Project Report on

Effective Intrusion Detection System with OSSEC and Splunk

Submitted in partial fulfillment for the award of

Post Graduate Diploma in IT Infrastructure, Systems and Security

from **C-DAC, ACTS (Pune)**

Guided by:

Mr. Roshan Gami

Presented By :

Aakash Bhagat	230340123005
Arjun Gupta	230340123009
Saif Shaikh	230340123045
Sachin Mungulmure	230340123044
Shital Barade	230340123058

Centre of Development of Advanced Computing (C-DAC), Pune

CERTIFICATE

TO WHOMSOEVER IT MAY CONCERN

This is to certify that

Aakash Bhagat	230340123005
Arjun Gupta	230340123009
Saif Shaikh	230340123045
Sachin Mungulmure	230340123044
Shital Barade	230340123058

have successfully completed their project on

Effective Intrusion Detection System with OSSEC and Splunk

under the guidance of **Mr. Roshan Gami.**

Project Guide

Project Supervisor

ACKNOWLEDGEMENT

This is to acknowledge our indebtedness to our guide for his constant guidance and helpful suggestion for preparing this project "**Effective Intrusion Detection System with OSSEC and Splunk".**

Our deep gratitude towards him for inspiration, personal involvement, constructive criticism that he provided beyond more technical guidance during the course of this project. His shared enthusiasm taught us patience and his word of advice acted as morale booster. We are very thankful to our guide **Mr. Roshan Gami** for his inspiration.

Our most heartfelt thanks go to **Mr. Soham Yeolekar** (Course Coordinator, PG-DITISS) who gave all the required support and kind coordination to provide all the necessities like required hardware, internet facility and extra Lab hours to complete the project and throughout the course up to the last day here in C- DAC ACTS, Pune.

Sincerely,

Aakash Bhagat
Arjun Gupta
Saif Shaikh
Sachin Mungulmure
Shital Barade

TABLE OF CONTENTS

1.INTRODUCTION

When it comes to protecting and maintaining infrastructures such as servers, File Integrity Monitoring is a key. This solution validates the integrity of a given environment, namely, it checks to see whether the contents of your files have changed unexpectedly.

You can use File Integrity Monitoring to detect file changes in operating systems, web servers. It can even prove useful for monitoring file-based software solutions such as databases and configuration files.

Organizations that uses a file integrity monitoring solution are more likely to detect security breaches early on, giving them a better chance of staying online and deterring any major damage. For this reason, File Integrity Monitoring is primarily considered to be a security solution.

Changes to configurations, files and file attributes across the IT infrastructure are common but hidden within a large volume of daily changes can be the few that impact file or configuration integrity. These changes can also reduce securityposture and in some cases may be leading indicators of a breach in progress.Values monitored for unexpected changes to files or configuration items include:

- Credentials
- Privileges and Security Settings
- Content
- Core attributes and size
- Hash values
- Configuration values

1.1 OBJECTIVE

This project is developed as a monitoring tool for the servers or the infrastructure to maintain the Confidentiality, Integrity and Availability of the data.

As we are very much aware with how a company's server and infrastructure are important to keep safe and secure from intruding activities. The integrity of the data should be maintaining all the time. Therefore, it is necessary to monitor them continuously to catch those activities. Our project which is **"Effective Intrusion Detection System with OSSEC and Splunk"** will generate alert logs in the system. Those alert logs are carried by the Splunk Forwarder and makes it available to Splunk Indexer. The Splunk will show the forwarded logs in the structured manner. The structured logs will be monitored on the Splunk Enterprise's Dashboard. This process will help to tackle with the real time incidents.

1.1 SCOPE

“Effective Intrusion Detection System with OSSEC and Splunk” helps to secure the servers of the infrastructure which has all the important data and processes are going on it. Provides the compliance security by maintaining the integrity of the data which will maintain the performance of the infrastructure smooth and securely working. In future we will try to upgrade the system with the IDS technology which will also monitor the attacks.

2.1 What is File Integrity Monitoring?

File integrity monitoring (FIM) refers to an IT security process and technology that tests and checks operating system (OS), database, and application software files to determine whether or not they have been tampered with or corrupted. FIM, which is a type of change auditing, verifies and validates these files by comparing the latest versions of them to a known, trusted "baseline." If FIM detects that files have been altered, updated, or compromised, FIM can generatealerts to ensure further investigation, and if necessary, remediation, takes place. File integrity monitoring encompasses both reactive (forensic) auditing as well as proactive, rules-based active monitoring.

File integrity monitoring was invented in part by Tripwire founder Gene Kim and went on to become a security control that many organizations build their cybersecurity programs around. The term "file integrity monitoring" was widely popularized by the PCI standard.

FIM is a technology that monitors and detects changes in files that may indicate a cyberattack. Unfortunately, for many organizations, FIM mostly means noise: too many changes, no context around these changes, and very little insight into whether a change actually poses a risk. FIM is a critical security control, but it must provide sufficient insight and actionable intelligence.

Otherwise known as change monitoring, file integrity monitoring involves examining files to see if and when they change, how they change, who changed them, and what can be done to restore those files if those modifications are unauthorized.

Companies can leverage the control to supervise static files for suspicious modifications such as adjustments to their IP stack and email client configuration. As such, FIM is useful for detecting malware as well as achieving compliance with regulations like the Payment Card Industry Data Security Standard (PCI DSS).

2.2 How File Integrity Monitoring works?

There are five steps to file integrity monitoring:

1. **Setting a policy:** FIM begins when an organization defines a relevant policy. This step involves identifying which files on which computers the company needs to monitor.
2. **Establishing a baseline for files:** Before they can actively monitor files for changes, organizations need a reference point against which they can detect alterations. Companies should, therefore, document a baseline, or a known good state for files that will fall under their FIM policy. This standard should take into account the version, creation date, modification date, and other data that can help IT professionals provide assurance that the file is legitimate.
3. **Monitoring changes:** With a detailed baseline, enterprises can proceed to monitor all designated files for changes. They can augment their monitoring processes by auto-promoting expected changes, thereby minimizing false positives.
4. **Sending an alert:** If their file integrity monitoring solution detects an unauthorized change, those responsible for the process should send out an alert to the relevant personnel who can fix the issue.
5. **Reporting results:** Sometimes companies use FIM tools for ensuring PCI DSS compliance. In that event, organizations might need to generate reports for audits in order to substantiate the deployment of their file integrity monitoring assessor.

2.3 Importance of FIM

FIM software will scan, analyze, and report on unexpected changes to important files in an IT environment. In so doing, file integrity monitoring provides a critical layer of file, data, and application security, while also aiding in the acceleration of incident response. The four primary file integrity monitoring use cases are:

1. **Detecting Illicit Activity**

   If a cyber attacker intrudes upon your IT environment, you will need to know if they have tried to alter any files that are critical to your operating systems or applications. Even if log files and other detection systems are avoided or altered, FIM can still detect changesto important parts of your IT ecosystem. With FIM in place, you can monitor and protect the security of your files, applications, operating systems, and data.

2. **Pinpointing Unintended Changes**

   Often, file changes are made inadvertently by an admin or another employee. Sometimes the ramifications of these changes may be small and go overlooked. Other times, they can create security backdoors, or result in dysfunction with business operations or continuity. File integrity monitoring simplifies forensics by helping you zero in on the errant change, so you can roll it back or take other remediation.

3. **Verifying Update Status and Monitoring System Health**

   You can check if files have been patched to the latest version by scanning installed versions across multiple locations and machines with the post-patch checksum.

4. **Meeting Compliance Mandates**

   The ability to audit changes, and to monitor and report certain types of activity is required for compliance with regulatory mandates such as GLBA, SOX, HIPAA and PCI DSS.

