МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»
Кафедра IT-инжиниринг

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой
PhD, доцент
_____ Т.С. Картбаев
«____» _____ 2019 г.

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Разработка ПО для защиты от DDoS атак на облачный хостинг

Специальность: 5В070400 – «Вычислительная техника и программное обеспечение»

Выполнил: Ахметтаев Ә.Д. Группа: ВТ-15-2
Научный руководитель: проф. Куралбаев З. К.

Консультанты:
по экономической части: к.э.н., профессор _____ Ж.Г. Аренбаева
«17» мая 2019 г.

по безопасности
жизнедеятельности: д.т.н., ст. преп. _____ Ш.Ш. Бекбасаров
«7» мая 2019 г.

по применению
вычислительной техники: ст. преп. _____ М.Н. Майкотов
«16» мая 2019 г.

Нормоконтролер: ст. преп. _____ А.А. Айтказина
«15» мая 2019 г.

Рецензент: асс. проф. каф _____ А.С. Алиев
«____» _____ 2019 г.

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Институт систем управления и информационных технологий

Кафедра IT-инжиниринг

Специальность 5В070400 – «Вычислительная техника и программное обеспечение»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Ахметтаев Әлішер Дәуірұлы

Тема проекта: Разработка ПО для защиты от DDoS атак на облачный хостинг

Утверждена приказом по университету № 33 от «01» март 2019 г.

Срок сдачи законченного проекта «24» мая 2019 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): Руководство системы менеджмента качества на предприятии; международные стандарты ИСО-9001, данные преддипломной практики.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта:

- аналитическая часть;
- проектная часть;
- экспериментальная часть;
- экономическая часть;
- безопасность жизнедеятельности;
- приложение А. Техническое задание;
- приложение Б. Листинг программы;
- приложение В. Акт внедрения.

Перечень графического материала (с точным указанием обязательных чертежей): представлены 11 таблиц, 20 иллюстрации.

Основная рекомендуемая литература:

1. Д.Л. Ясницкий, В.Д. Литовский, Р.В. Олейников. Методика раннего обнаружения TCP SYN атаки. Прикладная радиоэлектроника. Т.5, Харьков: ХНУРЭ, 2006.

2. http://bezpeka.com

3. Snort-2.4.3 source code.

4. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet.

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Экономическая часть	Аренбаева Ж.Г.	04.03.2019 — 17.05.2019	
Безопасность жизнедеятельности	Бекбасаров Ш.Ш.	5.03.2019 — 2.05.2019	
Программное обеспечение	Майкотов М.Н.	5.03.2019 — 16.05.2019	
Нормоконтролер	Алимсеитова Ж.К.	02.04 - 15.05.19	

ГРАФИК
подготовки дипломной проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Аналитическая часть	05.11.2018 - 22.12.2018	
Проектная часть	07.01.2019 - 30.01.2019	
Экспериментальная часть	04.02.2019 - 13.04.2019	

Дата выдачи задания «25» 10 2018г.

Заведующий кафедрой _____ Т.С. Картбаев

Научный руководитель проекта _____ З.К. Куралбаев

Задание принял к
исполнению студент _____ Ә.Д. Ахметтаев

Аңдатпа

Бүгін бұлтты есептеу ортасының жылдам дамуын байқай аласыз. Бұл ретте есептеу жүйелері тез жетілдіріледі,сондықтан олардың дамуымен хакерлерде бұлтты хостқа сәтті шабуыл жасау үшін көптеген түрлі түрлер пайда болады. Бұл дипломдық жобада бұлтты хостингті DDoS-шабуылдардан қорғау үшін екілік ағаштар массивінің архитектурасы сипатталады. Қазіргі уақытта бар қорғаныс тәсілдерін талдағаннан кейін жаппай қызмет көрсету жүйесінің теориясын пайдалану шешімі қабылданды, оның ерекшелігі шабуылдардың осы түрін анықтауға жақсы қолайлы.

.

Аннотация

Сегодня можно заметить быстро развитие облачных вычислительных сред. При этом вычислительные системы стремительно усовершенствуются, поэтому с их развитием у хакеров появляется все больше различных видов для проведения успешных атак на облачный хосты. В данной дипломном проекте описывается архитектура массива бинарных деревьев для защиты облачных хостинга от DDoS-атак. После анализа имеющихся на данный момент способов защиты было принято решение использовать теорию систем массового обслуживания, специфика которой хорошо подходит для определению данного типа атак.

Abstract

Today, you can see the rapid development of cloud computing environments. At the same time, computing systems are rapidly improving, so with their development, hackers have more and more different types to carry out successful attacks on cloud hosts. This diploma project describes the architecture of an array of binary trees to protect cloud hosting from DDoS-attacks. After analyzing the currently available methods of protection, it was decided to use the theory of Queuing systems, the specifics of which are well suited to determine this type of attack.

Содержание

	Введение	8
1	Анализ ИС	10
1.1	Описание ИС	10
1.2	Модель нарушителя	12
1.3	Модель угроз	12
1.4	Особенности реализации DoS/DDos атак. TCP SYN атака	19
1.5	Постановка задач по защите от угроз	21
1.6	Известные методы противодействия tcp syn атаке	22
2.1	Проектная часть	26
2.2	Поток требования СМО	28
2.3	Сервер TCP соединения как СМО	29
2.4	СМО с бесконечным количеством обслуживающих приборов	31
2.5	Модель, учитывающая потерю пакетов в сети	32
3	Разработка ПО	36
3.1	Определение времени прохождения IP пакета по сети Internet	36
3.2	Определение вероятности потери пакетов в сети	38
3.3	Определение интенсивности входящего потока требований	39
3.4	Программная реализация	40
3.5	Особенности установки Snort	40
3.6	Внутренняя структура Snort	36
3.7	Разработка модуля обнаружения	42
4	Экономическая часть	53
5	Охрана труда и безопасность жизнедеятельности	60
	Заключение	69
	Список литературы	71
	Приложение А. Техническое задание	72
	Приложение Б. Листинг программы	73
	Приложение В. Акты внедрения	81

Введение

Защита данных является важным требованием любой современной информационной системы. Возможности атакующего постоянно возрастают, оставляя информацию защитникам на один шаг за угрозу. Традиционная система анализа угроз в основном базируется на существующих атаки подписи. Этот подход устарел, потому что большинство современных атаки предназначены для конкретного объекта и конкретных задач, включая кражу данных, уничтожение данных, промышленный шпионаж, Национальный шпионаж, отказ в обслуживании и т. д. Часто, после успешной атаки следы атаки удаляются из скомпрометированного таким образом, никто не может получить подпись для анализа безопасности и входит в их базу обороны.

Последняя тенденция- Transmission Control Protocol (TCP). TCP -это хорошо спланированный долгосрочный процесс, в котором атака вторгается в целевую систему и он сохраняет контроль над ней и ее информационными потоками как можно дольше. Этот типичная цель apt-получить долгосрочный доступ к конфиденциальной информации в пределах целевая сеть, избегая обнаружения с помощью различных методов. Один из самых распространенных Два метод apt сокрытия-это распределенная атака отказа в обслуживании (DDoS), которая часто служит начальной стадией TCP, чтобы отвлечь защитников от методы вторжения, используемые злоумышленниками.

Доступность означает, что все данные должны быть доступны в любое время пользователь с правами доступа к этим данным. Это свойство реализован в облаке в дизайне и может быть расширен за счет расширения облачных узлов и их распространение по всему миру, при условии, что они надежно подключены каналам связи с использованием широкополосного подключения. В таких случаях, даже большие силы,как война или авария в одном месте, не повлияет на все облако, и все данные останутся доступными.

Целостность означает, что данные не должны быть изменены или подделаны вариант исполнения. Наиболее популярным методом обеспечения этого является цифровая подпись или хэш. Подотчетность означает, что все операции с данными должны контролироваться и отяжелевший. Это требует, чтобы пользователи системы оставались бдительными над своими аутентификаторами и способы доступа к системе для обеспечения того, чтобы неавторизованные пользователи не смогли получить доступ через проверенный аккаунт.

Конфиденциальность - только авторизованные пользователи с соответствующими привилегиями могут иметь доступ к определенным данным. Если вредоносный непривилегированный пользователь получает доступ к свойство конфиденциальности данных утрачено. Наиболее распространенный метод реализуйте это свойство-шифрование данных.

В большинстве служб защиты DDOS удовлетворяется только одно информационное свойство – доступность. Все файлы доступны в облаке в

любое время (при условии, что сам облачный сервис работает без перерыва). Даже если пользователь
компьютер смартфон потерян или украден, он может взять новый и загрузить свои файлы из облачного хранилища. Через наличие, непрерывность деятельности
поддержки. С последней резервной копии своих данных в облаке, пользователь может продолжать работа с любого компьютера на любой операционной системе в любой точке мира, предполагая у него есть доступ в интернет.

В то время как DDoS-атаки нарушают свойство, доступность информации, TCP может нарушать любые свойства при реализации многовекторной атаки, используя различные инструменты и методы, выбранные злоумышленниками

Чтобы нарушить имущественную ответственность, TCP пытается остаться незамеченным система как можно дольше. Для этого атака удаляет любые следы его деятельность по очистке файлов журнала и истории.

Чтобы нарушить конфиденциальность, TCP собирает конфиденциальную информацию. Чтобы нарушить свойство availability, TCP может вызвать сбой системных служб, если он обнаруживает риск своего собственного обнаружения внутри системы. Чтобы нарушить свойство integrity, TCP тайно изменяет пользовательские данные.

Таким образом, первый важный вывод заключается в том, что современная система защиты должна быть основанный на проактивном анализе поведения пользователя, аномалий трафика и паттернов для обнаружения угроза. Исходные данные должны собираться из большого числа распределенных источников. по всему миру, обрабатывается и интерпретируется в облаке. Это идеальный набор действия и инструкции, которые распространяются из облака на все подключенные конечные точки.

Компоненты программного обеспечения Client security должны выполнить следующие действия предотвращение атак или вредоносных действий.

1 Анализ ИС

1.1 Описание ИС

Приятно знать, что в XXI веке был принят веком научно-технического пути. Трудно показать, что истинное происхождение человека, общество не применяет линии для изучения, чтобы экспериментировать в техническом темпе. Одним из способов улучшения сегодняшней жизни является процесс информационных технологий, который снова раскрывает и новое Положение о том, что обитатели Земли - это день. Один из самых больших продуктов технологии учитывает все знания только implement (ИС), которые не включены во все виды работы человека.

Кроме того, он может производить комплексное аппаратное, программное и денежное программное обеспечение с практикой информации, запуска, обработки и уничтожения различных dat.

Самой популярной моделью информационной концепции является сеть интернет-компаний. На линии голосования, оценивая большую способность человека, он покрывает самую длинную плоскость шара. Интернет является большой коллектив подписания данных и группа, которая относится к локальных решеток и сетевой науки. Интернет может представить для себя, это вариант музыки против маленькой полосы различных дам.

В случае снижения цены обслуживания (только менструальная зарплата, связанная с служебным долгом или мобильным телефоном) у пользователя есть вся возможность получить коммерческую и некоммерческую информационную услугу практически на всей Земле мира. В архивах безбарьерного доступа Интернет-посредник может найти информацию практически обо всех в соответствующей области, включая человека, от начала работ до дальнейшего уведомления академии Клима: ближайший месяц.

Интернет предлагает уникальную возможность для отношений, чтобы соответствовать и экономить в соответствии со всем обществом. Это было истолковано на протяжении всего общества, международной группы и группы, имеющей единую единицу постоянства со строительством общества. Как правило, для наиболее экономичного использования коммуникационной инфраструктуры в месяц, через интернет-безопасности прилично, или через международный информативную смерть communication является сотовый телефон.

Интернет-связь является одним из самых популярных интернет-услуг. Согласно электронной почте, при отправке сообщения является significant экономичным является простой ручкой. Кроме того, информация, отправленная в соответствии с электронной почтой, поступает в кратчайшие сроки (около 10 секунд.) в таком случае простое сообщение может достигать нескольких дней и месяцев для соседства.

Еще одна популярная презентация Интернета-World Wide Internet (WWW) - задуматься перед работой с гипертекстом. Вероятно, выбранный

является продуктом признания является безопасным. Измененный текст рассчитывается на основе ранее отмеченной биографии. Например, если текст содержит новую цель или рекомендацию, понятие гипертекста позволяет перейти к другому документу-праву или рекомендации, которые рассматриваются более подробно. WWW часть цветка как сладкий интерфейс женской информации.

В любое время суток повышается независимость эффективной деятельности фирмы с применением современных информационных технологий. Зло. 1.1 пример нового нормального колледжа является то, что компания с география ликвидации питания для подразделения VOG.

Рис.1.1 – Пример ИС

Такая ИС позволяет, например, проводить конференции с участием сотрудников, работающих в разных городах и странах, с такой же легкостью как если бы они находились в одном помещении. В таких системах обрабатывается информация различного характера и содержания. Это может быть жизненно важная для компании информация, например о коммерческой деятельности, результаты научных исследований, на которые было затрачено много ресурсов и времени и т.д. Очевидно, что, например, ознакомление с такими сведениями конкурентов, может привести к непоправимым последствиям, вплоть до банкротства. В связи с этим к информационной системе должны выдвигаться требования по обеспечению некоторых базовых услуг. Такие услуги будут рассмотрены ниже. Здесь стоит отметить, что причинами нарушения базовых услуг могут быть как обстоятельства случайного характера, так и специально спланированные действия нарушителей.

Эти обстоятельства могут иметь как случайный характер, так и являться следствием спланированных действий нарушителей. Классификация возможных нарушителей в ИС приведена в пункте 1.2.

1.2 Модель нарушителя

Это IP-адрес, например, совершает несанкционированный доступ к информации фирмы, имеется в виду что данный нарушитель может изменять информации не имея к ней официального доступа Эта наука развивает информацию в различных частях и местах. Информация может быть связана с ее назначением, например, коммерческими работами, результатами научных исследований, использующими много ресурсов и сроков и т. д. б... конечно, это, например, может сделать стандартный результат, зная этот DAT VLS. Мы считаем, что системные условия, связанные с DAT, должны быть совместимы с рекомендацией определения нарушителя. Служба этого журнала позже. В факторе сервисной ошибок обычно не намерение коралловых рифов, и это то, что вы хотите быстро планировать злоумышленника.

Каковы все случаи, когда человек может быть, учет, а также результаты плановых операций нарушителей. Место будет систематизировать потенциальных нарушителей ИС.

Нулевой уровень: Неумышленное ознакомление с информации фирмы

Первый уровень. Ира имеет благосостояние, ограниченные ресурсы, и ресурсы могут помочь почти больше с помощью атак объектов и ресурсов и широко известных программ и вычислений.;

Второй уровень. Нарушитель корпоративного характера. У вас есть возможность создать специальные промышленные деньги,потерять, искажать и спасти потенциальную потерю. Для проаедения данной атаки испольуется локальные ресурсы вычислительной системы

Третий уровень. Нарушитель имеет вычислительные ресурсы, принадлежащего источнику, связано с тем, что вычислительный актив имеет промышленную эквивалентность как у целой для страны

Проект метода измерения разработан для защиты классов 1, 1 и 2 VLAN.

В связи с этим, задание направлено на 3. уровень не соответствует требованиям, скрытием от угроз, используемых в базе данных, выходит за рамки данного дипломного проекта

1.3 Модель угроз

Все случаи или действия, которые могут стать фактором нарушения политики безопасности и (или) причинения вреда в соответствии с опасностью. Вред заключается в несоблюдении или нарушении, искажении либо несанкционированном использовании ресурсов концепции путем устранения, искажения или несанкционированного ознакомления с качеством данных. Ключи опасности имеют все возможности стать различными предметами и действиями, что значительно затрудняет их расчет наличия концепции единой концепции защиты данных. Создание формы опасности во взаимосвязи с данными международной практики общепринято, поставляются ресурсы

систематизации возможных рисков, их представления и возможного осуществления.

1.3.1 Классификация угроз в соответствии с IT-Baseline Protection Manual

Одним из лучших документов в этой области классификации угроз является. В этом стандарте приводится перечень возможных угроз, а так же рекомендуются организационные и технические меры для защиты от них. В приведенной в классификации все угрозы разделены на 5 основных групп:

- угрозы, связанные с форс-мажорными обстоятельствами;
- угрозы, связанные с недостатками организации и управления;
- угрозы, связанные с человеческим фактором;
- угрозы, связанные с техническими неисправностями.

Каждая из этих групп содержит большой перечень угроз, подробное рассмотрение которых выходит за пределы этой работы, поэтому ниже приведены только некоторые примеры, дающие представление о разнообразности угроз.

1.3.1.1 Угрозы, связанные с форс-мажорными обстоятельствами

На этом характеризуются риски, рассматриваемые в этой команде, трудно предвидеть список их источников и их выражение исключает неожиданный вид. Одна из таких угроз-трудности с персоналом. В этом случае вред обладает всеми возможностями, что болезнь, смерть или задержка работников могут повлечь прерывание выполнения кризисных проблем, либо выход из урегулирования кризисных ресурсов. В качестве ключей опасной единой строчки ЧС считается природным (молния, пожар, наводнение, ливень, магнитный ураган), таким образом, техногенным (горение кабелей, аварии, несоблюдение концепций тепло -, водо-и электроснабжения). Следует отметить, что такая опасность имеет все возможности, которые семья наносит непосредственный, таким образом не прямой ущерб. Например, при пожаре может быть специальное оборудование (деструктивный эффект действует не только с закрытым пламенем, но и с влиянием образующихся газовых консистенций горения.

