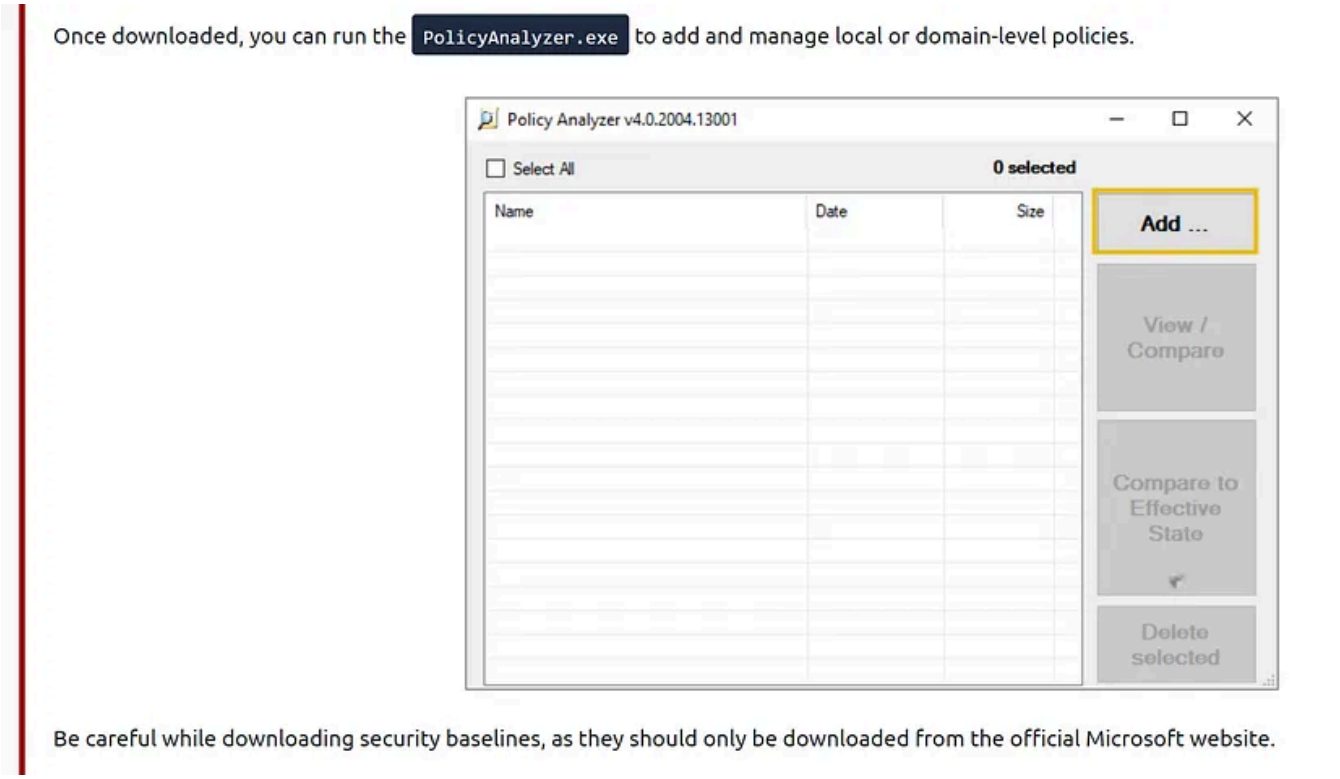
www.microsoft.com

```
Open extracted folder > Scripts > & select desired baseline & execute with PowerShell
```

