Podsumowanie wykonanych zadań:

1. **Konfigurowanie Domenowych Zasad Haseł i Blokady Konta:**

- Uczestnicy dostosowali obiekt zasad grupy "Default Domain Policy" w domenie "rol00.edu.pl" w celu wprowadzenia zasad haseł i blokady konta.

- Zmienili maksymalny okres ważności hasła na 90 dni, minimalną długość hasła na 10 znaków, oraz skonfigurowali blokadę konta po 5 nieudanych próbach logowania.

2. **Tworzenie Obiektu Ustawień Haseł (PSO):**

- Uczestnicy utworzyli obiekt PSO dla grupy "Domain Admins" z restrykcyjnymi zasadami haseł, takimi jak minimalna długość hasła 15 znaków, wymuszone reguły skomplikowania hasła, okres ważności hasła 45 dni, etc.

3. **Ustalanie Wynikowego Obiektu PSO dla Użytkownika:**

- Zidentyfikowali obiekt PSO, który określa zasady hasła i blokady konta dla konta "Administrator" na podstawie wynikowego obiektu PSO.

4. **Usuwanie Obiektu PSO:**

- Uczestnicy usunęli obiekt PSO utworzony wcześniej, eliminując jego wpływ na dalsze zadania.

Wnioski uczniów:

1. **Zarządzanie Politykami Haseł i Blokadą Konta:**

- "Teraz rozumiem, jak skonfigurować zasady haseł i blokady konta dla użytkowników w domenie. To istotne dla bezpieczeństwa systemu."

2. **Tworzenie Obiektu Ustawień Haseł (PSO):**

- "Utworzenie obiektu PSO dla grupy Domain Admins pozwoliło mi zastosować szczegółowe zasady haseł dla tej ważnej grupy użytkowników."

3. **Ustalanie Wynikowego Obiektu PSO dla Użytkownika:**

- "Przez zastosowanie obiektu PSO, mogę zobaczyć, jakie konkretne zasady haseł obowiązują dla danego użytkownika."

4. **Usuwanie Obiektu PSO:**

- "Usuwanie obiektu PSO było ważne, aby uniknąć konfliktów z zasadami haseł w kolejnych zadaniach. Teraz wiem, jak zarządzać tymi obiektami."

Podsumowując, uczniowie zdobyli praktyczne doświadczenie w konfiguracji polityk haseł i blokady konta w domenie, co umożliwi im skuteczne zarządzanie bezpieczeństwem w środowisku Windows Server.