**IBM Project**

**User Manual Report**

**On**

**Security Information and Event Management**

**(Splunk Enterprise)**

### Developed By: -

Priyansh Gupta (18162171005)

Jinal Kumari (18162171007)

Aradhya Chaurishiya(19162172001)

### Guided By:-

Mr. Ravindra Patel (Internal)

Mr. Ashwin Thandani (External)

### Splunk Enterprise User manual

### 1: Setup and install Splunk Enterprise.

### 2: Configure Splunk Enterprise to work on correct configured ports.

### 3: Start the Splunk GUI and explore the interface.

### 4: Setup and install Splunk forwarder on Kali client machine.

### 5: Setup and install Splunk forwarder on Ubuntu client machine.

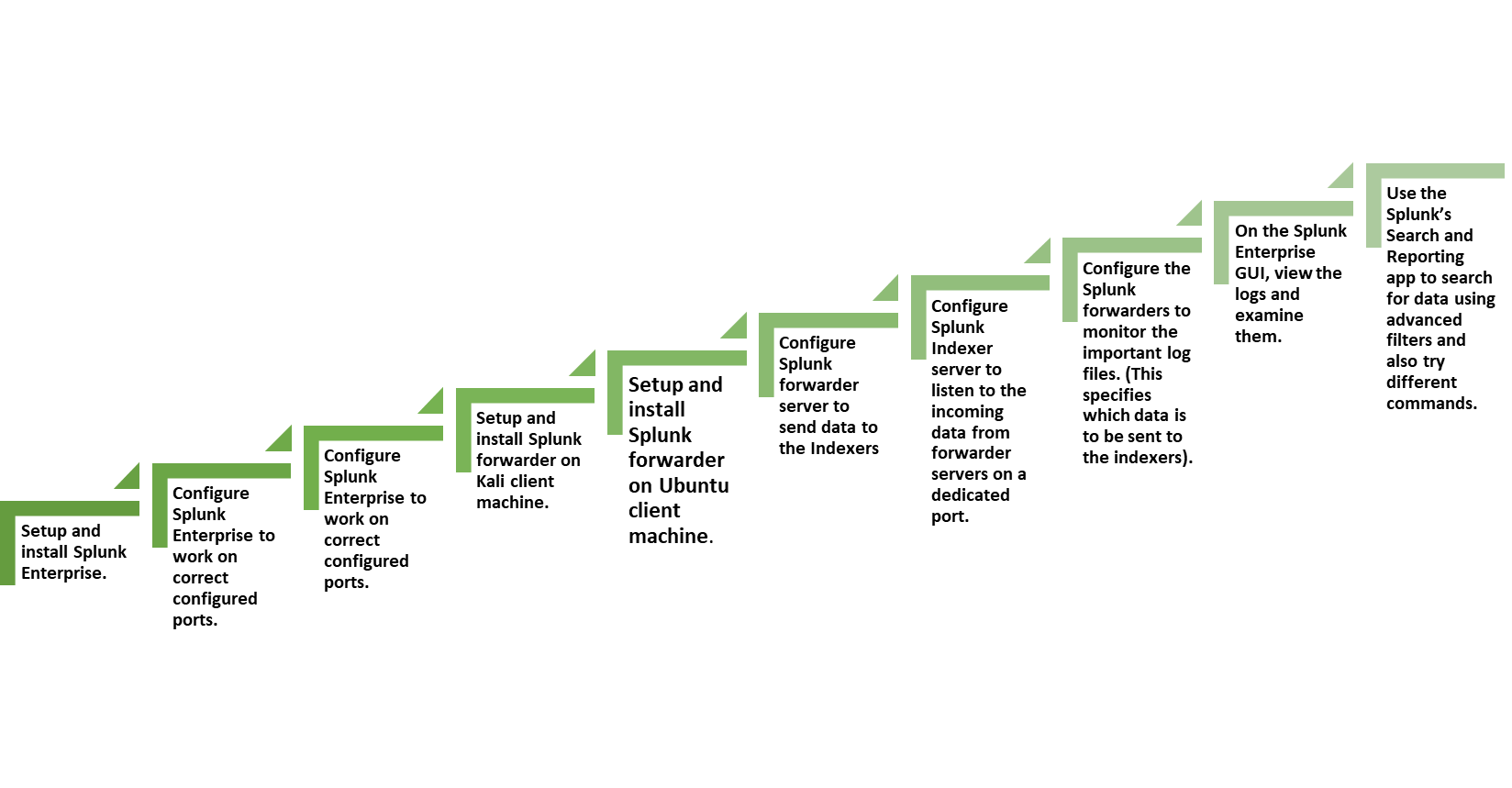
### 6: Configure Splunk forwarder server to send data to the Indexers

