12.6.2 Polityka haseł w domenie

Cel ogólny:

Nauczyć się konfigurowania różnych zasad haseł dla różnych grup użytkowników w domenie oraz przeprowadzać audyt polityki haseł.

Cele szczegółowe:

1. Konfiguracja zasad haseł dla różnych grup użytkowników:
   a. Utworzenie nowych grup użytkowników w Active Directory, takich jak "Zarząd" i "Pracownicy".
   b. Skonfigurowanie różnych zasad haseł dla każdej z tych grup za pomocą obiektów PSO (Password Settings Object).
   c. Przypisanie odpowiednich PSO do każdej grupy i przetestowanie czy zasady są poprawnie stosowane.
2. Implementacja polityki haseł z wykorzystaniem PowerShell:
   a. Napisanie skryptu PowerShell, który automatycznie konfiguruje zasady haseł i blokady konta zgodnie z wymaganiami.
   b. Uruchomienie skryptu na kontrolerze domeny i sprawdzenie czy zasady zostały poprawnie zastosowane.
   c. Modyfikacja skryptu, aby uwzględniał różne zasady dla różnych grup użytkowników.
3. Audyt polityki haseł:
   a. Skonfigurowanie narzędzi do monitorowania i raportowania zgodności z polityką haseł, np. za pomocą narzędzi wbudowanych w Windows Server lub dodatkowego oprogramowania.
   b. Przeprowadzenie audytu bieżących ustawień haseł i blokady konta.
   c. Sporządzenie raportu z wynikami audytu i zaproponowanie ewentualnych poprawek.

Przed przystąpieniem do ćwiczenia sprawdź i ustaw

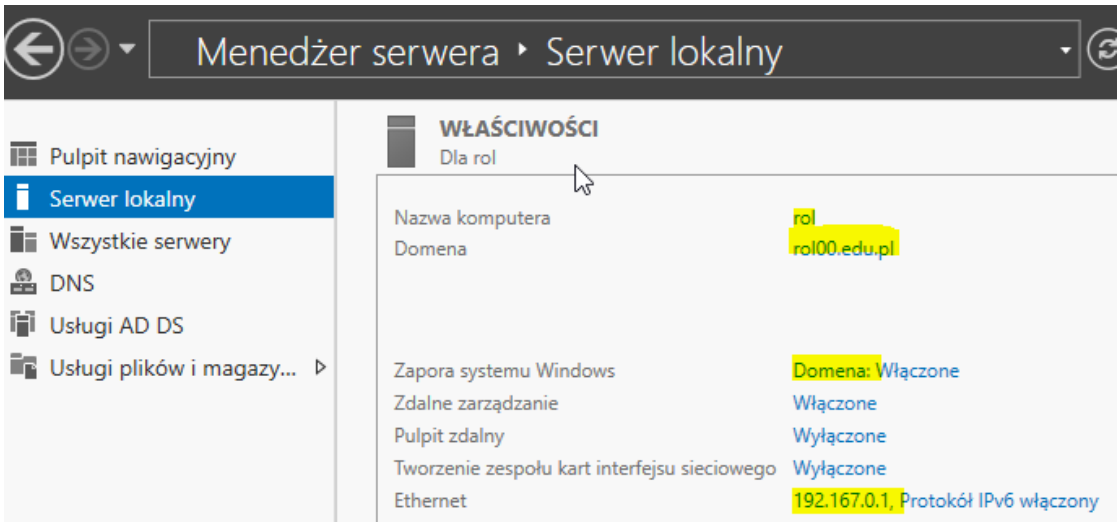
W Menedżer funkcji Hyper-V wybierz nazwa maszynę wirtualna twojej grupy_dc2019

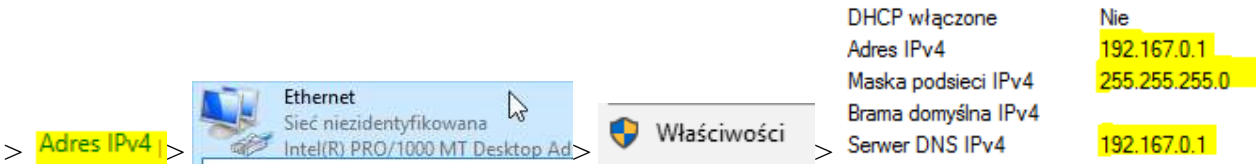
Upewnij się, że punk kontrolny, zawiera serwer z zainstalowanym kontrolerem domeny.