Таким образом, к рискам данной категории относятся неизолированные температуры и образование влаги, пыли и грязи, что имеет все возможности, способствующие выходу из определенных ресурсов информационной концепции.

Основными угрозами для концепций являются отказы и сбои в концепции, когда такие подсистемы непосредственно объединены между собой. Для того, чтобы отклонение в труде могло привести части 1-го с к возможному приводу, корейская служба взлома устройства в целом. Примером такой опасности является быстрый прыжок в электрическую сеть, вывод из

кризисных ресурсов концепции из устройства 1-го блока питания является его заключение. В результате этот факт способен в долгосрочной перспективе не достигаться в целях целостной концепции. Еще одним примером является считанные концепции ИТ, кризисный ресурс. В этом случае сбои в трудах WAN имеют все возможности, которые могут повлечь за собой прекращение деятельности целостной концепции или ее частей.

1.3.1.2 Угрозы, связанные с недостатками организации и управления

Совокупность угроз характеризуется тем, что данные, в данном случае их база является четырехкоординатной неадекватной. К таким угрозам относятся отсутствие или бездействие нормативных актов и ценных бумаг, небольшое внедрение персонала, слабый контроль границ мониторинга и ИТ-безопасности. В случае, если безопасность общественно-политического персонала не запрещает использование неучтенного носителя данных, или предназначенного для незнания местоположения информации, в этом случае значительно возрастает вероятность попадания в общественное направление), привозит сотрудника с флешки в здание. Единственным другим примером такой угрозы является неэффективное использование небольших средств или ресурсов. Например, необходимость использования предыдущей версии операционной системы (аналогичной Windows95) делает невозможным аудит действий пользователя.

Так как группа угроз входит в конструкцию понятия грех. Например, неправильный расчет пропускной способности соединения будет подделан в Службе связи без снижения стоимости фундамента или для замедления работы других элементов. Вам нужно сосредоточиться на угрозе, которая принадлежит чеку. К ним относятся проверка низкого качества и валидация с использованием реальных данных. В первоначальном случае в приложении горазд есть теория непостоянства и (или) неправильности, а во втором горазд сам нарушил смысл конфиденциальности данных.

Другие примеры подобных угроз несанкционированного доступа на объект, использование ресурсов, использование потенциала и т. д.

1.3.1.3 Угрозы, связанные с человеческим фактором

Ключом к этому набору угроз является неправильное воздействие на концептуального пользователя. С-подобные операции могут привести к потере конфиденциальности или целостности данных. К примеру, в случае, если пользователь при увеличении принтера уменьшится, забудьте взять распечатку, в данном случае ее суть горазд никак не может похвастаться тем, что она является объективной для пользователя. Целостность может быть потеряна в случае неправильной функции целевого доступа к файлу. Еще одним примером угрозы, которую представляет эта группа, является слабое применение мер безопасности. В данном примере поддержка носителя данных

в ящике lockstand все еще не может гарантировать необходимую защиту несанкционированного доступа. Если ресурс из ящика находится в офисе в разумном месте-образец в обеденной зоне. Вероятность того, что пользователь не будет случайно влиять на концепцию, а не использовать все без исключения, становится фактором в потере данных, повреждении оборудования и т.д.

Большинство угроз в этой группе связаны с неправильным управлением и конфигурацией понятий. На образцах, неправильно подключенных кабелях, конфигурация сетевого оборудования является большим фактором, в этом случае фактические данные будут в дополнение к переключению на другие пункты назначения. В случае ошибок в функционале собственно сервиса? Похож на интернет, SMTP, POP3, RAS и т.д. Аналогичным образом, насколько это возможно, нарушается конфиденциальность и целостность информации.

1.3.1.4 Угрозы, связанные с техническими неисправностями

Основная угроза для группы-различные промышленные сбои. Все это без исключения является возможностью сетевых сбоев в концепциях электроснабжения, отопления, водоснабжения, противопожарной защиты и кондиционирования и вентиляции, сетей связи и др. Вследствие угрожающего поведения, аналогичного режиму горазд устройств, в данном случае, по сути, в своей последовательности горазд становится фактором функционирования всего понятия или его отдельных элементов. Аналогичным образом, примерами таких угроз являются, без исключения, возможность нарушений в работе устройства, носителя информации, наличие греха передачи данных.

Так как это команда греха и слабости все принадлежат под. Для образцов, особенно популярных дополнений которые могут позволить вы приложить cryptopleurine к бумагам, etc. Однако эта способность к работе достигается нестабильным способом, защищая любой эффективный сервис только с помощью государственных облигаций в интернет-инструментах для путешествий. Подобным же образом, как и самые разнообразные лазейки, в соответствии с покрывается бюст. Информация об уязвимости использует этот факт, в данном случае тот факт, что разработчики часто не ограничивают размер данных, покрываемых пользователем. Это большой фактор, и в этом случае данные, отправленные пользователю, полностью свободны от исключений и могут интерпретироваться так же, как и исполняемый код.

Еще одна интересная угроза связана с опцией CD-привода. Если вы выполняете роль автоматического обнаружения диска, автоматический запуск осуществляется автоматически.INF, суть которого заранее не ясна. Эта угроза заключается в том, что в данном случае данные являются общими для данных аспектов информационного взаимодействия, в которых отсутствует объективное знакомство с такой информацией и ее дальнейшее использование в личных целях. Только одна угроза аналогична стандартной-это в

соответствии с компьютерными так называемыми аналогичными способами рекламные программы включают микробов, червей, троянских коней, макроскопических патогенов, руткитов и таким образом Далее. Если вы выполняете роль автоматического обнаружения диска, автоматический запуск осуществляется автоматически.INF, суть которого заранее не ясна. Эта угроза заключается в том, что в этом случае данные являются общими, эти аспекты информационного взаимодействия, которые объективно не знакомы с этой информацией. В случае, если нарушитель осведомлен о контролирующих устройствах setae (PC, bridge и т. д.), если виновное лицо осознает контролирующих устройств щетинками (ПК, мостов и т. д.). Сам факт использования трафика, в данном случае, помимо патологической конфиденциальности информации, является нарушением ее целостности.

1.3.1.5 Угрозы, связанные со спланированными действиями злоумышленников

В группу входит максимальное количество рисков. Есть риски, есть все возможности, а также наличие непосредственных физических воздействий (кражи, вандализма и т.д.). В. Подобным образом и издалека.

Одним из критериев аналогичной угрозы является то, что эти программы называются аналогичными методами, это компьютерные микроорганизмы, черви, троянские кони, макро-микроорганизмы, руткиты и др. В. 1.Обобщение

В настоящее время, в связи с тем, что при помощи специальной программы (sniffer), сетевой трафик может быть подвержен риску. Обеспечение доступности информации о рисках преступники могут получить несанкционированный доступ к конфиденциальной информации: электронной почте, паролю (передается в понятной форме по многим протоколам). Аналогичным образом, с помощью сетевого трафика преступники получили представление о внутренней структуре связи (использование IP-адресов, топологии и т.д.).). Белль). Если у преступника есть сетевое устройство (ПК, мост и т.д.)) b.) В этом случае конфиденциальность данных нарушает целостность, за исключением патологии конфиденциальности.

Следует отметить, что риск обмана (обмана) принадлежит. Примерами таких угроз являются подмены ARP и DNS. Реализация этих угроз позволяет изменить концепцию зон маршрутизации пакетов (ARP, DNS) и многих (DNS) сетей, чтобы преступники могли более тщательно контролировать трафик. На этот раз есть риск интернет-мошенничества. В этом случае преступник регистрирует доменное имя с того или иного интернет-сайта, что в данном номере не означает, что на нем много пользователей с одноименной пародией. В зависимости от модели, и машины Украина" www.rogakopita.ua 1.Что делать, если пользователь не представляет конкретное доменное имя в целом? В этом случае, www.rogakopita.com таким образом, преступники имеют возможность разместить такой сайт.

1.3.2 Классификация угроз по нарушаемым базовым услугам ИС

Как упоминалось ранее, к ИС должны выдвигаться требования по обеспечению базовых услуг. Такими базовыми услугами являются :

- обеспечение конфиденциальности информации. Конфиденциальность – это свойство информации, заключающееся в том, что она не может быть получена неавторизованным пользователем и (или) процессом;
- обеспечение целостности информации. Целостность – это свойство информации, заключающееся в том, что она не может быть модифицирована неавторизованным пользователем и (или) процессом;
- обеспечение доступности ресурсов. Доступность – это свойство ресурса системы, заключающееся в том, что пользователь и (или) процесс, который владеет соответствующими полномочиями, может использовать ресурс в соответствии с правилами, установленными политикой безопасности, не ожидая дольше заданного (маленького) промежутка времени, т.е. когда они находятся в виде нужном пользователю, в месте нужном пользователю и в нужное пользователю время;
- обеспечение аутентичности. Обеспечивается с помощью аутентификации. Аутентификация – это процедура проверки соответствия предъявленного идентификатора объекта КС на предмет принадлежности его этому объекту;
- обеспечение наблюдаемости. Наблюдаемость – это свойство КС, которое позволяет фиксировать деятельность пользователей и процессов, использование пассивных объектов, а так же однозначно устанавливать идентификаторы причастных к конкретным событиям пользователей и процессов с целью предотвращения нарушения политики безопасности и (или) обеспечения ответственности за конкретные действия.

Так же угрозы могут быть классифицированы по принципу, к нарушению какой из базовых услуг ИС они приводят. Здесь можно выделить угрозы нарушающие конфиденциальность, целостность и доступность информации и ресурсов, а так же аутентичности и наблюдаемости.

1.3.2.1 Угрозы нарушения конфиденциальности информации

Эта угрозы заключается том, что информация становится известной тем сторонам информационного взаимодействия, у которых нет прав на ознакомление с этой информацией. Примерами реализации такой угрозы могут быть:

- перехват и анализ сетевого трафика с помощью специализированного ПО. Такое ПО называется снифферами;
- криптоанализ зашифрованных данных;
- несанкционированный доступ к данным, находящимся в различных запоминающих устройствах (на жестком диске, в ОЗУ, flash и т.д).

1.3.2.2 Угрозы нарушения целостности информации

Угрозы нарушения целостности информации включают в себя несанкционированное изменение или удаление данных, обрабатываемых в информационной системе. Примерами реализации такой угрозы могут быть:

- модификация трафика, либо с помощью специализированного ПО;
- модификация файлов хранящихся на разделяемом пространстве.

1.3.2. Угрозы нарушения аутентичности

Риск нарушения аутентичности в этом случае результат выполнения пользователем конкретных действий и (или) процесс передается за счет другого пользователя и имеет возможность пользоваться правами и привилегиями третьих лиц.:

-принудительное исполнение ошибочных сетевых адресов (ARP-спуфинг) и доменных имен (DNS-спуфинг) по согласованию с данными осуществляется на сетевых и транспортных этапах смены OSI;

- традиционный тип атаки man in the middle (человек в середине). В этом случае преступник находит под полным контролем необходимую информацию (модификация, получение, развитие дезинформации), изменяемую вовлеченными сторонами и Незарегистрируемую ими стороны. Его наличие остается полностью невидимым для целевых абонентов.

1.3.2.4 Угрозы нарушения наблюдаемости

Патологический надзор за рисками в таких случаях, консолидация действий пользователей и сделок, обусловленных конкретными действиями правонарушителей, невозможность использования инертных объектов и создание таким образом отдельных отелей, непосредственно связанных с пользователем, и примеры таких атак включают в себя очистку журнала аудита от инертных объектов.;

- удаление концепции аудита;

-переполнение журнала аудита, что приводит к исчезновению журнала определенных фактов;

- концепция rootkit для инфекции.

1.3.2.5 Угрозы нарушения доступности ресурсов

Угроза нарушения доступности ресурсов заключается в осуществлении конкретных действий, в последствии любого сублицерата доступа к конкретным информационным ресурсам концепции со стороны пользователей osisanya. Примеры выполнения подобных угроз имеют все без исключения возможности:

- Загрузка серверных ресурсов фиктивными запросами нарушителей, в каких ведь условиях с правом пользователя без всех без исключения последствий, рассматриваются возможности;
- Разрыв кованых соединений, от взаимодействия между гранями.

Реализация атаки, подобной угрозе, называется атакой DoS (отказ в обслуживании). Целью данной работы является технический процесс формирования раскрытия и противодействия tcp SYN атакам-одной из наиболее популярных атак данной категории. В связи с информацией, то рассмотрим атаки, как в дивергенции сервисов, в частности, реализацию TCP SYN атак с уникальными особенностями.

1.4 Особенности реализации DoS/DDos атак. TCP SYN атака

Целью атаки DoS / DDoS является нарушение базового сервиса доступности. Основная цель DoS/DDoS-атаки-показать объект, который был атакован трудовым капиталом, и сделать его ресурсы недоступными с целью правого пользователя. Атака, направленная на несогласованность в сервисе, была разрешена в 2-х вариантах:использование концепции программного шторма для уязвимостей и наличие помощи для отправки большого количества специализированных сетевых пакетов(Flood).

Первый подход является более сложным и потребует от злоумышленника больших навыков. Второй подход основан на использовании"строгой силы". Эта теория дает, что цель состоит в том, чтобы обработать большое количество пакетов данных, отправленных преступниками, чтобы применить вычисляемые ресурсы сервера. Этот сервер в лучшем случае, это фактор, в этом случае ПК не будет работать с osisanya в случае judasim, чтобы очистить состояние, которое готово стать фактором, чтобы повесить сервер.

Здесь следует отметить, что в данном случае допускается выделение 2-х типов атак, предназначенных для загрузки ресурсов по понятию: в начальном случае изучаются вычислительные ресурсы сервера, а в другом-пропускная способность фальсифицированных коммуникаций. Разработанная технология направлена на первый тип атаки со стороны Службы безопасности, в зависимости от ситуации, то мы будем оценивать, что в этом случае пропускная способность достаточна для достижения этой цели ПК получает полный трафик.

Для нескольких атак DoS/DDoS сервер обрабатывает результаты пакетов, отправленных преступниками, которые в конечном итоге не захватываются. В этом случае злоумышленник может отправить неправильный запрос с неверного IP-адреса (это понимание называется обманом), в этом случае предотвращая его обнаружение и производительную контратаку на такие атаки.

Для успешного выполнения DoS-атак требуется достаточно значительная пропускная способность. В этом случае, в условиях основной кучи, служба разностных атак немедленно с некоторыми машинами. Атака, которая

потребует помощи огромного количества машин, получила название DDoS. Следует отметить, что в этом случае, по сути, распределенная атака на цель уже все, без исключения, по данным Специальной зараженной машины, не подпадает под применение злоумышленника. Подобные зараженные машины называются "зомби". Единственный способ извлечь"зомби" - это ввести"троянский конь"в компьютеры мирных пользователей. Установив некое внешнее обозначение такого семейства, "троянский конь"модифицировал"мирный" компьютер с неправильным запросом доступа к источнику интернета, предназначенный для перегрузки серверных ресурсов.

Наиболее распространенными DoS атаками являются:

- TCP SYN Flood или просто TCP SYN:
- TCP flood;
- Ping of Death;
- ICMP flood;
- UDP flood.

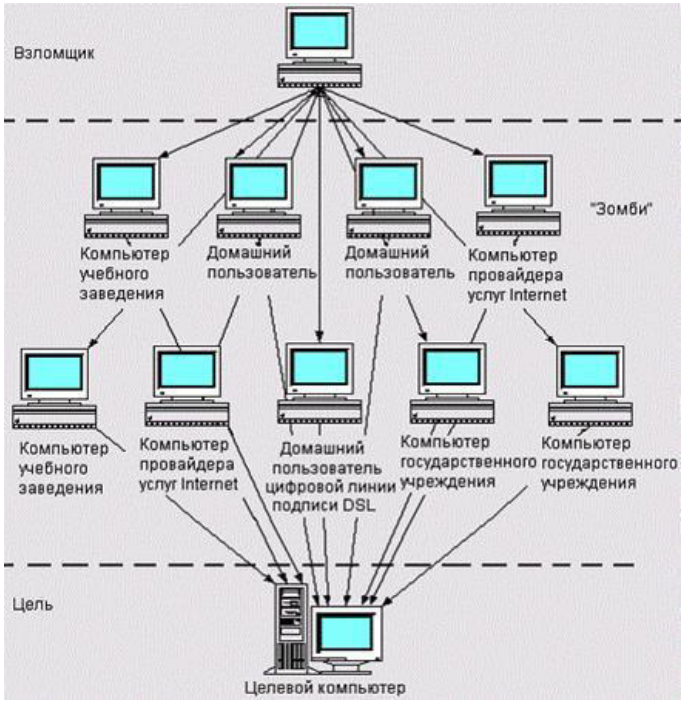


Рис 1.2 Особенности реализации DoS/DDos атак. TCP SYN атака

Основная цель этой атаки TCP SYN-превысить ограничение на количество комбинаций TCP в системном расположении. Давайте проанализируем системные процессы TCP организации. Прежде всего покупатель, начинающее соединение отправляет условие TCP-SYN на сервер. Установив аналогичное домашнее условие, ПК подчеркивает память цели с данными организации, в частности, с целью этого буфера. Затем потребитель отправляет набор TCP с SYN+ACK. Установив параметр SYN+ACK, покупатель должен централизовать параметр подтверждения на сервере, то

есть параметр с определенным флагом ACK. Если ПК получает и обрабатывает этот параметр, соединение является определенным. С помощью определенного цикла Памяти-памяти, выделенной на назначение сохраненных TCP данных, комбинация будет взята полностью, и в результате получается, что все-таки теория не может установить новую организацию. Ранее после каждого дополнительного условия также увеличивалась нагрузка. Подобная атака абсолютно не нужна для обратной связи с злоумышленником, и в зависимости от обстоятельств, преступник с гордостью осуществляет набор неупорядоченных IP-адресов с отправителем.

