IBM Project Report

On

Security Information and Event Management

Developed By: -
Priyansh Gupta (18162171005)
Jinal Kumari (18162171007)
Aradhya Chaurishiya(19162172001)

Guided By:-
Mr. Ravindra Patel (Internal)
Mr. Ashwin Thandani (External)

Submitted to

Department of Computer Science & Engineering
Institute of Computer Technology

Year: 2022

CERTIFICATE

This is to certify that the **IBM** Project work entitled **"Security Information and Event Management"** by Priyansh Gupta (18162171005), Jinal Kumari (18162171007) and Aradhya Chaurishiya(19162172001) of Ganpat University, towards the partial fulfillment of requirements of the degree of Bachelor of Technology – Computer Science and Engineering, carried out by them in the CSE(CS) Department. The results/findings contained in this Project have not been submitted in part or full to any other University / Institute for award of any other Degree/Diploma.

Name & Signature of Internal Guide

Name & Signature of Head

Place: ICT - GUNI

Date:

ACKNOWLEDGEMENT

IBM project is a golden opportunity for learning and self-development. I consider myself very lucky and honored to have so many wonderful people lead me through in completion of this project. First and foremost, I would like to thank Dr. Hemal Shah, Principal, ICT, and Prof. Dharmesh Darji, Head, ICT who gave us an opportunity to undertake this project. My grateful thanks to Mr. Ravindra Patel & Mr. Ashwin Thandani (Internal & External Guides) for their guidance in project work Setup enterprise mobility management to manage and secure devices which connect organizational networks, who despite being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where would have been without his/her help. CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

ABSTRACT

Security Information and Event Management (SIEM) systems have been generally sent as a useful asset to identify, and respond against digital assaults. SIEM arrangements have advanced to become complete frameworks that give a wide perceive ability to recognize areas of high dangers and proactively center around moderation systems targeting lessening expenses and time for occurrence reaction. At present, SIEM frameworks and related arrangements are gradually merging with enormous information examination devices. We overview the most generally utilized SIEMs with respect to their basic usefulness and give an investigation of outer variables influencing the SIEM scene in mid and long haul. A rundown of likely upgrades for the up and coming age of SIEMs is given as a feature of the audit of existing arrangements as well as an examination on their advantages and use in basic frameworks.

To accomplish an elevated degree of network protection mindfulness generally mid to enormous estimated organizations use Security Information and Event Management (SIEM) installed into a Security Tasks Center. These frameworks empower the concentrated assortment and examination of safety applicable data produced by a wide range of frameworks, to distinguish progressed dangers and to further develop response time if there should be an occurrence of an episode.

INDEX

CHAPTER: 1 INTRODUCTION

CHAPTER 1 INTRODUCTION

Security Information & Event Management

SIEM is advanced security data framework that examines security alarms and information created from gadgets on an organization progressively. Associations use SIEM instruments to distinguish security occurrences, log security information, oversee episode reaction, and create reports for consistence. The term SIEM was first utilized in 2005 by Imprint Nicolett and Amrit Williams. SIEM as an idea was proposed by them by consolidating the idea of safety data the board (SIM) and security occasion the executives (SEM).

Splunk:-

Splunk is an undeniable, flexible, and effective level that records and searches log logos set aside in the building. Research machine-generated data to provide useful information. The legal advantage of using Splunk is that it does not have to worry about any data source to store its data, as it usually uses its own records to store data.

Splunk is a device often used to view, monitor, and evaluate large-scale machine information by using web-based interaction. Splunk enables the acquisition, solicitation, and comparison of consistent data in an available manager where it can create drafts, reports, alerts, dashboards, and exposures. It hopes to make digitized data available through the organization and can detect data systems, generate estimates, investigate. With the help of Splunk programs, searching for specific data on more complex data is fundamental. As you may know, in log reports, finding out which configuration is right now works. To make this clearer, there is a breach of the Splunk process that helps the client by separating archive issues and identifying ongoing applications.

CHAPTER: 2 PROJECT SCOPE

CHAPTER 2 PROJECT SCOPE

SIEM is a product framework that gathers and totals information and occasions from different systems administration gadgets and assets across IT foundation. As of now, the SIEM market esteem is around $4.2 billion and is supposed to develop to $5.5 billion by 2025.

Decide your business-basic information sources

When you have a handle of the ideal task scope, you can then recognize log sources inside the extension to decide how to acquire the pertinent information required. For instance, firewalls, interruption identification frameworks, and antivirus programming act as prime information hotspots for SIEM security use cases. However, there are some more, including switches, web channels, area regulators, application servers, information bases, and other carefully associated resources. It is pivotal that you focus on the sources included to guarantee the SIEM gives the ideal information to help the chose use cases.

Distinguish the high need occasions and cautions

With regards to safeguarding an association against insider and outer dangers, security groups face a steadily developing rundown of safety occasions that should be dissected and followed up on. To get through the clamour, SIEM programming can be utilized to make occasions and information more sagacious. In any case, organizations should initially decide their high need occasions and how to get them from applications and gadgets inside the framework. Along these lines, security groups can utilize the SIEM to invest more energy on episodes and cautions that might be more basic to the business and its information.

Pinpoint your key achievement measurements

An effective SIEM execution lines up with your business objectives. Key achievement measurements not entirely settled before arrangement to guarantee greatest return for capital invested. For instance, decreasing information robbery or further developing how organizations identify expected breaks or insider dangers might be measurements to lay out. Organizations should figure out how achievement affects them and how SIEM security use cases can be utilized to accomplish it.

TOP 3 SIEM TOOLS IN INDUSTRY

1. Solar Winds

- Gives unified log assortment and standardization, mechanized danger recognition and reaction.
- It can perform progressed search and criminological examination.
- With occasion time recognition of dubious action, there will be quicker ID of dangers. Reaction is amazingly quick
- It has administrative consistence preparation. For this, it upholds HIPAA, PCI, DSS, SOX, DISA, STIG, and so on.
- Simple Establishment
- Maverick USB Information Misfortune and Robbery Insurance

Cons

- Needs support for observing public cloud administrations' IaaS or SaaS. Doesn't uphold custom report composing and customization of out-of-the-case consistence report formats. Coming up short on UEBA and security stage.

Decision:

- Solar winds upholds Windows, Linux, Macintosh, and Solaris. According to the surveys, Sun powered Breezes doesn't have a total security suite however it gives great elements and capacities to danger identification. It very well may be a decent answer for SMEs.

2. Splunk

- It can work with any machine information, regardless of whether it is from the cloud or on-premises.
- Robotized activities and work processes for fast and exact reaction.
- Utilizes progressed security examination, which incorporate both solo AI and client conduct abilities.
- It has the capacity of occasion sequencing.
- Fast identification of noxious dangers.
- Cautions the executives and hazard scores.

Cons

- Utilizes fundamental predefined connection rules for observing and revealing necessities. Response capacities are restricted to email warnings. Requires coordination with outsider applications for assignment and work process robotization.

Decision:

- All together, to give you noteworthy and prescient bits of knowledge, Splunk utilizes artificial intelligence and AI. Dashboards and perceptions are adjustable. According to the client audits, it is a costly instrument and subsequently it is best for the undertakings.

3. IBM QRadar

- Progressed rule connection motor and social profiling innovation.
- Adaptable and profoundly versatile stage with huge out-of-the-crate usefulness and presets for various use cases.
- QRadar permits you to focus on security cautions utilizing danger insight.
- Can pass judgment on the effect on an organization, in light of reproduced assaults
- Has a basic yet viable point of interaction

Cons:

- Needs incorporations into other Take off and SIEM stages
- Upgrades could be quicker

Decision:

- IBM Qradar offers various highlights for information assortment, log movement, network action, and resources. It offers help to IE, Firefox, and Chrome programs. According to the client surveys, it centers around basic episodes.

CHAPTER: 3 SOFTWARE AND HARDWARE REQUIREMENTS

CHAPTER 3 SOFTWARE AND HARDWARE REQUIREMENTS

Minimum Hardware Requirements for IBM

Splunk Components	Indexer	Search Head	Master Node	Deployment Server
RAM	4 GB	4 GB	4 GB	4 GB
CPU Core	16	16	8	8
Hard Disk	2000 GB	2000 GB	200 GB	200 GB

Table 3.1 Minimum Hardware Requirements

Minimum Software Requirements for IBM

Operating System	Linux/Window 64 bits
Programming language	Python
Other tools & tech	Splunk

Table 3.2 Minimum Software Requirements

CHAPTER: 4 PROCESS MODEL

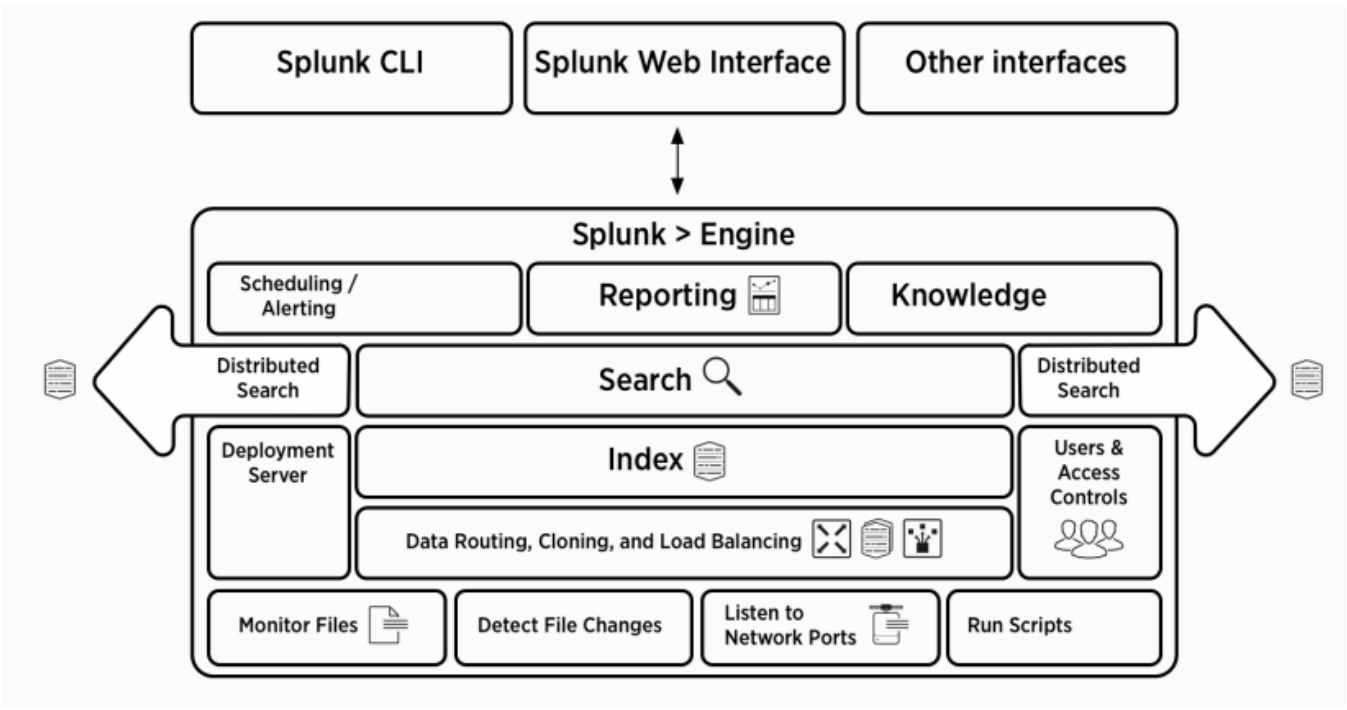


Figure 4.1 Process Model of Project

Splunk Components:-

By accepting that you are looking at the bottom of the image, you will capture the different data pipe sections where the Splunk parts fall under them.
There are **3 sections** of rules in Splunk:

- **Splunk Forwarder**, used to send data
- **Splunk Indexer**, used to sort and order data
- **Head Search,** is a GUI used for viewing, testing and disclosure

1. Splunk Forwarder

- Splunk Forwarder is the part you need to get social media logs. Accept, you want to assemble the logs on a remote machine, then, you can achieve that by using Splunk remote transmitters released from the Splunk special event.
- In all honesty, you can introduce a number of such transmitters to various machines, which will transfer log data to Splunk Indexer for you to take care of and collect. Imagine a situation where you want to make a continuous analysis of data. Splunk forwarders can be used with it as well. You can configure transmitters to send data consistently to Splunk indexes. You can present them in different formats and integrate the current data into different machines logically.
- To understand how similar data transfers happen, you can check out my blog on how Domino uses Splunk to get the best performance.
- Out of some common test devices, Splunk Forwarder consumes less than 1-2% CPU. You can successfully extend it to countless remote structures, and consolidate terabytes of data that has a significant impact on performance.
- From now on, let's list the different types of Splunk transmitters.
- All inclusive Forwarder - You can select a general forwarder if you have any desire to advance the crude information gathered at the source. It is a straightforward part which performs insignificant handling on the approaching information streams prior to sending them to an indexer.
- Information move is a significant issue with pretty much every device on the lookout. Since there is negligible handling on the information before it is sent, parcel of pointless information is likewise sent to the indexer bringing about execution overheads.
- Why go through the difficulty of moving every one of the information to the Indexers and afterward sift through just the pertinent information? Couldn't it be smarter to send the applicable information to the Indexer and save money on data transmission, time and cash as it were? This can be settled by utilizing Weighty forwarders which I have made sense of beneath.

Weighty Forwarder - You can utilize a Weighty forwarder and dispose of a portion of your concerns, since one degree of information handling occurs at the actual source prior to sending information to the indexer. Weighty Forwarder regularly does parsing and ordering at the source and furthermore cleverly courses the information to the Indexer saving money on data transfer capacity and extra room. So when a weighty forwarder parses the information, the indexer just has to deal with the ordering section

Universal Forwarder – You can choose a widespread forwarder if you have any desire to advance the crude information gathered at the source. It is a basic part which performs insignificant handling on the approaching information streams prior to sending them to an indexer.

Information move is a significant issue with pretty much every apparatus on the lookout. Since there is insignificant handling on the information before it is sent, parcel of superfluous information is additionally sent to the indexer bringing about execution overheads.

Why go through the difficulty of moving every one of the information to the Indexers and afterward sift through just the applicable information? Couldn't it be smarter to send the significant information to the

Indexer and save money on data transmission, time and cash as it were? This can be tackled by utilizing Weighty forwarders which I have made sense of beneath.

Heavy Forwarder – You can utilize a Weighty forwarder and kill a portion of your concerns, since one degree of information handling occurs at the actual source prior to sending information to the indexer. Weighty Forwarder commonly does parsing and ordering at the source and furthermore shrewdly courses the information to the Indexer saving money on data transfer capacity and extra room. So when a weighty forwarder parses the information, the indexer just has to deal with the ordering fragment

2. Splunk Indexer:-

Indexer is part of the Splunk that you should use to request and maintain data from the transmitter. The splunk case converts incoming data into events and saves it in documents so that search operations can be performed efficiently. When you receive data from the General Transfer, the index will first separate the data and then record it. Data analysis was performed to kill unfortunate data. However, if you get data from Weighty forwarder, the index will automatically list the data. As the Splunk model records your data, create separate archives. These records contain one of the following:

- Crude information in packed structure
- Lists that highlight crude information (record documents, likewise alluded to as tsidx records), in addition to some metadata records. These records dwell in sets of catalogs called containers. Allow me now to let you know how Ordering functions.

Splunk is processing future data to include faster applications and testing. Works on data in a variety of ways such as:

- Divide the distribution of data into individual, open events
- Making or seeing time stamps
- Extract fields such as host, source, and source type
- Performing client-defined tests on future data, for example, custom field recognition, encryption of sensitive data, creating new or modified keys, applying complex multi-line event rules, filtering disturbing events, and managing events on displayed documents or servers.

Another advantage of Splunk Indexer is data duplication. You do not have to worry about losing data when you consider how Splunk keeps various copies of recorded data. This integration is called file duplication or Indexer integration. This is achieved with the help of the Indexer package, which is a social networking event that is designed to speed up each other's data.

1. **Search Head**

The pursuit head is the part that permits you to work with Splunk. It provides clients with a graphical user interface for accomplishing various tasks. You can search and inquire about the information stored in the Indexer by entering search words, and you will get the expected result. The inquiry head can be used on its own or in conjunction with other Splunk components on a single server. There is no separate installation record for the search head; all you need to do is enable Splunk web administration on the Splunk server. A Splunk event can be used as both a pursuit head and a hunt peer. A devoted inquiry head is indeed a pursuit head who does nothing but look and does not order. During this time, an inquiry peer is in charge of ordering and distributing information

.Putting it All Together: Splunk Architecture

- Splunk accumulates logs by observing records, identifying document changes, tuning in on ports or running contents to gather log information - these are done by the Splunk forwarder.
- The ordering component, made out of at least one indexers, processes the information, or may get the information pre-handled by the forwarders
- The arrangement server oversees indexers and search heads, setup and strategies across the whole Splunk organization.
- Client access and controls are applied at the indexer level - every indexer can be utilized for an alternate information store, which might have different client authorizations.
- The hunt head is utilized to give on-request search usefulness, and furthermore drives planned look through started via programmed reports.
- The client can characterize Planning, Announcing and Information objects to plan look and make cautions.
- Information can be gotten to from the UI, the Splunk CLI, or APIs incorporating with various outer frameworks.

CHAPTER: 5 PROJECT PLAN

CHAPTER 5 PROJECT PLAN

5.1 List out the tasks

Task1: Setup and install Splunk Enterprise.

Task2: Configure Splunk Enterprise to work on correct configured ports.

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

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

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

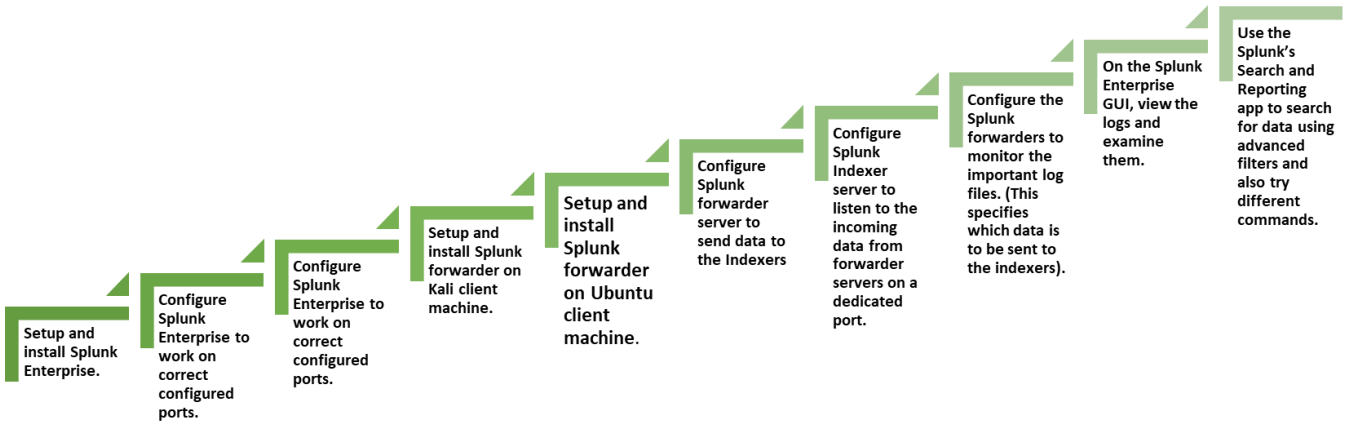
Task 6: Configure Splunk forwarder server to send data to the Indexers

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

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

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

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



5.2 List of Major Activities

Task1: Configure Splunk Indexer server to listen to the incoming data from forwarder servers on a dedicated port.

Task2: Configure the Splunk forwarders to monitor the important log files. (This specifies which data is to be sent to the indexers).

Task 3: Hosting a webserver with bWAPP on kali machine

Task 4: Performing SQL Injection using SQLMAP from ubuntu machine on kali machine

