**Security Information and Event Management**

***A***

***Project Report***

*Submitted in partial fulfillment of the*

*requirements for the award of the degree of*

**BACHELOR OF TECHNOLOGY**

**in**

**COMPUTER SCIENCE & ENGINEERING**

**With specialization**

**Banking, Finance, Security and Insurance**

**by**

|  |  |
| --- | --- |
| **Name** | **Roll No.** |
| **BINEEK RAJA** | **R133201410** |
| **VIKASH ANAND** | **R133214052** |
| **VANDANA SHARMA** | **R133214051** |
| **MOHIT PANDEY** | **R133214026** |

***Under the guidance of***

**Mr. Jatin Sethi**

**Assistant Professor**

**Computer Science Department, SOCS**



**Department of Analytics**

**School of Computer Science Engineering**

**University of Petroleum & Energy Studies**

**Bidholi, Via Prem Nagar, Dehradun, UK**

**December – 2017**



**CANDIDATE’S DECLARATION**

I/We hereby certify that the project work entitled **“ Security Information and Event Management”** in partial fulfilment of the requirements for the award of the Degree of BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING with specialization in Banking, Finance, Security and Insurance and submitted to the Department of Analytics at School of Computer Science Engineering, University of Petroleum & Energy Studies, Dehradun, is an authentic record of my/ our work carried out during a period from **August**, **2017** to **December**, **2017** under the supervision of **Mr. Jatin Sethi, Assistant Professor, School of Computer Science Engineering.**

The matter presented in this project has not been submitted by me/ us for the award of any other degree of this or any other University.

**(BINEEK RAJA, VIKASH ANAND, VANDANA SHARMA, MOHIT PANDEY)**

**Roll No. R1332104010, R133214052, R133214051, R133214026**

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date: 11th December 2017 **Jatin Sethi**

Assistant Professor

SOCS, UPES

Dr. T P Singh

Head – Department of Analytics

School of Computer Science Engineering

University of Petroleum & Energy Studies

Dehradun – 248 001 (Uttarakhand)

**ACKNOWLEDGEMENT**

We wish to express our deep gratitude to our guide **Jatin Sethi**, **Assistant Professor,** for all advice, encouragement and constant support that he has given us through out our project work. This work would not have been possible without his support and valuable suggestions.

We sincerely thank to our respected **Dr. T P Singh**, **Head of the Department** for his great support in doing our project.

We are also grateful to Dr. **Manish Prateek, Director, SOCS** and Dr. **Kamal Bansal, Dean SOE**, UPES for giving us the necessary facilities to carry out our project work successfully.

We would like to thank all our **friends** for their help and constructive criticism during our project work. Finally, we have no words to express our sincere gratitude to our **parents** who have shown us this world and for every support they have given us.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **BINEEK RAJA** | **VIKASH ANAND** | **VANDANA SHARMA** | **MOHIT PANDEY** |
| **Roll No.** | **R133214010** | **R133214052** | **R133214051** | **R133214026** |

**TABLE OF CONTENTS**

**S.No. Contents Page No**

1. **Abstract 5**
2. **Introduction 6**

**2.1 System Requirements 7**

**2.2 Pert Chart 7**

1. **Literature Review 8**
2. **Problem Statement 9**
3. **Objectives 9**
4. **Methodology 9-11**

**6.1 Requirement Analysis 9 -10**

* 1. **Design (Use Case Diagram) 10**
  2. **Implementation 11**

**6.4 Database 11**

1. **Snapshots 12 -13**
2. **Future Enhancements 14**
3. **References 15**

1. ***Abstract:***

**Security information and event management (SIEM)** technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyse events across disparate sources. There is a need to provide cost effective open source application that can provide threat detection through real time analysis of security alerts generated by network components which would be helpful for small organisations.

This application will provide real-time monitoring, correlation of events, notifications, console views and provides long-term storage as well as analysis, manipulation based on reporting of log data and security records.

Keywords: Real-time collection, Cost-Effective, Open Source, Correlation, Analysis

1. **Introduction:**

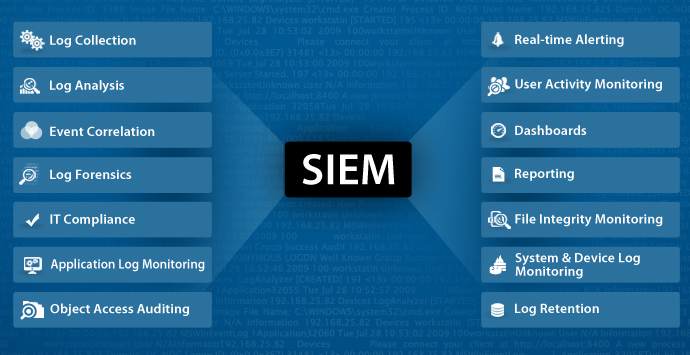
Security information and event management (SIEM) software products and services combine [security information management](https://en.wikipedia.org/wiki/Security_information_management) (SIM) and [security event management](https://en.wikipedia.org/wiki/Security_event_manager)(SEM). They provide real-time analysis of security alerts generated by network hardware and applications.

