ФГБОУ ВО «Уфимский университет науки и технологий»

Факультет информатики и робототехники
Кафедра вычислительной техники и защиты информации

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

по направлению 10.03.01 Информационная безопасность
(шифр, наименование)

НА ТЕМУ: Разработка комплексного решения защиты систем виртуализации, использующих VMware Workstation

К защите допущен

Заведующий кафедрой

Картак В.М. (_____)
(фамилия, инициалы) (подпись)

«_____»_____20___ г.

Обучающийся

Д. В. Золотарев_____ ___(_____)
(фамилия, инициалы) (подпись)

Руководитель выпускной квалификационной работы

Н. Д. Андреев _____(_____)
(фамилия, инициалы) (подпись)

ФГБОУ ВО «Уфимский университет науки и технологий»

Факультет информатики и робототехники
Кафедра вычислительной техники и защиты информации

«УТВЕРЖДАЮ»
Зав. кафедрой _____В. М. Картак
(подпись, Фамилия И. О.)

«___»_____2023 г.

ЗАДАНИЕ

по подготовке выпускной квалификационной работы

обучающемуся Золотареву Данилу Викторовичу группы ИБ-422

1. Тема выпускной квалификационной работы: Разработка комплексного решения защиты систем виртуализации, использующих VMware Workstation
(утверждена распоряжением факультета от 24.11.2023 № 5)
Тема спецчасти выпускной квалификационной работы не предусмотрена.

2. Срок сдачи обучающимся законченной выпускной квалификационной работы

3. Исходные данные к выпускной квалификационной работе:

- Нормативные требования к системам виртуализации

4. Перечень вопросов, подлежащих разработке в выпускной квалификационной работе (краткое содержание, при необходимости с указанием разделов)

- Провести обзор архитектуры современных систем виртуализации и выделить основные угрозы информационной безопасности и средства защиты от них.
- Изучить правовое поле систем виртуализации.
- Исследовать существующие решения и методы защиты систем виртуализации и провести их сравнительный анализ.
- Провести настройку комплексной системы защиты виртуализации VMware Workstation.
- Проанализировать полученное решение на защиту от выявленных уязвимостей

5. Цель и объем патентных исследований: не предусмотрены.

6. Объем и степень использования программного обеспечения: в ходе выполнения работы было активно использовано несколько программных продуктов, включая PFSENSE для контроля и фильтрации сетевого трафика, SURICATA для обнаружения и предотвращения атак, FLAN SCAN для сканирования сети и обнаружения уязвимостей, а также CLAMAV для обнаружения и предотвращения вредоносных программ.

7. Объем расчетно-пояснительной записки на 60 листах А4 формата.

8. Перечень графического материала (с указанием вида обязательных чертежей): не предусмотрены.

Всего не менее _____ листов.

Дата выдачи задания «17» апреля 2023 г.

Руководитель Н. Д. Андреев «____» _____20_____г.

ФГБОУ ВО «Уфимский университет науки и технологий»

Факультет информатики и робототехники
Кафедра вычислительной техники и защиты информации

«УТВЕРЖДАЮ»
Зав. кафедрой _____В. М. Картак
(подпись, Фамилия И. О.)

«___» _____ 2023 г.

КАЛЕНДАРНЫЙ ПЛАН

работы над выпускной квалификационной работой

обучающегося Золотарева Данила Викторовича группы ИБ-422

Тема выпускной квалификационной работы: Разработка комплексного решения защиты систем виртуализации, использующих VMware Workstation

Тема спецчасти: не предусмотрена

№ п/п	Наименование разделов выпускной квалификационной работы	Срок	Объем (в % от всей выпускной квалификационной работы)	Фактическое (объем работы в %)
Расчет и описание				
1	Введение	25.04.2023	5%	5%
1	Обзор современных технологий виртуализации	17.04.2023	10%	10%
2	Правовое поле виртуализации	24.04.2023	10%	20%
3	Выбор решения для реализации	2.05.2023	30%	50%
4	Настройка системы комплексной защиты	22.05.2023	30%	80%
5	Анализ полученных результатов	02.06.2023	10%	90%
6	Заключение	7.06.2023	10%	100%

Обучающийся:
Д. В. Золотарев _____ «__» _____ 2023 г.
(подпись)

Руководитель выпускной квалификационной работы:
Н. Д. Андреев _____ «__» _____ 2023 г
(подпись)

Ход выполнения выпускной квалификационной работы:

Дата просмотра выпускной квалификационной работы на кафедре	15.05.2023	25.05.2023	05.06.2023	10.06.2023
Объем выполнения выпускной квалификационной работы в %	35%	60%	95%	100%

Дата защиты выпускной квалификационной работы на заседании ГЭК
«____» _____ 2023 г.

АННОТАЦИЯ

Пояснительная записка содержит 60 страниц, 1 таблицу, 28 рисунков.

Тема выпускной квалификационной работы “разработка и установка комплексной системы обеспечения безопасности системы VMware Workstation.”

Выпускная квалификационная работа состоит из перечня принятых сокращений, введения, пяти разделов, поделённых на подразделы, заключения и списка литературы.

Во введении представлена актуальность анализируемой темы, цели и задачи, предмет и объект исследования.

В первой главе изучаются методы и технологии защиты систем виртуализации, её архитектура и уязвимости.

Во второй главе проводится исследование правового поля виртуализации в России.

Третья глава посвящена анализу существующих решений по защите систем виртуализации, использующих VMware Workstation.

Четвертая глава описывает разработку комплексного решения для защиты систем виртуализации и его реализацию.

Пятая глава включает анализ полученных результатов и оценку эффективности разработанного комплексного решения.

Оглавление

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

1. ВМ - виртуальная машина
2. СИ - система виртуализации
3. VMware WS - VMware Workstation
4. КРЗ - комплексное решение защиты
5. АС - архитектурная схема
6. УБ - уязвимость безопасности
7. СЗ - средства защиты
8. АУ - аутентификация и авторизация
9. КД - контроль доступа
10. МИ - механизмы изоляции
11. ШД - шифрование данных
12. МО - мониторинг и обнаружение
13. СО - системы обновления
14. АБ - аудит безопасности
15. ОЦБ - облачные сервисы безопасности
16. ПО - программное обеспечение
17. ПИД - процесс идентификации и документирования
18. ТП - техническое задание
19. ПТО - программно-техническое обеспечение
20. ИБ - информационная безопасность.

ВВЕДЕНИЕ

В свете непрерывно растущего объема цифровых данных и непрекращающегося технологического прогресса, виртуализация стала неотъемлемой частью современных информационных систем. Она предоставляет огромные возможности для эффективного использования аппаратных ресурсов, экономии энергии и управления ИТ-инфраструктурой. Однако вместе с этими преимуществами виртуализация привнесла и новые угрозы в область информационной безопасности. Программное обеспечение для виртуализации, такое как VMware Workstation, не является исключением из этого правила.

VMware Workstation – это одно из самых популярных и широко используемых программных решений для виртуализации на уровне операционной системы. Однако, несмотря на его популярность и мощные функции, он также подвержен множеству угроз информационной безопасности, таких как вредоносное ПО, атаки из сети и уязвимости в программном обеспечении, что ставит под угрозу целостность, доступность и конфиденциальность данных.

В настоящей работе проводится подробный анализ с точки зрения информационной безопасности. Определяются ключевые угрозы и уязвимости, на основе чего предлагается комплексное решение для обеспечения безопасности.

Основной целью данного исследования является разработка решения, эффективного как в рамках конкретной виртуализационной платформы, так и в области виртуализации в целом. Таким образом, нашей задачей является значительный вклад в повышение уровня информационной безопасности в данной сфере.

В центре исследования будет находиться разработка интегрированного решения для обеспечения информационной безопасности. Это решение будет включать использование существующих инструментов, а также создание уникального программного обеспечения. Цель заключается в создании

комплексного подхода, способного справиться с уязвимостями виртуализированных систем.

В соответствии с поставленной целью, выпускная квалификационная работа нацелена на представление всестороннего подхода к обеспечению максимальной информационной безопасности для виртуализированных систем.

Исходя из поставленной цели, выпускная квалификационная работа нацелена на представление комплексного подхода к обеспечению максимальной информационной безопасности для систем виртуализации VMware WorkStation.

Для достижения поставленной цели необходимо успешное выполнение следующих задач:

– Изучение методов и технологий защиты систем виртуализации
– Изучение уязвимости систем виртуализации и методы их эксплуатации
– Изучение анализ существующих решений по защите систем виртуализации, использующих VMware Workstation
– Разработка комплексного решения защиты систем виртуализации
– Анализ полученных результатов

1 Обзор современных технологий виртуализации

Виртуализация - группа технологий, основанных на преобразовании формата или параметров программных, или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы. В последнее десятилетие она стала особенно популярной в связи с быстрым развитием вычислительных мощностей компьютеров. Новые многоядерные процессоры, увеличение пропускной способности интерфейсов и рост емкости систем хранения данных создают условия для переноса множества серверов в виртуальную среду. Это достигается благодаря сочетанию современных технологий виртуализации и имеющихся ресурсов на одном физическом сервере.

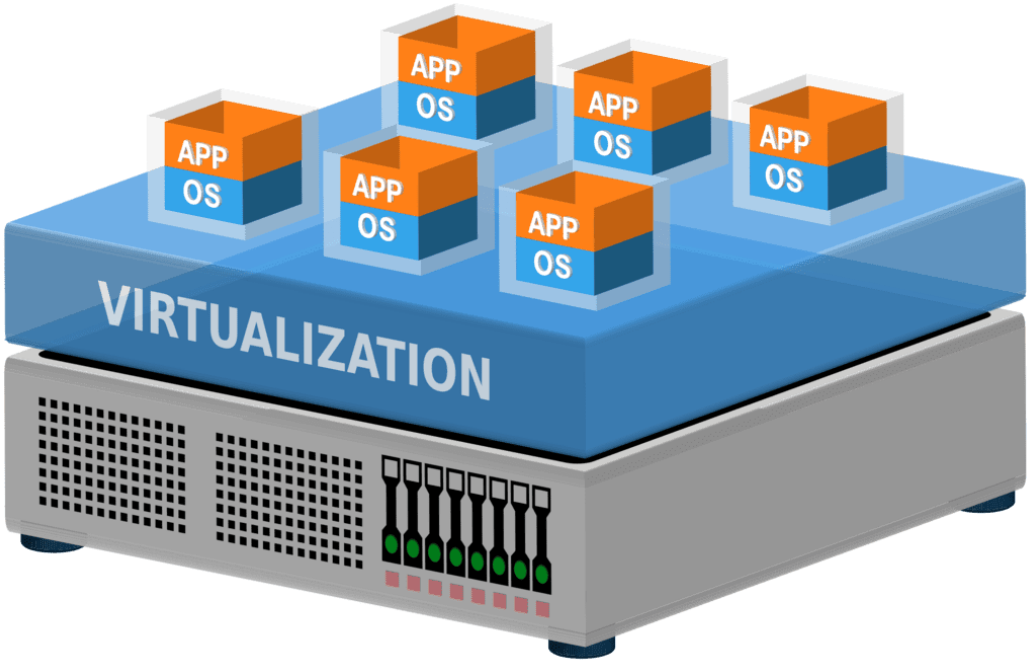

Рисунок 1 – Пример реализации виртуализации

Основная идея виртуализации состоит в возможности эффективного распределения ресурсов одного компьютера между изолированными средами, что позволяет использовать несколько виртуальных машин на одном физическом сервере, данное распределение проиллюстрировано на рисунке 1. Это позволяет

разместить различные операционные системы и приложения внутри виртуальных сред, создавая удобную и гибкую конфигурацию. Виртуализация также может использоваться в обратном направлении, объединяя несколько физических серверов в единый серверный кластер или grid computing.

