

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ
КАЗАХСТАН

Казахский национальный исследовательский технический университет
имени К.И.Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра “Кибербезопасность, обработка и хранения информации”

Тазабеков Шамиль Алмасович

Мониторинг безопасности сети на основе тестирования на проникновение

ДИПЛОМНЫЙ ПРОЕКТ

Специальность 5В100200 – Системы информационной безопасности

Алматы 2019

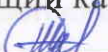
КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ имени К.И. САТПАЕВА

СЭТБАЕВ
УНИВЕРСИТЕТИ



ИНСТИТУТ ИНФОРМАЦИОННЫХ И
ТЕЛЕКОММУНИКАЦИОННЫХ
ТЕХНОЛОГИЙ

КАФЕДРА КИБЕРБЕЗОПАСНОСТЬ,
ОБРАБОТКА И ХРАНЕНИЕ ИНФОРМАЦИИ

«Допущен к защите»
Заведующий кафедрой КБОиХИ
 Н.А. Сейлова

ДИПЛОМНЫЙ ПРОЕКТ

на тему: «МОНИТОРИНГ БЕЗОПАСНОСТИ СЕТИ НА ОСНОВЕ
ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ»

по образовательной программе 5В100200 – «Системы информационной
безопасности»

Выполнил выпускник

Тазабеков Ш.А.

Научный руководитель

к.т.н., ассоц. проф. Айтхожаева Е.Ж.

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени
К.И.Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра "Кибербезопасность, обработка и хранения информации"

5В100200 - Системы информационной безопасности

УТВЕРЖДАЮ

Заведующий кафедрой
Кибербезопасность, обработка и
хранение информации
канд.техн.наук, ассист. профессор
Сейлова Н.А.

" 14 " 05 2019 г.

ЗАДАНИЕ

на выполнение дипломного проекта

Обучающемуся Тазабекову Шамилю Алмасовичу

Тема: Мониторинг безопасности сети на основе тестирования на проникновение

Утверждена приказом руководителя университета №1162-б от 16.10.2018г.

Срок сдачи законченного проекта: « ___ » _____ 2019 г.

Исходные данные к дипломному проекту: Выявление уязвимостей при помощи мониторинга безопасности с использованием сетевых сканеров. Анализ инцидентов безопасности осуществляется с помощью SIEM-системы.

Перечень подлежащих разработке в дипломном проекте вопросов: а) безопасность информационных процессов; б) тестирование на проникновение; в) мониторинг информационных структур предприятия.

Перечень графического материала (с точным указанием обязательных чертежей): тестирование на проникновение – 1А3; функциональные возможности SIEM-системы – 1А3; сканирование сетевыми сканерами - 1А3; анализ инцидентов с помощью SIEM-системы - 1А3.

Рекомендуемая основная литература: состоит из 11 наименований.


ГРАФИК

подготовки дипломного проекта

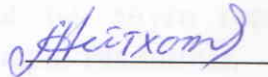
Наименования разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Безопасность информационных процессов	20.02.19	вып
Тестирование на проникновение	15.03.19	вып
Мониторинг информационных структур предприятия	30.04.19	вып

Подписи

консультантов и нормоконтролера на законченный дипломный проект с указанием относящихся к ним разделов проекта

Наименования разделов	Консультанты, И.О.Ф. (уч. степень, звание)	Дата подписания	Подпись
Нормоконтролер	А.А Зиро, магистр технических наук, лектор	13.05.2019	

Научный руководитель



Е.Ж.Айтхожаева

Задание принял к исполнению обучающийся



Ш.А.Тазабеков

Дата

«14» 01 2019 г.

ОТЗЫВ

НАУЧНОГО РУКОВОДИТЕЛЯ

на

дипломный проект

(наименование вида работы)

Тазабекова Ш.А.

(Ф.И.О. обучающегося)

5В100200 - Системы информационной безопасности

(шифр и наименование специальности)

Тема:

«Мониторинг безопасности сети на основе тестирования на проникновение»

Внедрение ИТ технологий, несмотря на их достоинства и преимущества, сдерживается наличием рисков и угроз безопасности информации. Одним из таких рисков является нарушение информационной безопасности предприятия посредством сетевых атак через общедоступную глобальную сеть.

В работе студента Тазабекова Ш.А. «Мониторинг безопасности сети на основе тестирования на проникновение» рассматривается анализ сетевых угроз и их источников, классификация сетевых атак, анализ инструментов тестирования на проникновение, их классификация.

В дипломном проекте выполняется также обзор методов защиты сетевых ресурсов и программного обеспечения (ПО), обеспечивающего мониторинг и выявление инцидентов, рассматриваются принципы их функционирования и функциональные возможности.