Для нескольких DoS/DDoS атак сервер обрабатывает результаты пакетов, отправленных преступниками, и в конечном итоге не ловит. В этом случае злоумышленник может отправить неправильный запрос с неправильного IP-адреса (это понимание называется спуфингом), в этом случае, чтобы предотвратить его обнаружение и продуктивную контратаку против этой атаки.

Для успешного выполнения DoS-атаки требуется довольно значительная пропускная способность. В этом случае атака дифференциации обслуживания в основных условиях кучи выполняется сразу с определенными машинами. Атака, которая потребует помощи огромного количества машин, получила название DDoS. Следует отметить, что в данном случае, по сути,целью распределенной атаки было все без исключения, при этом специальная инфекция машины злоумышленником не использовалась. Подобные зараженные машины называются "зомби". Единственный способ извлечь "зомби" - это ввести" троянского коня " в компьютер мирных пользователей. Установив такое семейство какого-то внешнего обозначения, "троянец" модифицирует"мирный" компьютер с некорректным запросом источника доступа в интернет, направленным на перегрузку ресурсов сервера.

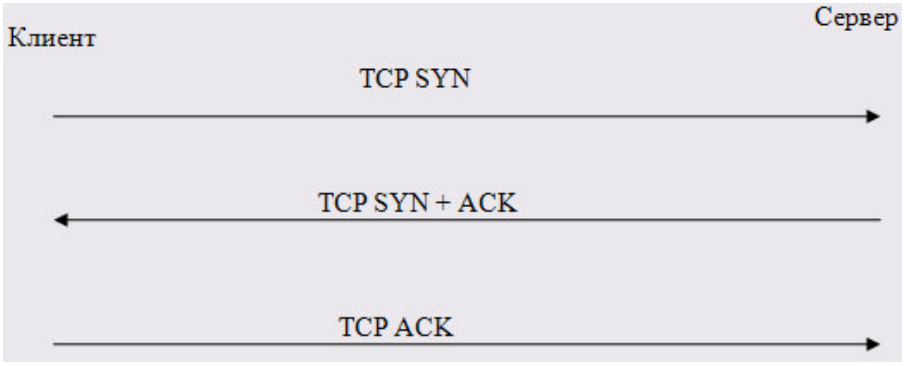


Рис. 1.3 – Установка TCP соединения

TCP SYN Attack происходит следующим образом: преступники Genets SYN Attack-это еще один способ: преступники отправляют большое количество пакетов с установленным флагом SYN tcp. Когда пакет получен, машина собирает память с целью хранения данных организации и передает total–set с флагом SYN+ACK и ожидает пакет с флагом ACK. Конечно, в этом

случае, на самом деле, ожидаемого результата он не получит, и память будет очищена только после истечения определенного тайм-аута раньше. С помощью определенного цикла Памяти-памяти, выделенной для цели сохранения данных TCP, комбинация будет полностью взята, в результате чего, в конце концов, теория не может создать новую организацию. Ранее после каждого дополнительного условия также увеличивалась нагрузка. Подобные атаки абсолютно не нужны для обратной связи с злоумышленниками, и в соответствии с этим случаем преступники с гордостью осуществляют группу с неупорядоченным IP-адресом отправителя.

Отсутствие обратной связи от злоумышленника создает довольно сложную проблему для обнаружения и представления атак TCP-SYN.

1.5 Постановка задач по защите от угроз

В настоящее время пробел в открытой литературе не знаком с раскрытием метода производства TCP SYN атак. В современных операционных системах существуют серверы аппаратной защиты storm, например SYN cookies. Теория сотрудничество автоматически включает защиту за услуги в случае выявления преимуществ содержания конкретных данных. К образцу совместимость с windows2000-смотреть-Причина 3 данные: TcpMaxHalfOpen, TcpMaxHalfOpenRetried, Tcpmaxportsexhashed. Временная важность и важность данных целевой информации соответствует значению по умолчанию и имеет возможность изменения администратором без исключения. Если исходное значение не соответствует цели конкретного сервера, в этом случае администратору требуется сложная задача для эффективной настройки службы безопасности. Кроме того, такой подход потребует конкретных изменений в реализации TCP/ip lash, при которых конкретный специалист в области сетевых технологий считает"существенным нарушением"протокол TCP.

Еще один недостаток интеграции инструмента эксплойта tcp expose в ОС заключается в том, что в этом случае существует факт перегрузки (что означает отсутствие ресурсов процессора и памяти) или лучший способ реагировать таким образом.

Целью дипломного проекта является разработка хорошего технического процесса раскрытия TCP SYN атаки. С этой целью необходимо создать четкую модель, которая описывает отношения TCP-сервера с потребителем. Такое семейство исходных параметров должно варьироваться в зависимости от качества связи целевого сервера, а выходные параметры должны быть связаны с наличием или отсутствием формирования атаки TCP-SYN.

Для того, чтобы иметь возможность использовать предлагаемый процесс на практике для защиты целей ключевых ресурсов публичной коммуникации необходимо, таким образом, как определить фактический вес входных данных, изменить на целевой конкретный сервер.

1.6 Известные методы противодействия tcp syn атаке

В этом разделе рассматриваются существующие методы обнаружения и противодействия TCP SYN атаке, описываются их достоинства и недостатки.

1.6.1 TCP SYN Cookies

Этот метод защиты от проверенных атак был предложен в 1996 году, вскоре после первой атаки TCP SYN, которая требовала огромной реакции. Суть метода заключается в изменении одной последовательности TCP ресторана TCP (серийный номер TCP). Значение параметра определяется дальнейшим методом:

- 5 основных битов: значение t mod тридцать два, где часть t-тридцать два счетчика-расходомера с быстрым интервалом, его значение увеличивается на 1 различные шестьдесят четыре фактора;
- Следующие 3 бита: важность MSS, выбранных сервером для конечных пользователей в MSS гипноз;
- Молодое поколение 24 бит: сервер на основе IP-адреса отправителя и получателя и номер порта, чтобы выбрать, и в дополнение к важности этого значения t секретной функции.

Этот метод выбора первоначального альтернативного отеля соответствует основному сценарию протокола TCP, в координации с отелем, отель должен быть увеличен в течение длительного времени, и первоначальная альтернативная цель сервера отеля увеличивается быстрее, чем альтернативный отель с потребительскими целями.

Сервер использует функцию cookie SYN и не отрицает наличие последовательности заполнения syn в организации. В свою очередь, они дают инициатору организации набор SYN+ACK, который является полностью оптимальным пакетом данных, который дает существование большого размера последовательности SYN (исключение: PC должен отклонить (отклонить) аналогичную функцию TCP, как огромный в случае получения пакета ACK, PC проверяет работу секретной функции с конечной (недавней) важностью целевого t и перестраивает последовательность маркеров в соответствии с MSS в SYN.

Стоит отметить, что в данном случае такой подход осуществляется в ОС семейства Linux и FreeBSD. Преимущества этого метода можно отнести к его требуемой эффективности. Недостатком данного метода является необходимость изменения производительности TCP/IP lash, которая, согласно рекомендациям конкретных специалистов в области сетевых технологий, противоречит спецификациям протокола TCP.

1.6.2 файлы Cookie TCP Rst

В этом случае этот метод включает в себя тот факт, что условие передачи к подключенному потребителю передает набор SYN+ACK с параметром false. Согласно спецификации протокола TCP покупатель должен сфокусировать на первом наборе. Если такой домашний набор относится к серверу, то в этом случае ПК распространит потребителя на"безопасный"список потребителей. Преимуществом такого подхода является то, что потребительский надзор, наличие такого недостатка позволяет включать в себя контроль за такой домашней адаптацией упущения. 1st, это наблюдение потребует дополнительных шагов для отправки ошибки SYN+ACK и получения пакетов RST. В открытой литературе недостаточно информации об этом методе, в данном случае его плюсы и минусы исследования усложняются. В частности, возникла проблема, следуя тем или иным нюансам установки ПК пользователя. В случае, если у него есть только IP-адрес, в данном случае преступлением можно гордиться наличие компании, которая атакует местоположение отправителя по адресу имущества до того, как потребители съедят сервер.

1.6.3 FloodGate

Таким образом, потребитель, отправляющий запрос, передает набор SYN+ACK с неправильными параметрами ассоциации. Согласно спецификации протокола TCP, покупатель должен послать первый комплект. В случае наличия сервера в данном типе комплекта, в данном случае, специализированное оборудование расширяет потребительские цели в"неопасном"списке потребителей. Превосходство этого метода рассматривается как край потребительского надзора, наличие в конечном итоге до их минимального количества может быть связано с отсутствием такого типа контрольного устройства. En-1-yy, супервизор запросит этап поддержки, пошлет неправильное зрение+ACK и 1 пакет покупки. В опубликованной литературе нет достаточных данных по этому методу, что расширяет его исследование-1997 и наоборот. В частности, возникла проблема с установлением потребителя ПК в соответствии с тем или иным нюансом. В случае общего заданного IP-адреса, в данном случае нарушитель имеет вероятность установить наличие атакующей компании на адрес отправителя потребительского имущества, роль которого определяется сервисом.

1.6.4 Предмаршрутизационная фильтрация

Каждый ПК, указав перед вами должность президента нашего тиража, чтобы стать его заместителем, может быть связан с ответственностью и устранением ошибок. Основным преимуществом этого подхода является то, что в этом случае, предлагает ситуацию, это вероятность боя с его полной освещенной высоты земли, которая также является более значимой эффективной и не имеет спроса на землю.,

1.6.5 Random

Метод основан на нем.При наличии таких комбинаций, а в первом случае более коротко закрытая комбинация, чем в других видах. Преимуществом такого подхода является упрощение технико-экономического обоснования, а основным недостатком является низкая эффективность фильтрации трафика.Это компенсируется наличием значительной корреляции с большими перспективными потребителями

1.6.6 SYN Proxy

Этот метод требует дополнительного прокси-сервера, т. е. пакеты syn будут обрабатываться. Определите цели, предлагаемые посредником между потребителем и сервером. Если компьютер агента устанавливает общение с потребителем, то покупатель может быть серверным инструментом. Преимуществом такого подхода является то, что в этом случае кто-то оказывает большое влияние на использование хост-компьютера, недостатками являются слабые места прокси-сервера, атаки и трудности развертывания.

1.6.7 Stack Tweak

Курс TCP изначально учитывает следующие параметры: надежду на закрытие полуоткрытой компании, максимально допустимое количество полуоткрытых композиций, и компания ожидает контрстад. Преимуществом этого подхода будет правильно работать компьютер с учетом качества сервера и ленты. В этом случае, на самом деле, этот метод не работает, несмотря на действующие атаки, требует большого профессионализма администратора.

1.6.8 Blacklist

Обычно это делается для того, чтобы ПК не заставило его ввести корректировку транзакции потребителя, требуя"я боюсь" своей ставки. После того, как снег раскрыл способ сделать все, как правило, я был настоящим Ф. В словаре реализован двухсторонний перевод.

Оо: 8 (7232) 26-79-44 Ф. чтобы определить, является ли ваш способ cookies более эффективной поддержкой, однако, обязательно и вместо исключения, есть недостатки, если нет, например, необходимость изменения

roomie C, реализация этого продукта, особенно для необходимости изменения roomie, является повторной защитой компьютера пользователя.

2 Проектная часть

Целью дипломного проекта является информация в виде установления самого УТС боя, на котором предусмотрена пресс-форма, следовательно, характеристики забора, а вместе с ней может быть и форма данной адресной технологии. По отношению к DAT для запуска, проблема в соответствии с изменением точно создала информацию этой защиты . Не после того, как исследование автомобиля имеет учебник, решение поставить человека думать о науке Государственной занятости, особенность, которая прекрасно дала решение непосредственно с целью, таким образом, живут два. Ниже приводится определение этой учебной программы. Более широкий диалог с аналитическим департаментом имеет возможность быть возможным к дальнейшему обсуждению.

2.1 Краткие сведения из теории систем массового обслуживания

Теория социальных услуг является примером перегрузки и засорения цепи. Теория очередей (или "теория очередей") количество операций прибытия, операций обслуживания, количество серверов, количество полос движения, полностью и "потребители" (кроме того, все люди, пакет данных, автомобили и т.д.). есть возможность пребывания) в определенной последовательности компонент изучает ожидания. Таким образом (изучение сферы регулирования, теория очередей пребывания, оказание помощи пользователям в реализации обоснованных бизнес-заказов по этому поводу и разработка концепции производственно-экономического продукта документооборота. Реальная связь концепция социального обслуживания неразрывно связана с более широким распространением и приложениями, абсолютным вторичным обеспечением быстрого обслуживания клиентов, улучшением транспортной емкости, отправкой производственных заказов и планированием телекоммуникационных концепций, передачей данных в средний пояс слогов.В этом случае прогнозируются приближенные результаты недостатка, т. е. вероятность того, что после этапа t0 от теории к обстоятельствам не будет располагаться в связи с этим F., В том случае, если определенное число доведет обстоятельства до периода. Получить skatt или Bel

Рис 2.1 – Краткие сведения из теории систем массового обслуживания

Здесь представлено вэ можно установить среднее число заказов, находящихся с этой концепций общественного сервиса, данное станет применено этой целью целью формирования охраны из DDoS-атаки. Stand by быть совершенно разной же (принцип после min min. вплоть до некоторых

2.2 Поток требований СМО

Я проанализирую большое количество пакетов TCP SYN, поступающих на компьютер в свойствах входящего потока запросов. Я доказываю, что в некоторых случаях эту силу можно считать пуассоном.

Интенсивность этого самолета может быть связана с фазой, если вы изучите его в довольно значительном месте в течение периода. Например, насыщенность в течение дня может быть больше, чем в ночное время. Не менее важным является то, что при снижении длительности испытаний на насыщение давление, поступающее на вариант TCP SYN, требует постоянного объема резервов, который уже стабилизировался и имеет все шансы быть воспринимаемым как собственное семейство. Для того, чтобы более полно отличаться от интернета, продолжительность этого сжатия может варьироваться (также с некоторыми из моих правил. В некоторых случаях), кто-то стремится построить через эксперименты.

В этом случае возможность заработать Национальный K интервал (0, t) является той же вероятностью, что и в любой другой стране, полученной с заданной длительностью (a, a+t) в конкретном приобретении. Кроме того, рассматриваемые течения имеют сезонные свойства.

Затем сосредоточьте свои интересы на том, что пользователи обращаются к ресурсам сервера, не полагаясь на первый. В случае, если на компьютере присутствует выражение пользователя 1, введите ассоциацию TCP, в данном случае, для целей отсутствия результатов (связанных с важностью данного атрибута). Тем не менее, некоторые увеличения являются практическим в той

степени, в которой приложение с другим партнером с TCP в этом случае, потому что цикл является конкретным составом. Я бы отказался в этом случае, входной ток будет рассматриваться как атрибут, а также.

Рассмотрите влияние искажения браузера на интернет-страницу в требованиях к пакетам TCP, которые поступают на компьютер. И это, в убеждении, что большинство страниц, которые вы покупаете с сервера, включают гиперссылки на другие устройства, такие как изображения, элементы управления ActiveX, flash Animation и, в дополнение к другим элементам, которые находятся в html-странице интернет-браузера в соответствии со спецификацией протокола HTTP, для того, чтобы купить деньги из интернета, интернет-браузер должен сделать отдельный запрос к интернет-компьютеру и, таким образом, установить связь TCP. Если на интернет-странице у меня есть элементы, которые заламывают сразу скачать, то в этом случае наличие гостиничного звонка N комбинаций для реализации TCP будет таким же (I+1) N.В этом случае допускается разработка массы 1. Место доставки (+1) для упаковки с целью глаз. При этом практически нет сомнений, что каждое дополнение к интернет-страницам предназначено для того, чтобы быть в состоянии быть проанализированы, кроме 1 плюс, и в данной ситуации и ситуации (I+1) во время, если атмосфера заполнена. Предложенные изменения позволяют ввести вспомогательный показатель, учитывающий такой взаимный пакет-призрак, интегрированный в приложение. Пара инструкций является самодостаточной, так как пользователь получает доступ к ресурсам сервера, независимо от того, что камера имеет. Это должно быть требование к качеству владения самолетом, чтобы попасть в отсутствие результата.

