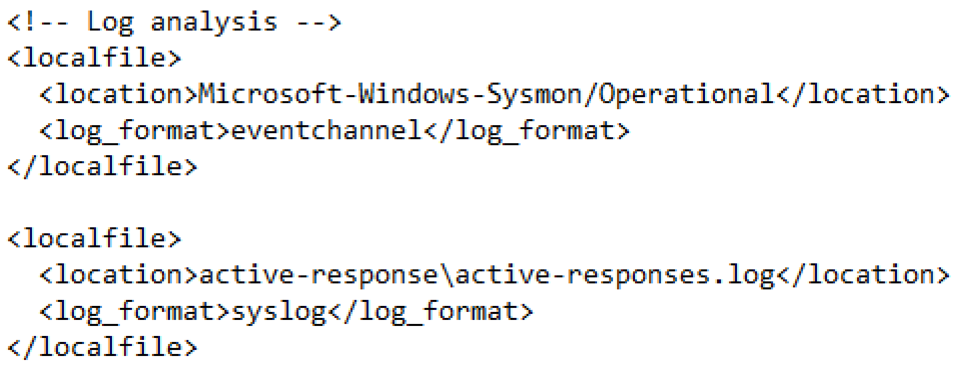
Wazuh Project

Installing Wazuh

1- `curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh`
2- `curl -sO https://packages.wazuh.com/4.9/config.yml`
3- `sudo nano config.yml` change the ip to yours
4- `sudo bash ./wazuh-install.sh --generate-config-files -i`
5- `sudo bash ./wazuh-install.sh -a -i`
Wait until the installation completes and note the **username** and **password** provided.
Navigate to your Wazuh dashboard `https://<your_ip_address>` Your Wazuh dashboard should now be accessible!

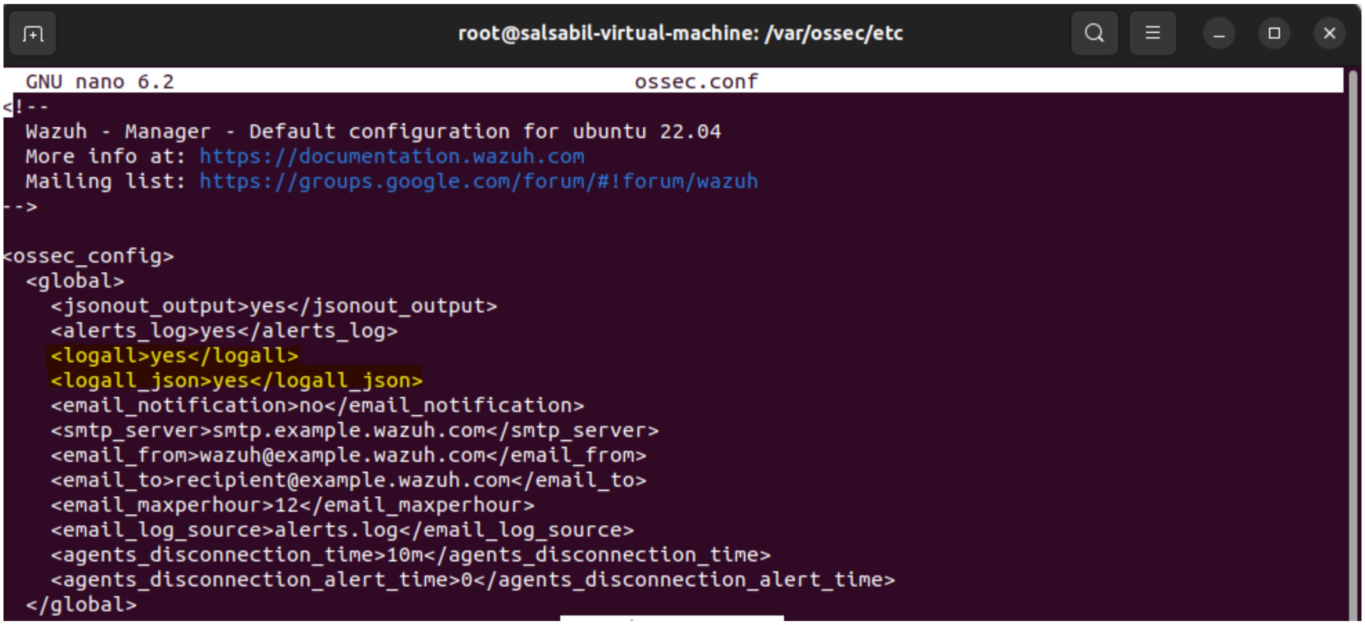
Detecting mimikatz

To enable Wazuh to ingest **Sysmon logs**, you need to update the `ossec.conf` file with a focus on Sysmon log collection.



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

<localfile>
  <location>active-response\active-responses.log</location>
  <log_format>syslog</log_format>
</localfile>
```

By default, Wazuh is not configured to capture all Sysmon events. To ensure proper log ingestion, update the settings in the Wazuh **manager's ossec.conf** file

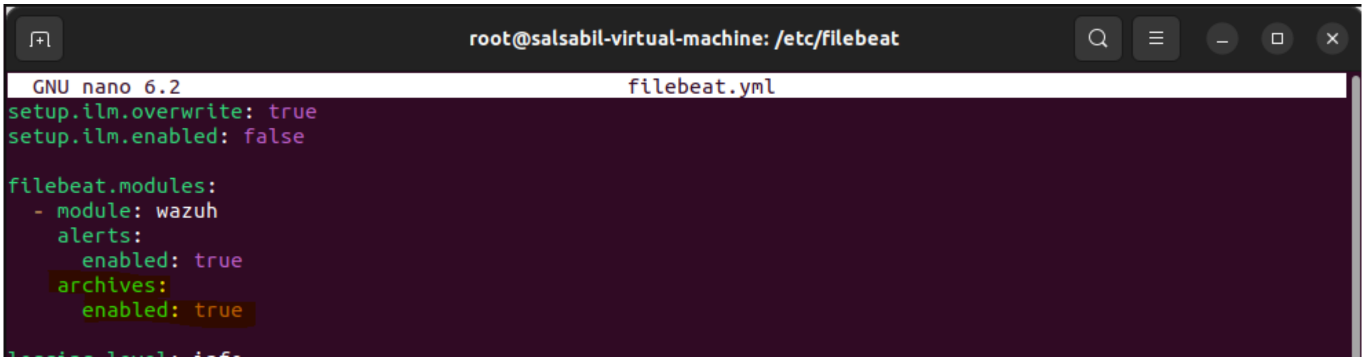


