

Wazuh Set up, Rule Creation, and configure Sysmon to be ingested into Wazuh.

Download and initiate Mimikatz on my windows VM

-prior to this I had to add my downloads folder to the security exclusion list

-Open powershell as admin>cd into mimikatz path and initiate .\mimikatz.exe

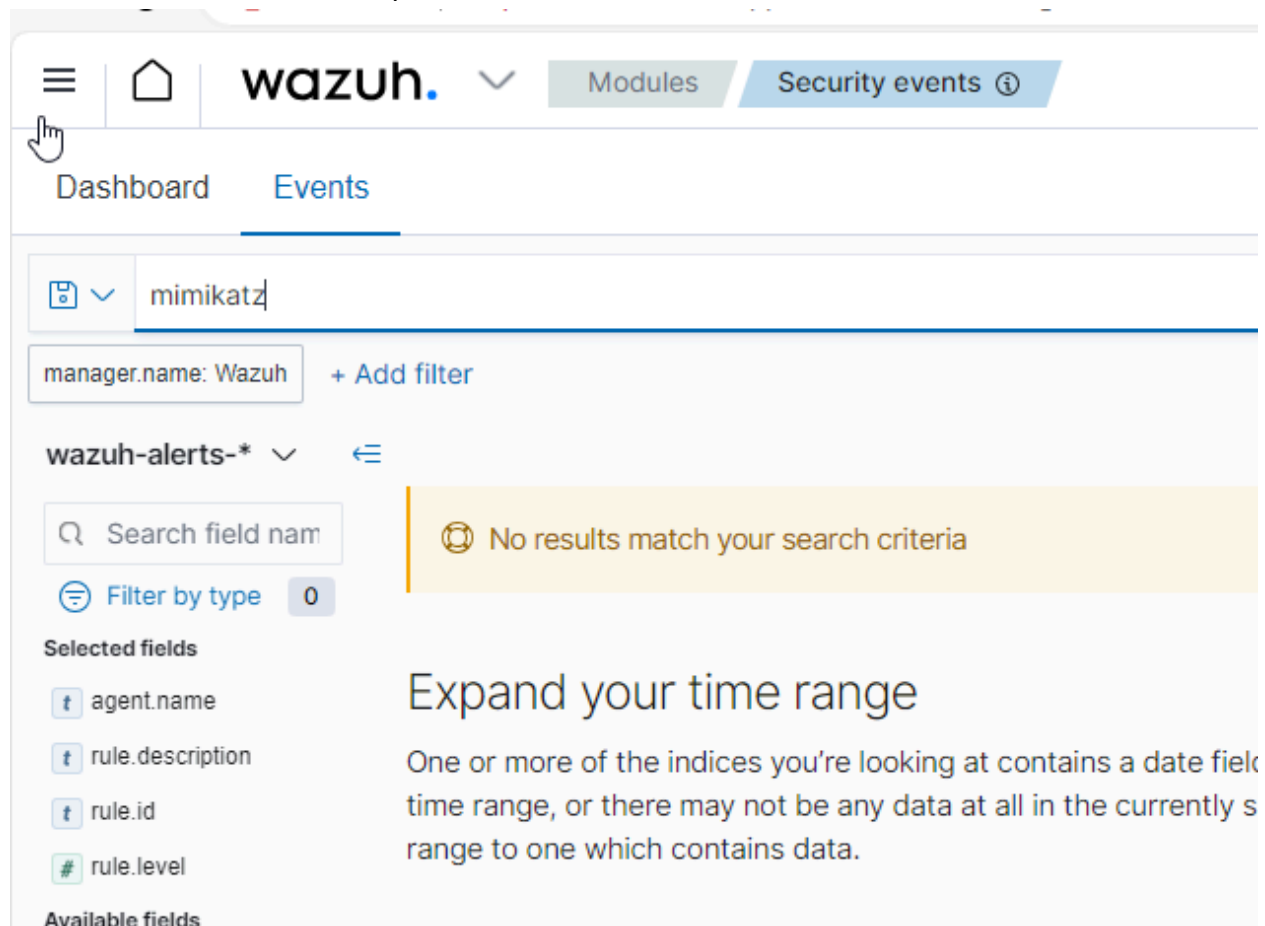
```
PS C:\Windows\system32> cd C:\Users\knuj9\Downloads\mimikatz_trunk\x64
PS C:\Users\knuj9\Downloads\mimikatz_trunk\x64> .\mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com **/

mimikatz #
```