3.Workflow Diagram

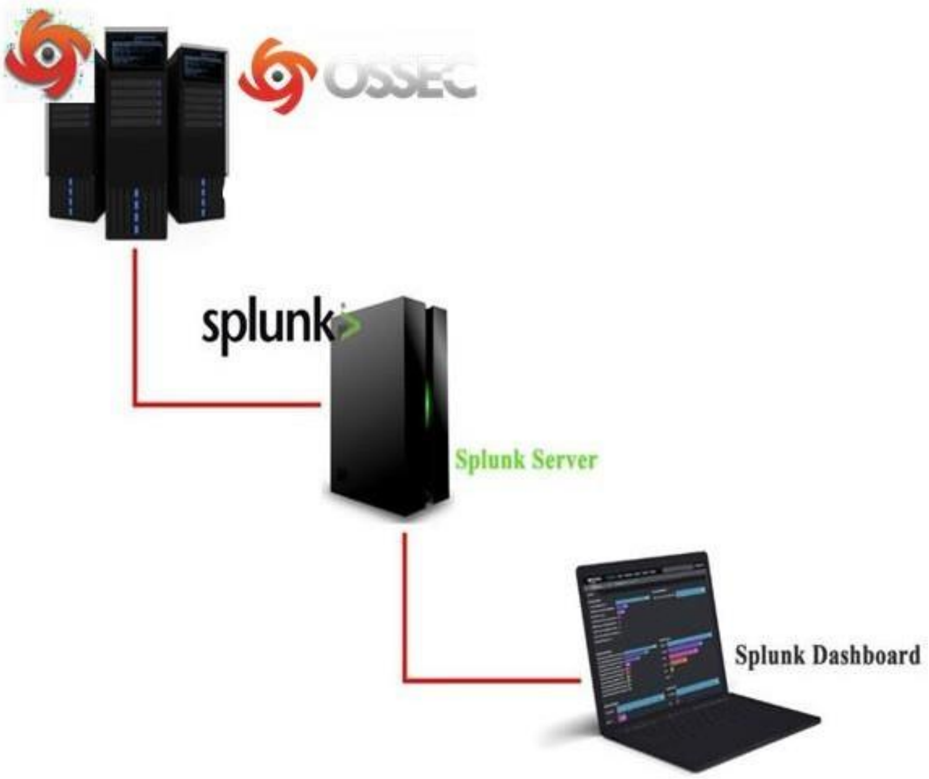


Fig 1: Host-Based Intrusion Detection System

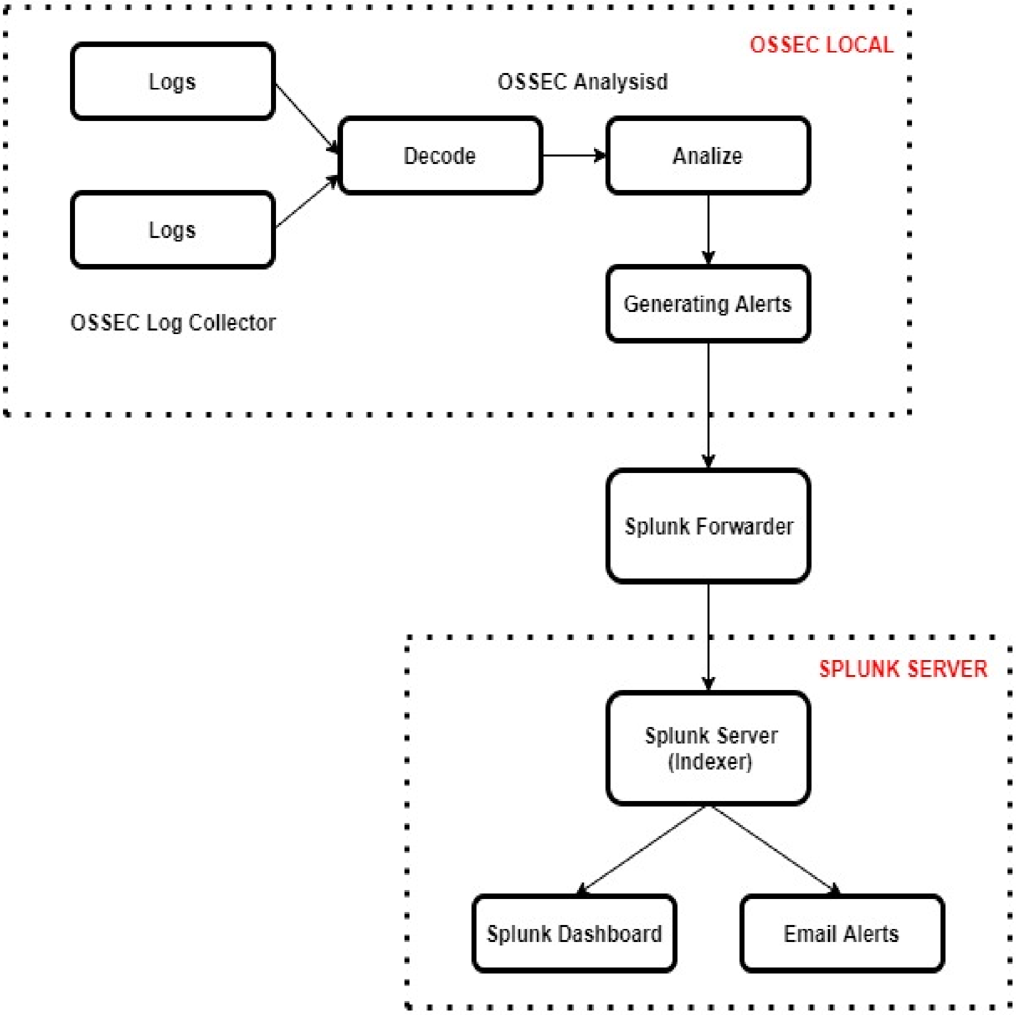


Fig2: Block Diagram

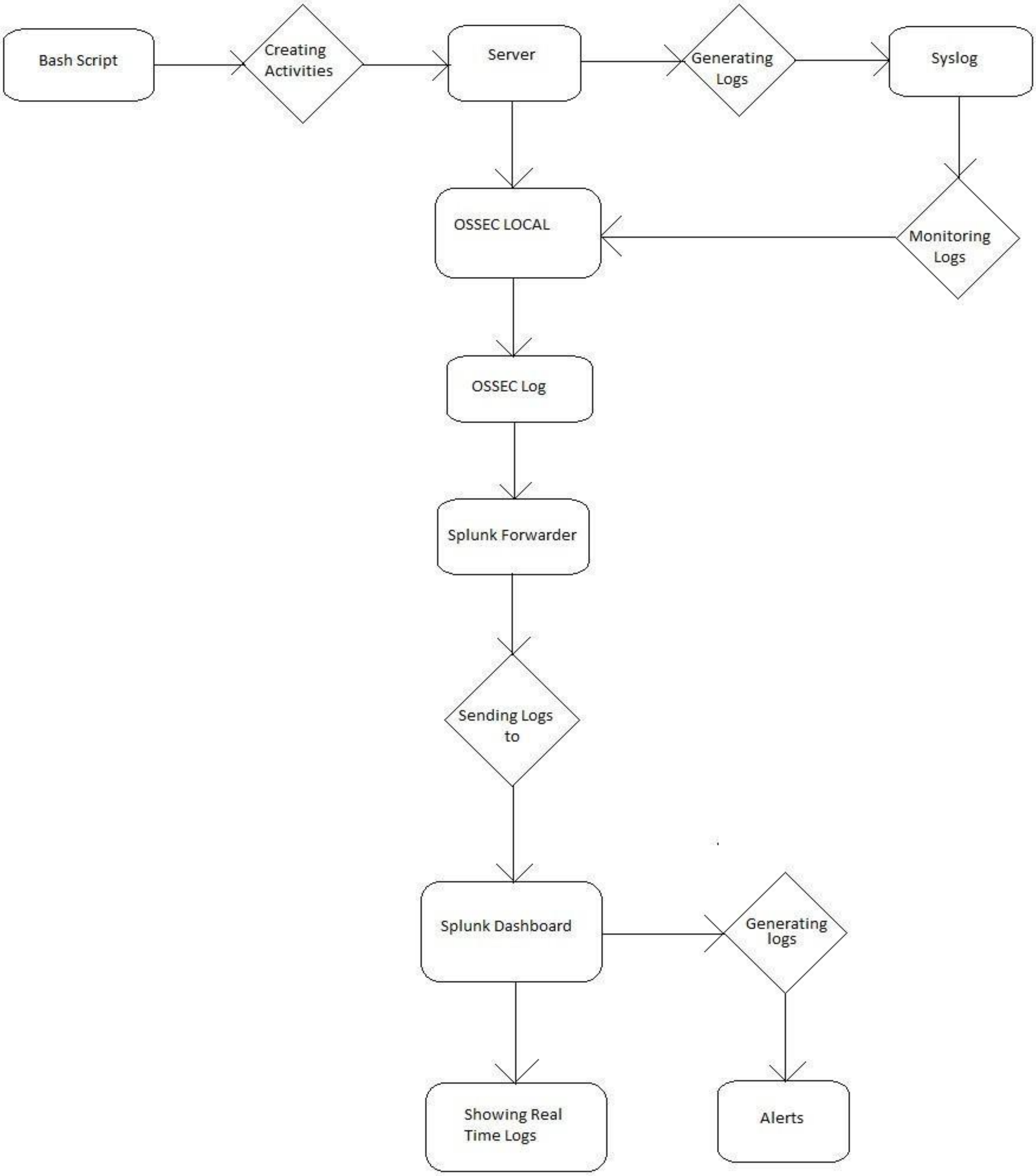


Fig 3: Flow Chart

4.1 What is OSSEC?

OSSEC is an Open Source Host-based Intrusion Detection System. It performs log analysis, integrity checking, Windows registry monitoring, Unix-based rootkit detection, real-time alerting and active.

Features:

- Log analysis
- File Integrity checking (Unix and Windows)
- Registry Integrity checking (Windows)
- Host-based anomaly detection (for Unix-rootkit detection)
- Active response
- Real-time log alert

OSSEC helps organizations meet specific compliance requirements such as PCI DSS. It detects and alerts on unauthorized file system modification and malicious behavior that could make you non-compliant.

Why OSSEC?

- Solves a real problem with log analysis
- Free
- Easy to install (sort of)
- Easy to customize
- Scalable (client/server architecture)
- Multi-platform (Windows, Solaris, Linux, etc)
- Secure by default
- Comes with decoders/rules out of the box. Unix Pam, sshd (OpenSSH), Solaris telnetd, Samba, Su, Sudo, Proftpd, Pure-ftpd, vsftpd, Microsoft FTPserver, Solaris ftpd, Imapd, Postfix, Sendmail, vpopmail, Microsoft Exchange.Apache, IIS5, IIS6, Horde IMP, Iptables, IPF. PF, Netscreen, CiscoPIX/ASA/FWSM, Snort, Cisco IOS, Nmap, Symantec AV, Arpwatch, Named,Squid, Windows event logs, etc.

