



wazuh.

**FIM – File Integrity Monitoring
(Windows & Linux)**

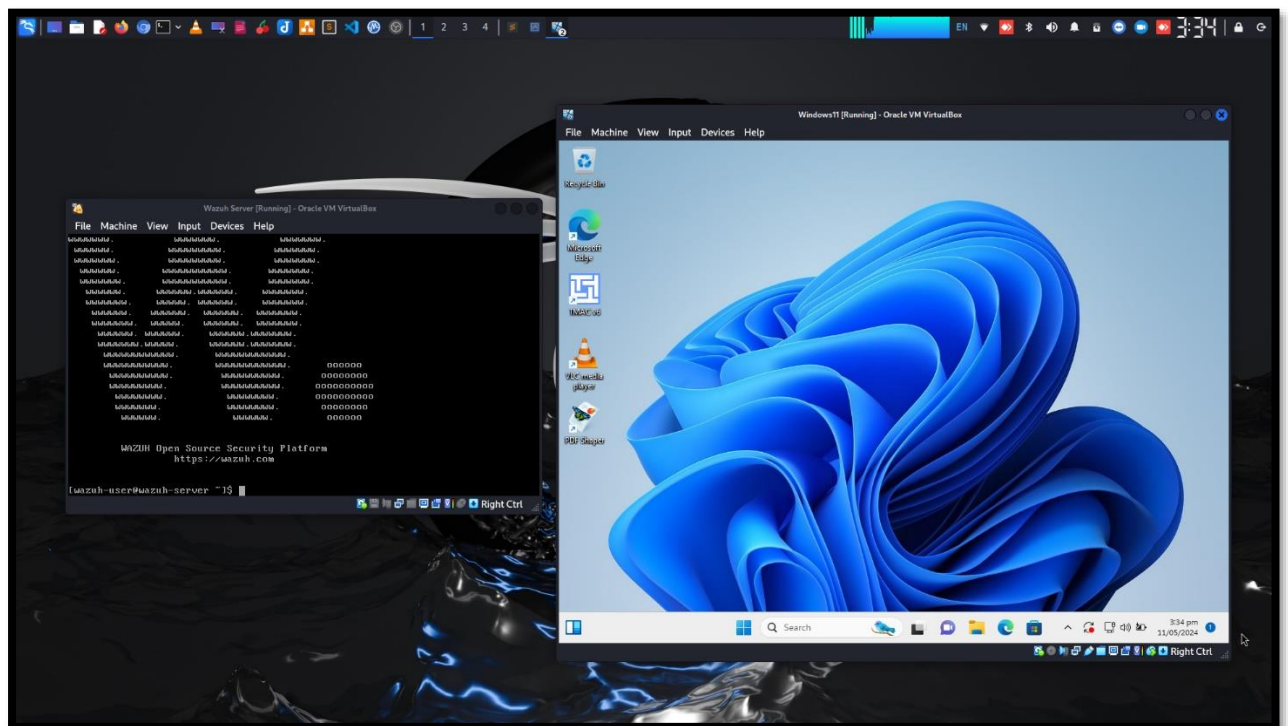
Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: [linkedin.com/in/moizuddinrafay](https://www.linkedin.com/in/moizuddinrafay)

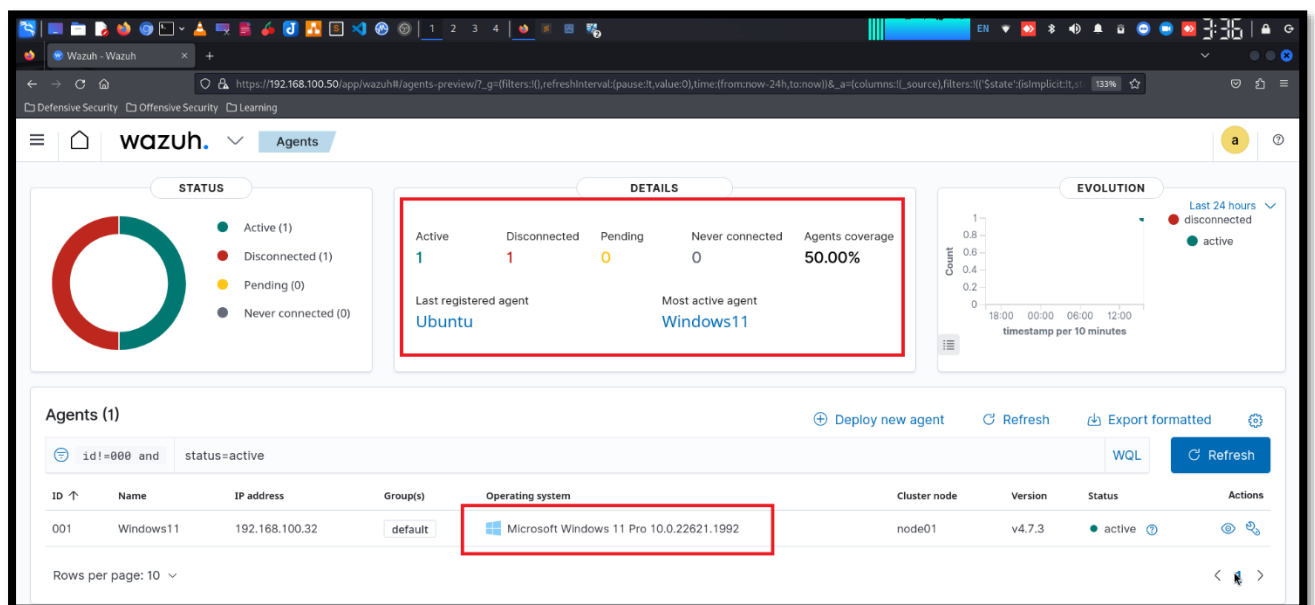
File Integrity Monitoring (FIM) is a critical component of cybersecurity that ensures the integrity of files and directories on a system. Wazuh, an open-source security monitoring platform, offers robust FIM capabilities to detect unauthorized changes to files and directories, helping organizations maintain the security and compliance of their systems.

- 1. Real-time Monitoring:** Wazuh continuously monitors file systems in real-time, detecting any modifications, additions, or deletions to files and directories.
- 2. Hash-based Verification:** Wazuh calculates cryptographic hashes (such as MD5, SHA-1, SHA-256) of files and compares them with predefined baseline values to identify any discrepancies indicative of tampering.
- 3. Customizable Policies:** Wazuh allows users to define custom policies based on their specific security requirements, enabling tailored monitoring and alerting for critical files and directories.
- 4. Alerting and Response:** Upon detecting unauthorized changes, Wazuh generates alerts and notifications in real-time, enabling prompt response to potential security incidents. These alerts can be integrated with SIEM platforms for centralized monitoring and analysis.
- 5. Centralized Management:** Wazuh provides centralized management capabilities through its management server, facilitating the configuration, deployment, and monitoring of FIM agents across multiple endpoints.
- 6. Compliance Auditing:** Wazuh FIM assists organizations in meeting compliance requirements by providing detailed audit trails and reports of file system activity, helping demonstrate adherence to regulatory standards such as PCI DSS, HIPAA, GDPR, and more.
- 7. Scalability and Flexibility:** Wazuh FIM is highly scalable and adaptable, suitable for environments ranging from small businesses to large enterprises, on-premises or in the cloud.

In my SOC lab environment Wazuh Server and Windows11-agent is running.

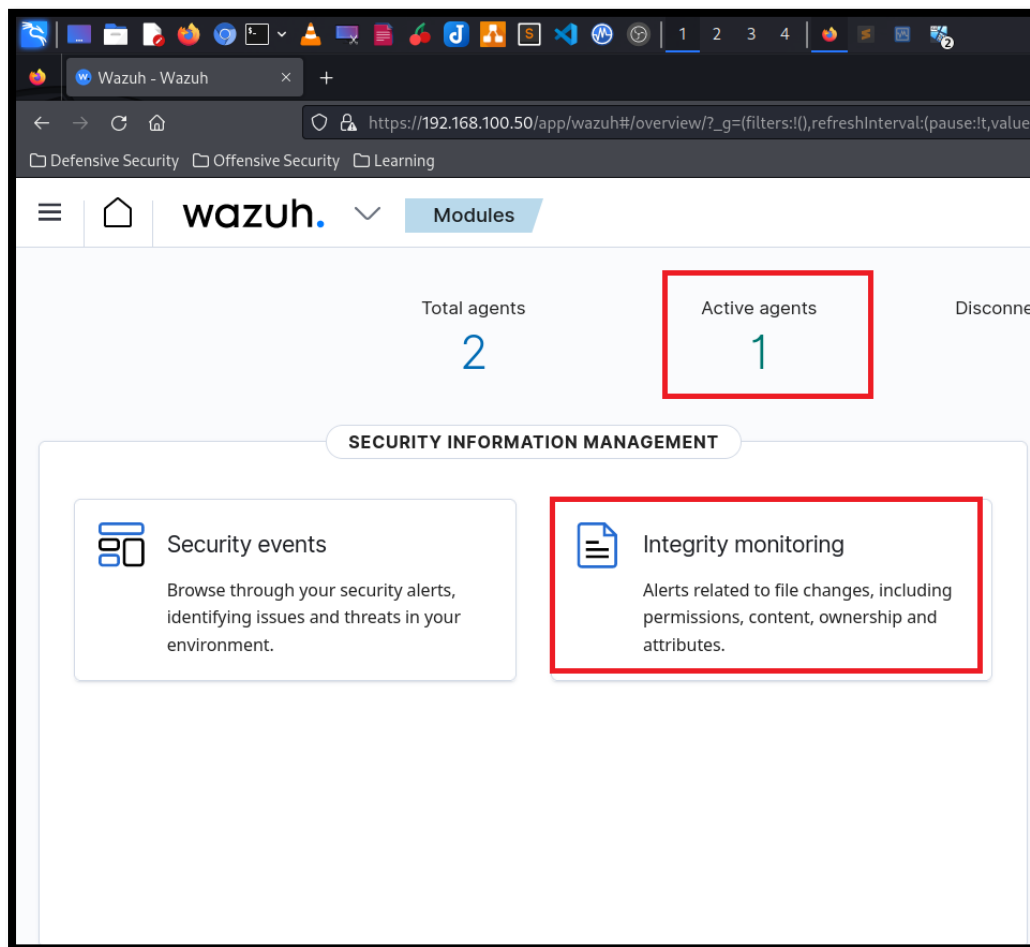


Dashboard of Wazuh Server

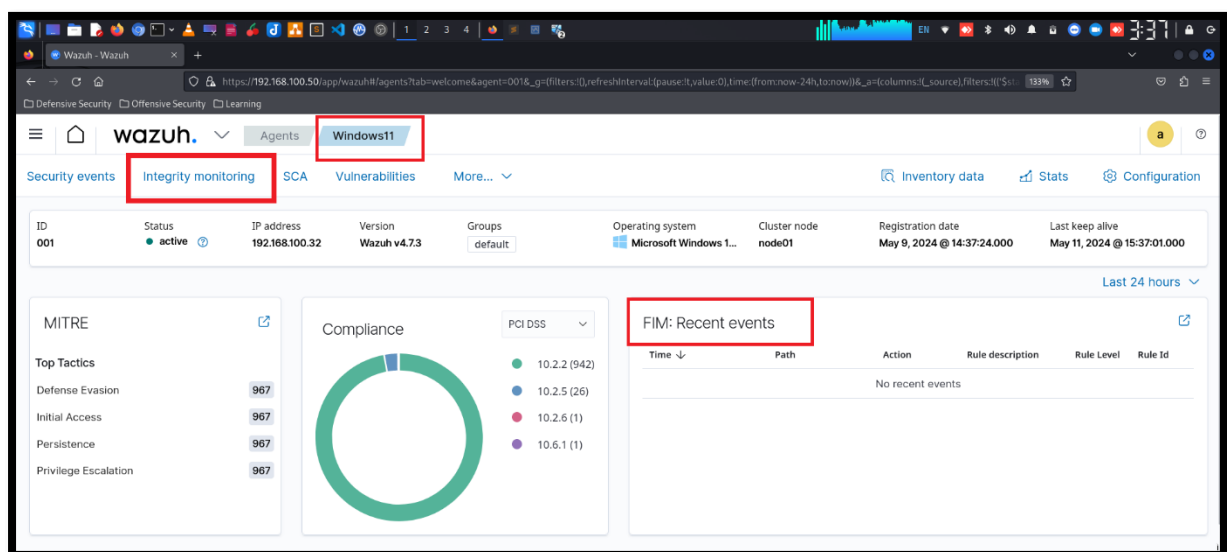


In Wazuh dashboard total agents is 2 and active agents is 1 and Windows 11 agent is active and running.

