OSSEC ASSIGNMENT

1) What is OSSEC and what are it key features/benefits?

OSSEC is a platform to monitor and control your systems. It mixes together all the aspects of HIDS (host-based intrusion detection), log monitoring, and Security Incident Management (SIM)/Security Information and Event Management (SIEM) together in a simple, powerful, and open source solution.

OSSEC is open Source Host-based Intrusion Detection System. It helps to monitor your systems by performing different methods which are mentioned below:

OSSEC is mainly useful for 3 things:

see what is going on;

Stop brute-force attacks (ftp, web, ssh);

Cover PCI-compliance requirements related to monitoring.

Key Features / Benefits

- Log Monitoring

Every operating system, application, and device on your network generate logs (events) to let you know what is happening. OSSEC collects, analyzes and correlates these logs to let you know if something suspicious is happening (attack, misuse, errors, etc).

- Rootkit detection

Criminal hackers want to hide their actions, but using rootkit detection you can be notified when the system is modified in a way common to rootkits.

- Active response

Active response allows OSSEC to take immediate action when specified alerts are triggered. This may prevent an incident from spreading before an administrator can take action.

- File Integrity checking

The goal of file integrity checking is to detect system changes and alert you. It can be an attack, or a misuse by an employee or even a typo by an admin, any file, directory or registry change will be alerted to you.

- Compliance Requirements

OSSEC helps customers meet specific compliance requirements such as PCI and HIPAA. It lets customers detect and alert on unauthorized file system modifications and malicious behavior embedded in the log files of commercial products as well as custom applications.

- Multi platform

OSSEC lets customers implement a comprehensive host based intrusion detection system with fine grained application/server specific policies across multiple platforms such as Linux, Solaris, Windows, and Mac OS X.

- Real-time and Configurable Alerts

OSSEC lets customers configure incidents they want to be alerted on, and lets them focus on raising the priority of critical incidents over the regular noise on any system. Integration with smtp, sms, and syslog allows customers to be on top of alerts by sending them to e-mail enabled devices. Active response options to block an attack immediately are also available.

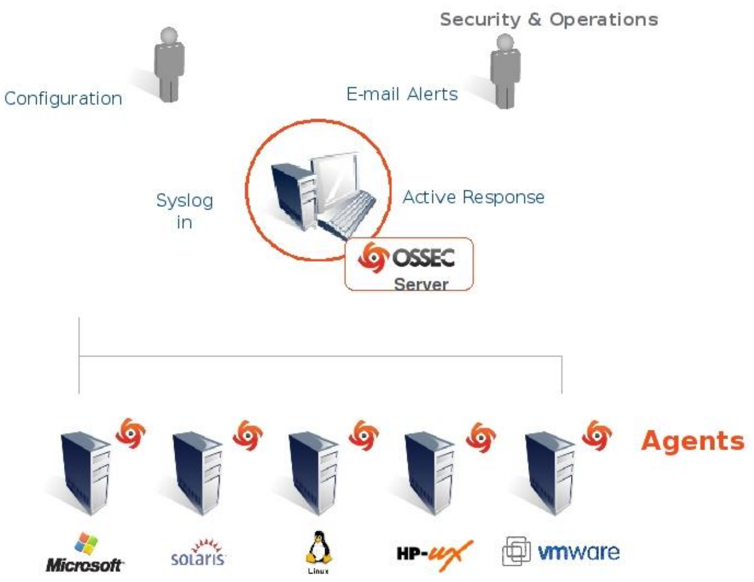
- Integration with current infrastructure

OSSEC will integrate with current investments from customers such as SIM/SEM (Security Incident Management/Security Events Management) products for centralized reporting and correlation of events.

- Centralized management

OSSEC provides a simplified centralized management server to manage policies across multiple operating systems. Additionally, it also lets customers define server specific overrides for finer grained policies.

2) What is the architecture of OSSEC?



This diagram shows the central manager receiving events from the agents and system logs from remote devices. When something is detected, active responses can be executed and the admin is notified.

OSSEC is composed of multiple pieces. It has a central manager for monitoring and receiving information from agents, syslog, databases, and from agentless devices.

- Manager (or Server)

The manager is the central piece of the OSSEC deployment. It stores the file integrity checking databases, the logs, events, and system auditing entries. All the rules, decoders, and major configuration options are stored centrally in the manager; making it easy to administer even a large number of agents.

Agents connect to the server on port 1514/udp. Communication to this port must be allowed for agents to communicate with the server.

- Agents

The agent is a small program, or collection of programs, installed on the systems to be monitored. The agent will collect information and forward it to the manager for analysis and correlation. Some information is collected in real time, others periodically. It has a very small memory and CPU footprint by default, not affecting the system's usage.

Agent security: It runs with a low privilege user (generally created during the installation) and inside a chroot jail isolated from the system. Most of the agent configuration can be pushed from the manager.

- Agentless

For systems that an agent cannot be installed on, the agentless support may allow integrity checks to be performed. Agentless scans can be used to monitor firewalls, routers, and even Unix systems.

- Virtualization/VMware

OSSEC allows you to install the agent on the guest operating systems. It may also be installed inside some versions of VMWare ESX, but this may cause support issues. With the agent installed inside VMware ESX you can get alerts about when a VM guest is being installed, removed, started, etc. It also monitors logins, logouts and errors inside the ESX server. In addition to that, OSSEC performs the Center for Internet Security (CIS) checks for VMware, alerting if there is any insecure configuration option enabled or any other issue.