Task 5: Capturing SQL data in splunk

Task 6: Analyzing the SQL logs

Task 7: Advanced search queries

Task 8: Creating visualizations

Task 9: Creating dashboards

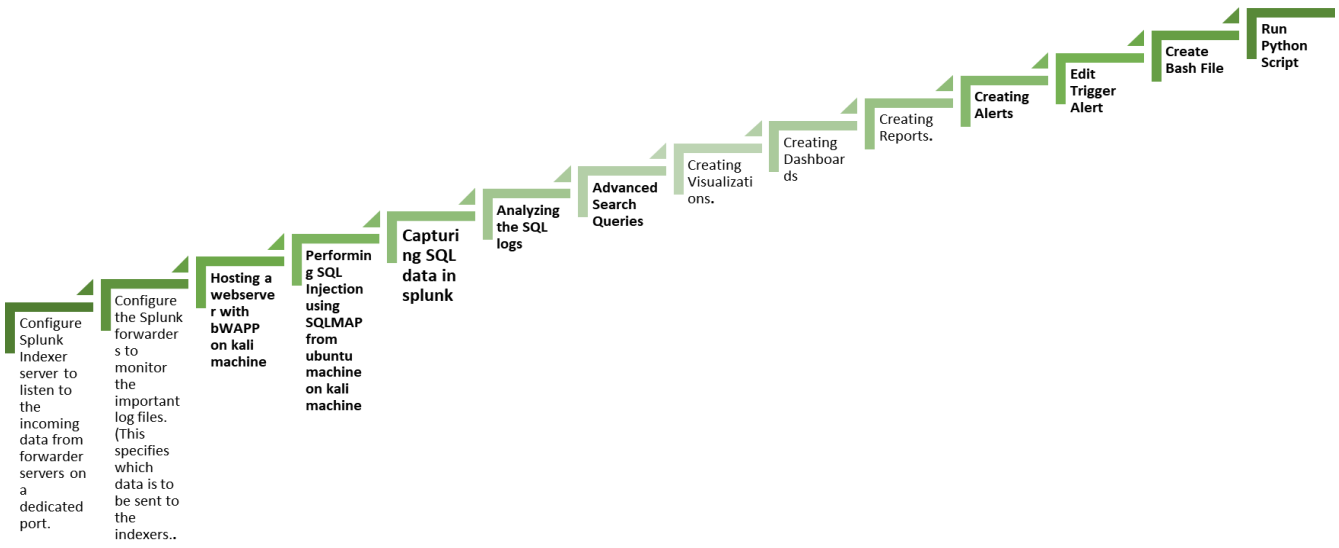
Task 10: Creating reports

Task 11: Creating alert

Task 12: Edit Trigger Alert

Task 13: Create Bash File

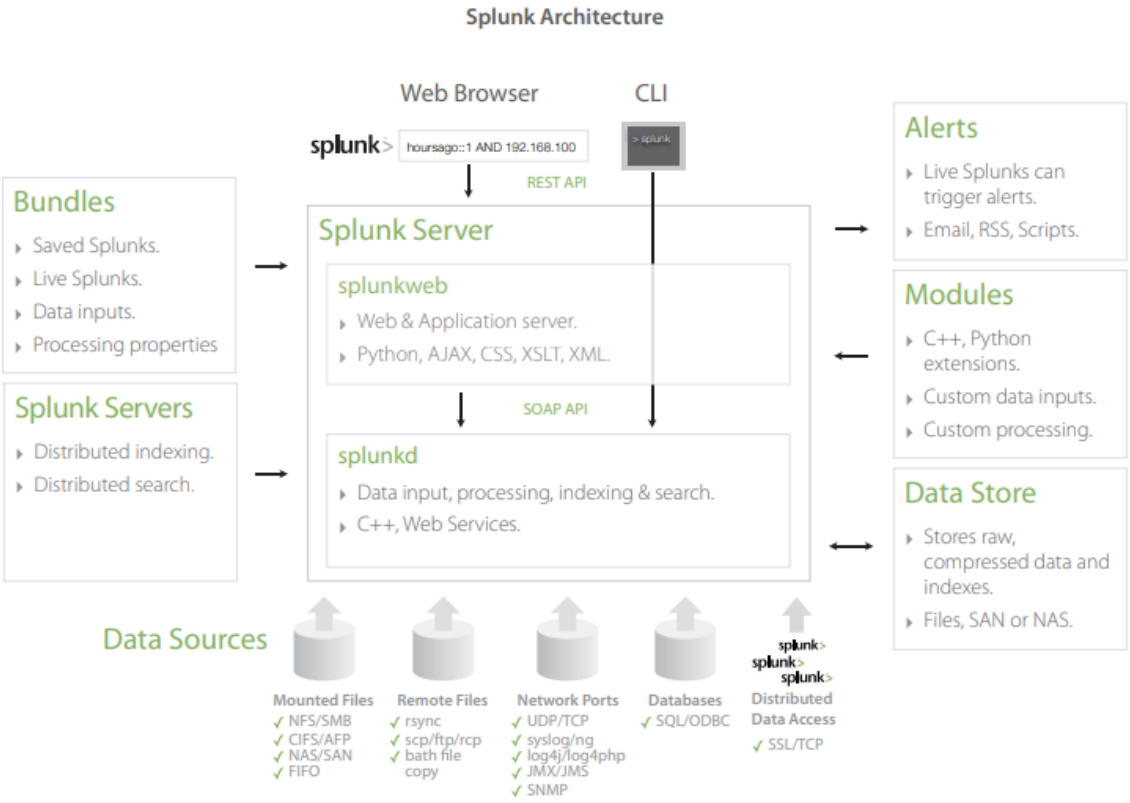
Task 14: Run Python Script



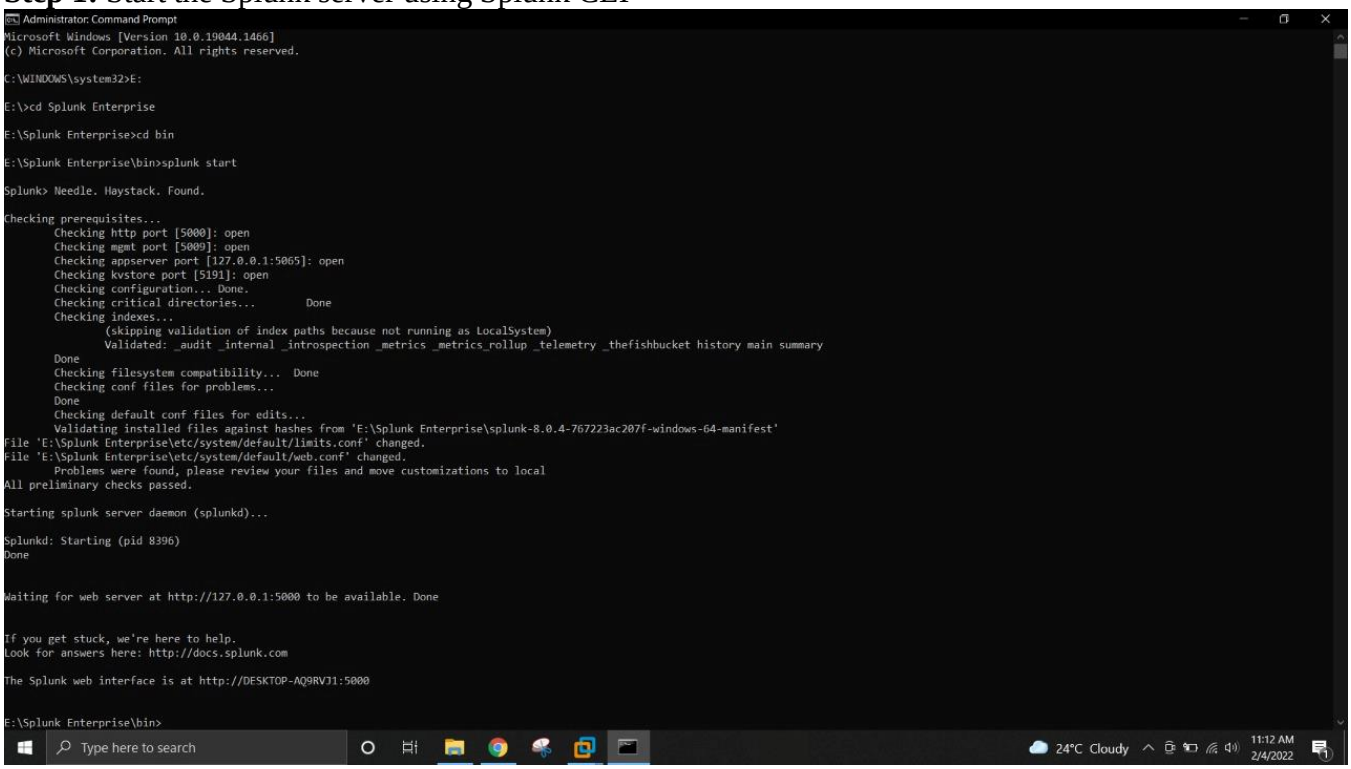
CHAPTER: 6 IMPLEMENTATION DETAILS

6.1.1 Data Collection

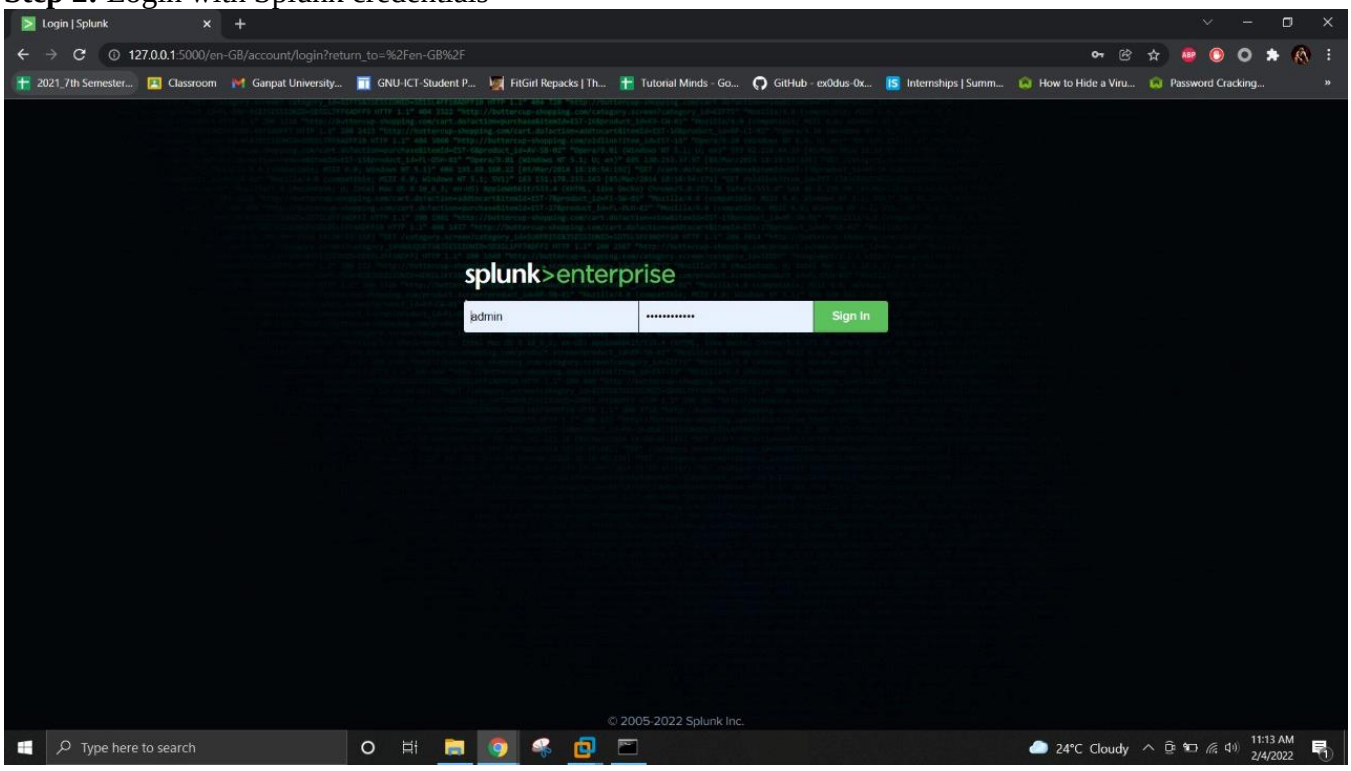
Figure 6.2 Method of Data Collection



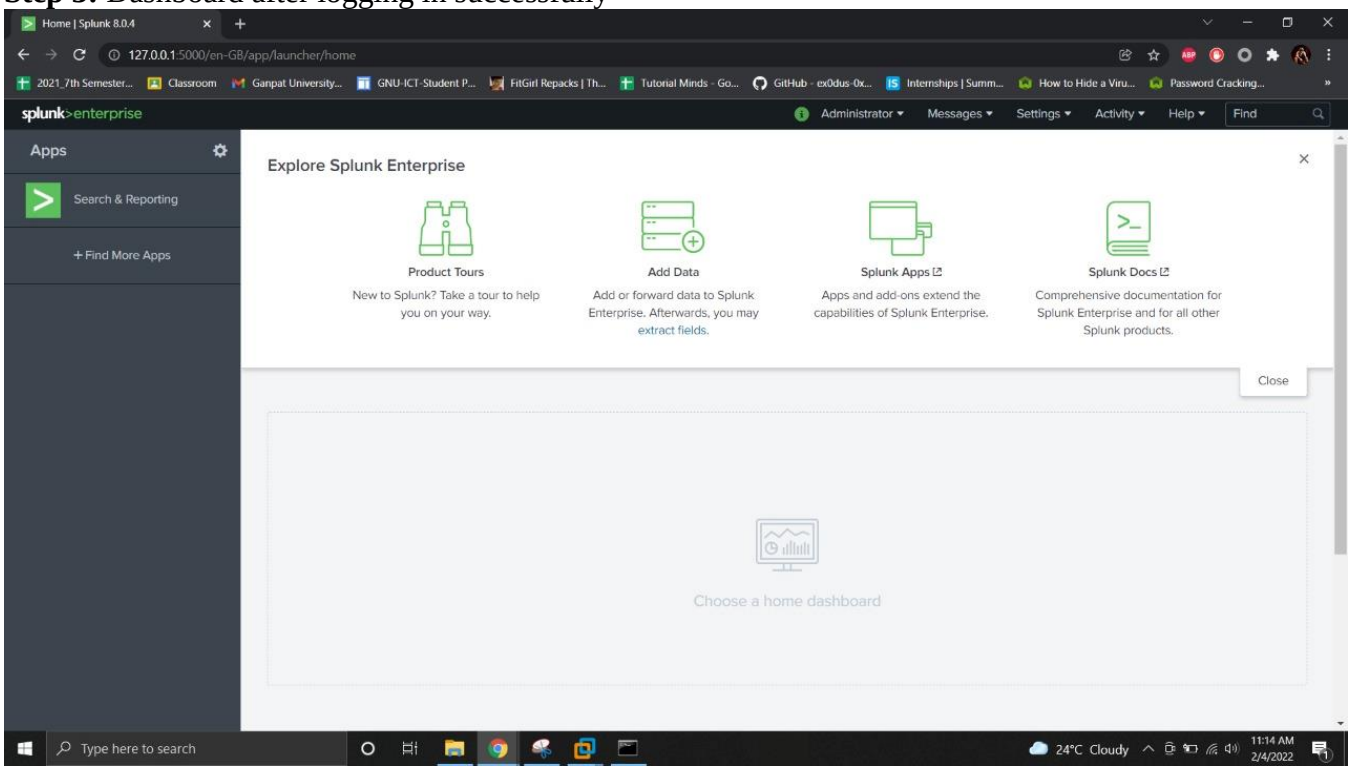
Step 1: Start the Splunk server using Splunk CLI



Step 2: Login with Splunk credentials

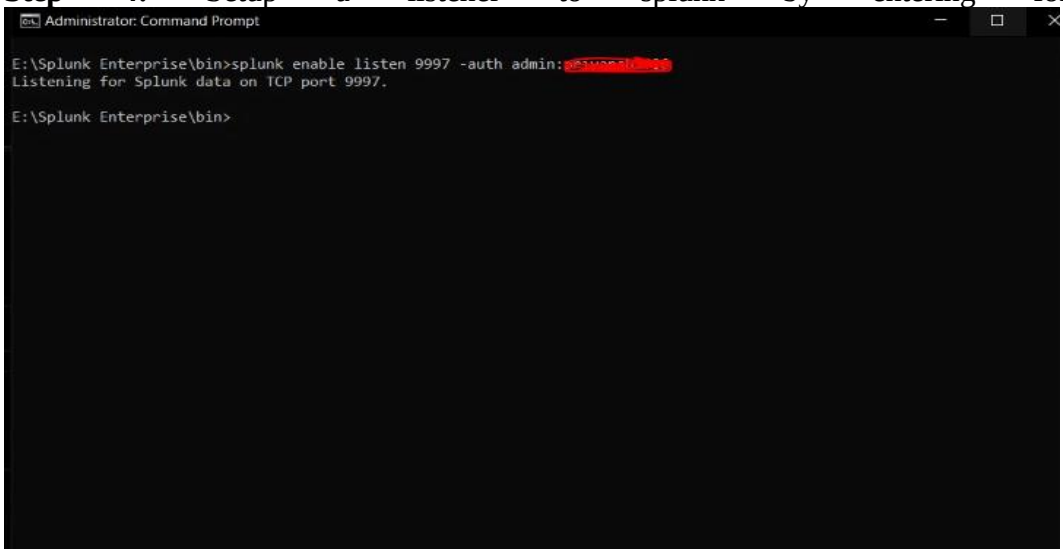


Step 3: Dashboard after logging in successfully



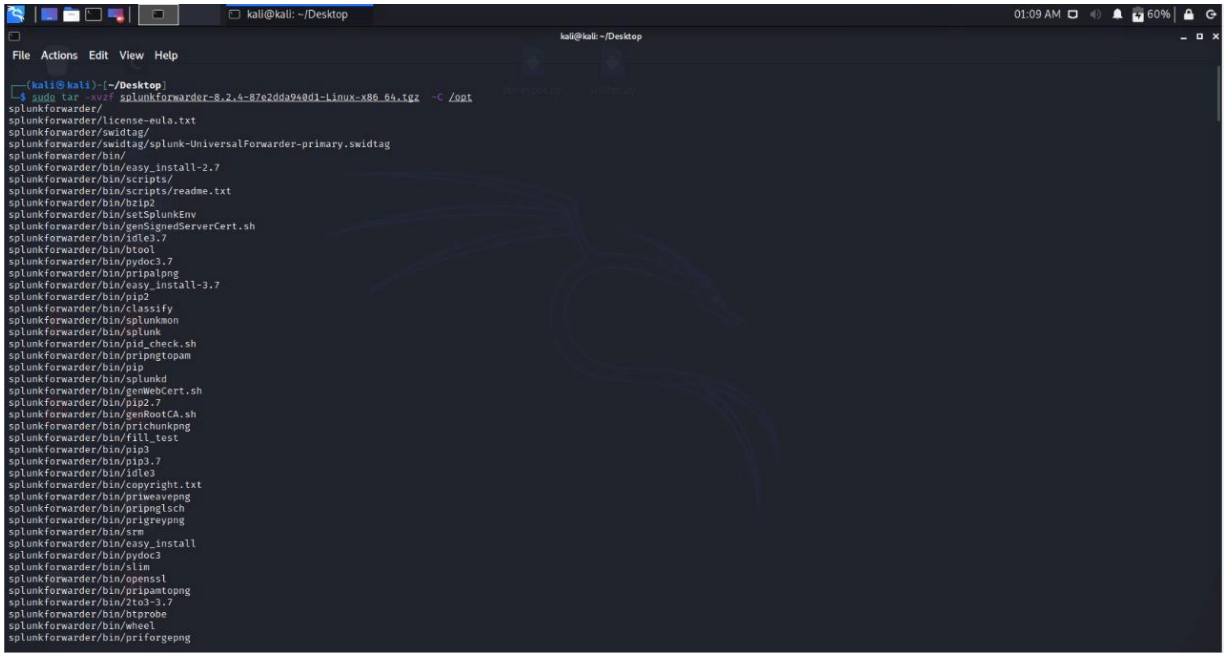
Now, we want to collect data from remote sources in the network. Hence, we will have to setup a listener on a dedicated port to be able to collect different logs from different data sources.

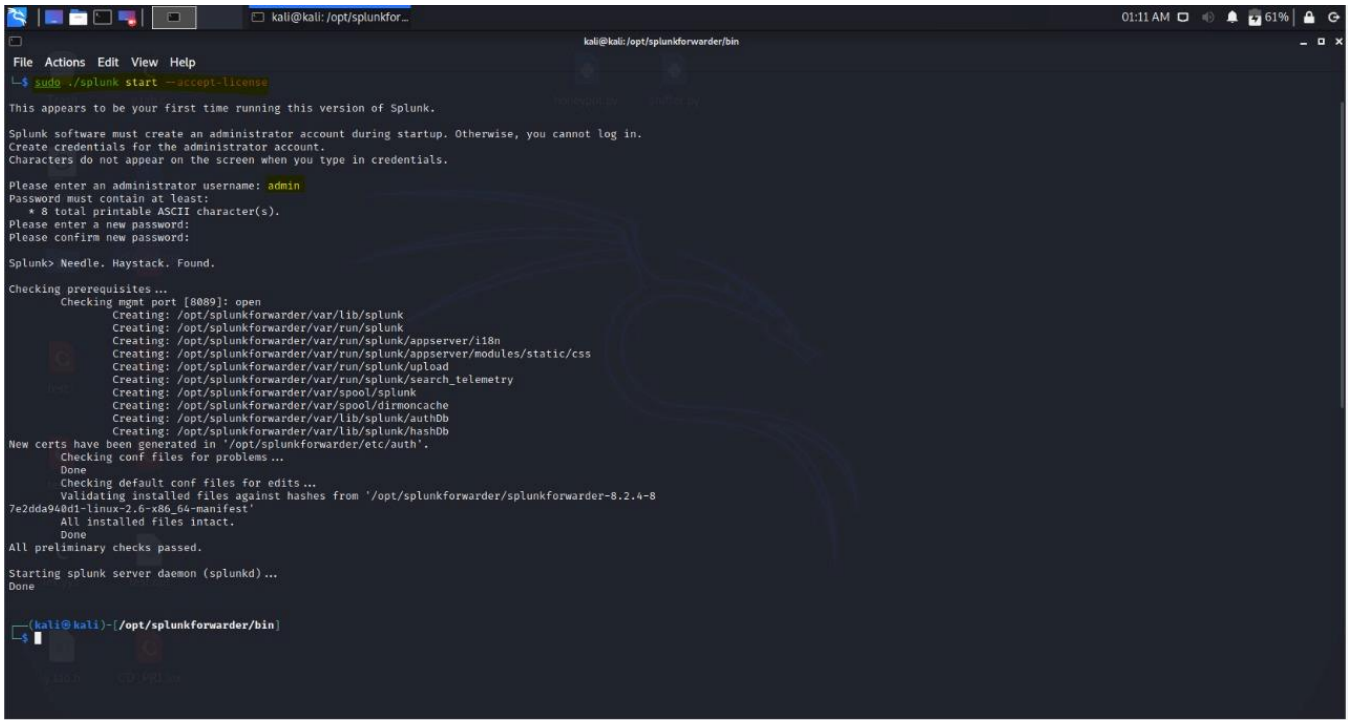
Step 4: Setup a listener to splunk by entering following command:

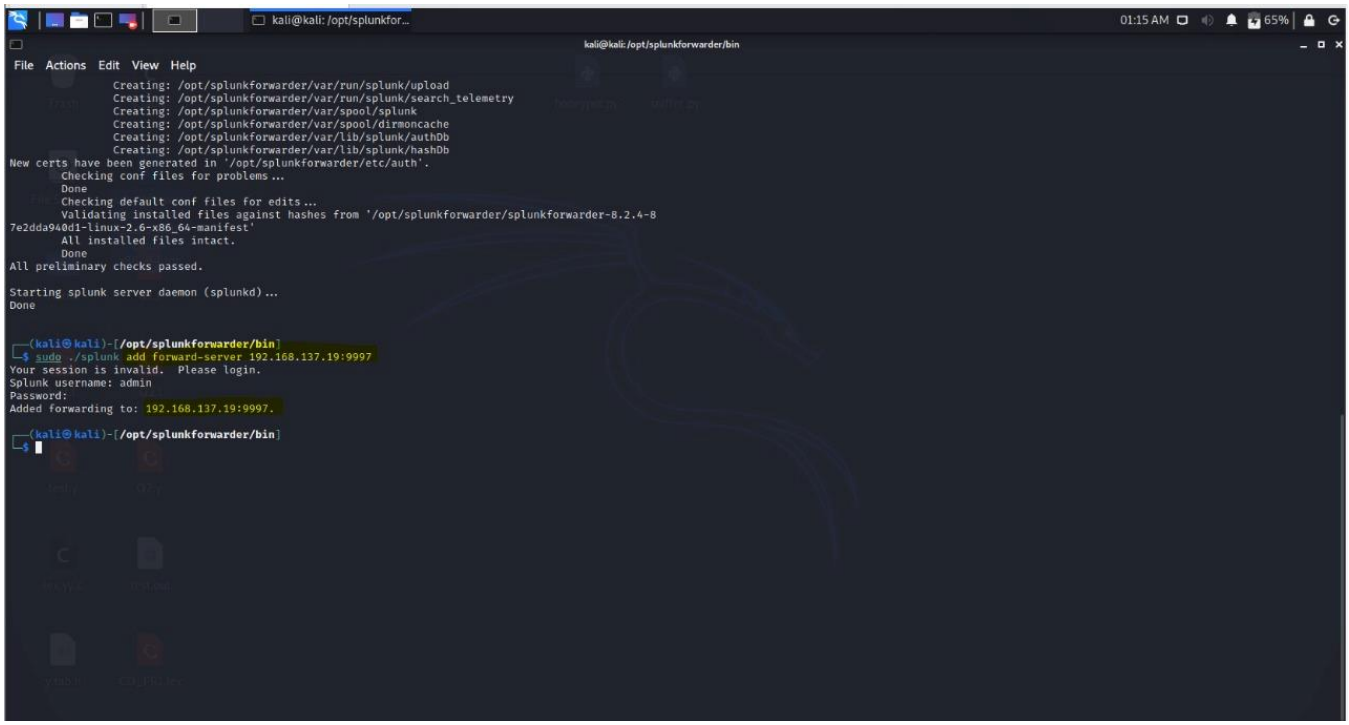


Now, to collect data from remote sources, we need to configure SPLUNK forwarder modules on either the machine themselves or within a forwarder server in the network.

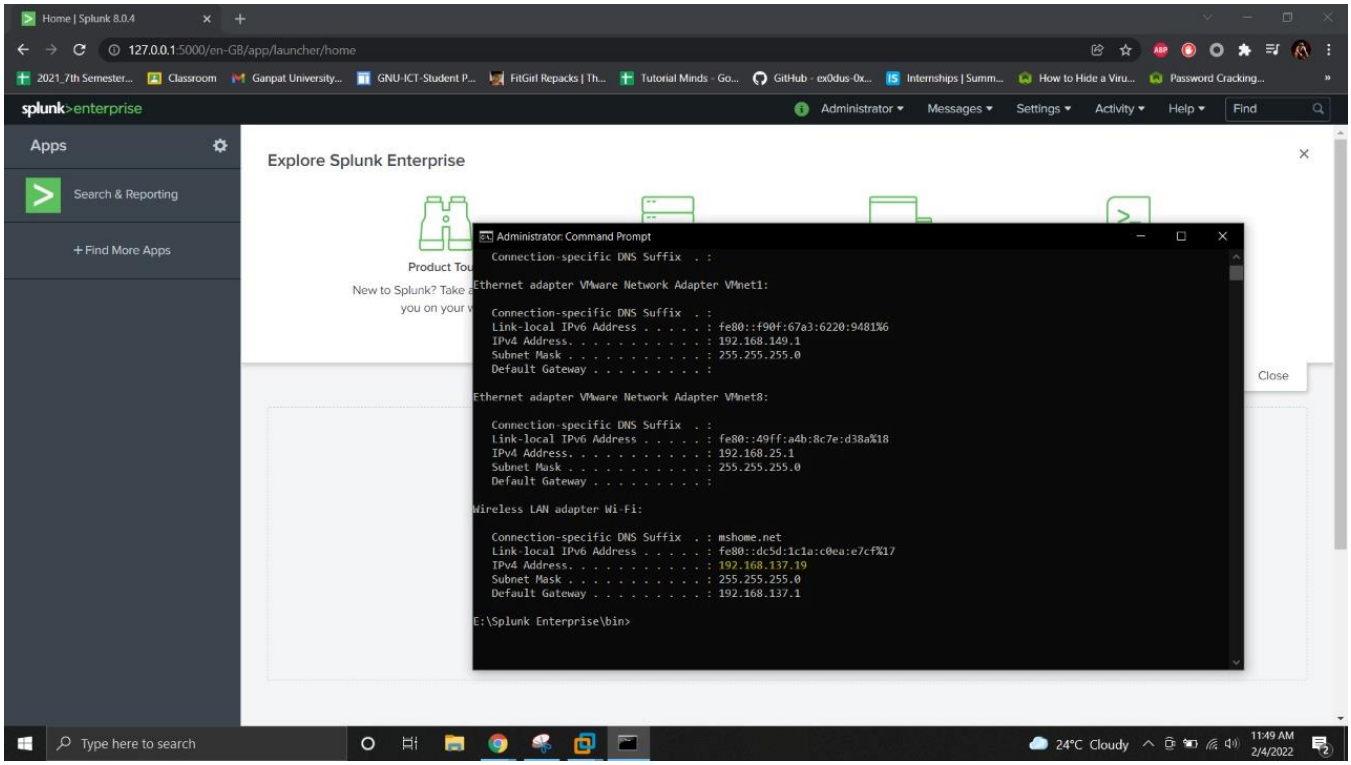
Step 5: Setting up SPLUNK forwarders:



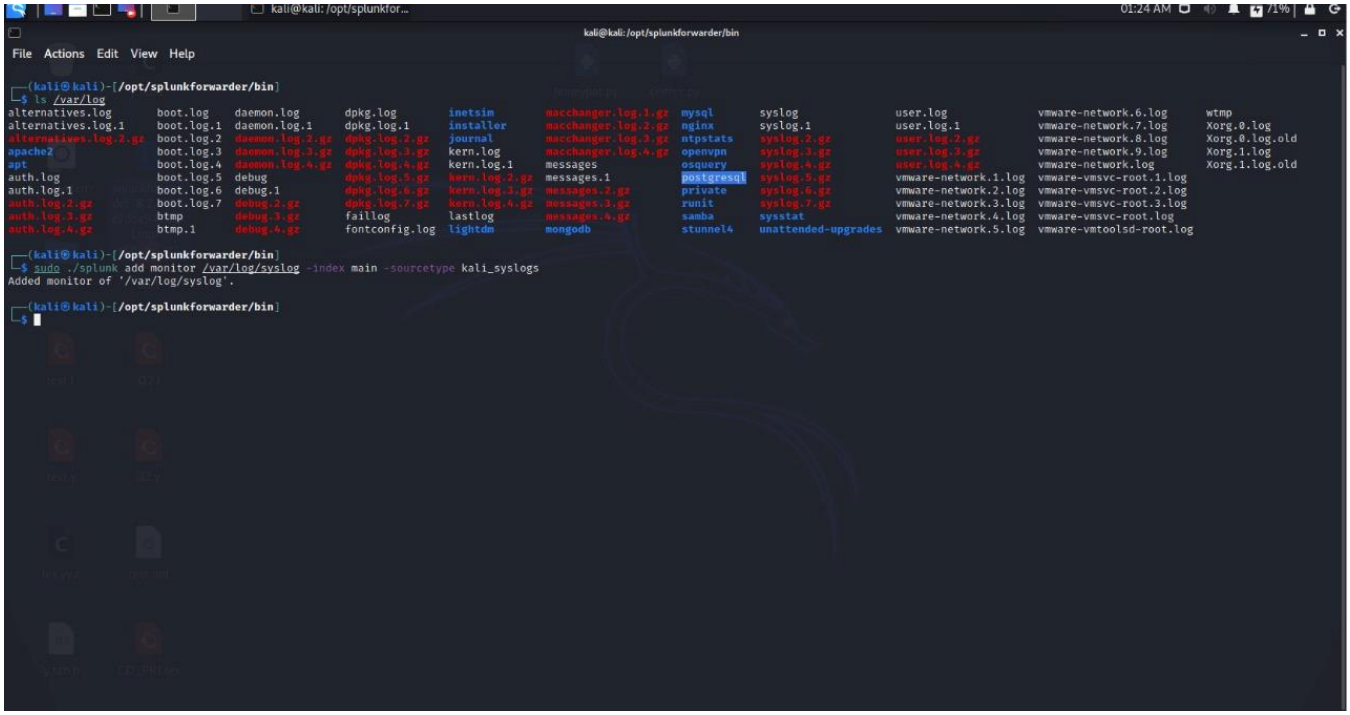




Note: The IP provided here to add forwarder server is the IP of our SPLUNK enterprise machine, where the SPLUNK indexer resides.