```
  GNU nano 6.2                                  ossec.conf
<!--
  Wazuh - Manager - Default configuration for ubuntu 22.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>yes</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>
```

Restart the Wazuh manager service to apply configuration changes:

`systemctl restart wazuh-manager.service`

- Open the Filebeat configuration file located at:
  `/var/filebeat/filebeat.yml`
- Change the relevant setting from `false` to `true` to enable log archiving.



```
  GNU nano 6.2                                  filebeat.yml
setup.ilm.overwrite: true
setup.ilm.enabled: false

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

logging.level: info
```

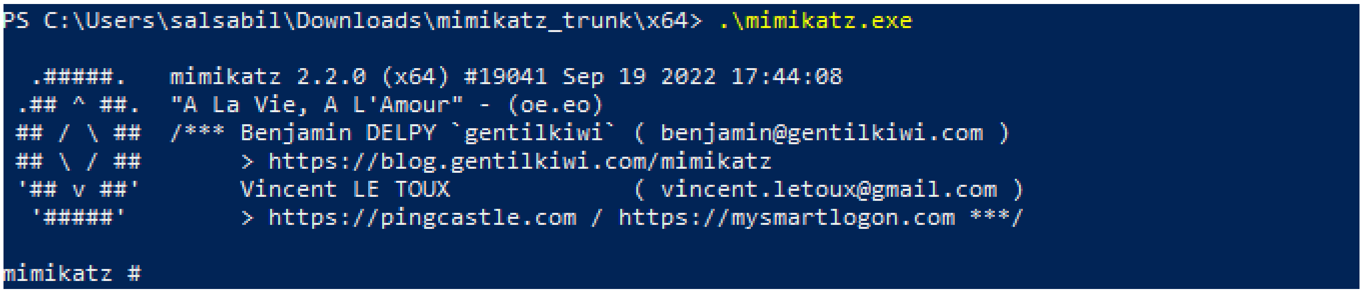
Restart the Filebeat service to apply changes:

`systemctl restart filebeat`

Create an index in Wazuh:

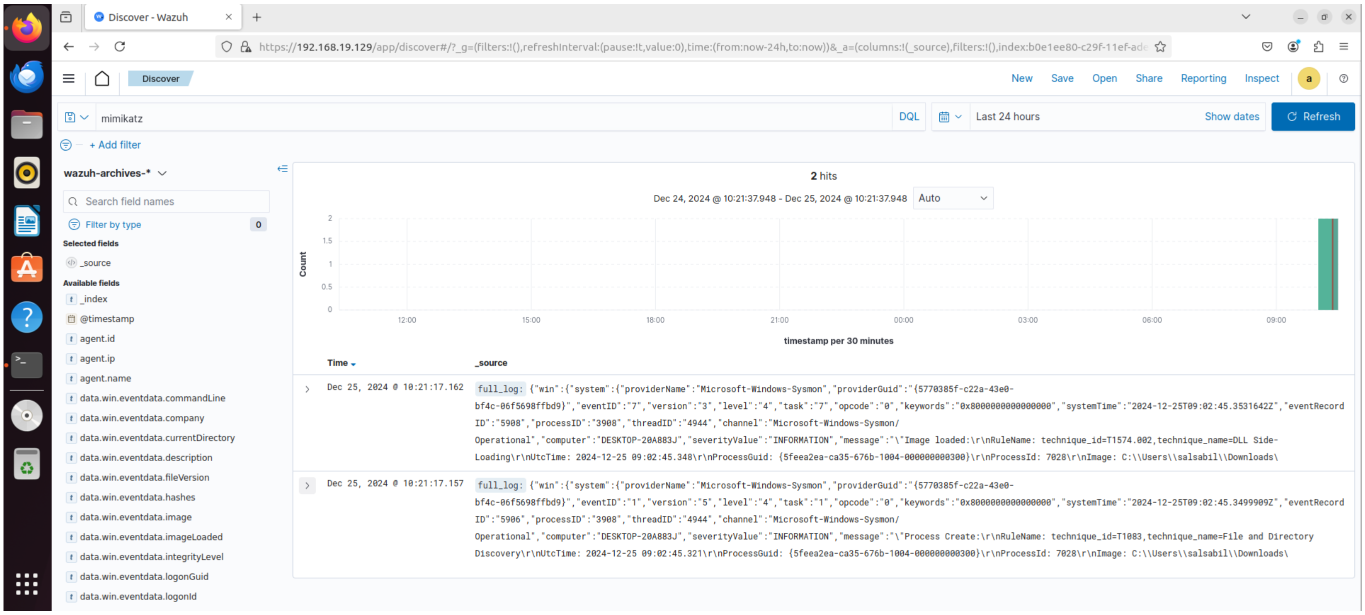
- Go to **Stack Management** → **Index Patterns** and create a new index for logs.

Run mimikatz

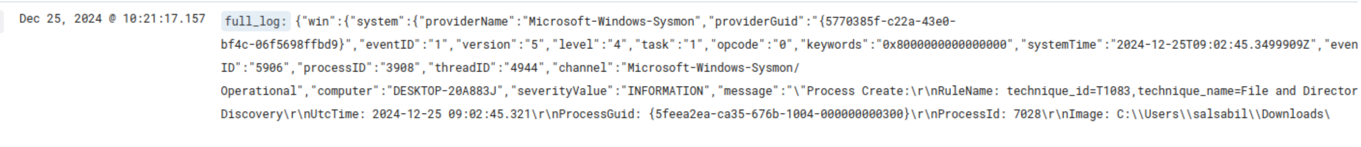