Understanding OSSEC:

There are 4 modes OSSEC can be Configured which are listed below :

- **Server: -** Server mode is the central piece of OSSEC deployment.
    - It helps to administrative of large number of agents.
- **Agent: -** In agent mode, OSSEC agent send events, audit entries and logs to Server.
- **Local Mode: -** Local mode is similar as server and agent installation, except that the server has been configured to listen for communication from the agents.
- **Hybrid: -** In this mode, OSSEC act same as server and client.

4.2 OSSEC Installation

You can install OSSEC by compiling it from source, or by using the package manager. Since there's no installable package in the official CentOS/Ubuntu repository, you'll have to add the project's official CentOS/Ubuntu repository to the system. The whole OSSEC Installation will be on FIM server.

1. Installing the prerequisites:

```
sudo apt-get install build-essential make zliblg-dev libpcre2-dev
libevent-dev libssl-dev
```

2. Download the latest version of the OSSEC from GitHub repository with the following command:

```
wget https://github.com/ossec/ossec-hids/archive/3.7.0.tar.gz
```

3. Extract the tar file:

```
tar -zxvf 3.7.0.tar.gz
```

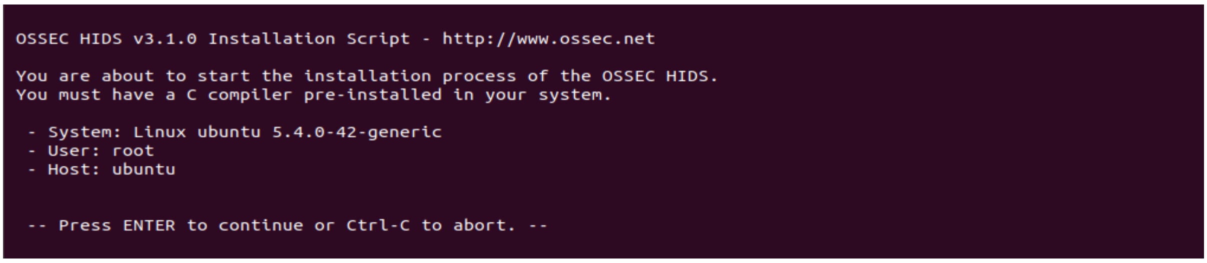
4. Update your systems Packages:

```
sudo apt update
```

5. Install OSSEC:

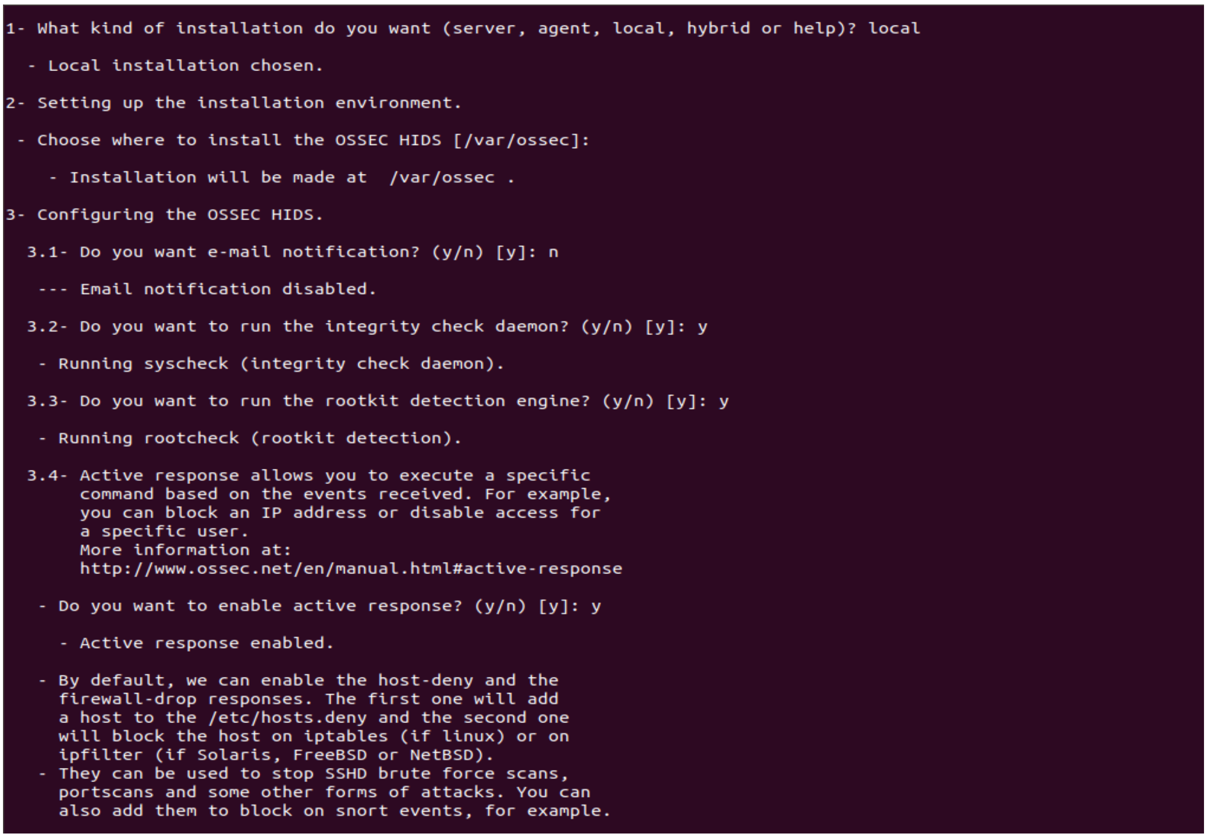
```
cd ossec-hids-3.7.0
sh install.sh
```

1.



