

Events Logs Methodology

Tools:

- 1.) Event Viewer
- 2.) Command Prompt
- 3.) Power Shell

Important Main security and system event IDs:

Security Event IDs

- **4624** - A logon

Security Event IDs

- **4720** - A user account was created
- **4722** - A user account was enabled
- **4723** - An attempt was made to change an account's password
- **4724** - An attempt was made to reset an account's password
- **4738** - A user account was changed
- **4725** - A user account was disabled
- **4726** - A user account was deleted
- **4732** - A member was added to a security-enabled local group
- **4688** - A new process has been created
- **1102** - The audit log was cleared



System Event IDs

System Event IDs



- **7045** - A service was installed in the system
- **7030** - The Service Control Manager tried to take a corrective action (Restart the service)
- **7035** - The Service Control Manager is transitioning services to a running state
- **7036** - The Service Control Manager has reported that a service has entered the running state

Important Questions:

- 1.) What is the **hostname** of the computer that generated the logs in the `challenge.evtx` file?
- 2.) What is the **Process ID (PID)** of the execution process that cleared the security event log?
- 3.) How many **logon events** are recorded in the logs?
- 4.) In **chronological order**, list the names of the accounts that were created within the logs.
- 5.) Which user account was **disabled** according to the event logs?
- 6.) Which user account was **deleted** according to the event logs?
- 7.) In chronological order, list the **security-enabled local groups** that the **backdoor** user account was added to
- 8.) Which user account was added to the **Backup Operators** group?

Important Cmds:

CMD.exe

Live Security Event analysis cmd via cmd.exe:

Security Event Cmd.exe

```
$ powershell -NoProfile -Command "Get-WinEvent -FilterHashtable  
@{LogName='Security'; ID=4720,4722,4723,4724,4738,4725,4726,4732,4688,1102} |  
Format-List *"
```

```
$ powershell -NoProfile -Command "Get-WinEvent -FilterHashtable  
@{LogName='Security'; ID=4720,4722,4723,4724,4738,4725,4726,4732,4688,1102} |  
Format-List * | Out-File -Encoding utf8 'C:\\Users\\soc\\Desktop\\SecurityEvents.txt'"
```

Security Logs output file analysis cmd via cmd.exe:

```
$ powershell -NoProfile -Command "Get-WinEvent -Path  
'C:\\Users\\soc\\Desktop\\03_Endpoint_Security\\Windows\\Challenges\\challenge.evtx'  
| Where-Object { $_.Id -in 4720,4722,4723,4724,4738,4725,4726,4732,4688,1102 } |  
Format-List *"
```

```
$ powershell -NoProfile -Command "Get-WinEvent -Path  
'C:\\Users\\soc\\Desktop\\03_Endpoint_Security\\Windows\\Challenges\\challenge.evtx'
```

```
| Where-Object { $_.Id -in 4720,4722,4723,4724,4738,4725,4726,4732,4688,1102 } |  
Format-List * | Out-File -Encoding utf8 'C:\\Users\\soc\\Desktop\\FilteredEvents.txt'
```

Live system event analysis cmd via cmd.exe :

System Event Cmd.exe

```
$ powershell -NoProfile -Command "Get-WinEvent -FilterHashtable  
@{LogName='Security'; ID= 7045,7030,7035,7036 } | Format-List *"
```

```
$ powershell -NoProfile -Command "Get-WinEvent -FilterHashtable  
@{LogName='Security'; ID=7045,7030,7035,7036} | Format-List * | Out-File -Encoding  
utf8 'C:\\Users\\soc\\Desktop\\SecurityEvents.txt'"
```

Systems Log output file analysis cmd via cmd.exe:

```
$ powershell -NoProfile -Command "Get-WinEvent -Path  
'C:\\Users\\soc\\Desktop\\03_Endpoint_Security\\Windows\\Challenges\\challenge.evtx' |  
Where-Object { $_.Id -in 7045,7030,7035,7036 } | Format-List *"
```

```
$ powershell -NoProfile -Command "Get-WinEvent -Path  
'C:\\Users\\soc\\Desktop\\03_Endpoint_Security\\Windows\\Challenges\\challenge.evtx' |  
Where-Object { $_.Id -in 7045,7030,7035,7036 } | Format-List * | Out-File -Encoding utf8  
'C:\\Users\\soc\\Desktop\\FilteredEvents.txt'"
```

Powershell.exe

Live security event analysis cmd via powershell:

security event PowerShell

```
$ Get-WinEvent -FilterHashtable @{LogName="Security";  
ID=4720,4722,4723,4724,4738,4725,4726,4732,4688,1102} | Format-List *
```

```
$ Get-WinEvent -FilterHashtable @{LogName="Security";  
ID=4720,4722,4723,4724,4738,4725,4726,4732,4688,1102} | Format-List * | Out-File -  
Encoding utf8 "C:\Users\soc\Desktop\SecurityEvents.txt" ⇒ ( Use real analysis case )
```

Live system event analysis cmd via powershell:

System event PowerShell

```
$ Get-WinEvent -FilterHashtable @{LogName="System"; ID=7045,7030,7035,7036} |  
Format-List *
```

```
$ Get-WinEvent -FilterHashtable @{LogName="System"; ID=7045,7030,7035,7036} |  
Format-List * | Out-File -Encoding utf8 "C:\Users\soc\Desktop\SecurityEvents.txt"
```

Live system event analysis cmd via PowerShell:

Security event PowerShell

```
$Get-WinEvent -Path  
"C:\Users\soc\Desktop\03_Endpoint_Security\Windows\Challenges\challenge.evtx" |  
Where-Object { $_.Id -in 4720,4722,4723,4724,4738,4725,4726,4732,4688,1102 } |  
Format-List *
```

```
$ Get-WinEvent -Path  
"C:\Users\soc\Desktop\03_Endpoint_Security\Windows\Challenges\challenge.evtx" |  
Where-Object { $_.Id -in 4720,4722,4723,4724,4738,4725,4726,4732,4688,1102 } |  
Format-List * | Out-File "C:\Users\soc\Desktop\FilteredEvents.txt" -Encoding utf8
```

Security event Log output file analysis cmd via powershell:

System event PowerShell

```
$ Get-WinEvent -Path  
"C:\Users\soc\Desktop\03_Endpoint_Security\Windows\Challenges\challenge.evtx" |  
Where-Object { $_.Id -in 7045,7030,7035,7036 } | Format-List *
```

```
$ Get-WinEvent -Path  
"C:\Users\soc\Desktop\03_Endpoint_Security\Windows\Challenges\challenge.evtx" |  
Where-Object { $_.Id -in 7045,7030,7035,7036 } | Format-List * | Out-File  
"C:\Users\soc\Desktop\FilteredEvents.txt" -Encoding utf8
```

Valid key-value pairs:

Key Name	Value Data	Wildcard?
LogName	<String>	Yes
ProviderName	<String>	Yes
Path	<String>	No
Keywords	<Long>	No
ID	<Int32>	No
Level	<Int32>	No
StartTime	<DateTime>	No
EndTime	<DateTime>	No
UserID	<SID>	No
Data	<String>	No