



## Bezpieczeństwo systemów informatycznych

### SPRAWOZDANIE Z ĆWICZENIA: Konta w systemie MS Windows

Imię Nazwisko: ..... nr albumu: .....

data ćwiczenia: ..... godzina: .....

#### 1. Konta użytkowników

##### 1.1 Parametry kont użytkowników

###### Zadania:

1. Zaloguj się w systemie jako Administrator. Sprawdź poleceniem `user2sid` jaki jest identyfikator SID użytkownika, na którego koncie pracujesz. Która część jest identyfikatorem systemu, a która to RID użytkownika? Zapisz ten RID:
2. Sprawdź SID użytkownika James Bond, Sherlock Holmes, konta Gość, konta SYSTEM, grupy Użytkownicy i Administratorzy.
3. Czy przy pomocy `user2sid` można odpytywać zdalne systemy? Przetestuj dla pętli zwrotnej. Zapisz polecenie:
4. Sprawdź SID usługi `dhcpclient` oraz `dnsclient`.
5. Odpytaj usługę Windows Management Instrumentation o konta lokalnych użytkowników.
6. Wykorzystaj polecenie `net user` do sprawdzenia informacji o wybranym użytkowniku.

##### 1.2 Hasła

7. Gdzie w systemie plików przechowywane są hasła użytkowników?

Sprawdź, czy plik z bazą SAM jest dostępny do odczytu próbując wczytać go do edytora tekstu.

8. Sprawdź, czy baza SAM jest dostępna dla administratora z wykorzystaniem Edytora Rejestru systemowego (`regedit`).
9. Uruchom `regedit` z konta SYSTEM, np. poleceniem:  
  
i zweryfikuj dostępność bazy SAM w tym przypadku.

### 1.2.2 Polityka silnych haseł

10. Włącz opcję Hasło ma spełniać wymagania co do złożoności i zaproponuj optymalne parametry:

- maksymalny wiek hasła:
- minimalną długość:
- minimalny okres ważności:
- ilość haseł pamiętanych w historii:

11. Ustaw takie hasło użytkownika Sherlock Holmes, które system zaakceptuje. Jakie wymagania musi spełniać hasło?

12. Aktywuj mechanizm blokady konta i zaproponuj optymalne parametry:

- próg blokady:  prób(-y)
- czas trwania blokady:  min
- zerowanie licznika prób po  min

### 1.3 Inspekcja zdarzeń logowania

13. Włącz i przetestuj inspekcję zdarzeń zalogowania i wylogowania zakończonych sukcesem i niepowodzeniem. Zaznacz, które ustawienie w polityce należy uaktywnić w tym celu:

- ☐ inspekcję zdarzeń logowania
- ☐ inspekcję zdarzeń logowania na kontach

Jakim narzędziem należy się posłużyć w celu dokonania tej inspekcji?

W zarejestrowanych zdarzeniach odszukaj nazwę użytkownika, którego dotyczy zdarzenie.

### 1.4 Dezaktywacja kont

14. Aby wyłączyć stare i niepotrzebne już konta, należałoby zidentyfikować te, które od dawna nie były używane. Jak sprawdzić, kiedy użytkownik logował się po raz ostatni?