Go to my Wazuh under events. Type in Mimikatz. However I initially did not see events as Sysmon did not trigger any alerts or rules from Wazuh. This is because by default Wazuh does not log everything. It will only log when a rule or alert is triggered. But we can change this by going to the Wazuh manager and configuring the ossec.conf file to make it so it logs everything

or create a rule that looks at specific events.



Lets modify the ossec.conf to log everything. To do this I will need to log into the wazuh CLI
After logging into the root@Wazuh we will make a copy of the ossec.conf file before we make changes and place it in my home dir.

```
*** System restart required ***
Last login: Mon Mar 11 16:43:55 2024 from 47.205.211.221
root@Wazuh:~# cp /var/ossec/etc/ossec.conf ~/ossec-backup.conf
```

```
root@Wazuh:~# ls
ossec-backup.conf  snap wazuh-install-files  wazuh-install-files.tar  wazuh-install.sh
root@Wazuh:~# nano /var/ossec/etc/ossec.conf
```

Logall and logall_json are set to no, we need to change these to yes

```

<!--
Wazuh - Manager - Default configuration for ubuntu 22.04
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>

  <logall>yes</logall>
  <logall_json>yes</logall_json>

```

Save file and restart Wazuh manager

```

root@wazuh:~# nano /var/ossec/etc/ossec.conf
root@wazuh:~# systemctl restart wazuh-manager.service

```

This will force Wazuh to archive all the files in a file called Archives

```

root@wazuh:~# cd /var/ossec/logs/archives/
root@wazuh:/var/ossec/logs/archives# ls
2024 archives.json archives.log
root@wazuh:/var/ossec/logs/archives#

```

To have Wazuh ingest the logs we need to change the config in file beat

```

2024 archives.json archives.log
root@wazuh:/var/ossec/logs/archives# nano /etc/filebeat/filebeat.yml

```

Nano into filebeat.yml and change archives enabled to 'true'

```

# - <elasticsearch_ip_node_2>:9200
# - <elasticsearch_ip_node_3>:9200

output.elasticsearch:
  protocol: https
  username: ${username}
  password: ${password}
  ssl.certificate_authorities:
    - /etc/filebeat/certs/root-ca.pem
  ssl.certificate: "/etc/filebeat/certs/wazuh-server.pem"
  ssl.key: "/etc/filebeat/certs/wazuh-server-key.pem"
setup.template.json.enabled: true
setup.template.json.path: '/etc/filebeat/wazuh-template.json'
setup.template.json.name: 'wazuh'
setup.ilm.overwrite: true
setup.ilm.enabled: false

filebeat.modules:
  - module: wazuh
    alerts:
      enabled: true
    archives:
      enabled: true

logging.level: info
logging.to_files: true
logging.files:
  path: /var/log/filebeat
  name: filebeat

```

Be sure to restart filebeat as with any config changes

```

root@wazuh:/var/ossec/logs/archives# nano /etc/filebeat/filebeat.yml
root@wazuh:/var/ossec/logs/archives# systemctl restart filebeat
root@wazuh:/var/ossec/logs/archives#

```

Now I will go back to wazuh dashboard>stack management> index pattern> create index
-I will create index for the archives so we can see the all the logs regardless if wazuh triggered an alert.

