In this blog I will share how I setup wazuh,wazuh agent(ubuntu,windows) in virtual box, suricata (NIDS)and some issues I have faced during setup.
Installatin wazuh in my host kali linux:
For that I go to wazuh documentation and read quick start guide.Here I found one command

curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

I run the command in my kali linux host machine.After the installation its show me the credentials in terminal.I keep the credentials to access wazuh.

Now it's time to access the wazuh through browser.I use ifconfig command to see my ip address.Now I use my host machine ip to access wazuh.I search in chrome with my ip but chrome tells me its insecure.So I go to the advance and accept the risk and able to access the wazuh.

Now it's time to set up wazuh-agent.So I need virtual box.I set up virtual box and two machines in the virtual box one is ubuntu and another one windows.

While setup ubuntu machine and windows I face some issues specially for enable drag and drop options.After some research I found that in virtual box settings->storage Controller:SATA,and Controller:IDE is not setup correctly.So I download manually Virtual box iso and set it into Controller:Sata.I double check if Controller:IDE is set up with vdi file.Then I set up drag and drop options bidirectional as well as shared clipboard from virtual box->General->Advance.Then I just start ubuntu machine and in ubuntu machine I set up virtual box the installer correctly.Finally my problem is solved.

Same issue I aslo faced for windows machine.From the previous experience I try to setup Controller:sata for iso file and Controller:IDE.But the problem is I don't find Controller:IDE options.So after reseach I find that how to add controller.In virtual box setting->storage there is options(a button with green plus) to add controller with tool tip which help me to get it quickly.But I don't find IDE attributes which makes me upset but I set up PIIX4 attribute which works for me.Again I turn on the bidirectional options for drag and drop as well as shared clipboard.Then I start my windows machine and go to virtual disk where I double click the amd64 exe file to run.Then all set up is done.I restart the machine againe and now drag and drop options work perfectly.

Now virtual box setup done.Let's make wazuh-agent these two machine.So I browse the ip in my browser.

From wazuh dashboard I goto Agent management add new agent,select linux package amd64,set server ip (my host machine ip where wazuh server is running),give a name of the agent.Now copy the command and paste in ubuntu terminal with root privilages permission and start agent following the given command.Same thing is also for windows machine where I paste the command in powershell which I run as administrator.

Suricata Setup
It is a network intrution dection system.It's used for analysis network based log to identify anomolies into the network.Let's look for the setup.I want to setup suricata in my ubuto machine.So I go to ubuntu terminal and paste these command

sudo add-apt-repository ppa:oisf/suricata-stable

sudo apt-get update

sudo apt-get install suricata -y

As suricata detect anomolies based on rules we needs rules,So I extracts rules

cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz

sudo tar -xvzf emerging.rules.tar.gz && sudo mkdir /etc/suricata/rules && sudo mv rules/*.rules /etc/suricata/rules/

sudo chmod 640 /etc/suricata/rules/*.rules

Modify Suricata settings in the /etc/suricata/suricata.yaml file and set the following variables:

HOME_NET: "<UBUNTU_IP>" [here I set my ubuntu ip and in virtual box setting I ensure that network type is bridge]

EXTERNAL_NET: "any"

default-rule-path: /etc/suricata/rules
rule-files:
- "*.rules" [here manually add all the rules not wildcard]

Global stats configuration
stats:
enabled: yes

Linux high speed capture support
af-packet:
  - interface: enp0s3 [it is my ubuntu interface found from ifconfig command]

Now restart the suricata using the following command.

sudo systemctl restart suricata
Now we need to read the suricata log file so we add in /var/ossec/etc/ossec.conf

the following code.

<localfile>

<log_format>json</log_format>

<location>/var/log/suricata/eve.json</location>

</localfile>

Now everyting setup I need to restart the wazuh-agent the command is:

sudo systemctl restart wazuh-agent

Issues:

Basically I found three issues while setting up suricata:

1. E: detect: opening rule file /etc/suricata/rule>
2. E: unix-manager: failed to create socket directory
3. W: unix-manager: Unable to create unix command>

To reslove first issue I double check the /etc/suricata/suricata.yaml file if I setup everything correctly.After some research I'm able to find that the suricata cannot read the rules file So I need to give proper permission So I use the following command to do that:

sudo chown -R root:root /etc/suricata/rules

sudo chmod -R 644 /etc/suricata/rules/*.rules

Which is used to change the ownership and permission to read the files.

To fix the others two errors I use the following command.

```
sudo mkdir -p /run/suricata
sudo chown suricata:suricata /run/suricata
```

Now let's check if the errors get removed

```
sudo systemctl restart suricata
sudo systemctl status suricata
```

Now to test if suricate is working correctly I ping a command in my host kali computer

```
ping -c 20 <ip of my ubuntu>
```

Now in wazuh look for the threat intelligence ->threat hunting->events for ping alert.

We aslo check it for nmap basic scan

```
nmap -sS <ip of my ubuntu>
```

FIM

I integrate my windows machine with wazuh server for file integratity monitoring.For this I go to C:\Program Files (x86)\ossec-agent\ossec.conf this folder in windows vm machine(agent) and give permission for editing the conf file as mehedi user and add the following segment of code in ossec.conf file.

```
<syscheck>
 <directories recursion_level="2" realtime="yes">C:\Users\mehedi\Desktop</directories>
</syscheck>
```

For testing I create a file in windows desktop and check it in wazuh server threat hunting event the alert is trigger perfectly.

Command Execution Monitoring

I use notepad.exe to monitor any command if executed by notepad in my windows machine.Create a batch script named tasklist.bat in the C:\ root directory of the Windows endpoint and add the following content. The script adds a tasklist header to the output of the tasklist command.I enable to proper permission to create tasklist.bat file in root directory and create the file.This is the content of the file.

```
@"
@Echo Off
setlocal enableDelayedExpansion

for /f "delims=" %%a in ('powershell -command "& tasklist"') do (
   echo tasklist: %%a
```

)

exit /b

"@ | Set-Content -Encoding ASCII -Path "C:\tasklist.bat"

Next I need to configure the ossec.conf file in the following folder C:\Program Files (x86)\ossec-agent\ossec.conf and add the following content in wazuh agent.

<ossec_config> <wodle name="command"> <disabled>no</disabled> <tag>tasklist</tag> <command>PowerShell.exe C:\tasklist.bat</command> <interval>2m</interval> <run_on_start>yes</run_on_start> <timeout>10</timeout> </wodle></ossec_config>

For test I create a file using notepad and it trigged alert into wazuh server.

Virustotal Integration

I integrated virus total to my ubuntu agent machine.To do that I go to my kali server in the following folder /var/ossec/etc/ossec.conf add the following segment of code

<integration>
<name>virustotal</name>
<api_key>API_KEY</api_key> <!-- Replace with your VirusTotal API key -->
<group>syscheck</group> <alert_format>json</alert_format>
</integration>

and in the unbuntu machine in the following folder /var/ossec/etc/ossec.conf I add the following segment.

<syscheck>
<directories check_all="yes" realtime="yes">/home/ubuntu/Desktop</directories>
</syscheck>

To test the integration I downlaod a malicious file into ubuntu Desktop using following command sudo curl -Lo suspicious-file.exe https://secure.eicar.org/eicar.com which generate alert in wazuh server.

Each time configuration of ossec.conf file we need to restart the agent and manager.