```
PS C:\Users\salsabil\Downloads\mimikatz_trunk\x64> .\mimikatz.exe

  .#####.   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 #
```

Successfully detected mimikatz with wazuh

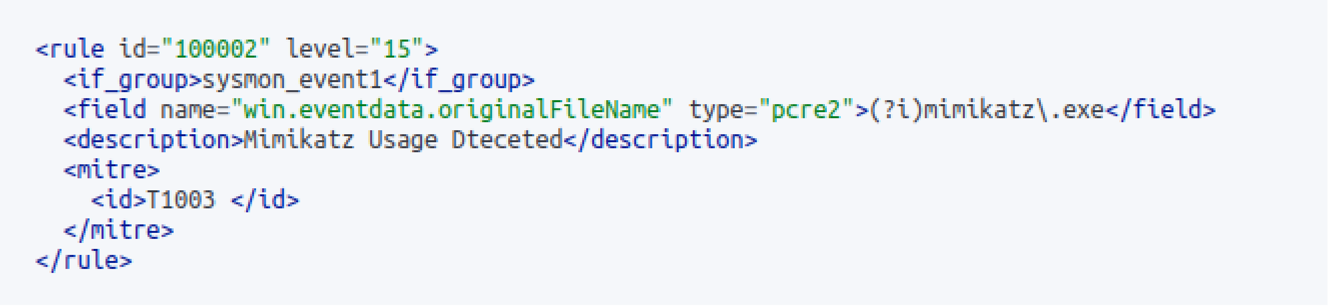

Discover - Wazuh
https://192.168.19.129/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(),index:b0e1ee80-c29f-11ef-ade
Discover
New
Save
Open
Share
Reporting
Inspect
mimikatz
DQL
Last 24 hours
Show dates
Refresh
+ Add filter
wazuh-archives-*
Search field names
Filter by type
0
Selected fields
_source
Available fields
_index
@timestamp
agent.id
agent.ip
agent.name
data.win.eventdata.commandLine
data.win.eventdata.company
data.win.eventdata.currentDirectory
data.win.eventdata.description
data.win.eventdata.fileVersion
data.win.eventdata.hashes
data.win.eventdata.image
data.win.eventdata.imageLoaded
data.win.eventdata.integrityLevel
data.win.eventdata.logonGuid
data.win.eventdata.logonId
2 hits
Dec 24, 2024 @ 10:21:37.948 - Dec 25, 2024 @ 10:21:37.948
Auto
Count
2
1.5
1
0.5
0
12:00
15:00
18:00
21:00
00:00
03:00
06:00
09:00
timestamp per 30 minutes
Time
_source

```
Dec 25, 2024 @ 10:21:17.162  full_log: {"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":"2024-12-25T09:02:45.3531642Z","eventRecord
ID":"5908","processID":"3908","threadID":"4944","channel":"Microsoft-Windows-Sysmon/
Operational","computer":"DESKTOP-20A883J","severityValue":"INFORMATION","message":"\"Image loaded:\r\nRuleName: technique_id=T1574.002,technique_name=DLL Side-
Loading\r\nUtcTime: 2024-12-25 09:02:45.348\r\nProcessGuid: {5feea2ea-ca35-676b-1004-000000000300}\r\nProcessId: 7028\r\nImage: C:\\Users\\salsabil\\Downloads\