Stack Management

Index patterns

a

OpenSearch Dashboards ⓘ
[Index Patterns](#)
Saved Objects
Advanced Settings

Index patterns

Create and manage the index patterns that help you retrieve your data from OpenSearch.

Search...

Pattern ↑

wazuh-alerts-*

Default

wazuh-monitoring-*

wazuh-statistics-*

Rows per page: 10 ▾

< 1 >

Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22`, or **multiple** data sources, `filebeat-*`.

[Read documentation](#)

Step 1 of 2: Define an index pattern

Index pattern name

`wazuh-archives-*`

Next step >

Use an asterisk (*) to match multiple indices. Spaces and the characters `\, /, ?, ", <, >, |` are not allowed.

☐ Include system and hidden indices

✓ Your index pattern matches 1 source.

wazuh-archives-4.x-2024.03.15

Index

Rows per page: 10 ▾

Activate Windows

Create index pattern

An index pattern can match a single source, for example, `filebeat-*` .

[Read documentation](#) 

Step 2 of 2: Configure settings

Specify settings for your **wazuh-archives-*** index pattern.

Select a primary time field for use with the global time filter.

Time field

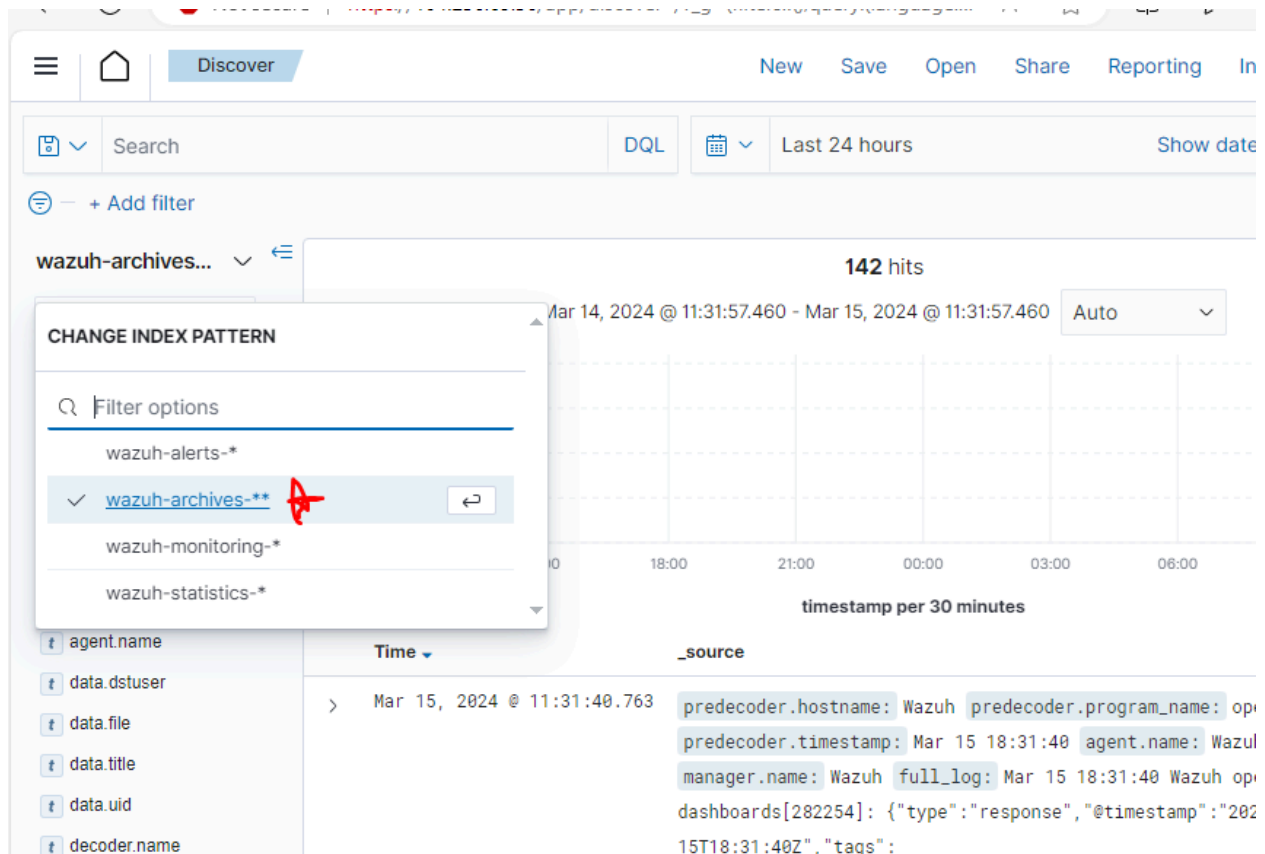
Refresh

timestamp



Create index pattern

Go back to discover and select the wazuh-archive index we just made.



This is important as Wazuh by default will not log anything. We enabled wazuh to archive everything for our test regardless if it triggers or not.

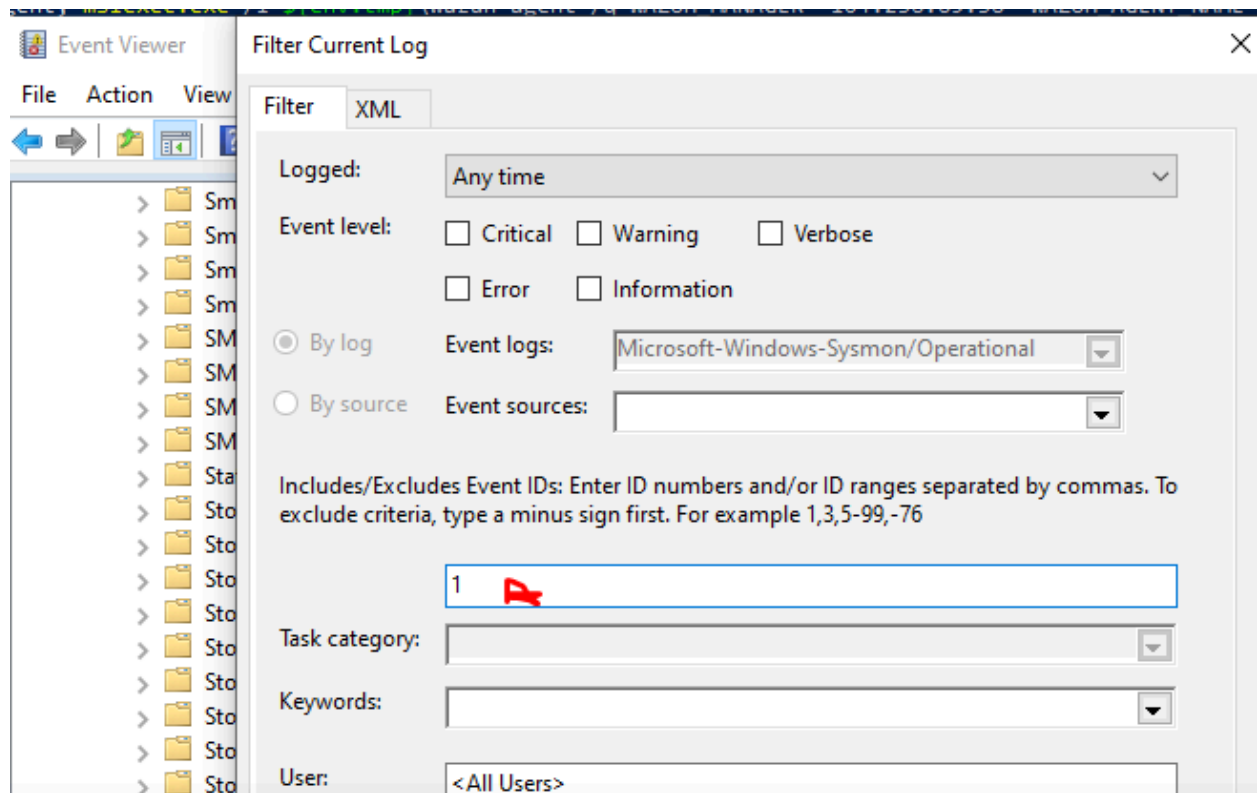
Lets restart mimikatz

```
mimikatz # exit
Bye!
PS C:\Users\knuj9\Downloads\mimikatz_trunk\x64> .\mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz #
```