В практической части дипломного проекта выполнено моделирование сетевых атак и рассмотрено их выявление с проведением анализа на основе SIEM-системы и сетевого сканера. SIEM-решения в настоящее время являются одной из основных технологий, обеспечивающих получение аналитики в SOC (Security Operation Center – центр мониторинга и реагирования на инциденты безопасности).

Тазабеков Ш.А. показал хорошие теоретические и практические навыки в области информационной безопасности, проявил инициативу и самостоятельность при решении задач дипломного проектирования, умение работать с инструментами пентеста, инструментом анализа инцидентов (SIEM-системой), умение работать с технической литературой.

Дипломный проект на тему «Мониторинг безопасности сети на основе тестирования на проникновение» выполнен Тазабековым Ш.А. на хорошем уровне и может быть допущен к защите.

Научный руководитель

ассоц.профессор, к.т.н.

(должность, ученая степень, звание)

 Айтхожаева Е.Ж.

(подпись)

« 8 » 05 2019 г.

РЕЦЕНЗИЯ

на _____ дипломный проект _____
(наименование вида работы)

Тазабекова Ш.А.
(Ф.И.О. обучающегося)

5B100200
(шифр и наименование специальности)

На тему: «Мониторинг безопасности сети на основе тестирования на проникновение»

Выполнено:

- а) графическая часть на 4 листах
б) пояснительная записка на 48 страницах

ЗАМЕЧАНИЯ К РАБОТЕ

Актуальность темы не вызывает сомнений в связи с цифровой трансформацией общества и, связанным с этим, увеличением количества и типа инцидентов информационной безопасности. Выявление и анализ сетевых атак, представляющих угрозу информационным ресурсам, является обязательным условием безопасного функционирования предприятия и обязательной функцией системы информационной безопасности предприятия.

Представленная работа оформлена аккуратно, хорошо структурирована: представленный материал разбит по главам, имеются оглавление, введение, заключение, список литературы, приложение.

В работе проведен обзор источников сетевых угроз и самих угроз, каналов утечки информации, защитного ПО от сетевых угроз. Выполняется анализ инструментов тестирования на проникновение, рассматриваются этапы и типы тестирования на проникновение (особое внимание уделяется сканерам уязвимостей), функции и задачи SIEM-систем.

Работа имеет практическую направленность. Были использованы возможности SIEM-системы для анализа инцидентов безопасности, которые возникли в результате моделирования сетевых атак, выполненное с помощью утилит Kali Linux.

Для обнаружения открытых портов на рабочих станциях использовался сканер Nmap. Для выявления уязвимостей по найденным IP-адресам использовался сканер уязвимости сети – OpenVas.

Приложения содержат графическую часть, отражают содержание дипломного проекта.

Пояснительная записка к дипломному проекту и графическая часть выполнены в соответствии с требованиями стандарта КазННТУ им. К.И.Сатпаева.

Оценка работы

Рецензируемый дипломный проект выполнен на актуальную тему и удовлетворяет требованиям, предъявляемым к дипломным проектам. Дипломный проект демонстрирует знание дипломником инструментов моделирования атак, систем анализа инцидентов – SIEM системы и умения пользоваться ими на практике.

Считаю, что дипломный проект Тазабекова Ш.А. на тему: «Мониторинг безопасности сети на основе тестирования на проникновение» заслуживает оценки отлично (А), а Тазабеков Ш.А. – присвоения академической степени бакалавра по специальности 5В100200 – Системы информационной безопасности.

Рецензент

Канд.Тех.Наук, Академик МАИН

профессор каф. СИБ АУЭС.

(должность, ученая степень, звание)

 Тынымбаев С.Т.

(подпись)

« 05 » 2019 г.

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Тазабеков Шамиль

Название: Мониторинг сетевых угроз на основе тестирования на проникновение

Координатор: Евгения Айтхожаева

Коэффициент подобия 1:25,9

Коэффициент подобия 2:15,1

Тревога:4

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

- обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;
- обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
- обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

Заимствования являются добросовестными

Дата 14.05.19 2

Подпись заведующего кафедрой /

начальника структурного подразделения

КБДекл

Окончательное решение в отношении допуска к защите, включая обоснование:

Допускается к защите

Дата 14.05.09

Подпись заведующего кафедрой

начальника структурного подразделения


И.В. Делли

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Тазабеков Шамиль

Название: Мониторинг сетевых угроз на основе тестирования на проникновение

Координатор: Евгения Айтхожаева

Коэффициент подобия 1: 25,9

Коэффициент подобия 2: 15,1

Тревога: 4

После анализа Отчета подобия констатирую следующее:

- обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;
- обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
- обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

Обнаруженное замещение явля-
ется добросовестным. Используется
единица термической обработки
и, а также название программных
продуктов.

