Windows Event Logs

## **Windows Event Logs**

### **Task 1 – What are Event Logs?**

* Event logs are records of system, security, and application events generated by Windows.
* Used for monitoring, troubleshooting, and investigating incidents.
* Stored in .evtx format, usually in C:\Windows\System32\winevt\Logs.
* Types of logs:
  + **Application Logs** – Events from installed software.
  + **System Logs** – OS and driver events.
  + **Security Logs** – Login attempts, resource access, policy changes.

### **Task 2 – Event Viewer**

* Built-in GUI tool to view event logs.
* Launched with eventvwr.msc.
* Components:
  + **Windows Logs** – Application, Security, System, Setup, Forwarded Events.
  + **Custom Views** – Filtered event views.
  + **Applications and Services Logs** – Logs from specific apps or services.
* Features:
  + Filter logs by time, source, event ID, etc.
  + Create custom views for specific monitoring needs.

### **Task 3 – wevtutil.exe**

* Command-line utility to manage Windows event logs.
* **Common commands**:
  + wevtutil el – List all event logs.
  + wevtutil qe <logname> – Query events from a log.
  + wevtutil cl <logname> – Clear logs.
* Supports XML queries and exporting logs.
* Useful for automation or remote investigation.

### **Task 4 – Get-WinEvent**

* PowerShell cmdlet for accessing event logs.
* More flexible than Get-EventLog.
* **Example**:

powershell

CopyEdit

Get-WinEvent -LogName Security -MaxEvents 10

* Can filter by:
  + -FilterHashtable
  + -FilterXPath
* Supports exporting to CSV or XML for analysis.

### **Task 5 – XPath Queries**

* Used to filter specific events in XML-based log format.
* **Example XPath**:

xml

CopyEdit

\*[System/EventID=4624]

* Can combine multiple conditions:

xml

CopyEdit

\*[System[(EventID=4624) and TimeCreated[@SystemTime>'2025-08-10T00:00:00']]]

* Helpful for precise log searches.

### **Task 6 – Event IDs**

* Numeric identifiers for specific event types.
* Common security-related Event IDs:
  + **4624** – Successful logon
  + **4625** – Failed logon
  + **4634** – Logoff
  + **4672** – Special privileges assigned
  + **4688** – New process created
  + **4720** – User account created
  + **4726** – User account deleted

### **Task 7 – Putting Theory into Practice**

* Example investigation flow:
  1. Identify suspicious logon Event IDs.
  2. Correlate with process creation logs.
  3. Check for privilege escalation events.
  4. Export relevant logs for deeper forensic analysis.

### **Task 8 – Conclusion**

* Event logs are crucial for:
  + Security monitoring
  + Incident investigation
  + Troubleshooting
* Combining GUI tools (Event Viewer) with CLI tools (wevtutil, Get-WinEvent) improves efficiency.
* Filtering with XPath makes analysis faster and more precise.

