

JHU SU20 IDS Module 3 Lab  
Audrey Long  
06/14/2020

## 1. Reading Assignment(s)

**Purpose:** The background reading assignment below will familiarize you with these components of OSSEC as a HIDS.

1. <http://en.wikipedia.org/wiki/OSSEC>

## 2. OSSEC File Monitoring

<https://ossec-docs.readthedocs.io/en/latest/docs/manual/monitoring/index.html>

<https://ossec-docs.readthedocs.io/en/latest/docs/manual/monitoring/file-log-monitoring.html>

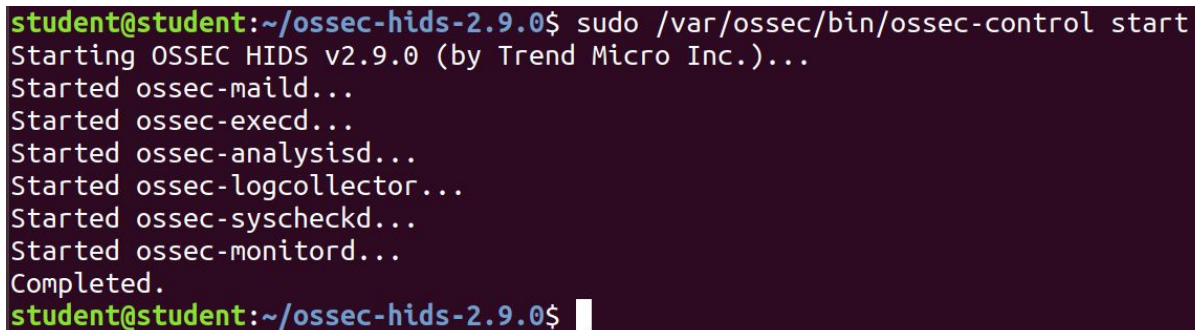
### Part A: Intro to OSSEC

**Assumption:** You have finished reviewing/reading links above.

**Purpose:** OSSEC is a specific HIDS. This assignment is to understand OSSEC functionalities as a HIDS.

**Exercise:** For this Module Assignment please do some research and answer the following questions with screenshots and descriptions.

#### 1) Within your Ubuntu VM, assure OSSEC is installed and running (provide screen shot)

A terminal window with a dark purple background. The prompt is 'student@student:~/ossec-hids-2.9.0\$'. The command 'sudo /var/ossec/bin/ossec-control start' has been entered. The output shows the OSSEC HIDS v2.9.0 starting, followed by several components: ossec-maild, ossec-execd, ossec-analysisd, ossec-logcollector, ossec-syscheckd, and ossec-monitord. The process ends with 'Completed.' and the prompt returns to 'student@student:~/ossec-hids-2.9.0\$' with a cursor.

```
student@student:~/ossec-hids-2.9.0$ sudo /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v2.9.0 (by Trend Micro Inc.)...
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
student@student:~/ossec-hids-2.9.0$
```

#### 2) What are the capabilities of OSSEC as a HIDS?

OSSEC is a fully open source and free server intrusion detection tool which can be tailored for each platform's security needs through its configuration options, log analysis, integrity checking, windows registry monitoring, rootkit detection, time-based alerting, and provides OS intrusion detection (for a vast majority of OS), custom rule management, custom alerts and custom script responses. This tool helps organizations meet compliance requirements such as PCI DSS as it detects and alerts on unauthorized file system modification and reports on malicious behavior.

#### 3) What are the components of OSSEC as a HIDS?

OSSEC consists of the following main components: a server (manager) required for distributed network, an Agent used on the system to be monitored, and Agentless mode which can be used to monitor firewalls, routers, and unix systems.

#### **4) How does OSSEC analyze the log? In other words, what is the internal log flow of the OSSEC?**

Log analysis is done inside OSSEC by the logcollector and analysis process. The first one collects the events and the second one analyzes by decoding, filtering, and classifies the events. This process is done in real time, so as soon as an event is written OSSEC will process them. OSSEC can read events from internal log files, from the Windows event log and also receive them directly via remote syslog.

#### **5) Explain how OSSEC performs file integrity monitoring?**

OSSEC includes FIM as a part of its comprehensive solution to host-based intrusion detection. File integrity monitoring looks at those attributes of a file that may indicate that its content has changed. These attributes include size, modification and creation times, one-way hashes of the contents of the file itself, and ownership and permissions of the file. Any change to one or more of these attributes triggers an alert. With OSSEC, we can customize the checks at a system-wide, per-directory, or even per-file level.