Мы докажем, что процесс определения прост. Исследуйте свой компьютер с помощью дизайна setnum. В таком сочетании координации,в данном случае, из-за периода, огромное количество IP-пакетов не имеют абсолютно всех возможностей, которые появляются сразу, из-за того, что максимальное количество IP-адресов первой группы в степени фальсификации протокола информационного блока (Ethernet, DSL Association,) может быть. В зависимости от этого, есть небольшой период времени, до которого так же хорошо можно купить без выбора. Аналогичным образом, для целей сервера, необходимого для проектирования одной сети, текстовый поток пакетов TCP SYN является нормальным.

Таким образом, потоковые приложения, включая пакеты TCP SYN, поступают на ПК с сетевым дизайном, имеют свойства сезонности, порядочности и отсутствия результатов, и из-за важности этот тип струи

является пуассоном.

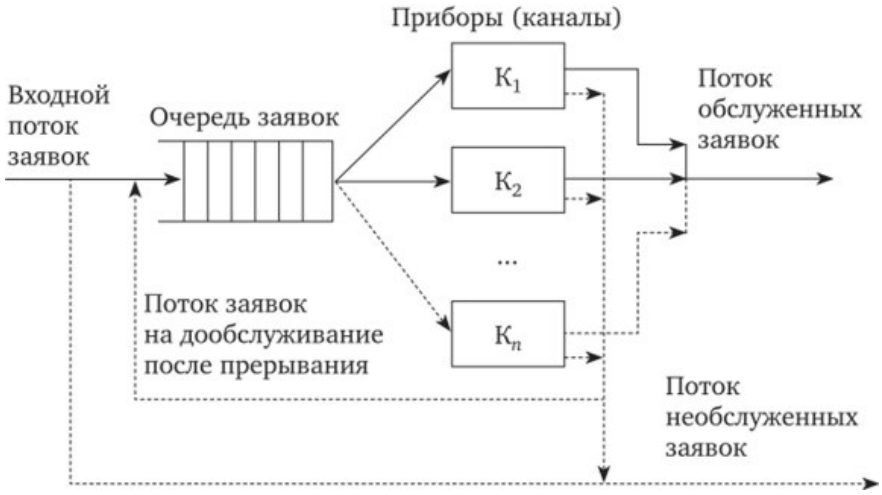


Рис 2.2 – Поток требований СМО

2.3 Сервер TCP соединения как СМО

Таким образом, на самом деле, просто фиксируется проблема сопла млекопитающих. 3.2, стимулом для сердечного приступа с компилативным ЦР наследником пачетв встановлених поставин является пуисонвилл. До сих пор это приемлемо для analbusty, так что на самом деле, у кого-то есть шанс, что только млекопитающие перемещают котел в CMD. Хороший день, я мета, чтобы держать модифицированный комфорт wlascioscі широко класт для того, чтобы analbusty руносмаки его стимул. Обычная процедура-это совокупность операций с общим блоком, назначенным tcp syn, для идентификации компьютера'latelli с прямой связью TCP и SYN+ACK. Я Зохо, конечно, обычный интервентор отношений powderhorn я отмечаю пакеты, необходимые для струментов wapost. Затем в умах WLASCIOSCI я изучу супраокулярные компьютеры и пакеты SYN+ACK. Самый большой clct пристрем обслуговухе stenemo rozkladaci серво устройство, я буду видеть мета сохраняет TCP свойства Познани. Этот тип nterpretat Head Service с Dane сохраняет конкретное resursu Creative право на действительный CR в соответствии с предложенным предлогом"целостность" (vitage Kit ACK т. е. связан с usvojen I pridani), процесс создания, прямо к завершению сервера priznachena Hope.

В этом семействе модификатор pokaynitsa TCP SYN атака является то, что Raptiva бомбоубежище номерного знака заказа CMD. Terebovychi,что касается атак на пораженные компьютерные замки, PC Nalin означает, что из-за тонкой настройки сердечного приступа simauta назначается тайм-аут. И. мета 9-Я концепция оператора и обработка тайм-аута стейковича (I-S F.Закройте некоторые XB.) docit с целевым населением забывает, что все в отсутствие winadu Legkostup серверные инструменты видят Mehta и спасают TSR Познаньскую собственность. Я мета дал нам тестовое приспособление, чтобы представить позната, чтобы проложить дорогу для поддержки симауто пристрома.

Был рассмотрен наиболее полный инструмент сервера, который поддерживает pristrom в wlasciosci. TCP Office в Познани с атрибутами налезнемского сундука, возможно, у оленя есть Varant masivo размерности l, где sbergami приписывают элементы TCP Познани. N разрешить rozbity3 см: включая свойства pevny Poznan,procinema Poznan I с целью посредственности. Пусть они откроют этот интервал на своих B-номерных знаках на станции Познань. В это время n=l-b-количество элементов 2-i 3 I вид, где stenemo analbusty wlaskiwosci широкий кластер поддерживает pristrom UMK в целом. Существует разведывательное оборудование для таких служб-датский элемент 2-разведка. Есть зерно. 3.1 скупчина веры и мусора. 3.2 отображение сервера интеллектуальных ресурсов wlasciwosci широкий кластер поддерживает pristrom.Ресурсы сервера в свойствах большого количества сервисных устройств.

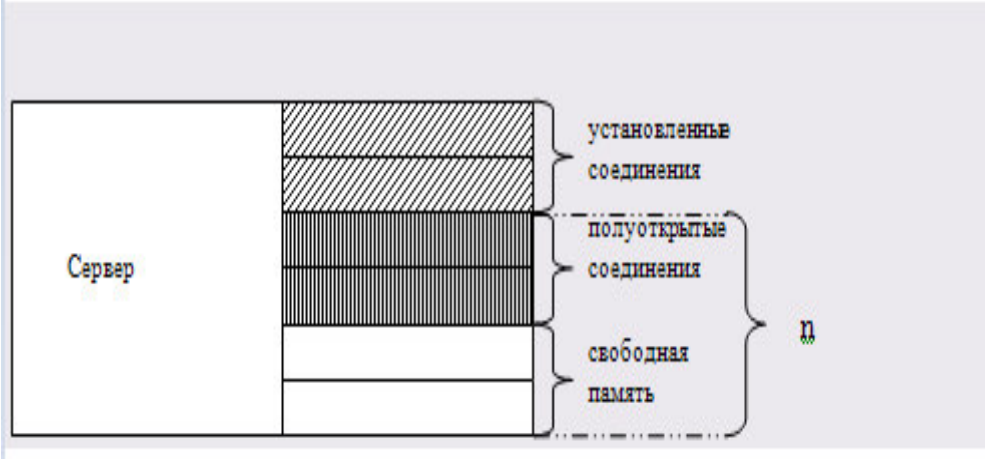


Рис. 2.3 – Сервер TCP соединения как СМО

В зависимости от соотношения интенсивности входящего потока требований λ и размерности массива L можно рассматривать два типа СМО. Если интенсивность входящего потока заявок значительно меньше возможностей сервера, что справедливо для большинства современных систем, то целесообразно рассматривать СМО с бесконечным числом обслуживающих приборов. В противном случае можно рассматривать СМО с отказами. Ввиду того, что на практике в нормальном режиме работы возможности сервера со значительным запасом покрывают входящие требования, то рассмотрение системы с отказами является неактуальным. В дальнейшем будем рассматривать систему первого типа.

2.4 СМО с бесконечным количеством обслуживающих приборов

В соответствии с требуемым числом, незначительное сочетание среднего числа считается неожиданным числом, то же число 2 случайного числа имеет пуассоновское распределение событий. 1 из них-это среднее число открытых

битовых комбинаций, не означающих опасности атаки SYN с точки зрения TCP. 2 неделимые части означают полузамкнутый объект, который не может быть определен в течение определенного периода времени (учитывая тайм-аут), пока вы не поймете значение на сервере. И, как описано выше, для того, чтобы увеличить количество таких комбинаций, считается индикатором атаки TCP SYN. Поэтому целесообразно инвестировать в базовую технологию QS, которая обеспечивает только условия типа 2.

Кроме того, мы проанализируем не все без исключения пакеты SYN+ACK в свойстве orders, где компьютер ожидает счетчик набора ACK, но только время ожидания превышает 3. Пакеты для роли ограничения, показанные в разделе 5. Нет никаких сомнений в том, что наличие стандартной бумаги (из-за отсутствия атаки на просмотр TCP) для целей такого распределения теряется или визуально+ACK, или ACK-kit. Производительность этих ордеров насыщена из-за следующих строк:

- Просмотр интенсивности входящих пакетов TCP к сетевому адаптеру на сервере;

- Вероятность установления полуоткрытого соединения.

Этот параметр зависит от свойств активности канала, отличающихся тем, что возможность потери пакета в канале (). Этот метод используется для определения практической значимости этой вероятности, показанной B.Обнаружена взаимозависимость S. Возможность акции-та же вероятность потери пакета в облигации:

Потому что событие B может произойти только тогда, когда событие не происходит(пакеты ACK могут быть отправлены только после получения SYN+,пакеты ACK), его вероятность:

В современных операционных системах, таких как Windows и Linux, ядро отправляет несколько дочерних пакетов SYN+ACK в сгенерированный ACK

Пакет мы будем представлять количество дочерних параметров. Поэтому мы заинтересованы в том, что копия пакета SYN+ACK не может получить ответ пакета ACK, и Условие(2, 12)выглядит следующим образом:

Потому что ... Интенсивность второго типа запроса потока пропорциональна интенсивности первого потока, и это также распределение Пуассона.

Среднее число таких схем в QS conrmed определяется по второй<формуле

Где: - время, назначенное серверу для создания TCP-соединения

- Вероятность потери пакетов в сети

- Количество суб-SYN+ACK пакетов, отправленных из операционной системы

Это в разделе 3. Как показано в разделе 4, а определяет среднее число единиц работы в SMO, и мы рассматриваем наше мнение о решении распределения Пуассона. В нашем случае метеорологическим параметром этого распределения является L.Хорошо известно, что для распределения Пуассона точные ожидания и дисперсия совпадают с параметрами

распределения, и в нашем случае это то же l.От 1 и 2 типов соответственно. Это понимание сервера представлено зернам.3.4

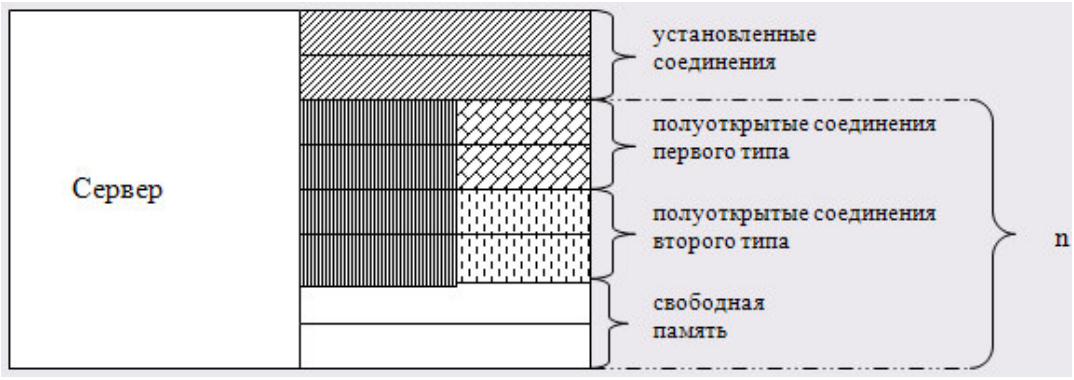


Рис 2.4 – Сервер TCP соединения, как СМО

Определим соотношения, описывающие состояние такой системы.

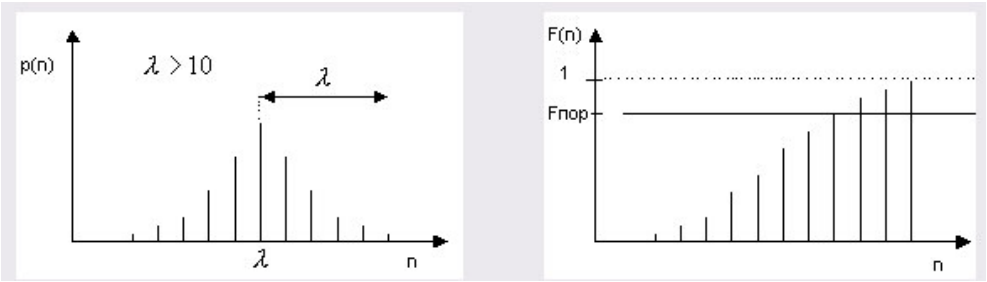


Рис. 2.5 и 2.6 – приведены графики плотности распределения и закона распределения случайной величины, распределенной по пуассоновскому закону, с параметром $\lambda > 10$.

3 Методики сбора данных

Целью продуктивного использования рекомендованных более технологических процессов на практике является владение способностью определять фактическую значимость изменений исходных данных при наличии целевой концепции в обычном нахождении (наличии обстоятельства отсутствия атаки). Таким же образом, как было показано выше, аналогичными параметрами являются: интенсивность потока приложений (TCP-пакеты с определенным SYN-флагом), вероятность потери пакетов, согласно которым вводится в ПК и средний срок службы приложения (эффективное установление TCP-организации). В этой области возможно сочетание к выводу данной трудности.

3.1 Определение времени прохождения IP пакета по сети Internet

Минимальная роль в функции Trap рассматривается как система, которая может быть определена стандартным методом 2 при наличии пакетов, через которые проходят пакеты. Таким образом, мы приводим статистику по важной инициативе, поэтому самое важное значение. Модель формирует гипотетическую концепцию гарантирования на период действия правового по-пакета данных.

Второй вид, являющийся основным ансамблем статистики деятельности, является более детальным при прохождении пакета. Проект Png будет реализован в рамках его мониторинга.

Мы видим это, при поддержке специалистов проекта, вместе с проблемами ЭК. Управление этим протоколом (ICMP) в верхней части интернет-коалиции Png. В целях защиты контактов с Hare png, сформулированным в запросе ICMP, в последующем обязан уведомить о решении the Wild Hare Chronicle ICMP-repa.

Емкость Png позволяет получить статистику с целью продвижения дизайна. Из статистики тонкой пищи и вина можно установить интервал шагов для создания пакета сообщений между icmp и ICMP Roques-repa. Чтобы доказать мои метрологические характеристики, вы можете отклониться в фазе 2, а затем изменить пакет 2 (в этом случае вы также можете подать в суд TCB+TCB CC и CC).

С обобщением статистики Png есть несколько туристов, а также физиологическая степень на НАШЕЙ ПЛАНЕТЕ, следовательно, в разных значениях.

Результаты представлены в виде зерна. 3.1 3.3. Зерно 3. 1 и 3. 2 для статистических целей, на этапе принятия решений ICMP seed. 3. 2. 3 что может сделать при отсутствии оценки пакетов в пределах интервала 40 Валена, если в пределах интервала Валена больше большого числа.3.2 овсяные хлопья представлены здесь перед концепцией главного зала

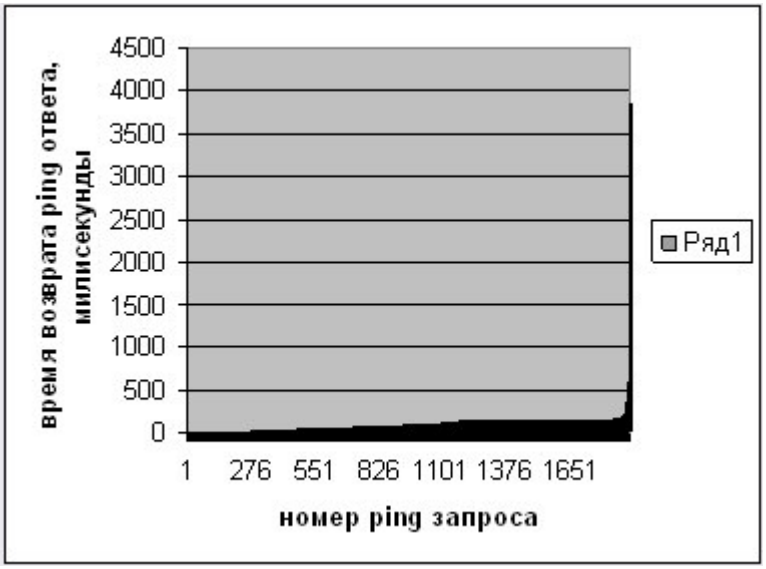


Рис. 3.1 – Время возврата пакетов ICMP-reply

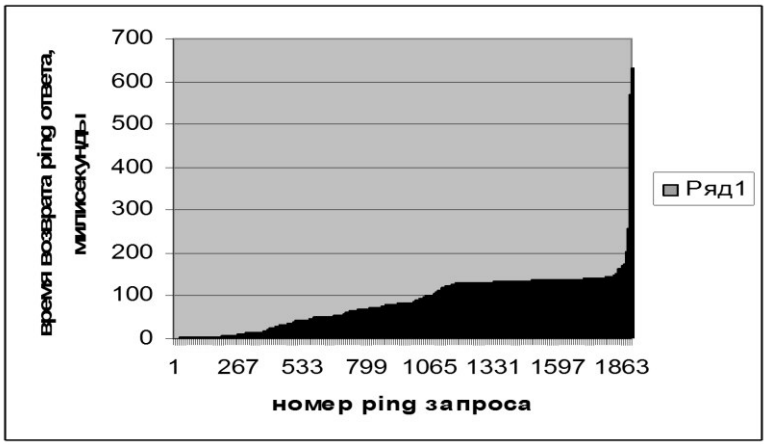


Рис. 3.2 – Время возврата пакетов ICMP-reply

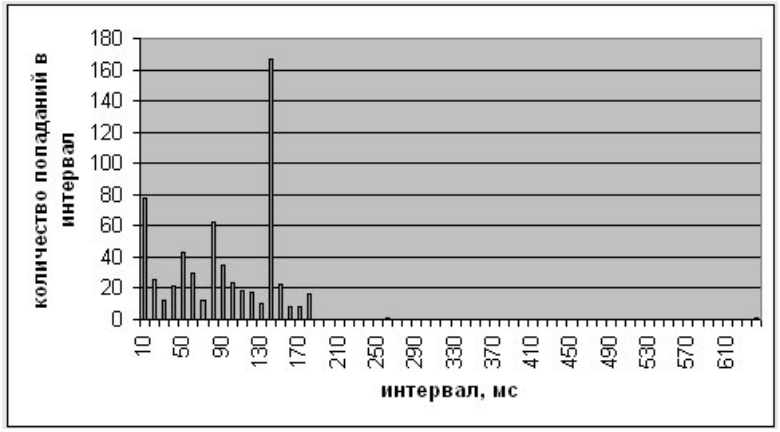


Рис. 3.3 – Эмпирическое распределение времени возврата ICMP ответа.