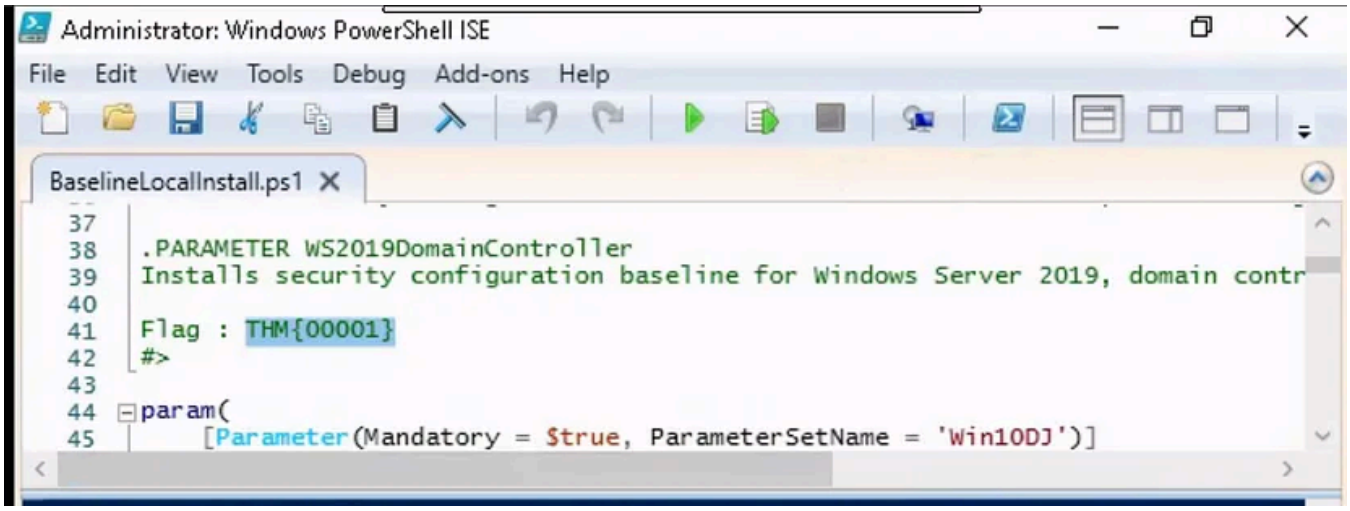


Policy Analyser

One of the Security Compliance ToolKit's features is a policy analyser which allows comparison of group policies to quickly check inconsistencies, redundant settings, and the alterations that need to be made between them. Consider a scenario where plenty of GPOs are applied at diverse levels. There will be conflicting, redundant settings and many more avenues that can be quickly resolved with a policy analyser. Same as security baselines, it is downloaded as a zip file from the same link, and one can easily extract the content and then follow the procedure, as shown in the following steps:

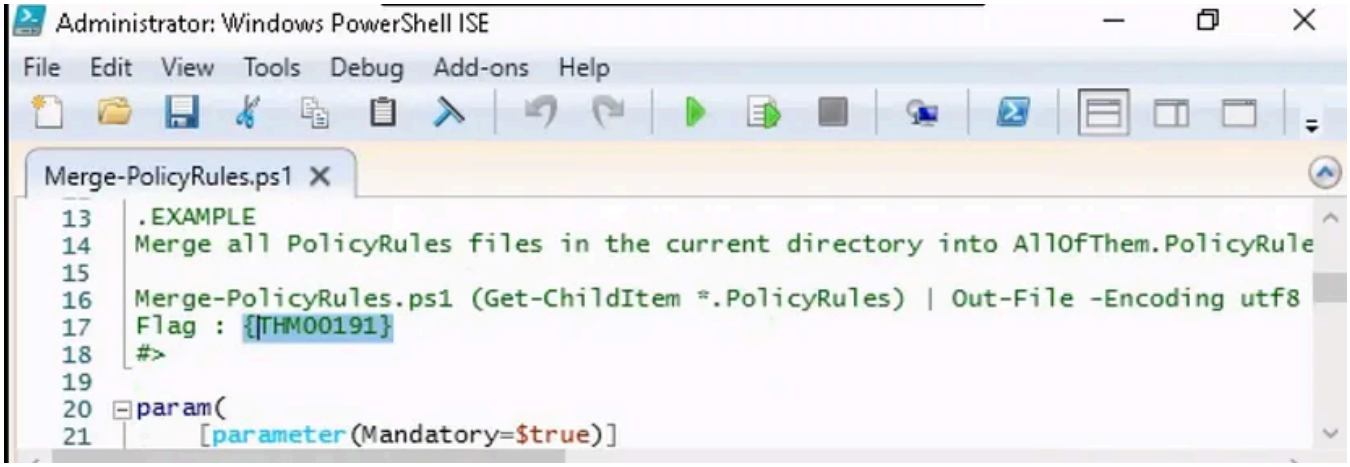


Find and open **BaselineLocalInstall** script in PowerShell editor — Can you find the flag?