Dec 25, 2024 @ 10:21:17.157  full_log: {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-
bf4c-06f5698ffbd9}","eventID":"1","version":"5","level":"4","task":"1","opcode":"0","keywords":"0x8000000000000000","systemTime":"2024-12-25T09:02:45.3499909Z","eventRecord
ID":"5906","processID":"3908","threadID":"4944","channel":"Microsoft-Windows-Sysmon/
Operational","computer":"DESKTOP-20A883J","severityValue":"INFORMATION","message":"\"Process Create:\r\nRuleName: technique_id=T1083,technique_name=File and Directory
Discovery\r\nUtcTime: 2024-12-25 09:02:45.321\r\nProcessGuid: {5feea2ea-ca35-676b-1004-000000000300}\r\nProcessId: 7028\r\nImage: C:\\Users\\salsabil\\Downloads\
```



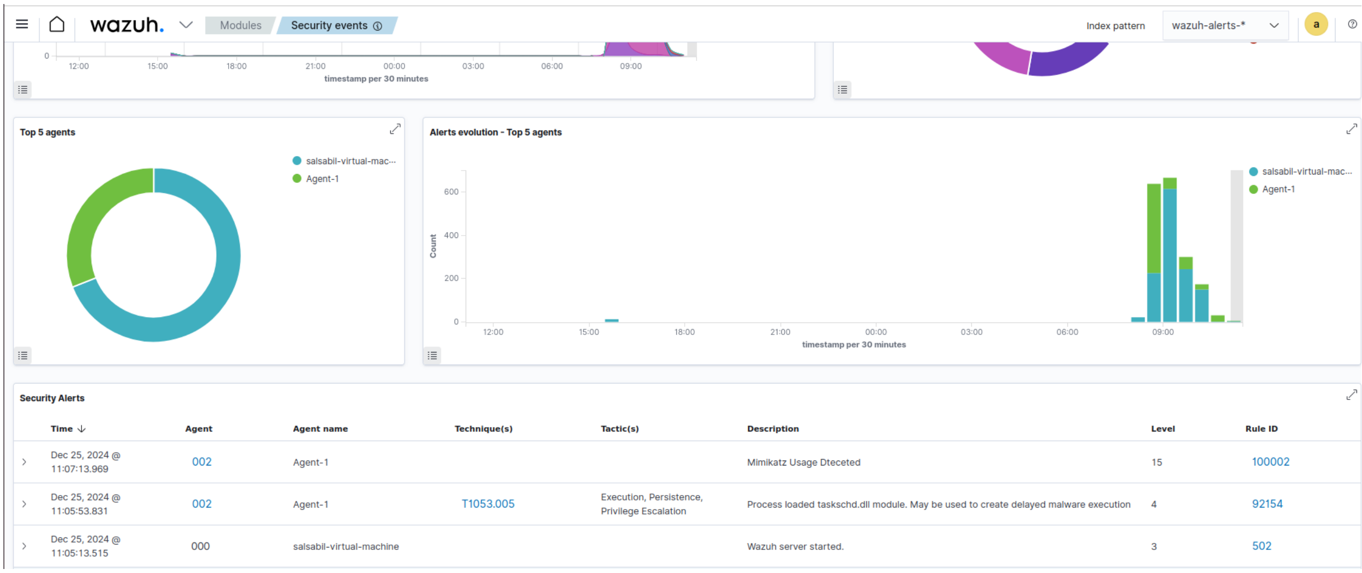
```
Dec 25, 2024 @ 10:21:17.157  full_log: {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-
bf4c-06f5698ffbd9}","eventID":"1","version":"5","level":"4","task":"1","opcode":"0","keywords":"0x8000000000000000","systemTime":"2024-12-25T09:02:45.3499909Z","even
ID":"5906","processID":"3908","threadID":"4944","channel":"Microsoft-Windows-Sysmon/
Operational","computer":"DESKTOP-20A883J","severityValue":"INFORMATION","message":"\"Process Create:\r\nRuleName: technique_id=T1083,technique_name=File and Director
Discovery\r\nUtcTime: 2024-12-25 09:02:45.321\r\nProcessGuid: {5feea2ea-ca35-676b-1004-000000000300}\r\nProcessId: 7028\r\nImage: C:\\Users\\salsabil\\Downloads\
```

Creating an Alert for Mimikatz Detection



```
<rule id="100002" level="15">
  <if_group>sysmon_event1</if_group>
  <field name="win.eventdata.originalFileName" type="pcre2">(?i)mimikatz\.exe</field>
  <description>Mimikatz Usage Dteceted</description>
  <mitre>
    <id>T1003 </id>
  </mitre>
</rule>
```

Here the alert message "Mimikatz Usage Detected"



Security Alerts

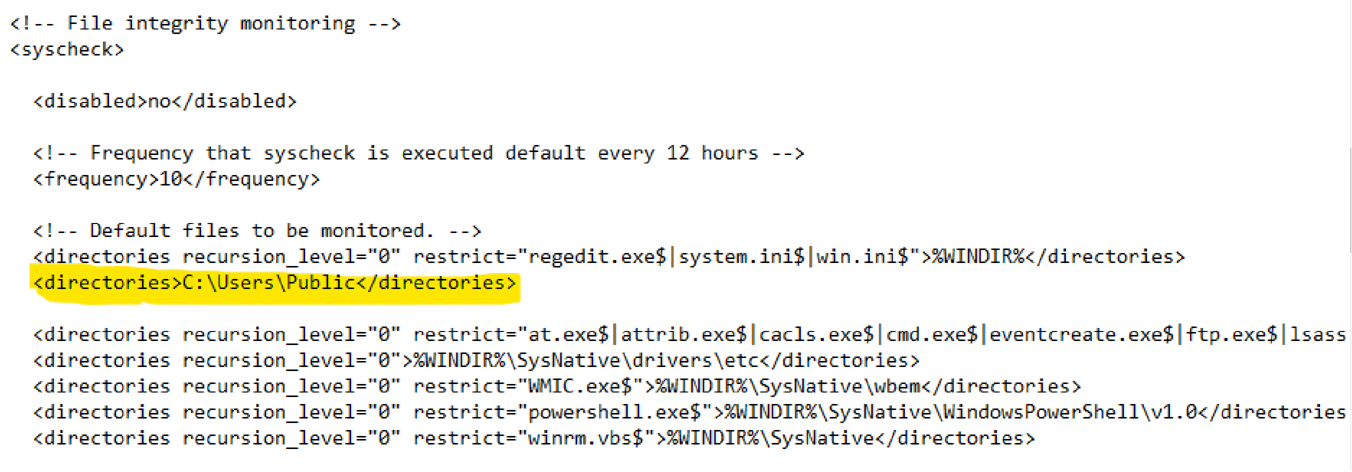
Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Dec 25, 2024 @ 11:07:13.969	002	Agent-1			Mimikatz Usage Dteceted	15	100002
Dec 25, 2024 @ 11:05:53.831	002	Agent-1	T1053.005	Execution, Persistence, Privilege Escalation	Process loaded taskschd.dll module. May be used to create delayed malware execution	4	92154
Dec 25, 2024 @ 11:05:13.515	000	salsabil-virtual-machine			Wazuh server started.	3	502

The Wazuh File Integrity Monitoring (FIM)

The **File Integrity Monitoring (FIM)** module in Wazuh helps monitor and detect changes in specific directories or files. Here's how to set it up and use it to monitor a directory for changes:

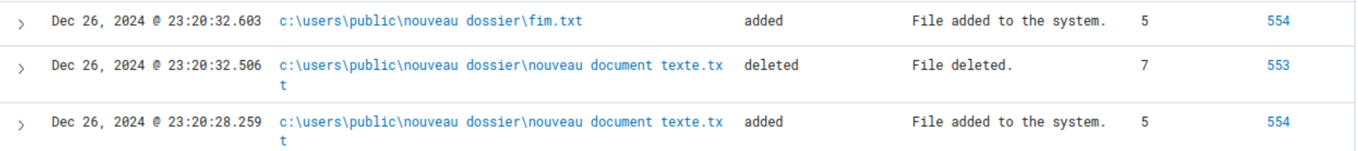
Specify the Directory to Monitor

- Add the path of the directory you want to monitor in the Wazuh configuration.
- For example, to monitor `C:\Users\Public`



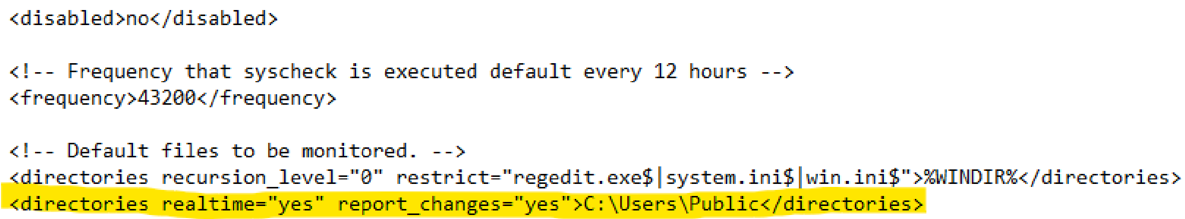
```
<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>10</frequency>

