

# Setting Sysmon and Splunk Universal Forwarder For Read CMD and Powershell Command

## Prerequisites

- Already Installed Universal Forwarder
  - Windows OS
- 

## Config Powershell and Cmd read log

### Config Powershell

#### 1. Buat Kunci Registri untuk membaca logging

Buat path registry untuk Module Logging

```
New-Item -Path  
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging" -Force
```

Aktifkan Module Logging

```
Set-ItemProperty -Path  
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging" -Name  
"EnableModuleLogging" -Value 1
```

Buat daftar modul yang akan dicatat

```
New-Item -Path  
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleName  
s" -Force  
  
Set-ItemProperty -Path  
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleName  
s" -Name "*" -Value "*"
```

#### 2. Aktifkan Script Block Logging

Buat path registri untuk Script Block Logging

```
New-Item -Path  
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -  
Force
```

Aktifkan script block logging

```
Set-ItemProperty -Path  
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -  
Name "EnableScriptBlockLogging" -Value 1
```

### 3. Verifikasi

1. Buka registry editor (Win + R) lalu type "regedit" kemudian enter.
2. Navigasikan ke
  - HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging
  - HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging
3. Pastikan nilai registry ada dan sesuai

### 4. Terapkan Perubahan

Jika semua sudah dibikin untuk menerapkan perubahannya ketikkan perintah berikut

```
gpupdate /force
```

### 5. Tes Logging

Untuk tes logging apakah dapat terbaca atau tidak bisa tuliskan perintah berikut :

```
Write-Host "Test PowerShell Log Zake"
```

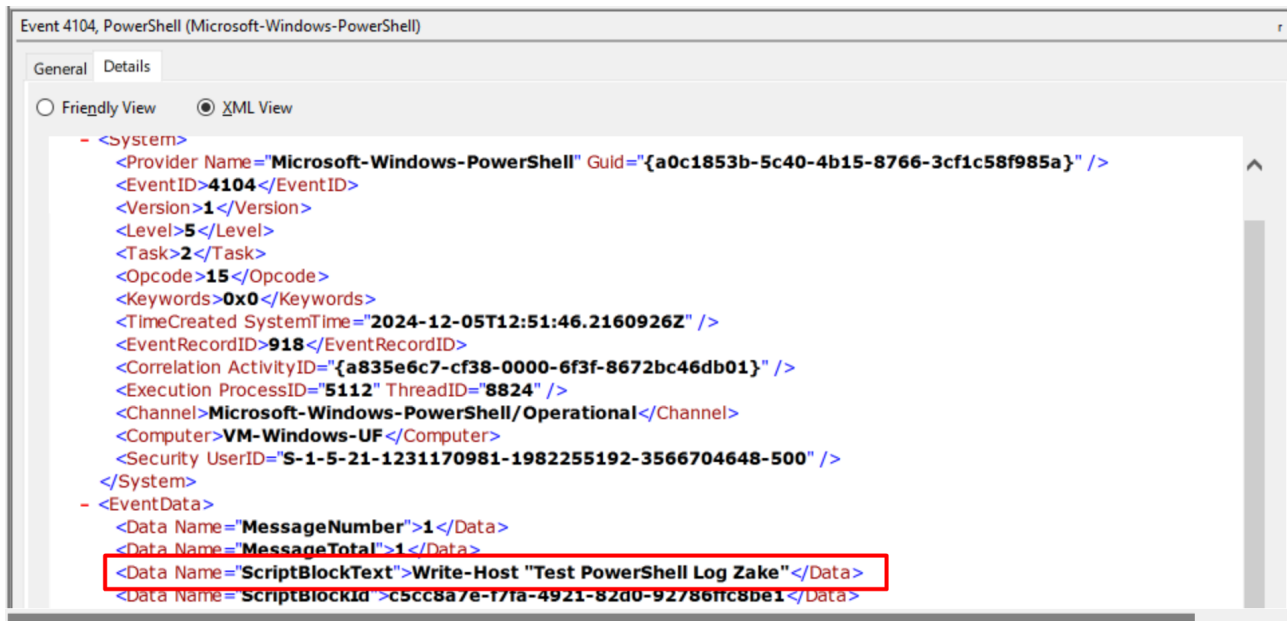
### 6. Verifikasi data log

Setelah log berhasil dibuat, check pada EventViewer untuk melihat apakah lognya berhasil dicatat.