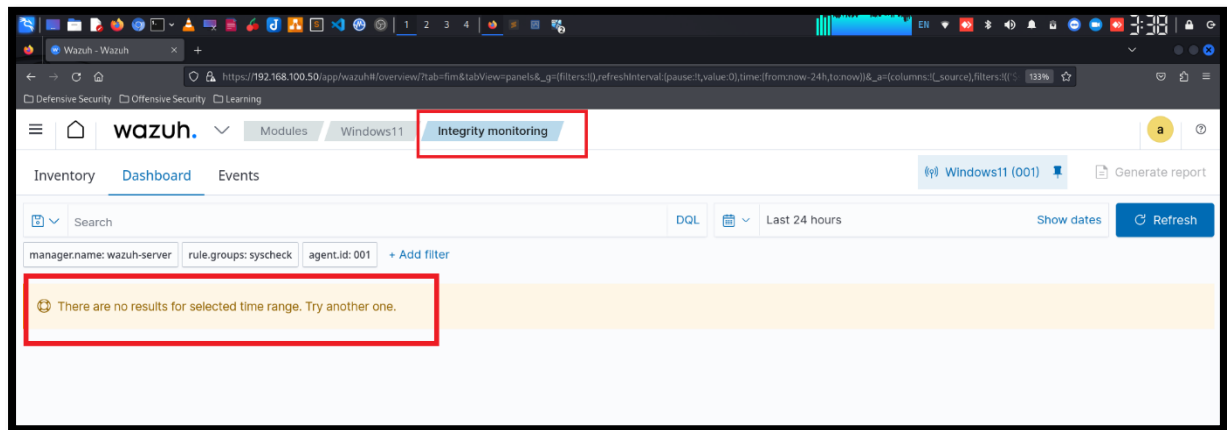
In Wazuh dashboard there is tab or section “SECURITY INFORMATION MANAGEMENT” under this we have “Integrity monitoring”



Select the windows11-agent and see in “FIM: Recent events” there is no data available for now, click on “integrity monitoring”

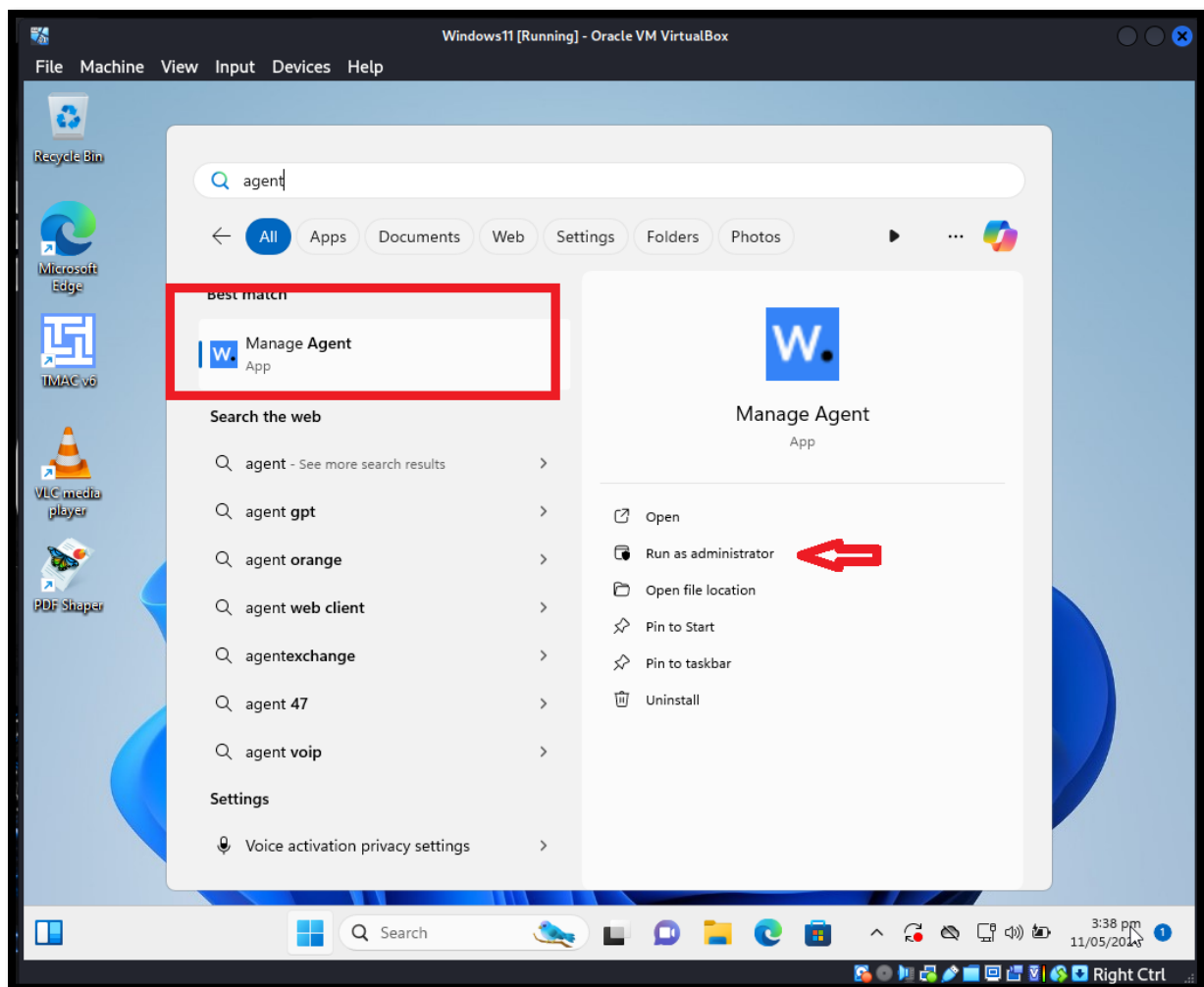


In integrity monitoring tab “There are not results for selected range” because there is no file for integrity monitoring configure.

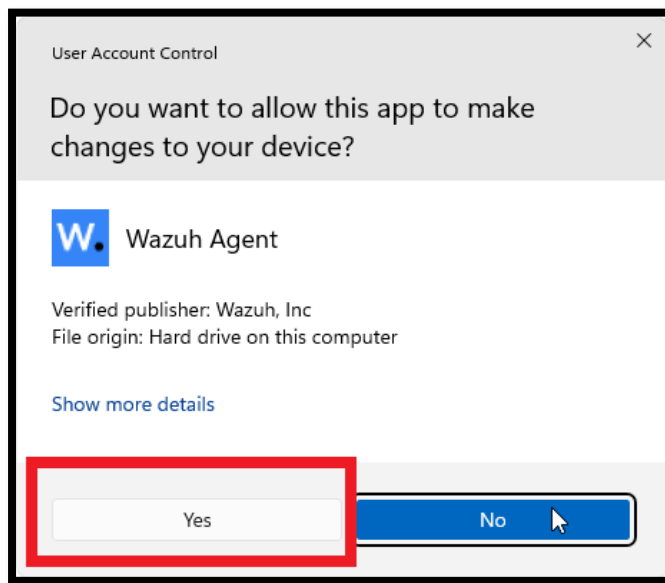


Let's configure a FIM

Search agent in search menu, select “Manage Agent” and run this as administrator.

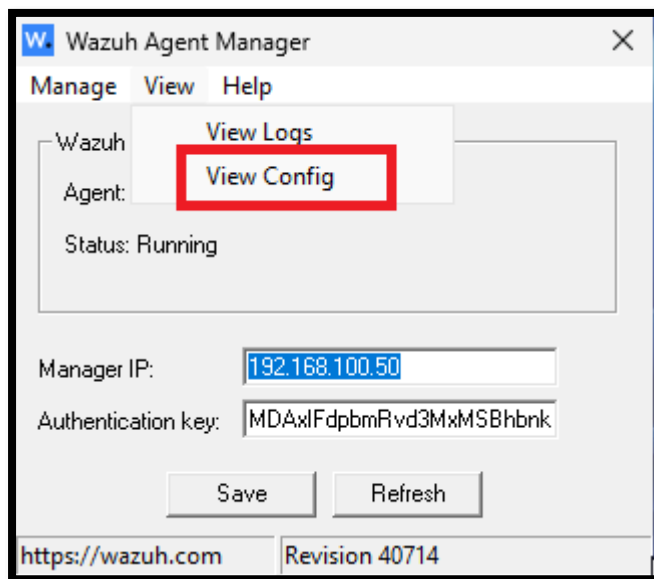


Click on “YES”