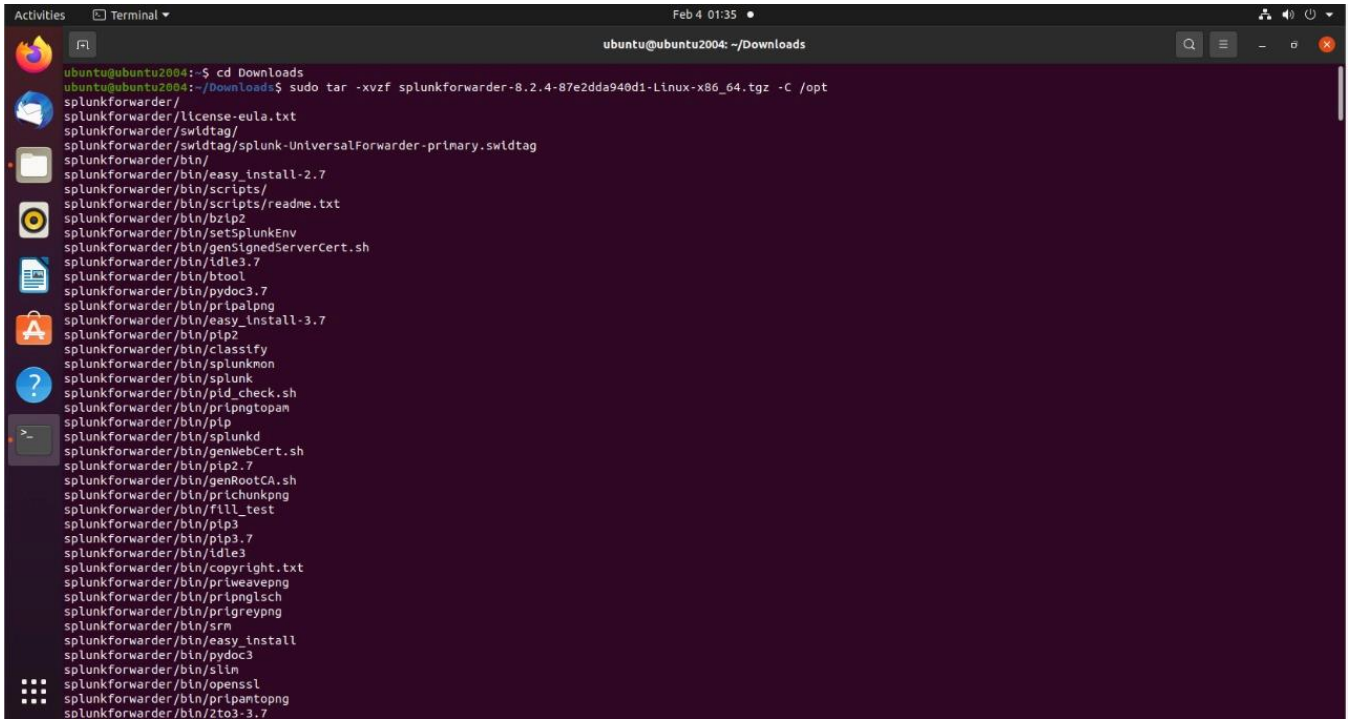


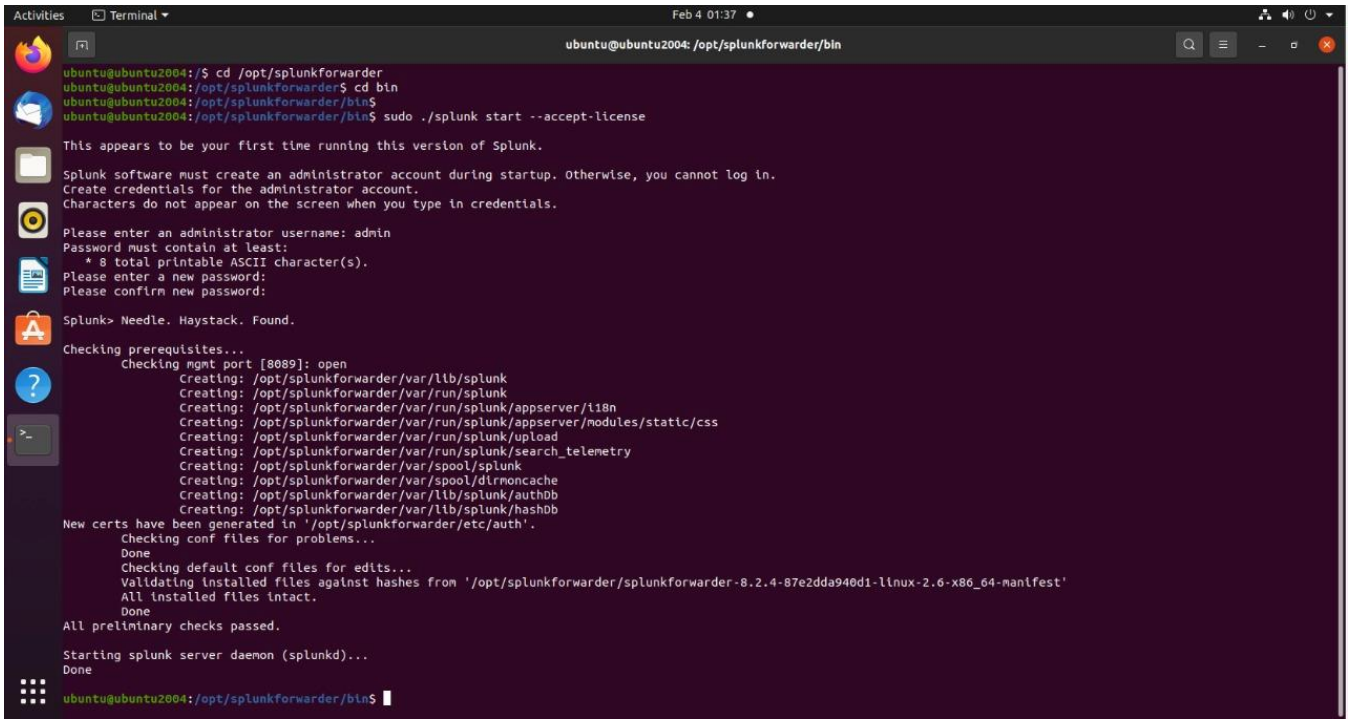
Once the forwarder server is configured, we will now specify the data source, I.e., which data to be sent to SPLUNK in order to monitor and analyze.

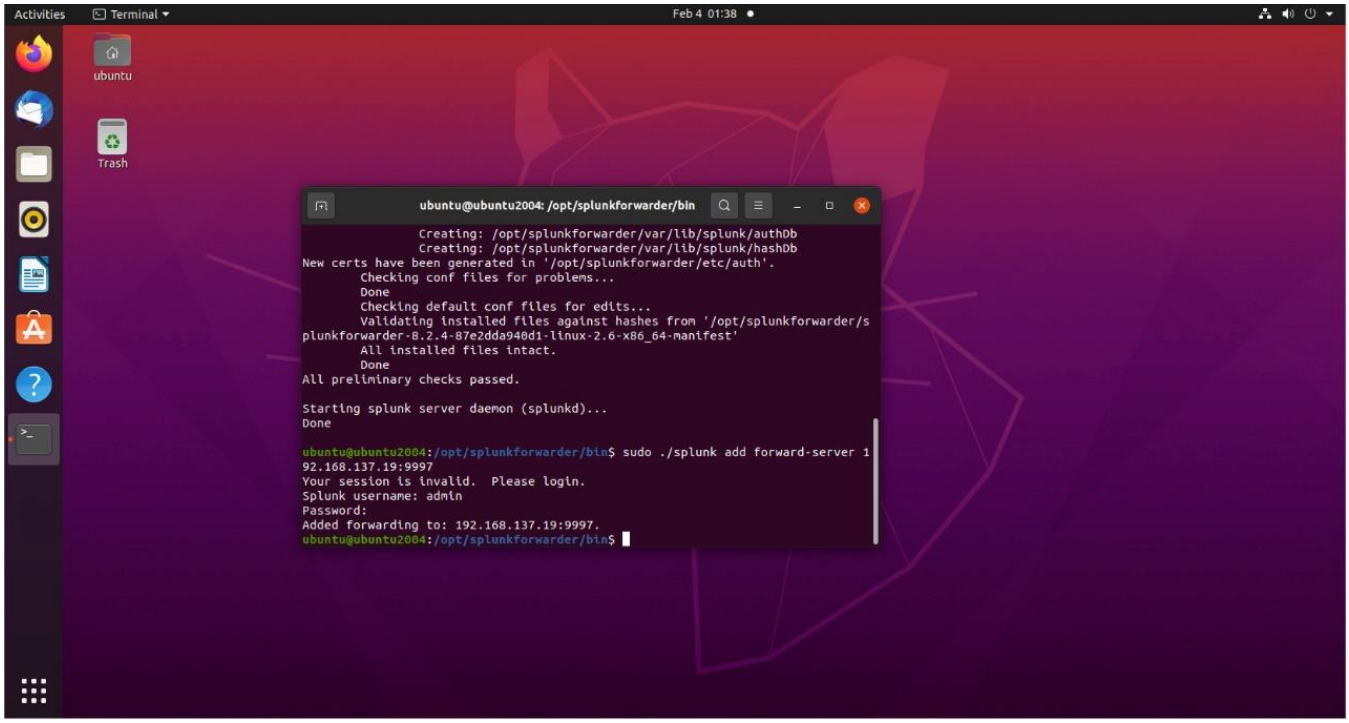


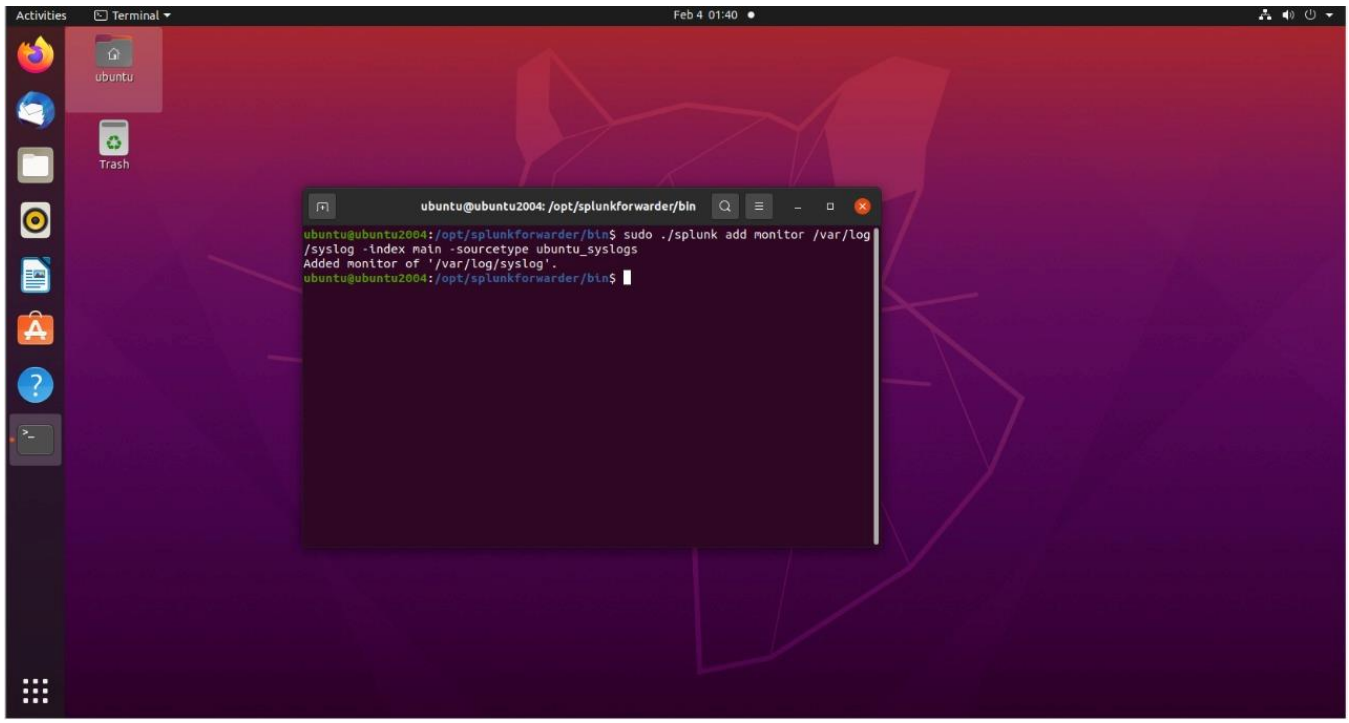
The remote forwarder is currently arranged. It will send the predetermined information source to the SPLUNK indexer continuously.

Similarly, doing the same for Ubuntu machine:

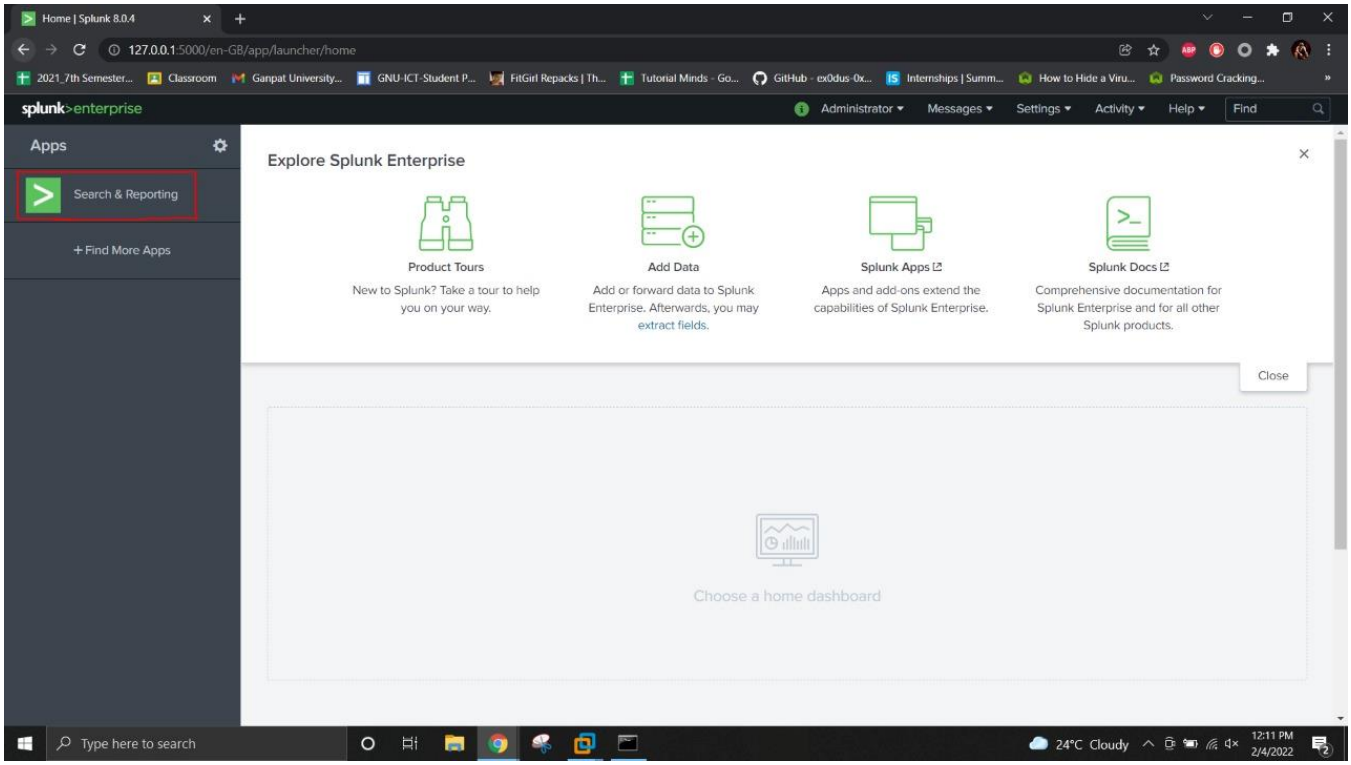




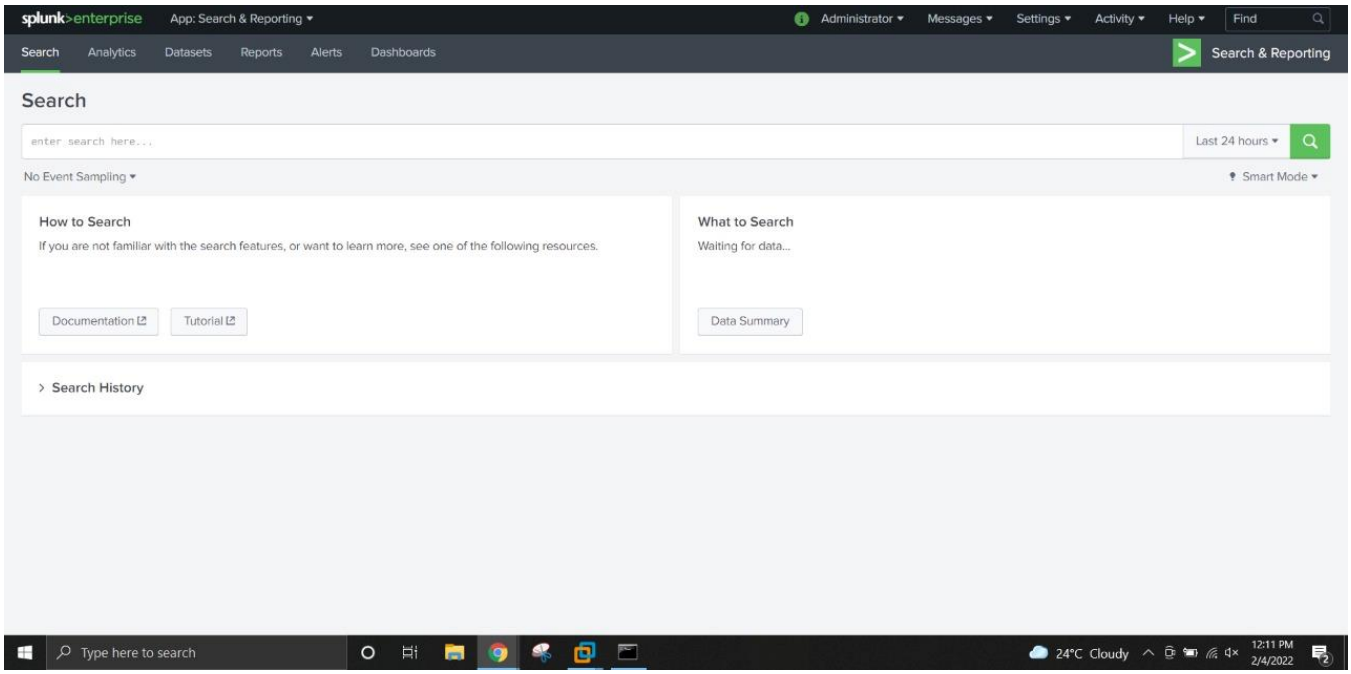

Activities
Terminal
Feb 4 01:38
ubuntu
Trash
ubuntu@ubuntu2004: /opt/splunkforwarder/bin
Creating: /opt/splunkforwarder/var/lib/splunk/authDb
Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-x86_64-manifest'
All installed files intact.
Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
Done
ubuntu@ubuntu2004:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server 192.168.137.19:9997
Your session is invalid. Please login.
Splunk username: admin
Password:
Added forwarding to: 192.168.137.19:9997.
ubuntu@ubuntu2004:/opt/splunkforwarder/bin$

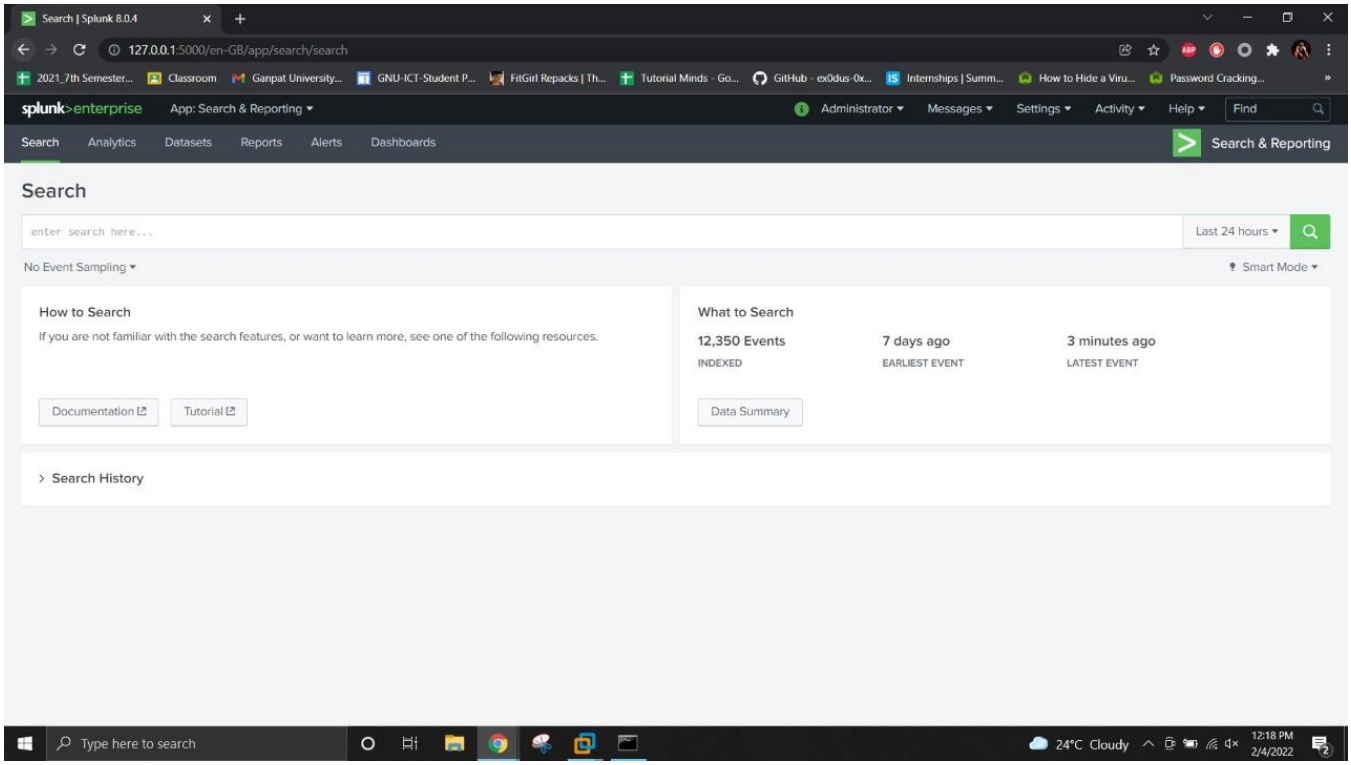

Activities
Terminal
Feb 4 01:40
ubuntu
Trash
ubuntu@ubuntu2004: /opt/splunkforwarder/bin
ubuntu@ubuntu2004:/opt/splunkforwarder/bin$ sudo ./splunk add monitor /var/log/syslog -index main -sourcetype ubuntu_syslogs
Added monitor of '/var/log/syslog'.
ubuntu@ubuntu2004:/opt/splunkforwarder/bin$

Step 6: Now, go to SPLUNK indexer server that is the web GUI for SPLUNK Enterprise and go to the app “Search and Reporting":

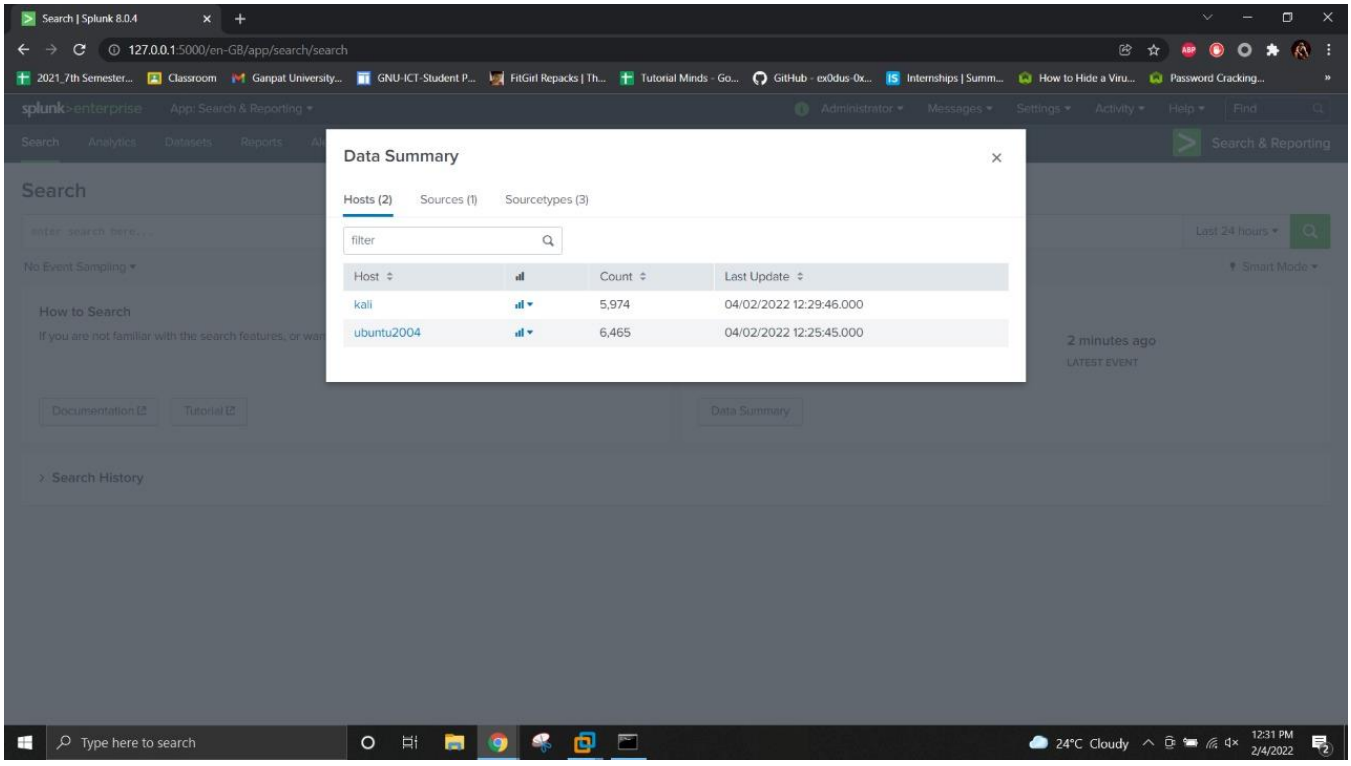


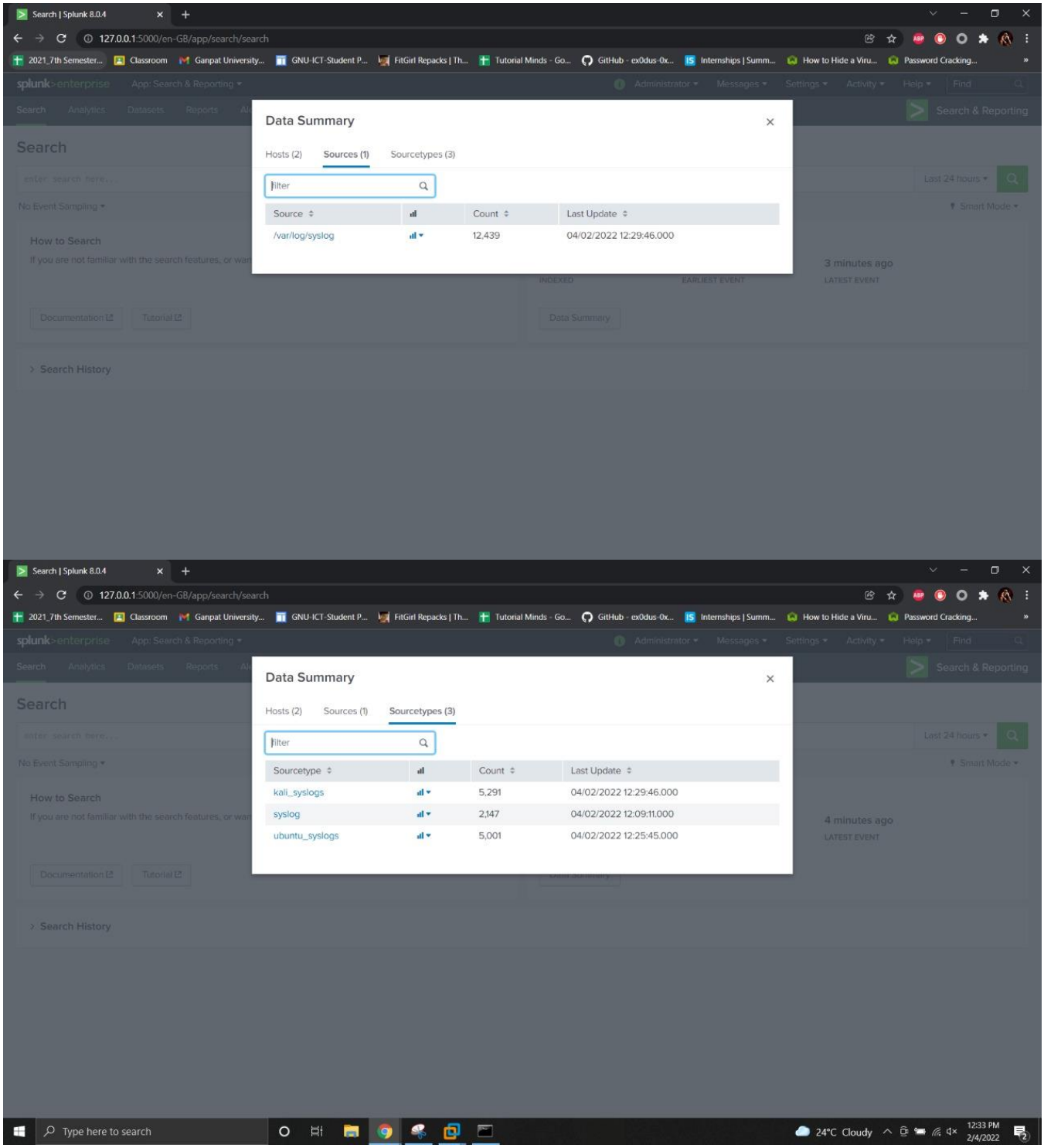
Step 7: Wait for the SPLUNK indexer to receiver to receive data from the remote forwarders:





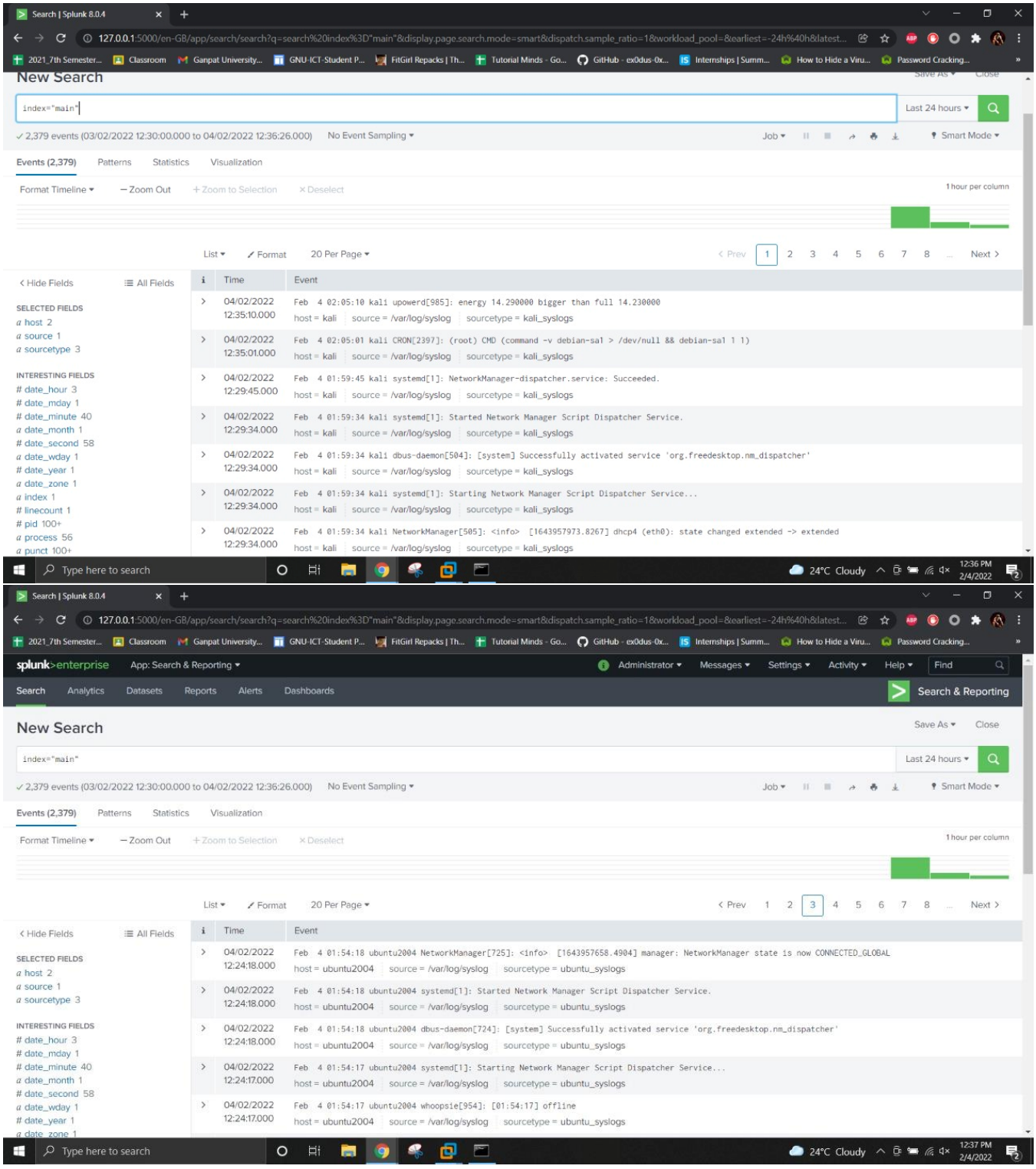
Step 8: Click on Data summary and view different stats.



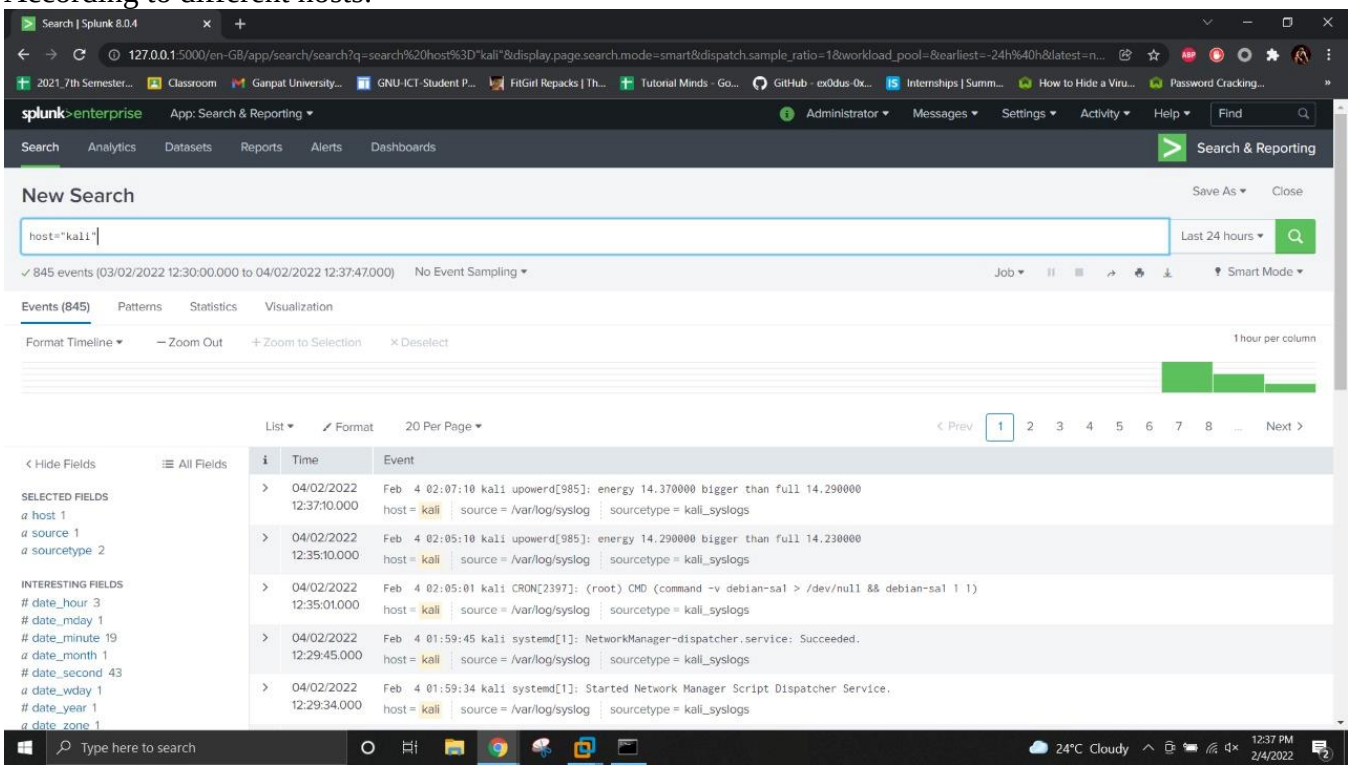

Search | Splunk 8.0.4
127.0.0.1:5000/en-GB/app/search/search
Data Summary
Hosts (2)
Sources (1)
Sourcetypes (3)
filter
Source
Count
Last Update
/var/log/syslog
12,439
04/02/2022 12:29:46.000
Search | Splunk 8.0.4
127.0.0.1:5000/en-GB/app/search/search
Data Summary
Hosts (2)
Sources (1)
Sourcetypes (3)
filter
Sourcetype
Count
Last Update
kali_syslogs
5,291
04/02/2022 12:29:46.000
syslog
2,147
04/02/2022 12:09:11.000
ubuntu_syslogs
5,001
04/02/2022 12:25:45.000
Type here to search
24°C Cloudy
12:33 PM
2/4/2022

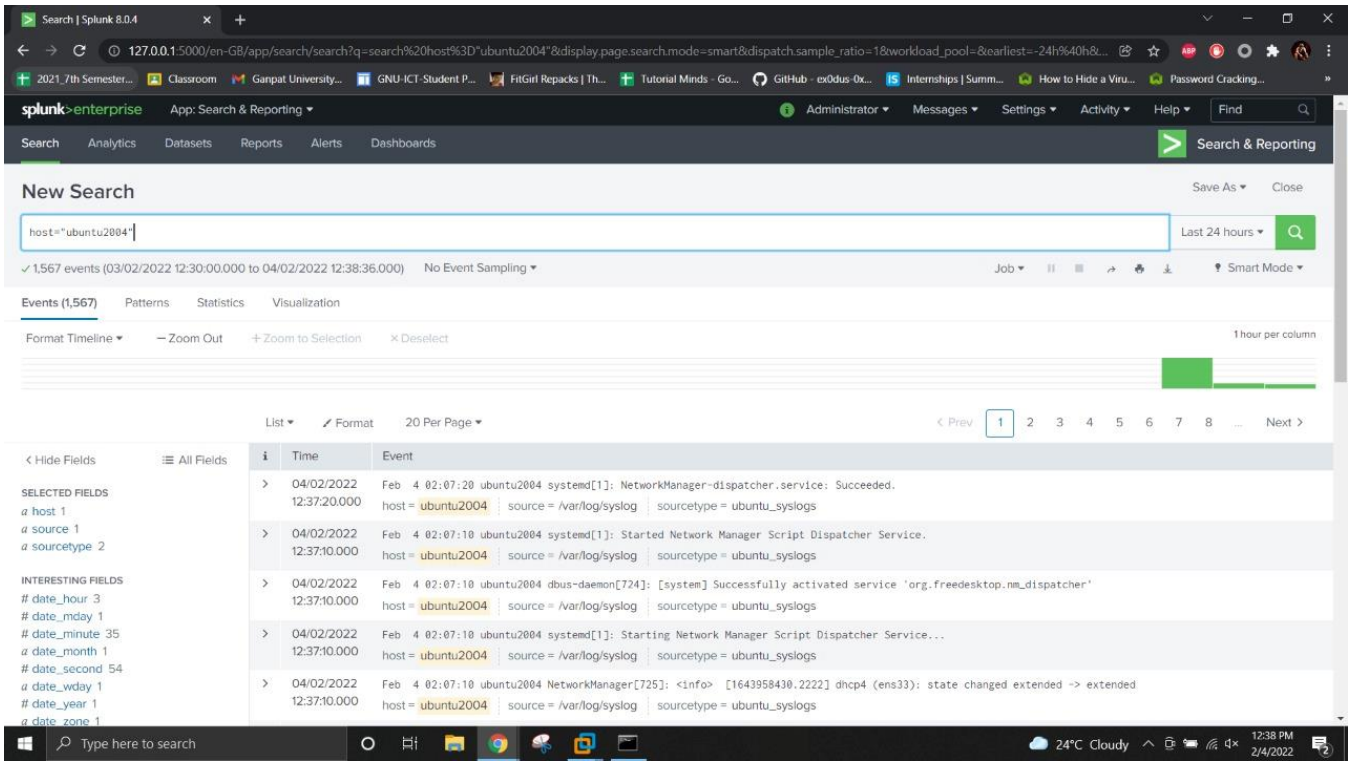
Step 9: Using SPLUNK search module to search and view the received data:

Index=”main”

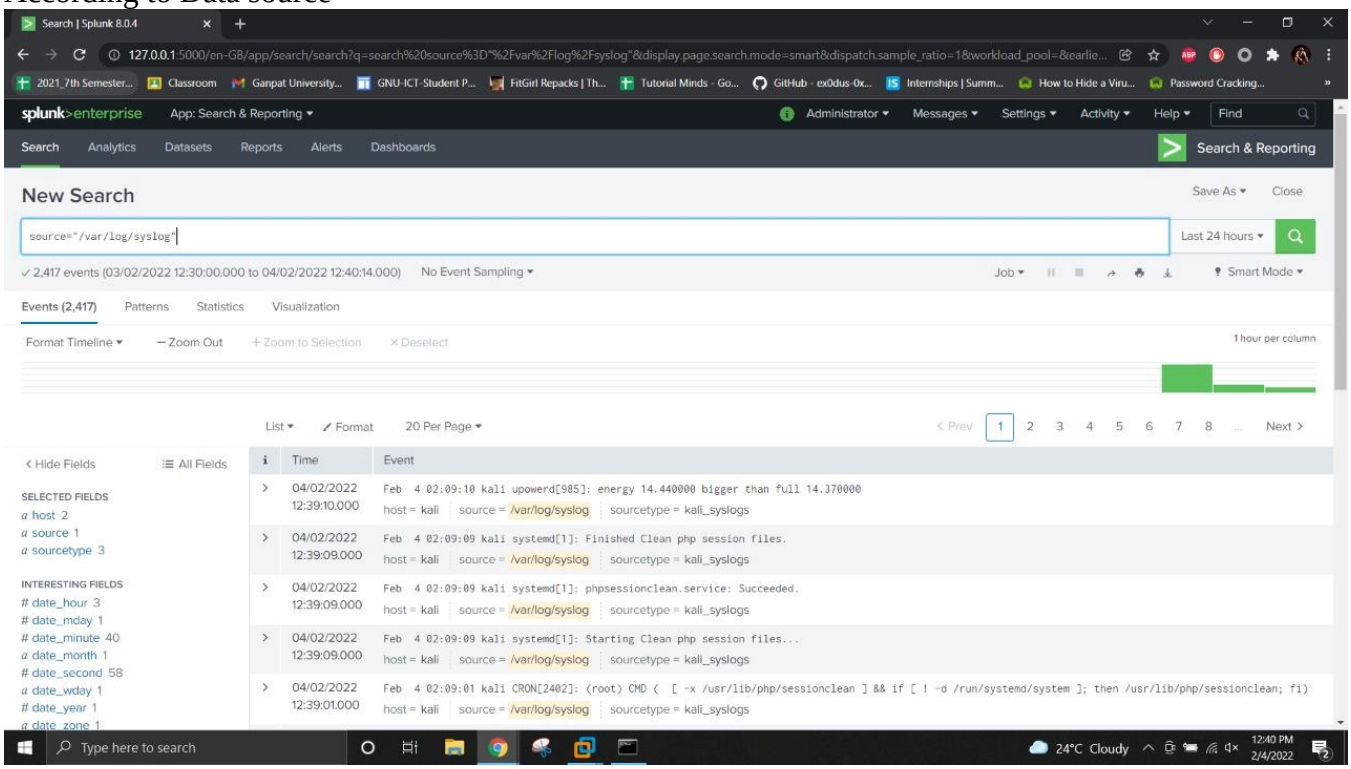


According to different hosts:

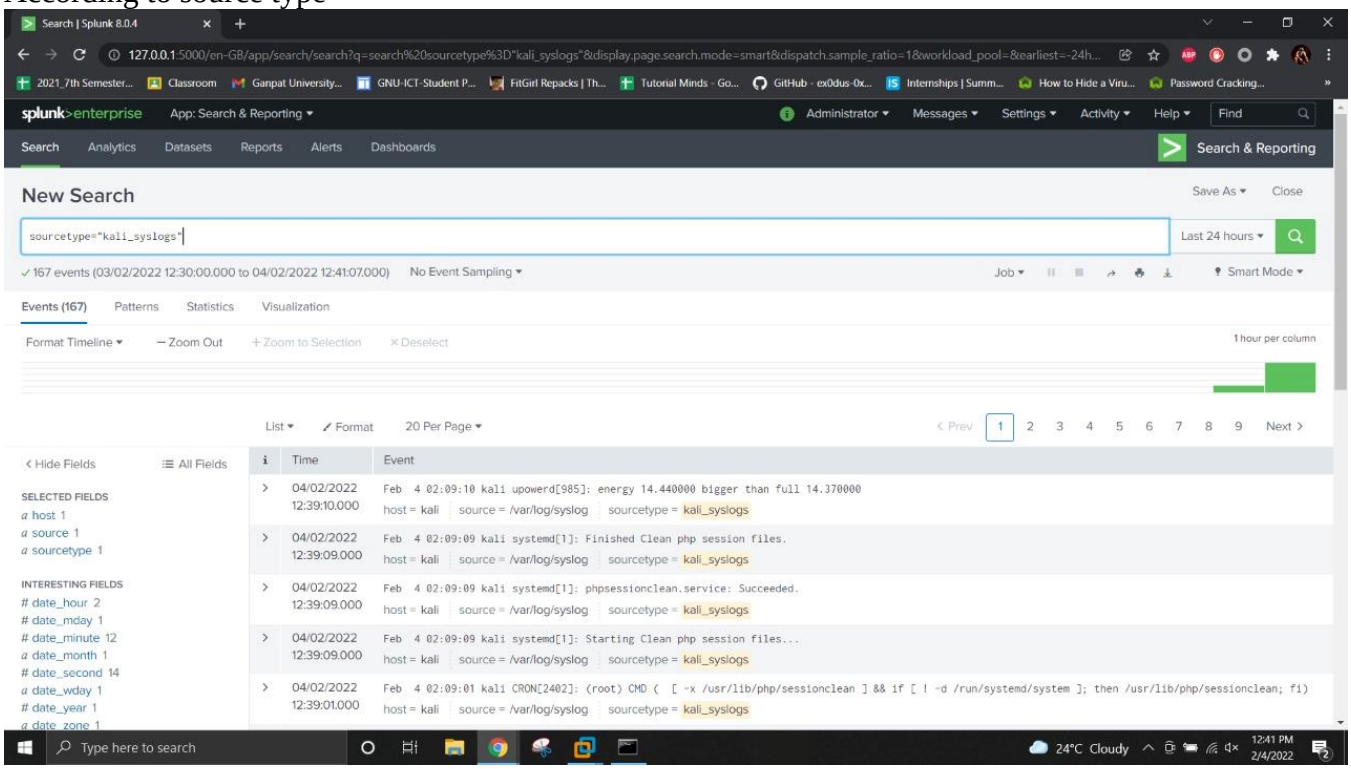


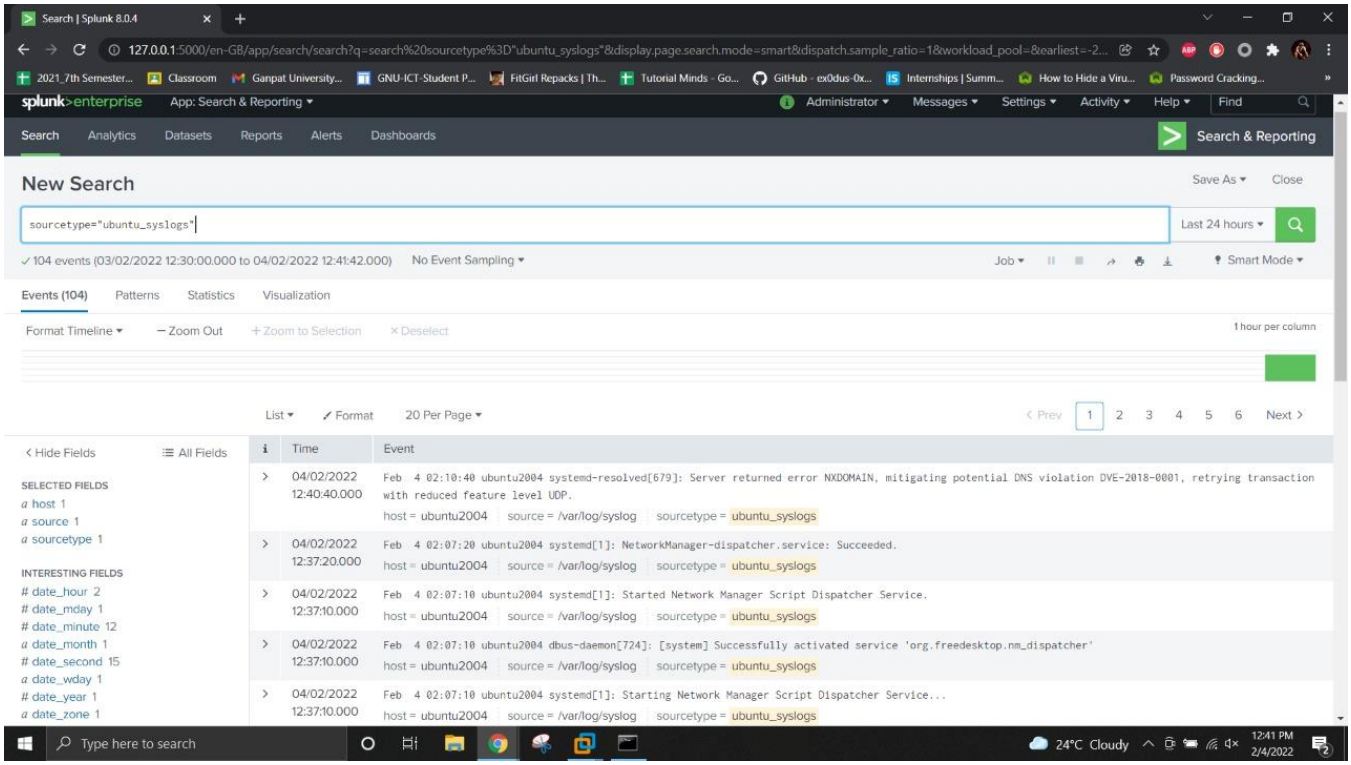


According to Data source

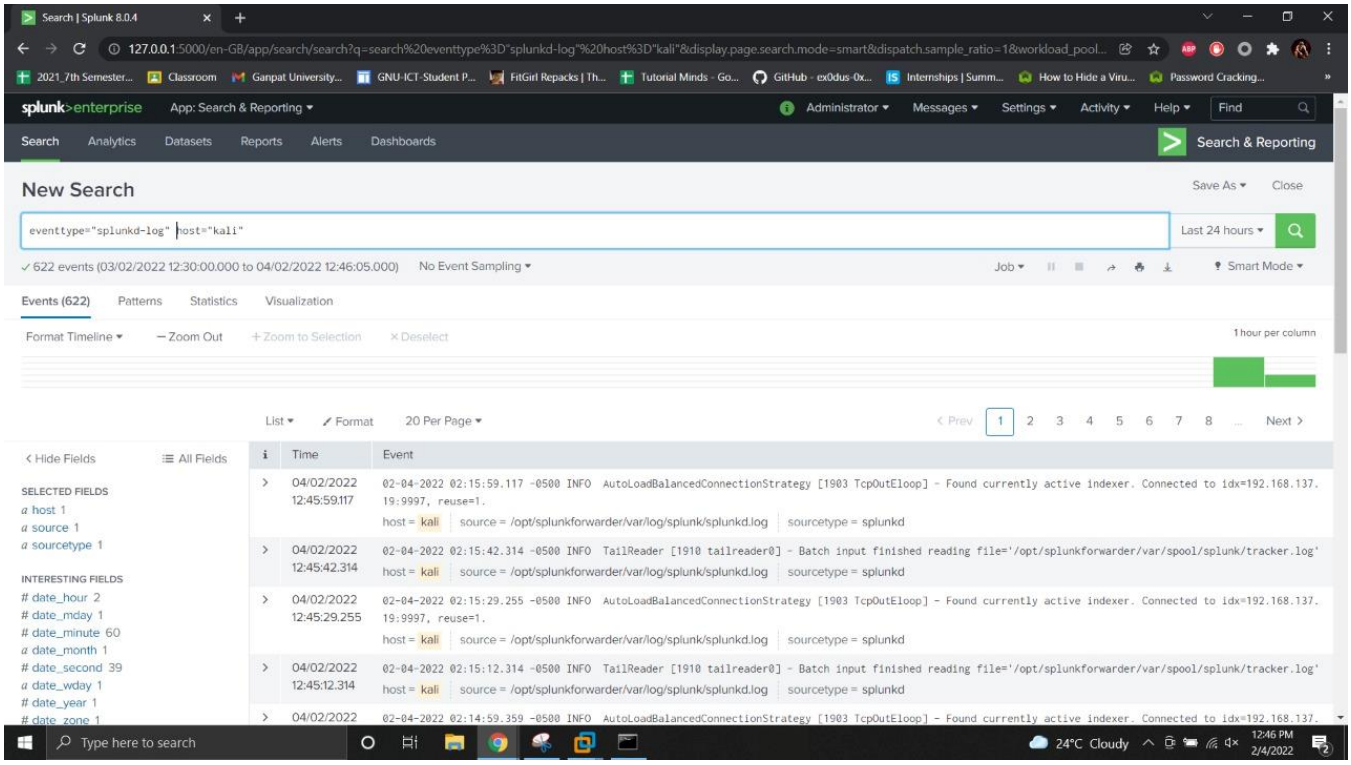


According to source type





According to event type



SPLUNK supports more such advanced search commands.