And check event view to ensure Sysmon is capturing mimikatz



We will filter with Event ID 1 as this is for process creations.

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 366

Level	Date and Time	Source	Event ID	Task Ca...
Information	3/15/2024 11:53:51 AM	Sysmon	1	Proces...
Information	3/15/2024 11:53:36 AM	Sysmon	1	Proces...
Information	3/15/2024 11:52:25 AM	Sysmon	1	Proces...
Information	3/15/2024 11:52:20 AM	Sysmon	1	Proces...
Information	3/15/2024 11:49:15 AM	Sysmon	1	Proces...

Event 1, Sysmon

General Details

Process Create:
 RuleName: technique_id=T1036,technique_name=Masquerading
 UtcTime: 2024-03-15 18:53:51.777
 ProcessGuid: {23402b15-993f-65f4-7309-000000000200}
 ProcessId: 14816
 Image: C:\Users\knuj9\Downloads\mimikatz_trunk\x64\mimikatz.exe
 FileVersion: 2.2.0.0
 Description: mimikatz for Windows
 Product: mimikatz
 Company: gentilkiwi (Benjamin DELPY)
 OriginalFileName: mimikatz.exe
 CommandLine: "C:\Users\knuj9\Downloads\mimikatz_trunk\x64\mimikatz.exe"

Log Name: Microsoft-Windows-Sysmon/Operational

Sysmon is generating on my windows machine and I configured ossec.conf to push this data to wazuh. I will check Wazuh manager again and grep for Mimikatz

```
root@wazuh:/var/ossec/logs/archives# systemctl restart filebeat
root@wazuh:/var/ossec/logs/archives# cat archives.json | grep -i mimikatz
```

```
}
2024 Mar 27 15:50:07 (mydfir) any->EventChannel {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":{"5770385f-c22a-43e0-bf4c-06f5698ffbd9"},"eventID":"7","version":"3","level":"4","task":"7","opcode":"0","keywords":"0x8000000000000000","systemTime":"2024-03-27T15:50:05.8484189Z","eventRecordID":"19140","processID":"6604","threadID":"2264","channel":"Microsoft-Windows-Sysmon/Operational","computer":"DESKTOP-9AVBRKK","severityValue":"INFORMATION","message":"\\\"Image loaded:\\\"\\nRuleName: technique_id=T1574.002,technique_name=DLL Side-Loading\\\"\\nUtcTime: 2024-03-27 15:50:05.751\\\"\\nProcessGuid: {23402b15-402d-6604-540b-000000000200}\\\"\\nProcessId: 7004\\\"\\nImage: C:\\Users\\knuj9\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe\\\"\\nImageLoaded: C:\\Users\\knuj9\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe\\\"\\nFileVersion: 2.2.0.0\\\"\\nDescription: mimikatz for Windows\\\"\\nProduct: mimikatz\\\"\\nCompany: gentilkiwi (Benjamin DELPY)\\\"\\nOriginalFileName: mimikatz.exe\\\"\\nHashes: SHA1=E3B6EA8C46FA831CECF6235A5CF48B384AE8D69,MD5=29EFD64DD3C7FE1E2B022B7AD73A1BA5,SHA256=61C0810A23580CF492A68A4F7654566108331E7A4134C968C2D6A05261B2D8A1,IMPHASH=55EE500B84BD49F27A98AE456D8EDF\\\"\\nSigned: false\\\"\\nSignature: -\\\"\\nSignatureStatus: Unavailable\\\"\\nUser: DESKTOP-9AVBRKK\\\"\\nknuj9\\\""},"eventdata":{"ruleName":"technique_id=T1574.002,technique_name=DLL Side-Loading","utcTime":"2024-03-27 15:50:05.751","processGuid":{"23402b15-402d-6604-540b-000000000200"},"processId":"7004","image":{"C:\\Users\\knuj9\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe","imageLoaded":{"C:\\Users\\knuj9\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe","fileVersion":"2.2.0.0"},"description":"mimikatz for Windows","product":"mimikatz","company":"gentilkiwi (Benjamin DELPY)","originalFileName":"mimikatz.exe","hashes":{"SHA1=E3B6EA8C46FA831CECF6235A5CF48B384AE8D69,MD5=29EFD64DD3C7FE1E2B022B7AD73A1BA5,SHA256=61C0810A23580CF492A68A4F7654566108331E7A4134C968C2D6A05261B2D8A1,IMPHASH=55EE500B84BD49F27A98AE456D8EDF"},"signed":"false","signatureStatus":"Unavailable","user":"DESKTOP-9AVBRKK\\knuj9"}}Go to Settings to activate Windows.
root@wazuh:/var/ossec/logs/archives#
```

