Blocking Known Malicious Files

Requirements :

FIM should be configured in prior.

<u>Configuration in Wazuh server:</u>

I have logged in to my wazuh server via SSH in another machine

Now, we need to create CDB{Constant Database} malware list. Create malware-hashes under the directory

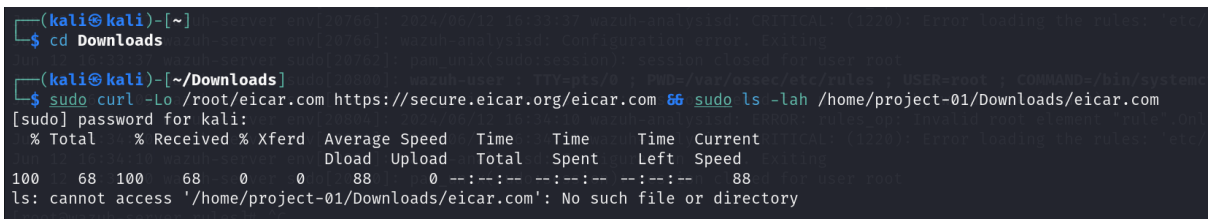
Command:

nano /var/ossec/etc/lists/malware-hashes

Now, try to add the known MD5 hashes to this “malware-hashes” file.

To do that, initially I have initially downloaded two freely available malware files from the internet

With the command “sudo md5sum Filename” → you can find the hash of that malware.exe file



Its hash value

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo md5sum cacert.der
e59750d809c266427c7cc9dcb21d7724  cacert.der
```

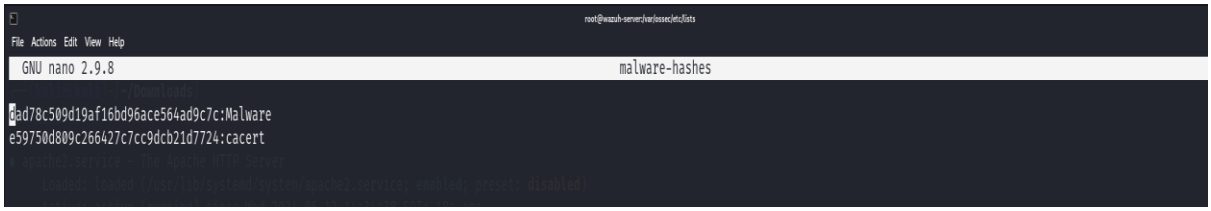
In similar way, I have downloaded another malware and its hashvalue is

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo md5sum Malware.exe
dad78c509d19af16bd96ace564ad9c7c  Malware.exe
```

Now, copy those two hash values and paste them in “malware-hashes” file

```
[root@wazuh-server lists]# nano malware-hashes
```

Paste those hashes:filename



After saving those file, we need to configure the ossec.conf file, in order to add this file in it

So, now go to

Command:

nano /var/ossec/etc/ossec.conf

Now, add this line under “**Default Ruleset**” section

<list>etc/lists/Your-file-name</lists>

```
[root@wazuh-server etc]# nano ossec.conf
```

Now, its time to edit “local_rules.xml” file, under

nano /var/ossec/etc/rules/local_rules.xml

```
[root@wazuh-server rules]# nano local_rules.xml
```

Add this block

```
 <!-- for malware hashes -->
 <rule id="110002" level="13">
   <if_sid>555</if_sid>
   <if_sid>551</if_sid>
   <list field="md5" lookup="match_key">etc/lists/malware-hashes</list>
   <description>Known Malware File Hash is Detected</description>
   <mitre>
     <id>T1204.002</id>
   </mitre>
 </rule>
</group>
```

In order to save all the changes that were made, we need to restart the wazuh-manager

```
[root@wazuh-server rules]# sudo systemctl restart wazuh-manager
```

Linux Agent :

Now, its time to configure Linux agent {Linux endpoint}

Configure the ossec.conf file in linux endpoint

```
root@project01-virtual-machine:/var/ossec/etc# nano ossec.conf
```

Now, try to append these lines under FIM(File integrity monotoring) section

Command:

<directories check_all="yes" realtime="yes">Your-FIM-integrated-Directory-path</directories>

```
  <!-- File integrity monitoring -->
  <syscheck>
    <disabled>no</disabled>
    <directories realtime="yes">/home/project-01/Downloads</directories>
    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</frequency>

    <scan_on_start>yes</scan_on_start>
<!------ For malware hashes functionality --->
    <directories check_all="yes" realtime="yes">/home/project-01/Downloads</directories>
```

We need to restart wazuh-agent, in order to apply the changes

Command:

Sudo systemctl restart wazuh-agent

```
root@project01-virtual-machine:/var/ossec/etc# sudo systemctl restart wazuh-agent
```

Attack simulation :

In order to perform these attacks, I have configured Apache2 and hosted my malwares in that webpage and downloaded them again in order to test our setup

For configuring Apache

Command :

