1. Zadanie
- Jakim poleceniem można otworzyć dziennik zdarzeń za pomocą CMD
- Jak jeszcze można otworzyć dziennik zdarzeń
- Jakie jest przeznaczenie „Subskrypcji zdarzeń”
- Jakie są działy „Dziennika Systemu Windows”
- Jaka jest fizyczna ścieżka wszystkich działów „Dziennika Systemu Windows” i pokaż nazwy pozostałych plików (ile ich jest)
- Jaka jest domyślna wartość wielkości poszczególnych działów dziennika
- Jakie inne dzienniki są rejestrowane przez system ? pokaż konkretne przykłady
- Wyświetl właściwości logów systemowych dotyczących Internet Explorera
- Jaka jest klasyfikacja wagi zdarzeń w systemie „Poziom” ? (pokaż emotki, ikonki )

2. Należy utworzyć widok niestandardowy (nowy dziennik który będzie zbierał następujące informacje)
- Wyświetl ostatnie 12 godzin
- Informacje oraz ostrzeżenia -podaj sensowny przykład
- zdarzenia z kategorii System -podaj sensowny przykład
- Zapisanie pod nazwą „systemowe zapiski 12 godzin nazwisko”
- w jaki sposób można zmienić – dany dziennik tak by pobierał informację z 24 godzin

3. Wprowadzić takie ustawienia by możliwe było rejestrowanie sukcesy i niepowodzenia (inspekcja) pliku o nazwie nazwisko (na dysku :D - jeżeli nie ma utworzyć dysk D dodając przestrzeń 10 GB)
- co najmniej 2 użytkowników (Imię, Nazwisko i Imię1 Nazwisko 1) ograniczyć uprawnienia do pliku użytkownikowi nazwisko a następnie spróbować
- ograniczonym użytkownikiem dokonać jakichś zmian w pliku – wykazać taką sytuację w dziennikach zdarzeń (Nazwa użytkownika, konkretny plik)
- czym różnią się od siebie Inspekcja sukcesów, inspekcja niepowodzeń (wymienić zdarzenia jakie mogą być oznaczone)
- zapisać jedno wybrane takie zdarzenie na pulpicie o nazwie ograniczenie (jakie rozszerzenie mają zapisane zdarzenia )
- jakie znaczenie ma Identyfikator zdarzenia do czego może nam się przydać ? podaj kilka przykładów z dziennika zdarzeń
- Wprowadzić przydziały dyskowe dla kilku użytkowników na nowym dysku X (wielkość 5 GB), Uż 1 100MB Poziom ostrzeżeń 75MB, Uż 2 50MB Poziom ostrzeżeń 40MB, przekrocz limity
- Wykaż w dziennikach iż użytkownik 2 przekroczył poziom ostrzeżeń

4. Wyłączyć komputer (niestandardowo – gniazdka – wirtualna maszyna – reset) wykazać takie zdarzenie w dziennikach zdarzeń

5. Wskazać jak wielki jest plik danego działu dziennika

6. Zapisać dziennik „System” pod nazwą Nazwisko202X gdzie X to aktualny rok
- Wyczyścić dany dziennik System np.
- Zaimportować dziennik - w którym miejscu znajduje się dziennik po importowaniu
- Wyeksportować jedno zdarzenie na pulpit (Inspekcja)

7. Wykaż jaki jest numer identyfikatora dla takich zdarzeń jak
- Sukces- zalogowania się na koncie
- Zmiana czasu systemowego
- Uruchamianie systemu Windows
- Nieprawidłowe wyłączenie komputera
- Podjęcie próby zresetowania hasła
- Zmieniono konto użytkownika
- Zmieniono nazwę konta

8. Określ ile razy zarejestrowano sukces w logowaniu się na koncie od początku rejestrowania zdarzeń

9. Znajdź 5 programów (pokaż ich działanie) które służą do zestawień, raportów dot zdarzeń systemowych, logów

10. Czy istnieje potrzeba archiwizowania danych z dziennika - uzasadnij swoją decyzję

11. Zabezpieczanie danych (w nawiązaniu do RODO- czym jest czym są i jak chronić dane )

A. Szyfrowanie funkcja BitLocker – Dodaj nowy dysk 50GB nadaj mu literę dysku O
1. Wypisz możliwości funkcji systemu
2. Zaszyfruj dysk hasłem – jakie powinno spełniać wymagania
3. Jakie mamy możliwości zmian dzięki tej funkcji (np. zmiany hasła)
4. Pokaż jak wygląda procedura usunięcia szyfrowania

B. Szyfrowanie EFS
1. Czym jest
2. Jak możemy zaszyfrować katalog na pulpicie

3. Wyeksportować klucz do innej lokalizacji

C. Program 7 zip

1. Utworzenie archiwum z hasłem – archiwum ma się składać 3 obrazki 2 pliki tekstowe

D. Znajdź 2 programy których zadaniem jest szyfrowanie katalogu bądź całego dysku (pokaż działanie)

4. Ograniczenie dostępu do dysku

A. Uprawnienia NTFS ograniczenie dostępu do dysku z danymi „O” dla konkretnych użytkowników

1. Odczyt (pokaż działanie)
2. Odmowa dostępu (pokaż działanie)