#### **6) Describe one major difference between OSSEC and Tripwire.**

Essentially Tripwire monitors files and reports unauthorized changes while cross referencing the files to ensure the integrity of the files. OSSEC runs on an OS and exchanges messages between the agent and the server via encrypted messages and comes equipped with an advanced log analysis engine.

### **Part B: Mod 3 Lab Testing OSSEC**

**Purpose:** The purpose of this assignment is to use your Ubuntu VM as a platform to practice IDS and to use it as a hands-on platform for the rest of the semester

#### **A) Devise and document a methodology to test for the proper operation of OSSEC**

Step 0.) Download and add configuration into ossec-logcollector to alert on new events OSSEC along with where email alerts get sent to.

Step 1.) is to edit the /var/ossec/etc/ossec.conf file to add rules for ossec to monitor and alert to log files for new events. Essentially when new log messages arrive, they get forwarded to other processes for analysis. Below demonstrates the local file to be monitored is in var/log/messages and we are looking for the log format of syslog files.

```
GNU nano 2.9.3 /var/ossec/etc/ossec.conf

<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
</localfile>

<localfile>
  <log_format>full_command</log_format>
  <command>netstat -tan |grep LISTEN |egrep -v '(127.0.0.1| ::1)' | sort</command>
</localfile>

<localfile>
  <log_format>full_command</log_format>
  <command>last -n 5</command>
</localfile>

<localfile>
  <location>/var/log/messages</location>
  <log_format>syslog</log_format>
</localfile>

</ossec_config>

<ossec_config> <!-- rules global entry -->
  <rules>
    <include>rules_config.xml</include>
    <include>pam_rules.xml</include>
    <include>sshd_rules.xml</include>
    <include>telnetd_rules.xml</include>
    <include>syslog_rules.xml</include>
    <include>arpwatch_rules.xml</include>
    <include>symantec-av_rules.xml</include>
    <include>symantec-ws_rules.xml</include>
    <include>pix_rules.xml</include>
    <include>named_rules.xml</include>
```

Step 2.) After the configuration file was modified and saved, I proceeded to download a few packages using sudo-apt get install, after the downloads were complete I was alerted that I received new mail.

```
oot@student:/var/ossec/etc# ls
client.keys  internal_options.conf  local_internal_options.conf  ossec.conf  ossec-init.conf
decoder.xml  internal_options.conf~  localtime             ossec.conf.19019.bak  shared
You have new mail in /var/mail/root
oot@student:/var/ossec/etc#
oot@student:/var/ossec/etc#
oot@student:/var/ossec/etc#
```