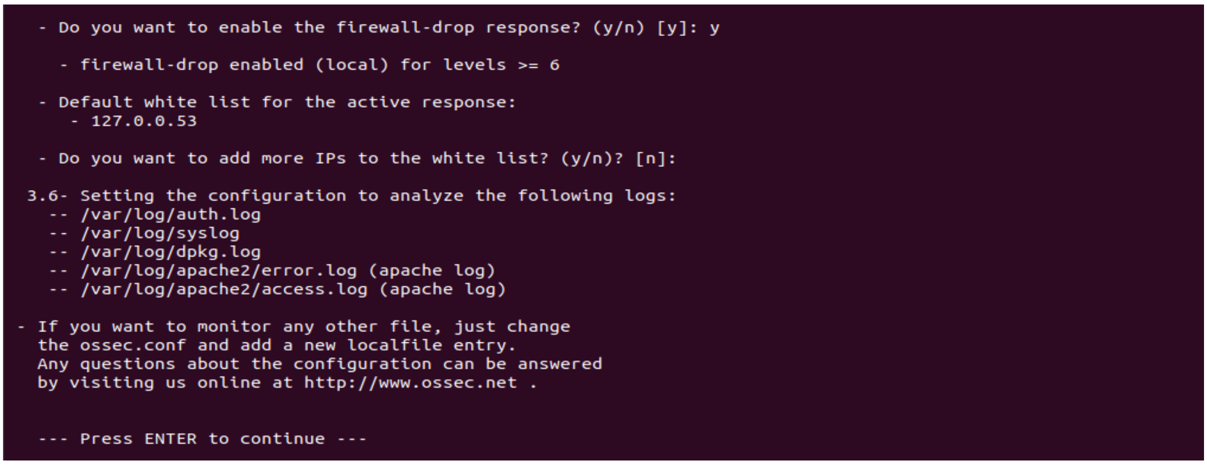
```
OSSEC HIDS v3.1.0 Installation Script - http://www.ossec.net

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 ubuntu 5.4.0-42-generic
 - User: root
 - Host: ubuntu


 -- Press ENTER to continue or Ctrl-C to abort. --
```

2.



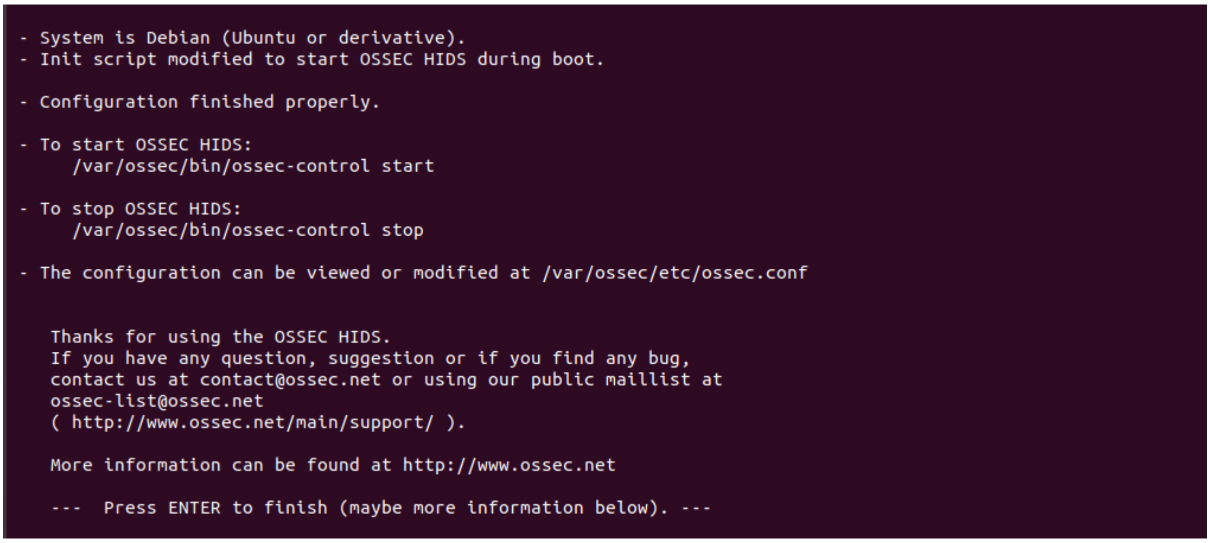
```
1- What kind of installation do you want (server, agent, local, hybrid or help)? local

  - Local installation chosen.

2- Setting up the installation environment.

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

    - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

  3.1- Do you want e-mail notification? (y/n) [y]: n

   --- Email notification disabled.

  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]: y

     - Active response enabled.

   - By default, we can enable the host-deny and the
     firewall-drop responses. The first one will add
     a host to the /etc/hosts.deny and the second one
     will block the host on iptables (if linux) or on
     ipfilter (if Solaris, FreeBSD or NetBSD).
   - They can be used to stop SSHD brute force scans,
     portscans and some other forms of attacks. You can
     also add them to block on snort events, for example.
```

3.



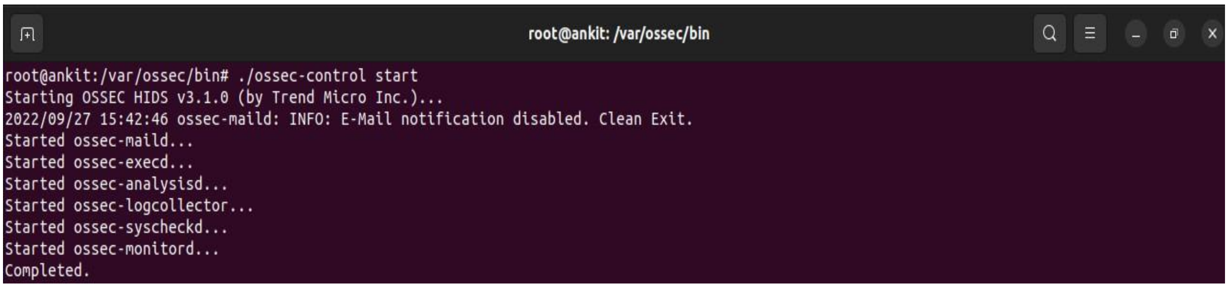
```
   - Do you want to enable the firewall-drop response? (y/n) [y]: y

     - firewall-drop enabled (local) for levels >= 6

   - Default white list for the active response:
      - 127.0.0.53

   - Do you want to add more IPs to the white list? (y/n)? [n]:

  3.6- Setting the configuration to analyze the following logs:
    -- /var/log/auth.log
    -- /var/log/syslog
    -- /var/log/dpkg.log
    -- /var/log/apache2/error.log (apache log)
    -- /var/log/apache2/access.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 ---
```

4.



```
- 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 contact@ossec.net or using our public maillist at
   ossec-list@ossec.net
   ( http://www.ossec.net/main/support/ ).

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

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

5.