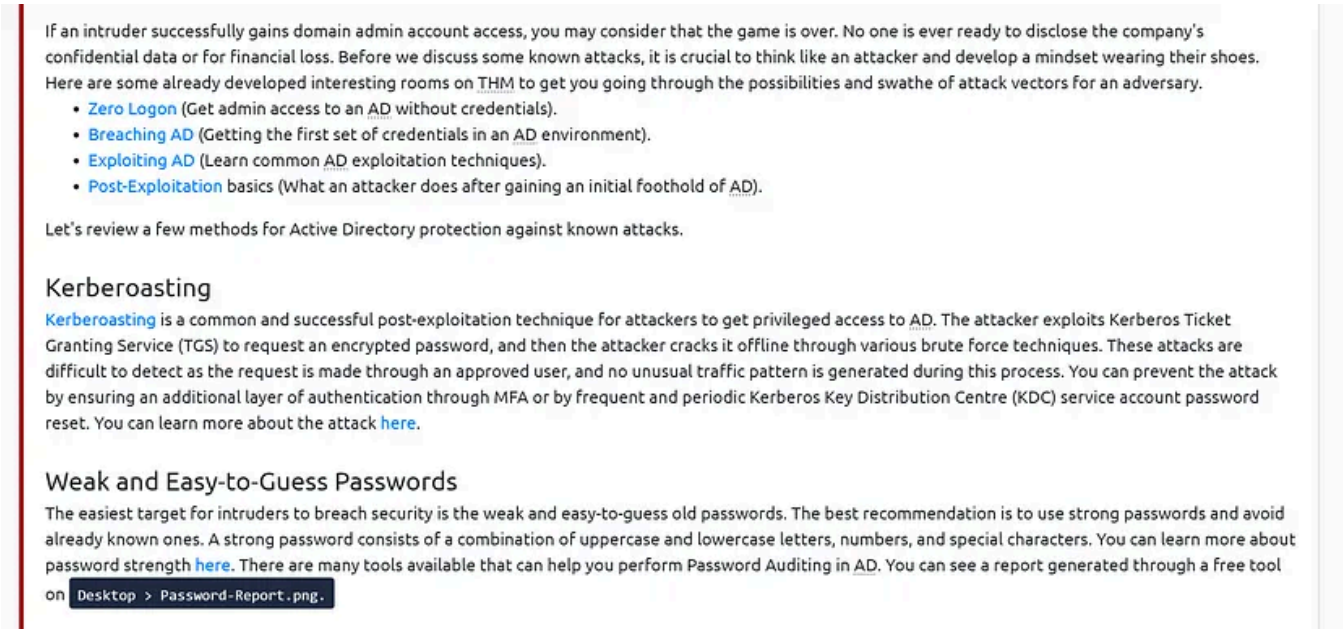
Answer: **THM{00001}**

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



Answer: **{THM00191}**

Task 6: **Protecting Against Known Attacks**


If an intruder successfully gains domain admin account access, you may consider that the game is over. No one is ever ready to disclose the company's confidential data or for financial loss. Before we discuss some known attacks, it is crucial to think like an attacker and develop a mindset wearing their shoes. Here are some already developed interesting rooms on THM to get you going through the possibilities and swathe of attack vectors for an adversary.

- Zero Logon (Get admin access to an AD without credentials).
- Breaching AD (Getting the first set of credentials in an AD environment).
- Exploiting AD (Learn common AD exploitation techniques).
- Post-Exploitation basics (What an attacker does after gaining an initial foothold of AD).

Let's review a few methods for Active Directory protection against known attacks.

Kerberoasting

Kerberoasting is a common and successful post-exploitation technique for attackers to get privileged access to AD. The attacker exploits Kerberos Ticket Granting Service (TGS) to request an encrypted password, and then the attacker cracks it offline through various brute force techniques. These attacks are difficult to detect as the request is made through an approved user, and no unusual traffic pattern is generated during this process. You can prevent the attack by ensuring an additional layer of authentication through MFA or by frequent and periodic Kerberos Key Distribution Centre (KDC) service account password reset. You can learn more about the attack here.