Step 3.) After receiving an email you can use the command “mail” to display all of the emails you've received from OSSEC.

```
root@student:/var/ossec/bin# mail
"/var/mail/root": 48 messages 48 new
>N 1 Anacron Sat Jun 13 11:22 660/46285 Anacron job 'cron.daily' on student
N 2 OSSEC HIDS Sat Jun 13 11:41 43/980 OSSEC Notification - student - Alert level 7
N 3 OSSEC HIDS Sat Jun 13 11:42 29/821 OSSEC Notification - student - Alert level 4
N 4 OSSEC HIDS Sat Jun 13 11:43 43/980 OSSEC Notification - student - Alert level 7
N 5 OSSEC HIDS Sat Jun 13 11:46 29/818 OSSEC Notification - student - Alert level 4
N 6 OSSEC HIDS Sat Jun 13 11:56 58/1369 OSSEC Notification - student - Alert level 7
N 7 OSSEC HIDS Sat Jun 13 13:44 28/766 OSSEC Notification - student - Alert level 7
N 8 OSSEC HIDS Sat Jun 13 15:44 28/766 OSSEC Notification - student - Alert level 7
N 9 OSSEC HIDS Sat Jun 13 17:45 28/766 OSSEC Notification - student - Alert level 7
N 10 OSSEC HIDS Sat Jun 13 19:45 28/766 OSSEC Notification - student - Alert level 7
N 11 OSSEC HIDS Sat Jun 13 20:05 28/782 OSSEC Notification - student - Alert level 2
N 12 OSSEC HIDS Sat Jun 13 20:20 40/934 OSSEC Notification - student - Alert level 7
N 13 OSSEC HIDS Sat Jun 13 20:21 30/898 OSSEC Notification - student - Alert level 7
N 14 OSSEC HIDS Sat Jun 13 20:22 30/898 OSSEC Notification - student - Alert level 7
N 15 OSSEC HIDS Sat Jun 13 20:22 30/897 OSSEC Notification - student - Alert level 7
N 16 OSSEC HIDS Sat Jun 13 20:23 90/2400 OSSEC Notification - student - Alert level 7
N 17 OSSEC HIDS Sat Jun 13 20:23 30/897 OSSEC Notification - student - Alert level 7
N 18 OSSEC HIDS Sat Jun 13 20:24 50/1396 OSSEC Notification - student - Alert level 7
N 19 OSSEC HIDS Sat Jun 13 20:24 175/3475 OSSEC Notification - student - Alert level 7
N 20 OSSEC HIDS Sat Jun 13 20:25 40/934 OSSEC Notification - student - Alert level 7
N 21 OSSEC HIDS Sat Jun 13 20:26 25/769 OSSEC Notification - student - Alert level 2
N 22 OSSEC HIDS Sat Jun 13 20:27 40/934 OSSEC Notification - student - Alert level 7
N 23 OSSEC HIDS Sat Jun 13 20:30 30/922 OSSEC Notification - student - Alert level 7
N 24 OSSEC HIDS Sat Jun 13 20:32 29/845 OSSEC Notification - student - Alert level 7
N 25 OSSEC HIDS Sat Jun 13 20:33 30/905 OSSEC Notification - student - Alert level 7
N 26 OSSEC HIDS Sat Jun 13 20:33 30/910 OSSEC Notification - student - Alert level 7
N 27 OSSEC HIDS Sat Jun 13 20:34 49/1392 OSSEC Notification - student - Alert level 7
N 28 OSSEC HIDS Sat Jun 13 20:34 30/899 OSSEC Notification - student - Alert level 7
N 29 OSSEC HIDS Sat Jun 13 20:35 29/865 OSSEC Notification - student - Alert level 7
N 30 OSSEC HIDS Sat Jun 13 20:36 29/870 OSSEC Notification - student - Alert level 7
N 31 OSSEC HIDS Sat Jun 13 20:36 29/879 OSSEC Notification - student - Alert level 7
N 32 OSSEC HIDS Sat Jun 13 20:37 30/897 OSSEC Notification - student - Alert level 7
N 33 OSSEC HIDS Sat Jun 13 21:00 99/2564 OSSEC Notification - student - Alert level 7
N 34 OSSEC HIDS Sat Jun 13 21:02 235/4852 OSSEC Notification - student - Alert level 7
N 35 OSSEC HIDS Sat Jun 13 21:05 25/690 OSSEC Notification - student - Alert level 7
```

Step 4:) Analyze the contents of the email and take action or declare the event a false positive and perhaps whitelist the item or change the confirmation file. Below shows the email of the /var/log/syslog event set up from the first step. Notice the Anacron Tripwire job.



```
? 3
Return-Path: <ossecm@student>
X-Original-To: root@localhost
Delivered-To: root@localhost
Received: from notify.ossec.net (localhost [127.0.0.1])
    by student (Postfix) with SMTP id D0A5187381
    for <root@localhost>; Sat, 13 Jun 2020 11:42:46 -0400 (EDT)
To: <root@localhost>
From: OSSEC HIDS <ossecm@student>
Date: Sat, 13 Jun 2020 11:42:46 -0400
Subject: OSSEC Notification - student - Alert level 4
Message-Id: <20200613154246.D0A5187381@student>

OSSEC HIDS Notification.
2020 Jun 13 11:42:33

Received From: student->/var/log/auth.log
Rule: 5403 fired (level 4) -> "First time user executed sudo."
User: student
Portion of the log(s):

Jun 13 11:42:33 student sudo: student : TTY=pts/0 ; PWD=/home/student/ossec-hids-2.9.0 ; USER=root ; COMMAND=/usr/sbin/service ossec-hids-server status

--END OF NOTIFICATION

? █
```

## 2. Execute your methodology to verify the proper operation of OSSEC and submit screenshots showing this procedure in practice