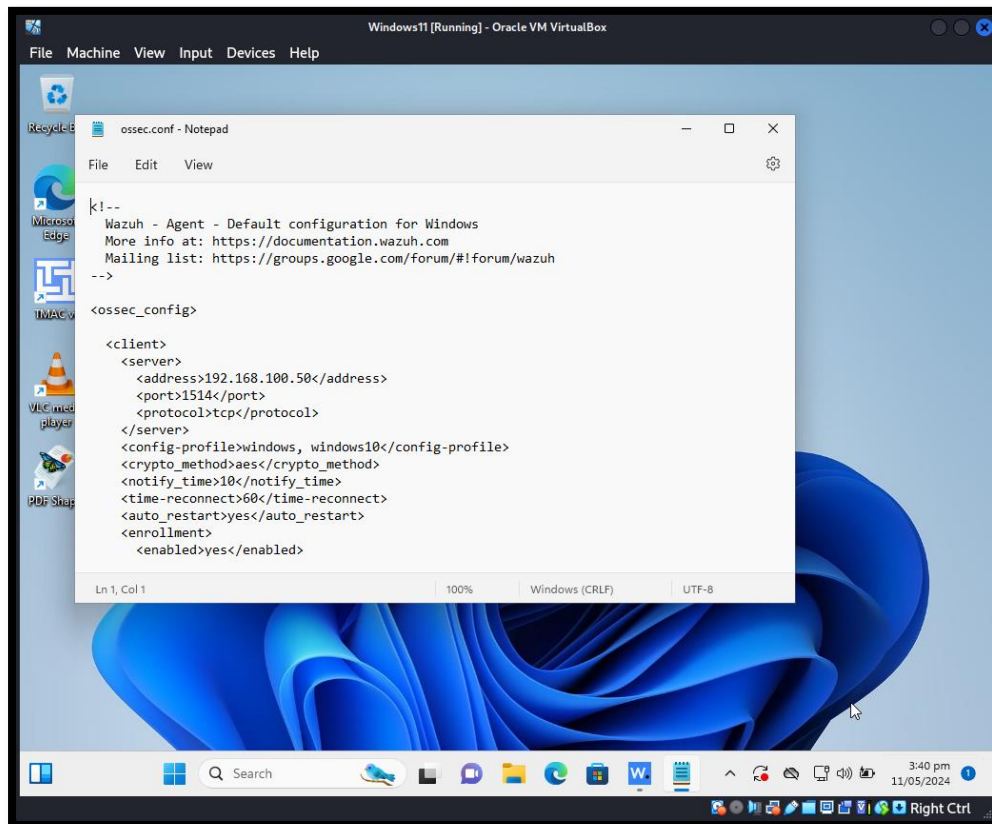


Wazuh Agent Manager is launched

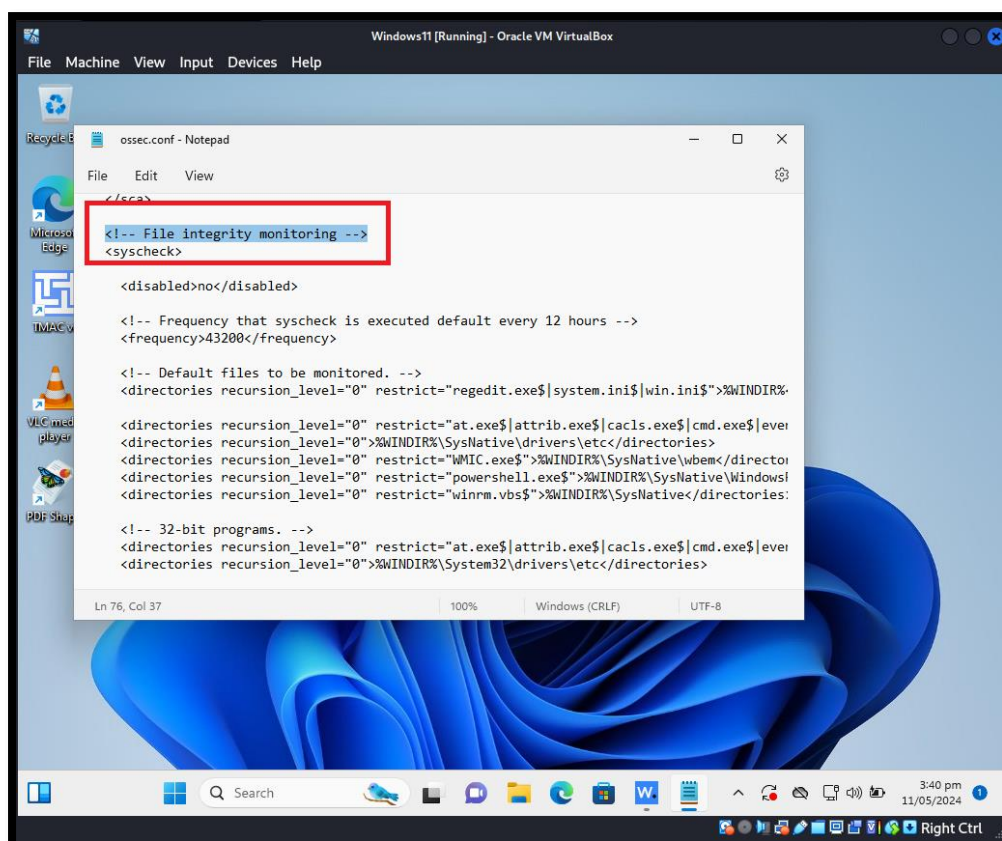
Go to View and select “View Config”



Here is “ossec.conf” file, scroll down a little and you will find “File integrity Monitoring” section. Here is <syscheck> configuration available.

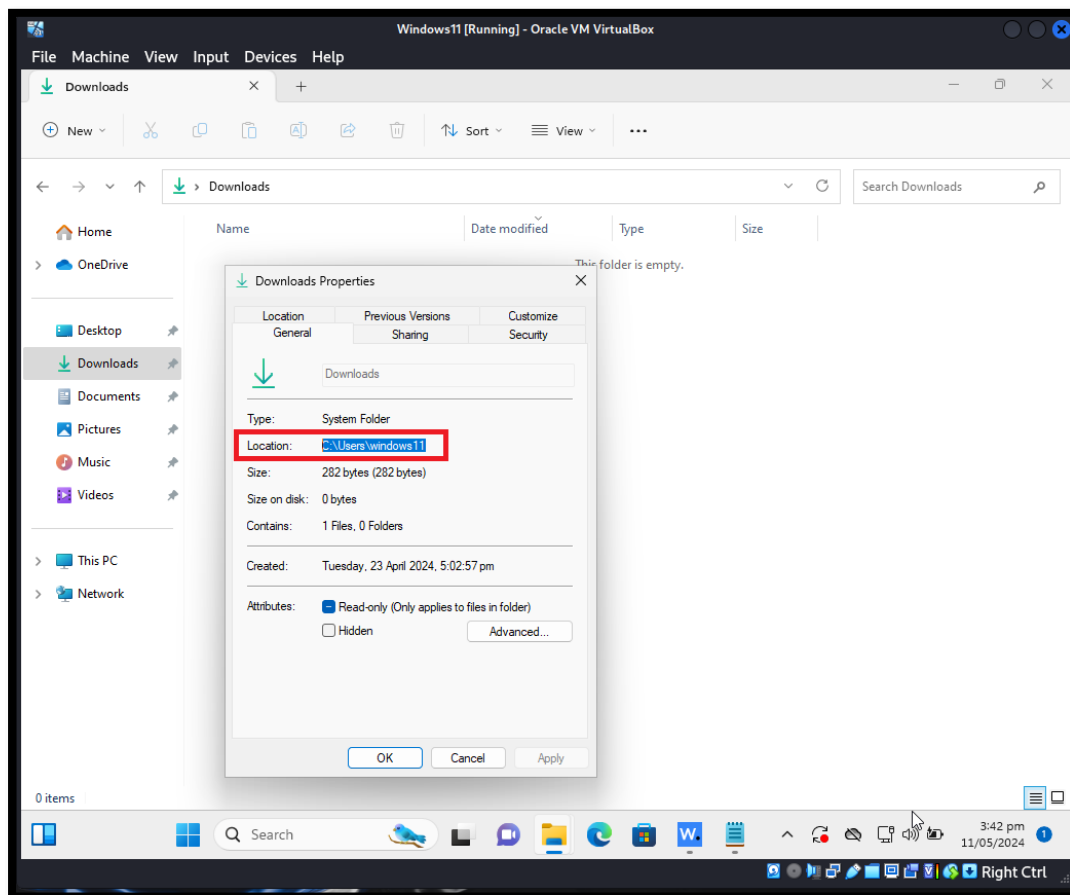


```
k!--  
Wazuh - Agent - Default configuration for Windows  
More info at: https://documentation.wazuh.com  
Mailing list: https://groups.google.com/forum/#!forum/wazuh  
-->  
  
<ossec_config>  
  
<client>  
  <server>  
    <address>192.168.100.50</address>  
    <port>1514</port>  
    <protocol>tcp</protocol>  
  </server>  
  <config-profile>windows, windows10</config-profile>  
  <crypto_method>aes</crypto_method>  
  <notify_time>10</notify_time>  
  <time-reconnect>60</time-reconnect>  
  <auto_restart>yes</auto_restart>  
  <enrollment>  
    <enabled>yes</enabled>
```



```
</ossec>  
  
<!-- File integrity monitoring -->  
<syscheck>  
  
  <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 recursion_level="0" restrict="at.exe|attrib.exe|cacls.exe|cmd.exe|event  
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>  
  <directories recursion_level="0" restrict="WMIC.exe">%WINDIR%\SysNative\wbem</directo  
  <directories recursion_level="0" restrict="powershell.exe">%WINDIR%\SysNative\WindowsI  
  <directories recursion_level="0" restrict="winrm.vbs">%WINDIR%\SysNative</directories>  
  
  <!-- 32-bit programs. -->  
  <directories recursion_level="0" restrict="at.exe|attrib.exe|cacls.exe|cmd.exe|event  
  <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
```

I want to monitor my Downloads folder files integrity. Copy the path of this folder. You can add folder path what you want to monitor.

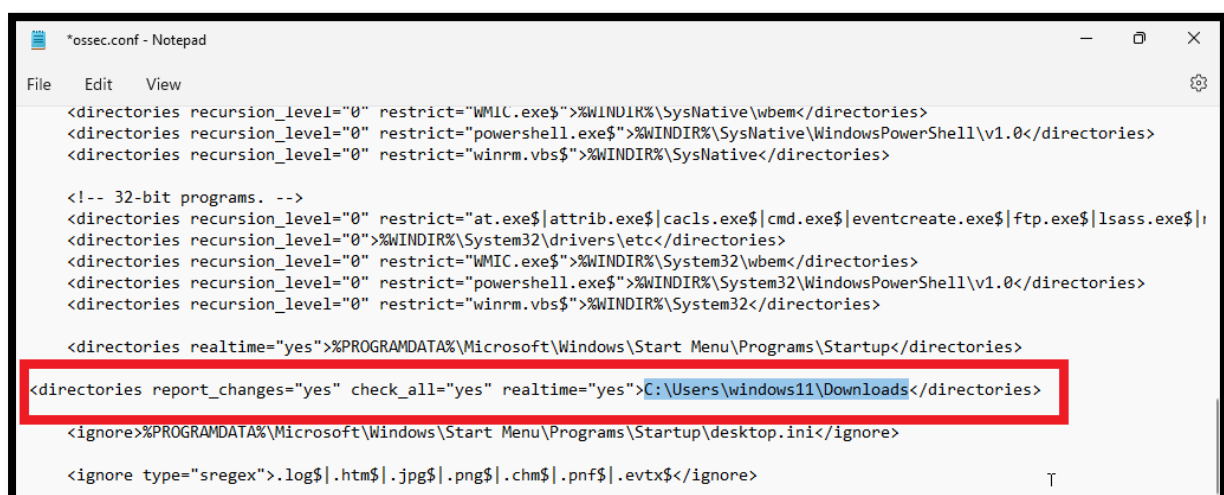


Now we have to add folder to integrity monitoring.