В более широком смысле виртуализация представляет собой концепцию, которая разделяет представление и реализацию объектов. Она позволяет абстрагироваться от конкретных деталей аппаратной реализации и предоставляет унифицированный интерфейс для работы с вычислительными ресурсами. В результате пользователи могут взаимодействовать с удобным представлением объектов, не заботясь о том, как они физически реализованы.

Таким образом, виртуализация играет важную роль в современных информационных системах, позволяя эффективно использовать ресурсы, облегчать управление и предоставлять гибкую конфигурацию. Она обеспечивает эффективное разделение физических ресурсов и создает абстракцию, которая скрывает детали реализации от пользователей, упрощая работу и повышая гибкость систем.

1.1 Архитектура систем виртуализации

Архитектура систем виртуализации основана на гипервизорах, которые играют ключевую роль в управлении виртуальными машинами и взаимодействии между физическим оборудованием и виртуальными ресурсами. Гипервизоры работают на уровне аппаратного обеспечения и предоставляют платформу для создания, запуска и управления виртуальными машинами.

Рисунок 2 – Структура гипервизора первого типа

Существует два типа гипервизоров: тип 1 и тип 2. Гипервизор типа 1 (нативный или беспосредственный) работает напрямую на физическом оборудовании и управляет виртуальными машинами, структура строения приведена на рисунке 2, обеспечивая им доступ к ресурсам сервера. Примеры гипервизоров типа 1 включают VMware ESXi, Microsoft Hyper-V и KVM. Гипервизор типа 2 (хостовый или основанный на ОС) работает поверх операционной системы хоста и позволяет запускать виртуальные машины как обычные приложения. Примерами гипервизоров типа 2 являются VMware Workstation, Oracle VirtualBox и Microsoft Virtual PC, его архитектура продемонстрирована на рисунке 3.

Рисунок 3 – Устройство гипервизора второго типа

Особое внимание стоит обратить на VMware Workstation. Это мощное программное обеспечение для виртуализации на рабочей станции, которое предоставляет пользователям возможность создавать и запускать несколько виртуальных машин на одном физическом компьютере. VMware Workstation позволяет эмулировать различные операционные системы, включая Windows, Linux и macOS. Он широко используется разработчиками программного обеспечения, системными администраторами и пользователями, которым необходимо иметь доступ к различным операционным системам на одной машине без необходимости физических устройств.

Преимущества VMware Workstation включают гибкость и настраиваемость виртуальных машин, удобство использования, возможность создания снимков состояния, что позволяет быстро восстанавливать виртуальные машины к

предыдущим состояниям, а также эффективное использование ресурсов компьютера.

Однако, важно понимать, что при использовании систем виртуализации, включая VMware Workstation, информационная защищенность играет решающую роль. Виртуализированные среды могут подвергаться различным угрозам и атакам, и необходимо принимать соответствующие меры безопасности для защиты данных и обеспечения надежности системы.

1.2 Уязвимости систем виртуализации и методы их эксплуатации

Системы виртуализации предоставляют значительные преимущества в эффективности и управляемости, однако они также подвержены многочисленным угрозам и уязвимостям. В контексте данной работы были выделены следующие основные категории угроз и уязвимостей:

− Уязвимости гипервизора: Гипервизор является ключевым компонентом системы виртуализации, обеспечивающим разделение ресурсов и управление виртуальными машинами. Однако уязвимости в гипервизоре могут привести к возможности получения несанкционированного доступа к всем виртуальным машинам на сервере. Это может быть вызвано неправильной конфигурацией, слабыми паролями или программными ошибками в самом гипервизоре.

− Атаки на разделение (Escape Attacks): Эти атаки направлены на преодоление изоляции между виртуальными машинами или между виртуальными машинами и гипервизором. Злоумышленники, успешно осуществившие такие атаки, могут выйти за пределы своей виртуальной машины и вмешаться в работу других виртуальных машин или даже контролировать гипервизор. Это может быть

достигнуто через эксплуатацию уязвимостей в гипервизоре или использование специально созданных программ.

− Внутренние и внешние атаки: Внутренние атаки могут быть выполнены злоумышленниками, уже имеющими доступ к виртуальной машине, например, через скомпрометированный аккаунт. Они могут осуществлять несанкционированные действия внутри виртуальной машины или пытаться получить доступ к другим виртуальным машинам на сервере. Внешние атаки, направленные на системы виртуализации, могут происходить из внешней сети и нацелены на гипервизор или другие виртуальные машины. Это могут быть попытки взлома, DDoS-атаки или попытки эксплойтов.

− Перехват сетевого трафика: Данные, передаваемые между виртуальными машинами, могут быть подвержены перехвату или подмене. Злоумышленники могут использовать средства перехвата, такие как sniffing или man-in-the-middle атаки, чтобы получить доступ к конфиденциальной информации или вмешаться в передачу данных между виртуальными машинами. Это может привести к компрометации данных или нарушению их целостности.

− Вредоносное программное обеспечение (ВПО): Виртуальные машины также подвержены угрозам вредоносного ПО, включая вирусы, троянские программы и другие. Злоумышленники могут использовать различные методы, такие как эксплойты или социальная инженерия, для внедрения вредоносного ПО в виртуальную машину. Это может привести к компрометации данных, уничтожению файлов или нарушению нормальной работы системы.

Важно отметить, что эффективная защита от этих угроз и уязвимостей требует комплексного подхода. Это включает в себя регулярное обновление и укрепление программного обеспечения, мониторинг и реагирование на инциденты безопасности, шифрование данных.

1.3 Средства защиты

Для преодоления описанных выше уязвимостей, разработаны специализированные методы и средства защиты систем виртуализации.

1. Защита гипервизора

Уязвимости гипервизора являются одним из основных факторов риска для систем виртуализации. Существует несколько мер защиты:

− Обновления: сохранение гипервизора и всей системы в актуальном состоянии, с установкой последних обновлений и патчей, является критически важным шагом для минимизации уязвимостей.

− Минимизация поверхности атаки: это подразумевает удаление всех ненужных служб и функций в гипервизоре, чтобы уменьшить количество потенциальных целей для злоумышленников.

− Использование аппаратной виртуализации: некоторые современные процессоры предлагают функции, которые увеличивают безопасность гипервизора, например, Intel VT-x и AMD-V.

2. Защита от атак на разделение

− Защита от так называемых "атак на разделение" или "escape attacks" может включать в себя мониторинг поведения виртуальных машин и гипервизора с помощью систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS).

− Отслеживание аномального поведения: поведенческий анализ может быть использован для выявления подозрительных действий, которые могут указывать на попытку вмешательства в работу других виртуальных машин или гипервизора.

3. Защита от внутренних и внешних атак

− Внутренние атаки: управление доступом и применение политики минимальных привилегий могут предотвратить несанкционированный доступ к виртуальной машине.

− Внешние атаки: использование межсетевых экранов (firewalls) и систем обнаружения вторжений (IDS) может обеспечить защиту от атак с внешней сети.

4. Защита сетевого трафика

− Использование шифрования: все данные, передаваемые между виртуальными машинами, следует шифровать, чтобы предотвратить их перехват или подмену.

− Сегментация сети: создание изолированных сетевых сегментов для виртуальных машин помогает снизить риск перехвата трафика.

5. Защита от вредоносного программного обеспечения

− Антивирусное программное обеспечение: установка антивирусных решений на каждую виртуальную машину помогает защитить их от вредоносного ПО.

− Обновление ПО: регулярное обновление операционной системы и приложений на виртуальных машинах помогает уменьшить риск заражения вредоносным ПО.

Важно подчеркнуть, что при создании комплексного решения защиты систем виртуализации на основе указанных выше инструментов и методов, следует тщательно учитывать соответствующие нормативные акты. Это обязательное условие, поскольку нерегулярное или неправильное использование систем виртуализации может привести к нарушению закона. С этой точки зрения, следующий раздел работы будет посвящен анализу законов и регулирований, регламентирующих работу систем виртуализации.

2 Правовое поле виртуализации

В Российской Федерации правовая база в области информационной безопасности и технического регулирования является ключевым фактором, определяющим условия и ограничения для использования систем виртуализации. Законодательство России регулирует использование систем виртуализации и устанавливает требования по безопасности информации, которые должны соблюдаться при разработке, внедрении и эксплуатации виртуализационных решений.

В данной главе рассматриваются законы и нормативные акты, которые регулируют использование систем виртуализации в России. Изучаются основные правовые требования, касающиеся безопасности информации, и определяются, каким образом эти требования влияют на процессы разработки и эксплуатации систем виртуализации.

2.1 Основные законодательные акты

В России существует несколько нормативных актов, которые прямо или косвенно относятся к системам виртуализации и их безопасности. Суть защиты изображена на рисунке 4.

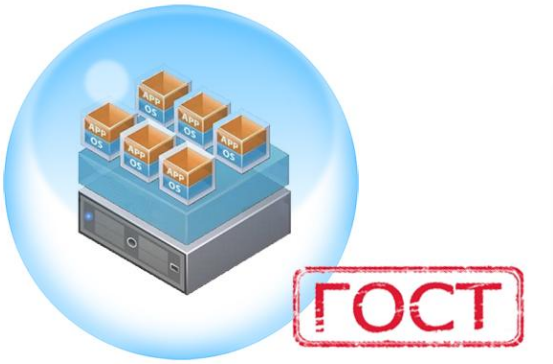

Рисунок 4 – Визуальное представление защиты виртуализации

1. ГОСТ Р 56938-2016

Данный ГОСТ был разработан Федеральным автономным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФАУ "ГНИИИ ПТЗИ ФСТЭК России") и внесен техническим комитетом по стандартизации "Защита информации" (ТК 362).

До введения ГОСТ Р 56938-2016 для обеспечения безопасности виртуализированных сред применялись рекомендации, изложенные в приказах ФСТЭК №17 и №21. В данных приказах имеется раздел, в котором описываются требования к защите среды виртуализации. Ниже представлена таблица 1 из приложения к указанным приказам, в которой перечислены эти требования.

Таблица 1 – Нормативы защиты виртуализации

XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.4	Рабочие станции, серверы, базы данных, сетевое оборудование Незаконный доступ, Кража информации,
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей

Не смотря на наличие требований к мерам по защите, в приказах не были определены термины по виртуализации, ГОСТ Р 56938-2016 закрывает данный пробел и определяет терминологическую базу.

ГОСТ Р 56938-2016 устанавливает два типа гипервизоров:

− Гипервизор 1 типа - устанавливается непосредственно на аппаратную платформу. Согласно ГОСТ, к таким гипервизорам относятся VMware vSphere, Hyper-V, Citrix XenServer и другие аналогичные системы.

− Гипервизор 2 типа - устанавливается в хостовую операционную систему. Примерами таких гипервизоров, указанными в ГОСТ, являются VirtualBox, VMware Workstation и аналогичные программы.

В блоке терминов ГОСТа особо выделяется гипервизор систем хранения данных, который определен следующим образом: это программа, устанавливаемая либо на аппаратное обеспечение в качестве системного программного обеспечения, либо в хостовую операционную систему в качестве прикладного программного обеспечения. Она выполняет функции посредника между логическим и физическим адресными пространствами, обеспечивая высокий уровень управления ресурсами хранения данных.