The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is known as security event management (SEM). The second area provides long-term storage as well as analysis, manipulation and reporting of log data and security records of the type collated by SEM software, and is known as security information management (SIM).

The term security information event management (SIEM), coined by Mark Nicolett and Amrit Williams of Gartner in 2005,

* The product capabilities of gathering, analyzing and presenting information from network and security devices
* Identity and access-management applications
* [Vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)) management and policy-compliance tools
* Operating-system, database and application logs
* External [threat](https://en.wikipedia.org/wiki/Threat_(computer)) data

A key focus is to monitor and help manage user and service privileges, [directory services](https://en.wikipedia.org/wiki/Directory_services) and other system-configuration changes; as well as providing log auditing and review and incident response.



Capabilities/Components:

* Data aggregation: [Log management](https://en.wikipedia.org/wiki/Log_management) aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
* Correlation: looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information. Correlation is typically a function of the Security Event Management portion of a full SIEM solution.
* Alerting: the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues. Alerting can be to a dashboard, or sent via third party channels such as email.
* Dashboards: Tools can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.[[8]](https://en.wikipedia.org/wiki/Security_information_and_event_management#cite_note-8)
* Retention: employing long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements. Long term log [data retention](https://en.wikipedia.org/wiki/Data_retention) is critical in forensic investigations as it is unlikely that discovery of a network breach will be at the time of the breach occurring.

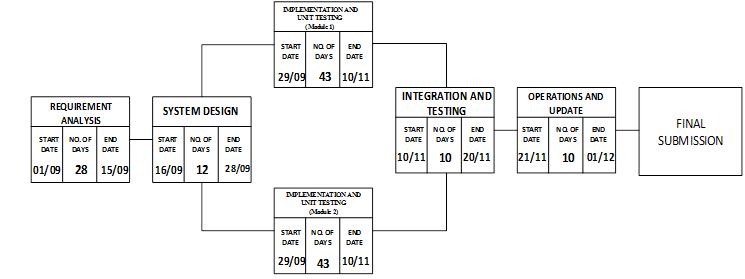
**2.1** **System Requirement**

* **SOFTWARE REQUIREMENTS**

1. Language – Python 3
2. Compiler – Python
3. Operating System – Windows
4. IDE – PyCharm

* **HARDWARE REQUIREMENTS**
  1. 2 GHz dual core processor or better
  2. 2 GB system memory
  3. 25 GB of free hard drive space

**2.2 Pert Chart**



1. **Literature Review:**

SIEM or [Security Information and Event Management](http://wiki.aanval.com/wiki/Library:The_Essential_Features_and_Capabilities_of_a_SIEM_Technology) is defined as a complex set of technologies brought together to provide a holistic view into a technical infrastructure.The SIEM gives you a holistic, unified view into not only your infrastructure but also workflow, compliance and log management. A SIEM can provide a multitude of capabilities and services efficiently.

At its core, a SIEM provides:

* **Event and Log collection:** This may come in many forms, especially with in-house applications.
* **Layered Centric Views or Heterogeneous:** This is usually in the form of dashboards or “views,” referred to as a bird’s-eye view.
* **Normalization:** a two-part function. This includes translating computerized jargon to readable data to be displayed, and mapping data to user- or vendor-defined classifications/characterizations. This is sometimes referred to as “field mapping.”
* **Correlation:** This essentially gives the data context and forms relationships based on rules, architecture and alerts. This should be either historical or real-time.
* **Adaptability (Scalable):**This dumbs down to being able to speak the language regardless of source vendor, format, type, change or compliance requirement.
* **Reporting and Alerting:** This may be used to not only show value to executives but also provide automated verification of continuous monitoring, trends and auditing. Some would argue that the auditing aspect is an essential function but the SIEM alone does nothing – like a retired general with no troops or a SQL instance with no tables or data.
* **Log Management:** Allowing the capability for storing event and logs into a central location, while also allowing the application of compliance storage or retention requirements. (Again, many would argue this is a separate function, and I would disagree.)

1. **Problem Statement:**

* There is a need to provide cost effective open source application that can provide threat detection through real time analysis of security alerts generated by network components which would be helpful for small organisations.