```
root@ankit:/var/ossec/bin# ./ossec-control start
Starting OSSEC HIDS v3.1.0 (by Trend Micro Inc.)...
2022/09/27 15:42:46 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
```

5.1 What is Splunk?

Splunk is an advanced, scalable, and effective technology that indexes and searches log files stored in a system. It analyzes the machine-generated data to provide operational intelligence. The main advantage of using Splunk is that it does not need any database to store its data, as it extensively makes use of its indexes to store the data.

Splunk is a software mainly used for searching, monitoring, and examining machine-generated Big Data through a web-style interface. Splunk performs capturing, indexing, and correlating the real-time data in a searchable container from which it can produce graphs, reports, alerts, dashboards, and visualizations. It aims to build machine-generated data available over an organization and is able to recognize data patterns, produce metrics, diagnose problems, and grant intelligence for business operation purposes. Splunk is a technology used for application management, security, and compliance, as well as business and web analytics.

With the help of Splunk software, searching for a particular data in a bunch of complex data is easy. As you might know, in the log files, figuring out which configuration is currently running is challenging. To make this easier, there is a tool in Splunk software which helps the user detect the configuration file problems and see the current configurations that are being utilized.

Let us discuss Splunk with an example. Suppose, you are a System Administrator and you have to find out what’s wrong in the machine/systemyou are working with. Take a look at the machine-generated data to get an idea of how it looks like.

It would take hours to find out what’s wrong with your system.

Now, this is where Splunk comes into the picture. It will do all the hefty tasks for you, i.e., processing of the whole data which was generated by your machine/system, and after obtaining the relevant data, it will be a lot easier to locate the problems.

5.2 What is Splunk Architecture?

The terms that are related to the Splunk architecture:

- **Universal Forwarder (UF):** It is a lightweight element that assists in pushing the data to the heavy Splunk forwarder. The principal task of this element is to just forward the log data from the server. You can easily install Universal Forward at the client-side or on the application side.
- **Load Balancer (LB):** In computing terms, Load balancing enhances the distribution of workloads over multiple computing resources. A load balancer is an element that distributes the network or the application traffic over a cluster of servers.
- **Heavy Forwarder (HF):** It is recognized to be the heavy element. This Splunk component enables you to filter the data. For instance, it will help in accumulating only the error logs.
- **Indexer:** The chief task of an indexer is to store and index the filtered data. It helps in improving Splunk's performance. By default, Splunk automatically implements the indexing like hosts, sources, date, and time.
- **Search Head (SH):** It is simply a Splunk instance that helps in distributing the searches to the other indexers, and it normally doesn't have any instance of its own. It is essentially used to achieve intelligence and perform reporting.
- **Deployment Server (DS):** It helps in deploying the configuration like updating the UF (Universal Forwarder) configuration file. You can use a DS to share data between the components.
- **License Master (LM):** A license slave is a Splunk Enterprise state which is controlled by a License Master. If you have a single Splunk Enterprise instance, it assists as its License Manager (once you have installed an Enterprise license on it). The license is based on quantity and usage. For example, for 50 GB per day usage, Splunk examines the licensing details daily.

5.3 Splunk Forwarder Installation

Their will Splunk server and a Splunk forwarder.

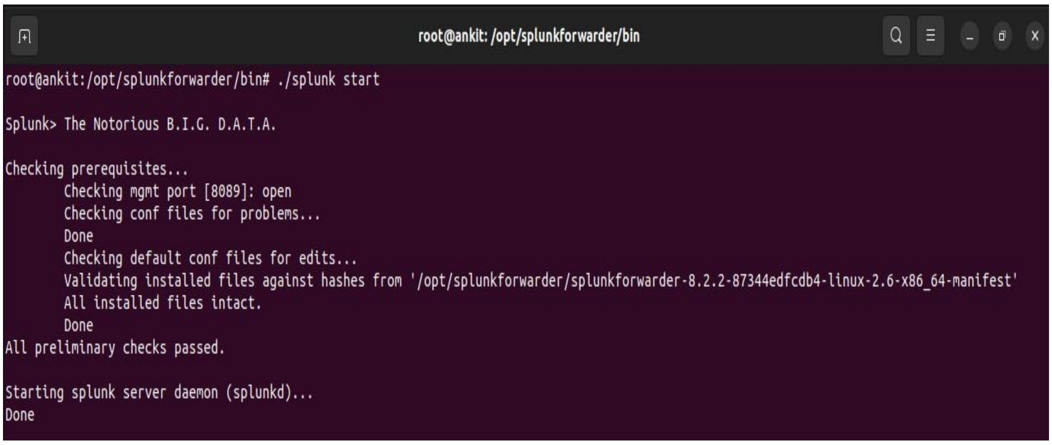
1. Installation on of Splunk Forwarder on FIM server(Client/Host Machine).
   a. Download or wget the splunk forwarder package on server.
   b.
   ```
   wget -O splunkforwarder-8.2.2.1-ae6821b7c64b-Linux-x86_64.tgz 'https://d7wz6hmoaavd0.cloudfront.net/products/universalforwarder/releases/8.2.2.1/linux/splunkforwarder-8.2.2.1-ae6821b7c64b-Linux-x86_64.tgz'
   ```

   c. Go to the directory of the splunk forwarder.

   ```
   cd /opt/splunkforwarder/bin/
   ```

   d. Start the splunk and accept the licence.

   ```
   ./splunk start --accept-licence
   ```



root@ankit: /opt/splunkforwarder/bin

```
root@ankit:/opt/splunkforwarder/bin# ./splunk start

Splunk> The Notorious B.I.G. D.A.T.A.

Checking prerequisites...
        Checking mgmt port [8089]: open
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-8.2.2-87344edfcdb4-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
```

2. Installation of Splunk in Splunk server.
    a. Download or wget the splunk package on server.

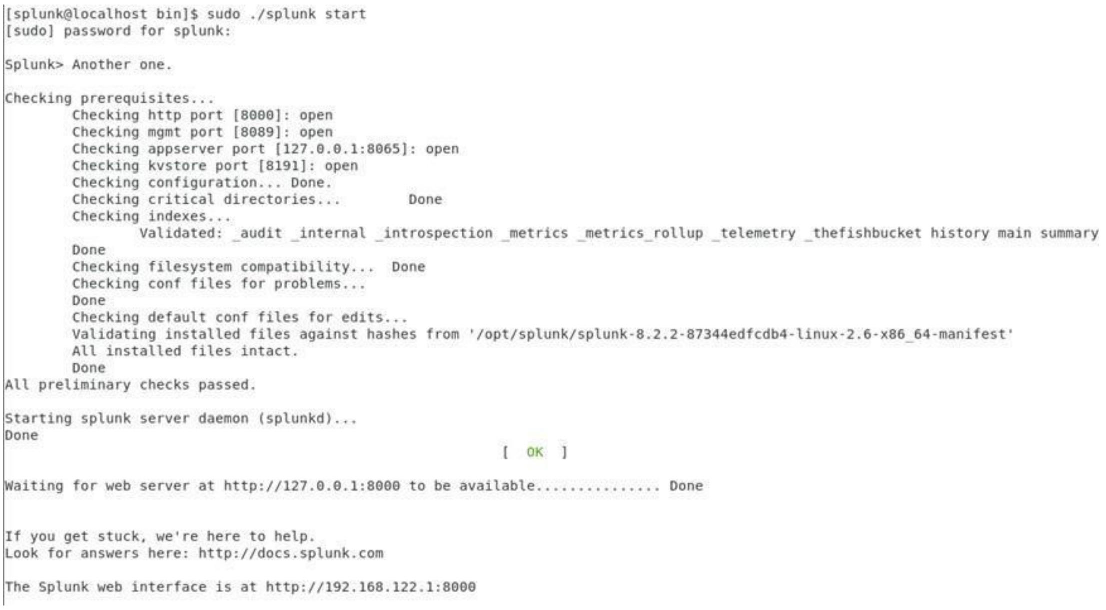
```
wget -O splunk-8.2.2.1-ae6821b7c64b-Linux-x86_64.tgz
'https://d7wz6hmoaavd0.cloudfront.net/products/splunk/rel
eases/8.2.2.1/linux/splunk-8.2.2.1-ae6821b7c64b-Linux- x86_64.tgz'
```

    b. Go to the directory of the splunk.

```
cd /opt/splunk/bin/
```

    c. Start the splunk and accept the licence.