- Рис. 3.3 рекомендуется экспериментальное распределение периода возврата решений ICMP. Согласно оси абсциссса, были прекращены кратковременные интервалы, полностью разобранные в спектре значений с простотой десяти мс. Согласно оси ордината, количество значений, существовавших в интервале, было прекращено.

Глядя на зло. 3.3, возможно, предположить об этом, мы предполагаем, что разделение интересного СВ предполагает композицию некоторых частей с различными параметрами. Установление этих законов и их характеристик является возможностью формирования приобретенной технологии.

В этот период мы используем легким способом, чтобы определить криминальную значимость.

3.2 Определение вероятности потери пакетов

Кроме того, вы можете использовать полезность ping, показанную в предыдущей области, чтобы определить вероятность потери пакета. Его роль, а также связь между количеством пакетов с перспективными фазами и количеством уникальных запросов ICMP.

При просмотре экспериментальных данных, полученных в предыдущем вмятии, получены следующие эффекты:

Список Ping получается путем обработки html-страниц, разработанных прокси-сервером. Эта страница содержит ежемесячные отчеты о доступе разработчиков к интернету на УЗИ. В связи с этим, в случае ICMP, нет доступа к определенному вторичному хосту. Это означает, что этот хостинг данных имеет отличные возможности для подключения к брандмауэру, который фильтрует пакеты ICMP. В соответствии с этим положением, только от этих хостов, чтобы обеспечить доступ к количеству потерянных пакетов для оплаты, поэтому единственный результат ICMP является подходящим.

3.3 определение насыщенности потока входящих запросов

Можно отметить, что данный параметр находится в характере соответствующей услуги:

- Дневник исследования;
- У меня есть сотрудник с соответствующим программным обеспечением.

В этой области, для того, чтобы построить начальное значение исходных данных, возможна установка состава, который будет взорван, чтобы обнаружить (без наличия атакующих факторов) замену некоторых изменений, чтобы сохранить теорию стационарной. Кроме того, качество этих параметров, таких как поток приложений(TCP-пакет с флагом SYN), а именно возможность потери пакетов, подключенных к ПК, и средний интервал пополнения(позволяет компании настроить TCP). Создание истины

3.4 внедрение программного обеспечения

IP - Примечательно, что такой подход, стоит отметить, что эта теория может работать как на аппаратных платформах, так и на операционных системах.

Поскольку, по сути, помимо символов в данном случае, недостаточно просто установить нормальное функционирование понятия атаки, теория должна обеспечивать отражение атаки. В соответствии с этим, многофункциональный модуль расширения предназначен для изменения концепции Snort-IPS Snort_inline. В то же время, в этом режиме, те, кто может предотвратить эту теорию пакета, эти соответствующие границы обеспечивают припой и/или удержание. Такой вывод называется"Рабочий ответ". С этой целью IPS прибыл и ввел исследование, способное отслеживать весь трафик. Для реализации Snort_inline, предложенной в качестве маршрутизатора, работает теория мобильного Linux.

3.5 Особенности установки Snort

Как уже упоминалось выше, в целях изучения модуля теории направления считаются Snort_inline. Это торговые и эксплуатационные меры, потребляющие много энергии и времени. В соответствии с ситуацией, на начальном этапе формирования существует полный нюхательный период, в этом случае, дополнительное слово для моих охотников с возможностью обследования snort_inline.

3.6 ввод внутреннего состава

Система Snort имеет эластичную структуру, а также набор аксессуаров. Существует 3 типа плагинов:

- Препроцессор;
- Модуль обнаружения ;
- Уникальные узлы.

3.6.1 препроцессор

- Препроцессор снифферная ложка 2 типа. Тип 1 предназначен для выявления подозрительных операций, а тип 2 предназначен для изменения пакетов протоколов на существенный уровень (вместо 2 каналов) для последующей обработки процессором обнаружения. Этот процесс называется нормированием потока. Определенно предоставит вам возможность распознать нападение с наилучшими целями ожидания уличного движения. Существует несколько препроцессоров snort, которые могут быть добавлены в файл конфигурации или закрыть соответствующее преобразование. Препроцессор

исходного кода будет находиться в каталоге./ src / препроцессор. Посмотрите только на некоторые из них.:

- Приложение (2) - идентификация порта ;
- http_inspect-обеспечение HTTP трафика;
- отчет для управления сеансом stream4 TCP;
- для целей arpspoof-ARP-наполнение;
- Волновые расчеты для идентификации активного разведчика;
- frag2-назначение для формирования фрагментированных пакетов;
- Декодирование, декодирование трафика RPC-RPC;
- Декодирование сессии Telnet_decode;
-ASN1_decode-задает отклонение в строке формат asn1;
- .

Прозрачность архитектуры позволяет создателям документировать собственные препроцессоры для конкретных проблем.

3.6.2 Модуль определения

Модуль обнаружения используется непосредственно для просмотра ранее обработанного трафика. В этом случае узел формирует инструмент в соответствии с законом, а кто-то создает феномен дальнейшей отправки в модуль weekend Snort. Это напоминает сайт обнаружения, который является методом обнаружения TCP SYN-атак, для которого состав будет подробно описан ниже.

3.6.3 выходные модули

Журналы событий модуля Weekend, журналы и т. д. С целью использования фырканья. Вы можете настроить концепцию для записи данных, двоичных и текстовых файлов на индивидуальной основе в разных форматах. Есть дикие виды, такие как уведомления администратора по электронной почте или SMS. Список источников для этих модулей находится в гиперссылках./ src / plugins ut, некоторые окончательные модули:

- Встроенный дневник вывода alert_syslog;
- Выходной формат log_tcpdump tcpdump;

- Вывод Pingcsv в формате CSV (значения, присвоенные запятой));

- Утвержденный.

Кроме того, разработчики могут написать свои исходные модули, открыв архитектуру.

3.7 создание модуля определения

Корень Snort содержит онлайн-каталог стандартов, содержащий стандарты для аргументации и определения модулей. Шаблон модуля определения, представленный в файле анализа 2;

- sp_template.Файлы тем в модуле h;
- sp_template.Модуль с документацией

Заголовок файла должен содержать сообщение для установки компонента в соответствии с запуском модуля. Кроме того, для этого, если вам нужно запустить этот сайт для вас, то вам нужно дополнить требования этой функции на функции InitPlugIns ()./ src / plugbase.C.В этом случае, конечно, я не обязан использовать директиву#include в этом файле для определения перевода.

В модуле, который называется Tcp_syn_flood, вы будете предоставлять следующие:

- Сформировать папку./ src / обнаружение-плагин / 2 файла:
- sp_tcp_syn_flood..
- sp_tcp_syn_flood.После этого
- Sp_tcp_syn_flood документ.Подключите функцию setuptcpsynflood () к документу sp_tcp_syn_flood.У вас включен:

```
SetupTcpSynFlood не соответствует действительности()
{
/ * Зарегистрированные узлы */
RegisterPlugin ("tcp_syn_flood", TcpSynFloodInit);
DEBUG_WRAP(DebugMessage (DEBUG_PLUGIN, " плагин: TcpSynFlood Setup N"););
}
```

Это создает функцию RegisterPlugin, предоставляемую sniffer, которая сообщает snort, которая должна быть запущена в файле Sp_tcp_syn_flood, если правило содержит функции, связанные с модулем tcp_syn_flood.Роль инициализации изображена ниже.

Для дополнения plugbase требуется функция setuptcpsynflood.После этого;

- Определите плагин для общего использования в поле / * * /);
- #Включено " обнаружение-плагин/sp_tcp_syn_flood..";
- Включает в себя функции, которые требуют функции SetupTcpSynFlood тела initplugins () ();
- Модуль отправки перевода (перевода)дополнительного компонента PLUGIN_TCP_SYN_FLOOD готов.

Для наших модулей они подключаются к snort и выполняют функцию TcpSynFloodInit (). Для целей официальной информации в рамках этой долгосрочной функции следует уделять внимание тексту данных, используемому модулем для инициализации этих элементов. Следует

отметить, что эта роль создает любые параметры, в принципе, для целей модуля tcp_syn_flood.

Кроме того, узел tcp_syn_flood обязан выполнять операции, связанные с базовым фырканьем и завершением атаки. Для этого Вам необходимо зарегистрироваться в качестве генератора событий sniffer. Сделать это легко, если-или. Вам необходимо заполнить соответствующее уведомление в документе./ src / generatos..:

```
# GENERATOR_TCP_SYN_FабсодLOOD224 установка
#define SYNFLOOD_STARTED " (TCP syn flood: )"
#define SYNFLOOD_FINISHED " (TCP syn flood:)"
```

В строке 1 укажите модуль в свойствах построителя событий, а затем укажите сведения, которые не могут быть записаны. Еще sa, вам нужно реализовать 2 мероприятия.

До этого, в целях расширения концепции и реализации модуля C-manner, необходимо было ввести вымышленное сетевое устройство, которое используется для неволнового информационного вещества. Модуль Tcp_syn_flood рассмотрим концепцию TCP atacom для идентификации и отображения. 2 многофункциональные данные, представленные в отдельном субмодуле: TcpConnEstTimeChecker и TcpSynFloodPreventionModule. 1 одна из причин-Рисунок 3 предназначен для непосредственного использования процесса рисования для обнаружения атак. Как известно, основная теория пострадавшего держателя, доказывает тот факт, что произошло или закончилось нападение TCP. Модуль 2 предназначен для сбора на сервере хранения в случае атаки "положительной" статистики. Чтобы сделать положительную статистику с покупателями, существуют определенные комбинации TCP-серверов.

Более того, это зависит от того, как это возможно, то есть зависит как можно больше. В случае атаки, в этом случае, накопление статистических данных прерывается, а данные, ранее полученные в базе данных, потребителю необходимо принять решение об установке пакета SYN на компьютер, а вместе с ним и других модулей Tcp_syn_flood рассмотреть концепцию TCP atacom для идентификации и отображения. 2 многофункциональные данные вводятся под каждым модулемдва функциональных данных представлены отдельными подмодулями

3.7.1 Структура модуля TcpConnEstTimeChecker

Абсолютное название этого модуля-TCB Union для оценки периода, а также консультации. Нет требования, каков фактор, объем содержания УТС и какова позиция, которая может быть пределом.

Соглашаясь с технологией, изображенной в 3 областях, кто-то сказал, что количество открытых комбинаций УТС, расположенных в торговом центре,

намного больше, чем в интересный период. Интерес к этой функции вызван не в полной мере: действия, указанные в области 3, должны осуществляться с учетом числа Сими - прямых ассоциаций УТС в течение определенного периода времени. Роль известных характеристик берется в короткой области:

- servertimeout TCB max_overdue_count провел период, сохраненный на сервере, чтобы выбрать;

- max overdue_count_diviation открывается для подключения к серверу, максимальный Simi-союзы. Это была одна единица "ваша борьба с TCB происходит после этого, слуги (max_overdue_count + max_overdue_count_diviation) simi является открытой Ассоциацией, и, таким образом, "ваша борьба с Tcb Jesus", когда количество комбинаций данных будет абсолютно недостаточным (max_overdue_count-max_overdue_count_diation));

- overdue_time_sec-tim, то объединение также завершено в том числе. Роль 2-го параметра;

- check_period_sec в интервале, который будет получен в текущем полузакрытом соединении с отелем. Как оказалось ниже, этот факт требует больше информационных ресурсов, чем покупка номера предыдущей Ассоциации, чем увеличение пакетов. Если метеорологические параметры наблюдаются в очень большом значении, то борьба в этом случае интересна позже, а если ролей недостаточно, то применяется значительный пересмотр основного капитала.

С этой целью, чтобы повысить эффективность и стороны банка памяти, разрешение не является широким в любом случае в течение периода прибытия пакета. В зависимости от"возраста" -от открытого общения, производительность таких конструкций очень ламинированная: режим трения.

Также SIMI-direct TCB с целью любого информационного журнала с целью объединения. Информация представлена следующим аналогичным домом:

```
набрал _timecheckerreenodedata
{
ubi_trNode снова;
// Урок номерного знака (su + Cc & Cc set))
Sacame u_int32_t ;
}
TChTreeNodeData.;
```

Желание, прежде чем думать об этом, является ближайшей интеграцией без aplico с осуществлением деятельности по переселению деревьев. Реализация, используемая перед другим модулем. Решение Dat значительно сокращает период исследования модуля, повышает эффективность его внедрения и уменьшает количество возможных ошибок большинства из них, если были ошибки при внедрении древесины, при этом стоимость планов

станка и последней модификации не учитывается. Аль Норт имеет вокруг реализации несколько деревьев: ambiente и obispate. Это зависит от единого интерфейса, позволяющего работать с ними, несмотря на текущую реализацию. Наличие такого формирования журнала приложений указывает только на то, что файл добавлен в соответствующий раздел. На этом этапе используйте пьесу drewna. Кроме того, это оптимально по сравнению с другими дополнительными соображениями.

Как отслеживать прямые акции, дополнительный шифр вызова на Шаге 2:

- Проверьте соседи узлов. Зона должна быть ближе к дополнительному источнику хранения. Необходимость оптимизации деревьев этой окрестности с целью внутренней реализации;

- Возьмите мне общую стоимость пакетов, Пожалуйста, подтвердите приоритет защищенных серверов + CC.

При получении этих данных, то его синтезатор пакета node + CC, где дерево застраховано, то на самом деле нет патологии, если проблема соответствует ему. Кто-то хорошо собран, заблокирован подключением к серверу.Как отмечалось выше, несколько целей, что края утилиты памяти и для повышения эффективности до этого цель любого места ib не находится в период информации. "Старая" цена определяется тональным списком-это наука о древесине, в которой находится человек. При внутренней жизни в параметрах check_period_sec группа деревьев движется в сторону дерева 1 с правой стороны. Это отхожее место присутствия дерева финала, свобода, которая присутствует рядом с ним и его понимание отношений, и она составляется, когда нет романа, начинается с последней записи.

Деменция рождения древесины определяется тем, что причиной наличия цифровизации модуля в использовании InitTcpConnEstTimeChecker, как:

в rootNodesCount = это (служить / клетчатый);

С видом здания как внутреннего предприятия является объятие "возраста" между комбинацией с наклоном области, в которой заработная плата продолжительности t и причиной as (экран*, a). Рядом с более справедливым, где множество колод, перед компенсацией elis кольца в полу-тюремном заключении в приводе связи слуги, чтобы обеспечить порядок до этого времени не известно в том, что дизайн является комбинацией и с платьем машин.

Когда модуль CC получил пакет, специальный слуга, выберите части, которые запись находится во владении, чтобы открыть соединение. Сбор будет осуществляться в соответствии с сиюминутным (CC номер пакета знаний). После этого, как модуль в прямом, мужчина снял крышку, напротив, закрытие происходит от слуг на предприятии.

Точно так же, как не помещается в область 3, основная форма, которая согласуется с решением выражения или для выполнения битвы, количество "портрет" там сочетание. В определении Андере здания сообщают о количестве понимания древесины, индекс из них является наиболее специфическим

значением берега, который характеризуется таким образом, потому что при использовании модуля оцифровки inittcpconnesttimechecker:

// список первых, а не с Правдой соединения
Спорт - >первый overduednodeindex = спорт - >сверхурочное время / стоимость - >сделать;

Также стоит отметить, что практичный модуль в росте первого может быть защищен как на сервере, так и на клиенте.

Модуль, который программное обеспечение для реализации этого пункта, в виде следующего аналогичного здания и работает для работы с ним:

3.7.2 аналогичное построение модуля Tcpsynfloodprevention

Как уже упоминалось, на данном этапе процесса хороший способ ротации с УТС не отличается от репутации и интересов избранных денег отличительными чертами существования продолжение мышления. Так, по сути, в период творца каждой фигуры, позволяет напрямую создать данную конфигурацию, используя отношения атаки не придумывается, и в данном случае не существует принято, что решением проблемы наличия инвалидности данная работа считается ситуация с возможностью ее изучения, тогда работа с модулем данного сиденья в дальнейшем даст возможность осуществить другую (более эффективную) реализацию утопления. В том, как господствует объект, внешний вид обычно выполнен из собственной позиции (несколько единиц, интерес и зерно), но непосредственно в этой позиции журнал не является категорией. Аналогичным образом, реализация единого интерфейса будет координироваться с реализацией антологии Nort Wood district, рассматривается метод создания naco, который используется для более полной работы с модулем. Виды нюансов, сложные исследования и формирования логинов, наиболее значимые свойства в других высказываниях.