Going back to our dashboard in wazuh and using the wazuh archives search we can see it has now logged mimikatz there as well.

Expanded document

View surrounding documents

View single document

Table

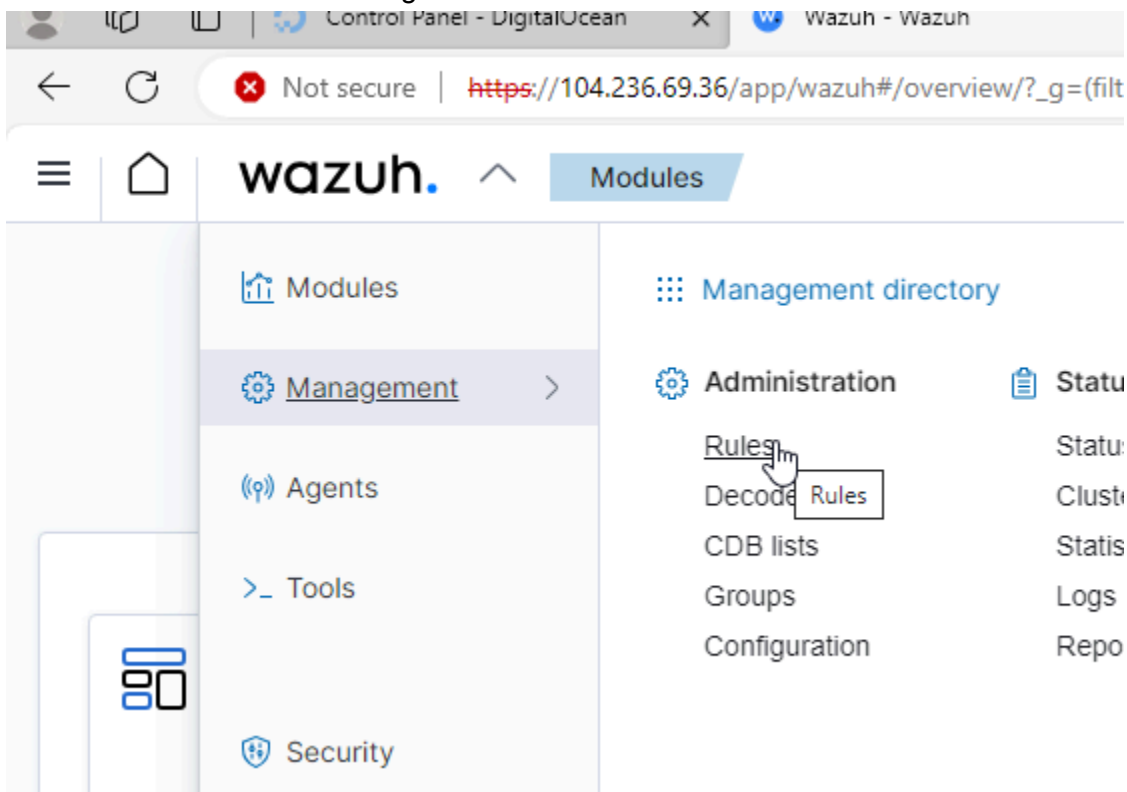
JSON

@timestamp	Mar 27, 2024 @ 08:50:07.361
_index	wazuh-archives-4.x-2024.03.27
agent.id	001
agent.ip	10.0.2.15
agent.name	mydfir
data.win.eventdata.company	gentilkiwi (Benjamin DELPY)
data.win.eventdata.description	mimikatz for Windows
data.win.eventdata.fileVersion	2.2.0.0
data.win.eventdata.hashes	SHA1=E3B6EA8C46FA831CEC6F235A5CF48B38A4AE8D69, MD5=29EFD64DD3C7FE1E2B022B7AD73A1BA5, SHA256=61C0810A23

Activate Windows

Go to Settings to activate Windows.

Now to set some rules we can go back to the wazuh home to utilize the dashboard



We are specifically interested in the event ID 1 for sysmon. Select manage rule files and type in sysmon

Rules files (10) [Manage rules](#) [Add new rules file](#) [Import files](#)

From here you can manage your rules files.

[Download](#) [Export](#)

File ↑	Path	Actions
0330-sysmon_rules.xml		
0595-win-sysmon_rules.xml		
<u>0800-sysmon_id_1.xml</u>	ruleset/rules	-
0810-sysmon_id_3.xml	ruleset/rules	
0820-sysmon_id_7.xml	ruleset/rules	

Note: A tooltip points to the eye icon for 0800-sysmon_id_1.xml with the text: "View the content of 0800-sysmon_id_1.xml"

I will copy one of these rules to use in my custom rule to detect mimikatz

0800-sysmon_id_1.xml

```

1 <!--
2 Copyright (C) 2015, Wazuh Inc.
3 -->
4
5 <!--
6 Sysmon Event ID 1 rules: 9200
7 -->
8
9 <group name="sysmon,sysmon_eid1">
10
11 <rule id="92000" level="4">
12   <if_group>sysmon_event1</if_group>