### 7: Configure Splunk Indexer server to listen to the incoming data from forwarder servers on a dedicated port.

**8:** Configure the Splunk forwarders to monitor the important log files. (This specifies which data is to be sent to the indexers).

**9:** On the Splunk Enterprise GUI, view the logs and examine them.

**10:** Use the Splunk’s Search and Reporting app to search for data using advanced filters and also try different commands.



**Splunk Download and Installation**

**Set up of Splunk Components and Log Generation**

1.Start the Splunk server using Splunk CLI

* Navigate to the path (cd E:/Splunk Enterprise > cd bin >)
* Start the splunk with command (splunk start)

2.Login with Splunk credentials

* admin/admin

Now, we want to collect data from remote sources in the network. Hence, we will have to setup a listener on a dedicated port to be able to collect different logs from different data sources.

3.Setup a listener to splunk by entering following command:

* Splunk enable 9997 –auth admin

**Now, to collect data from remote sources, we need to configure SPLUNK forwarder modules on either the machine themselves or within a forwarder server in the network.**

**Setting up SPLUNK forwarders:**

* Sudo tar –xvzf splunkforwader-8.2.4-87e2dda940d1-Linux-x86 64.tgz
* Sudo ./splunk start –accept-license
* Then enter the user name and password
* Sudo ./splunk add forward-server 192.168.137.19:9997

Note: The IP provided here to add forwarder server is the IP of our SPLUNK enterprise machine, where the SPLUNK indexer resides.

**Log collection**

**Once the forwarder server is configured, we will now specify the data source, I.e., which data to be sent to SPLUNK in order to monitor and analyze.**

**Navigate to the location of logs to be collected (ls /var/log )**

**on the path /opt/splunkforwarder/bin fir the following command :**

**sudo ./splunk add monitor /var/log/syslog –index main –sourcetype kali\_syslog (anyname)**

**The remote forwarder is now configured. It will send the specified data source to the SPLUNK indexer in real-time.**

**Similarly, doing the same for Ubuntu machine:**

Now, go to SPLUNK indexer server that is the web GUI for SPLUNK Enterprise and go to the app “Search and Reporting"

Wait for the SPLUNK indexer to receiver to receive data from the remote forwarders:

Click on Data summary and view different stats.

**Using SPLUNK search module to search and view the received data:**

* According to different hosts(source=”/var/log/syslog”)
* According to source type (sourcetype=”name”)
* According to event type (eventtype=”splunk log”)

SPLUNK supports more such advanced search commands.