```
./splunk start --accept-licence
```



```
[splunk@localhost bin]$ sudo ./splunk start
[sudo] password for splunk:

Splunk> Another one.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-8.2.2-87344edfcdb4-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
                                                           [  OK  ]

Waiting for web server at http://127.0.0.1:8000 to be available............... Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://192.168.122.1:8000
```

6.1 Hardware and Software Requirements

1. 8 GB RAM
2. VMware Workstation 16.1.2
3. Ubuntu 18.04.5
4. OSSEC 3.1.0
5. Splunk

6.3 Configuration of Splunk

On FIM serever:

1. We have to first forward the logs using universal splunk forwarder to the splunk server.

   ```
   ./splunk add forward-server 192.168.150.150:9997
   ```

   Where, 9997 is the default listening port of splunk.

2. Then we have to add the monitoring file to the splunk server which you want to monitor.

   ```
   ./splunk add monitor /var/ossec/logs/alerts/alerts.log
   ```

Now, we have to make sure that Splunk server also listen to 9997.

On the Splunk Server:

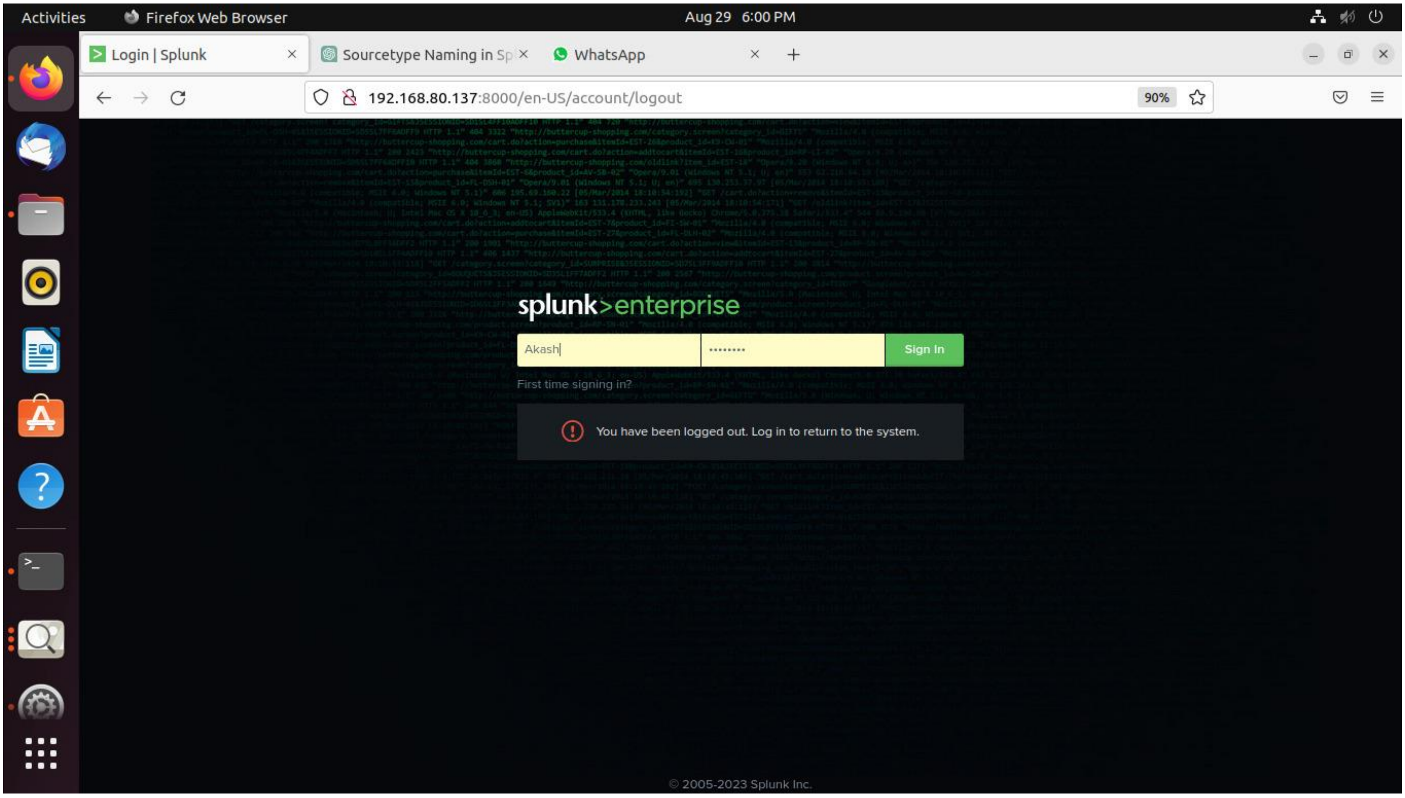
Add a listening port to the splunk serever.