- Firewalls, switches and routers

OSSEC can receive and analyze syslog events from a large variety of firewalls, switches and routers. It supports all Cisco routers, Cisco PIX, Cisco FWSM, Cisco ASA, Juniper Routers, Netscreen firewall, Checkpoint and many others.

3) **Where is the configuration file how can you configure/customise OSSEC behavior?**

After default and direct installation

Configuration file is on below path:

/var/**ossec**/etc/**ossec**.conf.

/var/ossec having sub directories like bin, etc, log, queue, rules, stats, tmp, var

Etc/ossec.conf has 6 sections

- global (global):- general information are set here : where to send notification and which SMTP server. Change it if you don’t receive alert, or want to white-list some host/ip.

- rules (rules):- has a list of files being monitored can add another you want to monitor, can write own rules <include> rules_config.xml</include>

- syscheck (syscheck/rootcheck):- <directories checkall=”yes”> with the path of directory</directories>

- alerts (alert):- alerts are sent to the mail. Each rule is configured with alert level.

- active-response (command/active-response);

- collector (localfile).

To configure : **logcollector**

to monitor one file:

```
<localfile>
        <log_format>apache</log_format>
        <location>/var/www/logs/error_log</location>
</localfile>
```

To configure : **analysisd**

to read a specific rules file:

```
<rules>
        <include>myrules.xml</include>
</rules>
```

To configure : **remoted**

to accept remote syslog:

```
<remote>
        <connection>syslog</connection>
        <port>514</port>
        <allowed-ips>192.168.2.0/24</allowed-ips>
</remote>
```

4) Where is OSSEC output stored?

The output from an event will be stored in an internal database
Internally stored in a tree structure.

All **logs** are stored in subdirectories of /var/**ossec**/**logs**/**ossec**.**log**

5) How to we control/fine tune events reported by OSSEC?

We can perform the following alerts

```
<alerts>
  <log_alert_level>1</log_alert_level>
  <email_alert_level>7</email_alert_level>
</alerts>
```

OSSEC reports feature provides a flexible way to send condensed reports to give you daily insight into alerts that are interesting, though not actionable as individual events. To configure a report of successful logins, add this to your ossec.conf file:

```
<reports>
  <category>authentication_success</category>
  <user type="relation">srcip</user>
  <title>OSSEC: Authentication Report</title>
  <email_to>security.alerts@example.com</email_to>
</reports>
```

6) Where are rules stored? How are rules matched?

Rules stored in:

/var/ossec/rules/*.xml

Each rule is defined in a separate XML file. The default installation of the OSSEC HIDS contains 43 rules files.

Starting with the 0 level those rules are tried and then all the other rules in a decreasing order by their level

If the level is the same the order will be decided based on the rules listed in /var/ossec/etc/ossec.conf

If there are any requirements in the rules those requirements are tried first

7) What are the different rules groups?

We currently use the following groups:

- invalid_login
- authentication_success
- authentication_failed
- connection_attempt
- attacks
- adduser
- sshd
- ids
- firewall
- squid
- apache
- syslog

8) What are different rules levels and what do they signify?

The rules are classified in multiple levels. From the lowest (00) to the maximum level 16. Some levels are not used right now. Other levels can be added between them or after them.

The rules will be read from the highest to the lowest level.

00 - Ignored - No action taken. Used to avoid false positives. These rules are scanned before all the others. They include events with no security relevance.

01 - None -

02 - System low priority notification - System notification or status messages. They have no security relevance.

03 - Successful/Authorized events - They include successful login attempts, firewall allow events, etc.

04 - System low priority error - Errors related to bad configurations or unused devices/applications. They have no security relevance and are usually caused by default installations or software testing.

05 - User generated error - They include missed passwords, denied actions, etc. By itself they have no security relevance.

06 - Low relevance attack - They indicate a worm or a virus that have no affect to the system (like code red for apache servers, etc). They also include frequently IDS events and frequently errors.

07 - “Bad word” matching. They include words like “bad”, “error”, etc. These events are most of the time unclassified and may have some security relevance.

08 - First time seen - Include first time seen events. First time an IDS event is fired or the first time an user logged in. If you just started using OSSEC HIDS these messages will probably be frequently. After a while they should go away, It also includes security relevant actions (like the starting of a sniffer or something like that).

09 - Error from invalid source - Include attempts to login as an unknown user or from an invalid source. May have security relevance (specially if repeated). They also include errors regarding the “admin” (root) account.

10 - Multiple user generated errors - They include multiple bad passwords, multiple failed logins, etc. They may indicate an attack or may just be that a user just forgot his credentials.

11 - Integrity checking warning - They include messages regarding the modification of binaries or the presence of rootkits (by rootcheck). If you just modified your system configuration you should be fine regarding the “syscheck” messages. They may indicate a successful attack. Also included IDS events that will be ignored (high number of repetitions).

12 - High importancy event - They include error or warning messages from the system, kernel, etc. They may indicate an attack against a specific application.

13 - Unusual error (high importance) - Most of the times it matches a common attack pattern.

14 - High importance security event. Most of the times done with correlation and it indicates an attack.

15 - Severe attack - No chances of false positives. Immediate attention is necessary.