Санкт-Петербургский государственный университет

Хакизимана Эвелин

Выпускная квалификационная работа

Название работы

Уровень образования: магистратура
Направление: 02.04.02 «Фундаментальная информатика и информационные технологии»
Основная образовательная программа: ВМ.5502 «Вычислительные технологии»

Научный руководитель:
профессор кафедры КММС,
доктор технических наук,
Bogdanov A.V.

Санкт-Петербург
2020 год

РЕЗЮМЕ ПРОЕКТА

Научно-исследовательский проект для магистров кафедры процессов управления компьютерного моделирования и многопроцессорных систем

НАЗВАНИЕ: ОНЛАЙН-ЗАЩИТА ДАННЫХ

Имя исследователя: Хакизимана Эвелин

Онлайн-защита данных - это проектная работа, которая поможет построить эффективный контроль безопасности данных для системы ОИЯИ. Она направлена на разработку скриптов для обнаружения и сообщения об угрозах в случае попыток хакеров атаковать систему. Система будет служить более надежным и эффективным средством борьбы с хакерской угрозой, определяя и сообщая о его поведении или этих угрозах. Кроме того, разработанные скрипты будут читать журналы хакера и проверять такое поведение в системе. Если какое-либо поведение обнаружено, оно будет записано в определенный файл или в базу данных.

Table of Contents

Глава 1

ОБЩЕЕ ВВЕДЕНИЕ

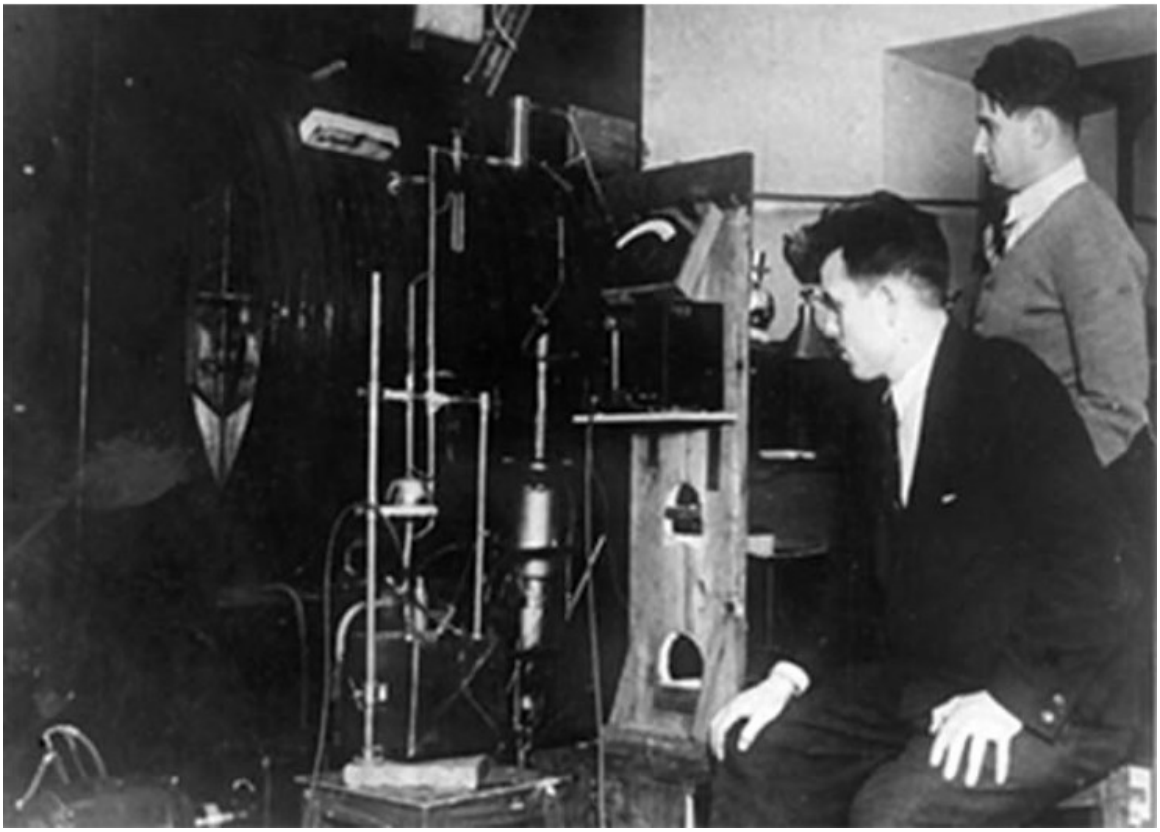
Нынешнее поколение испытывает технологии в области доступа к системе и доступа к данным. В связи с развитием технологий в области системного доступа и доступа к данным, в частности информационных технологий, хакеры пытаются атаковать онлайн-систему с плохой целью. В кибербезопасности конфиденциальность, целостность и доступность являются элементами безопасности данных наша цель-разработать и работать над проектом онлайн-безопасности данных с целью обеспечения доступности системы в ОИЯИ. Обнаружение пользовательских угроз в системах Linux на основе поведения пользователя мы думаем об автоматическом анализе собранных журналов системы Linux, создавая ваше продуманное подозрительное поведение, которое может помочь обнаружить и сообщить о потенциальных угрозах безопасности. Проект Online data security будет иметь сценарии оболочки, которые будут периодически запускаться для чтения различных лог-файлов, выполнения анализа и предоставления отчета о зарегистрированной информации, скорее можно сказать, что сценарий online data security был радикально изменен с точки зрения доступности данных организации и служб безопасности системы. Поведение пользователя в системе будет изменено в своих видах. Кроме того, поведение пользователя, ищущего информацию, изменилось в зависимости от того, кто есть и что он хочет делать.

