

W sprawozdaniu zamieść zrzuty ekranu z istotnych etapów oraz odpowiedzi na pytania.



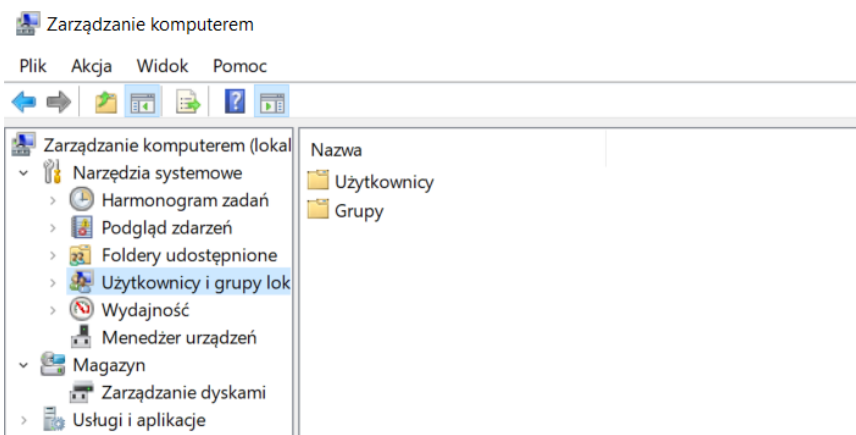
Taki symbol oznacza, że trzeba w sprawozdaniu dodać zrzut ekranu (najczęściej 1) z wyniku działania polecenie.



Taki symbol oznacza, że należy dodać opis (najczęściej 1 zdanie) z wyniku działania polecenia.

### I. Zarządzanie użytkownikami

- Przejdź do `win+x` -> zarządzanie komputerem -> Użytkownicy i grupy lokalne.



- Załącz konto o następujących parametrach:
  - login:** twój\_indeks,
  - hasło:** hasło dowolne,
  - użytkownik nie może zmienić hasła,
  - hasło nigdy nie wygasa.
- Dołącz konto do grupy `Użytkownicy zaawansowani`.
- Otwórz konsolę `cmd`.



- Za pomocą poniższej komendy wyświetl ustawienia konta dla utworzonego użytkownika:

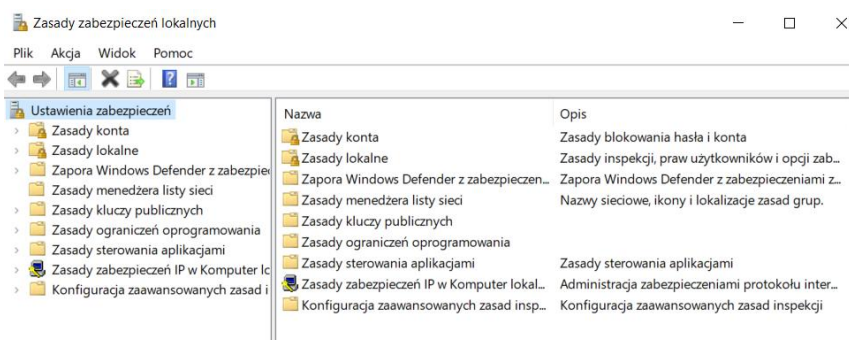
```
net user nazwa_konta
```

- Zaloguj się na utworzone konto.
- Przejdź do Zarządzaj kontem -> Opcje logowania -> Hasło.

-  8. Spróbuj zmienić hasło – operacja powinna być niemożliwa.
9. Wyloguj się.
10. Zaloguj się na konto główne.
11. Wróć do ppkt. 1.3, a następnie odznacz blokadę zmiany hasła przez użytkownika.
-  12. Spróbuj zmienić hasło po ponownym zalogowaniu się na konto użytkownika – tym razem powinno się udać.