Также в этом же блоке терминов ГОСТа приведены определения виртуальной машины, различные типы виртуализации и ресурсы, которые могут быть виртуализированы, и т.д.

В соответствии с ГОСТом, виртуальная инфраструктура представляет собой композицию иерархически взаимосвязанных групп виртуальных устройств обработки, хранения и/или передачи данных, а также соответствующих аппаратных и/или программных средств, необходимых для их работы. ГОСТ определяет три уровня иерархии в виртуальной инфраструктуре:

− На первом (нижнем) уровне иерархии (уровне оборудования) располагается аппаратная часть периметра виртуальной инфраструктуры. Здесь используются аппаратные средства, которые реализуют технологии виртуализации, включая аппаратную поддержку виртуализации.

− На втором уровне иерархии (уровне виртуализации) находятся гипервизоры и объекты, порожденные ими. Эти объекты могут включать

виртуальные машины, виртуальные серверы, виртуальные процессоры, виртуальные диски, виртуальную память, виртуальное активное и пассивное сетевое оборудование, виртуальные средства защиты информации и другие.

– На третьем (верхнем) уровне иерархии (уровне управления) располагается средство централизованного управления гипервизорами в рамках одной виртуальной инфраструктуры. Это консоль управления виртуальной инфраструктурой, которая обеспечивает централизованное управление всей инфраструктурой.

Итоговое иерархическое строение изображено на рисунке 5.

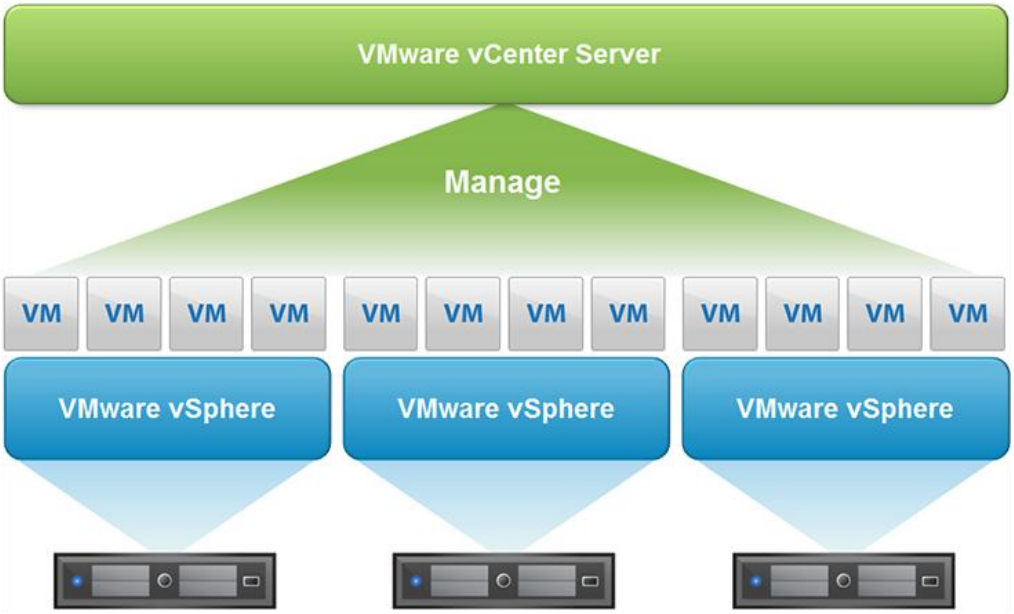

Рисунок 5 – Три уровня иерархии в виртуальной инфраструктуре на примере стека технологий VMware

Объекты защиты:

ГОСТ Р 56938-2016 выделяет следующие основные объекты защиты при использовании технологий виртуализации:

– Средства создания и управления виртуальной инфраструктурой: включают гипервизоры 1 и 2 типов, гипервизоры системы хранения данных, консоль управления виртуальной инфраструктурой и другие подобные средства.

– Виртуальные вычислительные системы: включают виртуальные машины, виртуальные серверы и другие аналогичные системы.

– Виртуальные системы хранения данных.

– Виртуальные каналы передачи данных.

– Отдельные виртуальные устройства обработки, хранения и передачи данных: такие как виртуальные процессоры, виртуальные диски, виртуальная память, виртуальное активное и пассивное сетевое оборудование, и другие.

– Виртуальные средства защиты информации (ЗИ) и средства ЗИ, предназначенные для использования в среде виртуализации.

– Периметр виртуальной инфраструктуры: включает центральные процессоры и их ядра, адресное пространство памяти, сетевые интерфейсы, порты подключения внешних устройств и другие компоненты, задействованные в реализации технологий виртуализации.

Угрозы безопасности:

ГОСТ Р 56938-2016 подчеркивает, что использование технологий виртуализации создает предпосылки для появления угроз безопасности, которые не характерны для информационных систем, построенных без использования виртуализации. ГОСТ перечисляет следующие 18 угроз, которые могут возникать при использовании технологий виртуализации:

– Атаки на активное и/или пассивное виртуальное и/или физическое сетевое оборудование из физической и/или виртуальной сети.

– Атаки на виртуальные каналы передачи данных.

– Атаки на гипервизор из виртуальной машины и/или физической сети.

– Атаки на защищаемые виртуальные устройства из виртуальной и/или физической сети.

– Атаки на защищаемые виртуальные машины из виртуальной и/или физической сети.

– Атаки на систему хранения данных из виртуальной и/или физической сети.

– Угрозы выхода процесса за пределы виртуальной машины.

– Несанкционированный доступ к данным за пределами зарезервированного адресного пространства, включая выделенное под виртуальное аппаратное обеспечение.

– Нарушение изоляции пользовательских данных внутри виртуальной машины.

– Нарушение процедуры аутентификации субъектов виртуального информационного взаимодействия.

– Перехват управления гипервизором.

– Перехват управления средой виртуализации.

– Неконтролируемый рост числа виртуальных машин.

– Неконтролируемый рост числа зарезервированных вычислительных ресурсов.

– Нарушение технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин.

– Несанкционированный доступ к хранимой в виртуальном пространстве защищаемой информации.

– Ошибки обновления гипервизора.

Важно отметить, что ГОСТ рассматривает угрозы, связанные с безопасностью виртуализации. При этом другие угрозы безопасности не теряют своей актуальности и также должны быть учтены при разработке модели угроз. Например, угрозы, связанные с физическим доступом к инфраструктуре, организационными вопросами доступа к информации, защитой учетных данных и т.д. Наличие дополнительных угроз, специфичных для среды виртуализации, видно из перечисленных в ГОСТе угроз, которых нет на более низком аппаратном уровне.

Меры защиты:

ГОСТ Р 56938-2016 представляет перечень мер защиты, разделенных на несколько групп в зависимости от объекта защиты. В нем выделяются следующие группы мер:

- Защита средств создания и управления виртуальной инфраструктурой.
- Защита виртуальных вычислительных систем.
- Защита виртуальных систем хранения данных.
- Защита виртуальных каналов передачи данных.
- Защита отдельных виртуальных устройств обработки, хранения и передачи данных.
- Защита виртуальных средств защиты информации и средств защиты информации, предназначенных для использования в среде виртуализации.

Следует также отметить, что понятие снимков виртуальных машин (snapshots) не рассматривается ни в ГОСТ, ни в приказах. В связи с этим, угрозы, связанные со снимками, не рассматриваются. Например, в американском стандарте NIST снимок виртуальной машины рассматривается как отдельный объект защиты.

2. Федеральный закон №149-ФЗ "Об информации, информационных технологиях и о защите информации"

Этот закон регулирует отношения в области информации, информационных технологий и защиты информации. Он предусматривает ряд обязательств и требований, связанных с обеспечением конфиденциальности, целостности и доступности информации. Закон устанавливает требования к организациям по защите информации, включая информацию, хранящуюся и обрабатываемую в системах виртуализации. Он определяет меры, направленные на предотвращение угроз безопасности информации, включая неправомерный доступ, уничтожение или изменение информации, а также требования к системам защиты информации и контроля доступа к ней.

3. Постановление Правительства РФ №1119 "Об утверждении требований к защите информации"

Данный нормативный акт содержит требования к защите информации, которые должны быть выполнены при создании и эксплуатации информационных систем. Он включает требования по защите информации от неправомерного доступа, модификации, блокировки, копирования, предоставления, распространения и других неправомерных действий. Постановление определяет обязательные меры и технические требования для обеспечения безопасности информации в системах виртуализации. Оно также предусматривает проведение аудита и контроля за соблюдением требований по защите информации.

4. ГОСТ Р ИСО/МЭК 27001 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

Этот международный стандарт был принят в России как ГОСТ и представляет собой набор требований к системам менеджмента информационной безопасности. Он определяет методы и средства обеспечения безопасности информации, включая информацию, хранящуюся и обрабатываемую в системах виртуализации. ГОСТ Р ИСО/МЭК 27001 устанавливает требования к разработке, внедрению, эксплуатации и улучшению системы менеджмента информационной безопасности. Он помогает организациям обеспечить непрерывность бизнеса, минимизировать риски ущерба от информационных инцидентов и оптимизировать инвестиции в безопасность.

2.2 Итоговые требования к системе

На основе анализа уязвимостей систем виртуализации и релевантных нормативных актов Российской Федерации, включая ГОСТ Р 56938-2016, можно выделить следующие требования к системе информационной безопасности:

- Защита от уязвимостей гипервизора: система должна обеспечивать безопасную и обновленную конфигурацию гипервизора, чтобы предотвратить возможные уязвимости и атаки.
- Защита от атак на разделение: система должна изолировать виртуальные машины и контролировать их взаимодействие, предотвращая атаки на разделение ресурсов и информации между виртуальными средами.
- Устойчивость к внутренним и внешним атакам: система должна обеспечивать контроль доступа и аутентификации для предотвращения несанкционированного доступа внутри и снаружи системы.
- Защита сетевого трафика: система должна защищать сетевой трафик от перехвата или подмены с помощью шифрования и сетевых экранов, обеспечивая конфиденциальность и целостность данных.
- Борьба с вредоносным программным обеспечением: система должна включать антивирусные решения и системы обнаружения и предотвращения вторжений для защиты от вредоносных программ и связанных атак.
- Соответствие нормам и стандартам: система должна соответствовать требованиям, установленным постановлением Правительства РФ №1119 и стандартам ГОСТ Р ИСО/МЭК 27001 в области систем менеджмента информационной безопасности.

Удовлетворение всем этим требованиям может быть сложной задачей, требующей значительных усилий и ресурсов. Поэтому важно проанализировать существующие инструменты обеспечения информационной безопасности и выбрать наиболее эффективные для удовлетворения этих требований.

3 Выбор решения для реализации

В предыдущей главе рассмотрены основные нормативные требования, регулирующие использование систем виртуализации в России. Они определяют стандарты безопасности и требования к программным средствам, обеспечивающим создание и функционирование изолированных программных сред в информационных системах. Однако, чтобы реализовать эти требования на практике, необходимо обратить внимание на существующие инструменты обеспечения информационной безопасности.

Следующий раздел представит общее решение, ориентированное как на устранение уязвимостей систем виртуализации, так и на соответствие требованиям правового поля. Проводимый анализ и сравнение различных инструментов, предлагаемых на рынке, позволит выявить те, которые наиболее эффективно решают проблемы безопасности систем виртуализации и соответствуют требованиям законодательства Российской Федерации.

Обзор существующих решений позволит нам оценить их функциональность, возможности контроля и мониторинга, а также механизмы обеспечения безопасности. Будут учтены их преимущества и ограничения, для определения наиболее подходящих инструментов и подходов к защите систем виртуализации с учетом требований безопасности и законодательства.