1.1 История развития киберпреступности

Киберпреступность впервые началась с попыток хакеров проникнуть в компьютерные сети. Некоторые делали это просто для острых ощущений от доступа к высокоуровневой безопасности, сети, но другие стремились получить секретные данные, секретные материалы, преступники начали заражать компьютерные системы компьютерными вирусами, что привело к поломкам на персональных и деловых компьютерах.

1.2 исторические предпосылки исследования

Объединенный институт ядерных исследований - международная межправительственная научно-исследовательская организация в наукограде Дубна Московской области, имеющая в настоящее время 18 государств-членов ОИЯИ. Исследования в области ядерной физики начались еще в годы Великой Отечественной войны по инициативе академика И. В. Курчатова, который взял на себя руководство развитием советской атомной науки и техники и собрал в Москве своих учеников и ряд выдающихся советских ученых.



Professor I.V.Kurchatov together with a postgraduate student M.G. Meshcheryakov working at the first Soviet cyclotron in the Radium Institute, 1936

По воспоминаниям М. Г. Мещерякова, во второй половине 1944 года в кругах советских ученых, занимающихся исследованиями в области ядерной физики, началась дискуссия о возможности строительства ускорителей элементарных частиц в нашей стране. Под руководством академика И. В. Курчатова в Лаборатории № 2 АН СССР было проведено несколько совещаний на эту тему. Впоследствии эта лаборатория, основанная выдающимся ученым, была преобразована в Институт атомной энергии АН СССР (ныне Научно-исследовательский центр “Курчатовский институт”). В результате обсуждения возникла идея о том, что для поддержки перспективных направлений фундаментальных физических исследований в Советском Союзе необходимо построить два ускорителя с рекордными энергиями-ускоритель протонов на

450-500 МэВ с последующим увеличением до 650-700 МэВ и ускоритель электронов на энергии не менее 250 МэВ.

Система Linux имеет свой способ ведения журналов всего, что происходит в системе. Мы пришли к идее определить конкретное поведение пользователя, которое, по нашему мнению, может быть подозрительным или представлять угрозу для системы, и написать сценарий, который будет запущен, чтобы сообщить об этих вещах.

1.3 постановка задачи исследования

Логин системы не может ограничить пользователей, не может сообщить о процессе ведения журнала, система не может предоставить способы обнаружения и сообщения о потенциальной угрозе безопасности. В нашем исследовании основными являются следующие проблемы:

* Хакеры могут попытаться войти в систему может в разное время и в короткие сроки.
* Хакеры могут попробовать несколько попыток входа в систему до тех пор, пока он не войдет в систему и после того, как он может установить некоторые пакеты или загрузить файлы в систему, а затем в системе Linux инициирует сетевую связь с одним и тем же исходным IP-адресом нескольких попыток.

1.4 решение исследовательских задач

Мы немедленно определим конкретное поведение пользователя, которое может быть подозрительным или представлять угрозу для системы, и напишем сценарии, которые будут запущены, чтобы сообщить об этих угрозах.
Мы пишем другой сценарий, который будет читать журналы и проверять такое поведение в системе, если какое-либо поведение обнаружено, оно будет записано в конкретный файл отчета или в базу данных.

1.5 цель исследования

Для защиты учетных записей в сети путем принятия набора средств управления, системы и методов, определяющих относительную важность различных наборов данных их чувствительность и логически защищающих систему ОИЯИ от хакеров, пытаются войти в систему через исследовательское название online data security. Путем разработки скриптов-кодов для обнаружения и сообщения о поведении хакеров.

1.6. Мотивация и заинтересованность проекта

Мотивация

Как студент Санкт-Петербургского государственного университета, который прошел через исследования по кибербезопасности, кодированию и дизайну после учета того, как процесс защиты данных осуществляется в системе ОИЯИ, мы наметили некоторые проблемы в обработке процесса защиты данных из-за онлайн-системы, а также после наблюдения за тем, как хакеры могут атаковать систему и последствия, которые могут повлиять на функциональные возможности системы, таким образом, все эти факторы подтолкнули нас к разработке кодов сценариев, которые могут позволить ОИЯИ иметь защищенную систему.

Общественный и конкретный интерес

общественный интерес

Эта проектная работа будет иметь значительные последствия в двух различных направлениях. Первый из них заключается в том, что после того, как будет введена онлайн-защита данных для системы ОИЯИ, с одной стороны, она будет обеспечена для обеспечения целостности конфиденциальности и доступности

как элемента системной безопасности, работники смогут использовать онлайн-систему через интернет, не опасаясь хакеров.

специфический интерес

Поскольку Санкт-Петербургский государственный университет-это университет, где ценится и поощряется научная деятельность и инновации, мне было разрешено участвовать в настоящем магистерском проекте, который привлекает мое интеллектуальное любопытство, удовлетворяет мою жажду открытий и дает мне выход для моего творчества.

1.7 значимость исследования

Работа над проектом поможет во многом обезопасить онлайн-систему в ОИЯИ, поскольку онлайн-защита данных поможет пользователям достичь всего, чего они хотят достичь, не приходя в различные офисы.
Явные преимущества обработки информации в Интернете по сравнению с традиционными незащищенными системами заключаются в более высокой доходности. Онлайн-защита данных позволяет пользователям осуществлять свою деятельность, не опасаясь хакеров.

1.8 задачи исследования

общая цель

Целью данного проекта является разработка скриптовых кодов, обеспечивающих оперативный процесс защиты данных в онлайн-системе

ОИЯИ. Коды скрипта позволят обнаружить хакера при попытке атаковать систему, чтобы получить доступ в систему с плохой целью.

конкретная цель

Конкретная цель этого проекта состояла в том, чтобы проанализировать безопасность онлайн-системы ОИЯИ и проблемы этой системы с целью разработки скриптовых кодов для обеспечения безопасности этой системы; это можно описать следующим образом:

* Конкретная цель состоит в том, чтобы предоставить интегрированные скрипты-коды для определения поведения хакера, который хочет войти в систему через логин.