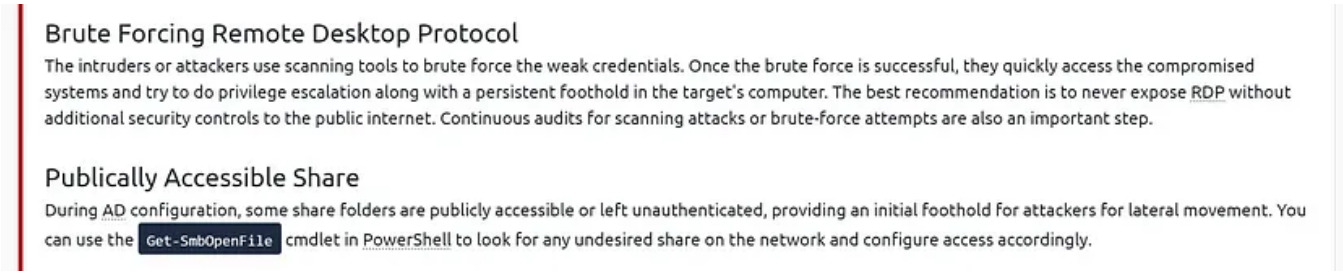
Weak and Easy-to-Guess Passwords

The easiest target for intruders to breach security is the weak and easy-to-guess old passwords. The best recommendation is to use strong passwords and avoid already known ones. A strong password consists of a combination of uppercase and lowercase letters, numbers, and special characters. You can learn more about password strength here. There are many tools available that can help you perform Password Auditing in AD. You can see a report generated through a free tool on `Desktop > Password-Report.png.`

Combined password policy and check for weak passwords in Azure Active Directory - Microsoft Entra

Learn about the combined password policy and check for weak passwords in Azure Active Directory

learn.microsoft.com


Brute Forcing Remote Desktop Protocol

The intruders or attackers use scanning tools to brute force the weak credentials. Once the brute force is successful, they quickly access the compromised systems and try to do privilege escalation along with a persistent foothold in the target's computer. The best recommendation is to never expose RDP without additional security controls to the public internet. Continuous audits for scanning attacks or brute-force attempts are also an important step.

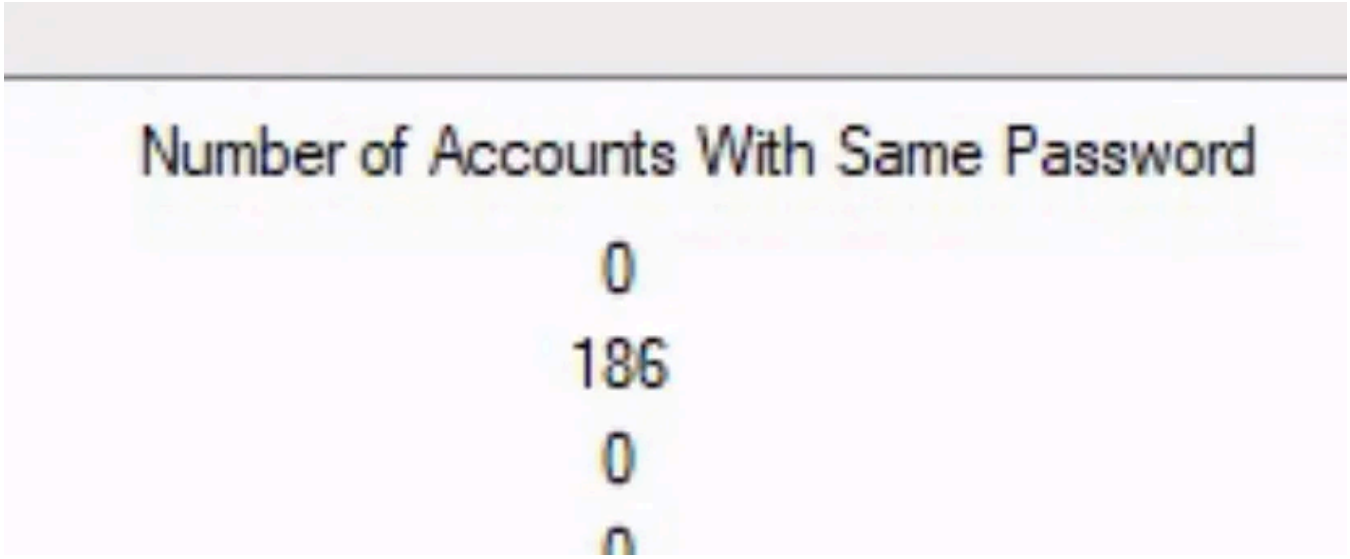
Publically Accessible Share

During AD configuration, some share folders are publicly accessible or left unauthenticated, providing an initial foothold for attackers for lateral movement. You can use the `Get-SmbOpenFile` cmdlet in PowerShell to look for any undesired share on the network and configure access accordingly.