3.1 Основные продукты

3.1.1 VMware NSX:

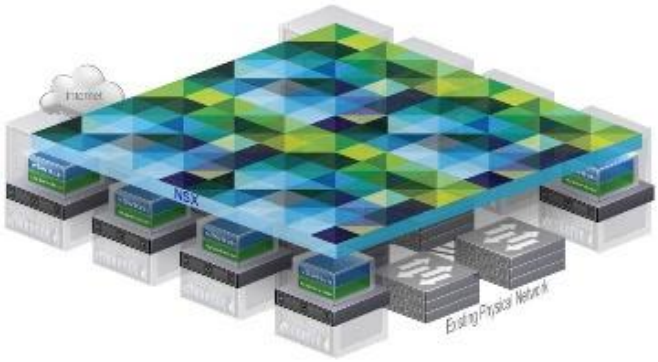

Рисунок 6 – Официальное представление VMware NSX

Данный инструмент представляет централизованное решение для управления виртуализированными сетями и службами безопасности, его суть отображена на рисунке 6.

Возможности VMware NSX:

− Микросегментация: NSX предоставляет возможность микросегментации, что позволяет создавать более мелкие и изолированные сегменты виртуальной сети для каждой виртуальной машины или группы виртуальных машин. Это обеспечивает более высокий уровень изоляции и снижает риск распространения угроз.

− Виртуальный брандмауэр: NSX включает в себя распределенный брандмауэр, который фильтрует трафик на уровне каждой виртуальной машины, обеспечивая детализированный контроль доступа.

− Прокси-серверы: NSX предоставляет функционал виртуальных прокси-серверов для мониторинга и контроля сетевого трафика, что способствует обнаружению аномалий и предотвращению угроз.

− Недостатки VMware NSX:

− Обнаружение сложных угроз: несмотря на предлагаемые функции защиты, NSX может испытывать трудности с обнаружением и предотвращением

более сложных атак, таких как атаки на разделение (escape attacks), которые направлены на преодоление изоляции виртуальных машин и доступ к гипервизору.

– Защита гипервизора: NSX фокусируется в основном на защите виртуализированных сетей и может не предоставлять адекватной защиты для гипервизора, который является критическим компонентом систем виртуализации и может стать мишенью для атак.

– Соответствие нормативным актам: в то время как NSX предлагает обширные возможности по обеспечению безопасности, оно может не обеспечивать полное соответствие требованиям нормативных документов в сфере защиты критической информационной инфраструктуры.

3.1.2 Trend Micro Deep Security

Это решение для обеспечения безопасности виртуализированных и облачных сред, обеспечивающее защиту от вредоносного ПО и угроз, пример возможностей данного ПО продемонстрирован на рисунке 7.

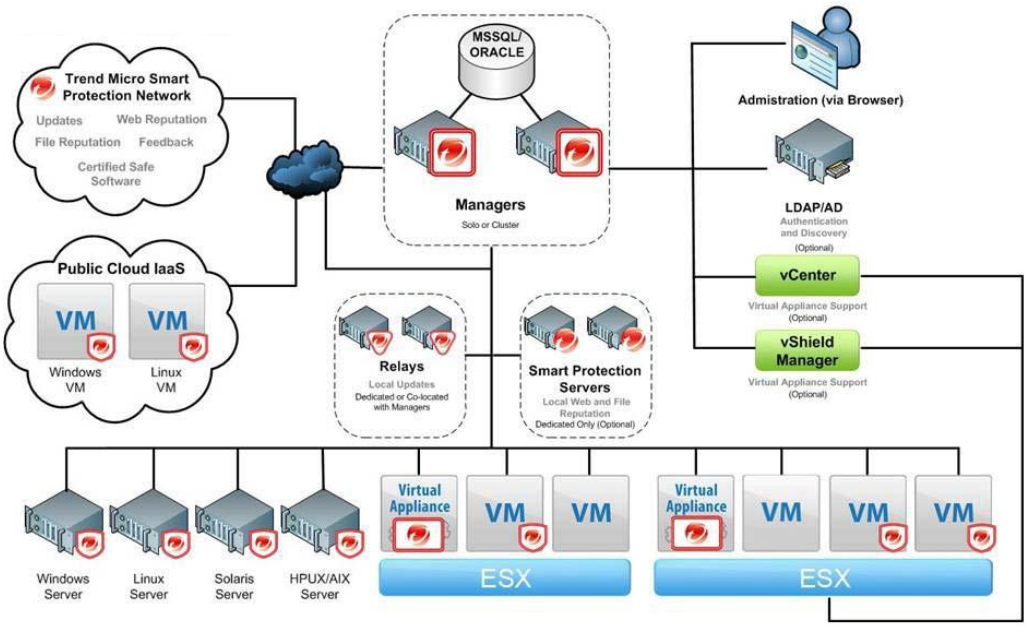

Рисунок 7 – Общая архитектура Trend Micro Deep Security 8.0

Возможности Trend Micro Deep Security:

− Защита от вредоносного ПО: Deep Security предлагает обширные функции защиты виртуальных машин от вредоносного ПО, включая реальное время сканирования и обновления баз данных вредоносных программ.

− Контроль целостности: это решение обеспечивает мониторинг и контроль целостности систем, что помогает обнаруживать и предотвратить несанкционированные изменения.

− Защита от вторжений (IPS): Deep Security имеет встроенный механизм защиты от вторжений, который обеспечивает обнаружение и блокирование атак на уровне сети и приложений.

Недостатки Trend Micro Deep Security:

− Ограниченные возможности автоматизации: хотя Trend Micro Deep Security обеспечивает большой набор функций для обеспечения безопасности, автоматизация процессов может быть ограничена. Это может привести к увеличению времени реакции на угрозы и снижению общей эффективности системы безопасности.

− Отсутствие поддержки микросегментации: в отличие от некоторых других решений, Trend Micro Deep Security не предлагает поддержку микросегментации. Это может создать проблемы с контролем доступа и изоляцией в среде с большим количеством виртуальных машин.

− Управление политиками: Deep Security может испытывать сложности с гибким управлением политиками безопасности в сложной или динамической среде виртуализации.

3.1.3 Check Point CloudGuard

Мощное решение для обеспечения безопасности виртуализированных и облачных сред, оно предлагает продвинутые функции защиты и управления доступом, все основные инструменты представлены на рисунке 8.

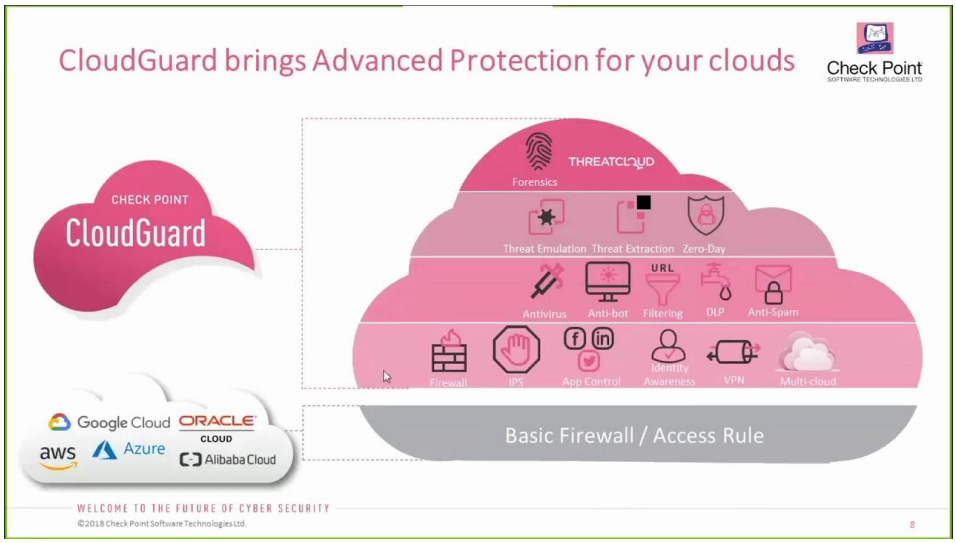

Рисунок 8 – Представление основных возможностей CPCG

Возможности Check Point CloudGuard:

– Продвинутая защита от угроз: CloudGuard использует AI и машинное обучение для обеспечения защиты от вредоносного ПО, эксплойтов zero-day и других угроз.

– Управление доступом: решение предлагает сильные функции управления доступом, позволяя контролировать, как пользователи и приложения могут взаимодействовать с виртуальными машинами.

– Микросегментация: CloudGuard поддерживает микросегментацию, что позволяет ограничивать сетевые потоки между виртуальными машинами и таким образом уменьшает риск перехвата или подмены данных.

Недостатки Check Point CloudGuard:

– Ограничения по совместимости: в то время как CloudGuard предлагает мощную защиту для большинства виртуализированных и облачных сред, в некоторых сценариях его совместимость может быть ограничена. Это включает

совместимость с некоторыми версиями гипервизоров или определенными архитектурами виртуализации.

– Детальность аудита и мониторинга: в то время как CloudGuard предоставляет обширные функции защиты, его возможности аудита и мониторинга могут быть недостаточными для некоторых сложных или высоко регулируемых сред. Это может создать трудности в обеспечении полной видимости и отчетности об угрозах и инцидентах безопасности.

– Управление политиками безопасности: CloudGuard может испытывать трудности при поддержке сложных и динамически изменяющихся политик безопасности. Это может создавать проблемы при быстрой адаптации к изменяющимся требованиям безопасности и угрозам.

3.1.4 Nutanix Flow

Это решение для микросегментации и обеспечения безопасности в виртуализированных и облачных средах. Это предлагает расширенный набор функций для защиты данных и управления сетевым трафиком, они представлены на рисунке 9.

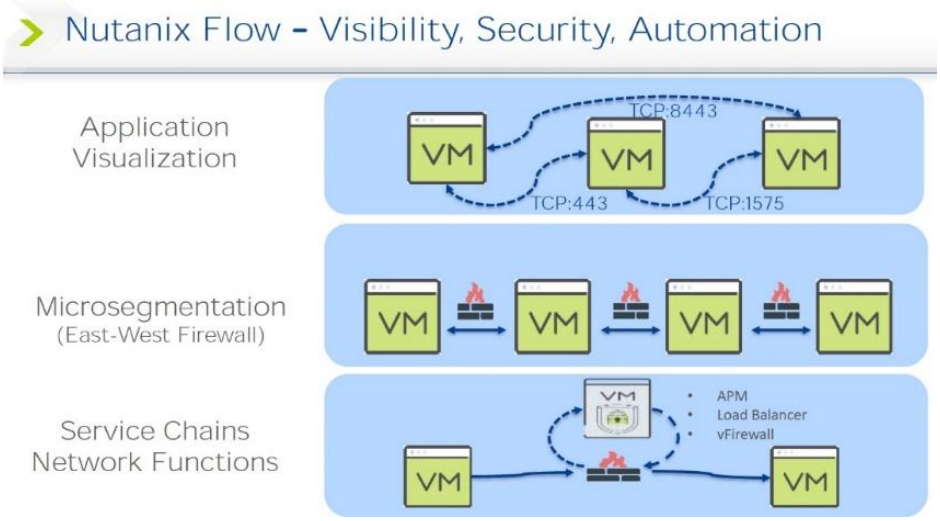

Рисунок 9 – Представление основных инструментов Nutanix Flow

Преимущества Nutanix Flow:

− Микросегментация: одной из ключевых функций Nutanix Flow является микросегментация, которая позволяет контролировать трафик между виртуальными машинами. Это помогает уменьшить риск перехвата или подмены данных.