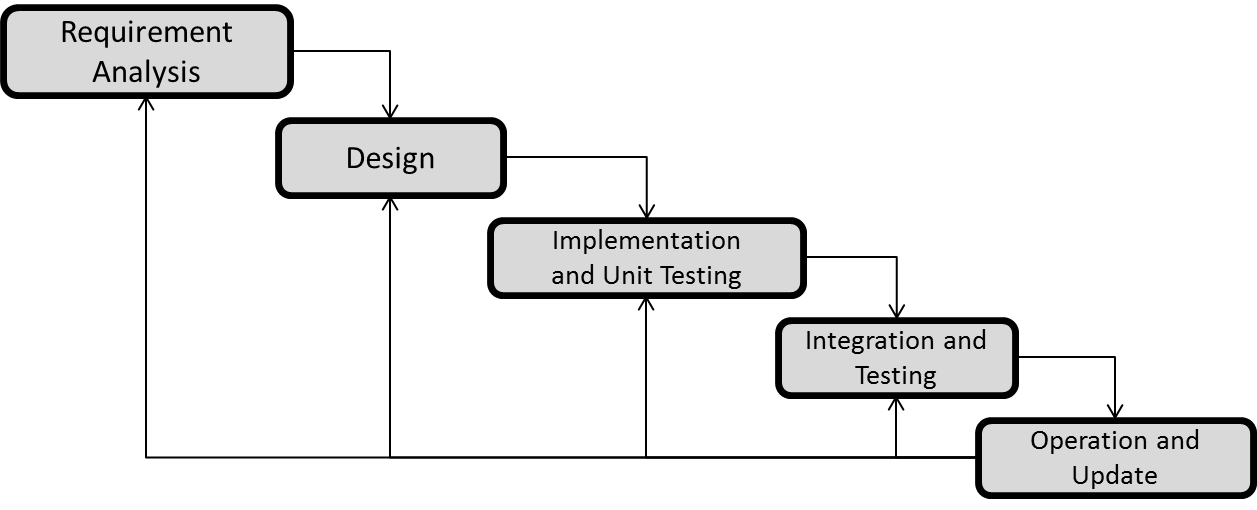
1. **Objectives:**

* To develop an application which can provide real-time monitoring, correlation of events, notifications, console views and provides long-term storage as well as analysis, manipulation and reporting of log data and security records.

1. **Methodology:**

We are using ITRERATIVE WATERFALL MODEL due to large data size and complexity of our project.

**ITERATIVE WATERFALL MODEL**

**6.1 Requirement Analysis:**

Logs are required for analyzing the successful and failed logs at firewall, apache server and application. For this we have collected different types of firewall logs, apache server logs and application logs.

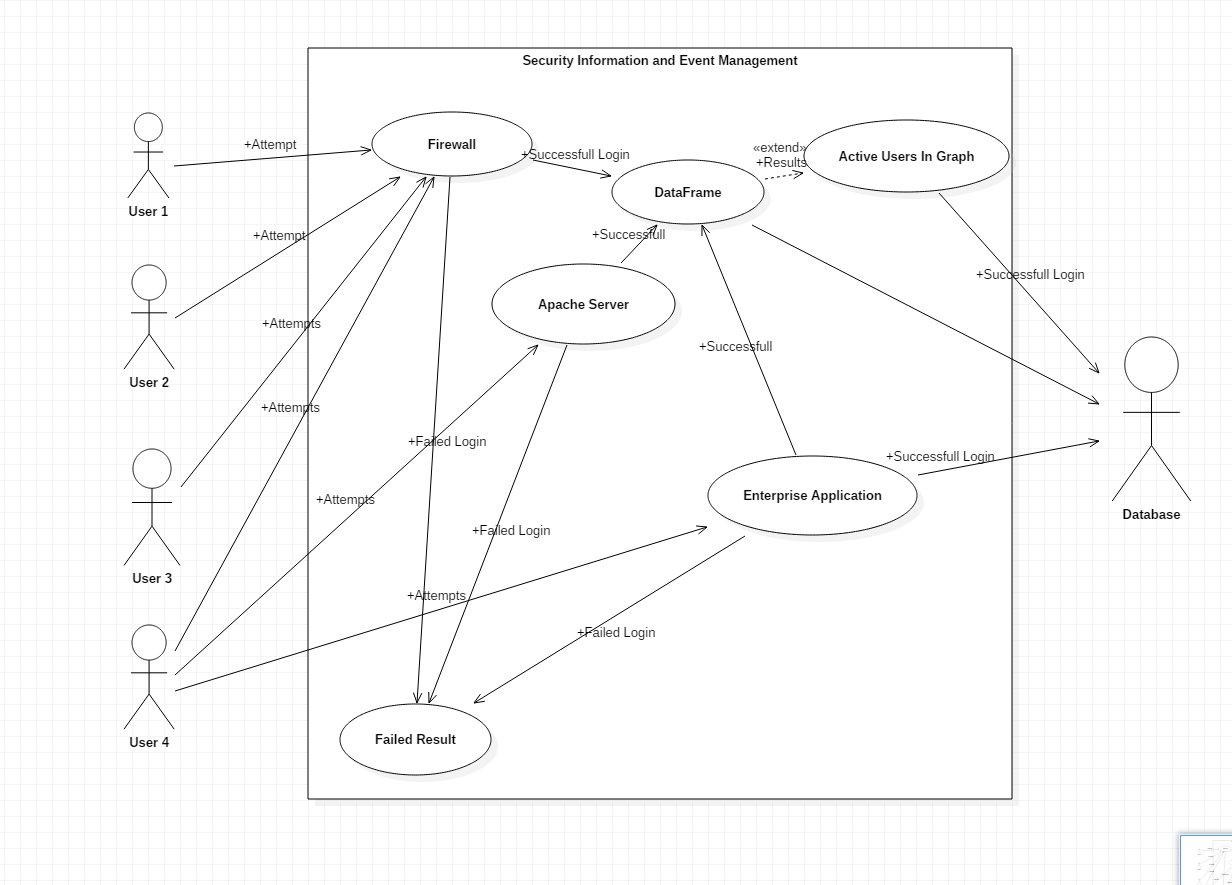
Firewell Logs:

|  |  |  |
| --- | --- | --- |
| 2006-09-19 03:26:26 DROP UDP 172.20.73.241 239.255.255.250 2250 1900 315 - - - - - - - RECEIVE | | |
| 2006-09-19 03:26:26 DROP UDP 172.20.73.241 239.255.255.250 2250 1900 305 - - - - - - - RECEIVE | | |
| 2006-09-19 03:27:05 CLOSE UDP 192.168.72.12 10.20.72.186 3682 88 - - - - - - - - - |  |  |
| 2006-09-19 03:27:05 CLOSE UDP 192.168.72.12 10.20.72.186 3683 88 - - - - - - - - - |  |  |
| 2006-09-19 03:27:53 CLOSE TCP 192.168.72.12 10.20.72.186 3680 445 - - - - - - - - - |  |  |
| 2006-09-19 03:29:24 DROP UDP 172.20.73.241 239.255.255.250 2250 1900 250 - - - - - - - RECEIVE | | |
| 2006-09-19 03:29:24 DROP UDP 172.20.73.241 239.255.255.250 2250 1900 315 - - - - - - - RECEIVE | | |
| 2006-09-19 03:29:24 DROP UDP 172.20.73.241 239.255.255.250 2250 1900 263 - - - - - - - RECEIVE | | |
| 2006-09-19 03:29:24 DROP UDP 172.20.73.241 239.255.255.250 2250 1900 315 - - - - - - - RECEIVE | | |
| 2006-09-19 03:29:24 DROP UDP 172.20.73.241 239.255.255.250 2250 1900 305 - - - - - - - RECEIVE | | |
| 2006-09-19 03:31:15 DROP UDP 192.168.183.114 239.255.255.250 65173 1900 310 - - - - - - - RECEIVE  Apache Logs:   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 1 | 192.168.72.12 | 9/19/2006 | 3:37:58 | GET | HTTP | 200 | 3683 | | 2 | 192.168.99.165 | 9/19/2006 | 3:45:36 | GET | HTTP | 200 | 1900 | | 3 | 192.168.183.114 | 9/19/2006 | 3:45:43 | GET | HTTP | 200 | 65166 | | 4 | 222.225.225.1 | 9/20/2006 | 3:29:24 | GET | HTTP | 200 | 2250 | | 5 | 193.168.82.10 | 9/20/2006 | 3:38:20 | GET | HTTP | 452 | 1025 | | 6 | 226.222.222.3 | 9/20/2006 | 3:35:57 | GET | HTTP | 200 | 65170 | | 7 | 128.2.2.2 | 9/20/2006 | 3:32:18 | GET | HTTP | 582 | 1900 | |  |  |  |  |  |  |  |  | | | |

Application Logs:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 192.168.72.12 | 9/19/2006 | 3:37:58 | GET | HTTP | 200 | 3683 |
| 2 | 192.168.99.165 | 9/19/2006 | 3:45:36 | GET | HTTP | 200 | 1900 |
| 3 | 192.168.183.114 | 9/19/2006 | 3:45:43 | GET | HTTP | 200 | 65166 |
| 4 | 222.225.225.1 | 9/20/2006 | 3:29:24 | GET | HTTP | 200 | 2250 |
| 5 | 226.222.222.3 | 9/20/2006 | 3:35:57 | GET | HTTP | 985 | 65170 |