• Сообщать о таком поведении в базе данных

Исследовательский вопрос

Обычно, прежде чем я начну писать грантовое предложение, мне нужно потратить некоторое время, чтобы наметить свою исследовательскую стратегию. Хороший первый шаг-сформулировать исследовательский вопрос. Исследовательский вопрос-это утверждение, которое идентифицирует явление, подлежащее изучению

• Как хакеры могли подключить онлайн-систему ОИЯИ?

• Что мы можем сделать для обеспечения безопасности онлайн-системы ОИЯИ?

Гипотеза исследования

Гипотеза этой работы заключается в следующем: для достижения нашей цели “онлайн-безопасность данных для онлайн-системы ОИЯИ” каждая попытка

хакера атаковать онлайн-систему ОИЯИ будет сообщаться и обнаруживаться. Онлайн-система защиты данных создана для того, чтобы помочь пользователям ОИЯИ сделать свою работу с большим количеством защищенных данных. Поэтому в данной работе обязательно будет разработан критический аргумент для доказательства правильности или неправильности этой гипотезы.

Объем исследования

Эта исследовательская работа будет касаться только онлайн-безопасности данных для онлайн-системы ОИЯИ. Другими словами, это исследование должно будет решить все проблемы, которые стоят перед онлайн-системой онлайн-системы ОИЯИ.

Разграничение

Этот проект будет реализован в виде скриптовых кодов, в которых будут сообщаться и обнаруживаться попытки хакеров получить доступ к онлайн-системе ОИЯИ.

Разделение работ

Этот проект содержит пять глав. В первой главе предлагается общее введение, состоящее из краткого введения, изложения проблемы и интересов исследования, объема исследования, исследовательских вопросов, гипотез, целей исследования, разделения работы и методологии исследования.

Во второй главе обзора литературы будут подробно рассмотрены проблемы безопасности онлайн-системы ОИЯИ. А затем третья глава будет посвящена анализу и разработке новой системы защиты данных в интернете. После этого в четвертой главе обязательно будет рассказано о внедрении новой системы онлайн-безопасности данных для онлайн-системы ОИЯИ, которая будет разработана для улучшения системы онлайн-безопасности данных. Наконец, выводы и рекомендации, связанные с результатами проекта, будут хорошо известны.

Методология и методы сбора данных

Метод МЕРИЗА

MERISE-это методология моделирования проектирования, разработки и реализации проектов обработки данных, которая была внедрена во Франции в начале 1980-х годов. МЕРИЗ переходит к раздельной обработке данных и процессов, где представление данных моделируется в три этапа: концептуальный и логический, вплоть до физического.

Методы сбора данных

Документация

Это метод, который был использован при консультировании различных систем защиты данных для того, чтобы понять онлайн-безопасность данных для онлайн-системы ОИЯИ.

Интервью

Интервью - это метод получения информации посредством устной, свободной и индивидуальной беседы с людьми, хорошо отобранными по факту или представлению, с проверкой степени релевантности, валидности и достоверности для целей сбора данных. Интервью-это тогда разговор между интервьюерами и интервьюируемыми в более поздних попытках получить информацию.

Эта техника имеет особенность быть прямой и неформальной.

Интервьюируемый вносит свой вклад в проект, давая устные ответы на вопросы, задаваемые интервьюером в непосредственном взаимодействии (за исключением телефонного интервью). Это процедура восстановления информации, которая проста и естественна.

Методика интервью очень полезна для сбора детальных данных о задаче или наборе конкретных задач. Собранная информация может быть направлена на описание существующей ситуации, а также на предложения или предложения относительно будущей ситуации (например, новое программное обеспечение или веб-сайт)

Мы использовали бесплатные интервью для того, чтобы выявить потребности пользователей ОИЯИ в защите системных данных.

Наблюдение

Наблюдение - это метод сбора данных, который использовался для описания того, что делают операторы и как они это делают. Для этого необходимо выйти на поле, где пользователь осуществляет свою деятельность, и максимально избегать влияния на него. Эти интервью заставили нас осознать идеи операторов о своих задачах и о том, как они выполняют эти задачи, и это наблюдение очень полезно для нас при сборе данных, имеющих отношение к работе.

Глава 2

ОБЗОР ЛИТЕРАТУРЫ

Вступление

Концепция любой новой системы безопасности требует серьезного и глубокого анализа существующей системы безопасности. Наше исследование будет сосредоточено на онлайн-безопасности данных для онлайн-системы ОИЯИ, где наш анализ сосредоточен на том, как сообщить и обнаружить любую попытку взлома, чтобы войти в систему.

2.1 определение терминологии

Конфиденциальность: это сокрытие информации или ресурсов. Кроме того, существует необходимость держать информацию в секрете от других третьих лиц, которые хотят иметь к ней доступ, чтобы только Правильные люди могли получить к ней доступ.

Целостность: это достоверность данных в системах или ресурсах с точки зрения предотвращения несанкционированных и ненадлежащих изменений. Как правило, целостность состоит из двух подэлементов-целостности данных, которая имеет отношение к содержанию данных, и аутентификации, которая имеет отношение к происхождению данных, поскольку такая информация имеет значение только в том случае, если она верна.

Доступность: относится к способности получить доступ к данным ресурса, когда это необходимо, поскольку такая информация имеет ценность только в том случае, если уполномоченные люди могут получить доступ в нужное время. Отказ в доступе к данным в настоящее время стал обычной атакой. Представьте себе время простоя живого сервера, насколько это может быть дорого.

Вход в систему: в компьютерной безопасности вход в систему - это процесс, с помощью которого человек получает доступ к компьютерной системе, идентифицируя и аутентифицируя себя. Учетные данные пользователя обычно представляют собой некоторую форму имени пользователя и соответствующего пароля, и сами эти учетные данные иногда называются логином.

