Ćwiczenie laboratoryjne: Monitorowanie logów systemowych w Windows Server

1. Cel ćwiczenia

Celem ćwiczenia jest zapoznanie uczestników z narzędziami i metodami monitorowania logów systemowych w Windows Server. Uczestnicy nauczą się analizować dzienniki zdarzeń z wykorzystaniem Event Viewer oraz PowerShell.

2. Wymagania

- Dostęp do serwera z Windows Server (np. SVR1 lub SVR2)
- Uprawnienia administratora lokalnego
- PowerShell oraz Event Viewer

3. Zadania do wykonania

3.1. Otwórz Event Viewer i przeanalizuj dzienniki:

- System
- Application
- Security (zalogowania, błędy logowania)
- Setup
- Forwarded Events (jeśli dostępne)

3.2. Wyszukaj błędy z ostatnich 24 godzin w dzienniku System.

3.3. Za pomocą PowerShell wykonaj następujące operacje:

```
Get-EventLog -LogName System -EntryType Error -After (Get-
Date).AddDays(-1)
```

3.4. Policz ile było logowań (ID 4624) w ostatnich 24h:

```
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4624;
StartTime=(Get-Date).AddDays(-1)} | Measure-Object
```

3.5. Eksportuj wyniki logów do pliku:

```
Get-EventLog -LogName System -Newest 50 | Export-Csv -Path
C:\logi\system_log.csv -NoTypeInformation
```

4. Przykłady poleceń PowerShell

Pobranie 10 najnowszych zdarzeń z dziennika Application:

```
Get-EventLog -LogName Application -Newest 10
```

Filtrowanie zdarzeń o błędach aplikacji (Event ID 1000):

```
Get-WinEvent -FilterHashtable @{LogName='Application'; ID=1000}
```

Monitorowanie prób logowania nieudanych (Event ID 4625):

```
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4625}
```

5. Pytania sprawdzające

- Ile błędów systemowych wystąpiło w ostatnich 24 godzinach?
- Czy na serwerze były nieudane próby logowania?
- Jak można zautomatyzować zbieranie logów do analizy?
- Które dzienniki zawierają informacje o uruchamianiu usług?

6. Uwagi końcowe

- Logi systemowe są podstawowym źródłem informacji diagnostycznej.
- Regularne monitorowanie dzienników pozwala na wczesne wykrycie incydentów.
- PowerShell umożliwia automatyzację analizy logów i eksport danych.