OSSEC HIDS

OSSEC is an open source host-based intrusion detection system (HIDS) that can be used to monitor file system changes on an operating system. For Windows OSSEC runs as a single service.

Agent/Server Communication

The OSSEC server listens on 1514/udp via ossec-remoted. Agents send messages to the server via ossec-agentd. The communication is two-way but initiated by the agent.

OSSEC installation:

Server side:

1. Use the link to download the VM file(https://www.ossec.net/downloads/)

2. Follow the steps below and as shown in the link

   https://www.ossec.net/docs/manual/installation/installation-windows.html#step-1-opening-the-agent-manager-menu

```
File  Edit  View  Search  Terminal  Help
[ossec@ossec-server ~]$ sudo su
[root@ossec-server ossec]# cd /var/ossec/bin/manage_agents
bash: cd: /var/ossec/bin/manage_agents: Not a directory
[root@ossec-server ossec]# cd /var/ossec/bin
[root@ossec-server bin]# ./manage_agents


****************************************
* OSSEC HIDS v2.9.2 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

```
****************************************
* OSSEC HIDS v2.9.2 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: a

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: Mywindowsmachine
   * The IP Address of the new agent: 192.168.0.16
   * An ID for the new agent[002]: 19871986
```

```
Confirm adding it?(y/n): y
Agent added.


****************************************
* OSSEC HIDS v2.9.2 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: e

Available agents:
   ID: 19871986, Name: Mywindowsmachine, IP: 192.168.0.16
Provide the ID of the agent to extract the key (or '\q' to quit): 19871986
```

3. Modify the agent.conf file under cd /var/ossec/etc/shared/agent.conf. Add the file path for Dropbox folder using the sample shown in this link (https://www.ossec.net/docs/manual/monitoring/file-log-monitoring.html#configuration)

Agent Side

For setting up the Windows Agent: (At present the download link for windows agent on OSSEC website does not work, hence we have to use alt. method)

1. https://bintray.com/artifact/download/ossec/ossec-hids/ossec-agent-win32-2.8.3.exe
2. Enter server ip- which is your VM IP and then extract key from server for agent(use steps above)
3. Hit save and restart agent.
4. /var/ossec/bin/ossec-control restart the OSSEC server
5. /var/ossec/bin/agent_control -lc on server terminal to check if connection is active. If yes agent is connected to server.