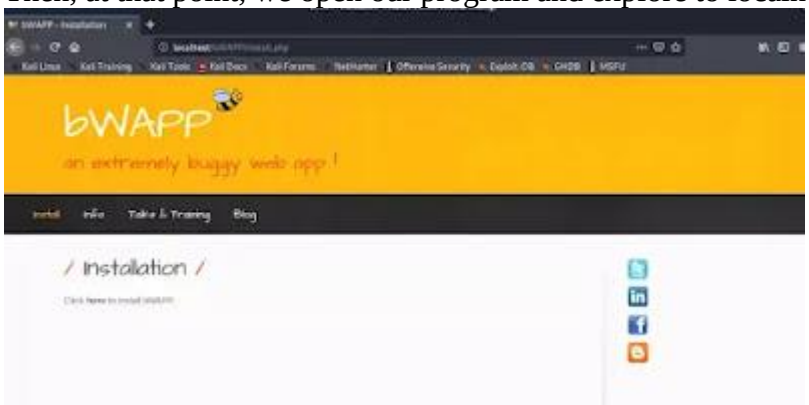
Project Approach: Splunk Enterprise

Splunk Enterprise is item thing that engages you to look, separate, and picture the data gathered from the pieces of your IT structure or business. Splunk Endeavor learns from locales, applications, sensors, contraptions, and so on. After you describe the data source, Splunk Endeavor records the data stream and parses it into a movement of individual events that you can view and look. Most clients partner with Splunk Undertaking with a web program and use Splunk Web to control their association, administer and make data objects, run look, make turns and reports, and so on. We can moreover use the request line association highlight deal with your Splunk Venture association. You can loosen up the Splunk Venture environment to fit the specific necessities of your relationship by using applications. An application is a combination of arrangements, data articles, points of view, and dashboards that unexpected spikes sought after for the Splunk stage. A single Splunk Venture foundation can run different application.

1. 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

Then, at that point, we open our program and explore to localhost/bWAPP/install.php



Here we click for introduce it. On the off chance that the setup is awesome, it ought to effectively introduce.

Then, at that point, we go to login page tapping on the menu bar.

The default username is honey bee and the default secret phrase is bug. Utilizing those we click on login with low security level.

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

- sqlmap is an open source login device that enables the process involved in detecting and implementing SQL installation imperfections and managing data set servers.
- Incorporates a powerful local engine, various expert features for direct introduction analysis, and a wide range of switches that include a set of fingerprint data, data acquisition data sets, approval of a basic record framework, and outsourcing orders through external organizations.

3. 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.

4. 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 Proofreader.
- 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.
11. Click the dashboard name to see the dashboard or snap the Add Graph symbol to add an extra perception.

5. 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.

1. In your Splunk Light instance, select Dashboards in the menu bar.
2. Click Make New Dashboard.
3. (Optional) Enter a Title.
4. Enter an ID.
5. Optional) Enter a Portrayal.
6. Click a consent level.
7. Click Make Dashboard.
8. On the Alter Dashboard page, add boards or contributions to your dashboard.
9. Click Save.
10. (Optional) To affirm that you have saved the dashboard, click Dashboards in the menu bar to see the dashboard recorded on the Dashboards page.

6. Create a real-time alert with per-result triggering:-

Constant cautions with per-result setting off are sometimes known by result alerts. This caution type and setting off use a relentless consistent pursuit to look for events. Each result sets off the wariness.

• Alert: In the event that have Splunk Venture high-accessibility arrangement, use per-result setting off with alert. In the event that a friend isn't accessible, an ongoing hunt doesn't caution that the inquiry may be fragmented. To keep away from this issue, utilize a booked caution

Follow these means to make a continuous caution with per-result setting off.

1. Move to the Pursuit page in Hunt & Revealing application.
2. Create a new pursuit.
3. Click on Save As and then Alert.
4. Enter title and discretionary portrayal.
5. Determine consents.
6. Select that Continuous alarm type.
7. Supplant the Terminates setting.This kinds of setting controls the future of established off alert standards, which appear on the Set off Cautions page.
8. Select the Per-Result trigger decision.
9. Arrange a trigger choking period.
10. Select something like one intolerable demonstration that happens when the alert triggers.
11. Click Save.

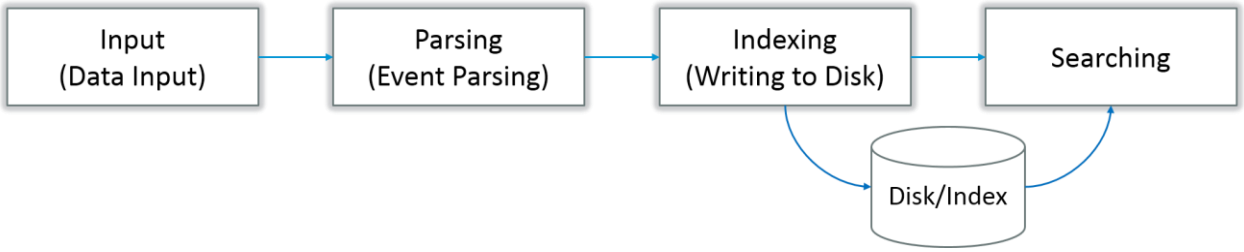
Email alert function

Send an email alert to the beneficiaries shown when the alarm goes off. Email notifications may include data from list items, query function, and alert setup. Splunk can send email notification using search page or search command.

6.1.2 Flow of Project

Data pipeline stages proceeds in three flows

- The input stage
- The storage stage for data
- The searching of data stage



1. Data Information Stage

At this stage, Splunk editing uses the stream of raw information from its source, breaks it into 64K squares, and specifies each square with metadata keys. Metadata keys include hostname, a type of unlimited source of information. Keys similarly can include attributes that are used internally, for example, coding information for distribution information and values that control information management during the order phase, for example, the record at which times should be discarded.**2.**

Data Capacity Stage

- The data limit consists of two phases: Analysis and editing.
- In the analysis phase, the Splunk system evaluates, evaluates, and modifies data to separate only important information. This is often called event management. It is during this stage that Splunk editing breaks the data stream into individual events. The stages are many sub-sections:

1. Divide the increase in data in each row
2. Identifying, sorting, and setting time stamps
3. Defining each event with a metadata copied to a broad source key
4. Modifying event data and metadata according to regex change rules
5. In the order section, the Splunk system makes the filtered events a summary on the plate. It makes both aggregated data and a separate record report. The advantage of ordering is that the data can be successfully retrieved during the scan.

2. Data Looking through Stage

This stage controls how the client gets to, perspectives, and utilizations the recorded information. As a component of the pursuit work, Splunk programming stores client made information objects, for example, reports, occasion types, dashboards, cautions and field extractions. The hunt work likewise deals with the inquiry cycle.

SQL Injection:-

SQL injection is sequel query language injection which exploits the database by inserting such data as user input which act as a part of query and perform action accordingly which result in great impact of data leakage.

Sqlmap:-

sqlmap is an entrance testing gadget that automates the technique associated with perceiving and exploiting SQL mixture deformities and taking over of data base servers. It goes with a solid area engine, various specialty features for an authoritative entry analyzer and a broad extent of switches persevering from informational index fingerprinting, over data getting from the informational index, to getting to the crucial record system and executing orders on the functioning structure all through of-band affiliations.

DOS:-

- Denial of Service (DoS) attack is kind of attack which is generated by multiple parallel processing result in losing accessibility and performance of the victim system.
- During the DOS attack, they additionally get to restricted intel. These PCs are then used to wage a DoS Assault in attacker's PC.
- Through various wellbeing endeavors have been taken to stop DOS Assault to shield our data, the aggressors have developed new techniques and attack reasoning. Consequently, it is fundamental that rather than answering new attacks, it is vital to manufacture an absolute DoS plan that will make preparations for a wide scope of DoS attacks. Along these lines, the experts ought to understand the web and methodologies used to hinder the DoS attacks.
- The proposed structure gives an exceptional method to perceive DoS attack using Splunk.We propose two techniques for counteraction of DoS assault.
- One is utilizing Haphazardly created Manual human tests and other one is utilizing Linux slam content to forestall DoS attack via naturally impeding IP of the client, who is sending different solicitation at a time.

Getting everything rolling with DOS assaults utilizing hping3:

To install hping3 on a linux based system fire the command: **apt install hping3 -y**

A simple dos attack performed by: **sudo hping3 - S - - flood - V - p 80 170.155.9.185**

sudo: gives required honors to run hping3.

hping3: command calls hping3 program.

-S: in the command indicates the SYN bundles.

-flood: take shots at carefulness, answers will be disregarded (that is the reason answers wont be shown) and parcels will be sent quick as could really be expected.

-V: stands for level of Verbosity.

-p 80: is the port number dedicated to 80

170.155.9.185: is IPof the target system.

CHAPTER: 7 CONCLUSIONS AND FUTURE WORK

CHAPTER 7 CONCLUSION AND FUTURE WORK

Challenges and how we overcame it

The splunk enterprise came up with the feature to run any script that could prevent simple attacks or help the system with security incident and event management, but lately the feature was depreciated. Splunk doesn't allowed to run any script in desired environment. So a manual bash file was created by us that run the python script which would build a SSH connection with remote system and generate a trigger alert notification.

Conclusion

Splunk is now an industry standard for examining continuous information and trigger subsequent activities. Splunk is being utilized all around the world by government offices, business specialist co-ops, colleges to dissect and comprehend business and client conduct continuously It can set off alarms in the event of any network safety extortion, and working on the presentation of the help being given, while lessening the expense for the everyday tasks in any association.

Future work

In future for this project we will be using splunk apps and gathering data from various sources and work with different features provided by Splunk Enterprise.

CHAPTER: 8 REFERENCES

CHAPTER 8
REFERENCES

1) https://docs.splunk.com/Documentation
2) https://sqlmap.org/
3) http://www.hping.org/
4) https://www.ibm.com/security/enterprise-mobility-management

ibm report

by Priyansh Gupta

Submission date: 27-Apr-2022 09:49PM (UTC+0530)
Submission ID: 1821983094
File name: G04_IBM_SIEM_Plagarism.docx (3.8M)
Word count: 5082
Character count: 27272

CHAPTER: 1 INTRODUCTION

CHAPTER 1 INTRODUCTION

Security Information & Event Management

SIEM is advanced security data framework that examines security alarms and information created from gadgets on an organization progressively. Associations use SIEM instruments to distinguish security occurrences, log security information, oversee episode reaction, and create reports for consistence. The term SIEM was first utilized in 2005 by Imprint Nicolett and Amrit Williams. SIEM as an idea was proposed by them by consolidating the idea of safety data the board (SIM) and security occasion the executives (SEM).

Splunk:-

Splunk is an undeniable, flexible, and effective level that records and searches log logos set aside in the building. Research machine-generated data to provide useful information. The legal advantage of using Splunk is that it does not have to worry about any data source to store its data, as it usually uses its own records to store data.

Splunk is a device often used to view, monitor, and evaluate large-scale machine information by using web-based interaction. Splunk enables the acquisition, solicitation, and comparison of consistent data in an available manager where it can create drafts, reports, alerts, dashboards, and exposures. It hopes to make digitized data available through the organization and can detect data systems, generate estimates, investigate. With the help of Splunk programs, searching for specific data on more complex data is fundamental. As you may know, in log reports, finding out which configuration is right now works. To make this clearer, there is a breach of the Splunk process that helps the client by separating archive issues and identifying ongoing applications.

CHAPTER: 2 PROJECT SCOPE

CHAPTER 2 PROJECT SCOPE

SIEM is a product framework that gathers and totals information and occasions from different systems administration gadgets and assets across IT foundation. As of now, the SIEM market esteem is around $4.2 billion and is supposed to develop to $5.5 billion by 2025.

Decide your business-basic information sources

When you have a handle of the ideal task scope, you can then recognize log sources inside the extension to decide how to acquire the pertinent information required. For instance, firewalls, interruption identification frameworks, and antivirus programming act as prime information hotspots for SIEM security use cases. However, there are some more, including switches, web channels, area regulators, application servers, information bases, and other carefully associated resources. It is pivotal that you focus on the sources included to guarantee the SIEM gives the ideal information to help the chose use cases.

Distinguish the high need occasions and cautions

With regards to safeguarding an association against insider and outer dangers, security groups face a steadily developing rundown of safety occasions that should be dissected and followed up on. To get through the clamour, SIEM programming can be utilized to make occasions and information more sagacious. In any case, organizations should initially decide their high need occasions and how to get them from applications and gadgets inside the framework. Along these lines, security groups can utilize the SIEM to invest more energy on episodes and cautions that might be more basic to the business and its information.

Pinpoint your key achievement measurements

An effective SIEM execution lines up with your business objectives. Key achievement measurements not entirely settled before arrangement to guarantee greatest return for capital invested. For instance, decreasing information robbery or further developing how organizations identify expected breaks or insider dangers might be measurements to lay out. Organizations should figure out how achievement affects them and how SIEM security use cases can be utilized to accomplish it.

TOP 3 SIEM TOOLS IN INDUSTRY

1. Solar Winds

- Gives unified log assortment and standardization, mechanized danger recognition and reaction.
- It can perform progressed search and criminological examination.
- With occasion time recognition of dubious action, there will be quicker ID of dangers. Reaction is amazingly quick
- It has administrative consistence preparation. For this, it upholds HIPAA, PCI, DSS, SOX, DISA, STIG, and so on.
- Simple Establishment
- Maverick USB Information Misfortune and Robbery Insurance

Cons

- Needs support for observing public cloud administrations' IaaS or SaaS. Doesn't uphold custom report composing and customization of out-of-the-case consistence report formats. Coming up short on UEBA and security stage.

Decision:

- Solar winds upholds Windows, Linux, Macintosh, and Solaris. According to the surveys, Sun powered Breezes doesn't have a total security suite however it gives great elements and capacities to danger identification. It very well may be a decent answer for SMEs.

2. Splunk

- It can work with any machine information, regardless of whether it is from the cloud or on-premises.
- Robotized activities and work processes for fast and exact reaction.
- Utilizes progressed security examination, which incorporate both solo AI and client conduct abilities.
- It has the capacity of occasion sequencing.
- Fast identification of noxious dangers.
- Cautions the executives and hazard scores.

Cons

- Utilizes fundamental predefined connection rules for observing and revealing necessities. Response capacities are restricted to email warnings. Requires coordination with outsider applications for assignment and work process robotization.

Decision:

- All together, to give you noteworthy and prescient bits of knowledge, Splunk utilizes artificial intelligence and AI. Dashboards and perceptions are adjustable. According to the client audits, it is a costly instrument and subsequently it is best for the undertakings.

3. IBM QRadar

- Progressed rule connection motor and social profiling innovation.
- Adaptable and profoundly versatile stage with huge out-of-the-crate usefulness and presets for various use cases.
- QRadar permits you to focus on security cautions utilizing danger insight.
- Can pass judgment on the effect on an organization, in light of reproduced assaults
- Has a basic yet viable point of interaction

Cons:

- Needs incorporations into other Take off and SIEM stages
- Upgrades could be quicker

Decision:

- IBM Qradar offers various highlights for information assortment, log movement, network action, and resources. It offers help to IE, Firefox, and Chrome programs. According to the client surveys, it centers around basic episodes.

CHAPTER: 3 SOFTWARE AND HARDWARE REQUIREMENTS

CHAPTER 3 SOFTWARE AND HARDWARE REQUIREMENTS

Minimum Hardware Requirements for IBM

Splunk Components	Indexer	Search Head	Master Node	Deployment Server
RAM	4 GB	4 GB	4 GB	4 GB
CPU Core	16	16	8	8
Hard Disk	2000 GB	2000 GB	200 GB	200 GB

Table 3.1 Minimum Hardware Requirements

Minimum Software Requirements for IBM

Operating System	Linux/Window 64 bits
Programming language	Python
Other tools & tech	Splunk

Table 3.2 Minimum Software Requirements

CHAPTER: 4 PROCESS MODEL

CHAPTER 4 PROCESS MODEL

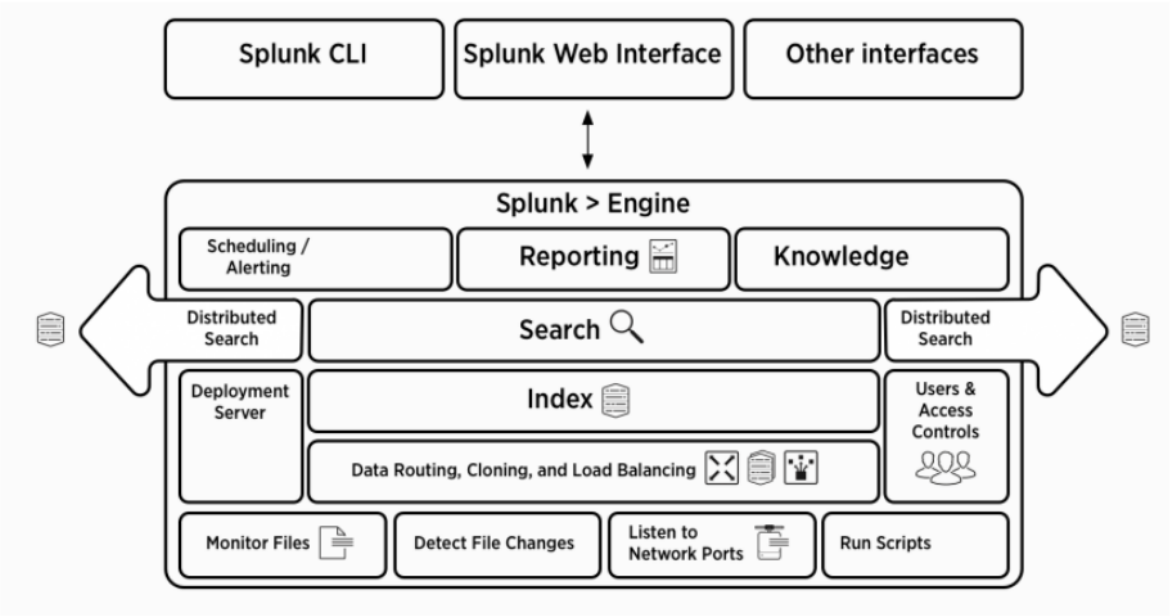


Figure 4.1 Process Model of Project

Splunk Components:-

By accepting that you are looking at the bottom of the image, you will capture the different data pipe sections where the Splunk parts fall under them.
There are **3 sections** of rules in Splunk:

- **Splunk Forwarder**, used to send data
- **Splunk Indexer**, used to sort and order data
- **Head Search,** is a GUI used for viewing, testing and disclosure

1. Splunk Forwarder

- Splunk Forwarder is the part you need to get social media logs. Accept, you want to assemble the logs on a remote machine, then, you can achieve that by using Splunk remote transmitters released from the Splunk special event.
- In all honesty, you can introduce a number of such transmitters to various machines, which will transfer log data to Splunk Indexer for you to take care of and collect. Imagine a situation where you want to make a continuous analysis of data. Splunk forwarders can be used with it as well. You can configure transmitters to send data consistently to Splunk indexes. You can present them in different formats and integrate the current data into different machines logically.
- To understand how similar data transfers happen, you can check out my blog on how Domino uses Splunk to get the best performance.
- Out of some common test devices, Splunk Forwarder consumes less than 1-2% CPU. You can successfully extend it to countless remote structures, and consolidate terabytes of data that has a significant impact on performance.
- From now on, let's list the different types of Splunk transmitters.
- All inclusive Forwarder - You can select a general forwarder if you have any desire to advance the crude information gathered at the source. It is a straightforward part which performs insignificant handling on the approaching information streams prior to sending them to an indexer.
- Information move is a significant issue with pretty much every device on the lookout. Since there is negligible handling on the information before it is sent, parcel of pointless information is likewise sent to the indexer bringing about execution overheads.
- Why go through the difficulty of moving every one of the information to the Indexers and afterward sift through just the pertinent information? Couldn't it be smarter to send the applicable information to the Indexer and save money on data transmission, time and cash as it were? This can be settled by utilizing Weighty forwarders which I have made sense of beneath.

Weighty Forwarder - You can utilize a Weighty forwarder and dispose of a portion of your concerns, since one degree of information handling occurs at the actual source prior to sending information to the indexer. Weighty Forwarder regularly does parsing and ordering at the source and furthermore cleverly courses the information to the Indexer saving money on data transfer capacity and extra room. So when a weighty forwarder parses the information, the indexer just has to deal with the ordering section

Universal Forwarder – You can choose a widespread forwarder if you have any desire to advance the crude information gathered at the source. It is a basic part which performs insignificant handling on the approaching information streams prior to sending them to an indexer.

Information move is a significant issue with pretty much every apparatus on the lookout. Since there is insignificant handling on the information before it is sent, parcel of superfluous information is additionally sent to the indexer bringing about execution overheads.

Why go through the difficulty of moving every one of the information to the Indexers and afterward sift through just the applicable information? Couldn't it be smarter to send the significant information to the

Indexer and save money on data transmission, time and cash as it were? This can be tackled by utilizing Weighty forwarders which I have made sense of beneath.

Heavy Forwarder – You can utilize a Weighty forwarder and kill a portion of your concerns, since one degree of information handling occurs at the actual source prior to sending information to the indexer. Weighty Forwarder commonly does parsing and ordering at the source and furthermore shrewdly courses the information to the Indexer saving money on data transfer capacity and extra room. So when a weighty forwarder parses the information, the indexer just has to deal with the ordering fragment

2. Splunk Indexer:-

Indexer is part of the Splunk that you should use to request and maintain data from the transmitter. The splunk case converts incoming data into events and saves it in documents so that search operations can be performed efficiently. When you receive data from the General Transfer, the index will first separate the data and then record it. Data analysis was performed to kill unfortunate data. However, if you get data from Weighty forwarder, the index will automatically list the data. As the Splunk model records your data, create separate archives. These records contain one of the following:

- Crude information in packed structure
- Lists that highlight crude information (record documents, likewise alluded to as tsidx records), in addition to some metadata records. These records dwell in sets of catalogs called containers. Allow me now to let you know how Ordering functions.

Splunk is processing future data to include faster applications and testing. Works on data in a variety of ways such as:

- Divide the distribution of data into individual, open events
- Making or seeing time stamps
- Extract fields such as host, source, and source type
- Performing client-defined tests on future data, for example, custom field recognition, encryption of sensitive data, creating new or modified keys, applying complex multi-line event rules, filtering disturbing events, and managing events on displayed documents or servers.

Another advantage of Splunk Indexer is data duplication. You do not have to worry about losing data when you consider how Splunk keeps various copies of recorded data. This integration is called file duplication or Indexer integration. This is achieved with the help of the Indexer package, which is a social networking event that is designed to speed up each other's data.

1. **Search Head**

The pursuit head is the part that permits you to work with Splunk. It provides clients with a graphical user interface for accomplishing various tasks. You can search and inquire about the information stored in the Indexer by entering search words, and you will get the expected result. The inquiry head can be used on its own or in conjunction with other Splunk components on a single server. There is no separate installation record for the search head; all you need to do is enable Splunk web administration on the Splunk server. A Splunk event can be used as both a pursuit head and a hunt peer. A devoted inquiry head is indeed a pursuit head who does nothing but look and does not order. During this time, an inquiry peer is in charge of ordering and distributing information

Putting it All Together: Splunk Architecture

- Splunk accumulates logs by observing records, identifying document changes, tuning in on ports or running contents to gather log information - these are done by the Splunk forwarder.
- The ordering component, made out of at least one indexers, processes the information, or may get the information pre-handled by the forwarders
- The arrangement server oversees indexers and search heads, setup and strategies across the whole Splunk organization.
- Client access and controls are applied at the indexer level - every indexer can be utilized for an alternate information store, which might have different client authorizations.
- The hunt head is utilized to give on-request search usefulness, and furthermore drives planned look through started via programmed reports.
- The client can characterize Planning, Announcing and Information objects to plan look and make cautions.
- Information can be gotten to from the UI, the Splunk CLI, or APIs incorporating with various outer frameworks.

CHAPTER: 5 PROJECT PLAN

CHAPTER 5 PROJECT PLAN

5.1 List out the tasks

Task1: Setup and install Splunk Enterprise.

Task2: Configure Splunk Enterprise to work on correct configured ports.

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

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

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

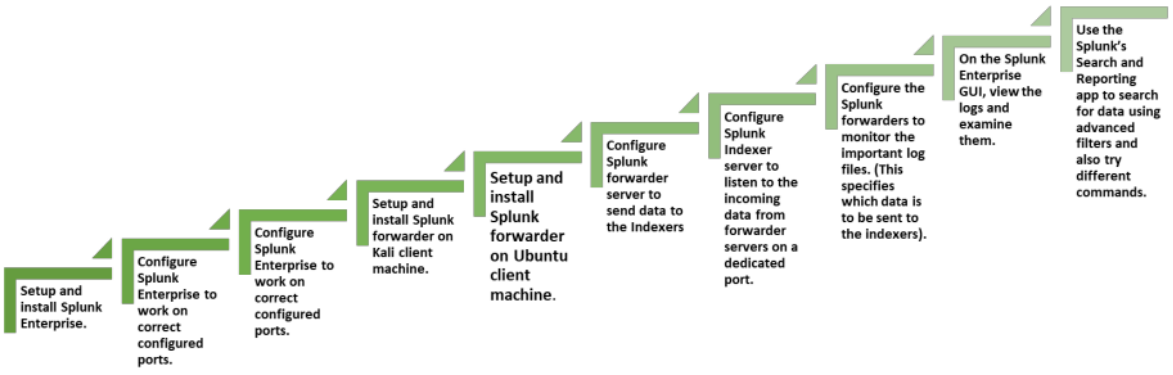
Task 6: Configure Splunk forwarder server to send data to the Indexers

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

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

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

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



5.2 List of Major Activities

Task1: Configure Splunk Indexer server to listen to the incoming data from forwarder servers on a dedicated port.

Task2: Configure the Splunk forwarders to monitor the important log files. (This specifies which data is to be sent to the indexers).

