Windows Event Viewer Practical Tasks

Practical 1: Basic Navigation and Event Filtering

Objective: Understand how to navigate and filter events in the Event Viewer.

- Steps:

1. Open Event Viewer (`eventvwr.msc` via the Run dialog).

1. 2. Explore the main sections:

- - Windows Logs (Application, Security, System, etc.)
- - Applications and Services Logs.

2. 3. Select System Logs and filter by:

- - Event Level (e.g., Errors or Warnings).
- - Time period (e.g., last 24 hours).

3. 4. Note down a critical or warning event, including the event ID and description.

- Outcome: Learn how to filter and identify specific events.

Practical 2: Analyze Boot and Shutdown Events

Objective: Track system boot and shutdown activities.

- Steps:

1. Navigate to Windows Logs > System.

4. 2. Use the following Event IDs to filter:

- - 6005: System Startup.
- - 6006: System Shutdown.
- - 6008: Unexpected Shutdown.

5. 3. Analyze the timestamps to identify system uptime.
6. 4. Document any abnormal shutdowns with their descriptions.

- Outcome: Understand how to monitor system startup and shutdown activities.

Practical 3: Audit Logon Events

Objective: Monitor user logon and logoff events.

- Steps:

1. Navigate to Windows Logs > Security.

7. 2. Filter by Event IDs:

- - 4624: Successful logon.
- - 4625: Failed logon attempt.
- - 4647: User-initiated logoff.

8. 3. Identify:

- - The user account involved.
- - Logon types (interactive, remote desktop, etc.).

9. 4. Investigate any failed logon attempts for potential security issues.

- Outcome: Learn to track and audit user authentication.

Practical 4: Create a Custom View

Objective: Create a custom view for critical system events.

- Steps:

1. In Event Viewer, click Action > Create Custom View.

10. 2. Select:

- - Event Levels: Critical, Warning, and Error.
- - Logs: System and Application.
- - Time Range: Last 7 days.

11. 3. Save the custom view with a name (e.g., "Critical System Events").
12. 4. Document and analyze any recurring critical errors.

- Outcome: Learn to customize event views for efficient monitoring.

Practical 5: Export and Share Logs

Objective: Export and analyze logs for troubleshooting.

- Steps:

1. Navigate to any log (e.g., System).

13. 2. Select Save All Events As... and save the log as an `.evtx` file.
14. 3. Open the file on another system with Event Viewer or convert it to `.csv` for analysis in Excel.
15. 4. Discuss key findings based on exported data.

- Outcome: Learn to share and interpret logs for collaborative troubleshooting.

These tasks will help you master the essentials of Windows Event Viewer and leverage it for system monitoring, troubleshooting, and auditing.