* 1. **Design:**
     1. **Use Case Diagram:**

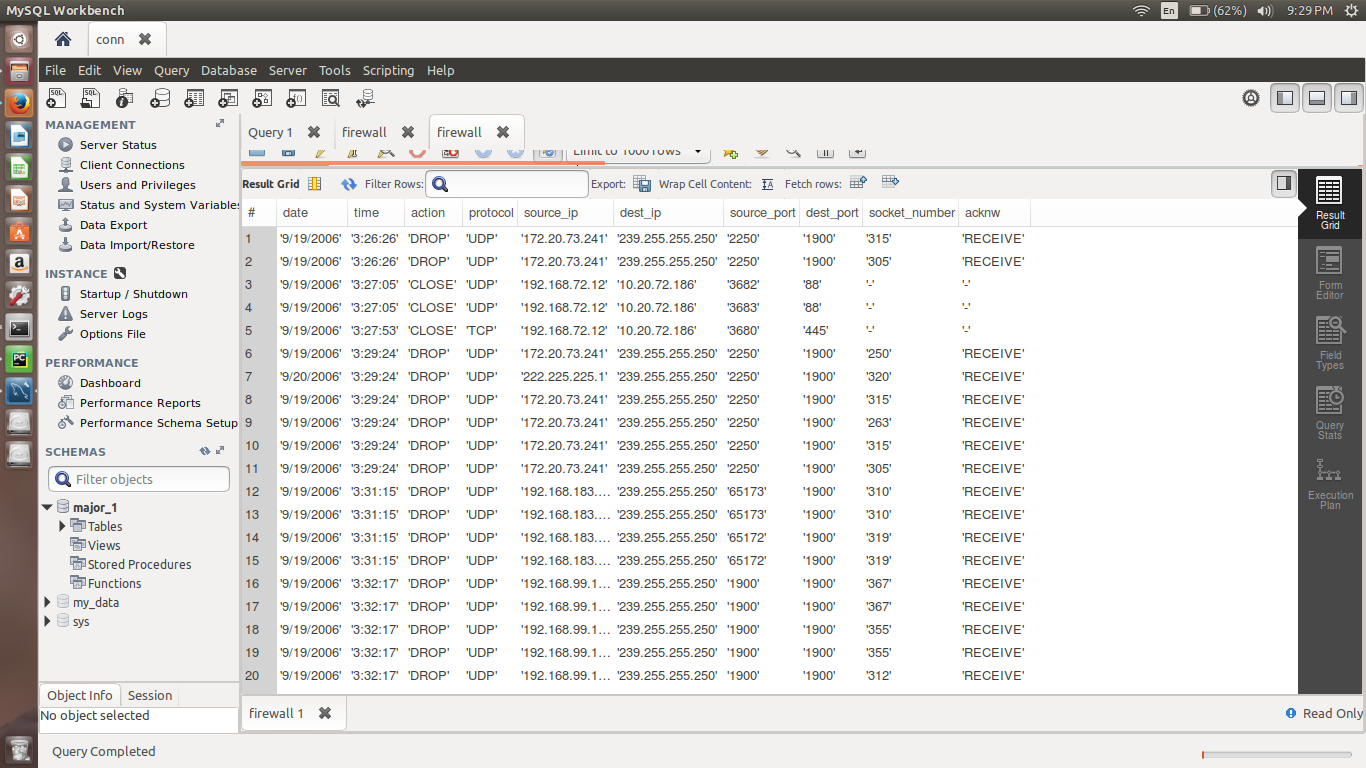


**6.3 Implementation:**

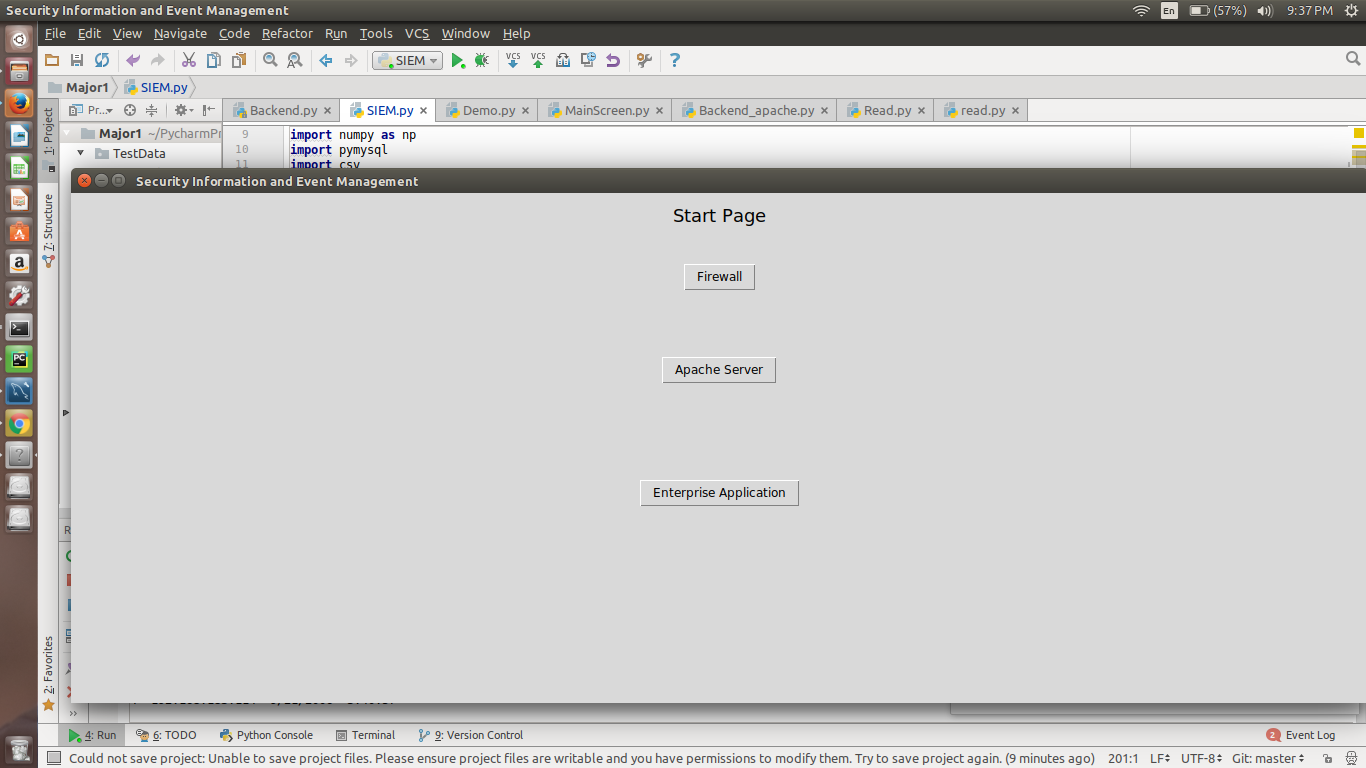
class SIEM\_Demo(tk.Tk):  
  