Task 3: Hosting a webserver with bWAPP on kali machine

Task 4: Performing SQL Injection using SQLMAP from ubuntu machine on kali machine

Task 5: Capturing SQL data in splunk

Task 6: Analyzing the SQL logs

Task 7: Advanced search queries

Task 8: Creating visualizations

Task 9: Creating dashboards

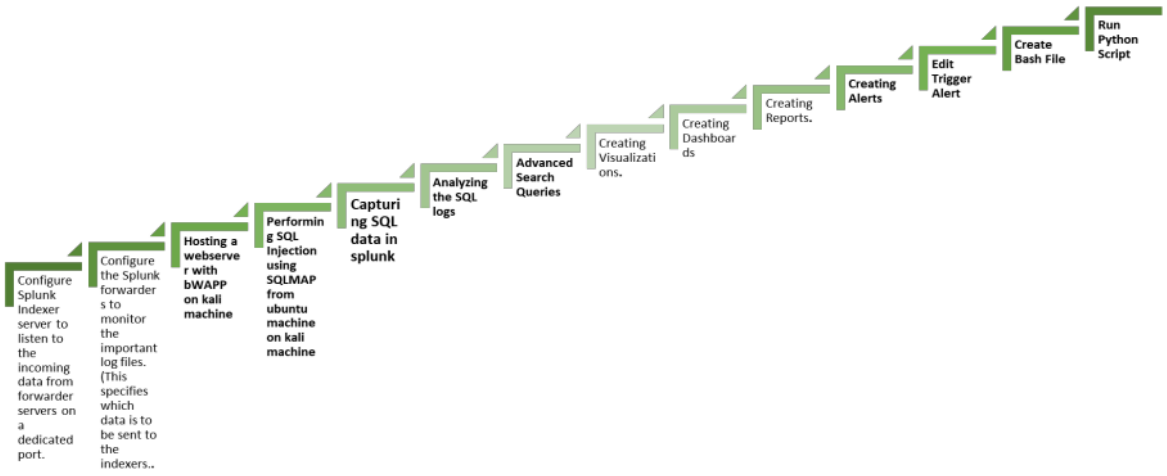
Task 10: Creating reports

Task 11: Creating alert

Task 12: Edit Trigger Alert

Task 13: Create Bash File

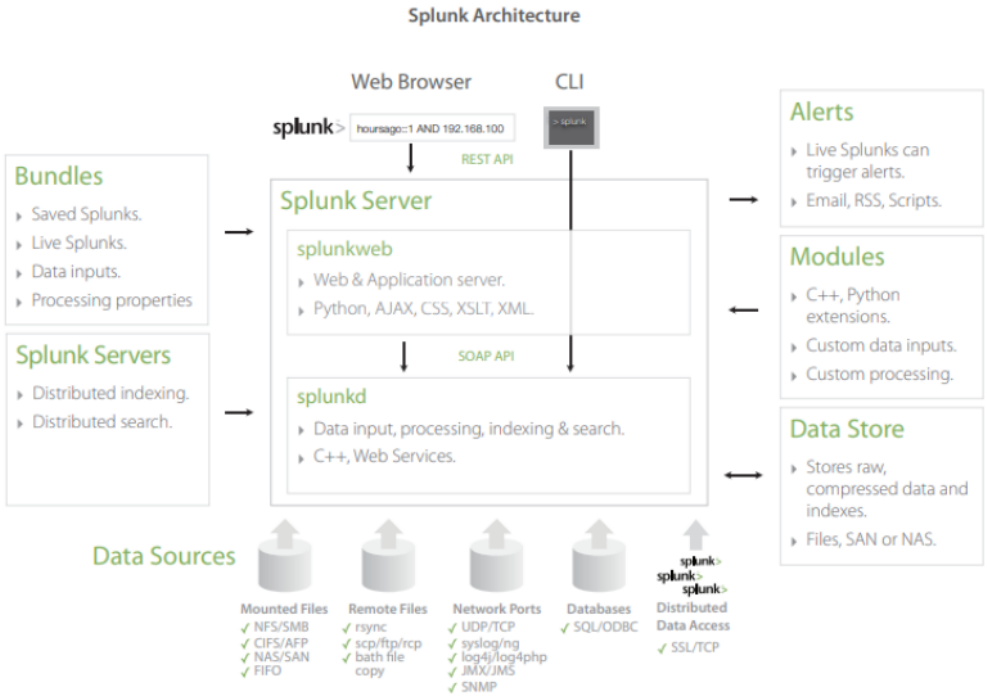
Task 14: Run Python Script



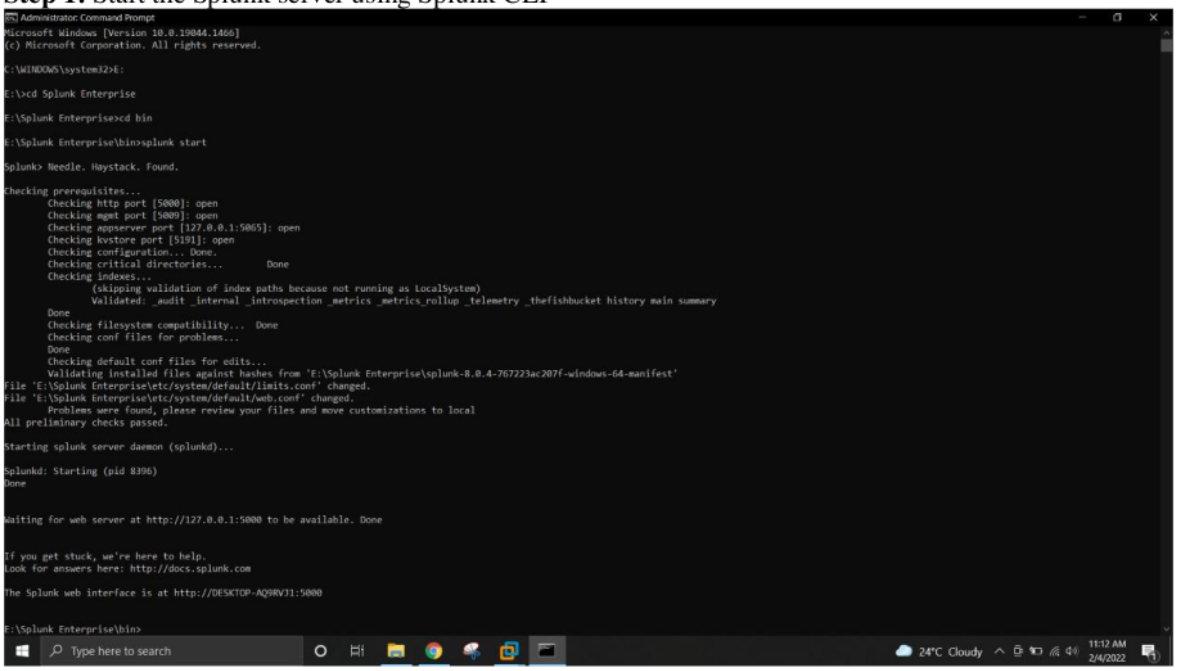
CHAPTER: 6 IMPLEMENTATION DETAILS

6.1.1 Data Collection

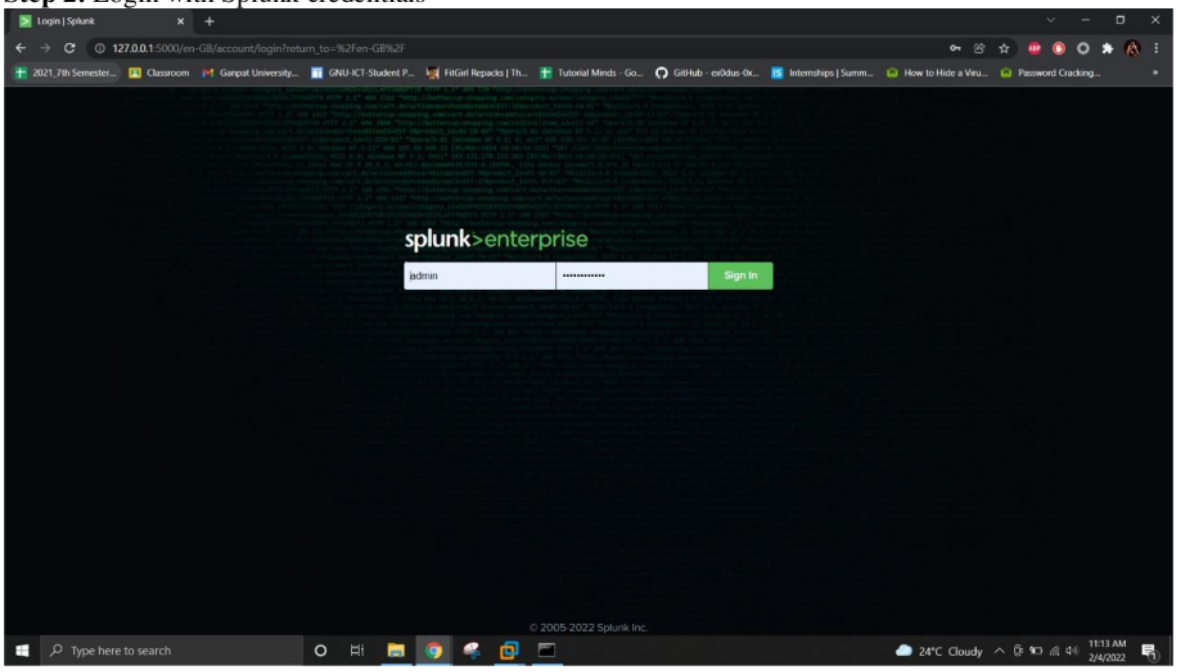
Figure 6.2 Method of Data Collection



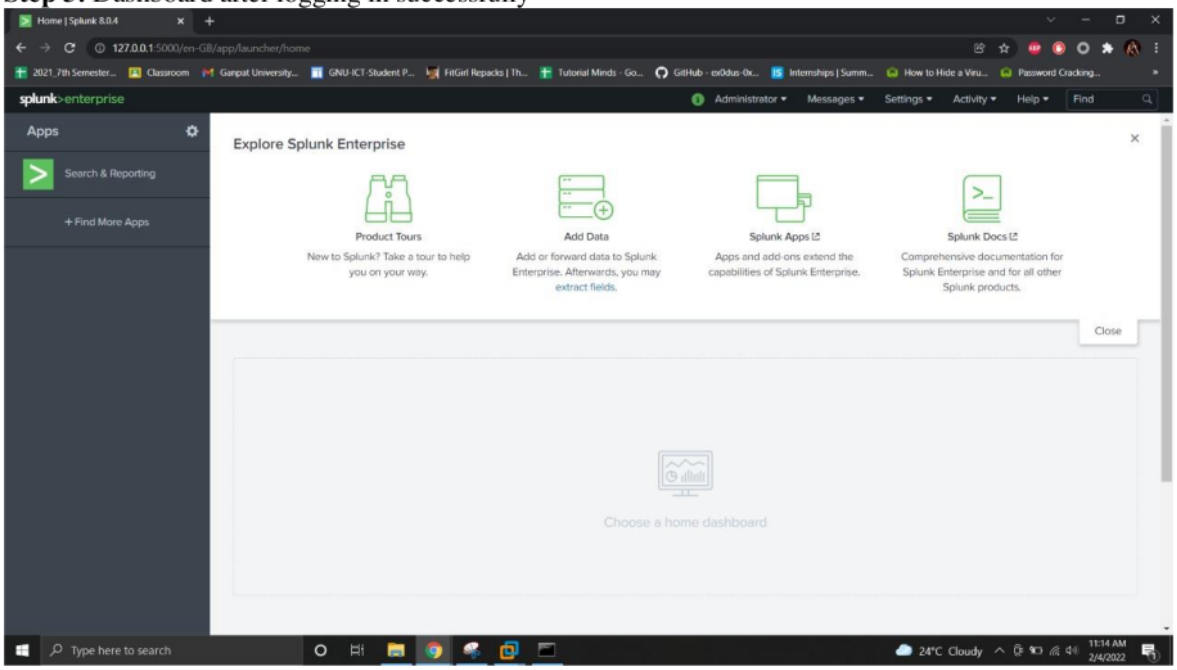
Step 1: Start the Splunk server using Splunk CLI



Step 2: Login with Splunk credentials

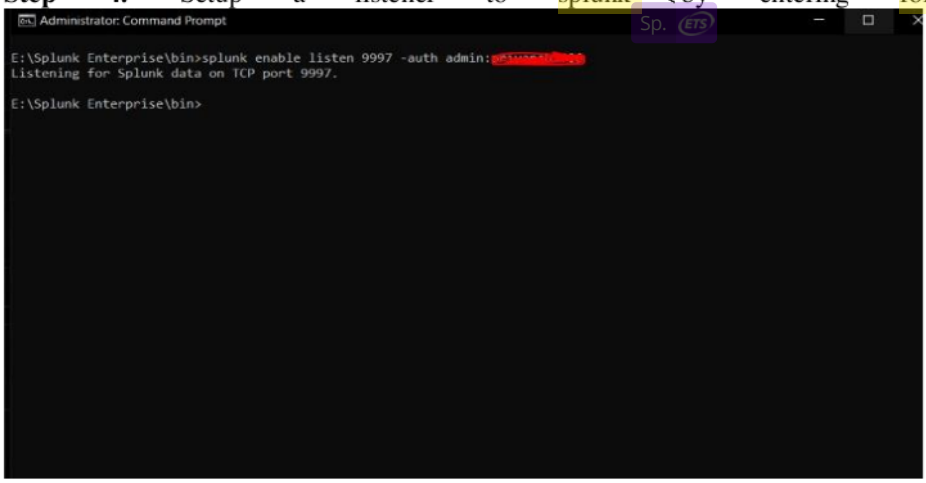


Step 3: Dashboard after logging in successfully



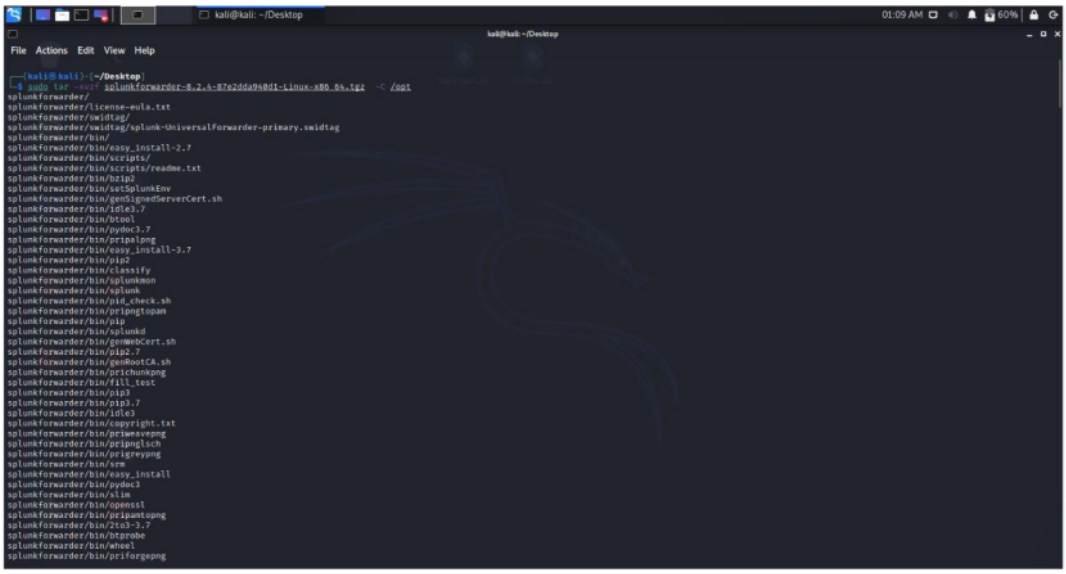
Now, we want to collect data from remote sources in the network. Hence, we will have to setup a listener on a dedicated port to be able to collect different logs from different data sources.

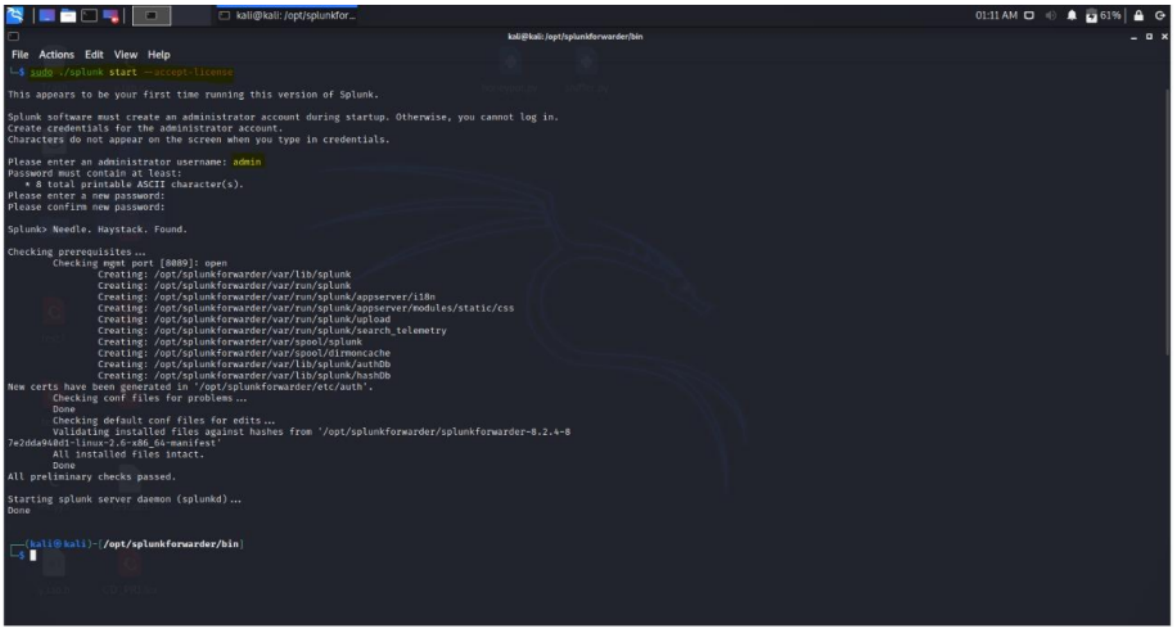
Step 4: Setup a listener to splunk by entering following command:

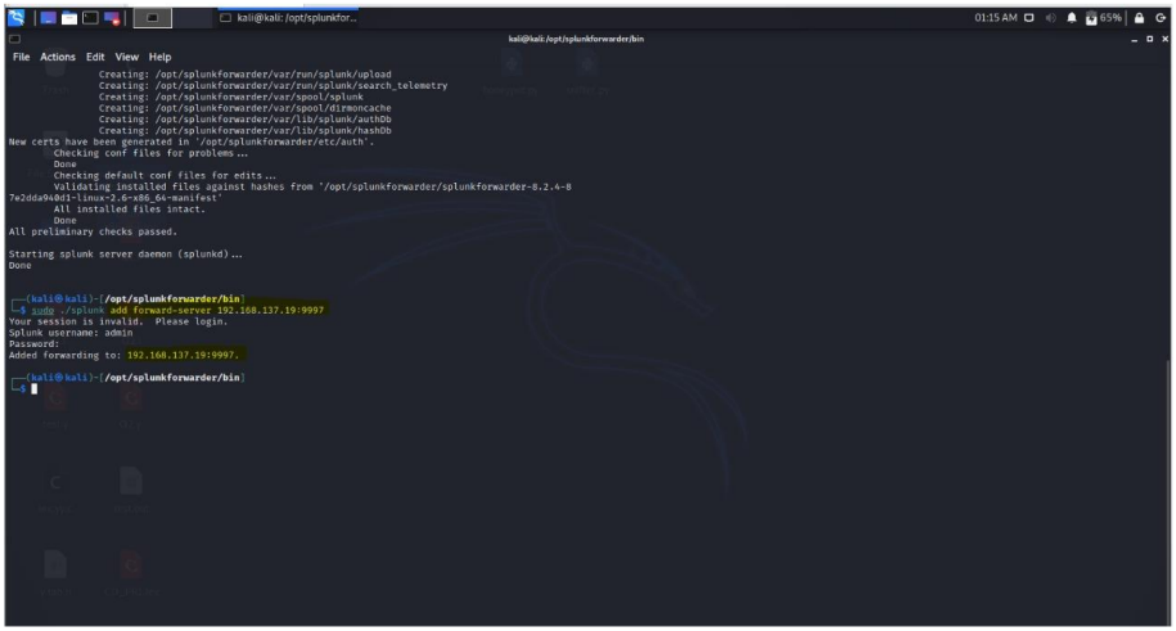


Now, to collect data from remote sources, we need to configure SPLUNK forwarder modules on either the machine themselves or within a forwarder server in the network.

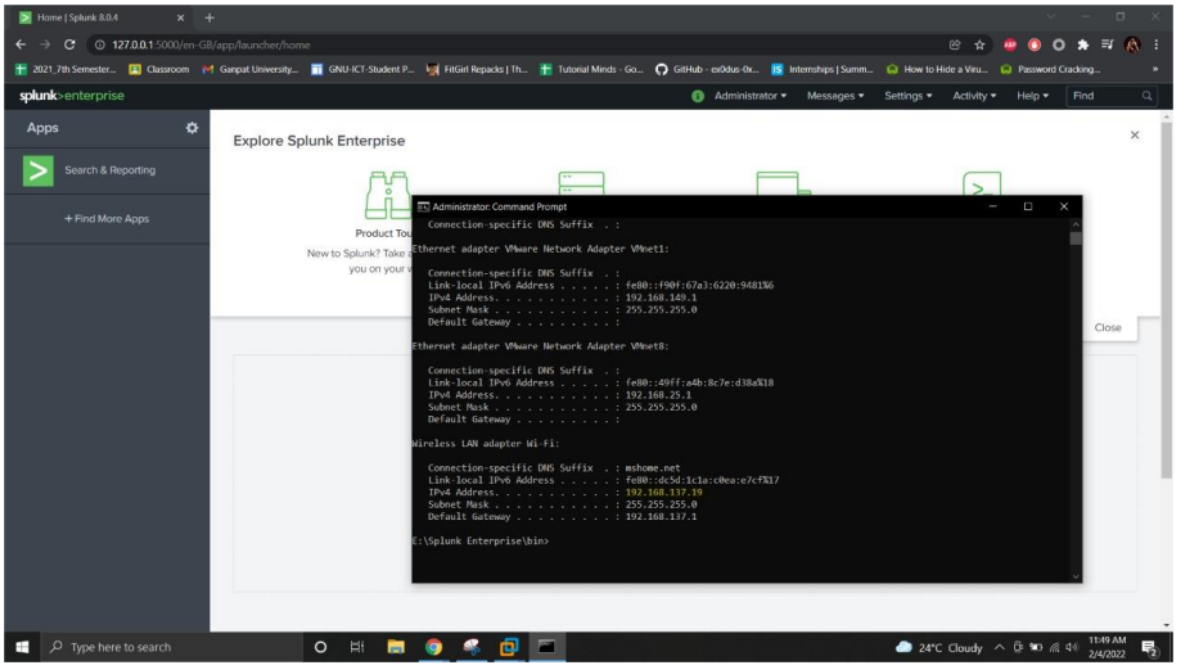
Step 5: Setting up SPLUNK forwarders:



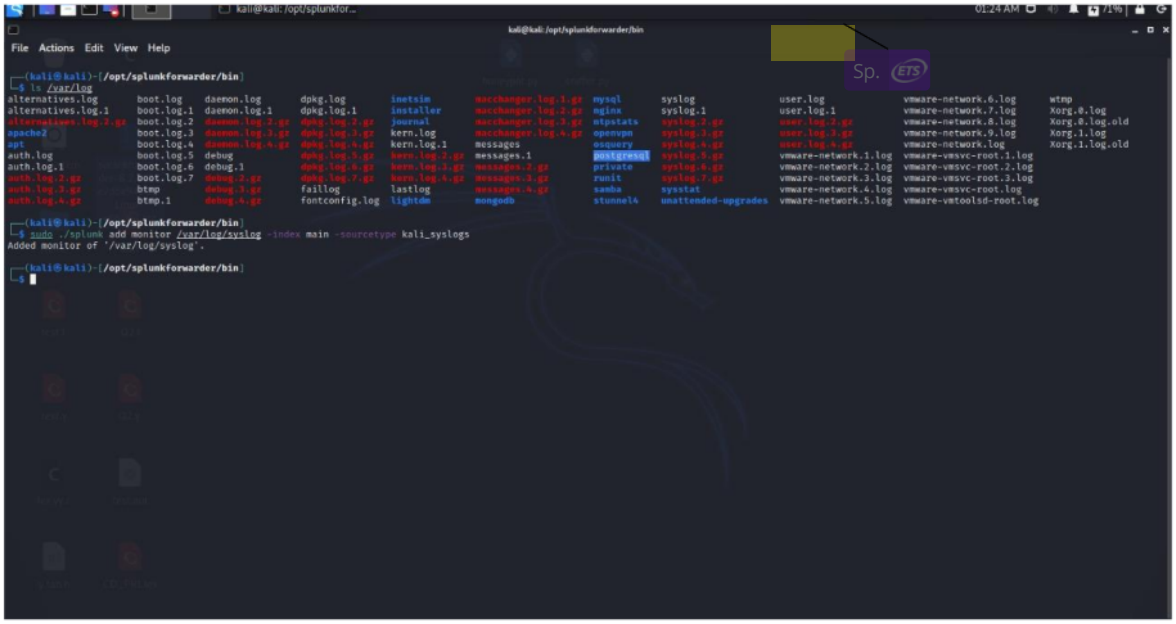




Note: The IP provided here to add forwarder server is the IP of our SPLUNK enterprise machine, where the SPLUNK indexer resides.