Sudo apt update

Sudo apt install apache2

Sudo systemctl start apache2

Sudo systemctl enable apache2

And you can check the status of your apache2

sudo systemctl status apache2

Now, its time host our downloaded malwares on apache server

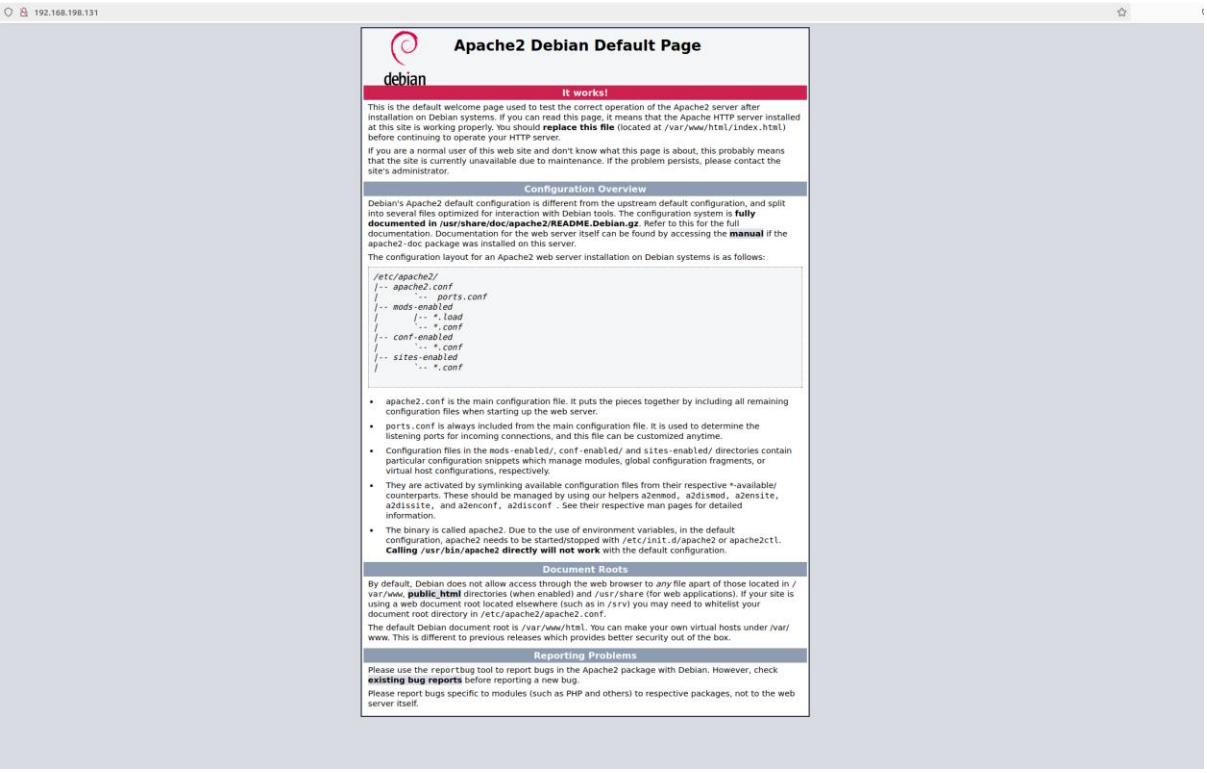
For that

Command:

Sudo cp filename /var/www/html

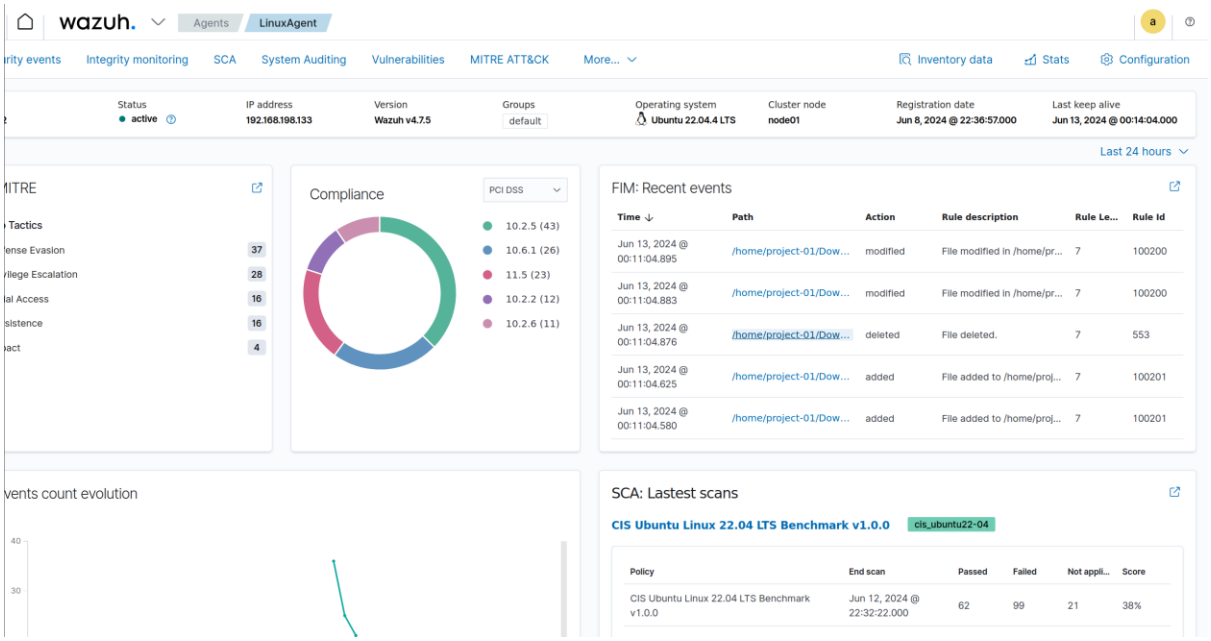
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo cp Malware.exe cacert.der /var/www/html
```

Now, you can access these by just typing your (Linux endpoint) IP address in your browser



From here, you need to download those previously hosted two malwares.

Now, you need to open your wazuh-dashboard, select your agent, under security event you can find the alerts



Thus, we were able to detect the knows malwares when downloaded by using CDB.