− Защита на уровне приложений: Nutanix Flow предлагает возможности защиты на уровне приложений, что позволяет предотвратить атаки на приложения, работающие на виртуальных машинах.

− Автоматизация политик безопасности: Nutanix Flow позволяет автоматизировать применение политик безопасности, что упрощает управление безопасностью в динамических виртуализированных средах.

Недостатки Nutanix Flow:

− Ограничения в области совместимости: в то время как Nutanix Flow предлагает широкий набор функций для обеспечения безопасности, его совместимость с некоторыми гипервизорами и архитектурами виртуализации может быть ограничена.

− Сложности в настройке: несмотря на свою мощь, Nutanix Flow может быть сложным в настройке и оптимизации. Это может потребовать значительных знаний и опыта в области обеспечения безопасности.

− Оптимизация производительности: как и любое решение для обеспечения безопасности, Nutanix Flow может оказывать влияние на производительность виртуализированной среды. Это требует постоянного мониторинга и оптимизации.

Все эти решения - VMware NSX, Trend Micro Deep Security, Check Point CloudGuard, и Nutanix Flow - обычно предлагаются как коммерческие продукты. Они обычно имеют структуру ценообразования, основанную на подписке, которая может варьироваться в зависимости от размера и сложности виртуализированной среды, которую вы хотите защитить.

Некоторые из этих компаний могут предлагать бесплатные пробные версии или демоверсии своих продуктов для тестирования, но эти версии обычно имеют ограниченный набор функций и предназначены только для ознакомления с продуктом, а не для полноценного использования в производственной среде.

Исходя из анализа, заключено, что каждое из этих решений имеет свои сильные стороны, но также имеет ограничения, которые могут привести к уязвимостям в определенных сценариях. Все они имеют некоторые ограничения в своих способностях предотвратить атаки и обеспечивать полную защиту систем виртуализации. Поэтому, для обеспечения высокого уровня безопасности и соответствия нормативным требованиям, необходимо разработать и реализовать комплексное решение, которое сочетает в себе различные инструменты и методы защиты.

3.2 Подбор необходимых инструментов

Чтобы построить комплексную систему защиты для виртуализированной среды, основанной на VMware Workstation, потребуются несколько ключевых инструментов. Важно понимать, что нет "серебряной пули" в области безопасности виртуализации. Только с помощью нескольких инструментов, работающих вместе, можно построить действительно надежную защиту.

3.2.1 Антивирусное программное обеспечение

Среди первых слоев защиты для любой системы всегда следует рассматривать антивирусное программное обеспечение. Это может быть антивирус, такой как ClamAV, который является открытым источником и довольно надежен в обнаружении известных угроз. ClamAV способен обнаруживать вирусы,

трояны, вредоносное программное обеспечение и другие угрозы, используя свою обновляемую базу данных. Кроме того, он может быть легко интегрирован с почтовыми серверами для сканирования вложений электронной почты на наличие угроз. Однако, нужно учитывать, что антивирусы защищают в основном от уже известных угроз и менее эффективны против новых, еще не известных угроз.

3.2.2 Сканер уязвимостей

Сканер уязвимостей - это еще один важный инструмент в арсенале безопасности. Он используется для обнаружения и классификации уязвимостей в системах и приложениях. В этом контексте стоит отметить Flan Scan.

Flan Scan - это сканер уязвимостей с открытым исходным кодом, который использует Nmap и Vulners для поиска уязвимостей в сетевой инфраструктуре. Он был разработан таким образом, чтобы быть простым в использовании и эффективным, при этом обеспечивая детализированные отчеты о найденных уязвимостях. Flan Scan использует мощность Nmap для сканирования сетей и Vulners для классификации и обнаружения уязвимостей, что позволяет ему быстро и точно находить уязвимости в системе.

Важно отметить, что сканирование уязвимостей является реактивным мероприятием, то есть оно помогает обнаружить и устранить уязвимости, которые уже существуют в системе. В то же время, необходимы проактивные меры для предотвращения воздействия новых угроз и уязвимостей, которые могут появиться в будущем.

3.2.3 Система обнаружения и предотвращения вторжений (IDS/IPS)

Системы обнаружения и предотвращения вторжений (IDS/IPS) являются центральными элементами любой стратегии безопасности. Они обеспечивают непрерывное мониторинг и анализ сетевого трафика в поисках подозрительной активности или известных угроз. Если обнаруживается подозрительная активность, система IDS/IPS может предпринять соответствующие действия, которые могут включать в себя блокировку трафика, отправку уведомлений или автоматическую корректировку правил firewall.

Среди открытых систем IDS/IPS стоит отметить Suricata. Это мощная и гибкая система, которая может быть настроена для обнаружения широкого спектра угроз и аномалий. Suricata поддерживает обнаружение вторжений на основе сигнатур, а также на основе аномалий, и может быть интегрирован с другими инструментами безопасности для улучшения обнаружения и реагирования на угрозы.

Однако следует отметить, что, хотя системы IDS/IPS являются мощными инструментами, они не являются панацеей. Они могут помочь обнаружить и возможно предотвратить атаки, но они не заменяют необходимость в основательной стратегии безопасности, которая включает также защиту на уровне приложений и данных, управление доступом и регулярное тестирование на проникновение. Suricata, будучи мощным инструментом, также требует определенной экспертизы для эффективной настройки и управления.

3.2.4 Файрвол

Файрвол является одним из ключевых элементов системы защиты любой сети. Он контролирует входящий и исходящий трафик, блокирует нежелательные

соединения и защищает сеть от вредоносных активностей. Использование файрвола обязательно в любой комплексной системе безопасности.

Одним из важных инструментов в этой категории является pfSense. pfSense - это бесплатный и открытый файрвол и маршрутизатор, который предлагает множество возможностей для защиты вашей сети. pfSense поддерживает широкий спектр функций, включая NAT, VPN, балансировку нагрузки, обнаружение вторжений и предотвращение вторжений (IDS / IPS) и другие функции безопасности.

Одним из основных преимуществ pfSense является его гибкость и настраиваемость. Вы можете легко настроить его для удовлетворения своих уникальных требований безопасности, и есть множество плагинов и дополнений, которые позволяют расширить его функциональность.

Однако, несмотря на все его возможности, pfSense, как и любой другой файрвол, не может обеспечить абсолютную защиту. Он должен быть частью более обширной стратегии безопасности, включающей также антивирусную защиту, обнаружение и предотвращение вторжений, сканирование уязвимостей и другие меры защиты.

3.3 Итоговый набор

Итоговый подобранного системного обеспечения выглядит так:

- ClamAV - антивирусное программное обеспечение, которое обеспечивает защиту от вирусов, троянов и другого вредоносного ПО.
- Flan Scan - сканер уязвимостей, который обеспечивает обнаружение и классификацию уязвимостей в вашей системе и приложениях.

– Suricata - система обнаружения и предотвращения вторжений (IDS/IPS), которая анализирует сетевой трафик в реальном времени, чтобы обнаружить подозрительную или вредоносную активность.

– pfSense - это файрвол и маршрутизатор, который контролирует весь входящий и исходящий трафик в вашей сети, блокирует нежелательные соединения и защищает от угроз.

Вместе эти инструменты обеспечивают комплексную защиту, покрывая все ключевые области информационной безопасности. Однако важно правильно их настроить и обновлять.

4 Настройка системы комплексной защиты

Взяв во внимание все обозначенные ранее требования к системе и рассмотрев основные инструменты для обеспечения информационной безопасности, сформирован комплекс, состоящий из ClamAV, Flan Scan, ELK Stack, Suricata и pfSense. Каждый из этих инструментов имеет свою роль в обеспечении безопасности, и вместе они составляют эффективную и гибкую систему защиты.

Однако выбор подходящих инструментов - это только первый шаг на пути к созданию безопасной системы. Важно также грамотно настроить эти инструменты и обеспечить их взаимодействие, чтобы максимально использовать их потенциал и обеспечить наилучшую защиту.

Следующий этап – настройка выбранных инструментов. В этой главе рассмотрен процесс настройки каждого из инструментов, их взаимодействие и ключевые моменты, на которые стоит обратить внимание для обеспечения эффективной работы всей системы.

При настройке системы защиты важно соблюдать определенный порядок для обеспечения эффективности и гармоничного взаимодействия компонентов. Идеальный порядок настройки выбранных инструментов может быть следующим:

1. pfSense (Firewall): Самым первым шагом является настройка Firewall на основе pfSense. Это обеспечит основной уровень защиты, фильтруя входящий и исходящий трафик и блокируя потенциально вредоносные запросы. Функционал pfSense включает в себя не только файрвол, но и ряд других сетевых сервисов, что делает его отличной основой для дальнейшей настройки системы безопасности.

2. Suricata (IDS/IPS): После настройки файрвол следует установить и настроить систему обнаружения и предотвращения вторжений (IDS/IPS) Suricata. Этот инструмент будет непрерывно анализировать сетевой трафик, обнаруживать подозрительную активность и предпринимать соответствующие действия. Suricata также способна блокировать атаки на уровне сети, предотвращая их проникновение в локальную сеть.

3. Flan Scan (Сканер уязвимостей): Следующим шагом является установка и настройка сканера уязвимостей Flan Scan. Этот инструмент поможет обнаруживать уязвимости в вашей системе и приложениях, а также проверять наличие обновлений и патчей безопасности.

4. ClamAV (Антивирус): После настройки сканера уязвимостей следует установить и настроить антивирус ClamAV. Это будет основным инструментом для обнаружения и удаления вредоносного ПО.

Начиная с файрвол, обеспечивается базовая защита сети, затем добавляем слои обнаружения вторжений и антивирусной защиты. Сканер уязвимостей поможет установить дополнительные защитные меры, а система сбора логов позволит наблюдать за всей этой активностью, делая нашу систему безопасности полностью функциональной и эффективной.

Перейдем к поэтапной настройке средств.

4.1 PfSense

pfSense — это мощная система для файрвол и маршрутизации, которая устанавливается в качестве основного слоя защиты в виртуальной среде VMware. Она будет контролировать и защищать весь трафик, проходящий от виртуальных машин к гостевой операционной системе и гипервизору, и наоборот, обеспечивая эффективный фильтр безопасности.

Для начала установки pfSense, производится переход на страницу загрузки, изображенную на рисунке 10, и выбор подходящих параметров. Выбрана архитектура AMD64, которая подходит для всех современных компьютеров, и формат образа ISO для виртуальных машин. После заполнения формы и нажатия кнопки "DOWNLOAD", происходит скачивание файла.

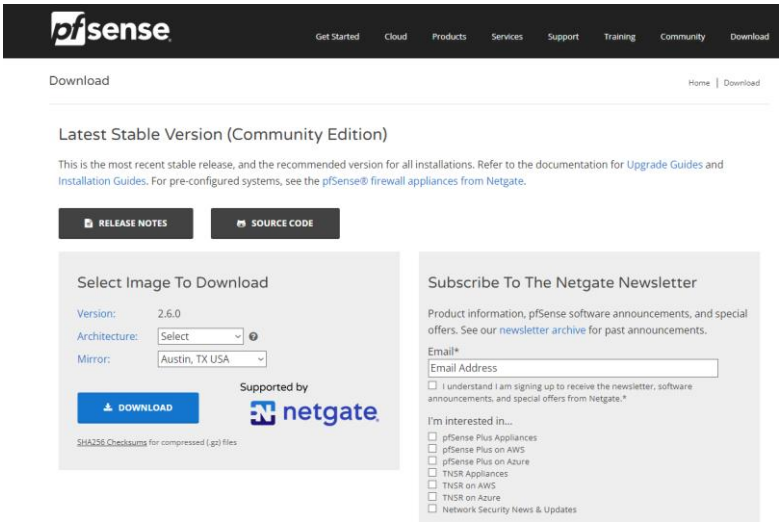

Рисунок 10 – Официальный сайт PfSense

После загрузки файла образ ISO монтируется к виртуальной машине в VMware. Затем, в настройках виртуальной машины выбирается загрузка с этого образа и запускается установщик.