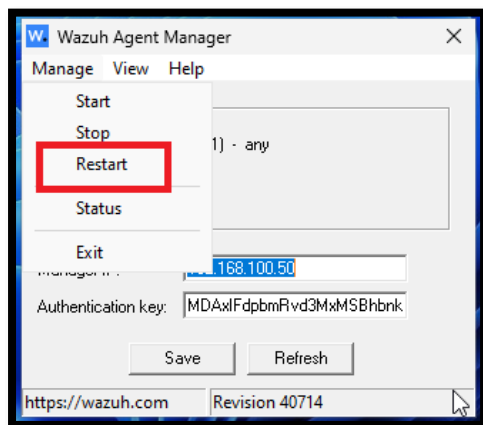
adding line:

```
<directories report_changes="yes" check_all="yes" realtime="yes"> Folder Path </directories>
```

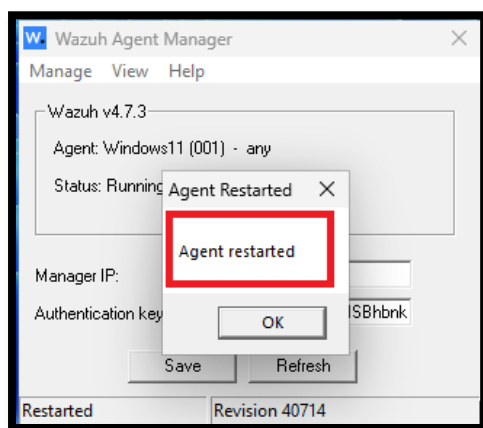
Save the changes and close the "ossec.conf" file



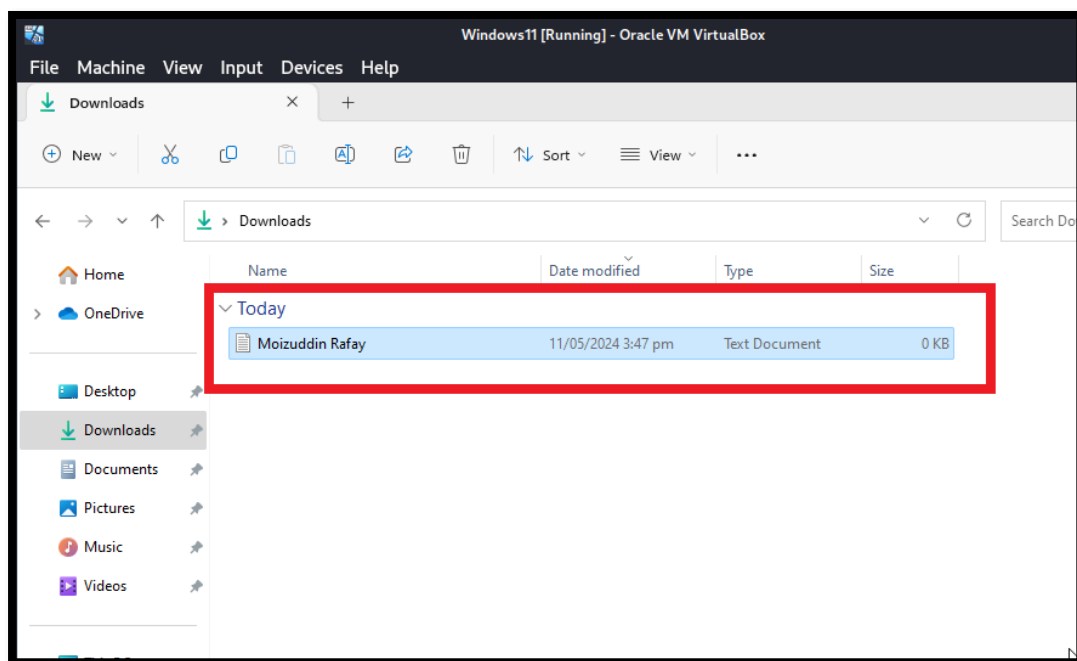
Restart the Wazuh-agent.



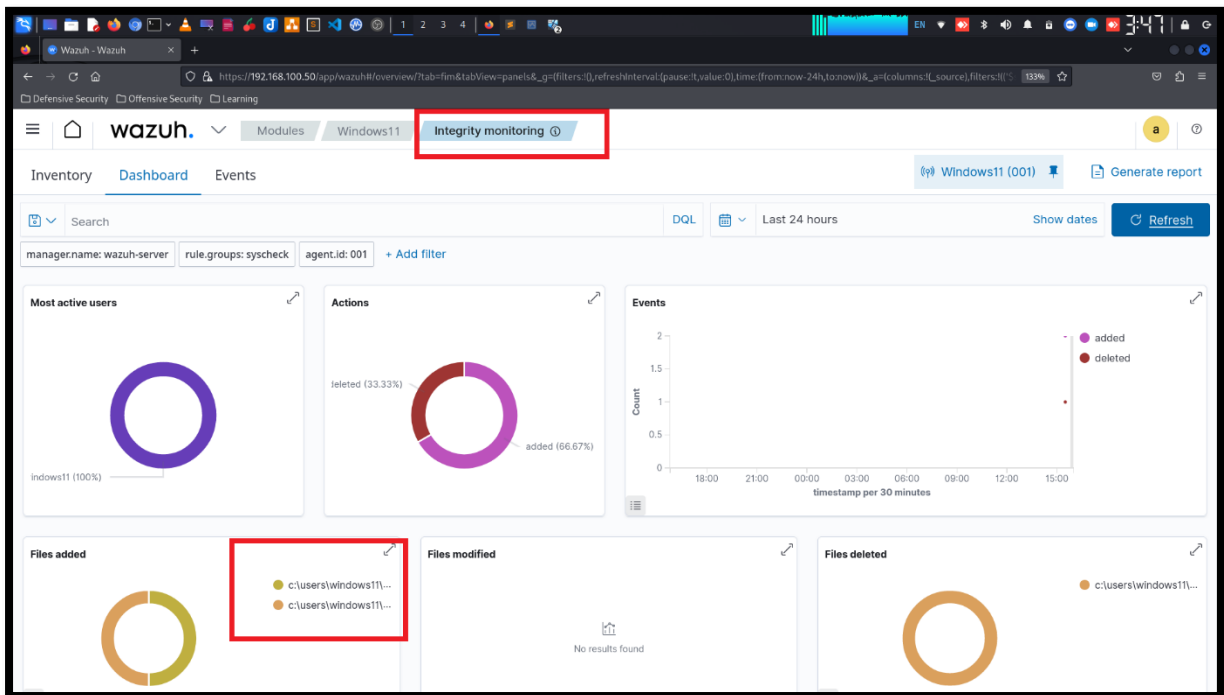
Wazuh-agent restarted.



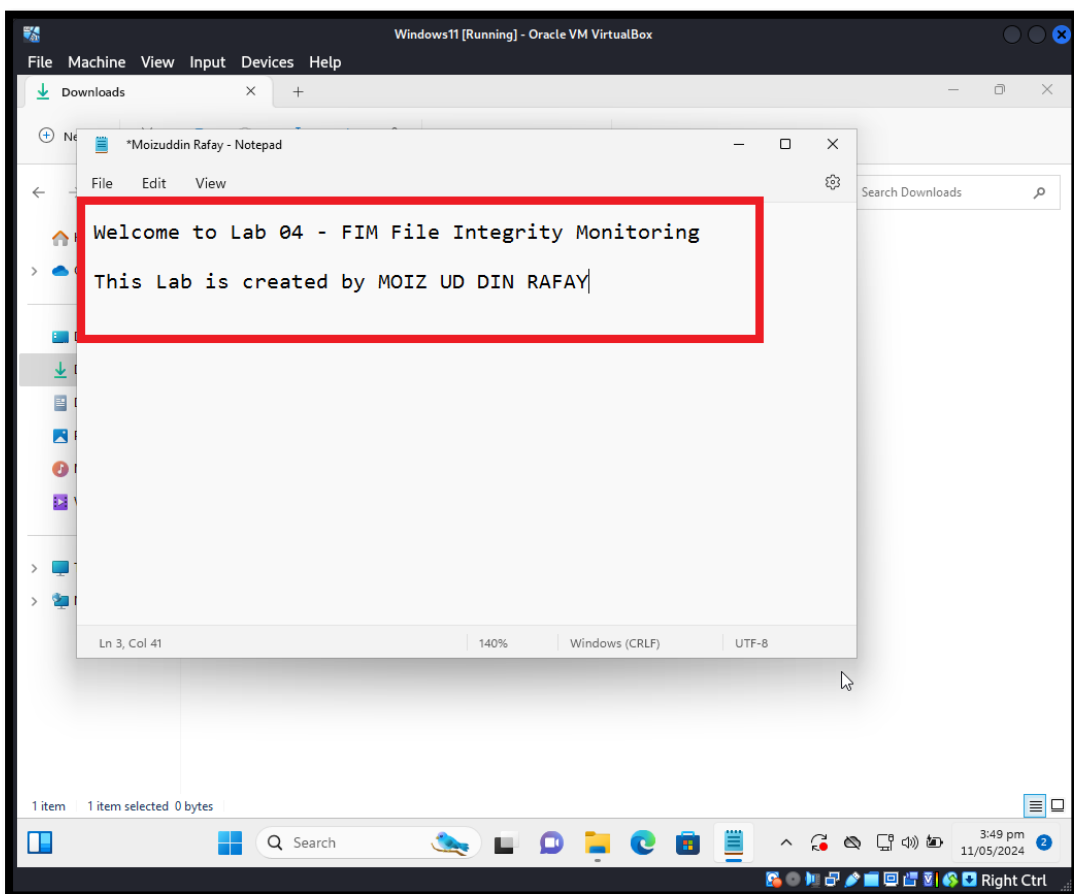
Now create a text file in the folder which is added for monitoring.



When you create a file, go to Wazuh “Integrity monitoring” tab and reload or refresh the page. Then you will see the results.

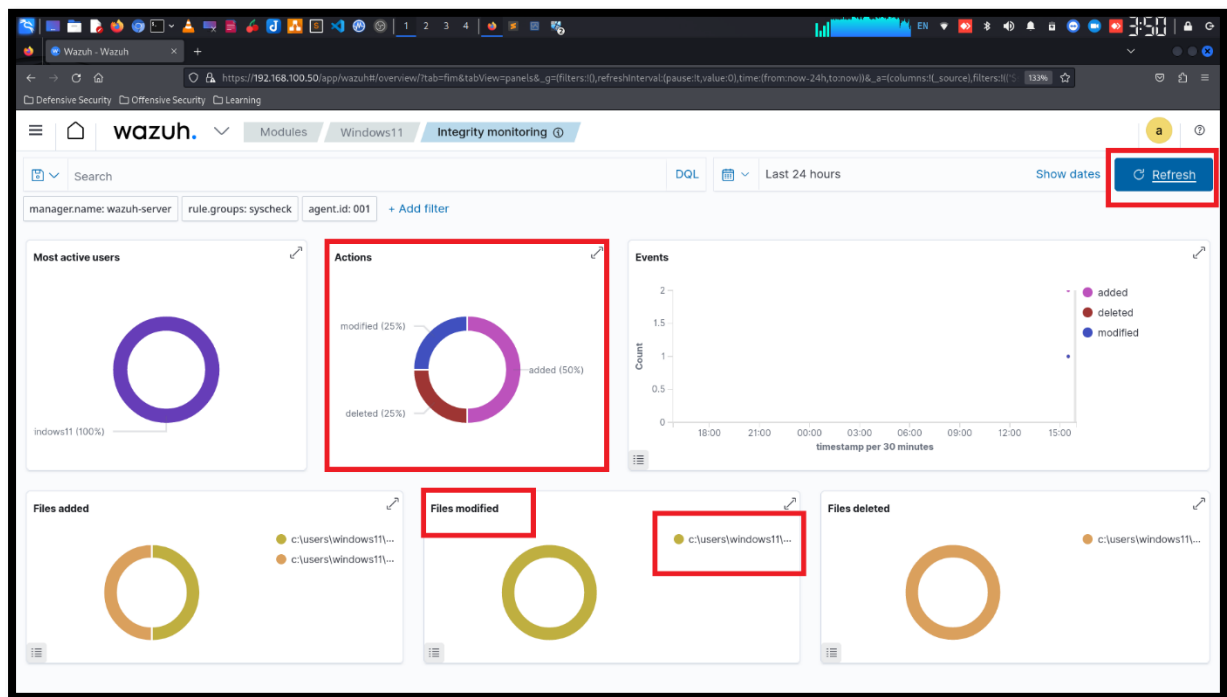


Let's do some modification in file, I am writing text in this file.

