Ćwiczenie 5b. Group Policy Object (GPO) cz 2.

Zadanie 1

1. Ala, Monika, Ewa, Iza, Agnieszka, Ania zostały zaangażowane dla programu testowego **KejaOnlyForWomen**.
2. Utwórz stosowną grupę globalną i dodaj konta ww. pracownic do tej grupy.
3. NA serwerze SVR1 utwórz folder c:**KejaOnlyForWomen** i udostępnij go dla grupy **KejaOnlyForWomen.** Członkowie ww. grupy powinni mieć możliwość modyfikacji zawartości folderu. Pozostali członkowie domeny nie powinni mieć dostępu do tego Folderu

4. Dla kont grupy **KejaOnlyForWomen powinny być wdrożone następujące GPO**
    - Właczony screen server
    - Czas 1 minuta
    - Screen server bubbles
    - Chroniony hasłem
    - DODAJ ewentualnie inne ustawienia

5. Pod literą **W** powinien być zmapowany folder utworzony w punkcie 3.

6. Polityka haseł dla **KejaOnlyForWomen** jest następująca:
    - Historia haseł 15
    - Maksymalny okres ważności hasła 30
    - Minimalny okres ważności hasła 2
    - Minimalna długość hasła 10
    - Hasła muszą spełniać wymogi co do złożoności

   UWAGI: Utwórz obiekt PSO

7. Przetestuj powyższe ustawienia dla kont ewa, iza , oraz upewnij się że pozostali nie mają wdrożonych powyższych ustawień. Przetestuj to na przykładzie konta **kuba**.

Uzupełnienie teoretyczne

1. Otwórz Active Directory Administrative Center (ADAC):
2. Przejdź do sekcji Password Settings Container:

- W lewej części okna ADAC znajdź swoją domenę i rozwiń jej widok.
- Rozwiń System.
- Znajdziesz folder o nazwie Password Settings Container – to tutaj są przechowywane wszystkie PSO.

Password Settings Object (PSO) to obiekt używany w **Active Directory (AD)**, który pozwala na przypisanie szczegółowych zasad dotyczących haseł i blokowania kont do konkretnych użytkowników lub grup użytkowników. Zasadniczo, PSO umożliwia wdrożenie różnych polityk haseł dla różnych grup użytkowników w tej samej domenie, co daje elastyczność większą niż domyślna polityka haseł przypisana do całej domeny (np. w **Default Domain Policy**).

Jak działa PSO:

1. **PSO** jest stosowany na poziomie konta użytkownika lub grupy zabezpieczeń.
2. Każdy **PSO** może określać:
    - Minimalną i maksymalną długość hasła,
    - Historię haseł (ile poprzednich haseł nie może być używanych),
    - Czas ważności hasła,
    - Wymogi dotyczące złożoności hasła,
    - Polityki blokady konta (np. ile razy można wpisać błędne hasło przed blokadą).

Priorytet PSO – Zasady dla użytkownika są ważniejsze niż dla grupy

Indywidualnie przypisany PSO ma wyższy priorytet niż PSO przypisany do grupy:

- Jeśli użytkownik ma przypisane różne PSO, zarówno bezpośrednio, jak i przez grupę, **zasady przypisane bezpośrednio do użytkownika mają wyższy priorytet** niż zasady przypisane do grup, nawet jeśli PSO dla grupy ma niższą wartość **precedence**.
- **Przykład**: Użytkownik **Ewa** ma przypisany PSO bezpośrednio do swojego konta z określonymi zasadami haseł. Ewa jest również członkiem grupy **Finance**, do której przypisano PSO z innymi zasadami. W takim przypadku zasady haseł przypisane bezpośrednio do Ewy mają pierwszeństwo nad tymi, które wynikają z członkostwa w grupie **Finance**.

Precedence (priorytet PSO):

- **Precedence** to wartość liczbową przypisaną do każdego PSO, która określa jego priorytet – **im niższa wartość**, tym **wyższy priorytet** PSO.
- W sytuacji, gdy użytkownik ma przypisane wiele PSO (np. przez kilka grup), **PSO o niższej wartości precedence** będzie miał pierwszeństwo.
- **Jednakże**, PSO przypisane bezpośrednio do użytkownika zawsze będzie miało **wyższy priorytet** niż jakiekolwiek PSO przypisane przez grupy, niezależnie od wartości **precedence**.

Przykład zastosowania PSO:

Użytkownik Ewa ma przypisany PSO bezpośrednio do jej konta, z ustawieniem:

- Minimalna długość hasła: 12 znaków.
- Maksymalny czas ważności hasła: 30 dni.

Grupa Finance, do której Ewa należy, ma przypisany inny PSO, z ustawieniem:

- Minimalna długość hasła: 8 znaków.