Установщик приветствует сообщением о принятии лицензионного соглашения. После принятия соглашения, выбирается выполнение установки. Далее раскладка клавиатуры остается по умолчанию и выбирается автоматическая разбивка диска.

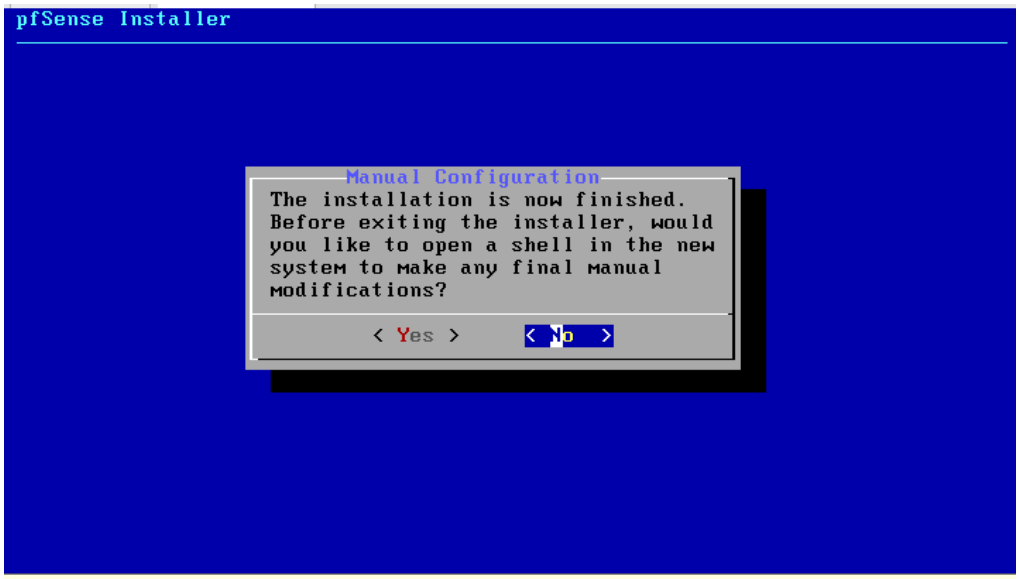

Рисунок 11 – Предложение модификации в конце установки

После завершения установки производится перезапуск системы, однако перед этим необходимо закрыть меню конфигурации показаное на рисунке 11.

Теперь pfSense установлена и готова к первоначальной настройке. В этом случае производится переход в веб-интерфейс pfSense по адресу 192.168.1.129 из подсети, используя браузер на локальном компьютере, где мы можем видеть страницу для доступа изображенную на рисунке 12.

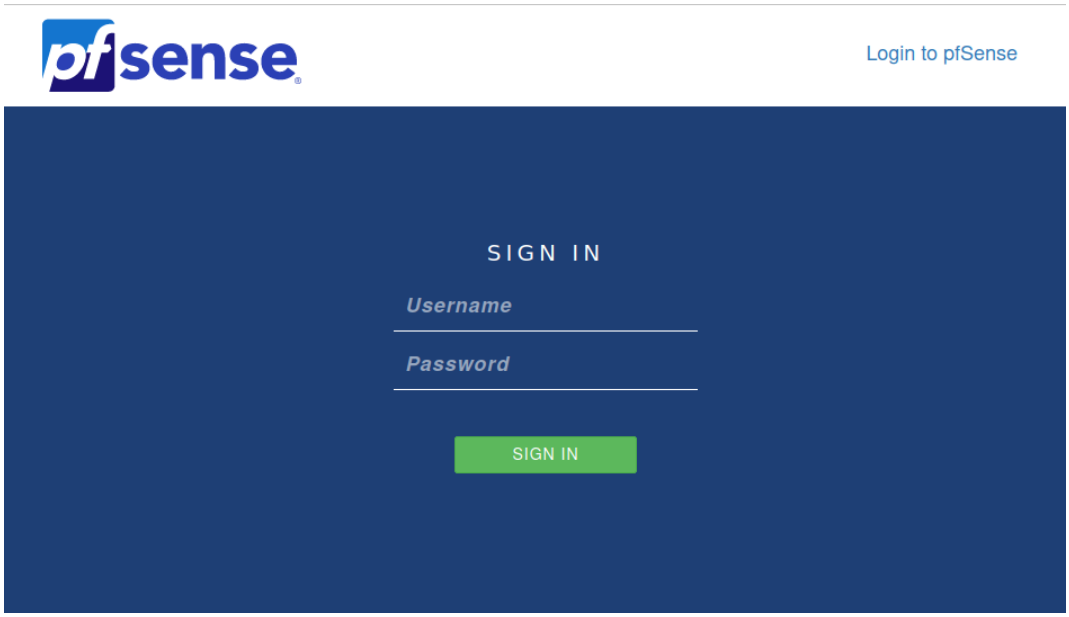

Рисунок 12 – Web сайт поднятого PfSense

Войдя в веб-интерфейс pfSense, для начала настройки используется имя пользователя и пароль по умолчанию (admin/pfsense) и начинается процесс конфигурации.

Сначала указывается имя и домен шлюза. В случае данной ВКР имя "firewall" и домен "company.lc". Далее задаются DNS-серверы; для этого примера используются серверы Яндекса (77.88.8.8 и 77.88.8.1). Данные настройки прописываются в специализированном разделе, он представлен на рисунке 13. Стандартно используются DNS-серверы google, однако для уверенности в доступности систем установлены сервера Яндекса.

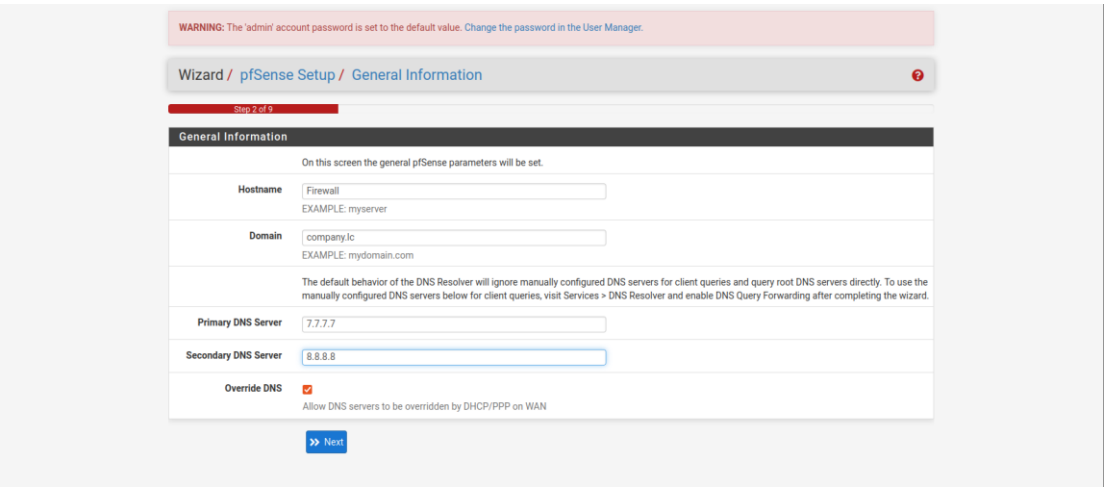

Рисунок 13 – Настройка основной конфигурации

Далее производится настройка PPPoE. В большинстве случаев не приходится вносить изменения на этом этапе, но, если провайдер требует специфические настройки PPPoE или определённый MAC-адрес, эти параметры указываются здесь.

Теперь настало время настройки внутреннего интерфейса. На данном этапе следует убедиться в правильной установке всех параметров внутреннего интерфейса.

На следующем шаге потребуется изменить пароль администратора. С целью обеспечения безопасности рекомендуется установить новый надежный пароль.

После внесения всех необходимых изменений следует применить настройки и перезагрузить систему. После перезагрузки, наша система будет готова для выполнения функций защиты и маршрутизации трафика в виртуальной среде.

После завершения базовых настроек и успешной перезагрузки системы, можно перейти к конфигурации сетевых интерфейсов виртуальных машин таким образом, чтобы весь их трафик проходил через виртуальный файрвол.

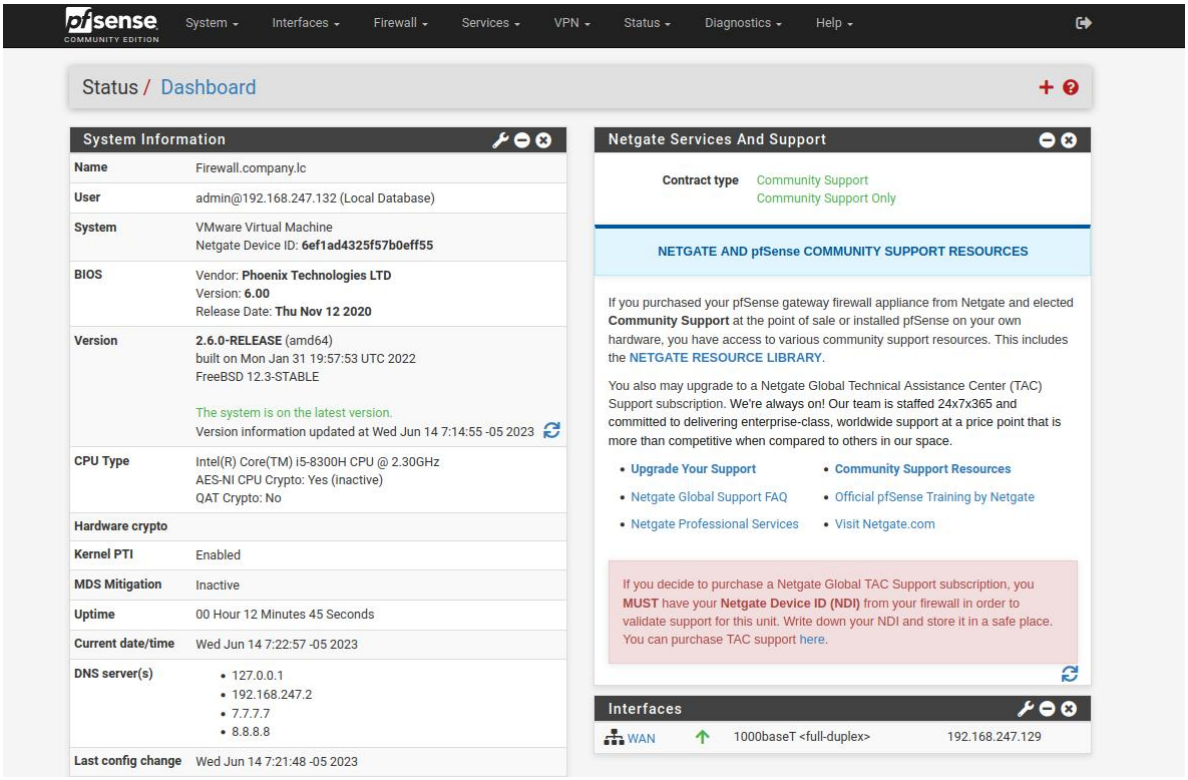

Рисунок 14 – Главная страница

Сначала должно быть убеждение, что каждая из виртуальных машин подключена к виртуальному сетевому интерфейсу pfSense. В интерфейсе управления VMware настраивается сетевое соединение на каждой виртуальной машине с виртуальным сетевым интерфейсом pfSense.