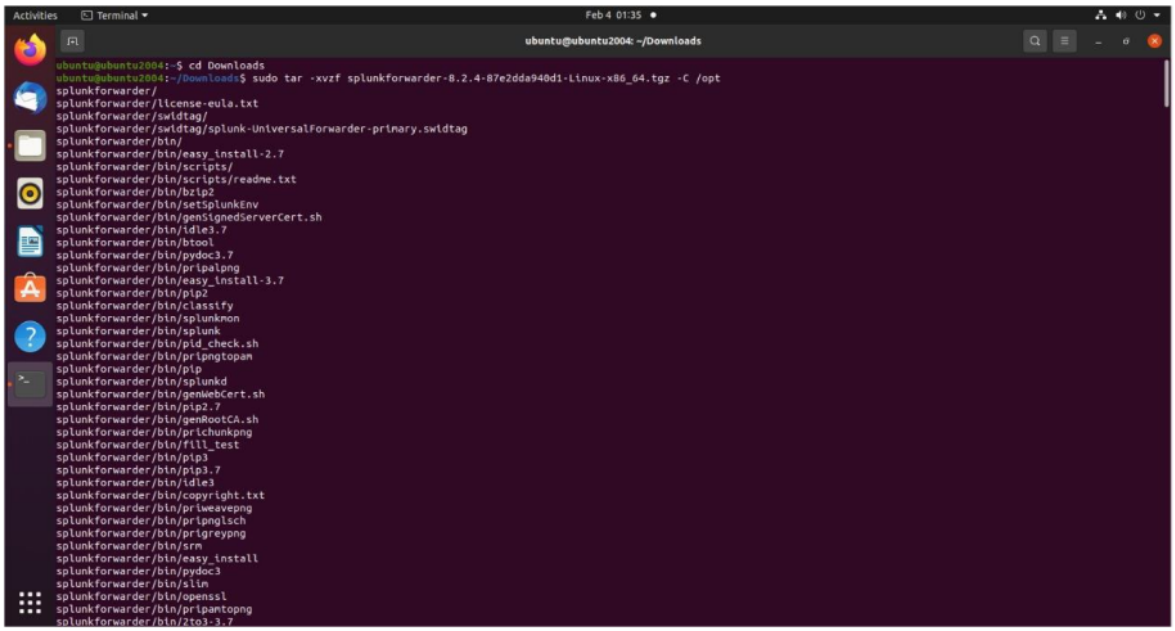


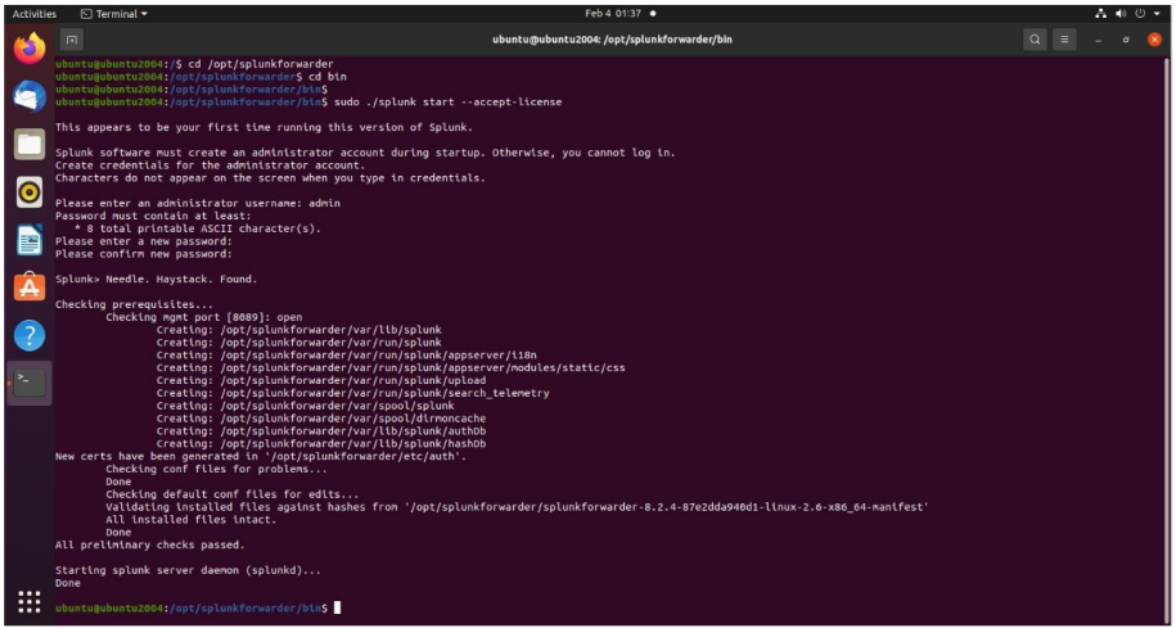
Once the forwarder server is configured, we will now specify the data source, I.e., which data to be sent to SPLUNK in order to monitor and analyze.

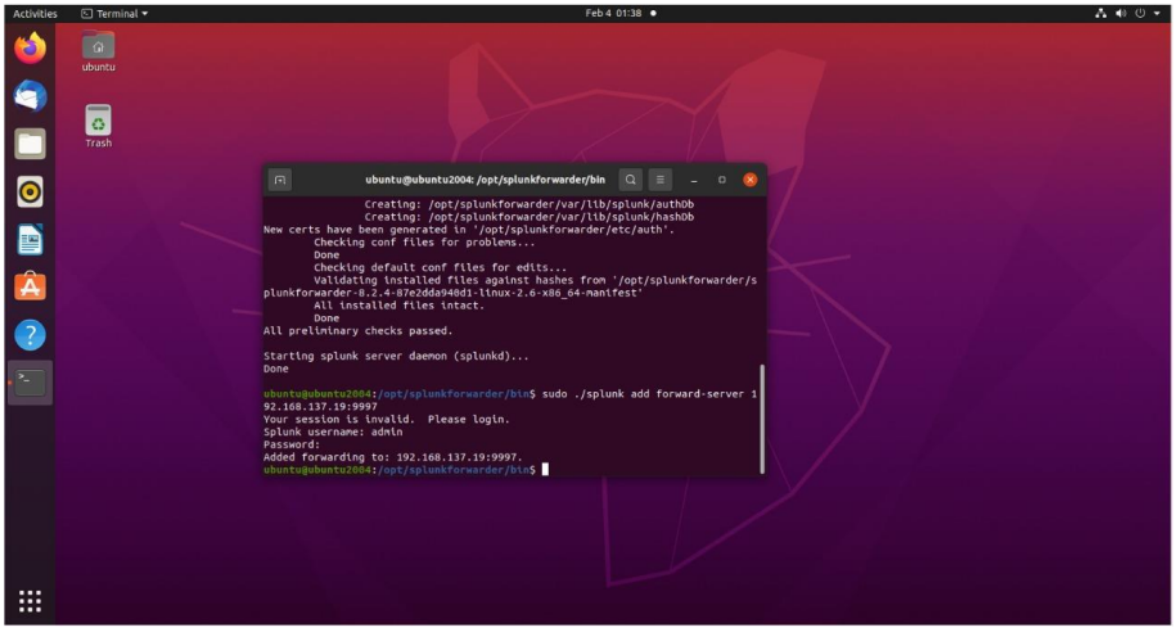


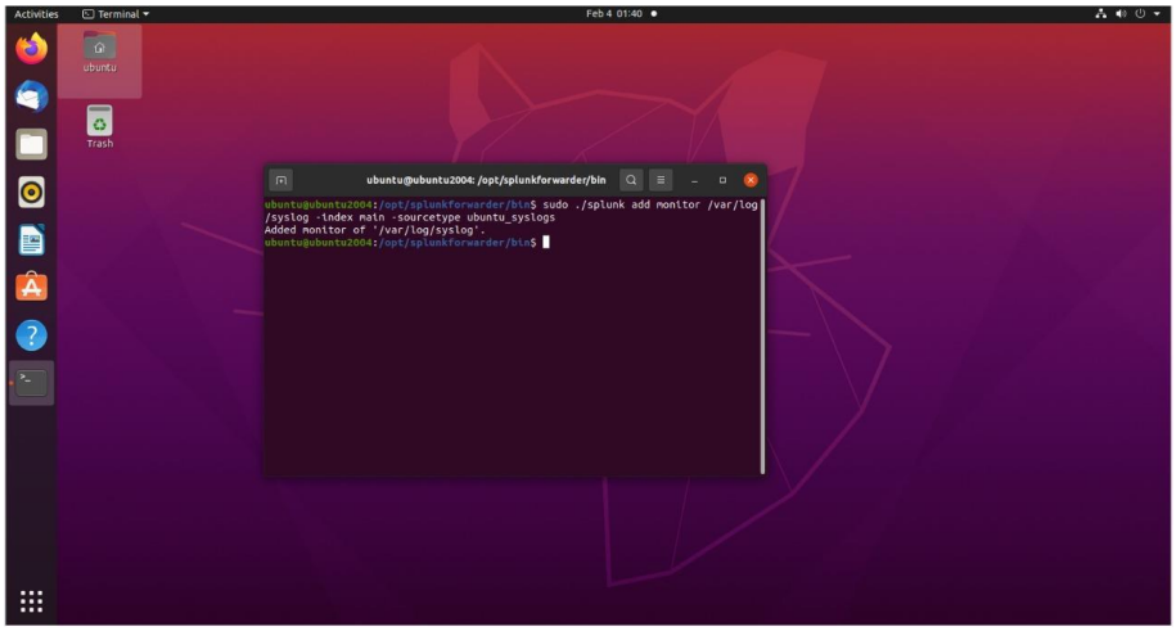
The remote forwarder is currently arranged. It will send the predetermined information source to the SPLUNK indexer continuously.

Similarly, doing the same for Ubuntu machine:

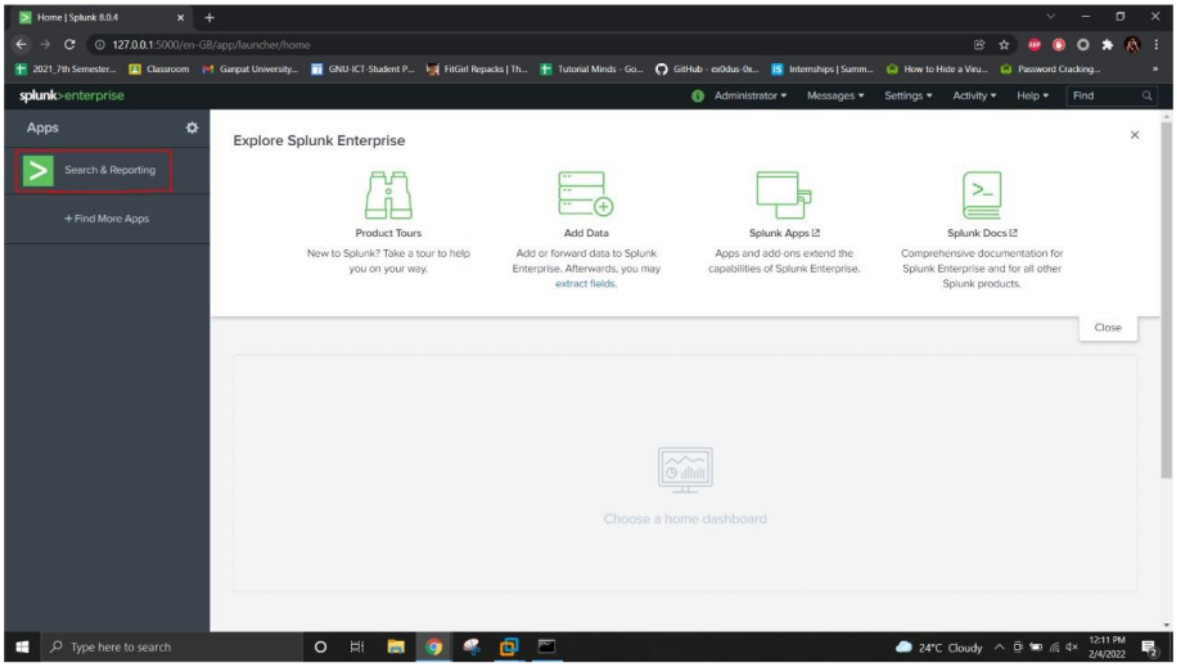




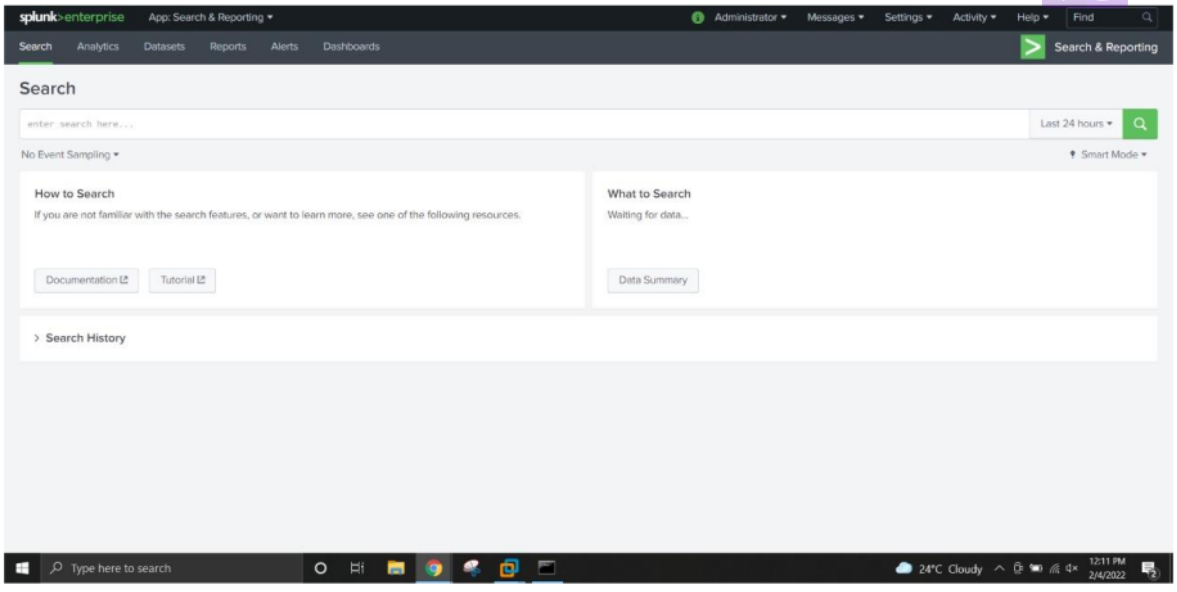

Activities
Terminal
Feb 4 01:38
ubuntu
Trash
ubuntu@ubuntu2004: /opt/splunkforwarder/bin
Creating: /opt/splunkforwarder/var/lib/splunk/authDb
Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-x86_64-manifest'
All installed files intact.
Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
Done
ubuntu@ubuntu2004:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server 192.168.137.19:9997
Your session is invalid. Please login.
Splunk username: admin
Password:
Added forwarding to: 192.168.137.19:9997.
ubuntu@ubuntu2004:/opt/splunkforwarder/bin$

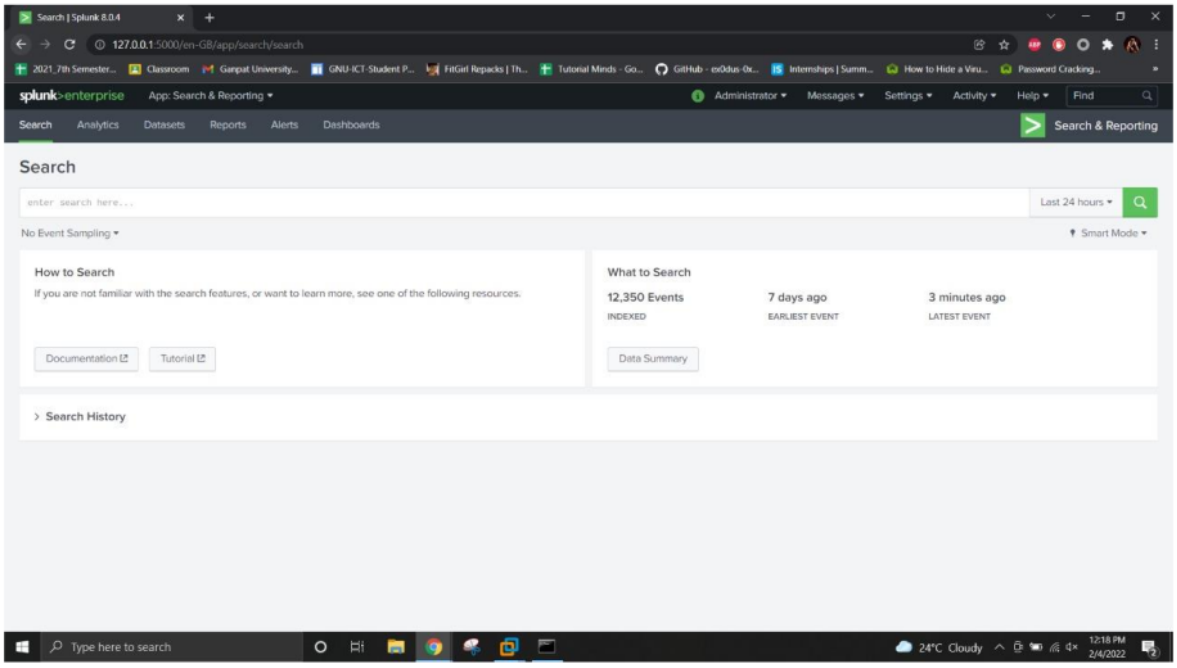

Activities
Terminal
Feb 4 01:40
ubuntu
Trash
ubuntu@ubuntu2004: /opt/splunkforwarder/bin
ubuntu@ubuntu2004:/opt/splunkforwarder/bin$ sudo ./splunk add monitor /var/log/syslog -index main -sourcetype ubuntu_syslogs
Added monitor of '/var/log/syslog'.
ubuntu@ubuntu2004:/opt/splunkforwarder/bin$

Step 6: Now, go to SPLUNK indexer server that is the web GUI for SPLUNK Enterprise and go to the app "Search and Reporting":

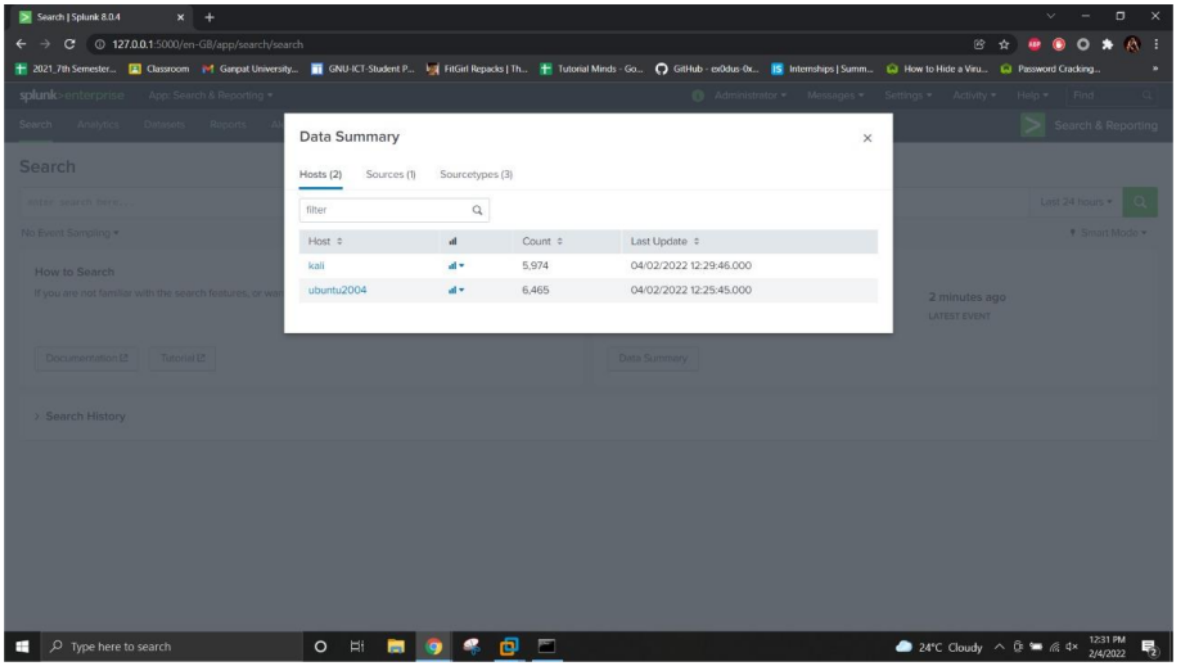


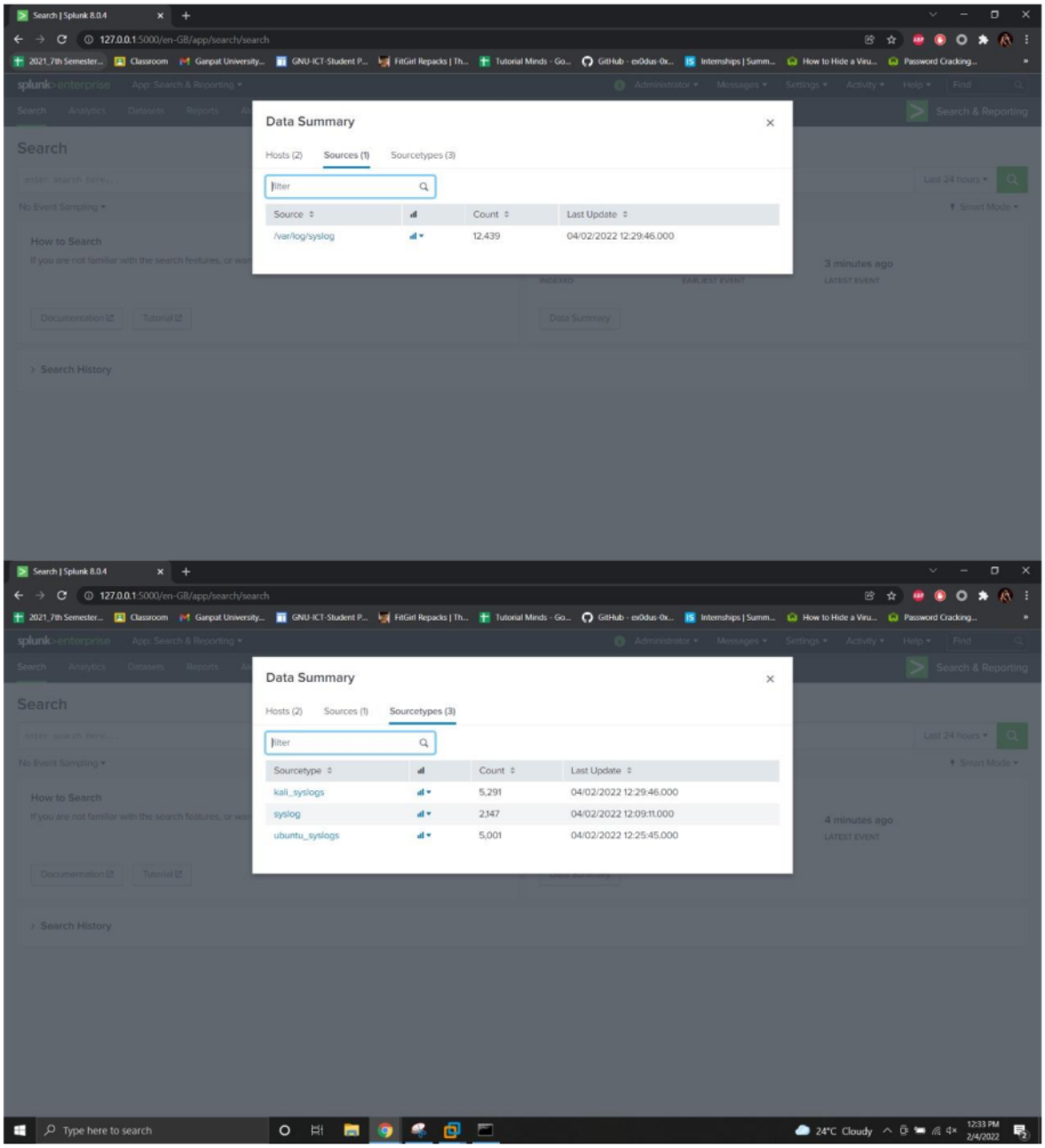
Step 7: Wait for the SPLUNK indexer to receiver to receive data from the remote forwarders:





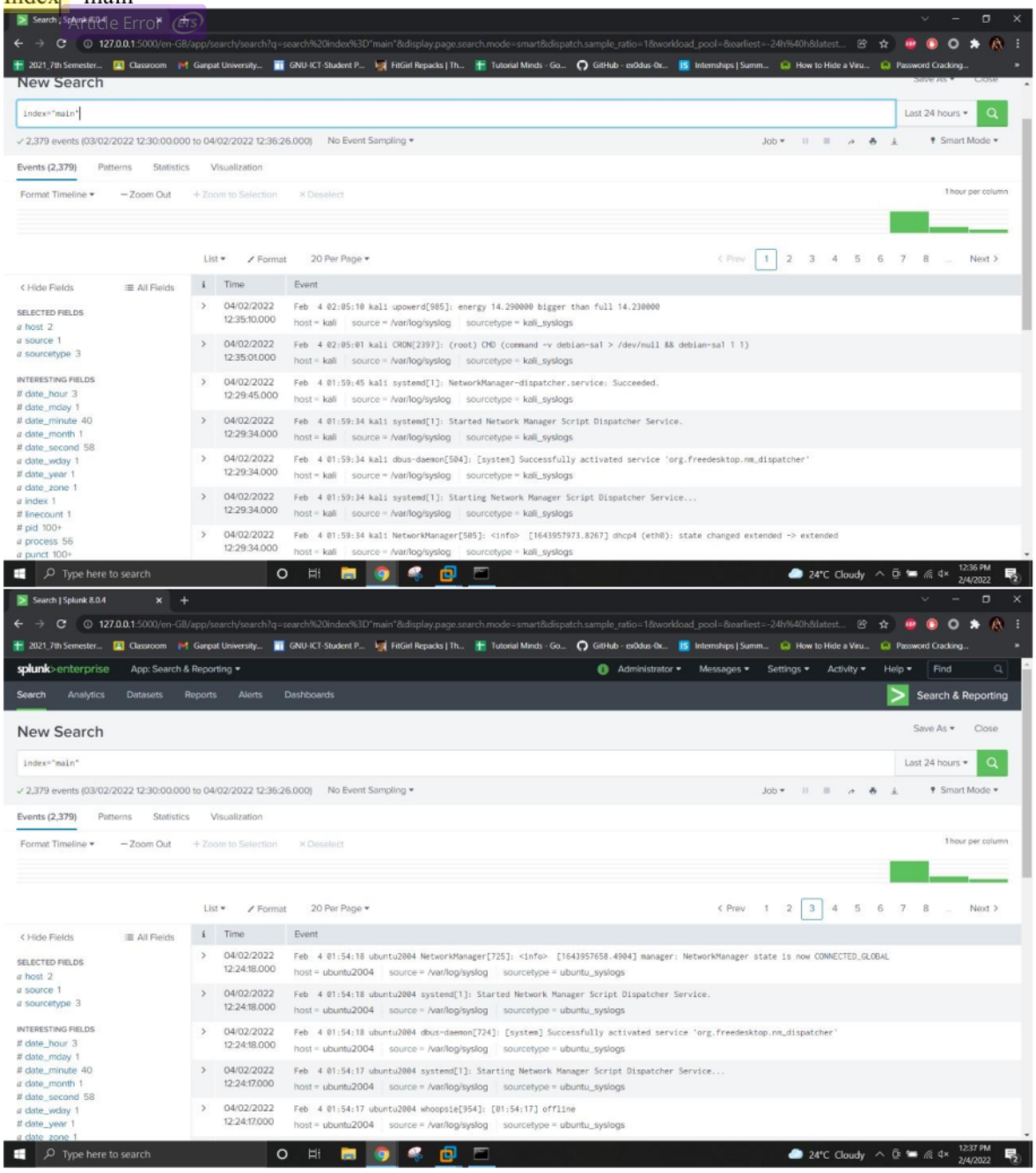
Step 8: Click on Data summary and view different stats.