**List of Major Activities**

### Hosting a webserver with bWAPP on kali machine

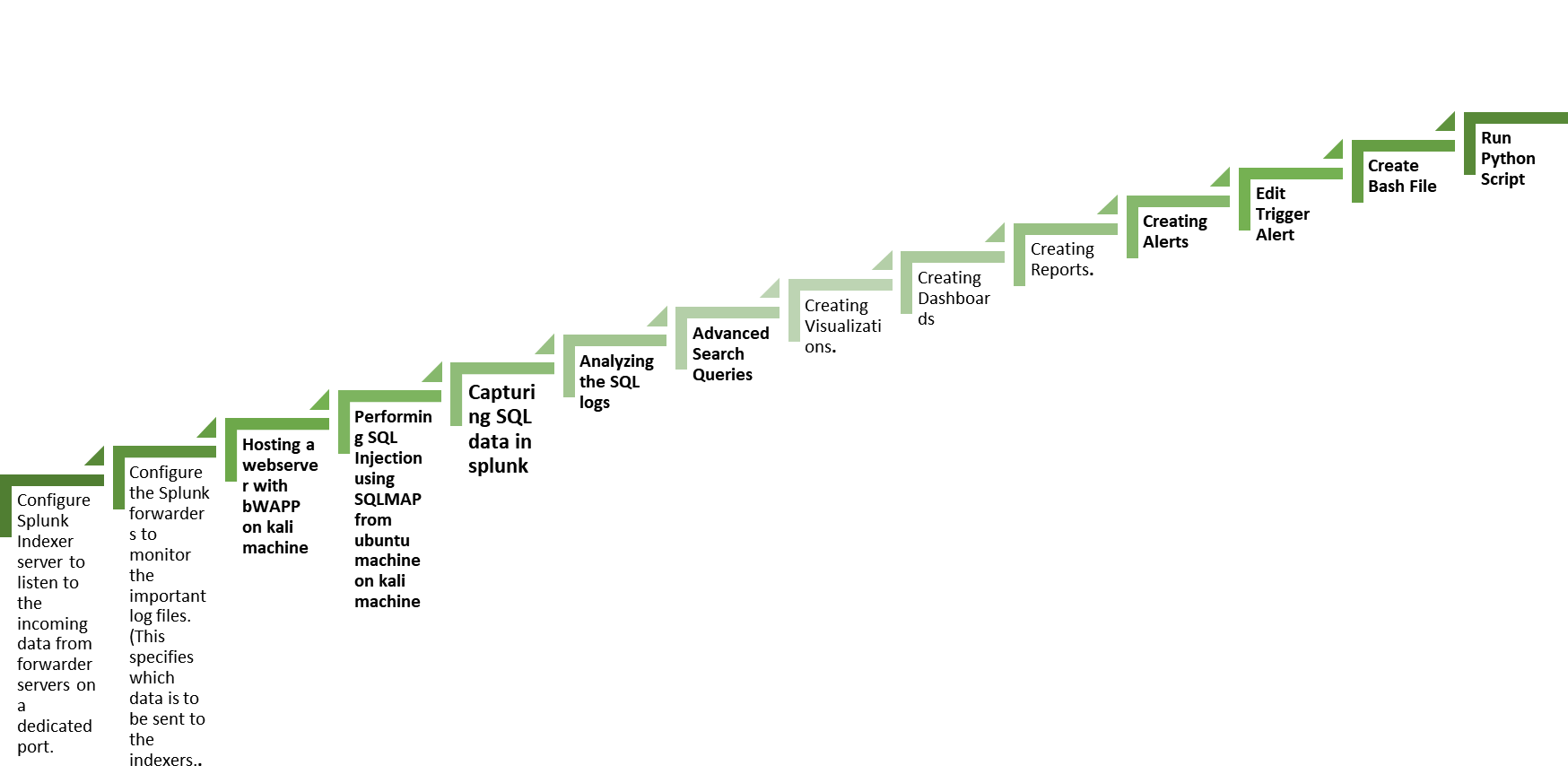
### Performing SQL Injection using SQLMAP from Ubuntu machine on kali machine

### Capturing SQL data in splunk

### Analysing the SQL logs

### Advanced search queries

* Creating visualizations
* Creating dashboards
* Creating reports
* Creating alert
* Edit Trigger Alert
* Create Bash File
* Run Python Script



**Hosting a webserver with bWAPP on kali machine:**

BWAPP is vulnerable web application for testing purpose , so we download and host the site on apache server.

Download the bwapp and navigate to the location

-Cd downloads

Now we unzip the zip file directly in apache web folder using following command

-sudo unzip –d /var/www/html bwapp.zip

Navigate to apache web folder

-cd /var/www/html

Then check the required bwapp files in the folder

-ls

Start the required services of apache and mysql server

-sudo service apache2 start

-sudo service mysql start

Configure the required mysql settings

-cd /bwapp/admin

**Performing SQL Injection using SQLMAP from ubuntu machine on kali machine:-**

sqlmap is an open-source entrance device that mechanizes the method involved with recognizing and taking advantage of SQL infusion imperfections and assuming control over data set servers.