  <!-- Default files to be monitored. -->
  <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>
  <directories>C:\Users\Public</directories>

  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories
  <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>
```

Any changes made to the specified directory will be logged and detected by Wazuh.



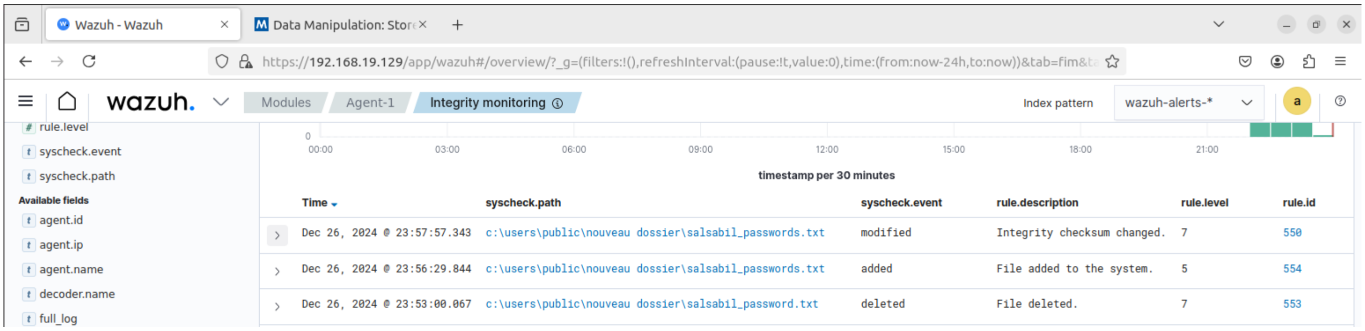
```
>  Dec 26, 2024 @ 23:20:32.603  c:\users\public\nouveau dossier\fim.txt                added    File added to the system.  5   554
>  Dec 26, 2024 @ 23:20:32.506  c:\users\public\nouveau dossier\nouveau document texte.tx  deleted  File deleted.              7   553
                                t
>  Dec 26, 2024 @ 23:20:28.259  c:\users\public\nouveau dossier\nouveau document texte.tx  added    File added to the system.  5   554
                                t
```

- Ensure **real-time monitoring** and **change reporting** are enabled in the FIM settings.
- Wazuh will report any detected modifications in the monitored directory.