1. Buka Eventviewer (Win + R) lalu type "eventvwr" kemudian enter.
2. Di panel kiri, ikutin path seperti ini

Applications and Services Logs > Microsoft > Windows > PowerShell > Operational

3. Pada "Operational" Click kanan terlebih dahulu, jika masih ada tulisan "Enable log" maka di click, jika tulisannya "Disable Log" biarkan saja dan lanjut di step selanjutnya (step 4)
4. Biasanya untuk Script block yang dijalankan akan berada pada ID 4104. Namun jika kesulitan menemukannya karena ditimpa event lain, bisa gunakan fitur "find" yang ada di panel kanan
5. Jika sudah ketemu dan scriptblock terlihat jelas maka tinggal setting ke Sysmon dan Universal Forwardernya.



## Config CMD

### 1. Aktifkan Audit Process Creation

- Buka Local Group Policy Editor (gpedit.msc)
- Navigasikan ke :

Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policies > Detailed Tracking

- Aktifkan opsi :
  - Audit Process Creation (Success / Failure) tergantung kebutuhan
  - Audit Command Line Process Creation (jika ada)

- Apply

## 2. Aktifkan Audit Process Creation

Jalankan perintah berikut pada powershell untuk memastikan audit command line aktif :

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit"  
/v ProcessCreationIncludeCmdLine_Enabled /t REG_DWORD /d 1 /f
```

Note : Perintah ini menginstruksikan Windows untuk mencatat perintah lengkap (termasuk argumen command line) pada Event ID 4688.

## 3. Verifikasi data

- Cek di registry editor (regedit)
- Navigasikan ke :

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit
```

- Pastikan kunci `ProcessCreationIncludeCmdLine_Enabled` ada dan bernilai `1`.

## 4. Terapkan perubahan

Jika semua sudah dibikin untuk menerapkan perubahannya ketikkan perintah berikut

```
gpupdate /force
```

## 5. Tes Logging

Untuk tes logging apakah dapat terbaca atau tidak bisa tuliskan perintah berikut :