13   <field name="win.eventdata.data" type="string">script\.exe</field>
14   <options>no_full_log</options>
15   <description>Scripting interpreter spawned a new process</description>
16   <mitre>
17     <id>T1059.005</id>
18   </mitre>
19 </rule>
20
21 <rule id="92001" level="6">
22   <if_sid>92000</if_sid>
23   <field name="win.eventdata.commandLine" type="pcre2">(?!\\)(c|w)script\.exe.+\\
24     .(bat|cmd|lnk|pif|vbs|vbe|js|wsh|ps1)</field>
25   <options>no_full_log</options>

```

Note: A context menu is open over the first rule, showing options like Copy, Print, Read aloud, Open in sidebar, Add page to Collections, Share, Screenshot, and Inspect.

I will go to make a custom rule in the local rules and paste this into that file. Be aware of the indentation as they use spaces and the rule IDs start at 100000. You can see the rule above this one is 100001 so i cannot use that.

```

3 <!-- Modify it at your will. -->
4 <!-- Copyright (C) 2015, Wazuh Inc. -->
5
6 <!-- Example -->
7 <group name="local,syslog,sshd,">
8
9   <!--
10   Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
11   -->
12   <rule id="100001" level="5">
13     <if_sid>5716</if_sid>
14     <srcip>1.1.1.1</srcip>
15     <description>sshd: authentication failed from IP 1.1.1.1.</description>
16     <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
17   </rule>
18
19   <rule id="92000" level="4">
20     <if_group>sysmon_event1</if_group>
21     <field name="win.eventdata.parentImage" type="pcre2">(?!i)\\(c|w)script\\.exe</field>
22     <options>no_full_log</options>
23     <description>Scripting interpreter spawned a new process</description>
24     <mitre>
25       <id>T1059.005</id>
26     </mitre>
27   </rule>