```
<disabled>no</disabled>

<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>43200</frequency>

<!-- Default files to be monitored. -->
<directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>
<directories realtime="yes" report_changes="yes">C:\Users\Public</directories>
```

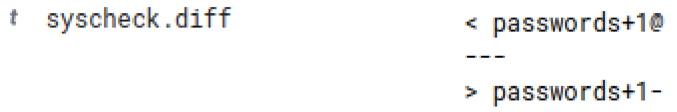
After modifying a file in the monitored directory, Wazuh detects the change and logs it



Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Dec 26, 2024 @ 23:57:57.343	c:\users\public\nouveau dossier\salsabil_passwords.txt	modified	Integrity checksum changed.	7	550
Dec 26, 2024 @ 23:56:29.844	c:\users\public\nouveau dossier\salsabil_passwords.txt	added	File added to the system.	5	554
Dec 26, 2024 @ 23:53:00.067	c:\users\public\nouveau dossier\salsabil_password.txt	deleted	File deleted.	7	553

The specific field `"syscheck.diff"` provides details of what was changed

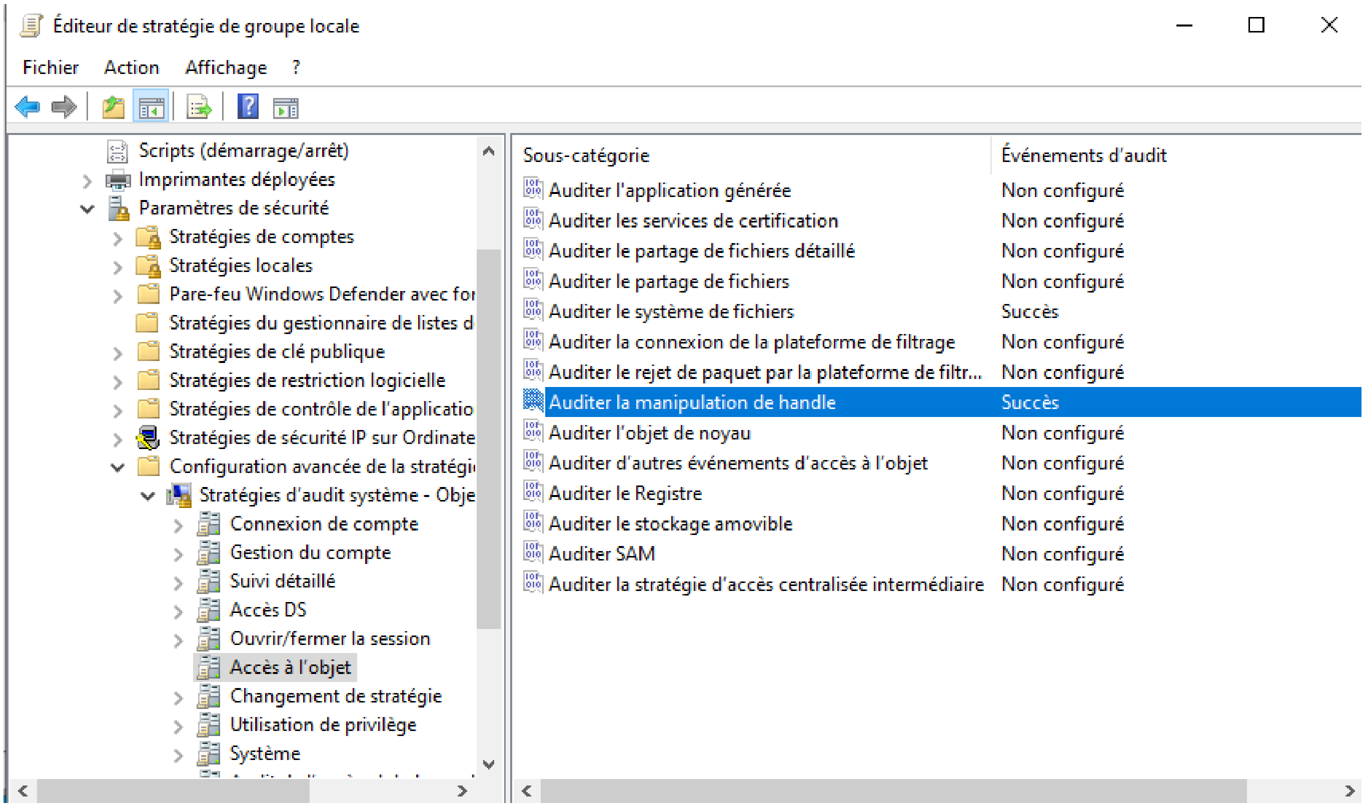
This allows you to pinpoint the exact modifications made to the file or directory



```
t  syscheck.diff          < passwords+1@
                          ---
                          > passwords+1-
```

Manual Configuration for Older Windows Versions

- In older Windows versions, the FIM configuration can be done manually.
- Customize the settings as shown below:

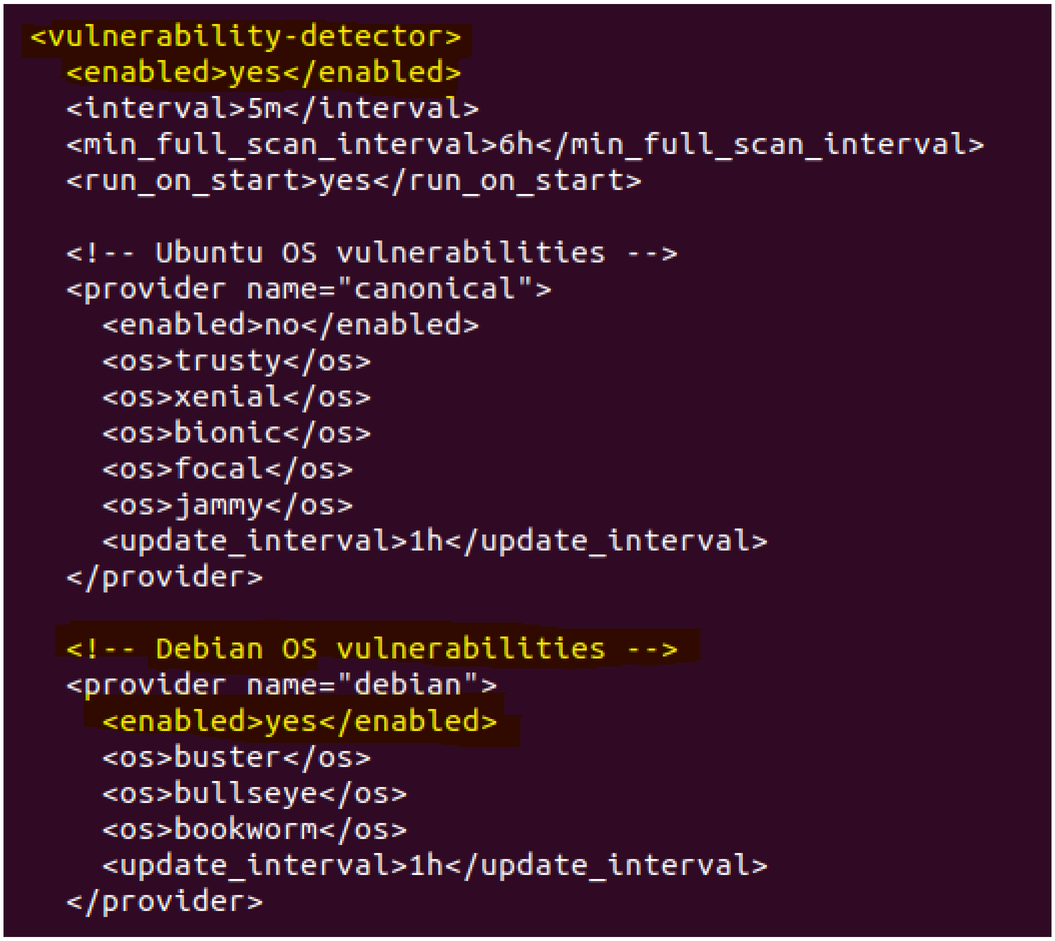


- Scripts (démarrage/arrêt)
- Imprimantes déployées
- Paramètres de sécurité
  - Stratégies de comptes
  - Stratégies locales
  - Pare-feu Windows Defender avec fo
  - Stratégies du gestionnaire de listes d
  - Stratégies de clé publique
  - Stratégies de restriction logicielle
  - Stratégies de contrôle de l'applicatio
  - Stratégies de sécurité IP sur Ordinate
  - Configuration avancée de la stratégi
    - Stratégies d'audit système - Obje
      - Connexion de compte
      - Gestion du compte
      - Suivi détaillé
      - Accès DS
      - Ouvrir/fermer la session
      - Accès à l'objet
      - Changement de stratégie
      - Utilisation de privilège
      - Système

Sous-catégorie	Événements d'audit
Auditer l'application générée	Non configuré
Auditer les services de certification	Non configuré
Auditer le partage de fichiers détaillé	Non configuré
Auditer le partage de fichiers	Non configuré
Auditer le système de fichiers	Succès
Auditer la connexion de la plateforme de filtrage	Non configuré
Auditer le rejet de paquet par la plateforme de filtr...	Non configuré
Auditer la manipulation de handle	Succès
Auditer l'objet de noyau	Non configuré
Auditer d'autres événements d'accès à l'objet	Non configuré
Auditer le Registre	Non configuré
Auditer le stockage amovible	Non configuré
Auditer SAM	Non configuré
Auditer la stratégie d'accès centralisée intermédiaire	Non configuré

Detecting Vulnerabilities

Modify the /var/ossec/etc/ossec.conf file

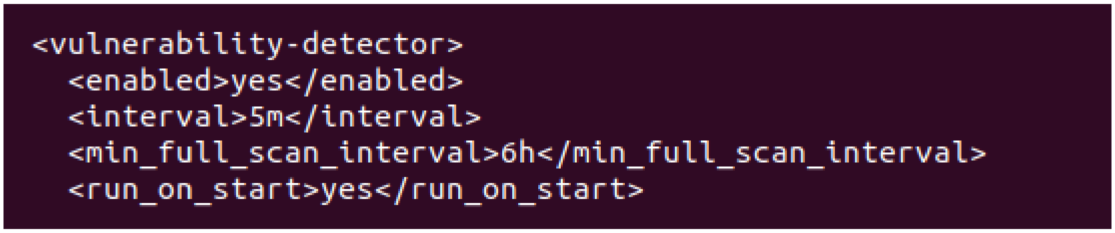