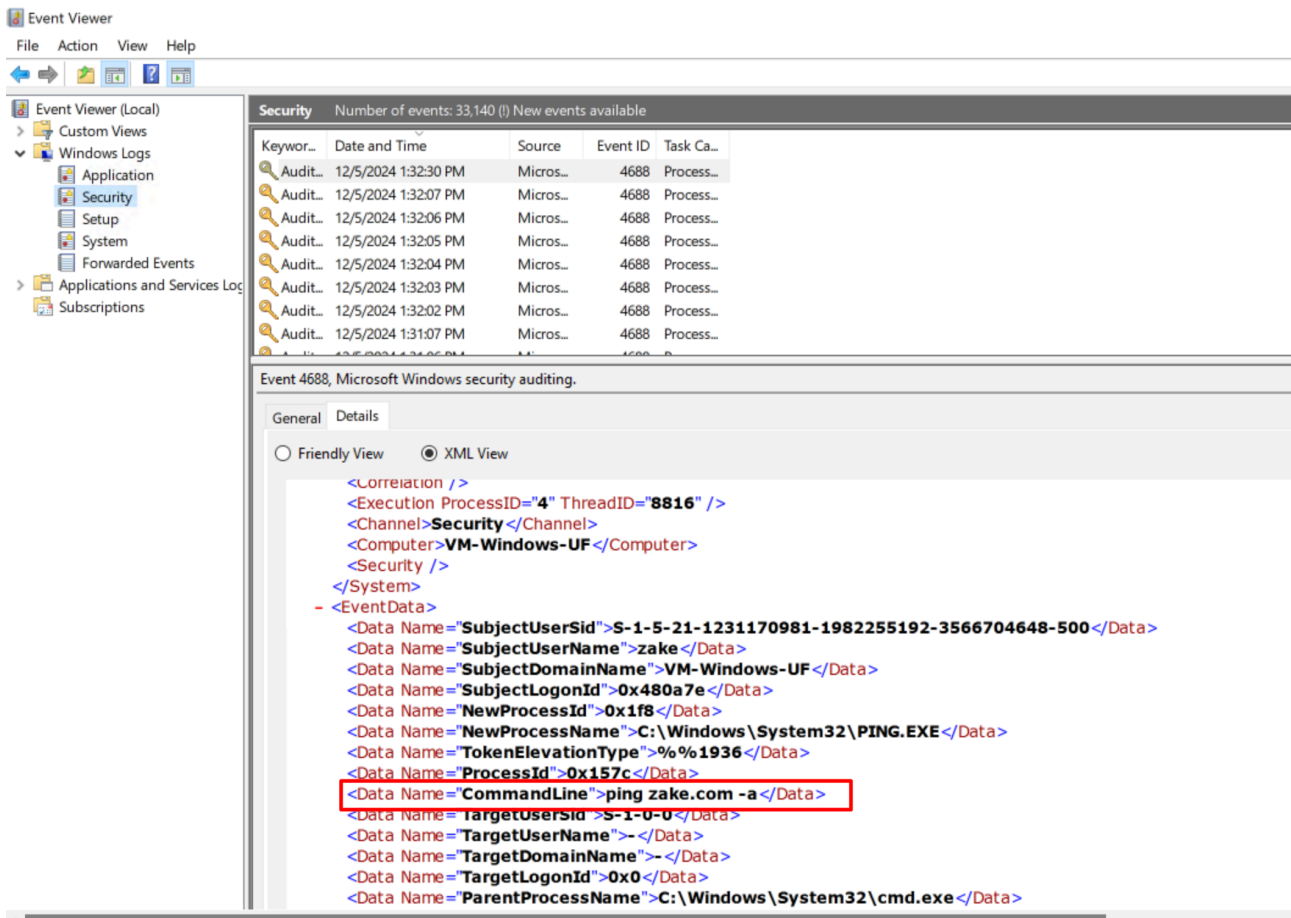
```
Write-Host "ping zake.com -a"
```

## 6. Verifikasi Data Log

1. Buka EventViewer (eventvwr)
2. Navigasikan ke :

```
Windows Logs > Security
```

### 3. Terlihat bahwa log tersebut bisa dibaca



### 4. Jika sudah ketemu terlihat jelas maka tinggal setting ke Sysmon dan Universal Forwardernya.

## Install dan Config Sysmon

1. Untuk bahan awal download Sysmon pada Official Website Microsoft  
<https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>
2. Kemudian download file xml custom by zake di [Github](#)
3. Open cmd dengan "Run As Administrator" lalu jalankan perintah berikut

```
sysmon.exe -i sysmonconfig-custom-by-zake.xml -accepteula
```

4. Jika sudah selesai lanjut config ke Universal Forwarder

## Setting Universal Forwarder

Pada Universal Forwarder, harus di setting agar membaca file sysmon yang sudah di custom ini. Tetapi harap diperhatikan jika settingan sudah sama selanjutnya hanya tinggal perlu merestart Universal Forwardernya saja .

1. Buka file inputs.conf (defaultnya berada pada directory berikut)

```
C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf
```

2. Didalam inputs.conf tambahkan konfigurasi seperti ini

```
[WinEventLog://Security]
disabled = 0
index = <yourindex>
sourcetype = Wineventlog:Security

[WinEventLog://System]
disabled = 0
index = <yourindex>
sourcetype = Wineventlog:System

[WinEventLog://Microsoft-Windows-PowerShell/Operational]
disabled = 0
index = <yourindex>
sourcetype = WinEventLog:PowerShell
```

*Note : ganti nama index sesuai dengan sebenarnya.*

3. Kemudian save lalu restart Universal Forwarder dengan perintah berikut

```
net stop splunkforwarder
net start splunkforwarder
```