Аутентификация: процесс или действие проверки подлинности пользователя или процесса.

Несанкционированный доступ: несанкционированный доступ - это когда кто-то получает доступ к серверу, веб-сайту или другим конфиденциальным данным, используя данные чужой учетной записи.

Хакер: это человек, который пытается использовать компьютерную систему по причине, которая может быть связана с деньгами, социальным делом, развлечением и т. д.

Угроза: это действие или событие, которое может поставить под угрозу безопасность.

Атака: это нападение на систему безопасности, которое доставляется человеком или машиной в систему. Это нарушает правила безопасности.

Уязвимость: это слабость, проблема проектирования или ошибка реализации в системе, которая может привести к неожиданному и нежелательному событию, связанному с системой безопасности.

IP-адрес (Internet Protocol): определяет компьютер в сети

База данных: это набор связанных данных.1 под данными мы подразумеваем известные факты, которые могут быть записаны и которые имеют скрытое значение. Например, рассмотрим имена, телефонные номера и адресную книгу людей, которых вы знаете. Возможно, вы записали эти данные в индексированную адресную книгу или сохранили их на жестком диске, используя персональный компьютер и программное обеспечение, например Microsoft Access или Excel. Эта совокупность связанных данных с неявным значением является базой данных.

Компьютерная сеть: компьютерная сеть - это система, которая соединяет два или более компьютеров вместе с помощью канала связи.

Web Browser: это особый вид программного обеспечения, которое обрабатывает гипертекстовый язык верстки (HTML) документа. Другими словами, веб-браузер - это компьютерная программа, которая интерпретирует команду HTML для сбора, упорядочивания и отображения частей веб-страницы.

Онлайн: подключается через компьютер, подключенный к центральной компьютерной сети или доступный через нее.

Offline: отключен от компьютерной сети; описывает компьютерный терминал или периферийное устройство, отключенное от компьютерной сети.

Система: совокупность компьютерных компонентов, то есть совокупность аппаратных, программных и периферийных устройств, функционирующих вместе.

[1]

2.2 уязвимость онлайн-системы ОИЯИ

Хакер может попробовать несколько попыток войти в систему до тех пор, пока не будет успешным, после успешного входа хакер устанавливает некоторые пакеты или загружает определенные файлы в систему. Пользователь может попробовать войти в систему может в разное время и в короткие сроки. Это большая проблема, потому что нет никаких способов узнать поведение этого хакера. Когда он / она может получить несанкционированный доступ в систему, он может сделать все для своей плохой цели.

2.3 предлагаемые решения наблюдаемых проблем

Мы разработали программу анализа журналов, которая имеет коды сценариев для просмотра всех журналов аутентификации, сведения о журнале аутентификации для IP-адреса, сведения о системных журналах, текущий

1 We will use the word data as both singular and plural, as is common in database literature; the context will determine whether it is singular or plural. In Standard English, data is used for plural and datum for singular.

заблокированный IP-адрес, чтобы добавить IP-адрес в черный список и удалить IP-адрес в черном списке.

Поскольку хакер может пытаться войти в систему много раз, программа покажет все данные об используемом IP-адресе, такие как дата, час, порт и количество сбоев во времени.

Поскольку хакер может попытаться войти в систему в разные дни, программа показывает журналы сбоев каждой даты. IP-адрес, используемый хакером, может быть занесен в черный список

Глава 3

АНАЛИЗ И ПРОЕКТИРОВАНИЕ СИСТЕМ БЕЗОПАСНОСТИ ДАННЫХ В РЕЖИМЕ ОНЛАЙН

Вступление

R. Elmasri & Shamkant B. Navathe (2011) показали: “базы данных или системы баз данных являются важным компонентом жизни в современном обществе: большинство из нас ежедневно сталкиваются с несколькими видами деятельности, которые предполагают некоторое взаимодействие с базой данных. Например, если мы идем в банк, чтобы внести или снять средства, если мы делаем заказ на авиаперелет, Если мы получаем доступ к компьютеризованному библиотечному каталогу для поиска библиографического элемента, или если мы покупаем что—то онлайн—например, книгу или компьютер-есть вероятность, что наша деятельность будет связана с кем-то или какой-то компьютерной программой, имеющей доступ к базе данных”. Справедливо будет сказать, что программное обеспечение для онлайн-защиты данных для онлайн-системы ОИЯИ, безусловно, будет играть решающую роль в ОИЯИ для защиты своих данных от хакеров.

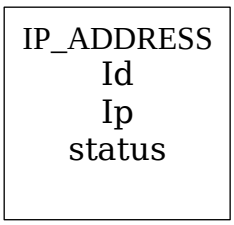
MERISE - это метод проектирования, разработки и реализации проектов обработки данных. Цель этого метода-создать информационную систему. Метод MERISE основан на разделении данных и процессов, которые должны выполняться в нескольких концептуальных логических и физических моделях. Метод MERISE был создан в 1978-1979 годах в ходе национальной

консультации, начатой в 1977 году Министерством промышленности с целью выбора компаний-консультантов по обработке данных для определения метода проектирования информационных систем.