```
<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>no</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Debian OS vulnerabilities -->
  <provider name="debian">
    <enabled>yes</enabled>
    <os>buster</os>
    <os>bullseye</os>
    <os>bookworm</os>
    <update_interval>1h</update_interval>
  </provider>
```

Restart the Wazuh Manager

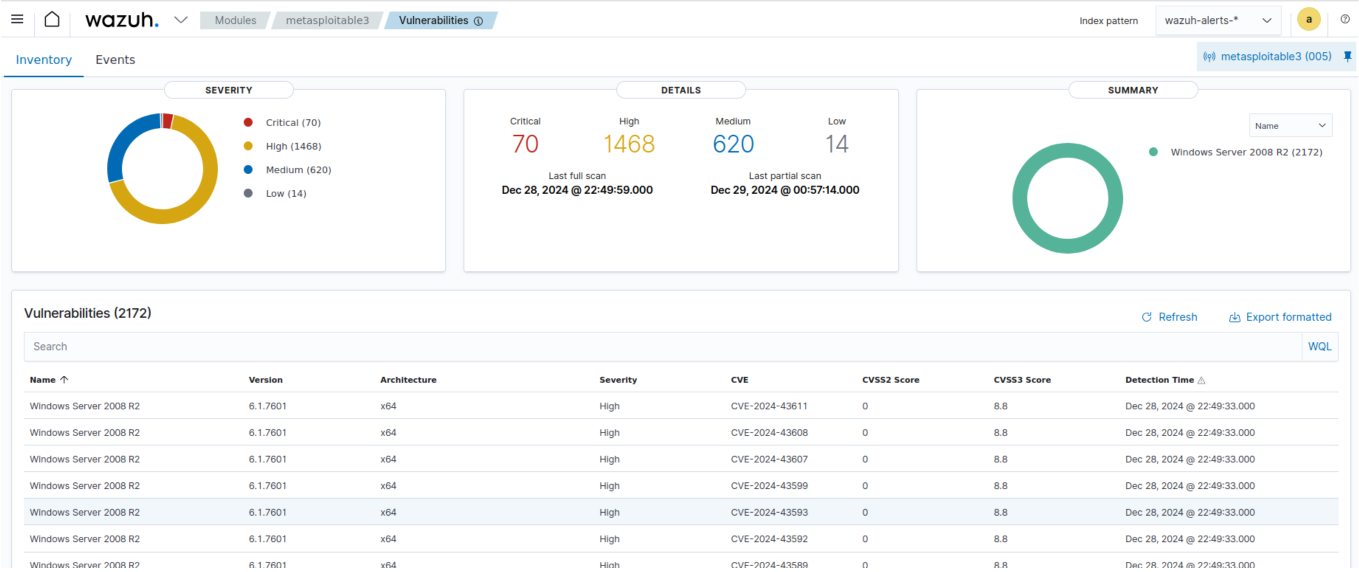
`service wazuh-manager restart`

Wazuh will now analyze installed software and detect vulnerabilities based on the configurations