---

## Proof Screenshots from this configuration

1. Proof cmd log history

From windows :

```
C:\Sysmon>ping zake.com -l 50

Pinging zake.com [3.33.130.190] with 50 bytes of data:
Reply from 3.33.130.190: bytes=50 time=2ms TTL=244
Reply from 3.33.130.190: bytes=50 time=1ms TTL=244
Reply from 3.33.130.190: bytes=50 time=1ms TTL=244
Reply from 3.33.130.190: bytes=50 time=1ms TTL=244

Ping statistics for 3.33.130.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

From Splunk :

The screenshot shows the Splunk interface with a search for "ping". The search results are displayed in a table with columns for Time and Event. The event details show the process name as "C:\Windows\System32\ping.exe" and the command line as "ping zake.com -l 50". The command line is highlighted in red.

Time	Event
12/5/24 9:03:42.000 PM	<p>... 26 lines omitted ...</p> <p>New Process ID: 0x10f4</p> <p>New Process Name: C:\Windows\System32\ping.exe</p> <p>Token Elevation Type: %1936</p> <p>... 2 lines omitted ...</p> <p>Creator Process Name: C:\Windows\System32\cmd.exe</p> <p>Process Command Line: ping zake.com -l 50</p> <p>Show all 4 lines</p>

## 2. Proof Powershell Log

From Windows :

```
PS C:\Users\zake> whoami
vm-windows-uf\zake
PS C:\Users\zake> Write-Host "I'am Attacker Lockbit 3.0"
I'am Attacker Lockbit 3.0
PS C:\Users\zake> whoami
vm-windows-uf\zake
PS C:\Users\zake> ping zake.com -a

Pinging zake.com [3.33.130.190] with 32 bytes of data:
Reply from 3.33.130.190: bytes=32 time=1ms TTL=244
Reply from 3.33.130.190: bytes=32 time=1ms TTL=244
Reply from 3.33.130.190: bytes=32 time=3ms TTL=244
Reply from 3.33.130.190: bytes=32 time=1ms TTL=244

Ping statistics for 3.33.130.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
PS C:\Users\zake>
```

## From Splunk :

The screenshot displays the Splunk Enterprise web interface. At the top, the navigation bar includes 'splunk>enterprise', 'Apps', and user information 'zake'. Below this, a secondary navigation bar lists 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' tab is active, leading to the 'New Search' page. The search bar contains the query 'index="zakewindows\_mii" | search "Lockbit"'. To the right of the search bar are buttons for 'Save As', 'Create Table View', and 'Close'. Below the search bar, a status bar indicates '2 events (12/5/24 8:54:27.000 PM to 12/5/24 9:09:27.000 PM)' and 'No Event Sampling'. A 'Job' dropdown and a 'Verbose Mode' toggle are also present. The main content area shows a table with two columns: 'Time' and 'Event'. The 'Time' column lists the date '12/5/24' and the time '9:08:18.000 PM'. The 'Event' column contains a log entry: 'Message=Creating Scriptblock text (1 of 1): Write-Host "I'am Attacker Lockbit 3.0"'. This specific line is highlighted with a red rectangle. Below the main table, there are sections for 'SELECTED FIELDS' (host 1, source 1, sourcetype 1) and 'INTERESTING FIELDS' (ComputerName 1, EventCode 1, EventType 1). The bottom of the interface shows a 'ScriptBlock ID: b11eb46f-e6d1-45f6-9812-9efa888635b5' and a link to 'Show all 19 lines'. The footer of the interface indicates '1 minute per column'.

splunk>enterprise Apps

zake Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

New Search Save As Create Table View Close

index="zakewindows\_mii" | search "Lockbit" Last 15 minutes

2 events (12/5/24 8:54:27.000 PM to 12/5/24 9:09:27.000 PM) No Event Sampling Job Verbose Mode

Events (2) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- ComputerName 1
- EventCode 1
- EventType 1

Time	Event
12/5/24	12/05/2024 02:08:18 PM
9:08:18.000 PM	... 13 lines omitted ... Message=Creating Scriptblock text (1 of 1): Write-Host "I'am Attacker Lockbit 3.0"

ScriptBlock ID: b11eb46f-e6d1-45f6-9812-9efa888635b5  
Show all 19 lines

host = VM-Windows-UF | source = WinEventLog:Microsoft-Windows-PowerShell/Operational | sourcetype = WinEventLog:PowerShell