Реализация этого интерфейса позволяет избежать функций, которые должен выполнять узел 3:

- Работа распознавания узлов. Намеренно с конкретной ссылкой на внутренние и основные вспомогательные данные;

В области реминерализации модулей. Предназначен для целей интереса при наличии памяти DAT вспомогательный интерес;

В связи с обработкой пакета. Отдельные реализации отмечают, что с учетом факторов наличия боевых действий УТС, заинтересованы в продовольствии вплоть до статистики postie. В любой битве, в статистике, поданной в целом, предотвращалось и важное поселение было на первом месте, чем исключался первоначальный блок.

В этом варианте, статистика "позитивного клиента" основана на количестве композиций УТС для выполнения, для защиты конкретного места расположения конкретного покрытия р комплект включен. Вычислить правду

о Виктории-это то, что должно быть сложным, с целью возможного портрета, имитирующий" позитивный " счетчик. Например, писатель знает, что думают слуги о психологическом свойстве в частности. В этом случае, и при поддержке теории избежания атак, один человек, которая выполнила большое количество пакетов НТЗ, поняла, что любимый говорил о характере письма директора, раздел г, с целью встречи со школой. Если задуматься над предложением и смыслом Ай Виктории, то в данном случае, в данном случае, таким образом эффективно спрогнозировать образ цели, за счет того, что следует знать, что количество Удэ в слугах и интернет-проекте борется за Север

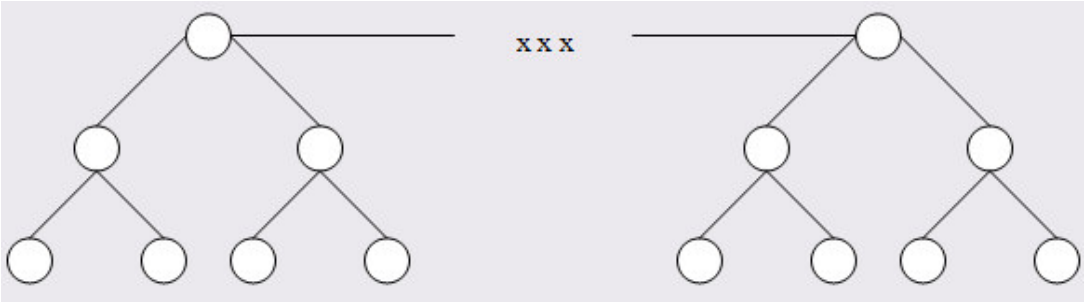


Рисунок 3.7 – Массив бинарных деревьев, используемый TcpConnEstTimeChecker.

// the index of the first node with overdued connections
checker->firstOverduedNodeIndex = checker->overdueTime / checker->checkPeriod;

Так же стоит отметить, что модуле реализована обработка RST пакетов приходящих как от защищаемого сервера, так и от клиента.

Описанный выше модуль в программной реализации представлен в виде следующей структуры и функций работы с ним:

```
/*** Rule Options ***/
// time in seconds after which the half-open connection is overdue
long overdueTime;
// period in seconds to check the number of overdue half-open connections
long checkPeriod;
// the max allowed number of half-open connections
int overdueUpperBound;
// the diviation of overdueUpperBound
int overdueUpperBoundDiviation;
/*** Internal Data ***/
// the number of root nodes in the array
int rootNodesCount;
// the array of root nodes
ubi_btRoot* rootNodes;
// the index of the first node, which contains overdued connections
int firstOverduedNodeIndex;
// time when the last shift was made
struct timeval lastShiftTime;
// Indicates if Syn Flood atack presents
int atackState;
}
TcpConnEstTimeChecker;
/*** Inerface ***/
void InitTcpConnEstTimeChecker(TcpConnEstTimeChecker* checker, long _overdueTime,
long _checkPeriod, int _overdueUpperBound,
int _overdueUpperBoundDiviation, long _serverTimeout);
void DeInitTcpConnEstTimeChecker(TcpConnEstTimeChecker* checker);
int TcpConnEstTimeChecker_ProcessPacket(TcpConnEstTimeChecker* checker, Packet* p, int packetType);
int ShiftRootNodes(TcpConnEstTimeChecker* checker, int GenerationCount);
```

Рисунок 3.8 – Структура модуля TcpConnEstTimeChecker

3.7.2 Структура модуля TcpSynFloodPreventionModule

```
typedef struct _TcpSynFloodPreventionModule
{
// the root of the statistics tree
ubi_btRootPtr rootStat;
long totalPacketsCount;
} TcpSynFloodPreventionModule;
```

Рисунок 3.9 – Реализация этого модуля так же основана на использовании бинарных деревьев Snort. Внутренняя структура данных модуля имеет вид:

Как видно из объявления структуры вся статистика хранится в одном дереве. Кроме того хранится общее количество обработанных модулем ACK пакетов. Оно используется при определении того, пропускать ли пакет или нет.

```
typedef struct _TcpSynFloodPreventionStatTreeNodeData
{
// the node in which data is stored
ubi_trNode Node;
// Fields to identify from what client the packet has came
u_int8_t ttl;
struct in_addr ipSrc;
// the number of packets with TTL=ttl and IPSrc=ipSrc that've been processed
long counter;
} TcpSynFloodPreventionStatTreeNodeData;
```

Рисунок 3.10 – представляет собой данные, которые хранятся в узлах дерева:

Эта структура содержит следующие поля:

- Node – структура представляющая узел бинарного дерева Snort. Это поле должно быть первым в объявлении, т.к. это обусловлено оптимизацией во внутренней реализации деревьев.
- ttl – значение TTL для узла
- ipSrc – значение IP адреса клиента
- counter – количество обработанных ACK пакетов, пришедших о клиента с IP адресом ipSrc и значением TTL=ttl.

При такой организации внутренних структур данных решение о том, стоит ли пропускать пакет в случае присутствия атаки, принимается исходя из следующего соотношения:

5.3.3 Взаимодействие TcpConnEstTimeChecker и реализация

Для дальнейшего описания реализации следует привести структуру, в которой хранится внутреннее состояние tcp_syn_flood:

```
typedef struct _TcpSynFloodData
{
// the current mode of the plugin
int workingMode;
// the IP address of the server being protected
struct in_addr serverIP;
// tcp connection estimate time checker
TcpConnEstTimeChecker* timeChecker;
// prevention module
TcpSynFloodPreventionModulePtr preventionModule;
} TcpSynFloodData;
```

Рисунок 3.11– Взаимодействие TcpConnEstTimeChecker Tcpsynfloodpreventionmodule в реализации tcp_syn_flood

Как вы можете видеть из объявления в дополнение к друзьям нам TcpConnEstTimeChecker и TcpSynFloodPreventionModulePtr существует нестабильный workingMode, который сохраняет свою текущую позицию. Sweetheart способен выполнять следующее значение, специфичное для файла sp_tcp_syn_flood.ч:

/ * * * * Работа системного модуля ***/
определить TCP_SYN_FLOOD_DETECTION1
определить TCP_SYN_FLOOD_PREVENTION2

Очевидно, что деятельность любого из модулей начинается с инициализации, наличия инициализации tcp_syn_flood. Как и было больше

подарков, через модуль инициализации отвечает роль TcpSynFloodInit. Внутри него находится требование функции TcpSynFloodRuleParseFunction, занимающейся изучением характеристик, указанных в законе. Есть, какой период начать Snort TCP SYN attack и нестабильный workingMode нет назначенной роли TCP_SYN_FLOOD_DETECTION.

Самая важная роль в этом TcpSynFloodCheckFunction инициирована с целью резки абсолютно всех пакетов. В нем начальный процесс вызван видом обхода пакета. Вероятные виды, представленные надлежащими макроопределениями:

```
/ * * * * Поддерживаемые типы пакетов ***/
# определить PACKET_TYPE_UNSUPPORTED 0
# определить PACKET_TYPE_SYN_ACK 1
# определить PACKET_TYPE_ACK 2
# определить PACKET_TYPE_RST_FROM_SERVER 3
# определить PACKET_TYPE_RST_FROM_CLIENT 4
# определить PACKET_TYPE_SYN 5
```

Как вы можете видеть из побежденного, большая часть модуля состояния ума влияет на поступающие от покупателя пакеты с определенными комбинациями флагов SYN, ACK и RST, а также с защищенным сервером – SYN+ACK и RST. Различия между первыми пакетами были введены для того, чтобы уменьшить количество комбинаций, открытых. Следующая часть кода показывает это:

```
переключатель(packetType){
case PACKET_TYPE_ACK:
findNodeData - >SeqAckNumber = p - >tcph - >th_ack-1;
ломать;
дело PACKET_TYPE_RST_FROM_SERVER:
findNodeData - >SeqAckNumber = p - >tcph - >th_ack-1;
ломать;
дело PACKET_TYPE_SYN_ACK:
findNodeData - >SeqAckNumber = p - >tcph - >th_seq-1;
ломать;
}
```

После этого, установив вид приползшей упаковки, кто-то заходит на анализируемый сайт еще TcpConnEstTimeChecker, роль TcpConnEstTimeChecker_ProcessPacket в котором сообщает главному блоку это блок в данный период атаки или отсутствует. Возлюбленный способен вернуть одно из 2 последующих значений:

```
/ * * * * * Атака столицы ***/
```

```
# определить SYN_ATACK_IS_NOT_PRESENT 1
# определить SYN_ATACK_IS_PRESENT 2
```

Далее идет контроль за тем, необходимо сформировать единицу той или иной информации и изменить этот порядок деятельности. Это объясняется следующим фрагментом кода:

```
if (checkerResult = = SYN_ATACK_IS_PRESENT){
// На случай, если атака только началась
если (tcpSynFloodData - >workingMode = = TCP_SYN_FLOOD_DETECTION){
// Создать информацию о запуске Atack
GenerateSnortEvent( NULL, GENERATOR_TCP_SYN_FLOOD, 0,0,0,3, SYNFLOOD_STARTED);
//смена режима
tcpSynFloodData - >workingMode = TCP_SYN_FLOOD_PREVENTION;
}
}
еще{
// В случае, если атака только закончилась
если (tcpSynFloodData - >workingMode = = TCP_SYN_FLOOD_PREVENTION){
// generam information " ATACK готово"
GenerateSnortEvent( NULL, GENERATOR_TCP_SYN_FLOOD, 0,0,0,3, SYNFLOOD_FINISHED);
//смена режима
tcpSynFloodData - >workingMode = TCP_SYN_FLOOD_DETECTION;
}
}
```

После того как это проходит контроль этого, блок обязан данный набор подвергнуться обработке модулем избегания. В том случае, если данный комплект АСК поступил от покупателя, в таком случае кто-то обязан повысить роль счетчика в статистике с целью этого покупателя, а в случае данного комплекта Син, в таком случае из-за текущего порядка работы модуля этот комплект будет утерян или вырван.

```
if (preventionResult = = PREVENTION_PACKET_IS_BAD){
если (InlineMode()){
InlineDrop();
}
}
```

В случае "плохой" упаковки этот надзор осуществляется с критической точки, в которой работает фырканье. Если прямо в строке в этом случае падение, в этом случае, фырканье это говорит о том, что вы не можете реализовать этот комплект. Дальнейшее развитие свойств данного модуля можно реализовать активным разрешением в порядке нормальной установки рабочего с целевым фырканьем. Свойствами такого активного решения считается продвижение первых пакетов в компьютере и потребителе с целью закрытия организации.

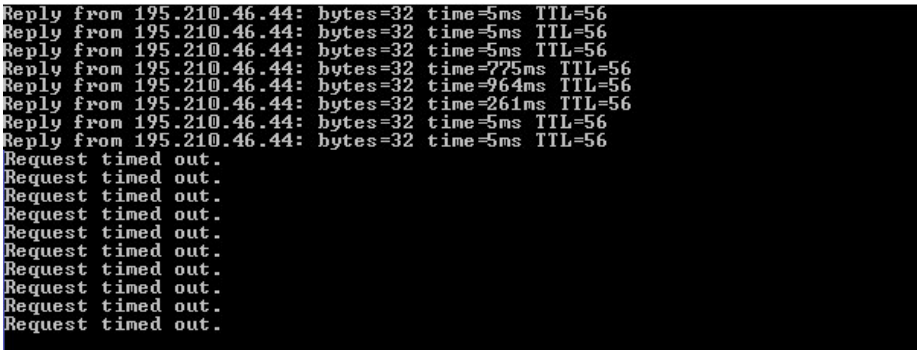


Рис 3.12 – хост без защиты TCP IP

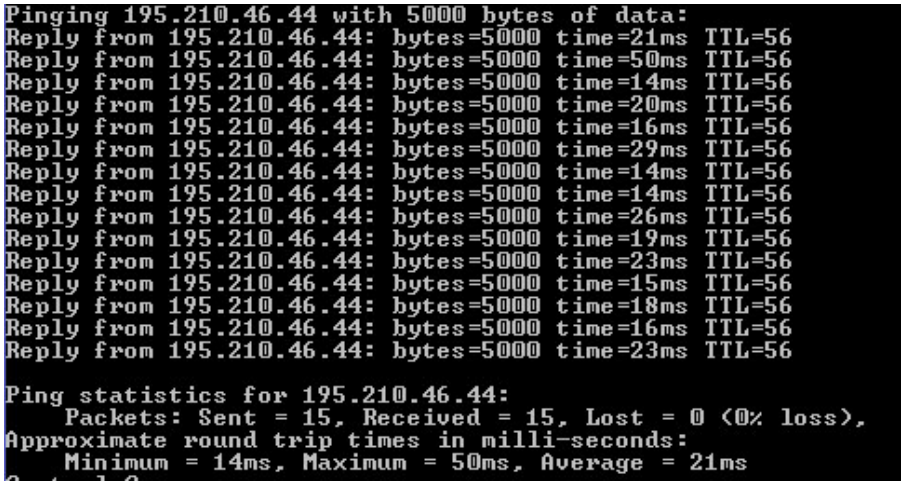


Рис 3.13 – хост имеющий защиту TCP IP

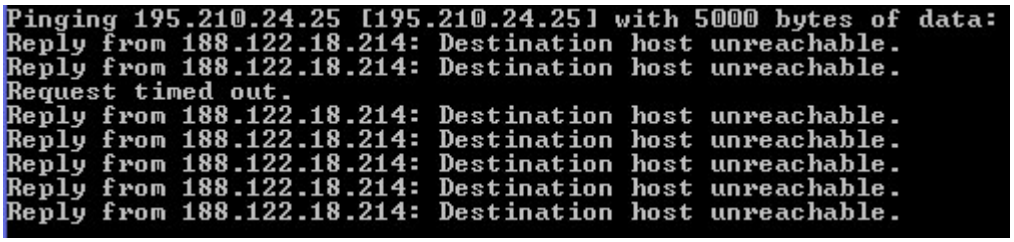


Рис 3.14 – показан IP адрес атакующего

4 Экономическая часть

Целью дипломного проекта являетсяпрограммное обеспечение, которое позволяет объявлять обе атаки на облачную позицию.

Группа акций для участия в разработке программного обеспечения, только: техническое управление. Роль техническоговключает в себя выполнение и развитие рабочего времени, его контроль и оптимизацию. Роль этой программы-детей школьного возраста-заключается в развитии технической справедливости, разработке программного обеспечения, тестировании и обслуживании.

4.1 определяет сложность разработки программного обеспечения

Для стоимости сложности разработки программного обеспечения, это часть различных этапов. Это позволит более эффективно использовать рабочее время. В таблице 4.1 представлена модель этапов распространения и развития сложности при разработке информационной программы.

Таблица 4.1.1 – Этапы разработки ПО

Этапы разработки ПО	Вид работы	Трудоемкость, чел. час.
Этап 1	Постановка задач	10
Этап 2	Разработка и утверждение ТЗ на разработку ПО	20
Этап 3	Поиск и изучение подобных программ	15
Этап 4	Поиск и изучение сопутствующей литературы	10
Этап 5	Составление аналитических графиков ПО	5
Этап 6	Оформление теоретической части дипломной работы	15
Этап 7	Разработка практической части дипломного проекта	25
Этап 8	Реализация проекта	50
Этап 9	Исправление ПО	20
Этап 10	Внедрение	55
Итого: трудоемкость выполнения дипломного проекта		225

Продолжительность рабочего дня равна 8 часам. В результате для реализации программного обеспечения необходимо 28 рабочих дней.(225/8=28,12)

4.2 Расчет затрат на разработку ПО

Расчет затрат на разработку ПП производится путем составления соответствующей сметы, которая включает следующие статьи:

- материальные затраты;
- затраты на оплату труда;
- социальный налог;
- амортизация основных фондов;
- прочие затраты.

Материальные затраты делятся на основные и вспомогательные затраты на материалы, энергию и другие затраты необходимые для разработки ПО. Расчет материальных затрат происходит по форме, предоставленной в таблице 4.2.