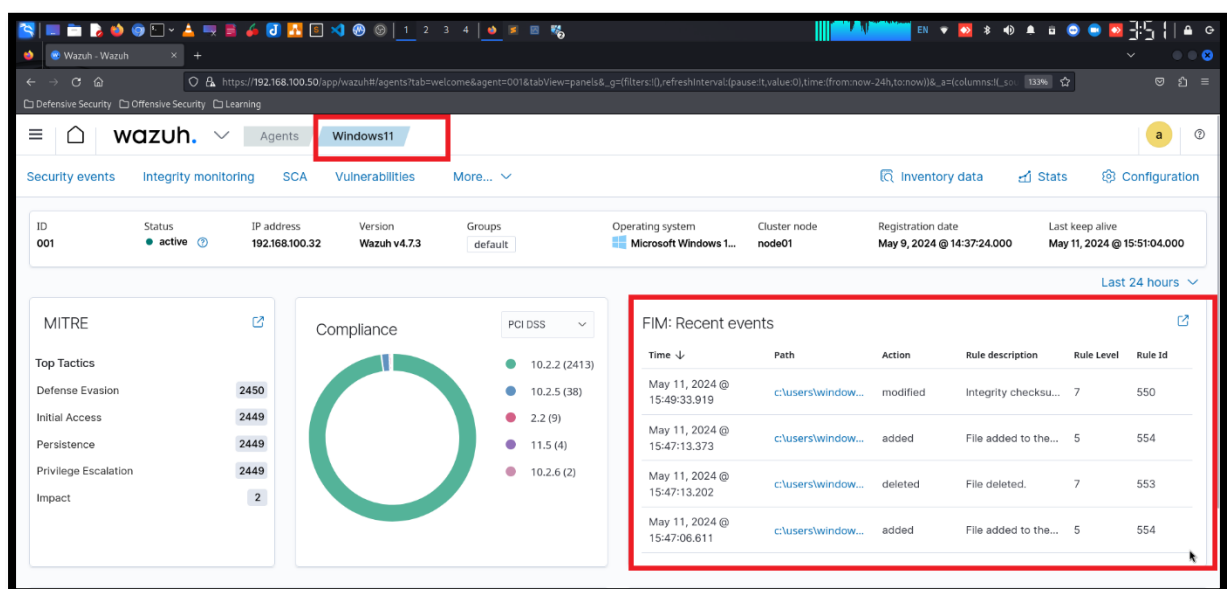


Wazuh FIM – File Integrity Monitoring: 04
Lab Created by: MUHAMMAD MOIZ UD DIN RAFAY

Go again in Wazuh “Integrity monitoring” dashboard and refresh the page. And you will see the new results. File is MODIFIED and hash of file is change.



Also you can go back to Windows11-agent and see FIM Record events is available.



Click on event and see the details.

The screenshot shows the Wazuh dashboard interface. A red box highlights the file path `c:\users\windows11\downloads\moizuddin rafay.txt` in the top navigation bar. Another red box highlights the 'Recent events' section in the details panel. The details panel shows the following information:

- Last analysis:** May 11, 2024 @ 15:49:35.000
- Last modified:** May 11, 2024 @ 15:49:35.000
- User:** windows11
- User ID:** S-1-5-21-3936295083-2612306440-923044628-1001
- Size:** 93 Bytes
- MD5:** 1e16515cb2ea628a930ca32163d647ce
- SHA1:** 824aac23d10796c9a63c5015c927754eb3c2acbf
- SHA256:** c805df46e7b5fea28dfb010fd7cda0d509bd8baaf1cfc2e76cb5024d6474ec35
- Permissions:** (icon)

The 'Recent events' section shows a table with the following data:

Time	Action	Description	Level	Rule ID
May 11, 2024 > @ 15:49:33.919	modified	Integrity checksum changed.	7	550

Now I am going to configure FIM in my Ubuntu machine.

Here is my SOC lab environment Wazuh Server or Ubuntu is running.

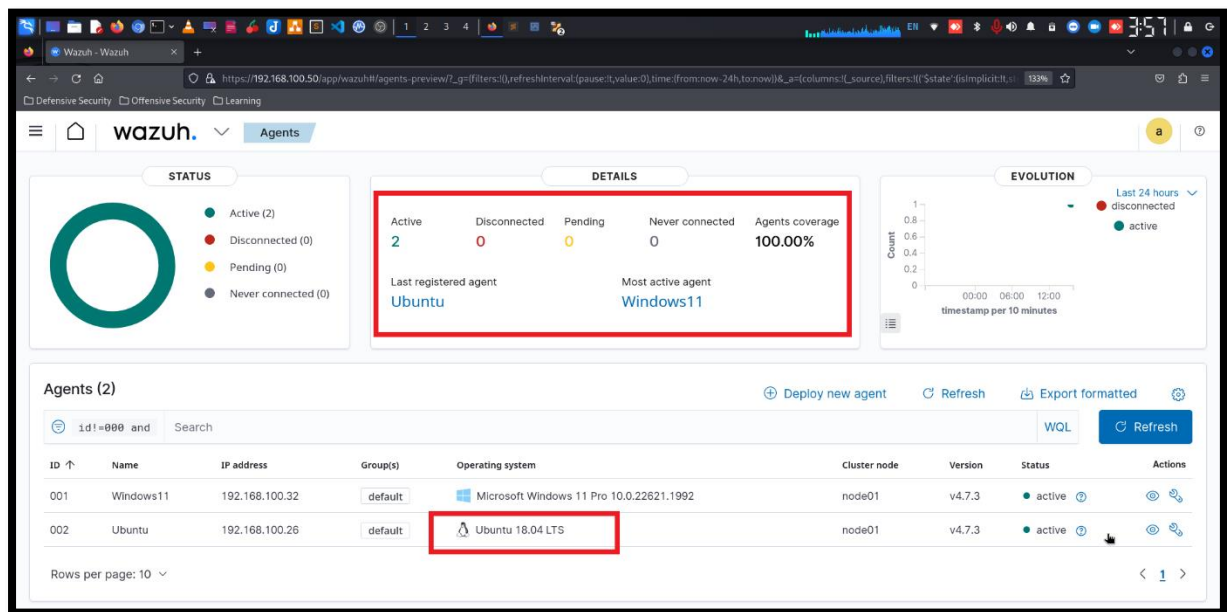
The screenshot shows a virtual machine environment with two windows. The top window is titled 'Ubuntu-WebApplication [Running] - Oracle VM VirtualBox' and displays a Ubuntu desktop with a red background and a white bird logo. The bottom window is titled 'Wazuh Server [Running] - Oracle VM VirtualBox' and displays a terminal window with the following output:

```
[wazuh-user@wazuh-server ~]$ ./wazuh-server -i 202.3180471 obxvideo: loading version 6.1.42 r155177
[ 202.562727] 10:35:59.905466 main   UbuntuService 6.1.42 r155177 (verbosity: 0)
[ 202.562727] 10:35:59.905471 main   Log opened 2024-05-11T10:35:59.905451000Z
[ 202.562727] 10:35:59.909022 main   OS Product: Linux
[ 202.562727] 10:35:59.909077 main   OS Release: 4.14.336-256.559.amzn2.x86_64
[ 202.562727] 10:35:59.911167 main   OS Version: #1 SMP Tue Feb 13 09:58:28 UTC 2024
[ 202.562727] 10:35:59.917317 main   Executable: /opt/UbuntuGuestAdditions-6.1.42/shim/UbuntuService
[ 202.562727] 10:35:59.917328 main   Process ID: 18154
[ 202.562727] 10:35:59.917332 main   Package type: LINUX 64BITS GENERIC
[ 202.562727] 10:35:59.925972 main   6.1.42 r155177 started. Verbosity level = 0
[ 202.562727] 10:35:59.949124 main   vbyIR3GuestCtrlDetectPeekGetCancelSupport: Supported (#1)
[wazuh-user@wazuh-server ~]$
```

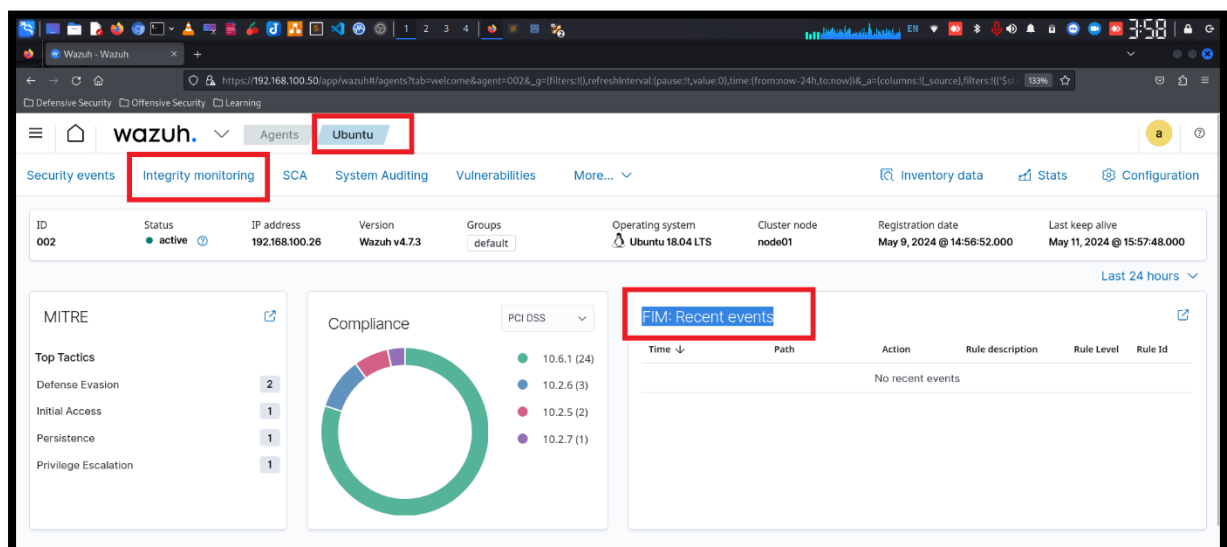
Wazuh FIM – File Integrity Monitoring: 04

Lab Created by: MUHAMMAD MOIZ UD DIN RAFAY

Go to Wazuh dashboard again and see we have both agent active now.