8.05.19

Дата

Ветхот

Подпись Научного руководителя

АННОТАЦИЯ

Данная работа посвящена мониторингу сетевых угроз на основе тестирования на проникновение. Выполнено выявление различных сетевых угроз с помощью мониторинга сетевых ресурсов предприятия.

Проведен анализ сетевых угроз и их источников, рассмотрена классификация сетевых атак, выполнен обзор инструментов тестирования на проникновение, проанализированы функции SIEM-системы.

Выполнено моделирование сетевых атак (переполнение буфера, дешифрование SSL/TSL сертификатов, человек-посередине и другие) с помощью утилит Kali Linux (Nmap, OpenVas), выполнен анализ инцидентов безопасности с использованием SIEM-системы.

Для устранения уязвимостей предложены определенные методы защиты.

АНДАТПА

Бұл дипломдық жұмыс еруге тестілеу негізінде желілік қауіп-қатерлердің мониторингіне арналған. Кәсіпорынның желілік ресурстарының мониторингі арқылы түрлі желілік қатерлерді анықтау орындалды.

Желілік қатерлер мен олардың көздеріне талдау жүргізілді, желілік шабуылдардың жіктелуі қарастырылды, еруге тестілеу құралдарына шолу жасалды, SIEM-жүйесінің функциялары талданды.

Желілік шабуылдарды модельдеу (буферді толтыру, SSL/TLS сертификаттарды шифрлеу, адам-ортасында және басқалар) Kali Linux утилитасы (Nmap, OpenVas) көмегімен орындалды, SIEM-жүйені пайдалану арқылы қауіпсіздік инциденттерін талдау жасалды.

Осалдықтарды жою үшін белгілі бір қорғаныс әдістері ұсынылды.

ANNOTATION

This project is devoted to monitoring of network threats on the basis of penetration testing. Identification of various network threats by means of monitoring of network resources of the enterprise is executed.

The analysis of network threats and their sources is carried out, classification of network attacks is considered, the review of tools of testing on penetration is executed, functions of SIEM-system are analyzed.

Modeling of network attacks (buffer overflow, SSL/TLS certificate encryption, man-in-the-middle and others) with the help of Kali Linux utilities (Nmap, OpenVas) was performed, analysis of security incidents using SIEM system was performed.

Certain methods of protection are proposed to eliminate vulnerabilities.

СОДЕРЖАНИЕ

Введение	6
1. Безопасность информационных процессов	7
1.1 Анализ сетевых угроз	7
1.2 Сетевые атаки и их классификация	9
2. Тестирование на проникновение	13
2.1 Анализ инструментов тестирования на проникновение	14
2.2 Методы защиты информации	15
3. Мониторинг информационных структур предприятия	17
3.1 Мониторинг и сетевые сканеры	17
3.2 SIEM-системы	18
3.3 Мониторинг безопасности сети на основе сетевых сканеров	23
3.4 Анализ инцидентов безопасности посредством SIEM-системы	27
Заключение	33
Список использованной литературы	34
Приложение А	35
Приложение Б	47

ВВЕДЕНИЕ

С началом внедрения информационных технологий, нынешний мир намного проник к новейшим благам в сфере IT-технологий, что порой не представить общество без наличия различных гаджетов в жизни человека. Благодаря этому, производительность труда увеличились в несколько раз, что позволило людям жить комфортнее и проще.

С появлением глобальной сети – интернет, участились случаи хищения конфиденциальной информации, различных организаций по сетевым каналам, что послужило причиной возникновения такой области IT, как информационная безопасность(ИБ).

Целью ИБ является соблюдение трех основных принципов – целостности, конфиденциальности и доступности информации.

Роль человеческого фактора не способна полностью выявить инциденты ИБ в реальном времени. Для исправления данной проблемы создаются комплексы быстрой диагностики, вырабатывающие оповещения об инцидентах в режиме онлайн и подробную информацию о них.

Важность в использовании мониторинга состоит в: сборе, регистрации, хранении, обработке оповещений, выявлении инцидентов и обеспечение своевременного реагирования на них. При отсутствии мониторинга было бы невозможно выявлять большую часть оповещений, требующих немедленного обеспечения безопасности информационных ресурсов.

Актуальность данной дипломной работы заключается в выявлении различных сетевых угроз с помощью мониторинга сетевых ресурсов, с целью сбора инцидентов и последующее обеспечение информационной безопасности организаций.