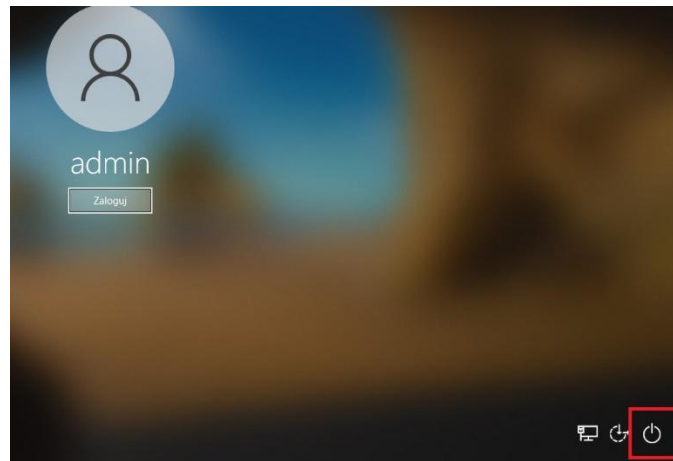
## II. Wymuszanie inspekcji haseł

1. Uruchom w terminalu `secpol.msc`.



2. Przejdź do Ustawienia zabezpieczeń -> Zasady konta -> Zasady haseł.
3. Ustaw następujące parametry:
- maksymalny okres ważności hasła: 40 dni
  - minimalna długość hasła: 10 znaków
  - 12 ostatnich haseł pamiętane w historii
4. Przejdź do Ustawienia zabezpieczeń -> Zasady konta -> Zasady blokady konta.
5. Ustaw następujące parametry blokady konta:
- próg blokady: 5 prób
  - czas trwania blokady: 30 minut
  - zerowanie licznika prób: po 30 minutach

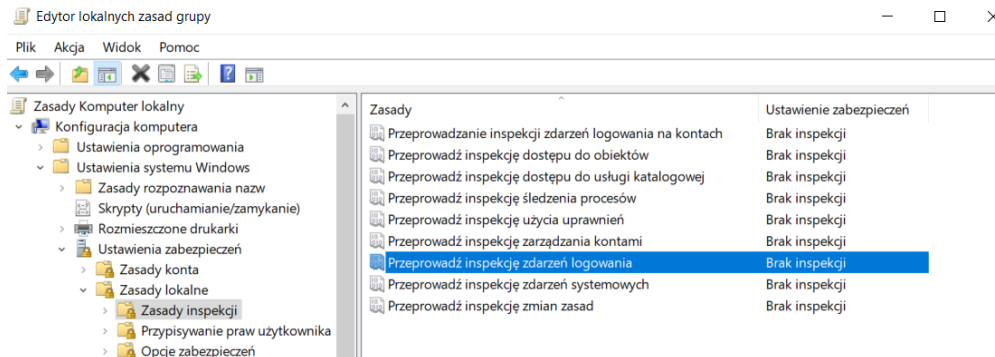
-  6. Zaloguj się na konto i przetestuj ustawione zasady, np. zmień hasło nie spełniające zasad długości.
7. Przejdź do Ustawienia zabezpieczeń -> Zasady lokalne -> Opcje zabezpieczeń.
8. Wyłącz Zamknięcie: zezwalaj na zamykanie systemu bez konieczności zalogowania – to ustawienie zabezpieczeń określa, czy można zamknąć komputer bez konieczności wylogowania się z systemu Windows.
-  9. Po wyłączeniu tej zasady polecenie zamykania powinno nie być wyświetlane na ekranie logowania do systemu Windows.



### III. Inspekcja zdarzeń logowania

System Windows oferuje funkcję **Inspekcja zdarzeń logowania**, która umożliwia monitorowanie prób logowania. Po włączeniu tej zasady Windows rejestruje zarówno udane, jak i nieudane logowania lokalne oraz sieciowe. Każde zdarzenie zawiera kluczowe informacje, takie jak nazwa konta i czas próby logowania.

1. Uruchom **gpedit.msc**.
2. Przejdź do **Konfiguracja komputera -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady inspekcji -> Przeprowadź inspekcję zdarzeń logowania**.



3. Aktywuj inspekcję zdarzeń dla prób kończących się **Sukces** i **Niepowodzenie**.
4. Zaloguj się kilkakrotnie do systemu, w tym używając nieprawidłowego hasła.

### IV. Podgląd zdarzeń

Podgląd zdarzeń (**eventvwr.msc**) wyświetla dzienniki, które mogą pomóc w identyfikacji problemów z systemem. Aby przejrzeć zdarzenia związane z logowaniem, wykonaj poniższe kroki:

1. Uruchom **Podgląd zdarzeń** poprzez Menu Start, wpisując **eventvwr.msc** w pole wyszukiwania i naciśnij **Enter**.
2. Kliknij na **Dzienniki systemu Windows -> Zabezpieczenia**.