Select Ubuntu-agent and see there is no FIM data available. Now click on “Integrity monitoring” section.

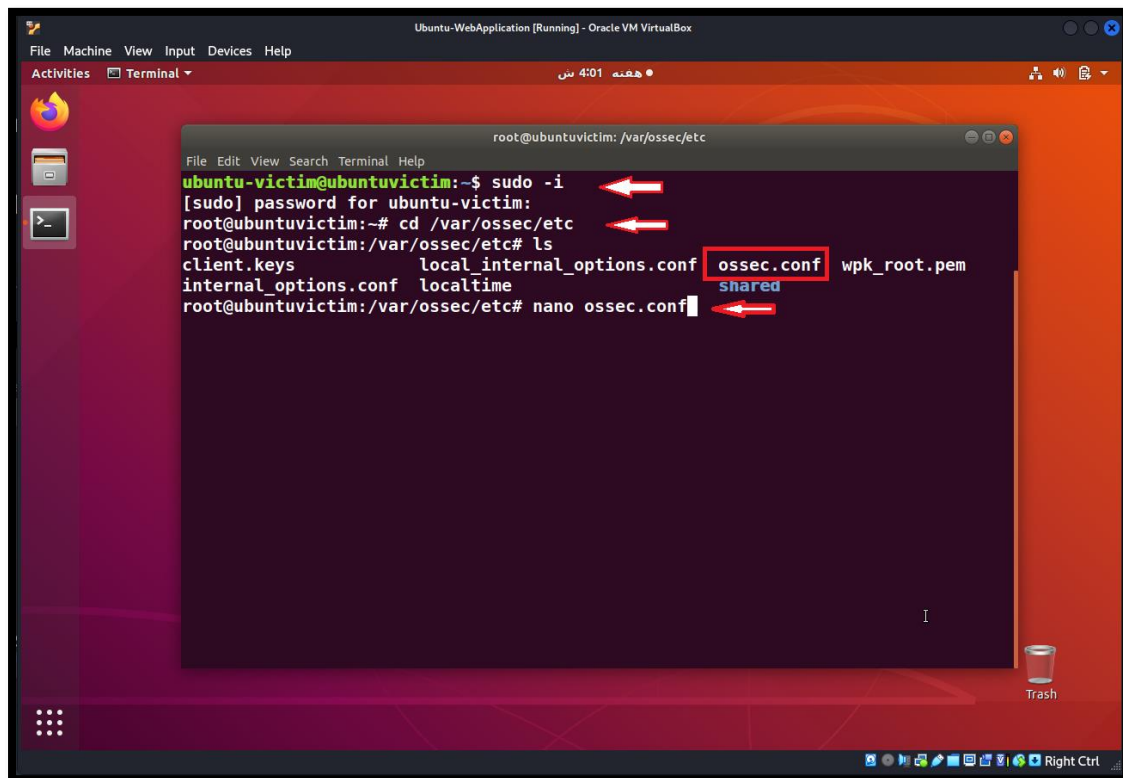


Now I am going to configure FIM in ubuntu machine. For this follow as shown in figure.

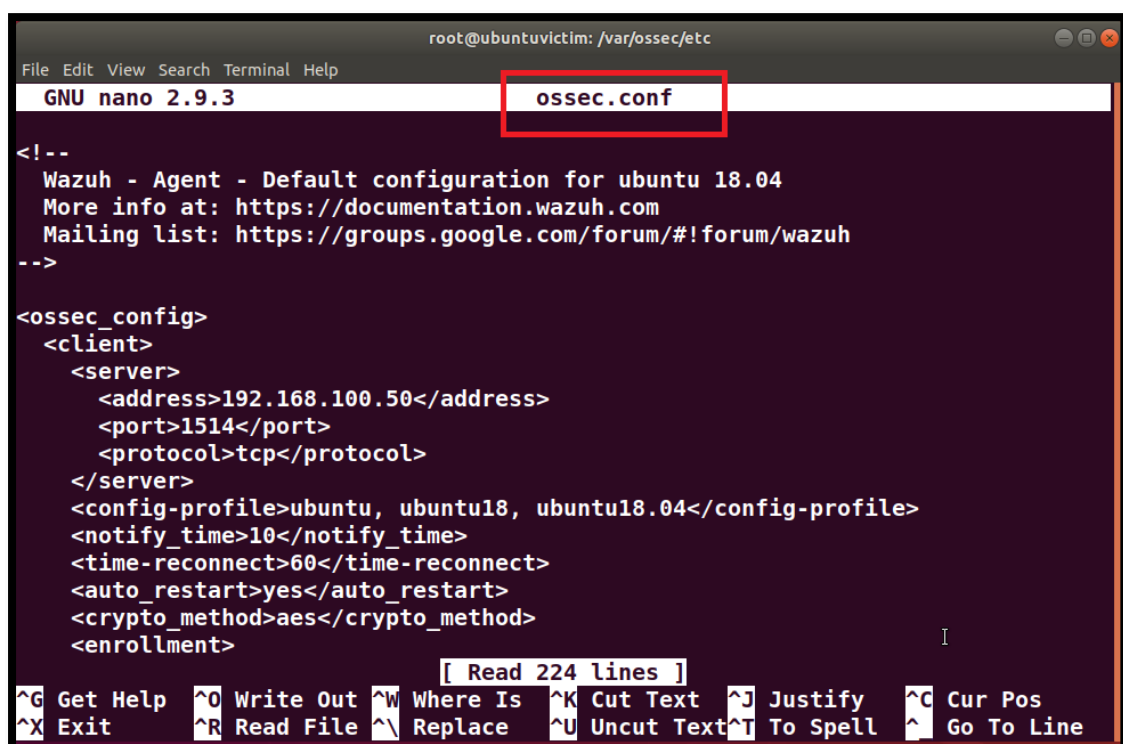
sudo -i (enter the root account)

cd /var/ossec/etc (locate the ossec.conf directory)

nano ossec.conf (edit the ossec.conf file)



```
File Machine View Input Devices Help
Activities Terminal
root@ubuntuvictim: /var/ossec/etc
ubuntu-victim@ubuntuvictim:~$ sudo -i
[sudo] password for ubuntu-victim:
root@ubuntuvictim:~# cd /var/ossec/etc
root@ubuntuvictim:/var/ossec/etc# ls
client.keys          local_internal_options.conf  ossec.conf  wpk_root.pem
internal_options.conf localtime
root@ubuntuvictim:/var/ossec/etc# nano ossec.conf
```

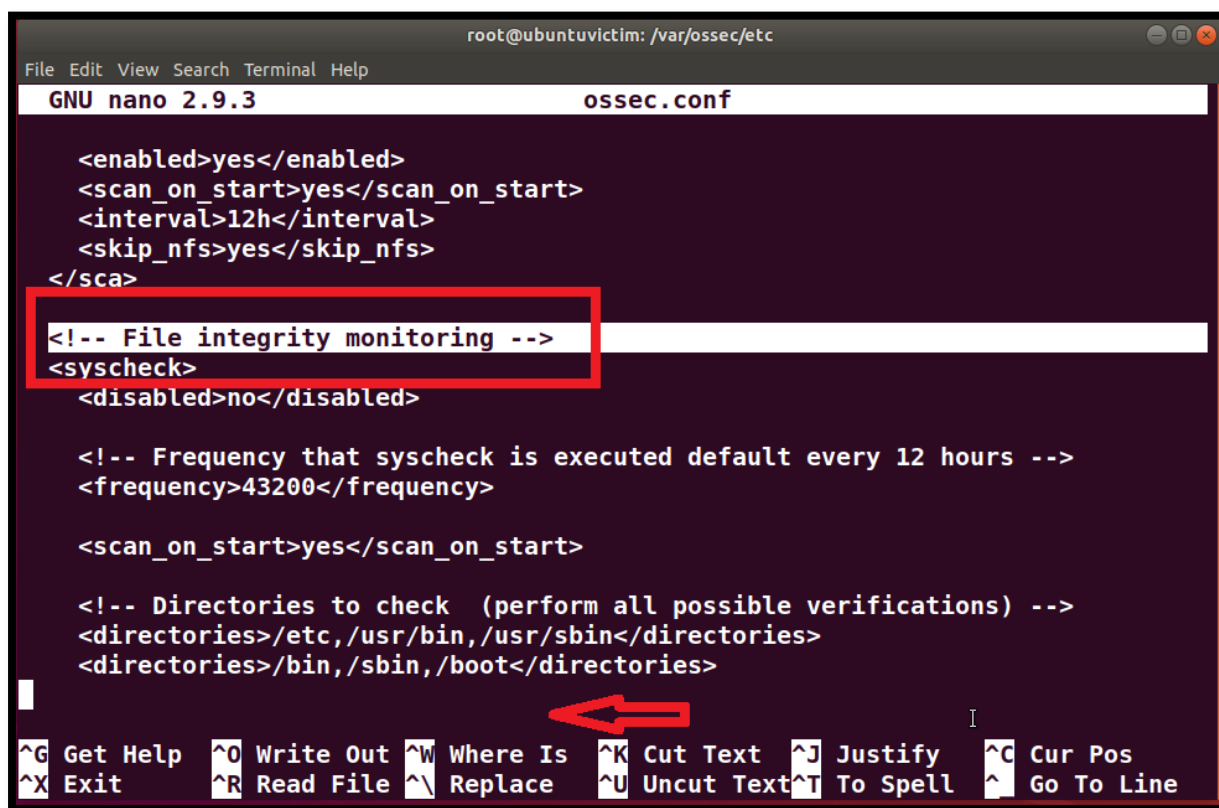


```
File Edit View Search Terminal Help
GNU nano 2.9.3 ossec.conf
<!--
Wazuh - Agent - Default configuration for ubuntu 18.04
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>192.168.100.50</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>ubuntu, ubuntu18, ubuntu18.04</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
    <enrollment>

[ Read 224 lines ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Now locate the “File Integrity Monitoring”



```
root@ubuntuvictim: /var/ossec/etc
GNU nano 2.9.3 ossec.conf

<enabled>yes</enabled>
<scan_on_start>yes</scan_on_start>
<interval>12h</interval>
<skip_nfs>yes</skip_nfs>
</sca>
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