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

Answer: **Yea**

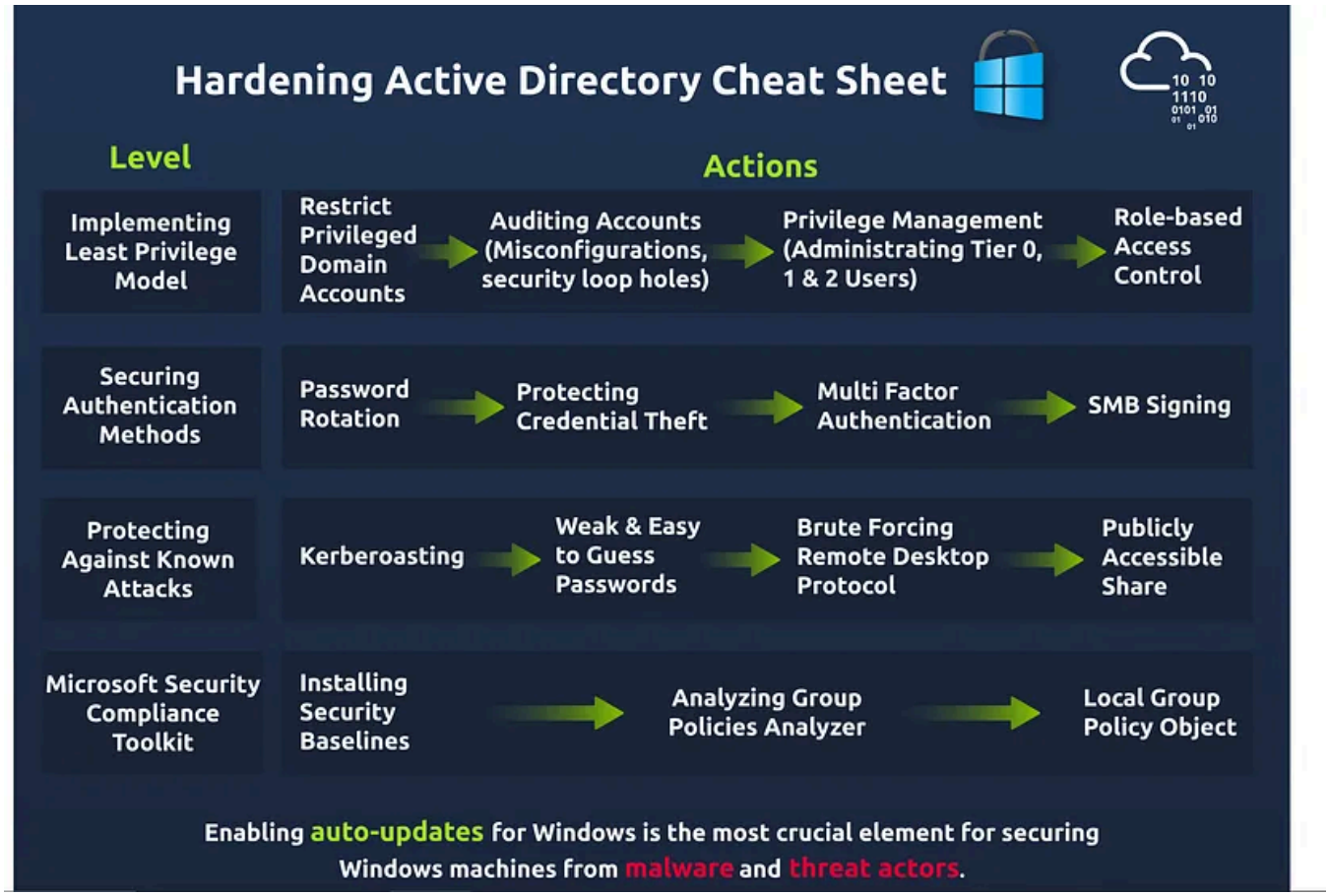
As per the generated report, how many users have the same password as aaron.booth?



Answer: **186**

Task 7: **Windows Active Directory Hardening Cheat Sheet**

> Are you sure your AD is secure from all types of attacks?
>
> Hardening of an AD is a continuous process and demands collective efforts by System Administrators and end-users. There have been various system hardening standards, and we discussed a few in this room. Below is a quick summary of the hardening techniques that will enable System Administrators to harden AD quickly.