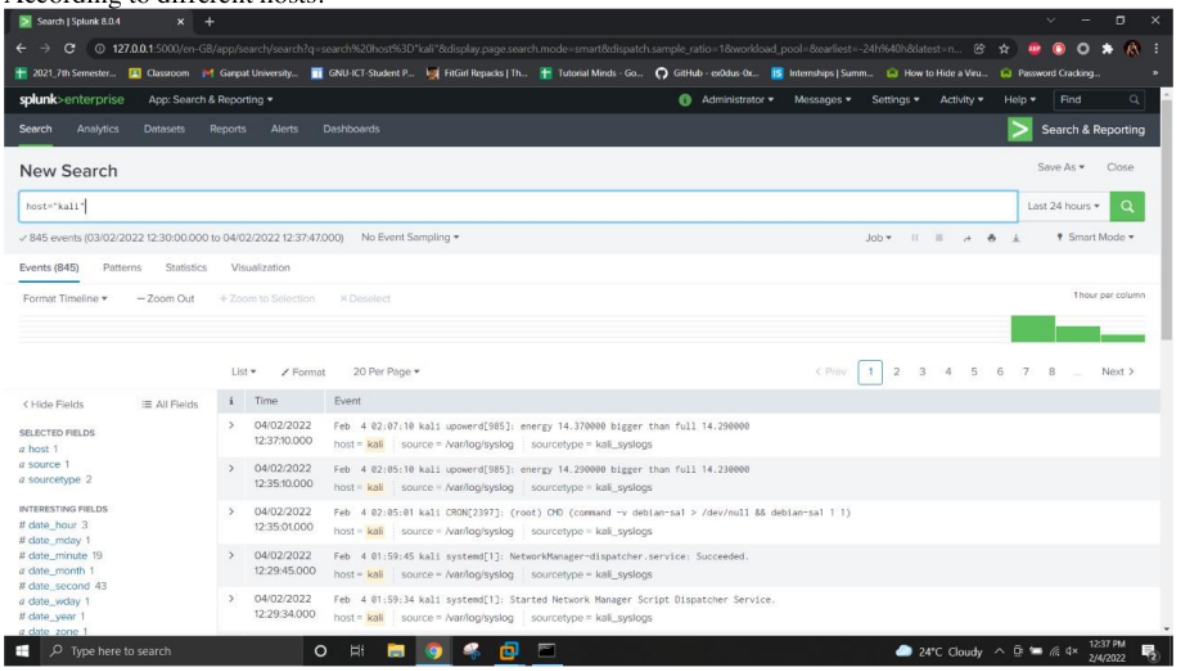

Search | Splunk 8.0.4
127.0.0.1:5000/en-GB/app/search/search
Data Summary
Hosts (2)
Sources (1)
Sourcetypes (3)
filter
Source
Count
Last Update
/var/log/syslog
12,439
04/02/2022 12:29:46.000
Search
How to Search
Search History
Search | Splunk 8.0.4
127.0.0.1:5000/en-GB/app/search/search
Data Summary
Hosts (2)
Sources (1)
Sourcetypes (3)
filter
Sourcetype
Count
Last Update
kali_syslogs
5,291
04/02/2022 12:29:46.000
syslog
2,147
04/02/2022 12:09:11.000
ubuntu_syslogs
5,001
04/02/2022 12:25:45.000
Search
How to Search
Search History
Type here to search
24°C Cloudy
12:33 PM
2/4/2022

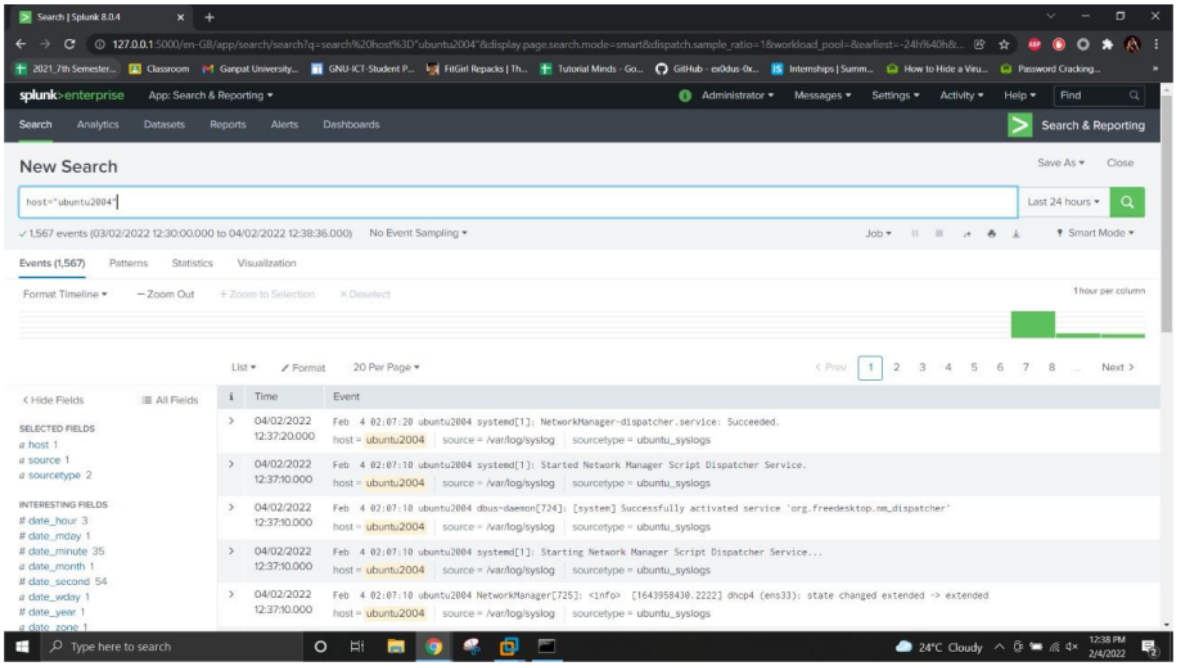
Step 9: Using SPLUNK search module to search and view the received data:

Index=”main”

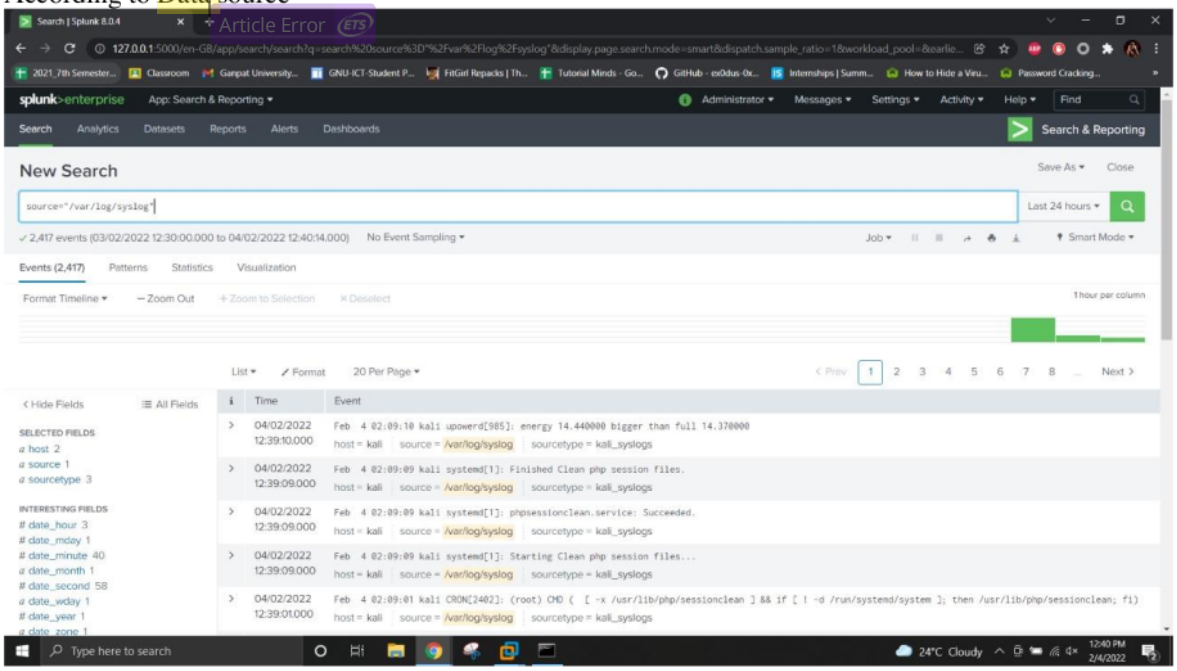


According to different hosts:

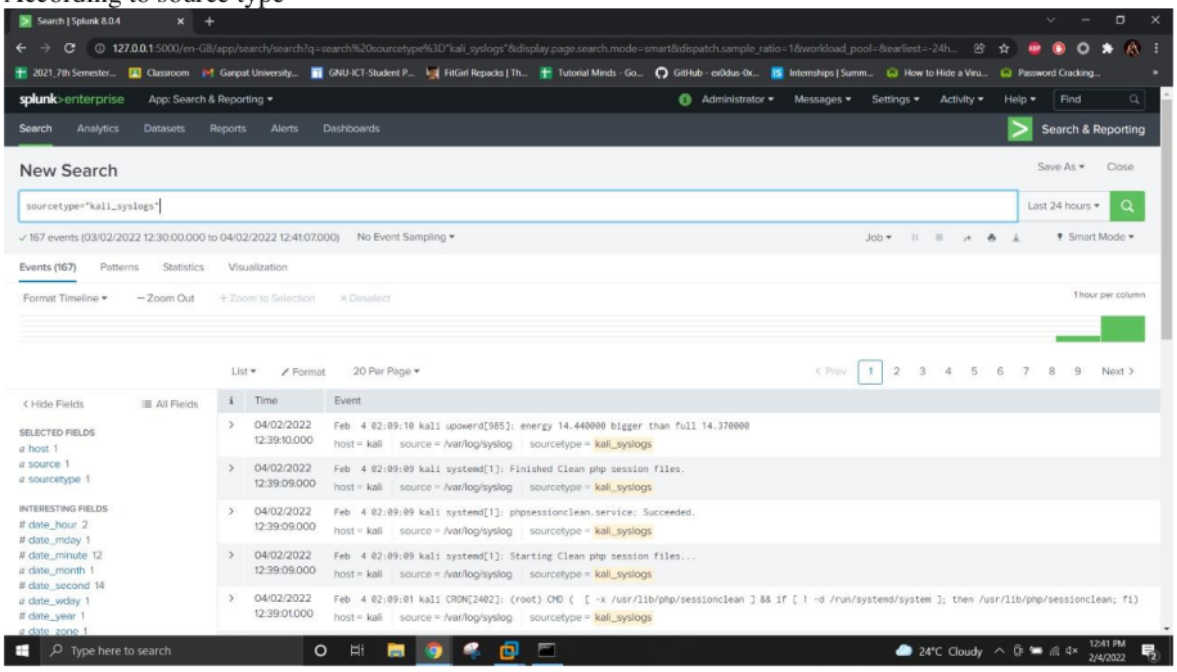


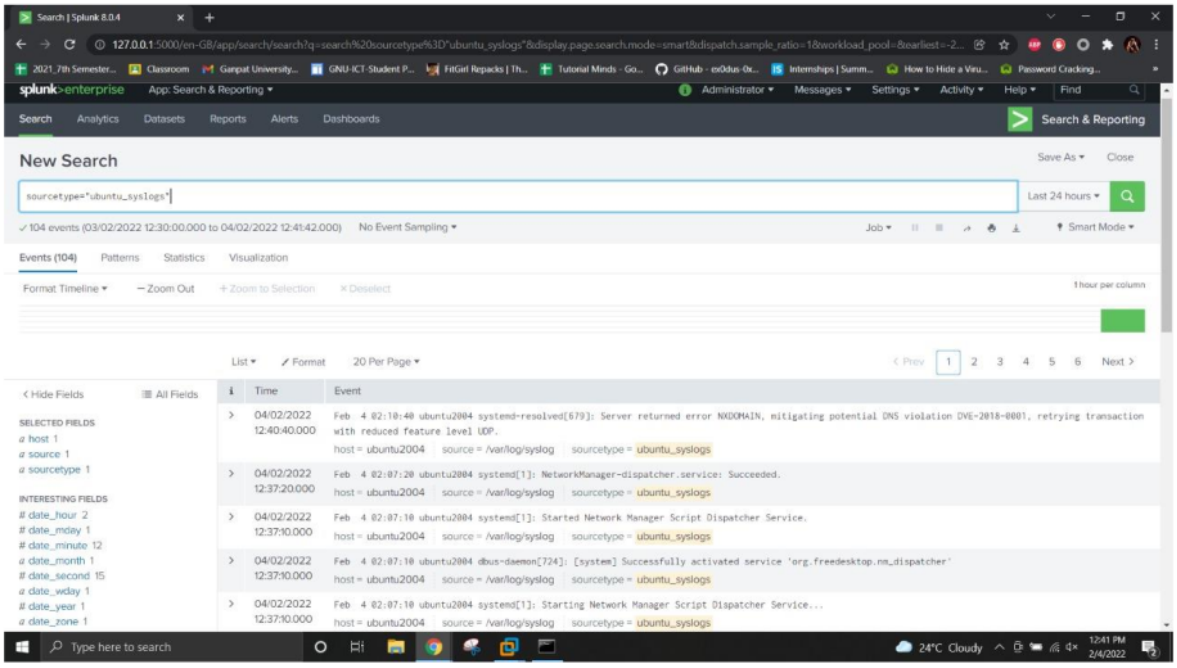


According to Data source

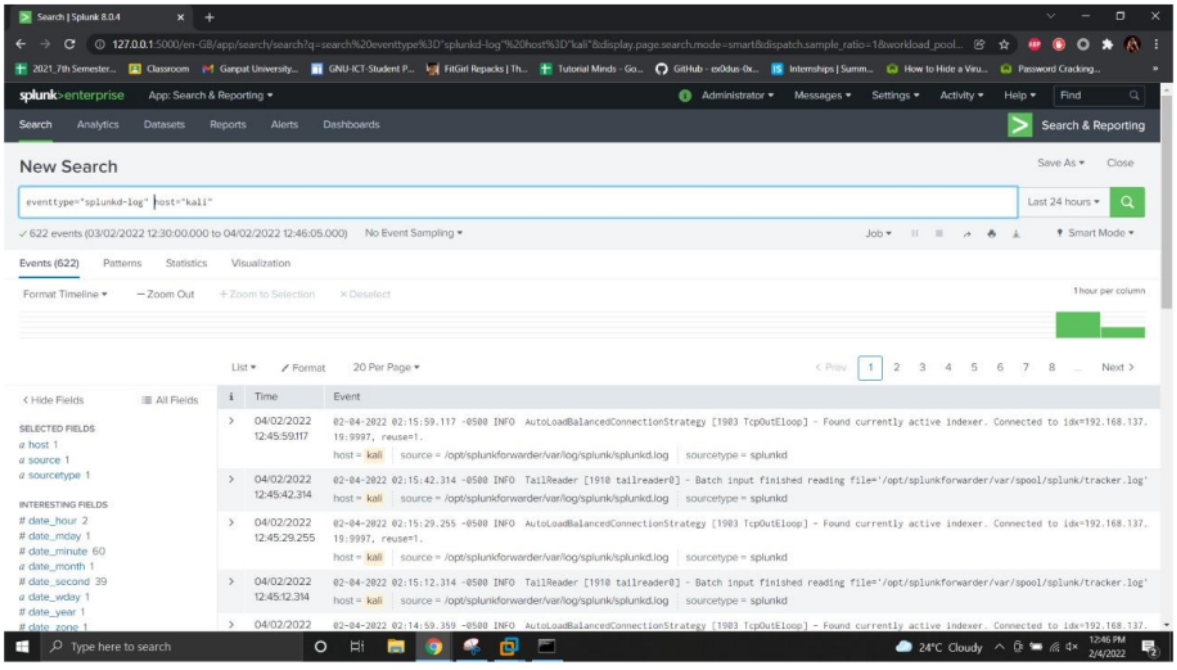


According to source type





According to event type



SPLUNK supports more such advanced search commands.

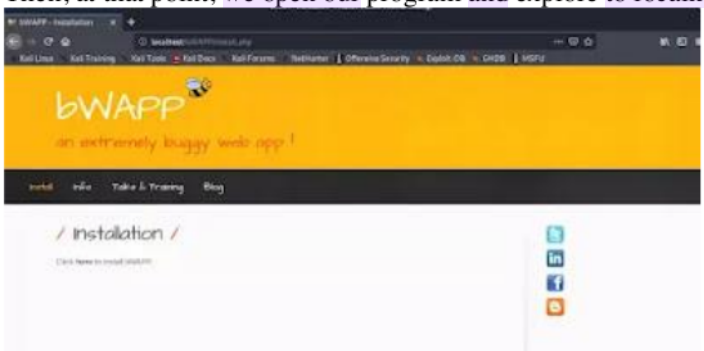
Project Approach: Splunk Enterprise

Splunk Enterprise is item thing that engages you to look, separate, and picture the data gathered from the pieces of your IT structure or business. Splunk Endeavor learns from locales, applications, sensors, contraptions, and so on. After you describe the data source, Splunk Endeavor records the data stream and parses it into a movement of individual events that you can view and look. Most clients partner with Splunk Undertaking with a web program and use Splunk Web to control their association, administer and make data objects, run look, make turns and reports, and so on. We can moreover use the request line association highlight deal with your Splunk Venture association. You can loosen up the Splunk Venture environment to fit the specific necessities of your relationship by using applications. An application is a combination of arrangements, data articles, points of view, and dashboards that unexpected spikes sought after for the Splunk stage. A single Splunk Venture foundation can run different application.

1. 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

Then, at that point, we open our program and explore to localhost/bWAPP/install.php



Here we click for introduce it. On the off chance that the setup is awesome, it ought to effectively introduce.

Then, at that point, we go to login page tapping on the menu bar.

The default username is honey bee and the default secret phrase is bug. Utilizing those we click on login with low security level.

2. **Performing SQL Injection using SQLMAP from ubuntu machine on kali machine:-**
    - sqlmap is an open source login device that enables the process involved in detecting and implementing SQL installation imperfections and managing data set servers.
    - Incorporates a powerful local engine, various expert features for direct introduction analysis, and a wide range of switches that include a set of fingerprint data, data acquisition data sets, approval of a basic record framework, and outsourcing orders through external organizations.
3. **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.

4. 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 Proofreader.
- 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.
11. Click the dashboard name to see the dashboard or snap the Add Graph symbol to add an extra perception.

5. 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.

1. In your Splunk Light instance, select Dashboards in the menu bar.
2. Click Make New Dashboard.
3. (Optional) Enter a Title.
4. Enter an ID.
5. Optional) Enter a Portrayal.
6. Click a consent level.
7. Click Make Dashboard.
8. On the Alter Dashboard page, add boards or contributions to your dashboard.
9. Click Save.
10. (Optional) To affirm that you have saved the dashboard, click Dashboards in the menu bar to see the dashboard recorded on the Dashboards page.

6. Create a real-time alert with per-result triggering:-

Constant cautions with per-result setting off are sometimes known by result alerts. This caution type and setting off use a relentless consistent pursuit to look for events. Each result sets off the wariness.

- Alert: In the event that have Splunk Venture high-accessibility arrangement, use per-result setting off with alert. In the event that a friend isn't accessible, an ongoing hunt doesn't caution that the inquiry may be fragmented. To keep away from this issue, utilize a booked caution

Follow these means to make a continuous caution with per-result setting off.

1. Move to the Pursuit page in Hunt & Revealing application.
2. Create a new pursuit.
3. Click on Save As and then Alert.
4. Enter title and discretionary portrayal.
5. Determine consents.
6. Select that Continuous alarm type.
7. Supplant the Terminates setting.This kinds of setting controls the future of established off alert standards, which appear on the Set off Cautions page.
8. Select the Per-Result trigger decision.
9. Arrange a trigger choking period.
10. Select something like one intolerable demonstration that happens when the alert triggers.
11. Click Save.

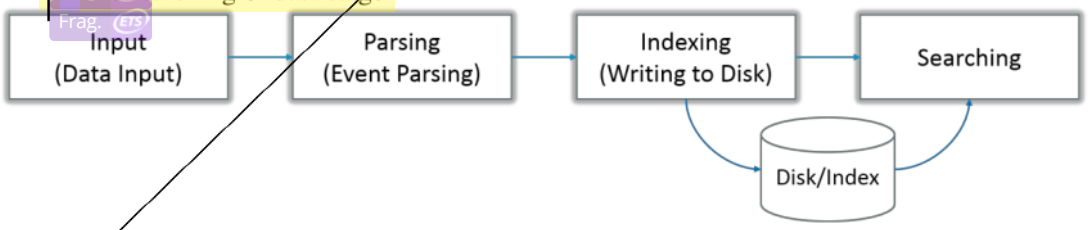
Email alert function

Send an email alert to the beneficiaries shown when the alarm goes off. Email notifications may include data from list items, query function, and alert setup. Splunk can send email notification using search page or search command.

6.1.2 Flow of Project

Data pipeline stages proceeds in three flows

- The input stage
- The storage stage for data
- The searching of data stage



1. Data Information Stage

At this stage, Splunk editing uses the stream of raw information from its source, breaks it into 64K squares, and specifies each square with metadata keys. Metadata keys include hostname, a type of unlimited source of information. Keys similarly can include attributes that are used internally, for example, coding information for distribution information and values that control information management during the order phase, for example, the record at which times should be discarded.**2.**

Data Capacity Stage

- The data limit consists of two phases: Analysis and editing.
- In the analysis phase, the Splunk system evaluates, evaluates, and modifies data to separate only important information. This is often called event management. It is during this stage that Splunk editing breaks the data stream into individual events. The stages are many sub-sections:

1. Divide the increase in data in each row
2. Identifying, sorting, and setting time stamps
3. Defining each event with a metadata copied to a broad source key
4. Modifying event data and metadata according to regex change rules
5. In the order section, the Splunk system makes the filtered events a summary on the plate. It makes both aggregated data and a separate record report. The advantage of ordering is that the data can be successfully retrieved during the scan.

2. Data Looking through Stage

This stage controls how the client gets to, perspectives, and utilizations the recorded information. As a component of the pursuit work, Splunk programming stores client made information objects, for example, reports, occasion types, dashboards, cautions and field extractions. The hunt work likewise deals with the inquiry cycle.

SQL Injection:-

SQL injection is sequel query language injection which exploits the database by inserting such data as user input which act as a part of query and perform action accordingly which result in great impact of data leakage.

Sqlmap:-

sqlmap is an entrance testing gadget that automates the technique associated with perceiving and exploiting SQL mixture deformities and taking over of data base servers. It goes with a solid area engine, various specialty features for an authoritative entry analyzer and a broad extent of switches persevering from informational index fingerprinting, over data getting from the informational index, to getting to the crucial record system and executing orders on the functioning structure all through of-band affiliations.

DOS:-

- Denial of Service (DoS) attack is kind of attack which is generated by multiple parallel processing result in losing accessibility and performance of the victim system.
- During the DOS attack, they additionally get to restricted intel. These PCs are then used to wage a DoS Assault in attacker's PC.
- Through various wellbeing endeavors have been taken to stop DOS Assault to shield our data, the aggressors have developed new techniques and attack reasoning. Consequently, it is fundamental that rather than answering new attacks, it is vital to manufacture an absolute DoS plan that will make preparations for a wide scope of DoS attacks. Along these lines, the experts ought to understand the web and methodologies used to hinder the DoS attacks.
- The proposed structure gives an exceptional method to perceive DoS attack using Splunk.We propose two techniques for counteraction of DoS assault.
- One is utilizing Haphazardly created Manual human tests and other one is utilizing Linux slam content to forestall DoS attack via naturally impeding IP of the client, who is sending different solicitation at a time.

Getting everything rolling with DOS assaults utilizing hping3:

To install hping3 on a linux based system fire the command: **apt install hping3 -y**

A simple dos attack performed by: **sudo hping3 - S - - flood - V - p 80 170.155.9.185**

sudo: gives required honors to run hping3.

hping3: command calls hping3 program.

-S: in the command indicates the SYN bundles.

-flood: take shots at carefulness, answers will be disregarded (that is the reason answers wont be shown) and parcels will be sent quick as could really be expected.

-V: stands for level of Verbosity.

-p 80: is the port number dedicated to 80

170.155.9.185: is IPof the target system.

7 CHAPTER: 7 CONCLUSIONS AND FUTURE WORK

CHAPTER 7 CONCLUSION AND FUTURE WORK

Challenges and how we overcame it

The splunk enterprise came up with the feature to run any script that could prevent simple attacks or help the system with security incident and event management, but lately the feature was depreciated. Splunk doesn't allowed to run any script in desired environment. So a manual bash file was created by us that run the python script which would build a SSH connection with remote system and generate a trigger alert notification.

Conclusion

Splunk is now an industry standard for examining continuous information and trigger subsequent activities. Splunk is being utilized all around the world by government offices, business specialist co-ops, colleges to dissect and comprehend business and client conduct continuously It can set off alarms in the event of any network safety extortion, and working on the presentation of the help being given, while lessening the expense for the everyday tasks in any association.

Future work

In future for this project we will be using splunk apps and gathering data from various sources and work with different features provided by Splunk Enterprise.

CHAPTER: 8 REFERENCES

CHAPTER 8
REFERENCES

1) https://docs.splunk.com/Documentation
2) https://sqlmap.org/
3) http://www.hping.org/
4) https://www.ibm.com/security/enterprise-mobility-management

ibm report

ORIGINALITY REPORT

9%	6%	0%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.acte.in Internet Source	3%
2	Submitted to Ganpat University Student Paper	2%
3	www.kalilinux.in Internet Source	1%
4	archive.org Internet Source	1%
5	Submitted to Wawasan Open University Student Paper	1%
6	linuxhint.com Internet Source	1%
7	repository.ntu.edu.sg Internet Source	<1%
8	economicalhost.com Internet Source	<1%
9	www.elettronicain.it Internet Source	<1%

10	www.nerc.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

ibm report

PAGE 1

PAGE 2

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word.

Prep. You may be using the wrong preposition.

PAGE 3

PAGE 4

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to remove this article.

Word Error Did you type "**the**" instead of "**they**," or have you left out a word?

Confused You have used **chose** in this sentence. You may need to use **choice** instead.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 5

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Missing "?" Remember to use a question mark at the end of a question.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

PAGE 6

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Missing "," You may need to place a comma after this word.

Wrong Form You may have used the wrong form of this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to remove this article.

PAGE 7

PAGE 8

Missing "," You may need to place a comma after this word.

Compound These two words should be written as one compound word.

PAGE 9

Confused You have used **Accept** in this sentence. You may need to use **except** instead.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **a**.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **a**.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Article Error You may need to remove this article.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

PAGE 12

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

PAGE 13

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Article Error You may need to remove this article.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Wrong Form You may have used the wrong form of this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Confused You have used **from** in this sentence. You may need to use **form** instead.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 17

PAGE 18

PAGE 19

PAGE 20

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 21

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 22

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 23

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 24

PAGE 25

PAGE 26

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 27

PAGE 28

PAGE 29

Article Error You may need to use an article before this word.

PAGE 30

PAGE 31

Article Error You may need to use an article before this word.

PAGE 32

PAGE 33

Article Error You may need to use an article before this word.

Missing "," You may need to place a comma after this word.

Possessive You may need to use an apostrophe to show possession.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word. Consider using the article **a**.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word.

Missing "," You may need to place a comma after this word.

Missing "," You may need to place a comma after this word.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

PAGE 36

Article Error You may need to use an article before this word.

Prep. You may be using the wrong preposition.

Article Error You may need to remove this article.

PAGE 37

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Wrong Form You may have used the wrong form of this word.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Prep. You may be using the wrong preposition.

Confused You have used **off** in this sentence. You may need to use **of** instead.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word.

PAGE 38

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Wrong Form You may have used the wrong form of this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Proper Noun If this word is a proper noun, you need to capitalize it.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Article Error You may need to remove this article.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sentence Cap. Remember to capitalize the first word of each sentence.

Article Error You may need to remove this article.

Missing Apos. Since this is a contraction, you need to use an apostrophe to form it.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

Confused You have a spelling mistake near the word **a** that makes **a** appear to be a confused-word error.

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Prep. You may be using the wrong preposition.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.