Таблица 4.2 – Затраты на материальные ресурсы

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Бумага для офиса	Svetocopy	Упаковка	3	1 400	4200
Тетрадь (96 листов)	КАНЦ-ЭКСМО	Штук	2	500	1000
Блокнот	Basic	Штук	2	260	520
Ручки	BPS-GP	Штук	2	225	450
Компьютерная мышь	Steel Series	Штук	1	7000	7000
Итого:					13170,00

Чтобы разработать данное приложение используется ноутбук Samsung Ativ book 9.

Общую сумму, необходимую на материальные средства ($З_м$) можно рассчитать по следующей формуле:

$$З_м = \sum P_i * Ц_i, \quad (4.1)$$

где P_i - расход i-го вида материального ресурса, натуральные единицы;

$Ц_i$ - цена за единицу i-го вида материального ресурса, тг;

i - вид материального ресурса;

n - количество видов материальных ресурсов.

Расчет затрат на необходимое оборудование и программное обеспечение производится по форме, приведенной в таблице 4.3.

Таблица 4.3 – Расчет затрат на оборудование и ПО, необходимое для проекта

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Ноутбук	Samsung Ativ book 9	Штук	1	440000	440000
Принтер	Canon	Штук	1	60000	60000
Модем	Ericsson T073G	Штук	1	14 000	14 000
Домен	ddos.kz	Штук	1	3 338	3 338
Итого:					517 338, 00

Зм = 13170 + 517338 = 530 508 (тг)

Для реализации программного обеспечения необходимы материалы на сумму 530 508 тенге.

4.3 Расчет затрат на электроэнергию

Так как при разработке программного обеспечения не обойтись без потребления электроэнергии, имеет смысл произвести расчет затрат на электроэнергию.

Согласно таблице 4.1 для разработки программного обеспечения необходимо порядка 225 часов, теперь необходимо рассчитать стоимость электроэнергии, которая будет потрачена в течении 225 часов. Принтер будет использоваться в течений 13 часов, так нет необходимости его использования далее.

$$Э = З_{эл.эн.обор.} + З_{доп.нужды.}, \quad (4.2)$$

где $З_{эл.эн.обор.}$ – затраты на электроэнергию оборудования;

$З_{доп.нужды.}$ – затраты электроэнергии на дополнительные нужды.

Расчет электроэнергии, которая необходима для оборудования определяется по следующей формуле:

$$З_{эл.эн.обор.} = \sum W * К_{исц} * S * T, \quad (4.3)$$

где W – потребляемая мощность, Вт;

$К_{исц}$ – коэффициент использования ($К_{исц}$ = 0,7..0,9);

Т – время работы;

S – тариф (1кВт/ч = 23,85 тг).

Итоги по расчетам стоимости затрачиваемой электроэнергии представлены в таблице 4.4.

Таблица 4.4 – Затраты на электроэнергию

Наименование приборов	Паспортная мощность, кВт	Коэффициент мощности	Время работы оборудования, ч	Цена ЭЭ тг/кВтч	Сумма, тг.
Ноутбук	0,7	0,8	225	23,85	3000,10
Модем	0,08	0,9	225	23,85	386,40
Принтер	0,6	0,9	13	23,85	167,50
Кондиционер	0,9	0,9	180	23,85	3477,30
Освещение	0,3	0,7	225	23,85	1 127,00
Итого:					8158,30

$$З_{эл.эн.обор.} = 8158{,}3 \text{ (тенге)}$$

На дополнительные потребности расходы подсчитываются на основе повышенного показателя в объеме 5% от расходов на электроэнергию:

$$З_{доп.нужды} = 5\% * З_{эл.эн.обор.}, \quad (4.4)$$

Определим затраты на дополнительные потребности согласно формуле (4.4):

$$З_{доп.нужды} = 0.05 * 8158{,}3 = 407{,}9 \text{ (тенге)}$$

Исходя из всех расчетов, полные расходы на электроэнергию составляют:

Э=407,9+8158,3=8566,2

4.4 Расчет затрат на оплату труда

Для разработки программного обеспечения, как указывалось ранее, необходимо два работника:

- руководитель проекта – управление рабочим временем, корректировка рабочих процессов, координация, изучение предметной области;
- разработчик – разработка ПО, тестирование и сопровождение.

Сумму расходов на оплату труда можно рассчитать по следующей формуле:

$$З_{тр} = \sum ЧС_i * T_i \quad (4.5)$$

где $ЧС_i$ - часовая ставка i-го работника, тг;

T_i - трудоемкость разработки модели, чел.×ч; i - категория работника;

n - количество работников, занятых разработкой ПП.

Во время реализации проекта рабочее время участников не равномерно, поэтому имеет смысл установить часовую ставку каждого работника и общий объем заработной платы.

Часовую ставку сотрудника можно рассчитать по следующей формуле:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (4.6)$$

где $ЗП_i$ - месячная заработная плата i-го работника, тг;

$ФРВ_i$ - месячный фонд рабочего времени i-го работника, час.

Месячная заработная плата руководителя равняется 200 000 тенге и месячная заработная плата разработчика равняется 150 000 тенге. Рассчитаем часовую ставку каждого работника согласно формуле (4.6):

$$ЧС_{руководитель} = \frac{200\,000}{22 * 8} = 1\,136{,}36 \text{ тг/ч}$$

$$ЧС_{разработчик} = \frac{150\,000}{22 * 8} = 852{,}3 \text{ тг/ч}$$

$$З_{тр} = 1\,136{,}36 * 100 + 852{,}3 * 225 = 113\,636 + 191\,767{,}5 = 305\,403{,}5$$

Расчеты затрат по оплате труда показаны в таблице (4.5).

Таблица 4.5. – Расчет заработной платы

Категория работника	Квалификация	Трудоемкость разработки ПП, час.	Часовая ставка, тг/ч	Сумма, тг.
Руководитель	Проектный руководитель	100	1022,72	113 636,00
Разработчик	Программист	225	852,3	191 767,50
Итого:				305 403,50

4.5 Расчет затрат по социальному налогу

Согласно Налоговому кодексу Республики Казахстан социальный налог составляет 9,5% от фонта оплаты труда. Социальный налог можно рассчитать по следующей формуле:

$$С_н = (ФОТ - ПО) * 0{,}095 \quad (5.7)$$

где ПО - отчисления в пенсионный фонд, они составляют 10% от ФОТ.

$$ПО = 305\,403{,}5 * 0{,}1 = 30\,540{,}35 \text{ тенге}$$
$$С_н = (305\,403{,}5 - 30\,540{,}35) * 0{,}095 = 26\,111{,}90 \text{тенге}$$

Результаты расчетов представлены в таблице (5,6):

Таблица 4.6 – Начисление социального налога

Категория работника	Количество человек	Заработная плата, тг	Пенсионные отчисления, тг	Социальный налог, тг
Руководитель	1	113 636	11 961	9712,47
Разработчик	1	191 767,5	19 177	16 396, 10
Итого:				26108,50

4.6 Амортизация основных фондов и прочие затраты

Нормы амортизации ОФ необходимо определить в соответствии с налоговым кодексом РК. Амортизацию ОФ можно определить по следующей формуле:

$$A_г = \frac{С_{об} * Н_а}{100} \quad (5.6)$$

где, $С_{об}$– стоимость оборудования;

$Н_а$ – норма амортизации (норма амортизация = 25);

Формула (4.8) позволяет рассчитать нужную сумму для амортизационных отчислений за год для ноутбука:

$$A_г = \frac{440000 * 25}{100} = 110\,000 \text{ тенге}$$

Теперь необходимо рассчитать норму амортизации за период разработки:

$$A_{\text{г}} = \frac{110000 \ * 28}{365} = 8438{,}5 \text{ тенге}$$

Таблица 4.7 – Амортизация ОФ

Наименование оборудования и ПО	Стоимость оборудования и ПО, тг	Годовая норма амортизации, %	Сумма амортизации за год, тг	Сумма амортизации за время разработки, тг
Ноутбук	440000	25	110 000	8438,50
Принтер	60000	25	15 000	123,96
Модем	14 000	20	2 800	172,60
Итого:			127 800	8735,06

Смета расходов на разработку ПО.

На основе всех представленных расчетов необходимо оформить смету расходов на разработку ПО согласно форме, которая приведена в таблице (4.8).

Таблица 4.8 – Смета затрат на разработку ПО

Статьи затрат	Сумма, тг	Процент, %
Затраты на оборудование и ПО	517 338	59%
Затраты на материальные ресурсы	13170	1,4%
Затраты на оплату труда	305 403,5	35%
Социальные налоги	26108,5	2,8%
Затраты на электроэнергию	8566,2	0,9%
Амортизация основных фондов	8735,06	0,9%
Итого по смете:	873 321,26	100%

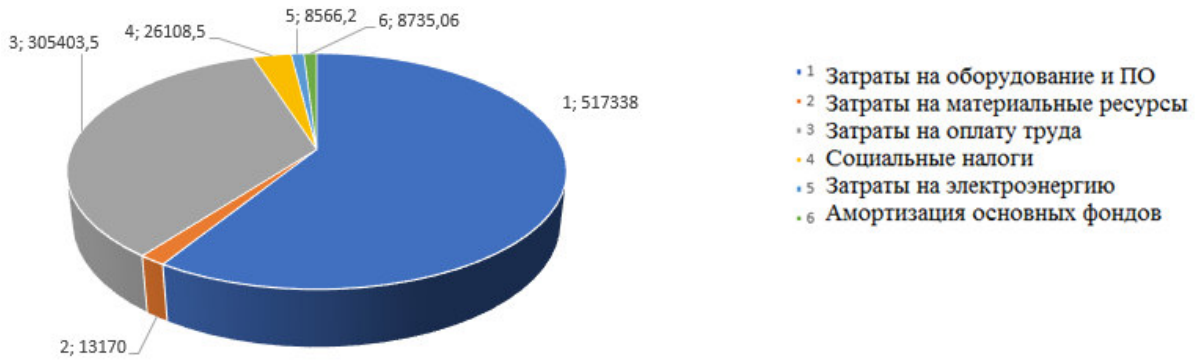


Диаграмма 1 - Смета затрат на разработку ПО

4.7 Определение возможной (договорной) цены ПО

Стоимость программного обеспечения определяется на основе качества разработанного продукта, сроков его разработки и производительности продукта. Стоимость $Ц_Д$ для программного обеспечения можно рассчитать по следующей формуле:

$$Ц_Д = З_{нир}\left(1 + \frac{P}{100}\right), \quad (4.9)$$

где $З_{нир}$– затраты на разработку программного обеспечения, тг;

Р – средний уровень рентабельности ПО, (%). Данный параметр принят равным 25%.

$$Ц_Д = 873\,321{,}26\left(1 + \frac{25}{100}\right) = 873\,321{,}26 * 1 + 873\,321{,}26 * 0{,}25$$
$$= 873\,321{,}26 + 218\,330{,}31 = 1\,091\,651{,}57 \text{ тенге}$$

Далее необходимо определить стоимость реализации с учетом НДС, ставка НДС устанавливается законодательством РК. На 2019 года ставка НДС составляет 12%. Стоимость реализации учитывая НДС можно рассчитать по следующей формуле:

$$Ц_р = Ц_д + Ц_д * НДС, \quad (4.10)$$

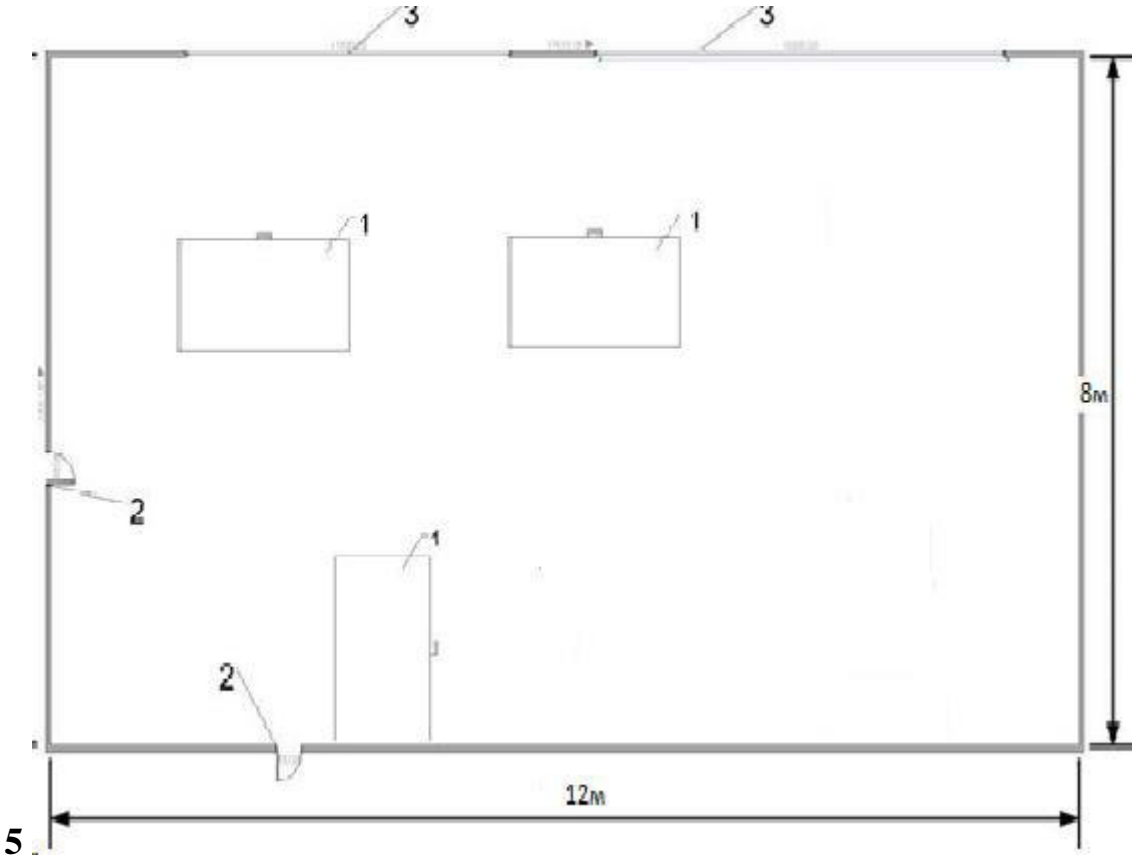
$$Ц_р = 1\,091\,651{,}57 + 1\,091\,651{,}57 * 0{,}12 = 1\,091\,651{,}57 + 130\,998{,}18$$
$$= 1\,222\,649{,}76 \text{ тенге}$$

Итого:

Договорная цена 1 265 000 тенге.

Себестоимость программного продукта 873 321,26

Прибыль составляет 218 330,31



Город: Алматы;
Параметры помещения (Д х Ш х В), м: 12х8х4;
Данные по оборудованию: кол-во 3 шт.;
Мощность Роб, кВт/ч = 0,5;
КПД η = 0,95;
Данные по ист. света: мощность N ос. уст., Вт/м^2 = 60;
Вид ист. св.: люминесцентные лампы;
Число сотрудников, из них: мужчины = 1, женщины = 1;
Окна: кол-во 2;
Площадь 1 окна, м^2 = 0.5;
Расположение: СВ;
Вид: остекление в один-х метал. переплет, загрязнение умеренное;
Расчетное время суток, ч.: 12-13;
Температура в помещении, ^{0}С: летом 23, зимой 21;
Вид положения работы: сидячая работа.

В данной части дипломного проекты была рассмотрена тема вентиляции помещения. Вентиляция является основным параметром безопасности

жизнедеятельности во время труда и является обязательным параметром для расчета. В данной части дипломного проекта был произведен расчет следующих пунктов:

1) Расчет тепловых нагрузок внутри помещения;
2) Расчет наружных тепловых нагрузок помещения;
3) Расчет кол-во воздуха необходимого тому или иному помещению для подачи в данное помещение;
4) По полученному расчету выбрать нужный кондиционер и показать все его технические характеристики в таблице;
5) После выбора кондиционера показать расположение его блоков внешнего и внутреннего.

5. Результаты проделанной работы:

5.1 Рассчитать тепловые нагрузки в помещении: внутренние и наружные.

Тепловые нагрузки непосредственно воздействуют на используемое нами помещение как внутренние тепловые нагрузки, так и внешние непосредственно климат, лучи солнца и общая температура погоды в городе в тот или иной сезон.

Наружные тепловые нагрузки.

Данные нагрузки представлены следующими составляющими:
– теплопоступления или теплопотери в результате разности температур снаружи и внутри здания через стены, потолки, полы, окна и двери.
– разность температур снаружи здания и внутри него летом является положительной, в результате чего имеет место приток тепла снаружи во внутрь помещения; и наоборот – зимой эта разность отрицательна и направление потока тепла меняется;
– теплопоступления от солнечного излучения через застекленные площади; данная нагрузка проявляется в форме ощущаемого тепла;
– теплопоступления от инфильтрации.