Tryhackme Walkthrough Tryhackme Writeup

Follow

Written by Daniel Schwarzentraub

116 Followers · 4 Following

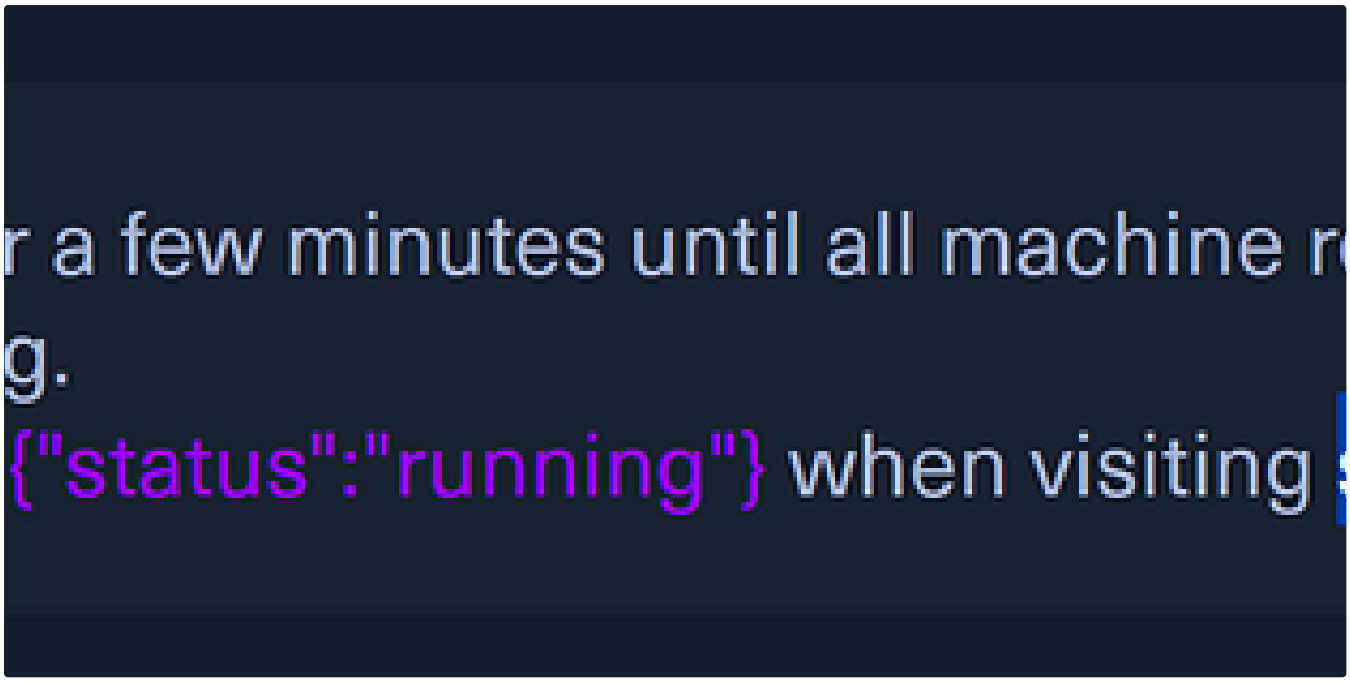
PNW_Hacker

No responses yet

What are your thoughts?