```

We will use 100002, and change the level to 15, this is the max level and the higher the level, the more important. Also will change the "parentImage" to "originalFileName". The field name is capitalized so we must match it or else the rule will never be used.

```

</rule>

<rule id="100002" level="15">
  <if_group>sysmon_event1</if_group>
  <field name="win.eventdata.originalFileName" type="pcre2">(?!i)\\(c|w)script\\.exe</field>
  <options>no_full_log</options>
  <description>Scripting interpreter spawned a new process</description>
  <mitre>
    <id>T1059.005</id>
  </mitre>
</rule>

```

The pcre2 is basically regex. Set to ignore case sensitivity. We will edit this to search for mimikatz.

```

<rule id="100002" level="15">
  <if_group>sysmon_event1</if_group>
  <field name="win.eventdata.originalFileName" type="pcre2">(?!i)mimikatz\\.exe</field>
  <options>no_full_log</options>
  <description>Scripting interpreter spawned a new process</description>
  <mitre>
    <id>T1059.005</id>
  </mitre>
</rule>

```

Next:

Remove option for no full logs because we want the full logs.

Change description to "Mimikatz Usage Detected"

And mitre id to T1003 which is credentialed dumping

```

<rule id="100002" level="15">
  <if_group>sysmon_event1</if_group>
  <field name="win.eventdata.originalFileName" type="pcr2">(?!mimikatz\.exe</field>
  <description>Mimikatz Usage Detected</description>
  <mitre>
    <id>T1003</id>
  </mitre>
</rule>

```

Save and restart manager. Go back to dashboard.

To test this we can see nothing is running at the moment. We will then change the mimikatz.exe file to "youareawesome" and re run it on our command prompt and see if wazuh will pick it up with the new rule.

The screenshot shows the Wazuh Security Alerts dashboard with a table of alerts. Below the dashboard, a Windows file explorer window shows the 'mimikatz_trunk' directory where 'mimikatz.exe' has been replaced by 'youareawesome.exe'.

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Mar 27, 2024 @ 09:29:50.440	000	Wazuh			Wazuh server started.	3	502
Mar 27, 2024 @ 09:29:38.356	000	Wazuh			Host-based anomaly detection event (rootcheck).	7	510
Mar 27, 2024 @ 09:29:38.303	000	Wazuh			Host-based anomaly detection event (rootcheck).	7	510
Mar 27, 2024 @ 09:28:43.032	001	mydfir	T1053.005	Execution, Persistence, Privilege Escalation	Process loaded taskschd.dll module. May be used to create delayed malware execution	4	92154

File Explorer Path: This PC > Downloads > mimikatz_trunk > Win32

Files in mimikatz_trunk > Win32:

- mimidrv.sys
- youareawesome.exe** (selected)
- mimilib.dll
- mimilove
- mimispool.dll

```
Bye!
PS C:\Users\knuj9\Downloads\mimikatz_trunk\x64> .\mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
# \ / ##    > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # exit
Bye!
PS C:\Users\knuj9\Downloads\mimikatz_trunk\x64> .\youareawesome.exe
```

Security Alerts							
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Mar 27, 2024 > @ 09:37:12.299	001	mydfir	<u>T1003</u>	Credential Access	Mimikatz Usage Detected	15	100002
Mar 27, 2024 > @ 09:29:50.440	000	Wazuh			Wazuh server started.	3	502

Boom! Because we changed the rule to look at the original File Name and not the image regardless of the name change.