Windows Event Logs

Running it from the command line

```
wevtutil.exe
```

requesting the help menu

```
wevtutil.exe /?
```

quering the application logs and returning 3 results, descending order and text format

```
wevtutil qe Application /c:3 /rd:true
/f:text
```

Investigating Event logs with Powershell

Listing log providers with 'powershell' as a keyword

```
Get-WinEvent -ListProvider *PowerShell
```

Listing events related to windows powershell

```
(Get-WinEvent -ListProvider Microsoft-
Windows-PowerShell).Events | Format-Table
Id, Description
```

Listing available logs containing given keyword

```
Get-WinEvent -ListLog * | findstr “kw”
```

Listing events on a specific log path

```
Get-WinEvent -FilterHashtable
@{logname=”Microsoft-Windows-
PrintService/Admin”} | fl -property *
```

Finding process related information using a given keyword about the process

```
Get-WinEvent -Path .\file.evtx -
FilterXPath ‘*/System/EventID=1’ | Sort-
```

```
Object TimeCreated | Where-Object
{$_.Message -like “*kw*”} | fl
```

listing application logs from WLMS provider and generated at the given time

```
Get-WinEvent -LogName Application -
FilterXPath
'*/System/Provider[@Name="WLMS"] and
*/System/TimeCreated[@SystemTime="2020-12-
15T01:09:08.940277500Z"]'
```

Displaying events logged for processes initiated network connections.

```
**Get-WinEvent -Path .\file.evtx -
FilterXPath ‘*/System/EventID=3’ | Sort-
Object TimeCreated | fl**
```

listing security logs with sam as target usrname and event id equals

to 4724

```
Get-WinEvent -LogName Security -
FilterXPath
'*/EventData/Data[@Name="TargetUserName"]=
"Sam" and */System/EventID=4724'
```

listing security logs with event id equals to 400

```
Get-WinEvent -LogName Security -
FilterXPath '*/System/EventID=400'
```

listing logs from log file with event id = 104 and format as list displaying all events properties

```
Get-WinEvent -Path .\merged.evtx -
FilterXPath '*/System/EventID=104' | fl -
property *
```

listing logs from log file with event id = 4104 with string 'ScriptBlockText'

and format as list displaying all events properties

```
Get-WinEvent -Path .\merged.evtx -FilterXPath '*/System/EventID=4104 and */EventData/Data[@Name="ScriptBlockText"]' | fl -property *
```

listing logs from log file with event id =13 with string 'enc' in the message field and format as list displaying all events properties

```
Get-WinEvent -Path .\file.evtx -FilterXPath ‘*/System/EventID=13’ | Sort-Object TimeCreated | Where-Object {$_.Message -like “*enc*”} | fl
```

filtering events using time range

```
$startdate = Get-Date -Date "date"
$end-date = Get-Date -Date "date"
Get-WinEvent -Path .\file.evtx -FilterXPath ‘*/System/*’ | Where-Object {
```

```
$_.TimeCreated -ge $startdate -and
$_.TimeCreated -le $endtime
} | Sort-Object TimeCreated
```

```
$date = Get-Date -Date "date"
Get-WinEvent -Path .\file.evtx -
FilterXPath ‘*/System/*’ | Where-Object {
$_.TimeCreated -like $date } | fl
```

listing security logs with sam as target usrname and event id equals to 4799

```
Get-WinEvent -LogName Security -
FilterXPath '*/System/EventID=4799'
```

Investigating Logs with Sysmon and Powershell

Hunting for Metasploit events

```
Get-WinEvent -Path .\Filtering.evtx -
FilterXPath '*/System/EventID=3 and
*/EventData/Data[@Name="DestinationPort"]
and */EventData/Data=4444'
```

Filtering for Network connections

```
Get-WinEvent -Path .\Filtering.evtx -
FilterXPath '*/System/EventID=3'
```

Filtering for Network connections in format list with maximum quantity of one

```
Get-WinEvent -Path .\Filtering.evtx -
FilterXPath '*/System/EventID=3' -
MaxEvents 1 -Oldest | fl -property *
```

Filtering for process access events specifically lsass.exe

```
Get-WinEvent -Path <Path to Log> -
FilterXPath '*/System/EventID=10 and
*/EventData/Data[@Name="TargetImage"] and
*/EventData/Data="C:\Windows\system32\lsas
s.exe"'
```

Filtering for Alternate Data Streams events

Filtering for process hollowing events

```
Get-WinEvent -Path <Path to Log> -FilterXPath '*/System/EventID=8'
```

Windows Event IDs

Security

4720: User created or added

Sysmon Events

Event ID 1: Process Creation

Event ID 3: Network Connection

Event ID 7: Image Loaded

Event ID 8: CreateRemoteThread [Persistence operations - process migration]

Event ID 11: File Created

Event ID 12 / 13 / 14: Registry Event

Event ID 15: FileCreateStreamHash

Event ID 22: DNS Event

Event ID 13: Registry Value Set