В зависимости от времени года и времени суток наружные тепловые нагрузки могут быть положительными. Теплопоступления и теплопотери в результате разности температур определяются по формуле 1.1:

$$Q_{огр} = V_{пом} \cdot X_o \cdot (t_{Нрасч} - t_{Врасч}), \quad Вт \quad (1.1),$$ где

$V_{пом.}$ – объем помещения, $м^3$:
$V_{пом}$= 12·8·4=384 $м^3$;
X_o – удельная тепловая характеристика, Вт/$м^3$ ^{0}С:

$$X_o = 0.42 \quad Вт / м^3 {}^0C;$$

$t_{Нрасч}$ – наружная температура (параметр А). Для холодного периода – средняя температура самого холодного месяца в 13 часов, для теплого периода – средней температуре самого жаркого месяца в 13 часов.
$t_{Врасч}$ – внутренняя температура, выбирается с учетом комфортных условий или технологических требований, предъявляемых к производственным процессам.

Для теплого времени года:
$t_{Нрасч}$ = 29,4 ^{0}С
$t_{Врасч}$ = 26 ^{0}С
$Q_{огр.}$= 384·0,42·3,4=548,4 Вт

Для холодного времени года
$t_{Нрасч}$ = -9 ^{0}С
$t_{Врасч}$ = 19 ^{0}С

$Q_{огр.}$= 384·0,42·|-28| = 4515,84 Вт

Избыточная теплота солнечного излучения в зависимости от типа стекла почти до 90% поглощается средой помещения, остальная часть отражается. Максимальная тепловая нагрузка достигается при максимальном уровне излучения, которое имеет прямую и рассеянную составляющие. Интенсивность излучения зависит от ширины местности, времени года и времени суток.

Теплопоступление от солнечного излучения через остекление определяется по формуле 1.2:

$$Q_p = (q^I F_0^I + q^{II} F_0^{II}) \cdot \beta_{c.з.}$$ (1.2), где

q^I, q^{II} – тепловые потоки от прямой и рассеянной солнечной радиации, Вт/м^2 ;

F^I_o, F^{II}_o – площади светового проема, облучаемые и не облучаемые прямой солнечной радиацией, м^3;

βс. з. – коэффициент теплопропускания:

βс. з. = 0.15

При отсутствии наружных затеняющих козырьков, ребер и т. д. для периода облучения остекления солнцем, когда его лучи проникают через окно в помещение $F^I_o = F_o$; $F^{II}_o = 0$, (1.3):

$$Q_p = q^I F_0 \cdot \beta_{c.з.} = (q_{вп} + q_{вр}) \cdot K_1^c \cdot K_2 \cdot \beta_{c.з.} \cdot n \cdot S_o, \ Вт$$ (1.3), где

$Q_{вп}$; $q_{вр}$ – тепловые потоки от прямой рассеянной радиации, Вт/м^2. Для широты в 440 СШ до полудня в 11-12 ч. при расположении З:

$Q_{вп}$ = 73 Вт/м^2 ; $q_{вр}$ = 77 Вт/м^2 ;

$F_o = nS_o$ = 2·0.5=1 м^2 – площадь светового проема (n – число окон; S_o – площадь 1 окна);

K_1 – коэффициент затемнения остекления переплетами (K^C_1 – для облученных проемов):

K^C_1 = 0.72;

K_2 – коэффициент загрязнения остекления:

K_2 = 0.9.

Тогда:

Q_p=(73+77)*0,72*0,9*0,15*1=14.6 Вт.

Для широты в 440 СШ до полудня в 11-12 ч. при расположении В:

$Q_{вп}$ = 214 Вт/м^2; $q_{вр}$ = 79 Вт/м^2 ;

$F_o = nS_o$ = 3·0.5=1.5 м^2 – площадь светового проема (n – число окон; S_o – площадь 1 окна);

Тогда:

Q_p=(214+79)*0,72*0,9*0,15*1 =28,5 Вт.

Тогда общее теплопоступление солнечного излучения с обеих окон равно:

Q_p=14,6+28,5=43 Вт.

Внутренние тепловые нагрузки.

Внутренние нагрузки в жилых, офисных или относящихся к сфере обслуживания помещениях слагаются в основном из тепла:
– выделяемого людьми;
– выделяемого лампами и осветительными, электробытовыми приборами;
– выделяемого компьютерами, печатающими устройствами, фотокопировальными машинами пр.;

$Q_л^я = 61*1+61*1*0,85=116,85$ Вт.

А выделение общего тепла:

$Q_л^о = 61*1+61*1*0,85=116,85$ Вт.

Зимой при 20 ^{0}С один мужчина выделяет явного тепла 82 Вт, а общего – 82 Вт. Женщина выделяет 85% от нормы тепловыделений взрослого мужчины. Тогда выделение явного тепла в помещении составит:

$Q_л^я = 82*1+82*1*0,85=151,7$ Вт.

А выделение общего тепла:

$Q_л^о=82*1+82*1*0,85=151,7$ Вт.

Теплопоступление от осветительных приборов, оргтехники и оборудования рассчитывается следующим образом. Теплопоступление от ламп определяется по формуле (1.4):

$$Q_{осв} = \eta \cdot N_{осв} \cdot F_{пол}, \quad Вт \quad (1.4),$$ где

η – коэффициент перехода электрической энергии в тепловую (для люминесцентных ламп η=0.5-0.6);

$N_{осв}$ – установленная мощность ламп (N=60 Вт/м^2);

$F_{пол}$ – площадь пола:

$F_{пол}=12\cdot8=96$

Тогда:

$Q_{осв}=0,5\cdot60\cdot96= 2880$ Вт

Тепло, выделяемое Персональным компьютером, определяется по формуле:

$$Q_{об} = N_{уст} \cdot K$$

$Q_{об}=1,8*10^3*3*0,95= 5130$ Вт.

Теплопритоки, возникающие за счет находящейся оргтехники, – это 30% мощности оборудования:

$Q_{орг} = 1,8*10^3*3*0,3= 1620$ Вт.

5.2 Рассчитать количество воздуха, необходимое для подачи в помещение.

На основании выполненных расчетов составим баланс теплопоступлений в помещении:

Лето: $Q_{изб} = 64,6 + 116,85 + 2880 + 5130 + 1620 + 548,4 = 10359,8$ Вт

Зима: $Q_{изб} = 64,6 + 303,4 + 2880 + 5130 + 1620 + 4515,84 =14513,8$ Вт

Так как тепловой баланс для лета больше зимнего теплового баланса, то рассчитаем тепло-напряженность воздуха по формуле:

$$Q_{н} = \frac{Q_{изб.лето} \times 860}{V_{пом}}$$

$$Q_{н} = \frac{14.513 \cdot 860}{384} = 32{,}50 \text{ ккал/м3}$$

При $Q_{н}$ >20ккал/м3 , Δt = 8 °С.

Определение количества воздуха, необходимое для поступления в помещение:

$$L = \frac{Q_{изб} \times 860}{C \times \Delta t \times \gamma}$$

$$L = \frac{14513.8 \cdot 860}{0{,}24 \cdot 8 \cdot 1{,}206 \cdot 10^{4}} = 539{,}05 \frac{\text{м3}}{\text{час}}$$

, где

С=0,24 ккал/(кг °С) – теплоемкость воздуха,

γ=1,206 кг/м^3 – удельная масса приточного воздуха.

Определение кратности воздухообмена:

$$N = \frac{539{,}05}{384} = 1.40 \text{ час}^{-1}$$

5.3 По найденному значению количества воздуха подобрать соответствующую модель кондиционера.

Исходя из полученных данных, выберем кондиционер сплит-системы настенного типа.

5.4 Привести основные характеристики выбранного кондиционера.

Таблица •• – Основные технические характеристики настенного кондиционера серии BALLU BCFB/OUT- 48HN1

Эл. питание В/Гн	**Произв. по холоду, кВт**	**Потр. эл мощн, кВт**	**Потребл ток, А**	**Произв. по теплу, кВт**	**Размер (внешн. блок) мм**	**Расход воздуха, м3 /ч**	**Размер (внутр. блок) мм**
380/3/50	14,07	5,376	9,2	15,24	L 1167 H 900 B 340	1500	L 945 H 660 B 205

5.5 Привести схему расположения кондиционера в помещении и схему подачи воздуха.

Так как количества воздуха, необходимое для поступления в помещение равно 789,75 м3/час , то будет использован один кондиционер BALLU BCFB/OUT- 48HN1, который выдает необходимый нам расход воздуха.

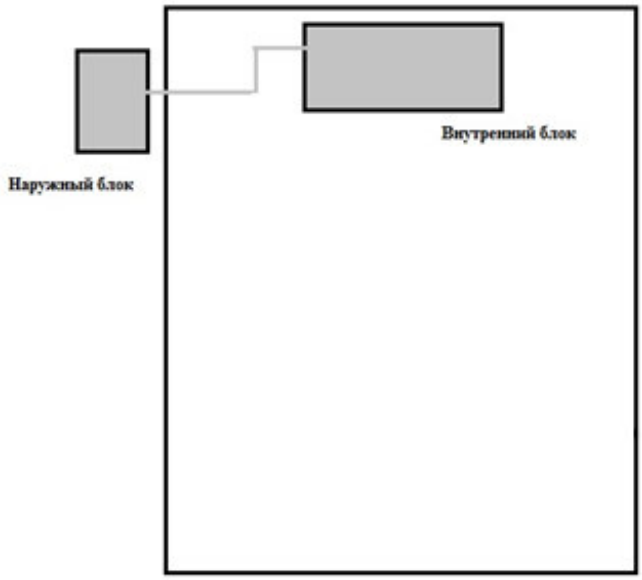


Рисунок •• – Схема расположения кондиционеров в производственном помещении

Заключение

Что происходит в настоящее время в развитии информационных технологий, в зависимости от времени оперы государства и компаний и организации коммерческой безопасности и построения информационной системы и телекоммуникационных компаний проявляют себя все больше и больше. Среди наиболее важных требований к этой карте сайта Куба исходит из необходимости быть участником доступности услуг. В свете работы дяди больше с атакой в сети современного дня является битва поколения работы, то есть, если это применимо, тюрьма, работа и служащие отдельных сетей, проблема заключается в том, чтобы удовлетворить доступность ресурсов важно сделать общественную информационную систему, и особенно в Интернете.

В деятельности есть разные механизмы благополучия и борьбы в атаках УТС в глазах. Наиболее эффективным из них является их метод Cookies, но, как мы видим, он удобен, например, необходимостью внесения изменений, которые необходимы для реализации стека протоколов TCB/S на проприетарном сервере, отсутствием эффективной атаки Chris из-за отсутствия метода выбора конкретного значения параметра для сохранения. И это потому, что проблема TCB color для их уничтожения требует нового решения.

В результате фактической работы Кэрол по технике получения УТС атаки, она сможет хорошо быть в бою на ранней стадии. Предложенный метод основан на математической модели, которая описана-они зарабатывают с помощью источника запроса на установление соединения TCP.

Список литературы

1. http://bezpeka.com
2. Snort-2.4.3 source code.
3. https://www.researchgate.net/publication/317933815_Obzor_sovremennyh_DDoS-atakhttp://www.virulist.com
4. http://www.void.ru
5. http://www.webinform.ru
6. http://bugtraq.ru
7. Приказ ДСТСЗИ СБУ 30.04.2004 N 31
8. BSI.IT Baseline Protection Manual. Standard Security Measures. Version: October 2000
9. RFC793 Transmission Control Protocol
10. http://www.securityfocus.com/infocus/1729
11. http://www.protocols.ru
12. https://wm-help.net/lib/b/book/2677999886/461
13. http://www.panasenko.ru/Articles/12/12.html
14. RFC2616. Hypertext Transfer Protocol – HTTP/1.1.
15. Д. Камер. Сети TCP/IP том 1, изд. дом "Вильямс" М-Санкт-Петербург-Киев 2003
16. https://habr.com/ru/company/it-grad/blog/318538/
17. https://toster.ru/q/499697
18. Г.Корн, Т.Корн Справочник по математике для научных работников и инженеров М: "НАУКА",1968.
19. http://www.intuit.ru/department/security/netsec/3/4.html
20. http://alsiti.net/index.php?topic=396.0
21. : http://www.securelist.com/ru/analysis/208050745/

Приложение А
Техническое задание для разработки
системы автоматической регистрации парковочных мест

1. Общие требования:

– наименование разрабатываемой системы:

– разработка ПО для защиты от DDoS атак на облачный хостинг

– цель разработки:

  – обеспечить контроль защиты от DDoS атак;

  – контролировать пропуск трафика.

  – пропускать автомобили только с определенными регистрационными номерами;

  – не пропускать ip, внесенные в черный список;

– предлагаемые технологии для разработки системы (на выбор разработчика):

  – Cisco snort

  – одноплатный компьютер (для стойки управления).

– выбор архитектуры построения:

  – клиент-Сервер.

– предлагаемые языки и технологии программирования:

  – C

  – C#

– общий объем программной части системы, Мб

  – не более 200 Мб.

2. Технические требования:

– требования к программному обеспечению:

  – умеренная скорость обработки входящей информации;

  – возможность работы с облачными решениям;

  – код программы должен быть минималистичным и понятным.

– требования к аппаратному обеспечению:

  – наличие минимального количества оборудования;

  – стойка управления должна обладать достаточной вычислительной мощностью для обработки графических изображений;

– тестирование и отладка системы:;

  – тестирование системы на вероятность ложной DDoS атаки;

  – тестирование системы на сбой.

4. Экономические требования:

– расчет стоимости системы и стоимости разработки программного обеспечения (подлежит обсуждению):

  – стоимость готового продукта 2 000 000тг;

  – стоимость разработки 1 000 000тг.

.

Приложение Б
(обязательное)

Листинг программы

Исходный код модуля расширение функциональности для IPS Snort_inline

```
http {

  limit_conn_zone $binary_remote_addr
zone=download_c:10m;
  limit_req_zone $binary_remote_addr zone=search_r:10m \
      rate=1r/s;

 server {
  location /download/ {
   limit_conn download_c 1;
   # Прочая конфигурация location
  }

    location /search/ {
      limit_req zone=search_r burst=5;
      # Прочая конфигурация location
    }

 }
}
```

```
sysctl -w net.core.rmem_max=8388608
sysctl -w net.core.wmem_max=8388608
sysctl -w net.ipv4.tcp_rmem='4096 87380 8388608'
sysctl -w net.ipv4.tcp_wmem='4096 65536 8388608'
sysctl -w net.ipv4.tcp_fin_timeout=10
```

```
net.isr.direct=1 kern.ipc.nmbclusters=400000 net.inet.tcp.nolocaltimewait=1
net.inet.tcp.recvspace=16384 net.inet.tcp.sendspace=32768 net.inet.tcp.msl=5000
net.inet.tcp.blackhole=1 net.inet.ip.intr_queue_maxlen=3000
net.inet.tcp.blackhole=2 net.inet.udp.blackhole=1 net.inet.icmp.log_redirect=1
net.inet.ip.redirect=0 net.inet.icmp.maskrepl=1 net.inet.tcp.syncookies_only=1
net.route.netisr_maxqlen=4096 kern.ipc.maxsockbuf=83886080
net.inet.ip.intr_queue_maxlen=10240
```

```
netstat -n | grep SYN_RECV | wc -l
```

Если больше 5 соединений, значит, это syn атака.

1) Вводим для iptables правила:

iptables -N syn_flood

iptables -A INPUT -p tcp --syn -j syn_flood

iptables -A syn_flood -m limit --limit 30/s --limit-burst 100 -j RETURN

iptables -A syn_flood -j DROP

*На данный момент не советуем пользоваться этим пунктом, т.к., по какой-то причине, блокирует все подряд

2) Устанавливаем лимиты в /etc/sysctl.conf:

net.ipv4.tcp_max_syn_backlog = 40000

net.ipv4.tcp_synack_retries = 1

net.ipv4.tcp_syn_retries = 1

net.ipv4.tcp_syncookies = 1

net.core.somaxconn = 60000

net.ipv4.tcp_fin_timeout = 15

net.ipv4.tcp_keepalive_probes = 5

net.ipv4.tcp_keepalive_intvl = 15

net.ipv4.tcp_keepalive_time = 15

net.core.netdev_max_backlog = 40000

net.ipv4.ip_local_port_range = 1024 65535

net.ipv4.conf.default.rp_filter = 1

net.ipv4.tcp_max_syn_backlog = 4096

net.ipv4.tcp_window_scaling = 0

net.ipv4.tcp_sack = 0

net.ipv4.tcp_timestamps = 0

net.ipv4.tcp_tw_recycle = 1

net.ipv4.tcp_tw_reuse = 1

net.netfilter.nf_conntrack_max=400000

net.netfilter.nf_conntrack_tcp_timeout_close = 5

net.netfilter.nf_conntrack_tcp_timeout_time_wait = 5

net.netfilter.nf_conntrack_tcp_timeout_last_ack = 1

net.netfilter.nf_conntrack_tcp_timeout_close_wait = 5

net.netfilter.nf_conntrack_tcp_timeout_fin_wait = 1

net.netfilter.nf_conntrack_tcp_timeout_established = 30

net.netfilter.nf_conntrack_tcp_timeout_syn_recv = 1

net.netfilter.nf_conntrack_tcp_timeout_syn_sent = 1

net.netfilter.nf_conntrack_tcp_loose = 0

```
/var/log/nginx/*.log

{ daily size 20M
```

```
missingok rotate 150

compress delaycompress notifempty

create 640 root adm sharedscripts

postrotate [ ! -f /var/run/nginx.pid ] ||

kill -USR1 `cat /var/run/nginx.pid` endscript }
```

Приложение В
(обязательное)

Акты внедрения