3. W centralnej części okna pojawi się lista zdarzeń związanych z inspekcją zabezpieczeń, w tym zdarzeń logowania.



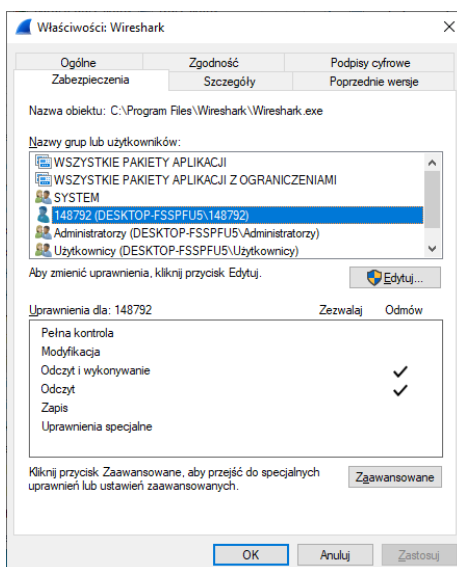
4. Zwróć uwagę na identyfikatory zdarzeń związane z logowaniem:

- a) 4624 – Udane logowanie.
- b) 4625 – Nieudane logowanie.
- c) 4634 – Wylogowanie.
- d) 4672 – Logowanie z przywilejami specjalnymi.
- e) 4768 / 4769 / 4776 – Próby uwierzytelnienia w sieci.

| Słowa kluczowe          | Data i godzina      | Źródło                               | Identyfikator zdarzenia | Kategoria zadania       |
|-------------------------|---------------------|--------------------------------------|-------------------------|-------------------------|
| Sukcesy inspekcji       | 30.11.2024 14:11:24 | Microsoft Windows security auditing. | 4627                    | Group Membership        |
| Sukcesy inspekcji       | 30.11.2024 14:11:24 | Microsoft Windows security auditing. | 4624                    | Logon                   |
| Sukcesy inspekcji       | 30.11.2024 14:11:24 | Microsoft Windows security auditing. | 4627                    | Group Membership        |
| Sukcesy inspekcji       | 30.11.2024 14:11:24 | Microsoft Windows security auditing. | 4624                    | Logon                   |
| Sukcesy inspekcji       | 30.11.2024 14:11:24 | Microsoft Windows security auditing. | 4648                    | Logon                   |
| Niepowodzenie inspekcji | 30.11.2024 14:11:21 | Microsoft Windows security auditing. | 4625                    | Logon                   |
| Sukcesy inspekcji       | 30.11.2024 14:11:14 | Microsoft Windows security auditing. | 4798                    | User Account Management |
| Sukcesy inspekcji       | 30.11.2024 14:11:14 | Microsoft Windows security auditing. | 4798                    | User Account Management |
| Sukcesy inspekcji       | 30.11.2024 14:11:14 | Microsoft Windows security auditing. | 4672                    | Special Logon           |
| Sukcesy inspekcji       | 30.11.2024 14:11:14 | Microsoft Windows security auditing. | 4627                    | Group Membership        |
| Sukcesy inspekcji       | 30.11.2024 14:11:14 | Microsoft Windows security auditing. | 4624                    | Logon                   |

## V. Zabezpieczanie przed uruchomieniem potencjalnie niebezpiecznych aplikacji dla określonych użytkowników

1. Zaloguj się na konto lokalne i sprawdź, czy program Wireshark można uruchomić – powinien działać.
2. Wróć na konto główne.
3. Przejdź do folderu `C:\Program Files\Wireshark`.
4. Kliknij prawym przyciskiem myszy na plik `Wireshark.exe` i wybierz `Właściwości`.
5. Przejdź do zakładki `Zabezpieczenia`.
6. Kliknij `Edytuj`,
7. Dodaj lokalnego użytkownika, a następnie ogranicz jego uprawnienia do uruchamiania programu.



8. Zatwierdź zmiany i wyloguj się.



9. Zaloguj się ponownie na konto lokalne i spróbuj uruchomić program – tym razem uruchomienie powinno być zablokowane ze względu na brak uprawnień.