```
./splunk enable listen 9997
```

6.4 Configuration of Splunk

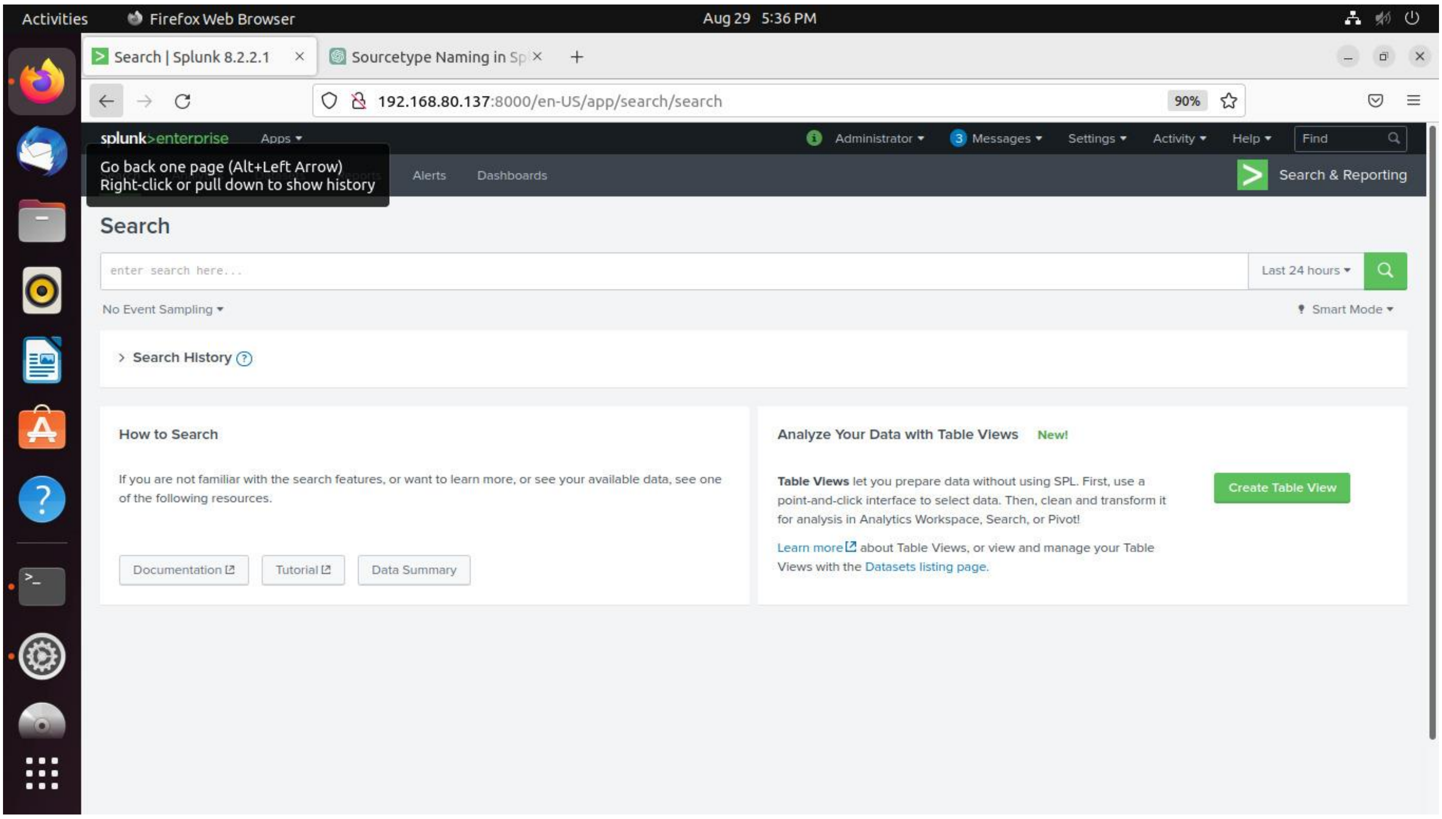
After getting the logs on the Splunk server. We will set up the splunk dashboard for better visualization of the events which are generating.

1. **Open the browser and type the splunk server's ip in the URL following by the port number.**



You have been logged out. Log in to return to the system.

2. **After login you will get the home page of the splunk dashboard.**



Go back one page (Alt+Left Arrow)
Right-click or pull down to show history

How to Search

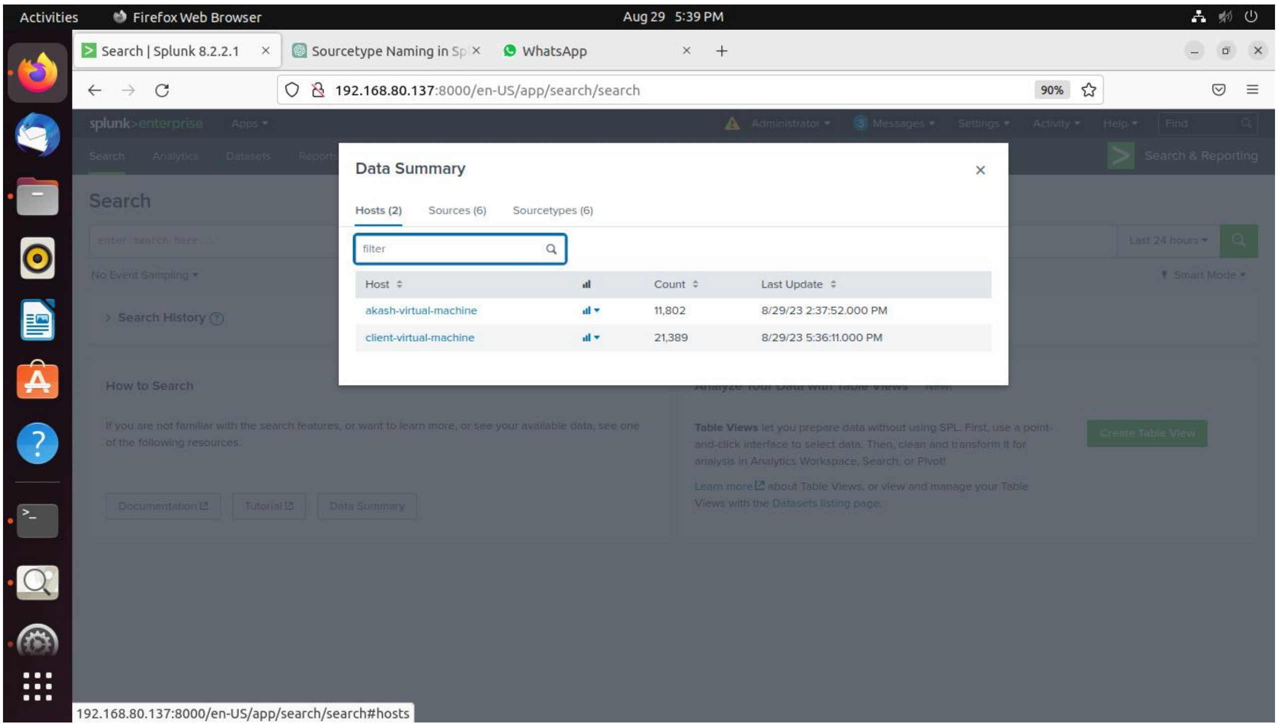
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Analyze Your Data with Table Views New!

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

3. Click on the Data Summary option.



Data Summary

Hosts (2) | Sources (6) | Sourcetypes (6)

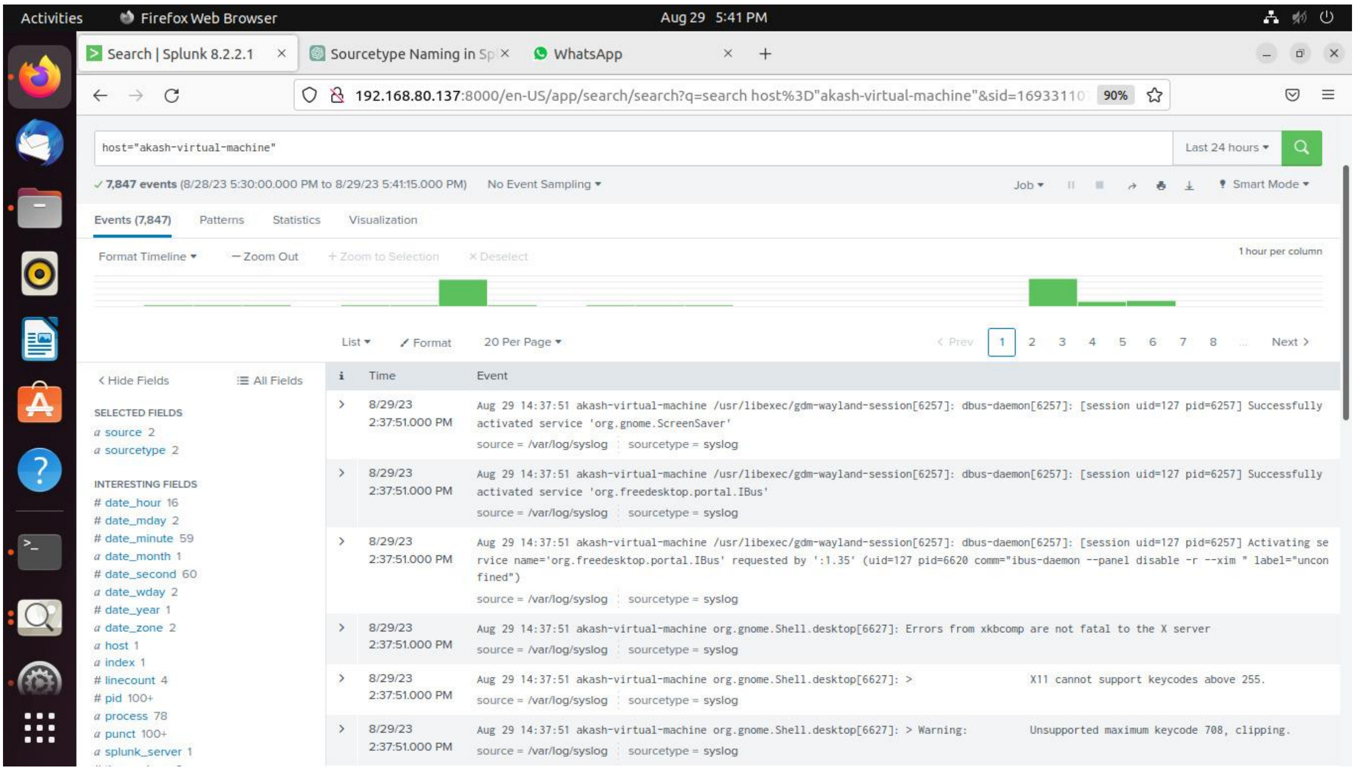
Host		Count	Last Update
akash-virtual-machine		11,802	8/29/23 2:37:52.000 PM
client-virtual-machine		21,389	8/29/23 5:36:11.000 PM

192.168.80.137:8000/en-US/app/search/search#hosts

4. You will see that logs are coming to the dashboard.

5. Fire the proper queries in the search bar to get the log.

…



192.168.80.137:8000/en-US/app/search/search?q=search host%3D"akash-virtual-machine"&sid=1693311