В качестве инструмента анализа новой системы был выбран метод MERISE. МЕРИЗ имеет три уровня концепции, и каждый уровень имеет модель данных и модель процессов.

a. концептуальный уровень:

Целью данного уровня является моделирование базы данных и внесение необходимых изменений в информационную систему без изменения организационного аспекта, тем самым диктуя функции текущей системы. Концептуальный уровень состоит из следующих моделей:



- ✓ The Conceptual Data Model (CDM)
- ✓ The Conceptual Process Model (CPM)

b. логический или организационный уровень:

Цель этого уровня заключается в применении концепций, полученных на концептуальном уровне, для включения временных рамок проекта, масштабов проекта и участвующих в нем субъектов. Организационный уровень состоит из

следующих моделей:

✓ The Logical Data Model (LDM)

IP_ADDRESS(Id,Ip,Status)

✓ The Organizational Processes Model(OPM)

c. физический или операционный уровень:

Этот уровень будет выполнять реализацию техник, представленных на предыдущих уровнях. Операционный уровень состоит из следующих моделей:

✓ The Physical Data Model (PDM)

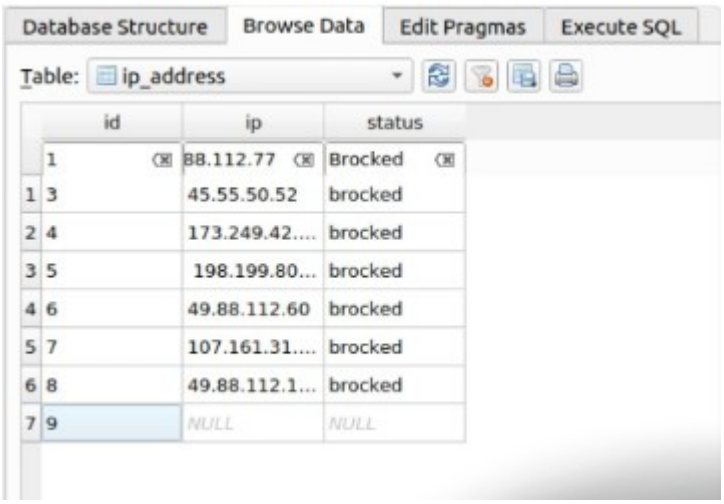


Рисунок 1: Таблица Ip-адресов

✓ The Operational Processes Model (OPPM)

Актеры на сцене

R. Elmasri & Shamkant B. Navathe (2011) сказал, что для небольшой персональной базы данных один человек обычно определяет, конструирует и манипулирует базой данных, и нет никакого общего доступа. Однако в крупных организациях многие люди участвуют в разработке, использовании и обслуживании большой базы данных с сотней пользователей. Те люди, чья

работа связана с повседневной работой большой базы данных; мы называем их актерами на сцене.

анализ требований

Целями этого являются:

• Определить требования к данным базы данных в терминах примитивных объектов

* Классифицировать и описывать информацию об этих объектах •

* Идентифицировать и классифицировать отношения между объектами

• Определение типов транзакций, которые будут выполняться в базе данных, и взаимодействий между данными.

Data Flows Diagram

Data Flows Diagram (DFD) это графическое представление "потока" данных через бизнес-функции или процессы. В более общем виде схема потока данных используется для визуализации процесса обработки данных. Он иллюстрирует процессы, хранилища данных и внешние объекты.

Data flow diagram будет поддерживаться 4 основных вида деятельности:

Анализ: DFD используется для определения требований пользователей

Дизайн: DFD is used to map out a plan and illustrate solutions to analysts and users while designing a new system

Коммуникация: одной из сильных сторон DFD является его простота и понятность аналитикам и пользователям;

Документы: DFD используется для предоставления специального описания требований и дизайна системы.

DFD предоставляет обзор ключевых функциональных компонентов системы, но не предоставляет никаких подробностей об этих компонентах.

Мы должны использовать другие инструменты, такие как словарь базы данных, чтобы получить представление о том, какая информация будет обмениваться и как она должна быть обменена.

Компоненты диаграммы потоков данных

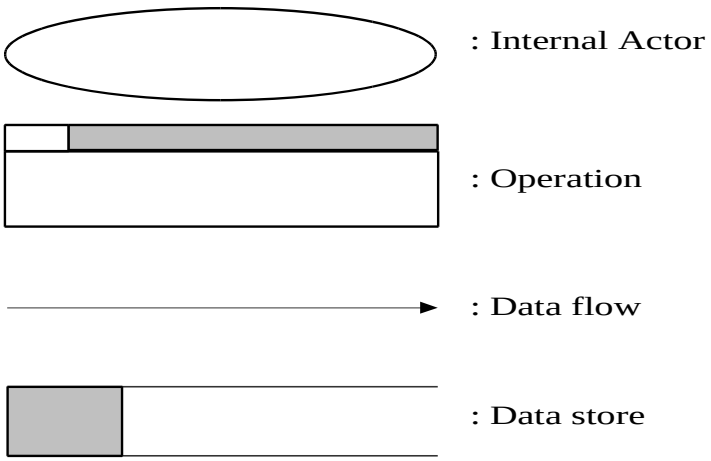
Процесс: процесс преобразует входящий поток данных в исходящий поток данных.

Хранилище данных: хранилище данных - это хранилища данных в системе. Иногда их также называют файлами.

