



## Scenario 4: Log Tampering Simulation (T1562.002)

1.  Enable PowerShell Logging:
2.  **Install and Configure Sysmon**
  - Download [Sysmon](#).
  - Install Sysmon with a config that logs command-line executions:

```
Microsoft Windows [Version 10.0.19045.5854]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Sysmon

C:\Sysmon>.\Sysmon64.exe -accepteula -i sysmon_config.xml

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Error: Failed to open xml configuration: sysmon_config.xml (No such file or directory)
Usage:
Install:           Sysmon64.exe -i [<configfile>]
Update configuration: Sysmon64.exe -c [<configfile>]
Install event manifest: Sysmon64.exe -m
Print schema:      Sysmon64.exe -s
Uninstall:         Sysmon64.exe -u [force]
  -c Update configuration of an installed Sysmon driver or dump the
      current configuration if no other argument is provided. Optionally
      take a configuration file.
  -i Install service and driver. Optionally take a configuration file.
  -m Install the event manifest (done on service install as well)).
  -s Print configuration schema definition of the specified version.
      Specify 'all' to dump all schema versions (default is latest)).
  -u Uninstall service and driver. Adding force causes uninstall to proceed
      even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in
the boot that the service will write to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational". On
older systems, events are written to the System event log.

Use the '-? config' command for configuration file documentation. More examples are available on the Sysinternals
website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to
accept it.

Neither install nor uninstall requires a reboot.
```

### 3. Enable Winlogbeat

Ensure Winlogbeat is configured on Windows 10 to send:

- Security logs
- PowerShell logs
- Sysmon logs to your Splunk/Logstash setup.

```
PS C:\Sysmon> .\Sysmon64.exe -accepteula -i sysmon_config.xml
```

```
System Monitor v15.15 - System activity monitor  
By Mark Russinovich and Thomas Garnier  
Copyright (C) 2014-2024 Microsoft Corporation  
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.  
Sysinternals - www.sysinternals.com
```

```
Loading configuration file with schema version 4.50  
Sysmon schema version: 4.90  
Configuration file validated.  
Sysmon64 installed.  
SysmonDrv installed.  
Starting SysmonDrv.  
SysmonDrv started.  
Starting Sysmon64..  
Sysmon64 started.  
PS C:\Sysmon>
```

#### 4. Perform a Brute Force (Optional)

- You can simulate brute force using tools like hydra from Kali or repeated RDP attempts (xfreerdp).

#### 5. Detect wevtutil via Sysmon Event ID 1

- **index=winlogbeat EventCode=1 Image="\*\wevtutil.exe"**  
**CommandLine="\*cl\*Security\*"**

#### 6. Detect Clear-EventLog PowerShell via Event ID 4104

- **index=winlogbeat EventCode=4104 ScriptBlockText="\*Clear-EventLog\*"**

The screenshot shows the Splunk Enterprise Search interface. The search bar contains the query: `| catalog values(metric_name) as metrics WHERE NOT metric_name ~ "_rollup_" AND ("index" ~ "*" OR "index" ~ "-")`. The search results show 3,595 events from 5/22/25 10:30:00.000 AM to 5/23/25 11:22:51.000 AM. The interface includes tabs for Events, Patterns, Statistics (420), and Visualization. The Statistics tab is active, showing a list of metrics including `spl_mlog_tpool_work_units`, `spl_mlog_tpool_workers`, `spl_mlog_ushttp_global_thread_count`, `spl_mlog_version_control_bytes`, `spl_mlog_version_control_total_commits`, and `spl_mlog_version_control_tracked_files_count`.