 # Initialisation of parameters  
 def \_\_init\_\_(self, \*args, \*\*kwargs):  
 tk.Tk.\_\_init\_\_(self, \*args, \*\*kwargs)  
 container= tk.Frame(self)  
  
 container.pack(side="top", fill="both", expand = True)  
  
 container.grid\_rowconfigure(0, weight= 1)  
 container.grid\_columnconfigure(0, weight=1)  
  
 self.frame = {}  
  
 for F in (StartPage, PageFirewall, PageApache, PageFirewallActiveUser, PageEnterpriseApplication):  
 frame= F(container, self)  
  
 self.frame[F]= frame  
  
 frame.grid(row=0,column=0,sticky="nsew")  
  
 self.show\_frame(StartPage)  
  
 def show\_frame(self, cont):  
 frame =self.frame[cont]  
 frame.tkraise()

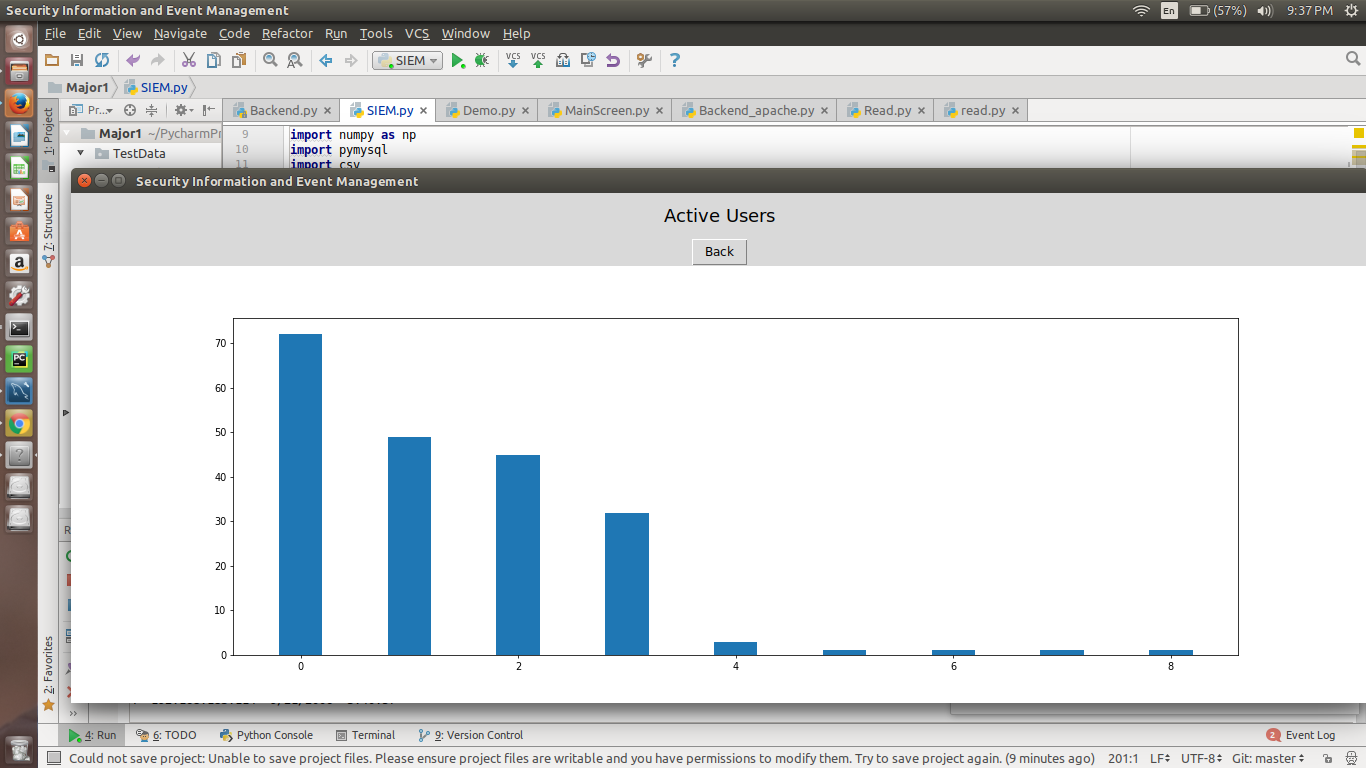
Complete back end work is done in python - PyCharm IDE using tkinter framework.