Respond

More from Daniel Schwarzentraub

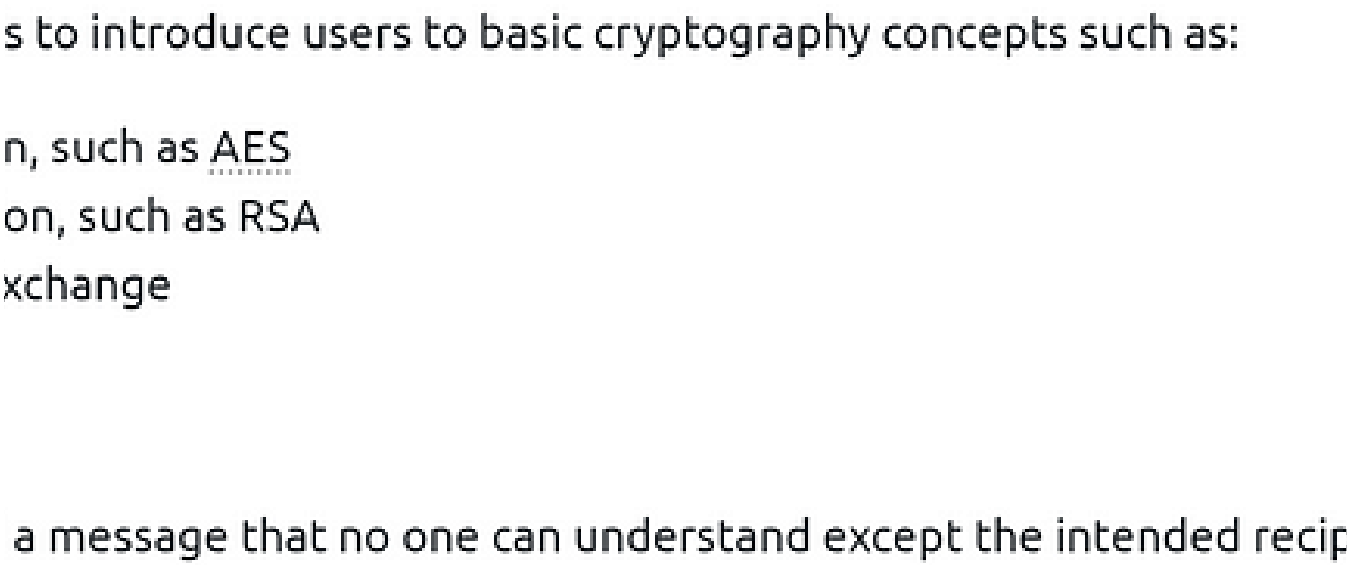


Daniel Schwarzentraub

HTB—Tier 1 Starting Point: Three

HTB—Tier 1 Starting Point: Three

Jul 20, 2023 4 2

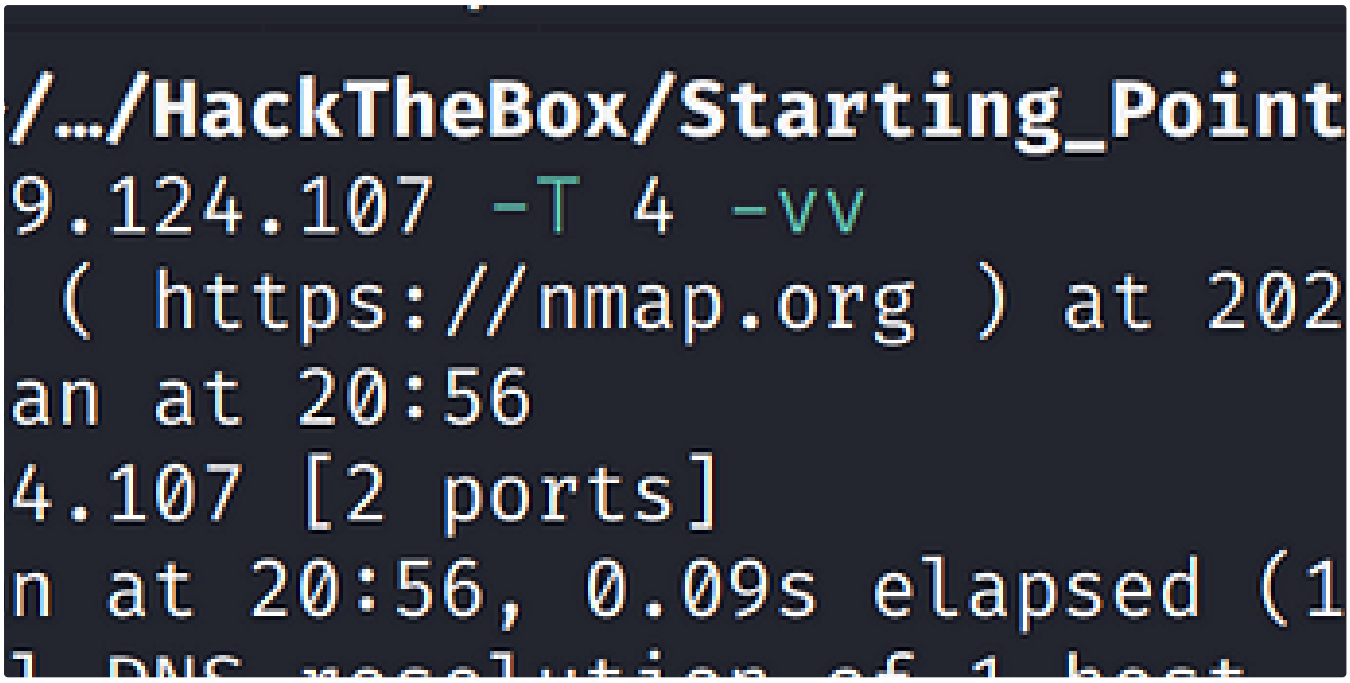


Daniel Schwarzentraub

Tryhackme: Introduction to Cryptography

Tryhackme: Introduction to Cryptography

Sep 26, 2023 2



Daniel Schwarzentraub

HTB—Tier 2 Starting Point: Archetype

HTB—Tier 2 Starting Point: Archetype

Jul 21, 2023

erative that we understand and can protect against common attacks.