•It incorporates a vigorous location motor, various expert elements for a definitive infiltration analyzer, and a wide scope of switches that range data set fingerprinting, information recovery from data sets, admittance to the fundamental record framework, and executing orders on the working framework through out-of-band associations.

**Capturing and Analyzing the SQL logs in splunk:-**

One of the numerous capacities of Splunk is constant observing of IT framework.

• In particular, Splunk can be utilized to screen SQL Server examples

• Splunk information authorities assemble the information from your information sources (logs, takes care of, measurements, documents, etc) across a scope of various stages, organizations, servers, applications, data sets and administrations. Anything information you want to gather, you'll probably find an application or extra that is preconfigured to gather it, or can arrange it physically.

• This capacity to file your information to such an extent that it very well may be rapidly and effectively looked is one of Splunk's assets; it is now and again alluded to as a web crawler for machine information and it can assist you with grasping the reason for issues, track accessibility, limit and execution, oversee setup and security of your server components, etc.

• Thus, for instance, you could utilize Splunk to do your framework observing, gathering measurements and log information for Windows servers (in addition to Linux, MacOS), as well as bunches, Docker compartments and the sky is the limit from there.

• You can then stretch out the observing to SQL Server, as well as other social information base and NoSQL information stores, utilizing the proper applications and additional items.

• You can run and save look against every one of the information it gathers, inspecting a blend of critical 'occasions' gathered over the equivalent time period, maybe corelating SQL Server execution measurements and log information with point by point foundation information. You assemble visual dashboards from the outcomes so you can detect patterns, relationships between's various measurements, bizarre way of behaving, and begin to figure out the significant reasons for execution issues, vacation, and other framework issues.

**Creating visualizations:-**

Whenever you make a dashboard board, you select how the board shows the consequences of a hunt or report with a representation.

• Perceptions are graphical portrayals of your information, like a diagram, table, or outline. You can change your perception determination with the Dashboard Board Proof reader.

• Add a perception to a pursuit and save as a dashboard board

• Change a perception on a dashboard board

• View, send out, investigate or revive a perception

1. Open your desired dashboard to alter for altering.

2. Click the Add Graph symbol .

3. Select an outline that you need to use to envision your information. For instance, select Line to add a line diagram.

4. Click Drop in the New Information Source board.

5. In the Arrangement board, click + Arrangement Essential Information Source.

6. Select one of the information sources that you made.

7. (Optional) Add a title and a portrayal for the representation.

8. (Optional) Alter the position and size of the representation.

9. (Optional) Change other perception settings.

10. Click Run and Save to run the pursuit and save the perception settings.

# **Create dashboards in Splunk :-**

There are multiple ways of making dashboards in Splunk.

• Make a dashboard from the Dashboards page, and afterward add boards or contributions to the dashboard.

• Use prebuilt boards to make a dashboard.

• Clone a current dashboard.

Make a dashboard from the Dashboards page, and afterward add boards from searches, reports, or prebuilt boards.

In your Splunk Light instance, select Dashboards in the menu bar.

1. Click Make New Dashboard.

2. (Optional) Enter a Title.

3. Enter an ID.

4. (Optional) Enter a Portrayal.

5. Click a consent level.

6. Click Make Dashboard.

7. On the Alter Dashboard page, add boards or contributions to your dashboard.

8. Click Save.

9. (Optional) To affirm that you have saved the dashboard, click Dashboards in the menu bar to see the dashboard recorded on the Dashboards page.

**Create a real-time alert with per-result triggering: -**

1. Navigate to the Pursuit page in the Hunt and Revealing application.

2. Create a pursuit.

3. Select Save As>Alert.

4. Enter a title and discretionary portrayal.

5. Specify consents.

6. Select the Continuous alarm type.

7. (Optional) Change the Terminates setting. This setting controls the life expectancy of set off alarm records, which show up on the Set off Cautions page.

8. Select the Per-Result trigger choice.

9. (Optional) Arrange a trigger choking period.

10. Select no less than one heinous act that happens when the alarm triggers.

11. Click Save.