```
<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>
```

Detailed metadata of the detected vulnerabilities will be displayed in the Wazuh dashboard and logs



SEVERITY

- ● Critical (70)
- ● High (1468)
- ● Medium (620)
- ● Low (14)

DETAILS

Critical	High	Medium	Low
70	1468	620	14

Last full scan
Dec 28, 2024 @ 22:49:59.000

Last partial scan
Dec 29, 2024 @ 00:57:14.000

SUMMARY

● Windows Server 2008 R2 (2172)

Vulnerabilities (2172)

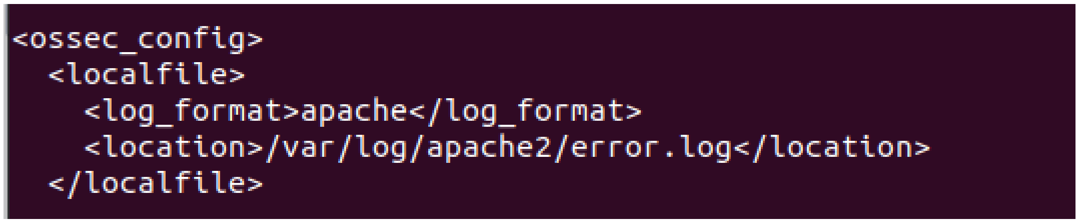
Name ↑	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time ⚠
Windows Server 2008 R2	6.1.7601	x64	High	CVE-2024-43611	0	8.8	Dec 28, 2024 @ 22:49:33.000
Windows Server 2008 R2	6.1.7601	x64	High	CVE-2024-43608	0	8.8	Dec 28, 2024 @ 22:49:33.000
Windows Server 2008 R2	6.1.7601	x64	High	CVE-2024-43607	0	8.8	Dec 28, 2024 @ 22:49:33.000
Windows Server 2008 R2	6.1.7601	x64	High	CVE-2024-43599	0	8.8	Dec 28, 2024 @ 22:49:33.000
Windows Server 2008 R2	6.1.7601	x64	High	CVE-2024-43593	0	8.8	Dec 28, 2024 @ 22:49:33.000
Windows Server 2008 R2	6.1.7601	x64	High	CVE-2024-43592	0	8.8	Dec 28, 2024 @ 22:49:33.000
Windows Server 2008 R2	6.1.7601	x64	High	CVE-2024-43589	0	8.8	Dec 28, 2024 @ 22:49:33.000

Detecting Sql Injection

Check the status of the Apache service to verify that the web server is running

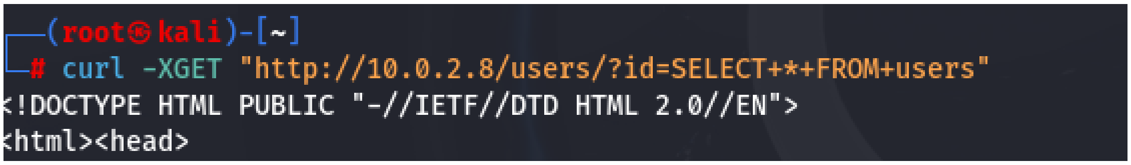
`sudo systemctl status apache2`

This allows the Wazuh agent to monitor the access logs of your Apache server



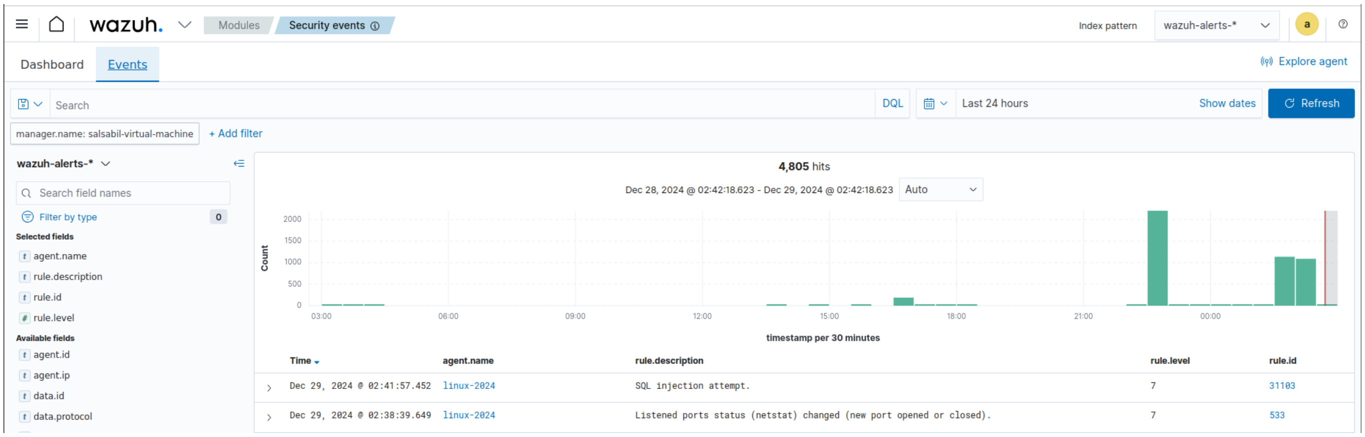
```
<ossec_config>
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/error.log</location>
  </localfile>
```

Execute the following command from the attacker endpoint



```
┌──(root㉿kali)-[~]
└─# curl -XGET "http://10.0.2.8/users/?id=SELECT+*+FROM+users"
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
```

Visualize the Alert in Wazuh



Time	agent.name	rule.description	rule.level	rule.id
Dec 29, 2024 @ 02:41:57.452	linux-2024	SQL injection attempt.	7	31103
Dec 29, 2024 @ 02:38:39.649	linux-2024	Listened ports status (netstat) changed (new port opened or closed).	7	533