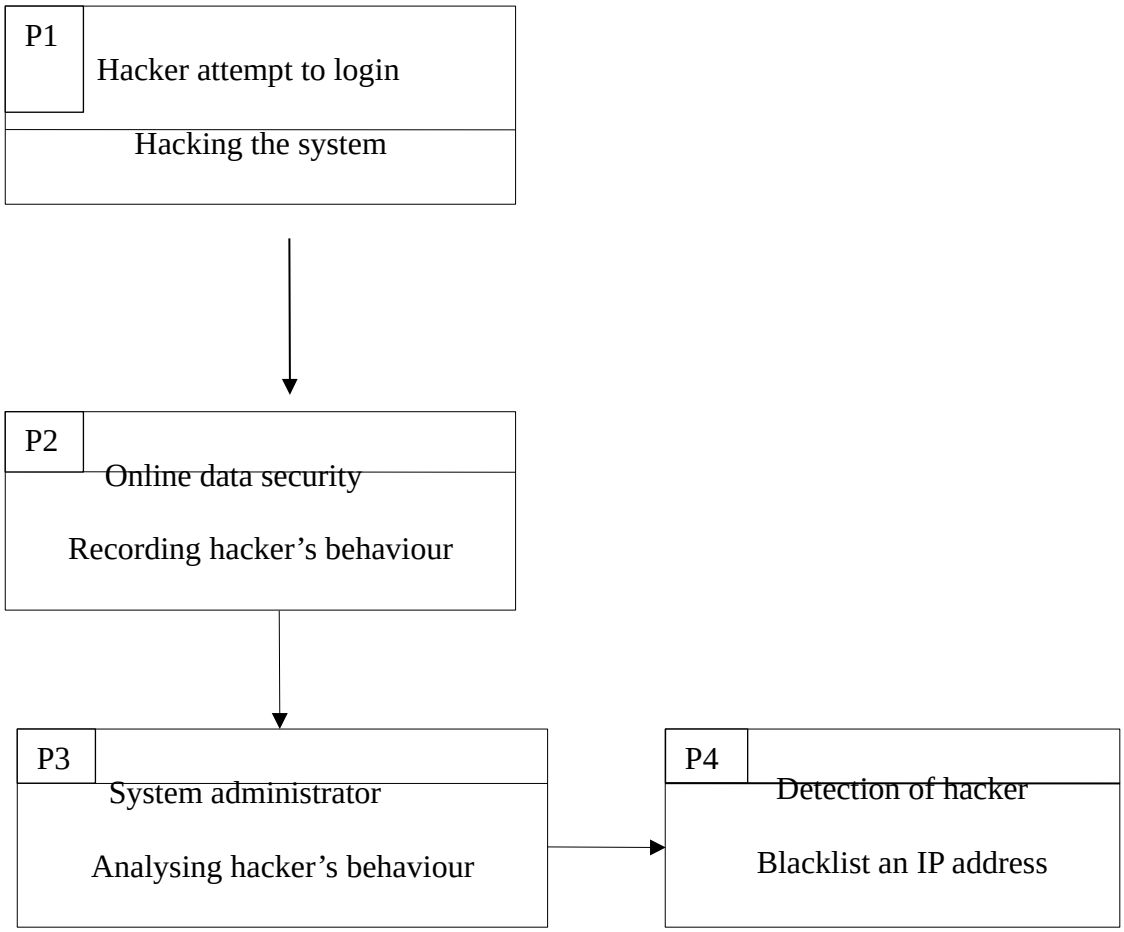
Поток данных: поток данных - это конвейер, по которому проходят пакеты информации.

Внешняя сущность: внешние сущности - это объекты вне системы, с которыми система

взаимодействует; внешние сущности-это источники и адресаты входов и выходов системы.



Data Flows Diagram for online data security



Глава 4

ПРЕЗЕНТАЦИЯ И ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ ОНЛАЙН-БЕЗОПАСНОСТИ ДАННЫХ

Вступление

В этой главе мы расскажем о новой системе и о том, как было задумано ее применение. Кроме того, мы попытаемся объяснить технологии, применяемые для построения онлайн-системы защиты данных.

Инструменты, используемые для разработки программного обеспечения

Python: это интерпретатор, высокоуровневый язык программирования общего назначения.
Pycharm: это интегрированная среда разработки (IDE), используемая в компьютерном программировании специально для языка python.
SQLite: это библиотека программного обеспечения, которая обеспечивает реляционную систему управления базами данных.

Проверка инструмента отчетности

В терминах компьютеризации тест означает процедуру частичной верификации информационной системы. Цель заключается в обеспечении того, чтобы информационная система реагировала так, как этого ожидают ее разработчики, а также конечный пользователь. Тест является основной опорой при желании создать это программное обеспечение, которое разделено в определенной

логике тестов, никто как короткий путь в системе не может дать реальную производительность всего программного обеспечения, есть причина идти краснее за краснее, чтобы гарантировать, что от, первой проверки, в конечном итоге будет с верхним хорошим уровнем конечного результата.

V-образная модель, известная в компьютеризированном мире в области разработки программного обеспечения, была взята в качестве нашего тестера для нашей системы, как показано на диаграмме ниже:

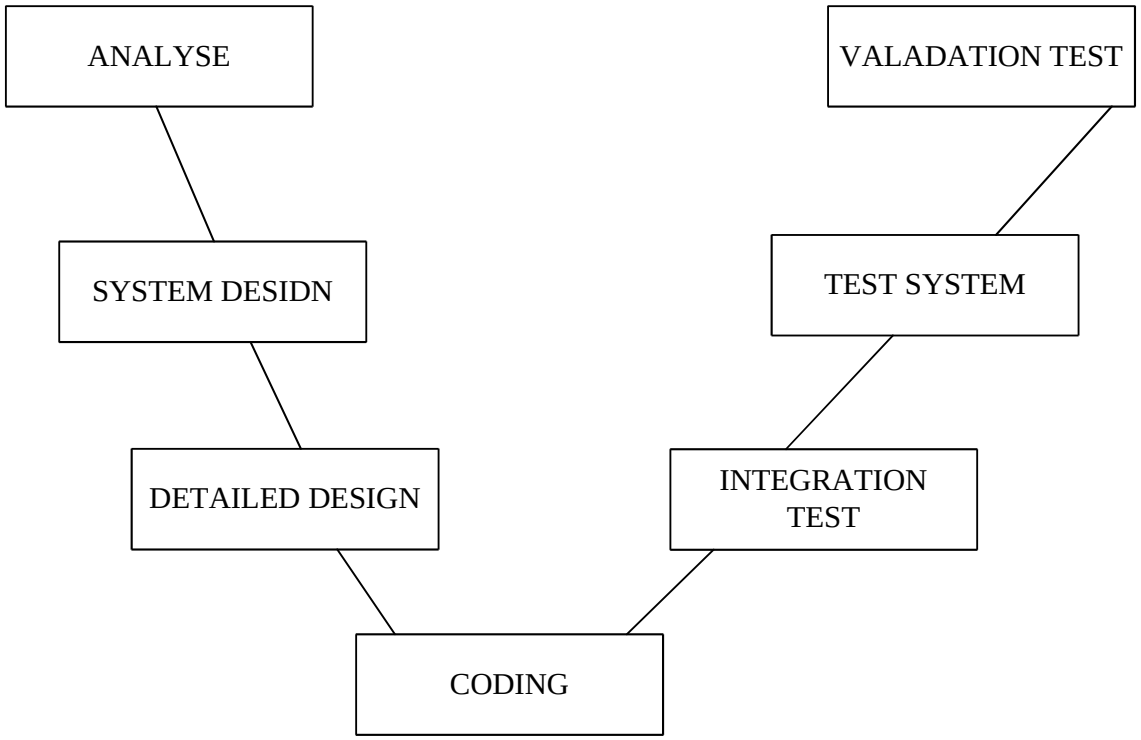


Рисунок 2: Проверка инструмента отчетности

Разработка программного обеспечения была произведена следующим образом:

a. анализ

Первый вопрос состоял в том, чтобы увидеть, нет ли какого-либо другого способа установить систему, чтобы дать решение, первый этап состоит в том, чтобы понять систему как исследователя, прежде чем предлагать какой - либо

другой, мы придумали линию, чтобы следовать на научном и логическом языке того же понимания с отделом поддержки ИКТ, V-модель, которая работает в цепочке операций при ее разработке, позволяя позади и впереди результат и директивный способ очистить все ограничения на разработку онлайн-инструмента защиты данных, который поставляется в компиляции с главой первой.

б) системное проектирование

Проектирование системы имеет своей целью вычесть из спецификации архитектуру программного обеспечения. Это было использовано во второй главе, где была описана существующая система с точки зрения ее функциональных возможностей и требований, с тем чтобы обеспечить надлежащий отклик на созданную новую систему.

в **) детальное проектирование**

Эта фаза помогает узнать данные (переменные, константы, атрибуты, поля и т. д.) и функций (процедур, методов и т. д.) которые необходимы и должны быть использованы в приложении. Мы использовали этот этап в третьей главе, где были подняты данные и процессы новой системы.

д) кодирование

Кодирование на языке информатики указывает на все развитие научного письма, где в этой области существует множество переменных языков, одним из которых был PHP, который закончился созданием источника кодов для использования при интеграции в тесте.

е**) интеграционный тест**

Интеграционный тест используется для того, чтобы пройти через систему

кодирования, сделанную ранее для проверки и проверки сборки различных частей программного обеспечения, идущих к ногам или для указания ошибок. После того, как нет связи от одного кода к другому, наша работа занимает длительный срок, а также тестируется во всем проекте, чтобы быть использованным в качестве программного обеспечения для взаимодействия с пользователями в настоящее время, чтобы позволить одному генерировать результаты и достижения ожидаемого результата.

В нашей работе после выполнения различных тестов мы протестировали весь проект, чтобы увидеть, хорошо ли взаимодействуют различные части программного обеспечения и позволяют ли они генерировать результаты и достигать ожидаемого результата. Во время теста мы использовали различные значения, чтобы увидеть, действительно ли программа делает то, что она должна делать.

ё) испытание системы

Системное тестирование программного или аппаратного обеспечения тестируется для проведения на завершенной интегрированной системе с целью оценки соответствия системы ее заданным требованиям.
Мы использовали этот тест для проверки графических пользовательских интерфейсов, безопасности системы.

ж) проверка

Валидационный тест имеет важное значение, так как необходимо проверить, соответствует ли настройка приложения выраженным потребностям.
Мы провели этот тест с будущими пользователями, чтобы они могли проверить наше приложение исходя из своих потребностей и ожидаемых результатов

Online Data security System Graphical interface

Это очень важный этап. Ужасная концепция пользовательских интерфейсов может привести к меню анализа журналов:

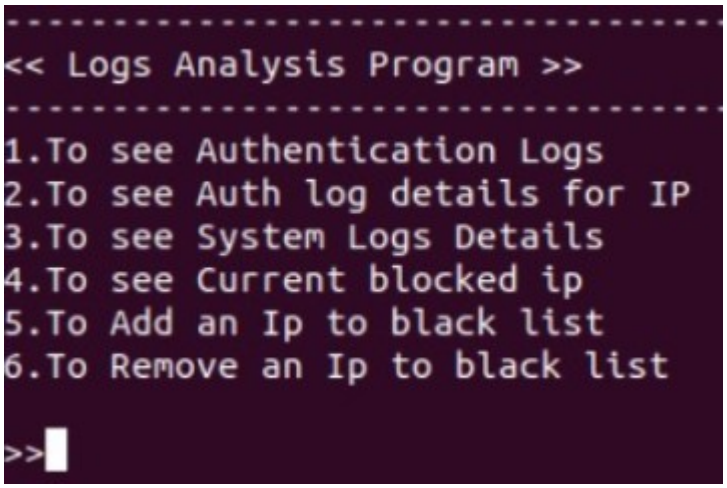


Рисунок 3: программа анализа журналов

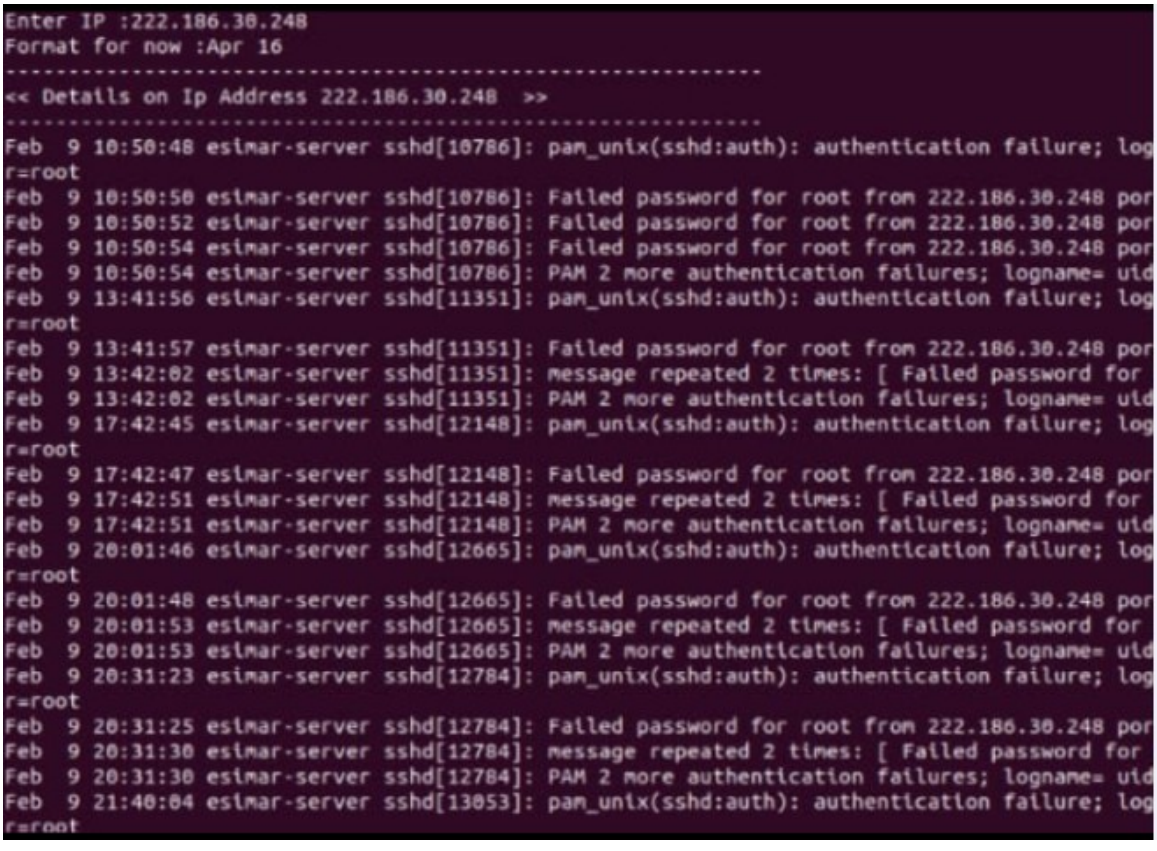


Рисунок 4: подробная информация об IP-адресе

Глава 5

ЗАКЛЮЧЕНИЕ И РЕКОМЕНДАЦИИ

Вывод

Прежде чем мы завернемся, ни одна бумага не получит полного взгляда без надлежащего заключения. В настоящее время онлайн-безопасность данных стала модным словом в сфере безопасности и имеет голую необходимость для любой онлайн-безопасности данных. Онлайн-система защиты данных для онлайн-системы ОИЯИ, безусловно, обеспечит лучшие услуги по защите данных для более правильного обслуживания онлайн-системы, чего не может сделать необеспеченная система. Поведение хакеров будет легко обнаружено. Но успех любой онлайн-программы защиты данных зависит от ее правильного планирования и выполнения. Следовательно, специалисты по безопасности данных должны предпринимать правильные инициативы в правильном направлении.

Рекомендация

Выполняемые проектные работы ограничиваются системой онлайн-защиты данных для онлайн-систем ОИЯИ. Я был бы очень признателен, если бы другие институты использовали эту новую систему, и поскольку я не знаю, что будет в будущем, исследователи могут улучшить ее в соответствии с потребностями.

ссылки на литературу

[1] CIO Asia,September 3rd,H1 2013:Cyber security in malasia by Avanthi Kumar

[2] International Journal of Scientific& Engeneering Research, volume 4,Issue 9,September-2013 page nos.68-71 ISSN 2229-5518, Study of cloud computing in Healthcare Industry by G. Nikhita Reddy.

[3] Ramez Elmasri, Shamkant B. Navathe (2011). *Database Systems (6th ed.).* United States of America: Pearson Education

[4] Fischer, P., MacDaniel, J.,& Hughes, J. (n.d)*System Development Life Cycle Models and Methodologies.* Retrieved on March 25, 2019 from http://famed.ufrgs.br/pdf/csih/mod3/Mod_3_3.htm, 2020

[5] ROCHFELD A. et MOREJON J., La méthode Merise, Tome 3, les éditions d'organisations, Paris, 1986.

[6] A beginner's guide to network security, CISCO Systems, found at http://www.cisco.com/warp/public/cc/so/neso/sqso/ beggu_pl.pdf, 2019

[7] Brenton, C. and Hunt, C. (2002): Mastering Network Security, Second Edition, Wiley

[8] Farrow, R., Network Security Tools, found at http://sageweb.sage.org/pubs/whitepapers/farrow.pdf,2019

[9] Importance of Network Security, found at http://www.content4reprint.com/computers/security/importance-of-network-security-system.htm,2019

[10] McClure, S., Scambray J., Kurtz, G. (2009): Hacking Exposed: Network Security Secrets & Solutions, Sixth Edition, TMH.

[11] Stallings, W. (2007): Network security essentials: applications and standards, Third Edition, Prentice Hall.

[12] CIO Asia,September 3rd,H1 2013:Cyber security in malasia by Avanthi Kumar

[13] International Journal of Scientific& Engeneering Research, volume 4,Issue 9,September-2013 page nos.68-71 ISSN 2229-5518, Study of cloud computing in Healthcare Industry by G. Nikhita Reddy.