Project Report

Enterprise Security Threat Detection and Prevention System

**Steps involved:**

1. **Start Wazuh Server in virtual**

* ip a ( to know the ip address of the wazuh)

1. **Start the kali linux OS**

#Open terminal

* ifconfig (to know the ip address of kali)

1. **Install Wazuh Agent on Victim Refer to:**

# https://documentation.wazuh.com/current/installation-guide/index.html

* Configure Wazuh Manager to Collect Logs
* Sudo nano /var/ossec/etc/ossec.conf

#paste the command in the bash

Wazuh - Agent - Default configuration for kali 2025.1

More info at: https://documentation.wazuh.com

Mailing list: https://groups.google.com/forum/#!forum/wazuh

-->

<ossec\_config>

<client>

<server>

<address>Manager Ip</address>

<port>1514</port>

<protocol>tcp</protocol>

</server>

<config-profile>kali, kali2025, kali2025.1</config-profile>

<notify\_time>10</notify\_time>

<time-reconnect>60</time-reconnect>

<auto\_restart>yes</auto\_restart>

<crypto\_method>aes</crypto\_method>

</client>

<client\_buffer>

<!-- Agent buffer options -->

<disabled>no</disabled>

<queue\_size>5000</queue\_size>

<events\_per\_second>500</events\_per\_second>

</client\_buffer>

<!-- Policy monitoring -->

<rootcheck>

<disabled>no</disabled>

<check\_files>yes</check\_files>

<check\_trojans>yes</check\_trojans>

<check\_dev>yes</check\_dev>

<check\_sys>yes</check\_sys>

<check\_pids>yes</check\_pids>

<check\_ports>yes</check\_ports>

<check\_if>yes</check\_if>

<!-- Frequency that rootcheck is executed - every 12 hours -->

<frequency>43200</frequency>

<rootkit\_files>etc/shared/rootkit\_files.txt</rootkit\_files>

<rootkit\_trojans>etc/shared/rootkit\_trojans.txt</rootkit\_trojans>

<skip\_nfs>yes</skip\_nfs>

<ignore>/var/lib/containerd</ignore>

<ignore>/var/lib/docker/overlay2</ignore>

</rootcheck>

<wodle name="cis-cat">

<disabled>yes</disabled>

<timeout>1800</timeout>

<interval>1d</interval>

<scan-on-start>yes</scan-on-start>

<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 -->

<synchronization>

<max\_eps>10</max\_eps>

</synchronization>

</wodle>

<sca>

<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>

<!-- 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>

<ignore>/etc/utmpx</ignore>

<ignore>/etc/wtmpx</ignore>

<ignore>/etc/cups/certs</ignore>

<!-- File types to ignore -->

<ignore type="sregex">.log$|.swp$</ignore>

<!-- Check the file, but never compute the diff -->

<nodiff>/etc/ssl/private.key</nodiff>

<skip\_nfs>yes</skip\_nfs>

<skip\_dev>yes</skip\_dev>

<skip\_proc>yes</skip\_proc>

<skip\_sys>yes</skip\_sys>

<!-- Nice value for Syscheck process -->

<process\_priority>10</process\_priority>

<!-- Maximum output throughput -->

<max\_eps>50</max\_eps>

<!-- Database synchronization settings -->

<synchronization>

<enabled>yes</enabled>

<interval>5m</interval>

<max\_eps>10</max\_eps>

</synchronization>

</syscheck>

<!-- Log analysis -->

<localfile>

<log\_format>command</log\_format>

<command>df -P</command>

<frequency>360</frequency>

</localfile>

<localfile>

<log\_format>full\_command</log\_format>

<command>netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:]]\+\ \+\(.\*\):\([[:digit:]]\*\)\ \+\([0-9>

<alias>netstat listening ports</alias>

<frequency>360</frequency>

</localfile>

<localfile>

<log\_format>full\_command</log\_format>

<command>last -n 20</command>

<frequency>360</frequency>

</localfile>

<!-- Active response -->

<active-response>

<disabled>no</disabled>

<ca\_store>etc/wpk\_root.pem</ca\_store>

<ca\_verification>yes</ca\_verification>

</active-response>

<!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->

<logging>

<log\_format>plain</log\_format>

</logging>

</ossec\_config>

<ossec\_config>

<localfile>

<log\_format>journald</log\_format>

<location>journald</location>

</localfile>

<localfile>

<log\_format>apache</log\_format>

<location>/var/log/nginx/access.log</location>

</localfile>

<localfile>

<log\_format>apache</log\_format>

<location>/var/log/nginx/error.log</location>

</localfile>

<localfile>

<log\_format>apache</log\_format>

<location>/var/log/apache2/error.log</location>

</localfile>

<localfile>

<log\_format>apache</log\_format>

<location>/var/log/apache2/error.log</location>

</localfile>

<localfile>

<log\_format>apache</log\_format>

<location>/var/log/apache2/access.log</location>

</localfile>

<localfile>

<log\_format>syslog</log\_format>

<location>/var/ossec/logs/active-responses.log</location>

</localfile>

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/dpkg.log</location>

</localfile>

</ossec\_config>

* Open the browser and enter the ip address of the wazuh manager and open it with username and passward (admin and admin).
* Deploy new agent.

1. **Implement a firewall in OS**
2. **Initiate SSh attack:**

#sudo apt update

sudo apt install openssh-server

sudo systemctl enable ssh

sudo systemctl start ssh

1. **Simulate Malware Execution**

* Download the EICAR Test File (Safe Dummy Malware) curl -o eicar.com.txt <https://www.eicar.org/download/eicar.com.txt>.
* Execute the File on Victim (Just Opening It) cat [eicar.com](http://eicar.com).txt
* Log Monitoring and Alerting

# sudo tail -f /var/ossec/logs/ossec.log

1. **Create Sigma or YARA Rule**

Sample Sigma Rule for SSH Brute Force:

# Use Hydra on Kali to Launch Brute Force Attack

hydra -l username -P /usr/share/wordlists/rockyou.txt ssh://<victim\_ip>

# Check Logs on Victim

sudo cat /var/log/auth.log | grep "Failed password"

1. **Set Up a honey pot**

* Install cowrie
* Install docker and dionaea
* Run it in virtual environment
* Start the cowrie honeypot
* Monitor the logs by again initiating the attack

1. **Log collection and monitoring**

* Use MISP Docker for collection of logs
* Write python code for gathering information using shodan.
* To automate log analysing using python