Przed przystąpieniem do ćwiczenia sprawdź i ustaw, jeśli to konieczne

Uruchom maszynę > Ctrl+Delete > Administrator > zaq1@WSX

system serwera są jak poniżej:





W zeszycie opisz procedury tworzenie polityki haseł w domenie.

Zadanie 1: Konfiguracja zasad haseł dla różnych grup użytkowników

Cel: Nauczyć się konfigurowania różnych zasad haseł dla różnych grup użytkowników w domenie.

Kroki:

- Utwórz dwie nowe grupy użytkowników w Active Directory, np. "Zarząd" i "Pracownicy".
- Skonfiguruj różne zasady haseł dla każdej z tych grup za pomocą obiektów PSO.
- Przypisz odpowiednie PSO do każdej grupy i przetestuj, czy zasady są poprawnie stosowane.

Szczegółowo czynności:

1. Utworzenie nowych grup użytkowników w Active Directory:
   - Otwórz przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
   - Rozwiń drzewo domeny i kliknij prawym przyciskiem myszy kontener Users.
   - Wybierz New (Nowy), a następnie Group (Grupa).
   - Utwórz grupę o nazwie "Zarząd":
     - W polu Group name (Nazwa grupy) wpisz "Zarząd".
     - Wybierz Group scope (Zakres grupy) jako Global (Globalna).
     - Wybierz Group type (Typ grupy) jako Security (Zabezpieczeń).
     - Kliknij OK.
   - Utwórz grupę o nazwie "Pracownicy":
     - Powtórz powyższe kroki, wpisując "Pracownicy" jako nazwę grupy.
2. Skonfigurowanie różnych zasad haseł dla każdej z grup za pomocą obiektów PSO:
   - Otwórz ADSI Edit (Edytor ADSI) z folderu Administrative Tools (Narzędzia administracyjne).
   - Kliknij prawym przyciskiem myszy ADSI Edit i wybierz Connect to (Połącz z).
   - W polu Name (Nazwa) pozostaw domyślną wartość i kliknij OK.
   - Rozwiń węzeł CN=System i zaznacz CN=Password Settings Container.
   - Kliknij prawym przyciskiem myszy Password Settings Container, wybierz New (Nowy), a następnie Object (Obiekt).
   - W oknie dialogowym Create Object (Tworzenie obiektu) wybierz msDS-PasswordSettings i kliknij Next (Dalej).
   - Według tabeli poniżej skonfiguruj PSO dla grupy "Zarząd",

- Według tabeli poniżej skonfiguruj PSO dla grupy " Pracownicy" wpisz wartości z tabeli dla grupy "Zarząd", a następnie zmodyfikuj na te dla grupy " Pracownicy", ustal których zmodyfikować nie możesz i za co odpowiadają te wartości:

Tabela porównawcza zasad PSO dla grup Zarząd i Pracownicy:

Parametr	Zarząd	Pracownicy	Opis funkcji
msDS-PasswordSettingsPrecedence	1	2	Priorytet PSO – niższa wartość oznacza wyższy priorytet
msDS-PasswordReversibleEncryptionEnabled	False	False	Czy hasła mogą być przechowywane w formie odwracalnej
msDS-PasswordHistoryLength	24	12	Liczba zapamiętanych poprzednich haseł
msDS-PasswordComplexityEnabled	True	True	Wymuszenie złożoności hasła
msDS-MinimumPasswordLength	12	8	Minimalna długość hasła
msDS-MinimumPasswordAge	1:00:00:00	0:00:00:00	Minimalny czas przed zmianą hasła
msDS-MaximumPasswordAge	30:00:00:00	60:00:00:00	Maksymalny czas ważności hasła
msDS-LockoutThreshold	5	10	Liczba nieudanych prób logowania przed blokadą
msDS-LockoutObservationWindow	0:00:30:00	0:01:00:00	Okno czasowe dla zliczania prób logowania
msDS-LockoutDuration	0:00:30:00	0:00:15:00	Czas trwania blokady konta

Na podstawie tabeli przeanalizuj różnice w politykach haseł. Zwróć uwagę na parametry: długość hasła, historia haseł, czas ważności, próg blokady konta. W zeszycie opisz, które ustawienia są bardziej restrykcyjne i dlaczego.

3. Przypisanie odpowiednich PSO do każdej grupy i testowanie zasad:
- Otwórz przystawkę Active Directory Users and Computers.
- Rozwiń domenę i kliknij kontener Users.
- Kliknij prawym przyciskiem myszy grupę Zarząd i wybierz Properties (Właściwości).
- Przejdź do zakładki Attribute Editor (Edytor atrybutów).
- Znajdź atrybut msDS-PSOAppliesTo i kliknij Edit (Edytuj).

Jeśli atrybut msDS-PSOAppliesTo nie jest widoczny w Edytorze Atrybutów Dodaj atrybut ręcznie:

a. W ADSI Edit, przejdź do CN=Password Settings Container,CN=System,DC=TwojaDomena,DC=pl.
b. Znajdź odpowiedni PSO (np. CN=PSO_Zarząd).
c. Kliknij prawym przyciskiem myszy i wybierz Properties.
d. Znajdź msDS-PSOAppliesTo i dodaj odpowiednią wartość (np. CN=Zarząd,CN=Users,DC=TwojaDomena,DC=pl).
e. W polu Value (Wartość) wpisz CN=PSO_Zarząd,CN=Password Settings Container,CN=System,DC=TwojaDomena,DC=pl i kliknij OK.

- Powtórz powyższe kroki dla grupy Pracownicy, wpisując odpowiednią wartość dla PSO_Pracownicy. Udokumentuj dowody wykonania.
- Przetestuj zasady:
  - Zaloguj się na konto użytkownika należącego do grupy **Zarząd** i spróbuj zmienić hasło, aby sprawdzić, czy zasady są stosowane. Udokumentuj dowody wykonania.
  - Powtórz test dla użytkownika należącego do grupy **Pracownicy**.
- Przetestuj polecenia PowerShell do weryfikacji przypisania PSO

Get-ADFineGrainedPasswordPolicy

Get-ADFineGrainedPasswordPolicySubject -Identity "PSO_Zarząd"

Te kroki powinny pomóc w skonfigurowaniu i przetestowaniu różnych zasad haseł dla różnych grup użytkowników w domenie. Udokumentuj dowody wykonania.

Przedstaw wyniki twojego działania.

Zgłoszenie 1

Zadanie 2: Implementacja polityki haseł z wykorzystaniem PowerShell

Cel: Nauczyć się konfigurowania polityki haseł za pomocą skryptów PowerShell.

Kroki:

- Napisz skrypt PowerShell, który automatycznie konfiguruje zasady haseł i blokady konta zgodnie z wymaganiami. Działa tylko na poziomie domeny, nie na grupach.
- Uruchom skrypt na kontrolerze domeny i sprawdź, czy zasady zostały poprawnie zastosowane.
- Zmodyfikuj skrypt, aby uwzględniał różne zasady dla różnych grup użytkowników.