### B) Demonstrate

1. Verify that OSSEC is running by opening up a command terminal and entering the following line: `sudo service ossec-hids-server status`

```
root@student:/var/ossec/bin# sudo service ossec status
● ossec.service - LSB: Start and stop OSSEC HIDS
   Loaded: loaded (/etc/init.d/ossec; generated)
   Active: inactive (dead)
     Docs: man:systemd-sysv-generator(8)
root@student:/var/ossec/bin# sudo service ossec start
root@student:/var/ossec/bin# sudo service ossec status
● ossec.service - LSB: Start and stop OSSEC HIDS
   Loaded: loaded (/etc/init.d/ossec; generated)
   Active: active (exited) since Sat 2020-06-13 21:11:40 EDT; 2s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 9064 ExecStart=/etc/init.d/ossec start (code=exited, status=0/SUCCESS)

Jun 13 21:11:38 student systemd[1]: Starting LSB: Start and stop OSSEC HIDS...
Jun 13 21:11:38 student ossec[9064]: Starting OSSEC HIDS v2.9.0 (by Trend Micro Inc.)...
Jun 13 21:11:38 student ossec[9064]: ossec-maild already running...
```

Now let's demonstrate adding a rule to the `/var/ossec/rules/local_rules.xml` file. Below ive added the custom rule "Local Rules for Example" with the rule id of 100000

```
File Edit View Search Terminal Help
GNU nano 2.9.3 /var/ossec/rules/local_rules.xml

<group name="local,syslog,">

  <!-- Note that rule id 5711 is defined at the ssh_rules file
  - as a ssh failed login. This is just an example
  - since ip 1.1.1.1 shouldn't be used anywhere.
  - Level 0 means ignore.
  -->
  <rule id="100001" level="0">
    <if_sid>5711</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>Example of rule that will ignore sshd </description>
    <description>failed logins from IP 1.1.1.1.</description>
  </rule>

<!-- Local Rules for Example.com -->
<group name="local,syslog,">
  <rule id="100000" level="0">
    <if_sid>1002</if_sid>
    <program_name>custom-app</program_name>
    <description>Ignore errors for custom-app</description>
  </rule>
</group>
<!-- This example will ignore ssh failed logins for the user name XYZABC.
-->
<!--
<rule id="100020" level="0">
  <if_sid>5711</if_sid>
  <user>XYZABC</user>
  <description>Example of rule that will ignore sshd </description>
  <description>failed logins for user XYZABC.</description>
</rule>
-->

<!-- Specify here a list of rules to ignore. -->
```

Once the rule was added and saved then the "ossec-logtest" was ran and below demonstrates the alert being displayed for the log entered.

```
root@student:/var/ossec/rules# sudo /var/ossec/bin/ossec-logtest
2020/06/14 16:47:54 ossec-testrule: INFO: Reading local decoder file.
2020/06/14 16:47:54 ossec-testrule: INFO: Started (pid: 19894).
ossec-testrule: Type one log per line.
```

```
**Phase 3: Completed filtering (rules).
  Rule id: '100000'
  Level: '0'
  Description: 'Ignore unknown errors for custom-app'

**Phase 1: Completed pre-decoding.
  full event: '**Phase 3: Completed filtering (rules).'
  hostname: 'student'
  program_name: '(null)'
  log: '**Phase 3: Completed filtering (rules).'

**Phase 2: Completed decoding.
  No decoder matched.

**Phase 1: Completed pre-decoding.
  full event: '      Rule id: '100000''
  hostname: 'student'
  program_name: '(null)'
  log: '      Rule id: '100000''

**Phase 2: Completed decoding.
  No decoder matched.

**Phase 1: Completed pre-decoding.
  full event: '      Level: '0''
  hostname: 'student'
  program_name: '(null)'
  log: '      Level: '0''

**Phase 2: Completed decoding.
  No decoder matched.
```

## References

<https://blog.rapid7.com/2017/06/30/how-to-install-and-configure-ossec-on-ubuntu-linux/>  
[https://subscription.packtpub.com/book/networking\\_and\\_servers/9781782167648/1/ch01lvl1sec14/file-integrity-monitoring-simple](https://subscription.packtpub.com/book/networking_and_servers/9781782167648/1/ch01lvl1sec14/file-integrity-monitoring-simple)  
<https://www.upguard.com/articles/tripwire-open-source-vs.-ossec-which-is-right-for-you#:~:text=Summary,bells%20and%20whistles%20are%20needed.>  
[https://subscription.packtpub.com/book/networking\\_and\\_servers/9781782167648/1/ch01lvl1sec11/writing-your-own-rules-simple](https://subscription.packtpub.com/book/networking_and_servers/9781782167648/1/ch01lvl1sec11/writing-your-own-rules-simple)