```
host="akash-virtual-machine"
```

✓ 7,847 events (8/28/23 5:30:00.000 PM to 8/29/23 5:41:15.000 PM)   No Event Sampling

Events (7,847) | Patterns | Statistics | Visualization

SELECTED FIELDS
- a source 2
- a sourcetype 2

INTERESTING FIELDS
- # date_hour 16
- # date_mday 2
- # date_minute 59
- a date_month 1
- # date_second 60
- a date_wday 2
- # date_year 1
- a date_zone 2
- a host 1
- a index 1
- # linecount 4
- # pid 100+
- a process 78
- a punct 100+
- a splunk_server 1

Time	Event

8/29/23 2:37:51.000 PM	`Aug 29 14:37:51 akash-virtual-machine /usr/libexec/gdm-wayland-session[6257]: dbus-daemon[6257]: [session uid=127 pid=6257] Successfully activated service 'org.gnome.ScreenSaver'`
	source = /var/log/syslog sourcetype = syslog

8/29/23 2:37:51.000 PM	`Aug 29 14:37:51 akash-virtual-machine /usr/libexec/gdm-wayland-session[6257]: dbus-daemon[6257]: [session uid=127 pid=6257] Successfully activated service 'org.freedesktop.portal.IBus'`
	source = /var/log/syslog sourcetype = syslog

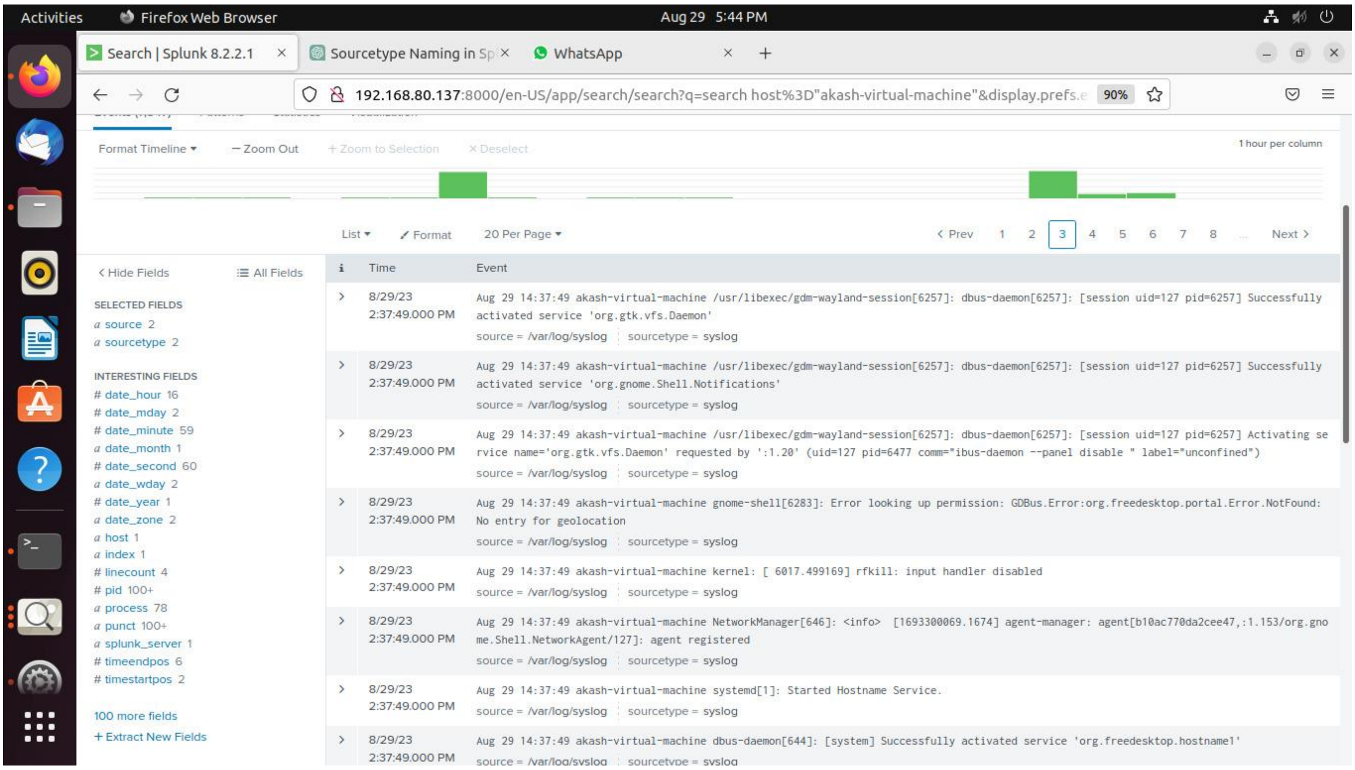
8/29/23 2:37:51.000 PM	`Aug 29 14:37:51 akash-virtual-machine /usr/libexec/gdm-wayland-session[6257]: dbus-daemon[6257]: [session uid=127 pid=6257] Activating service name='org.freedesktop.portal.IBus' requested by ':1.35' (uid=127 pid=6620 comm="ibus-daemon --panel disable -r --xim " label="unconfined")`
	source = /var/log/syslog sourcetype = syslog

8/29/23 2:37:51.000 PM	`Aug 29 14:37:51 akash-virtual-machine org.gnome.Shell.desktop[6627]: Errors from xkbcomp are not fatal to the X server`
	source = /var/log/syslog sourcetype = syslog

8/29/23 2:37:51.000 PM	`Aug 29 14:37:51 akash-virtual-machine org.gnome.Shell.desktop[6627]: >                   X11 cannot support keycodes above 255.`
	source = /var/log/syslog sourcetype = syslog

8/29/23 2:37:51.000 PM	`Aug 29 14:37:51 akash-virtual-machine org.gnome.Shell.desktop[6627]: > Warning:          Unsupported maximum keycode 708, clipping.`
	source = /var/log/syslog sourcetype = syslog

6. We have also created the Splunk dashboard where we are getting alerts, statistics of events and Realtime logs.



SELECTED FIELDS

- a source 2
- a sourcetype 2

INTERESTING FIELDS

- # date_hour 16
- # date_mday 2
- # date_minute 59
- a date_month 1
- # date_second 60
- a date_wday 2
- # date_year 1
- a date_zone 2
- a host 1
- a index 1
- # linecount 4
- # pid 100+
- a process 78
- a punct 100+
- a splunk_server 1
- # timeendpos 6
- # timestartpos 2

100 more fields

+ Extract New Fields

i	Time	Event
›	8/29/23 2:37:49.000 PM	Aug 29 14:37:49 akash-virtual-machine /usr/libexec/gdm-wayland-session[6257]: dbus-daemon[6257]: [session uid=127 pid=6257] Successfully activated service 'org.gtk.vfs.Daemon' source = /var/log/syslog sourcetype = syslog
›	8/29/23 2:37:49.000 PM	Aug 29 14:37:49 akash-virtual-machine /usr/libexec/gdm-wayland-session[6257]: dbus-daemon[6257]: [session uid=127 pid=6257] Successfully activated service 'org.gnome.Shell.Notifications' source = /var/log/syslog sourcetype = syslog
›	8/29/23 2:37:49.000 PM	Aug 29 14:37:49 akash-virtual-machine /usr/libexec/gdm-wayland-session[6257]: dbus-daemon[6257]: [session uid=127 pid=6257] Activating service name='org.gtk.vfs.Daemon' requested by ':1.20' (uid=127 pid=6477 comm="ibus-daemon --panel disable " label="unconfined") source = /var/log/syslog sourcetype = syslog
›	8/29/23 2:37:49.000 PM	Aug 29 14:37:49 akash-virtual-machine gnome-shell[6283]: Error looking up permission: GDBus.Error:org.freedesktop.portal.Error.NotFound: No entry for geolocation source = /var/log/syslog sourcetype = syslog
›	8/29/23 2:37:49.000 PM	Aug 29 14:37:49 akash-virtual-machine kernel: [6017.499169] rfkill: input handler disabled source = /var/log/syslog sourcetype = syslog
›	8/29/23 2:37:49.000 PM	Aug 29 14:37:49 akash-virtual-machine NetworkManager[646]: <info> [1693300069.1674] agent-manager: agent[b10ac770da2cee47,:1.153/org.gnome.Shell.NetworkAgent/127]: agent registered source = /var/log/syslog sourcetype = syslog
›	8/29/23 2:37:49.000 PM	Aug 29 14:37:49 akash-virtual-machine systemd[1]: Started Hostname Service. source = /var/log/syslog sourcetype = syslog
›	8/29/23 2:37:49.000 PM	Aug 29 14:37:49 akash-virtual-machine dbus-daemon[644]: [system] Successfully activated service 'org.freedesktop.hostname1' source = /var/log/syslog sourcetype = syslog

7. Limitation and Future Scope

Limitation:

1. Real Time Incident Monitoring System can only detect the events generating according to the defined rules but cannot respond to it.
2. We cannot detect the malicious activity.

Future Scope:

1. We will add a mechanism which can also detect the malicious activities on based of their signature and hash code.
2. Automated response with attack learning technology.

8.Conclusion

OSSEC is a powerful tool, useful for running one-off and scheduled queries using a familiar SQL syntax. OSSEC is the OSSEC component for writing one-off queries, while OSSEC is for scheduling queries. To make sense of the results of scheduled queries, you need to ship them off to an external log analysis platform.

Splunk is the best way to represent those OSSEC logs at it provide many functionalities and a flexible environment to work.

9.References

1. https://www.ossec.net/docs/
2. https://docs.splunk.com/Documentation/Splunk
3. https://docs.splunk.com/Documentation/Forwarder/8.2.2/Forwarder/Aboutthe universal forwarder