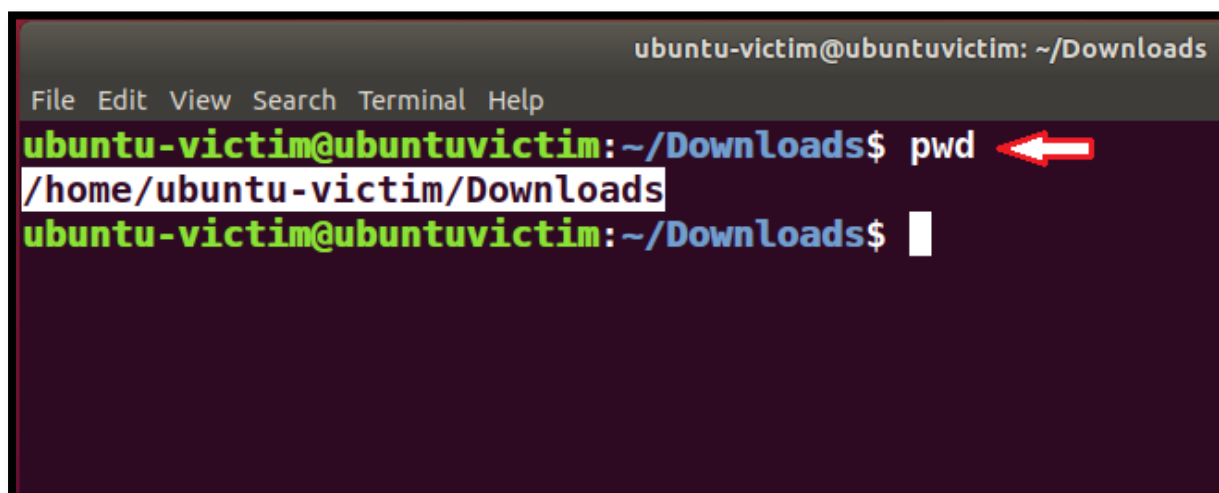
  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Directories to check (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>

  
```

Selecting the path of folder which you want to monitor.

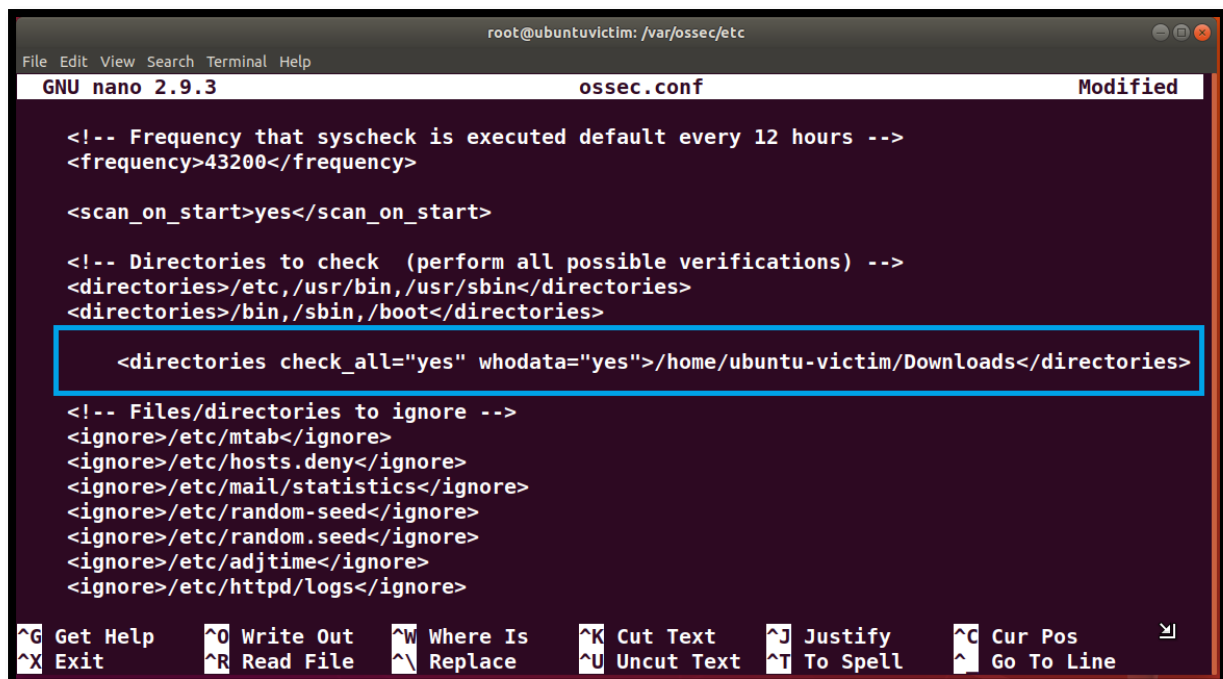


```
ubuntu-victim@ubuntuvictim: ~/Downloads
File Edit View Search Terminal Help
ubuntu-victim@ubuntuvictim:~/Downloads$ pwd
/home/ubuntu-victim/Downloads
ubuntu-victim@ubuntuvictim:~/Downloads$
```

Add configuration line here:

<directories check_all="yes" whodata="yes"> Path of folder </directories>

If you want to explanation of this configuration do comment I will explain everything.



```
root@ubuntuvictim: /var/ossec/etc
GNU nano 2.9.3 ossec.conf Modified

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

<scan_on_start>yes</scan_on_start>

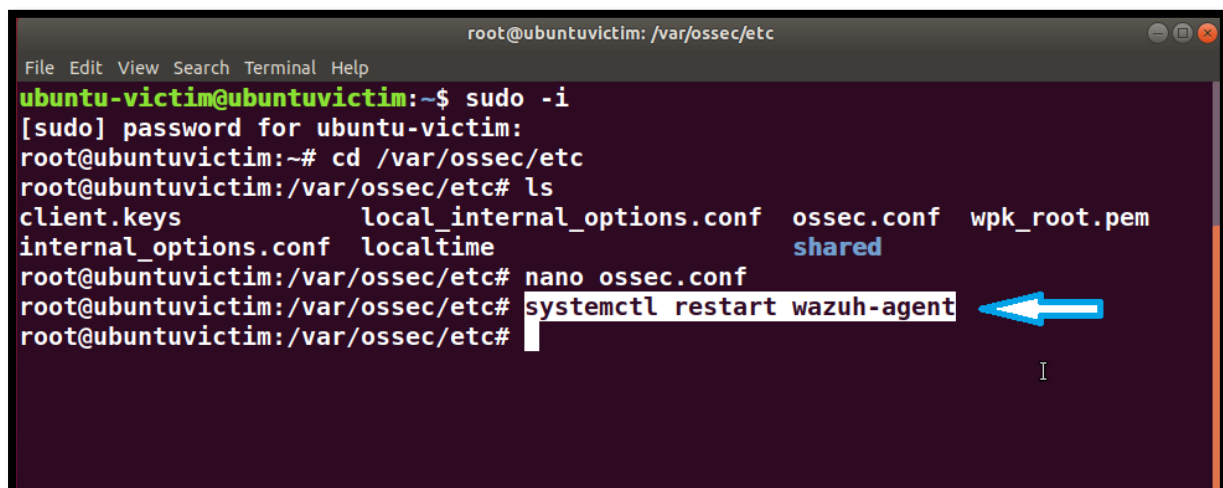
<!-- Directories to check (perform all possible verifications) -->
<directories>/etc,/usr/bin,/usr/sbin</directories>
<directories>/bin,/sbin,/boot</directories>

<directories check_all="yes" whodata="yes">/home/ubuntu-victim/Downloads</directories>

<!-- Files/directories to ignore -->
<ignore>/etc/mtab</ignore>
<ignore>/etc/hosts.deny</ignore>
<ignore>/etc/mail/statistics</ignore>
<ignore>/etc/random-seed</ignore>
<ignore>/etc/random.seed</ignore>
<ignore>/etc/adjtime</ignore>
<ignore>/etc/httpd/logs</ignore>