Szczegółowo czynności:

1. Napisz skrypt PowerShell, który automatycznie konfiguruje zasady haseł i blokady konta zgodnie z wymaganiami. Srypt PowerShell, który konfiguruje zasady haseł i blokady konta:

```
# Importowanie modułu Active Directory
Import-Module ActiveDirectory

# Konfiguracja zasad haseł
$domain = "DC=rol00,DC=edu,DC=pl"
$passwordPolicy = @{
    "MaxPasswordAge" = "30.00:00:00" # Maksymalny okres ważności hasła: 30 dni
    "MinPasswordLength" = 12 # Minimalna długość hasła: 12 znaków
    "PasswordHistoryCount" = 24 # Historia haseł: 24 poprzednie hasła
    "ComplexityEnabled" = $true # Wymuszenie skomplikowania hasła
}
```

```
# Konfiguracja zasad blokady konta
$lockoutPolicy = @{
    "LockoutThreshold" = 5 # Próg blokady konta: 5 nieudanych prób logowania
    "LockoutDuration" = "00:30:00" # Czas trwania blokady konta: 30 minut
    "LockoutObservationWindow" = "00:30:00" # Okno obserwacji blokady: 30 minut
}

# Zastosowanie zasad haseł
Set-ADDefaultDomainPasswordPolicy -Identity $domain @passwordPolicy

# Zastosowanie zasad blokady konta
Set-ADDefaultDomainPasswordPolicy -Identity $domain @lockoutPolicy

Write-Output "Zasady haseł i blokady konta zostały skonfigurowane."
```

2. Uruchom skrypt na kontrolerze domeny i sprawdź, czy zasady zostały poprawnie zastosowane:
   - Zapisz powyższy skrypt do pliku, np. KonfiguracjaZasad.ps1.
   - Otwórz PowerShell jako administrator na kontrolerze domeny.
   - Uruchom skrypt, wpisując w PowerShell:

```
.\KonfiguracjaZasad.ps1
```

   - Po uruchomieniu skryptu, sprawdź, czy zasady zostały poprawnie zastosowane, np. poprzez przystawkę Group Policy Management lub Active Directory Users and Computers.

3. Zmodyfikuj skrypt, aby uwzględniał różne zasady dla różnych grup użytkowników:

Aby skonfigurować różne zasady dla różnych grup użytkowników, musisz utworzyć obiekty PSO (Password Settings Object) i przypisać je do odpowiednich grup.

Obiekty o nazwach PSO_Zarząd i PSO_Pracownicy już istnieją w katalogu Active Directory. Możesz rozwiązać ten problem na kilka sposobów:

1. Usuń istniejące obiekty PSO: Jeśli chcesz usunąć istniejące obiekty i utworzyć je na nowo, możesz użyć poniższego skryptu:

```
# Importowanie modułu Active Directory
Import-Module ActiveDirectory

# Usuń istniejące obiekty PSO
Remove-ADFineGrainedPasswordPolicy -Identity "PSO_Zarząd"
```

```
Remove-ADFineGrainedPasswordPolicy -Identity "PSO_Pracownicy"

# Konfiguracja zasad haseł dla grupy Zarząd
$domain = "DC=rol00,DC=edu,DC=pl"
$policyZarzad = @{
    Name = "PSO_Zarząd"
    Precedence = 1
    MaxPasswordAge = "30.00:00:00" # Maksymalny okres ważności hasła: 30 dni
    MinPasswordLength = 12 # Minimalna długość hasła: 12 znaków
    PasswordHistoryCount = 24 # Historia haseł: 24 poprzednie hasła
    ComplexityEnabled = $true # Wymuszenie skomplikowania hasła
    ReversibleEncryptionEnabled = $false
    LockoutThreshold = 5 # Próg blokady konta: 5 nieudanych prób logowania
    LockoutDuration = "00:30:00" # Czas trwania blokady konta: 30 minut
    LockoutObservationWindow = "00:30:00" # Okno obserwacji blokady: 30 minut
}

# Tworzenie PSO dla grupy Zarząd
New-ADFineGrainedPasswordPolicy @policyZarzad

# Przypisanie PSO do grupy Zarząd
Add-ADFineGrainedPasswordPolicySubject -Identity "PSO_Zarząd" -Subjects
"CN=Zarząd,CN=Users,$domain"

# Konfiguracja zasad haseł dla grupy Pracownicy
$policyPracownicy = @{
    Name = "PSO_Pracownicy"
    Precedence = 2
    MaxPasswordAge = "60.00:00:00" # Maksymalny okres ważności hasła: 60 dni
    MinPasswordLength = 10 # Minimalna długość hasła: 10 znaków
    PasswordHistoryCount = 12 # Historia haseł: 12 poprzednich haseł
    ComplexityEnabled = $true # Wymuszenie skomplikowania hasła
    ReversibleEncryptionEnabled = $false
    LockoutThreshold = 7 # Próg blokady konta: 7 nieudanych prób logowania
```

```
    LockoutDuration = "00:15:00" # Czas trwania blokady konta: 15 minut
    LockoutObservationWindow = "00:15:00" # Okno obserwacji blokady: 15 minut
}

# Tworzenie PSO dla grupy Pracownicy
New-ADFineGrainedPasswordPolicy @policyPracownicy

# Przypisanie PSO do grupy Pracownicy
Add-ADFineGrainedPasswordPolicySubject -Identity "PSO_Pracownicy" -Subjects
"CN=Pracownicy,CN=Users,$domain"

Write-Output "Zasady haseł dla grup Zarząd i Pracownicy zostały skonfigurowane."
```

2. Zaktualizuj istniejące obiekty PSO: Jeśli chcesz zaktualizować istniejące obiekty PSO zamiast tworzyć nowe, możesz użyć poniższego skryptu:

```
# Importowanie modułu Active Directory
Import-Module ActiveDirectory

# Konfiguracja zasad haseł dla grupy Zarząd
$domain = "DC=rol00,DC=edu,DC=pl"
$policyZarzad = @{
    MaxPasswordAge = "30.00:00:00" # Maksymalny okres ważności hasła: 30 dni
    MinPasswordLength = 12 # Minimalna długość hasła: 12 znaków
    PasswordHistoryCount = 24 # Historia haseł: 24 poprzednie hasła
    ComplexityEnabled = $true # Wymuszenie skomplikowania hasła
    ReversibleEncryptionEnabled = $false
    LockoutThreshold = 5 # Próg blokady konta: 5 nieudanych prób logowania
    LockoutDuration = "00:30:00" # Czas trwania blokady konta: 30 minut
    LockoutObservationWindow = "00:30:00" # Okno obserwacji blokady: 30 minut
}

# Aktualizacja PSO dla grupy Zarząd
Set-ADFineGrainedPasswordPolicy -Identity "PSO_Zarząd" @policyZarzad
```

```
# Konfiguracja zasad haseł dla grupy Pracownicy
$policyPracownicy = @{
    MaxPasswordAge = "60.00:00:00" # Maksymalny okres ważności hasła: 60 dni
    MinPasswordLength = 10 # Minimalna długość hasła: 10 znaków
    PasswordHistoryCount = 12 # Historia haseł: 12 poprzednich haseł
    ComplexityEnabled = $true # Wymuszenie skomplikowania hasła
    ReversibleEncryptionEnabled = $false
    LockoutThreshold = 7 # Próg blokady konta: 7 nieudanych prób logowania
    LockoutDuration = "00:15:00" # Czas trwania blokady konta: 15 minut
    LockoutObservationWindow = "00:15:00" # Okno obserwacji blokady: 15 minut
}

# Aktualizacja PSO dla grupy Pracownicy
Set-ADFineGrainedPasswordPolicy -Identity "PSO_Pracownicy" @policyPracownicy

Write-Output "Zasady haseł dla grup Zarząd i Pracownicy zostały zaktualizowane."
```

Wybierz odpowiednią opcję w zależności od tego, czy chcesz usunąć i utworzyć nowe obiekty PSO, czy zaktualizować istniejące.

