Osquery and Wazuh

1. Setup and Installation

- Install and configure Osquery and Wazuh on a virtual machine.

```
  GNU nano 8.1     /etc/systemd/system/osqueryd.service
[Unit]
Description=osqueryd service
After=network.target

[Service]
ExecStart=/usr/bin/osqueryd --flagfile=/etc/osquery/osquery.flags
StandardOutput=syslog
StandardError=syslog
Restart=always
RestartSec=5

[Install]
WantedBy=multi-user.target
```

- Install Osquery: Download and install Osquery on the chosen system.

  Debian and Ubuntu based Linux distributions:

  export OSQUERY_KEY=1484120AC4E9F8A1A577AEEE97A80C63C9D8B80B

  apt-key adv --keyserver keyserver.ubuntu.com --recv-keys $OSQUERY_KEY

  add-apt-repository 'deb [arch=amd64] https://pkg.osquery.io/deb deb main'

  apt-get update

  apt-get install osquery

```
root@ntsapi:/home/ntsapi# osqueryi --version
osqueryi version 5.13.1
```

  For kali

  sudo apt-get update

  sudo apt-get install osquery

```
┌──(root㉿kali)-[~]
└─# osqueryi --version
osqueryi version 5.13.1
```

- Configure Osquery to run as a daemon.Validate the installation by running some basic queries.

```
  GNU nano 8.1          /etc/osquery/osquery.conf
{
  "options": {
    "config_plugin": "filesystem",
    "logger_plugin": "filesystem",
    "logger_path": "/var/log/osquery/",
    "enable_monitor": true,
    "disable_logging": false,
    "disable_events": false,
    "events_expiry": 3600,
    "schedule_splay_percent": 10,
    "events_max": 50000
  },
  "schedule": {
    "system_info": {
      "query": "SELECT hostname, cpu_brand, physical_memory FROM sys>
      "interval": 3600
    },
    "processes": {
      "query": "SELECT pid, name, path, cmdline FROM processes;",
      "interval": 300
    },
    "listening_ports": {
      "query": "SELECT * FROM listening_ports;",
      "interval": 300
    }
  }
}
```

Restart Osquery Daemon:

systemctl restart osqueryd

Validate Configuration:

osqueryi "SELECT * FROM listening_ports;"

- Install the Wazuh manager on the same virtual machine. Install the Wazuh agent on the system where Osquery is installed.

- Installation of wazuh repository:

  curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -

  echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list

- Installation of wazuh manager:

  sudo apt-get update

  sudo apt-get install wazuh-manager

- Start wazuh Manager:

```
┌──(root㉿kali)-[~]
└─# sudo systemctl start wazuh-manager
sudo systemctl enable wazuh-manager

Created symlink '/etc/systemd/system/multi-user.target.wants/wazuh-manager.
service' → '/usr/lib/systemd/system/wazuh-manager.service'.
```

- Ensure that the Wazuh agent can communicate with the Wazuh manager.
  Installation of the agent:
  sudo apt-get install wazuh-agent
  Configure Wazuh Agent:
  sudo nano /var/ossec/etc/ossec.conf
  * insert the manager ip under <server> (host_ip in my case)
  Start Wazuh Agent:
  sudo systemctl start wazuh-agent

  sudo systemctl enable wazuh-agent

2. Configure Wazuh to collect data from Osquery and create rules and alerts.
- Configure Osquery to log events in a structured format.
- Modify the Osquery configuration file to include useful tables (e.g., processes, listening ports, scheduled tasks).
- Configure Wazuh to read Osquery logs.
- Ensure the Wazuh agent is correctly parsing Osquery logs and forwarding them to the Wazuh manager.
- Create custom decoders in Wazuh for Osquery logs if necessary.

3. Testing the Integration:
- Perform various actions on the system (e.g., start/stop services, add new users) and verify that these activities are logged by Osquery and forwarded to Wazuh.
- Create test alerts in Wazuh based on Osquery logs.

4. Develop and deploy Osquery queries and Wazuh alerts to monitor critical system activities.
- Create a set of Osquery queries to monitor critical activities (e.g., user logins, file modifications, network connections).
- Schedule these queries to run at regular intervals using the Osquery scheduler.
- Create alert rules in Wazuh based on the data collected from the custom Osquery queries.
- Define thresholds and conditions for triggering alerts.
- Perform actions that should trigger the queries and alerts.
- Verify that the alerts are being generated and are accurately reflecting the monitored activities.

5. Documentation:
- Configuration and integration process.

- Analysis of the logs and alerts collected. Identification of patterns, anomalies etc. Include charts/ graphs (optional) and screenshots to illustrate key points.

Be ready to present the project to your of peers and coach, highlighting the benefits of integrating Osquery with Wazuh.