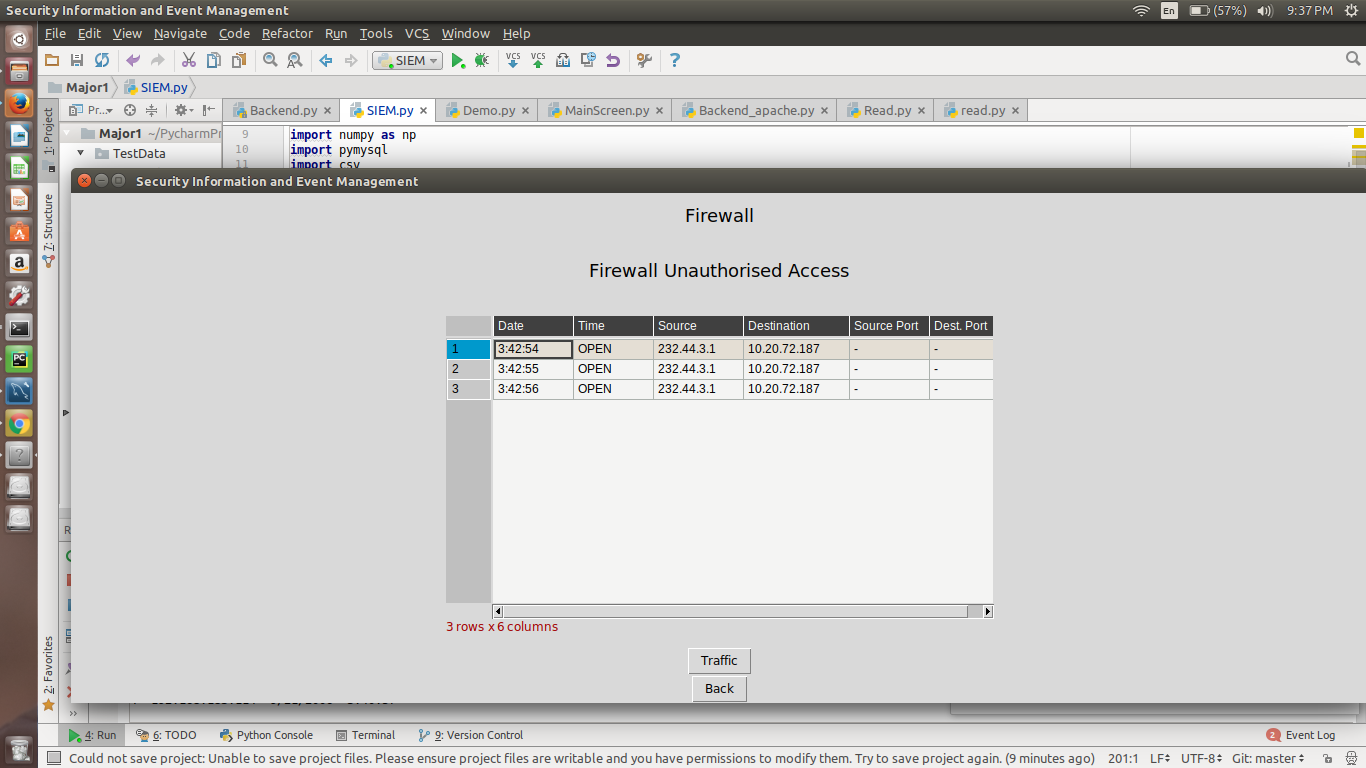
**6.4 Database:**

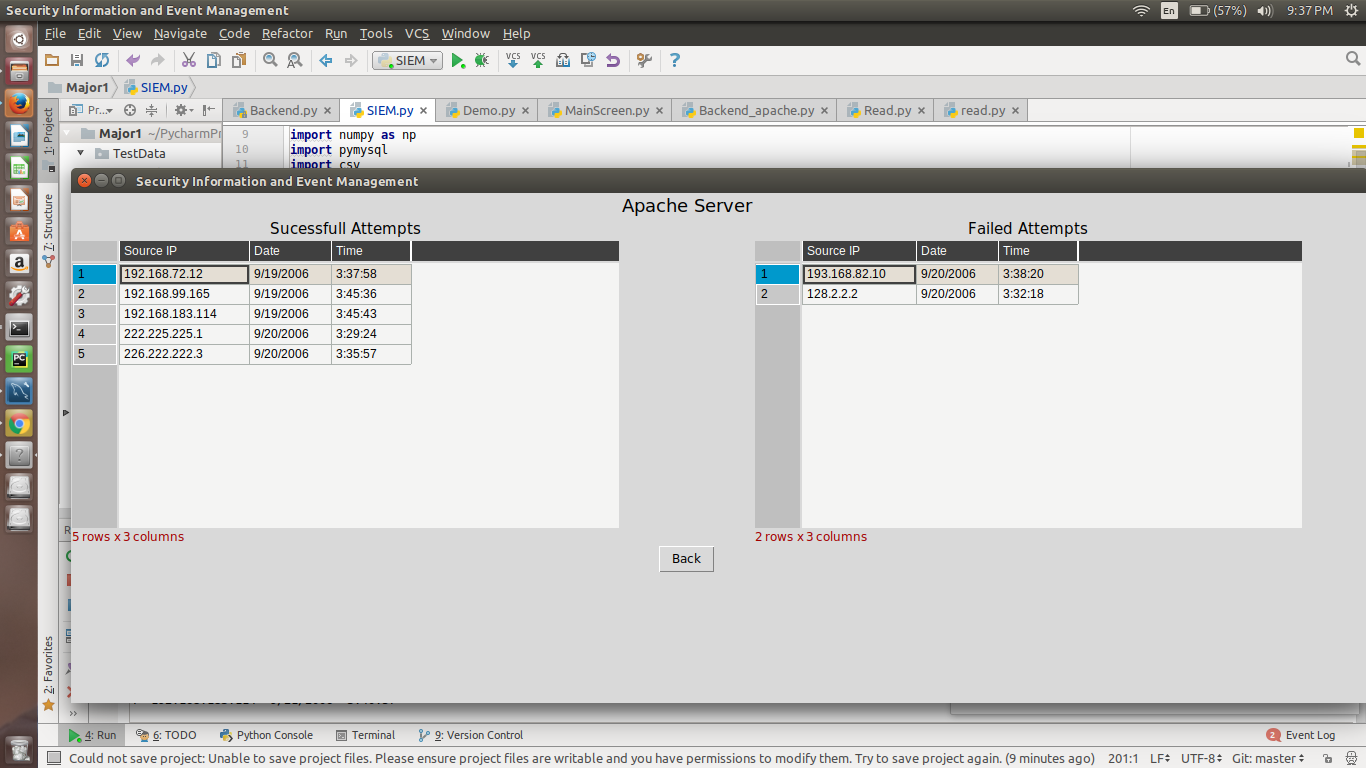


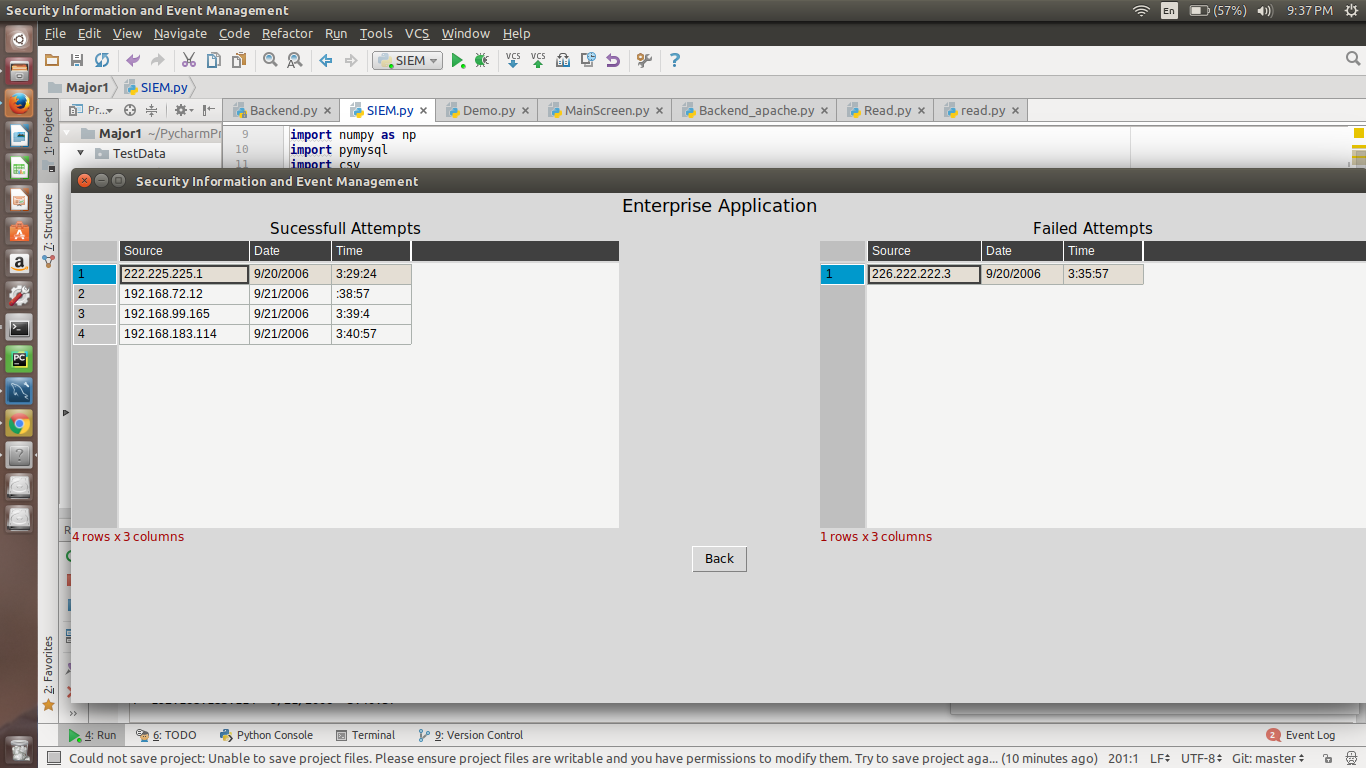
1. **Snapshots**











1. **Future Enhancements**

There is always a room for improvements in any software package, however good or efficient it may be done. But the most important thing is flexible to accept further modification. We can always increase analysis of logs by increasing the data set provides as it will lead to more accurate results. Apart from that we restrict our self only on the logs generated by firewall, apache server and enterprise application in this project but these can also be expanded as per the need.

9. **References:**

1. “*Successful SIEM and Log Management Strategies for Audit and Compliance*”

Swift, David, 4 November 2010

1. “*Magic Quadrant for Security Information and Event Management”*

Bussa, Toby & Kavanagh, Kelly, 10 August 2016

1. “*SIEM Technology Assessment*” Chuvakin, Anton,18 January 2017

**Approved By**

**Mr. JATIN SETHI Dr. T P Singh**

**Project Guide Head – Department of Analytics**