После этого происходит возвращение в веб-интерфейс pfSense и настройка правила для каждого из виртуальных сетевых интерфейсов, соответствующих виртуальным машинам. Это позволяет контролировать, какой трафик разрешен для прохождения через файрвол и обеспечивает защиту виртуальных машин.

Таким образом, pfSense настраивается для работы как центральный файрвол в виртуальном окружении, контролирующий все сетевые соединения и обеспечивающий безопасность среды. В конечном итоге мы можем наблюдать изменение основной информации на центральном дашборде системы показанном на рисунке 14.

4.2 Suricata

Suricata — это мощная система предотвращения и обнаружения вторжений, которая будет установлено на виртуальные машины и гостевую операционную систему. Это программа, которая не только находит потенциальные угрозы в сетевом трафике в реальном времени, но и может предпринять действия, чтобы защититься от них. Это может включать в себя блокировку подозрительного трафика, прекращение соединений или даже отправку предупреждений оператору.

Софт создан командой, которая ранее работала над системой предотвращения вторжений Snort, но внесла несколько улучшений. Одним из них является способность использовать графический процессор для ускорения обработки данных, что позволяет Suricata обрабатывать очень большие объемы трафика — до 10 гигабит в секунду, даже на стандартном оборудовании.

Когда Suricata начинает свою работу, она сначала направляет пакеты данных через программу управления сетью под названием iptables. Iptables отправляет эти пакеты в специальную очередь под названием NFQUEUE, где Suricata затем может просмотреть их и принять решение о том, что с ними делать. Если пакет выглядит подозрительно, Suricata может просто отбросить его, пропустить его, или даже отправить его обратно на начало очереди для дальнейшей обработки. Начиная с версии 1.4, Suricata также поддерживает так называемый "zero copy" режим в системе под названием AF_PACKET. Это позволяет ей работать еще быстрее, особенно когда она используется в системе, которая служит в качестве сетевого шлюза с двумя сетевыми интерфейсами. Если подозрительный пакет попадает под правило "DROP", он просто не пересылается на второй интерфейс, что сохраняет ресурсы и ускоряет процесс.

```
$ sudo add-apt-repository ppa:oisf/suricata-stable
$ sudo apt-get update
$ sudo apt-get install suricata
```

Рисунок 15 – Команды для установки suricata на Ubuntu

В ходе установки загружаются и устанавливаются последние версии правил Suricata и наборы правил ETOpen, команды запуска показаны на рисунке 15. Это обеспечивает постоянное обновление системы безопасности для отслеживания самых последних угроз.

Затем проводится настройка конфигурационного файла Suricata, suricata.yaml. В нем содержится большое количество параметров, многие из которых аналогичны тем, что используются в системе обнаружения вторжений Snort. Несмотря на схожесть, конфигурационный файл Suricata тщательно изучается и адаптируется под специфические потребности системы.

Основное внимание уделяется секции outputs файла suricata.yaml, которая отвечает за логирование событий. В ней настраиваются и активируются все необходимые варианты вывода. Важно отметить, что использование готовых примеров настроек из интернета не всегда приносит ожидаемый результат. Поэтому настройки тщательно адаптируются под конкретные потребности системы.

В конце, перед первым запуском Suricata, происходит проверка значений переменных, определенных в разделе vars конфигурационного файла. Это помогает гарантировать, что Suricata будет правильно взаимодействовать с сетевым трафиком в системе.

После успешной установки и базовой конфигурации Suricata, производится дальнейшая настройка системы.

Параметр host-mode задаётся в автоматический режим (auto), что позволяет Suricata определить оптимальный режим работы в зависимости от конфигурации и задач виртуальной машины. В некоторых случаях, может потребоваться

переключение в режим маршрутизатора (router) для работы Suricata в IPS-режиме AF_PACKET или в режим только для сниффинга (sniffer-only) для работы в IDS-режиме.

Для обеспечения эффективной работы Suricata, также устанавливается оптимальное значение default-packet-size, соответствующее MTU сети.

Следующим шагом является проверка и настройка подключенных правил. Все активные правила хранятся в директории /etc/suricata/rules. В этой директории удобно контролировать все используемые в системе правила и добавлять новые при необходимости.

Были применены следующие правила показанные на рисунке 16.

```
default-rule-path: @e_sysconfdir@rules
rule-files:
    - drop.rules
    - emerging-activex.rules
    - emerging-attack_response.rules
```

Рисунок 16 – Установка правил для suricata

Далее производится настройка контроля протоколов. В данном случае включена проверка протокола TLS на порту 443, настройки проиллюстрированы на рисунке 17.

```
app-layer:
    protocols:
            tls:
            enabled: yes
            detection-ports:
                dp: 443
```

Рисунок 17 – Настройка TLS

Следуя этим шагам, Suricata была настроена на защиту виртуальных машин и гостевой операционной системы, обеспечивая высокий уровень безопасности сетевого взаимодействия.

4.3 Flan Scan

Flan Scan - это легковесный инструмент для сканирования уязвимостей, основанный на открытом и легко настраиваемом сканере портов Nmap.

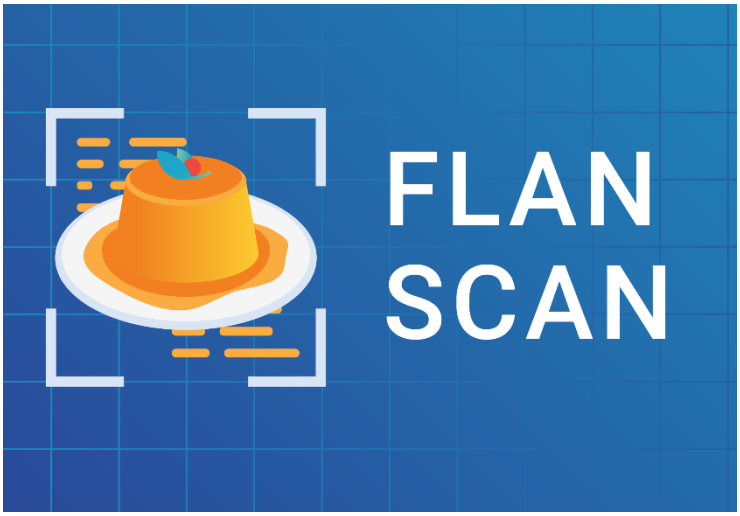

Рисунок 18 – логотип Flan Scan

Flan Scan запускает сканирование Nmap для обнаружения служб и сканирования уязвимостей, логотип компании изображен на рисунке 18. После обнаружения служб на открытых портах, Flan Scan преобразует структурированный XML-вывод Nmap в информативный отчет.

Отчеты Flan Scan структурированы по службам, перечисляя уязвимости и все соответствующие IP-адреса для каждой службы. Такой формат отчета делает его коротким и позволяет быстро идентифицировать службы, требующие внимания.

Для создания качественного отчета Flan Scan использует LaTeX, что обеспечивает хорошо отформатированные результаты. Полученный файл LaTeX можно легко преобразовать в красивый PDF с помощью инструментов, таких как pdf2latex или TeXShop.

Для начала настройки Flan Scan, выполняются следующие действия:

Клонируется репозиторий для установки на виртуальные машины посредством команды изображенной на рисунке 19.

```
$ git clone https://github.com/cloudflare/flan
```

Рисунок 19 – Клонирование flan scan

Эта команда клонирует репозиторий Flan Scan на компьютер.

Проверка установленного Docker происходит при выполнении команды изображенной на рисунке 20.

```
$ docker --version
```

Рисунок 20 – Команда проверки docker

Эта команда позволяет убедиться, Docker установлен и работает на наших системах. Если команда успешно выполняется, будет отображена информация о версии Docker.

В файл shared/ips.txt добавляется список IP-адресов или CIDR, которые требуется просканировать. Можно использовать любой текстовый редактор для внесения корректировок.

Сборка контейнера производится командой, показанной на рисунке 21.

```
$ make build
```

Рисунок 21 – Настройка сборки

Эта команда соберет контейнер для выполнения сканирования с помощью Flan Scan. В процессе сборки контейнера могут загружаться необходимые зависимости и пакеты.

Сканирование запускается при вводе команды изображенной на рисунке 22.

```
$ make start
```

Рисунок 22 – Команда для начала сканирования

Эта команда запускает сканирование с использованием Flan Scan. Он будет сканировать указанные IP-адреса и генерировать отчет о найденных уязвимостях.

Для получения отчета в формате html, выполняется следующая команда, показанная на рисунке 23.

Рисунок 23 – Создание html отчета

Эта команда генерирует отчет в формате HTML на основе результатов сканирования. Отчет будет доступен для просмотра и анализа.

Теперь настройка Flan Scan проведена успешно и может использоваться для сканирования уязвимостей на указанных IP-адресах.

4.4 ClamAV

ClamAV - это антивирус с открытым исходным кодом, который играет ключевую роль в обнаружении и предотвращении вирусов, вредоносных программ и вредоносного ПО. Открытый код позволяет проводить независимую проверку и аудит программы, обеспечивая прозрачность и доверие. Это особенно важно в контексте безопасности, поскольку сторонние эксперты и сообщество могут анализировать и улучшать программу, обнаруживая и устраняя уязвимости.

Установка ClamAV на все виртуальные машины в нашей системе, а также на гостевую операционную систему, позволит обеспечить надежную защиту от вирусов и вредоносных программ, поддерживая высокий уровень безопасности наших систем.

На рисунке 24 представлена команда для установки необходимого пакета.

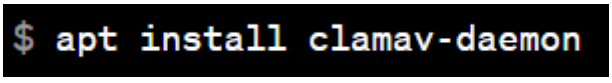

Рисунок 24 – Установка ClamAV

Установка пакета clamav-daemon, который включает в себя все необходимые компоненты ClamAV.

Для использования максимальных возможностей ClamAV, производится отказ от подключения точек монтирования и используются только директории. Для

этого открывается файл конфигурации ClamAV посредством команды с рисунка 25.

```
$ nano /etc/clamav/clamd.conf
```

Рисунок 25 – Редактирование конфигурации

В файле в секции настройки On Access Scanning и добавляются следующие опции, продемонстрированные на рисунке 26.

```
OnAccessMaxFileSize 5M
OnAccessIncludePath /samba/public
OnAccessExcludeUname clamav
OnAccessPrevention yes
OnAccessExtraScanning yes
```

Рисунок 26 – Настройка опций

Эти опции устанавливают максимальный размер файла для проверки на лету, указывают директорию для проверки, исключают пользователя clamav из проверки, включают блокировку файлов и более эффективное сканирование при создании, перемещении или переименовании файлов.

Создается служба ClamAV On Access Scanner с помощью юнита systemd. В файл вносятся корректировки, показанные на рисунке 27.

```
[Unit]
Description=ClamAV On Access Scanner
Requires=clamav-daemon.service
After=clamav-daemon.service syslog.target network.target

[Service]
Type=simple
User=root
ExecStart=/usr/sbin/clamonacc -F --fdpass --log=/var/log/clamav/clamav-onaccess.log --move=/samba/quarantine
Restart=on-failure
RestartSec=7s

[Install]
WantedBy=multi-user.target
```

Рисунок 27 – Конфигурация файла

Создаем файлы лога и карантина с помощью команд с рисунка 28.

```
$ touch /var/log/clamav/clamav-onaccess.log
$ mkdir /samba/quarantine
```

Рисунок 28 – Создание файлов

Запускается служба ClamAV On Access Scanner. Проверка, что служба успешно запущена и работает без ошибок, проходит без ошибок. Производится добавление службы ClamAV On Access Scanner в автозагрузку, чтобы она запускалась при каждом включении системы.