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos
^X Exit          ^R Read File    ^_ Replace      ^U Uncut Text   ^T To Spell     ^_ Go To Line
```

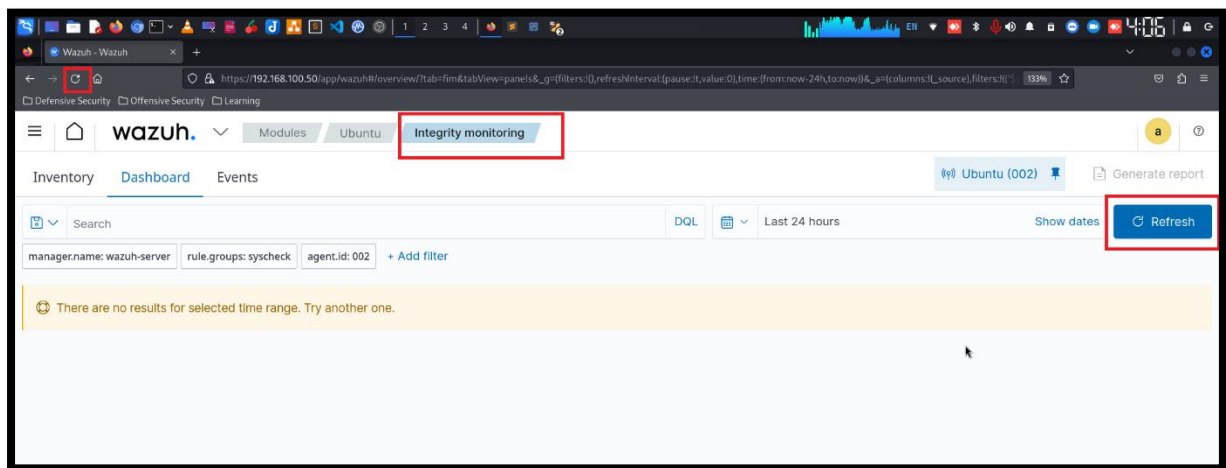
Save the changes in “ossec.conf” file and restart the Wazuh-agent.



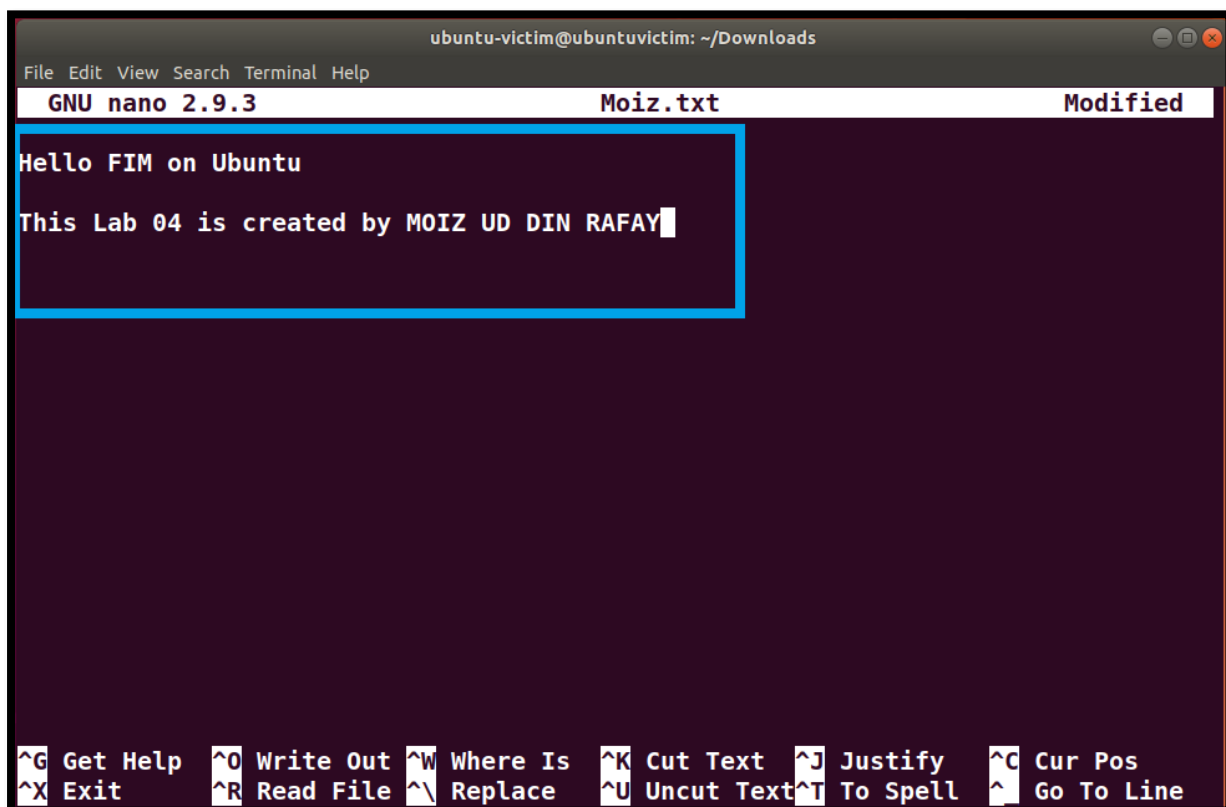
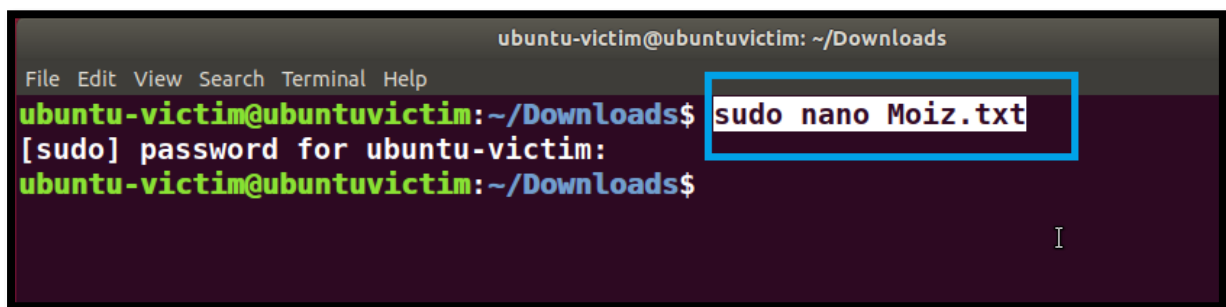
```
root@ubuntuvictim: /var/ossec/etc
File Edit View Search Terminal Help
ubuntu-victim@ubuntuvictim:~$ sudo -i
[sudo] password for ubuntu-victim:
root@ubuntuvictim:~# cd /var/ossec/etc
root@ubuntuvictim:/var/ossec/etc# ls
client.keys          local_internal_options.conf  ossec.conf  wpk_root.pem
internal_options.conf localtime                  shared
root@ubuntuvictim:/var/ossec/etc# nano ossec.conf
root@ubuntuvictim:/var/ossec/etc# systemctl restart wazuh-agent
root@ubuntuvictim:/var/ossec/etc#
```

Command: systemctl restart wazuh-agent

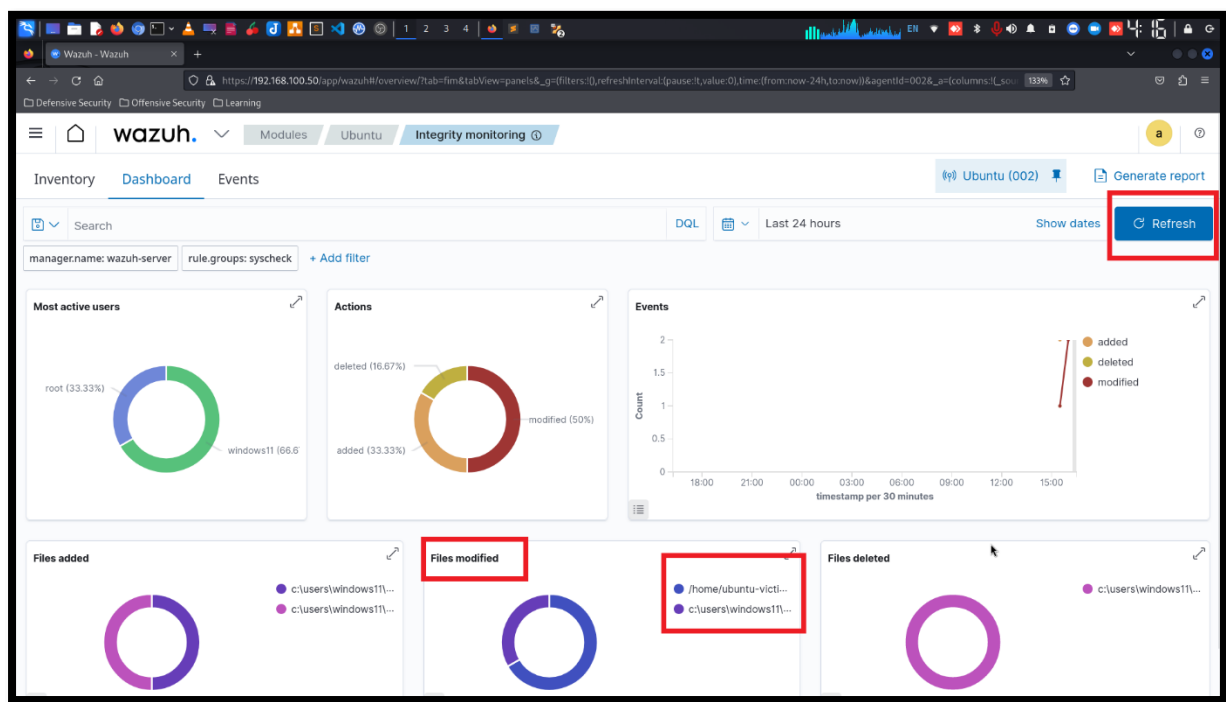
Now go to “Integrity monitoring” dashboard and refresh and reload the page.



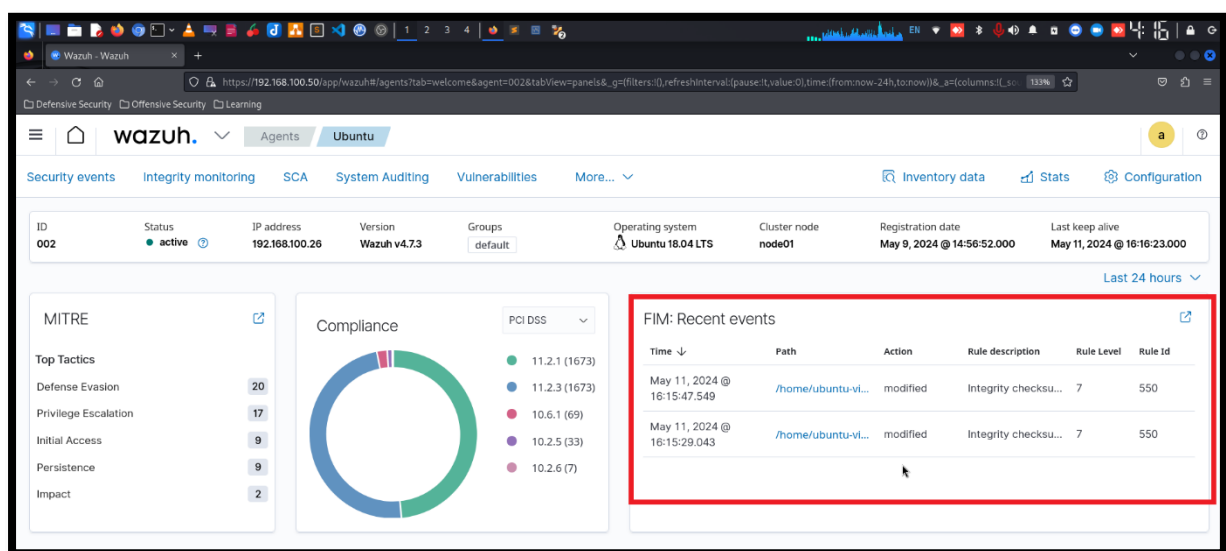
Now create and edit the text file.



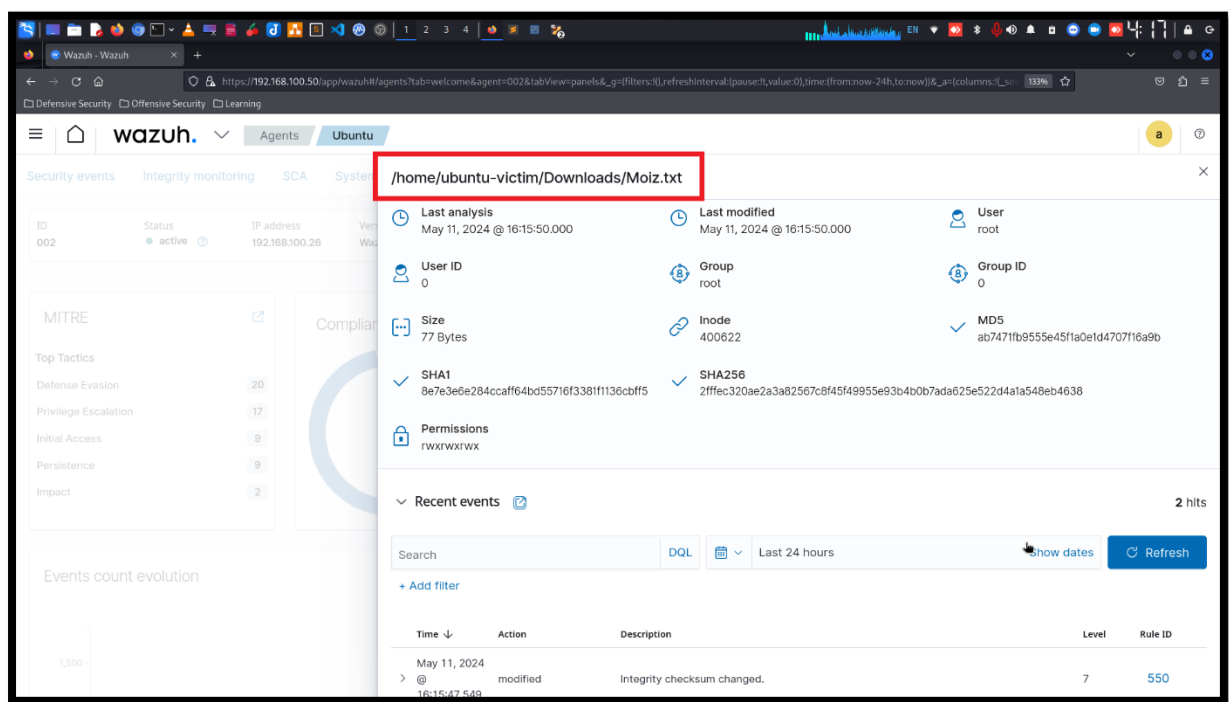
Here is you can see the result in “Integrity monitoring” dashboard. See the highlighted sections.



Now go back in Ubuntu-agent dashboard and see the events in “FIM: Recent events”



Now click on any event and see the details of events.



SUMMARY

In summary, Wazuh File Integrity Monitoring offers a comprehensive solution for detecting and responding to unauthorized changes to files and directories, enhancing the security posture of organizations and helping them maintain compliance with regulatory requirements.