- Zapisz zmodyfikowany skrypt do pliku, np. KonfiguracjaZasadGrup.ps1.
- Uruchom skrypt na kontrolerze domeny, wpisując w PowerShell: powershell

.\KonfiguracjaZasadGrup.ps1

- Sprawdź, czy zasady zostały poprawnie zastosowane dla odpowiednich grup użytkowników.

Te kroki powinny pomóc w automatyzacji konfiguracji polityki haseł za pomocą skryptów PowerShell oraz w dostosowaniu zasad do różnych grup użytkowników. Udokumentuj dowody wykonania. Przedstaw wyniki twojego działania.

Zgłoszenie 2

Zadanie 3: Audyt polityki haseł

Cel: Nauczyć się przeprowadzać audyt polityki haseł w domenie.

Kroki:

1. Skonfiguruj narzędzia do monitorowania i raportowania zgodności z polityką haseł, np. za pomocą narzędzi wbudowanych w Windows Server lub dodatkowego oprogramowania.
2. Przeprowadź audyt bieżących ustawień haseł i blokady konta.
3. Sporządź raport z wynikami audytu i zaproponuj ewentualne poprawki.

Szczegółowo czynności:

A. Audyt polityki haseł i blokady konta za pomocą Group Policy Management Console (GPMC)

1. Otwórz Group Policy Management Console (GPMC):
   a. Kliknij przycisk Start.
   b. Wpisz Zarządzanie zasadami grupy i naciśnij Enter.
2. Przejdź do odpowiedniego obiektu zasad grupy (GPO):
   a. W lewym panelu rozwiń swoją domenę.
   b. Rozwiń Obiekty zasad grupy.
   c. Znajdź i kliknij prawym przyciskiem myszy Domyślna zasada domeny (lub inny GPO, który chcesz sprawdzić) i wybierz Edytuj.
3. Przejrzyj ustawienia polityki haseł:
   a. W oknie edytora GPO, przejdź do Konfiguracja komputera > Zasady > Ustawienia systemu Windows > Ustawienia zabezpieczeń > Zasady kont > Zasady haseł.
   b. Sprawdź ustawienia takie jak Maksymalny okres ważności hasła, Minimalna długość hasła, Hasło musi spełniać wymagania dotyczące złożoności, itp.
4. Przejrzyj ustawienia blokady konta:
   a. W tym samym oknie edytora GPO, przejdź do Zasady blokady konta.
   b. Sprawdź ustawienia takie jak Próg blokady konta, Czas trwania blokady konta, Resetowanie licznika blokady konta po.

- Active Directory Administrative Center (ADAC):
  - Umożliwia przeglądanie i zarządzanie obiektami PSO.
  - Otwórz ADAC, przejdź do Dynamic Access Control, a następnie do Password Settings Container.
  - Przeglądaj i edytuj obiekty PSO, aby upewnić się, że są zgodne z polityką haseł.

Audyt polityki haseł oraz ustawień blokady konta za pomocą Centrum administracyjnego usługi Active Directory (Active Directory Administrative Center – ADAC).

1. Otwórz Active Directory Administrative Center (ADAC):
   a. Kliknij przycisk Start.
   b. Wpisz Centrum administracyjne usługi Active Directory i naciśnij Enter.
2. Przejdź do kontenera Password Settings Container:
   a. W lewym panelu, rozwiń swoją domenę.
   b. Przejdź do System > Password Settings Container (Kontener ustawień haseł).
3. Przeglądaj i zarządzaj obiektami PSO:
   a. W kontenerze Kontener ustawień haseł znajdziesz wszystkie Fine-Grained Password Policies (PSO).

b. Kliknij prawym przyciskiem myszy na wybrany PSO i wybierz Właściwości, aby przeglądać i edytować jego ustawienia.