5 Анализ полученных результатов

Благодаря настройке и использованию компонентов системы комплексной защиты виртуализации, включая PfSense, Flan Scan, ClamAV и Suricata, был достигнут высокий уровень защищенности и обеспечена надежная защита от основных уязвимостей и атак.

Вся используемая в системе комплексной защиты виртуализации программа основана на открытом исходном коде. Это позволяет обеспечить прозрачность и независимость в проверке и аудите безопасности. Каждый из компонентов системы выполняет определенные функции и играет важную роль в обеспечении безопасности.

– Уязвимости гипервизора: при использовании VMware и правильной конфигурации минимизируются риски и обеспечивается безопасность гипервизора. Это включает в себя обновление и настройку гипервизора с использованием рекомендаций безопасности, установку соответствующих патчей и применение настроек безопасности для предотвращения возможных уязвимостей.

– Атаки на разделение (Escape Attacks): с помощью PfSense и соответствующей изоляции виртуальных машин предотвращаются возможные атаки на разделение и обеспечиваются безопасность каждой виртуальной машины. PfSense выполняет функцию межсетевого экрана (firewall), обеспечивая контроль доступа между виртуальными машинами и предотвращая несанкционированный доступ.

– Внутренние и внешние атаки: система комплексной защиты виртуализации с помощью своих компонентов, таких как PfSense, Flan Scan, ClamAV и Suricata, обеспечивает необходимый уровень контроля доступа и аутентификации, чтобы предотвратить и обнаружить внутренние и внешние атаки. PfSense выполняет функцию межсетевого экрана и контролирует доступ к виртуальным машинам и сетевым ресурсам. Flan Scan осуществляет сканирование

сети на предмет обнаружения уязвимостей. ClamAV обеспечивает защиту от вредоносных программ и вредоносных файлов. Suricata выполняет функцию системы обнаружения и предотвращения вторжений.

– Перехват сетевого трафика: с использованием соответствующих сетевых экранов и шифрования защищая сетевой трафик от перехвата или подмены, обеспечивая конфиденциальность и целостность данных. PfSense выполняет функцию межсетевого экрана и контролирует трафик между виртуальными машинами и сетевыми интерфейсами. Шифрование данных обеспечивает защиту от несанкционированного доступа и подмены информации.

– Вредоносное программное обеспечение (ВПО): система комплексной защиты виртуализации включает ClamAV и Suricata, обеспечивает эффективную защиту от вредоносного программного обеспечения и обнаружение подозрительной активности. ClamAV осуществляет сканирование файлов и обнаружение вредоносных программ, а Suricata предоставляет средства обнаружения и предотвращения вторжений.

Все эти компоненты работают в синергии, обеспечивая комплексную защиту виртуализированной среды и обнаружение потенциальных угроз безопасности.

Также используемые компоненты системы комплексной защиты виртуализации в среде соответствуют релевантным нормам и стандартам информационной безопасности. Давайте рассмотрим их соответствие некоторым нормативным актам:

– PfSense: этот компонент, выполняющий функцию межсетевого экрана, обеспечивает контроль доступа и аутентификации. Он соответствует требованиям Федерального закона №149-ФЗ "Об информации, информационных технологиях и о защите информации" относительно защиты информации и предотвращения несанкционированного доступа.

– Flan Scan: данный компонент предназначен для сканирования сети и обнаружения уязвимостей. Он помогает обеспечить соответствие требованиям

постановления Правительства РФ №1119 "Об утверждении требований к защите информации" в отношении обнаружения и устранения уязвимостей системы.

− ClamAV: компонент ClamAV, обеспечивающий защиту от вредоносного программного обеспечения, соответствует требованиям Федерального закона №149-ФЗ "Об информации, информационных технологиях и о защите информации" относительно обеспечения безопасности информации и предотвращения вредоносных программ.

− Suricata: данный компонент выполняет функцию системы обнаружения и предотвращения вторжений. Он соответствует требованиям Федерального закона №149-ФЗ "Об информации, информационных технологиях и о защите информации" в отношении обеспечения безопасности информации и предотвращения несанкционированного доступа.

Общая система комплексной защиты виртуализации, основанная на этих компонентах, соответствует также стандарту ГОСТ Р ИСО/МЭК 27001 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования". Этот стандарт определяет требования к системам менеджмента информационной безопасности, включая непрерывность бизнеса и оптимизацию инвестиций в безопасность.

Таким образом, вся система комплексной защиты виртуализации в vvсреде соответствует применимым нормативным актам и стандартам, обеспечивая надежную защиту информации и соответствуя требованиям законодательства Российской Федерации.

Заключение

В рамках выполнения данной выпускной квалификационной работы было проведено исследование и разработка комплексного решения для обеспечения безопасности систем виртуализации, использующих VMware Workstation. Защита систем виртуализации является актуальной и важной задачей, поскольку они играют ключевую роль в современной информационной инфраструктуре, обеспечивая гибкость, эффективность и экономию ресурсов в различных сферах деятельности.

Целью данной работы было разработать комплексное решение, которое способствовало бы обеспечению высокого уровня безопасности систем виртуализации. Данную цель можно считать достигнутой вследствие выполнения всех основных задач, части которых планомерно развивались в основных главах. Так, выделяя решение каждой из них, можно расписать следующие результаты:

1. В первой главе работы был проведен обзор современных методов и технологий защиты систем виртуализации. Была изучена архитектура систем виртуализации, включая основные компоненты и механизмы работы. Далее был осуществлен анализ уязвимостей, характерных для систем виртуализации, и рассмотрены методы их эксплуатации. Это включало изучение атак, таких как внедрение вредоносного кода, обход изоляции и компрометацию виртуальных машин.

2. Во второй главе работы было проведено изучение нормативно-правовой базы, регулирующей использование систем виртуализации в России. Были рассмотрены основные законодательные акты и правовые нормы, которые оказывают влияние на обеспечение безопасности систем виртуализации. Важными аспектами изучения были правила и требования, касающиеся обработки персональных данных, защиты информации, обеспечения конфиденциальности и доступности данных.

3. В третьей главе работы был проведен глубокий анализ существующих решений и методов защиты систем виртуализации, основанных на использовании VMware Workstation. Были рассмотрены различные инструменты и технологии, предназначенные для защиты виртуальных сред. Был проведен анализ их возможностей, преимуществ и ограничений с целью определения наиболее подходящих инструментов для комплексной защиты систем виртуализации.

4. Четвертая глава работы была посвящена разработке комплексного решения для обеспечения высокого уровня безопасности систем виртуализации, использующих VMware Workstation. На основе проведенного анализа были выбраны соответствующие инструменты и компоненты. В рамках разработки решения была осуществлена настройка PFSENSE, межсетевого экрана с широкими возможностями, для обеспечения контроля над сетевым трафиком виртуальной среды. Далее был использован SURICATA, система обнаружения вторжений, для обеспечения раннего обнаружения и предотвращения атак. Также в состав решения были включены FLAN SCAN, сканер уязвимостей, для регулярного сканирования виртуальных машин на предмет наличия уязвимостей, и CLAMAV, антивирусная программа, для обнаружения и блокировки вредоносных программ. Все компоненты решения были настроены и интегрированы для обеспечения совместной работы и максимальной эффективности в области защиты систем виртуализации.

5. В заключительной главе работы был проведен анализ полученных результатов и оценка эффективности разработанного комплексного решения. Было проведено сопоставление разработанного решения с анализом уязвимостей и существующими решениями, представленными в предыдущих главах. В результате этого сопоставления было подтверждено, что разработанное решение позволяет эффективно устранять уязвимости и обеспечивать безопасность систем виртуализации, использующих VMware Workstation. Полученные результаты свидетельствуют о значительном прогрессе в области защиты систем

виртуализации и подтверждают целесообразность использования разработанного комплексного решения.

В итоге данная работа позволила достичь поставленных целей, а именно изучение методов и технологий защиты систем виртуализации, анализ уязвимостей и методов их эксплуатации, изучение существующих решений, разработку комплексного решения и анализ полученных результатов. Разработанное решение представляет собой важный шаг в области обеспечения безопасности систем виртуализации и может быть использовано в реальных средах для повышения уровня защиты и минимизации рисков эксплуатации уязвимостей.

.

СПИСОК ЛИТЕРАТУРЫ

1 ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения»

2 Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

3 Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

4 ГОСТ Р ИСО/МЭК 27001 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

5 Clamav [Электронный ресурс] URL: https://clamav.ru/downloads.html (дата обращения 21.05.2023)

6 Deep security [Электронный ресурс] URL: https://www.trendmicro.com/ru_ru/business/products/hybrid-cloud/deep-security.html (дата обращения 21.05.2023)

7 flan scan [Электронный ресурс] URL: https://github.com/cloudflare/flan (дата обращения 21.05.2023)

8 How To Install Suricata on Ubuntu 20.04 [Электронный ресурс] URL: https://www.digitalocean.com/community/tutorials/how-to-install-suricata-on-ubuntu-20-04 (дата обращения 21.05.2023)

9 Introducing Flan Scan: Cloudflare’s Lightweight Network Vulnerability Scanner [Электронный ресурс] URL: https://blog.cloudflare.com/introducing-flan-scan/ (дата обращения 23.05.2023)

10 Nutanix Flow [Электронный ресурс] URL: https://cbs.ru/lib/faq/nutanix/nutanix-flow/ (дата обращения 25.05.2023)

11 Pfsense [Электронный ресурс] URL: https://www.pfsense.org (дата обращения 26.05.2023)

12 Suricata [Электронный ресурс] URL: https://suricata.io (дата обращения 27.05.2023)

13 Suricata как IPS [Электронный ресурс] URL: https://habr.com/ru/articles/192884/ (дата обращения 29.05.2023)

14 VMware NSX Documentation [Электронный ресурс] URL: https://docs.vmware.com/en/VMware-NSX/index.html (дата обращения 30.05.2023)

15 Антивирус для Linux – ClamAV [Электронный ресурс] URL: https://habr.com/ru/articles/654541/ (дата обращения 18.05.2023)

16 Архитектура виртуальных машин [Электронный ресурс] URL: https://www.osp.ru/os/2005/05-06/185586 (дата обращения 01.06.2023)

17 Безопасность Виртуализации. Часть 1 [Электронный ресурс] URL: https://habr.com/ru/articles/243845/ (дата обращения 04.06.2023)

18 Обзор Check Point CloudGuard SaaS, средства защиты облачных сервисов [Электронный ресурс] URL: https://www.anti-malware.ru/reviews/Check-Point-CloudGuard-SaaS (дата обращения 01.06.2023)

19 Угрозы ИБ систем виртуализации и современные средства защиты [Электронный ресурс] URL: http://information-security.ru/articles2/Oborandteh/ugrozy-ib-sistem-virtualizatsii-i-sovremennye-sredstva-zaschity (дата обращения 18.05.2023)

20 Установка и настройка pfSense [Электронный ресурс] URL: https://selectel.ru/blog/tutorials/how-to-install-and-configure-pfsense/ (дата обращения 01.06.2023)