mon techniques used by attackers to target people online. It will also teach some of the best wa

Daniel Schwarzentraub

Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024

See all from Daniel Schwarzentraub

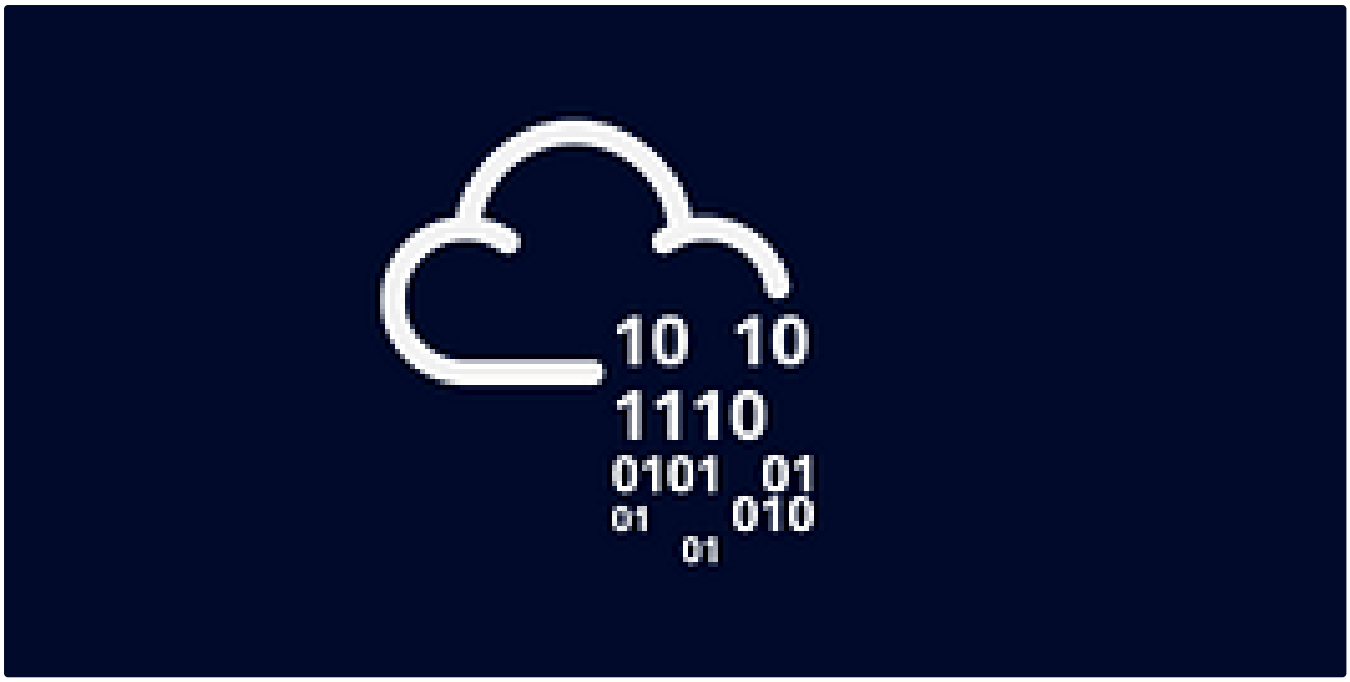
Recommended from Medium

Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

Sep 7, 2024 10



In T3CH by Axoloth

TryHackMe | AD Certificate Templates | WriteUp

Walkthrough on the exploitation of misconfigured AD certificate templates

Sep 11, 2024 70

Lists

Staff picks

793 stories · 1549 saves

Stories to Help You Level-Up at Work

19 stories · 909 saves

Self-Improvement 101

20 stories · 3184 saves

Productivity 101

20 stories · 2698 saves

In T3CH by Axoloth

TryHackMe | Search Skills | WriteUp

Learn to efficiently search the Internet and use specialized search engines and technical docs

Oct 26, 2024 61

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

erative that we understand and can protect against common attacks.

mon techniques used by attackers to target people online. It will also teach some of the best wa

Daniel Schwarzentraub

Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024

See more recommendations