b. Dodatkowe oprogramowanie (dla chętnych ten podpunkt top na końcu jak już wszystko zrobisz, teraz pomiń b. i ewentualnie wróć na koniec):

- Microsoft Advanced Threat Analytics (ATA):
  - Monitoruje i analizuje aktywność w sieci, w tym zgodność z polityką haseł.
  - Konfiguracja ATA wymaga zainstalowania centrum ATA oraz bramki ATA, które będą zbierać i analizować dane.
- Specjalistyczne narzędzia audytowe:
  - Narzędzia takie jak Netwrix Auditor, LepideAuditor, czy ManageEngine ADAudit Plus oferują zaawansowane funkcje audytu i raportowania zgodności z polityką haseł.
  - Skonfiguruj wybrane narzędzie zgodnie z dokumentacją producenta, aby monitorować i raportować zgodność z polityką haseł.

B. Przeprowadź audyt bieżących ustawień haseł i blokady konta:

a. Audyt za pomocą PowerShell:

- Użyj poniższego skryptu PowerShell, aby wyświetlić bieżące ustawienia polityki haseł i blokady konta:

```
# Importowanie modułu Active Directory
Import-Module ActiveDirectory
# Pobranie bieżących ustawień polityki haseł
$domain = "DC=rol00,DC=edu,DC=pl"
$passwordPolicy = Get-ADDefaultDomainPasswordPolicy -Identity $domain
# Wyświetlenie ustawień polityki haseł
Write-Output "Bieżące ustawienia polityki haseł:"
Write-Output "Maksymalny okres ważności hasła: $($passwordPolicy.MaxPasswordAge)"
Write-Output "Minimalna długość hasła: $($passwordPolicy.MinPasswordLength)"
Write-Output "Historia haseł: $($passwordPolicy.PasswordHistoryCount)"
Write-Output "Wymuszenie skomplikowania hasła: $($passwordPolicy.PasswordComplexityEnabled)"
# Wyświetlenie ustawień blokady konta
Write-Output "Bieżące ustawienia blokady konta:"
Write-Output "Próg blokady konta: $($passwordPolicy.LockoutThreshold)"
Write-Output "Czas trwania blokady konta: $($passwordPolicy.LockoutDuration)"
 Write-Output "Okno obserwacji blokady: $($passwordPolicy.LockoutObservationWindow)"
```

b. Audyt za pomocą narzędzi wbudowanych:

- Otwórz Group Policy Management Console (GPMC) i przejdź do odpowiedniego obiektu zasad grupy (GPO).
- Przejrzyj ustawienia polityki haseł i blokady konta, aby upewnić się, że są zgodne z wymaganiami.
- Użyj Active Directory Administrative Center (ADAC), aby przeglądać i zarządzać obiektami PSO.

C. Sporządź raport z wynikami audytu i zaproponuj ewentualne poprawki:

a. Sporządzenie raportu:

- Zbierz dane z audytu, w tym bieżące ustawienia polityki haseł i blokady konta.
- Użyj narzędzi takich jak Excel lub specjalistyczne oprogramowanie audytowe do stworzenia czytelnego raportu.

b. Analiza wyników:

- Porównaj bieżące ustawienia z wymaganiami polityki haseł.
- Zidentyfikuj wszelkie niezgodności lub obszary wymagające poprawy.

c. Propozycje poprawek:

- Na podstawie wyników audytu zaproponuj konkretne zmiany w ustawieniach polityki haseł i blokady konta.
- Przedstaw propozycje w formie pisemnej, wraz z uzasadnieniem i planem wdrożenia.

Przeprowadzenie audytu polityki haseł w domenie jest kluczowe dla zapewnienia bezpieczeństwa i zgodności z wymaganiami organizacji. Udokumentuj dowody wykonania.

Przedstaw wyniki twojego działania.

Zgłoszenie 3