Целью дипломного проекта является мониторинг безопасности сети на основе тестирования на проникновение, выявление инцидентов ИБ с использованием современных систем.

Задачами дипломного проекта являются анализ сетевых угроз и их источников, классификация сетевых атак, анализ инструментов тестирования на проникновение, их классификация.

Будет выполнен обзор методов защиты сетевых ресурсов и программного обеспечения (ПО), обеспечивающего мониторинг и выявление инцидентов ИБ, рассмотрены принципы их функционирования и функциональные возможности.

В практической части дипломного проекта будет выполнено выявление уязвимостей с помощью сетевых сканеров путем тестирования сети и рассмотрено выявление инцидентов безопасности с проведением анализа на основе SIEM-системы.

1 Безопасность информационных процессов

Информация является важнейшим объектом передачи, хранения и использования, а также ее преобразования. В свою очередь информационные технологии помогают связывать все информационные ресурсы, которые в данный момент являются значительным фактором его развития. Тем самым, можно утвердить то, что информационные ресурсы позволяют сэкономить на социальном времени, оборудования, сырья и временами людскими ресурсами. Общепринятое развитие человечества в сторону оптимизации информационных процессов, результатами труда которого становятся ценности не материального характера, а сама информация. Важнейшими типами наиболее труднейших производственных, также и социальных процедур являются информационные процессы. Сами процессы, как правило, предпринимают в наибольшей степени важные функции этих технологий. Играя существенную роль в поддержании взаимодействия между людьми, таких как в средствах массовой информации используют различного рода телекоммуникаций (электронная почта, социальные сети, мессенджеры и т.д.). Из-за огромного потока информации возрастает риск ее утечки. Тем самым возникают угрозы безопасности.

1.1 Анализ сетевых угроз

В настоящее время многие компании в своей работе сталкиваются с вопросами информационной безопасности, а именно информационными угрозами.

Процессы или события, наносящие ущерб компьютерным системам, называют угрозами информационной безопасности. Эти угрозы имеют как внутренние, так и внешние источники [1].

Информационными угрозами могут являться:

- воздействия хакеров и вредоносных программ;
- умышленные внутренние вредители, инсайдеры;
- халатность со стороны сотрудников компании;
- форс-мажорные обстоятельства, такие как: пожары, аварии в энергосистемах и др.

Выделим основные цели атаки на информационные системы компании:

- овладение ценными ресурсами, например, кража финансовой информации или контроль доступа за вычислительными ресурсами внутренней сети компании;
- заказ недобросовестных конкурентов с целью ограничения деятельности компании, сбоя в работе информационной системы, нарушения связей с корпоративными клиентами и партнерами.

Различают два типа угроз безопасности: естественные и искусственные. К естественным угрозам относятся природные явления, не зависящие от человека, такие как: ураганы, пожары и другие стихийные

бедствия. А искусственные зависят от участия человека и бывают преднамеренными и непреднамеренными.

Непреднамеренные угрозы появляются из-за невнимательности и несоблюдения сотрудниками внутренних требований компании, что не освобождает их от ответственности.

Преднамеренные угрозы создаются специально. К ним относят атаки злоумышленников (хакеров) как извне, так и внутри компании. Успешная атака поможет злоумышленникам завладеть конфиденциальной информацией и личными данными компании (денежные средства, ценные бумаги и т.д.).

Обнаружить проведение удаленной атаки не так-то просто. Трудность заключается в несвоевременном выявлении таких атак. В результате чего, у хакеров увеличиваются шансы проведения успешной атаки.

Безопасность локальной сети отличается от безопасности межсетевого взаимодействия тем, что на первое место выходят нарушения зарегистрированных пользователей, так как в основном каналы передачи данных локальной сети находятся в контролируемой зоне.

Сетевые атаки поступают из различных источников угроз. К таким источникам относят:

- нежелательный контент;
- несанкционированный доступ;
- утечка информации;
- потеря данных;
- мошенничество;
- кибервойны и кибертерроризм.

Одним из наиболее популярных источников является нежелательный контент. Нежелательный контент охватывает потенциальные программы вредоносного характера и спам, основанные на уничтожение и кражу информации. Также различные сайты, нежелательного характера, которые не соответствуют возрасту того, кто их использует.

Использование несанкционированных программ приводит к нарушению прав доступа к любой важной информации компании. Утечки данного типа могут осуществляться различными способами, например, через атаки на сайты, перехват данных по сети, через сниффер пакетов.

Потеря данных – повреждение или утрата информации в результате различных факторов. При этом информация может быть удалена или повреждена в результате ряда случайных или намеренных действий. Потерять данные можно во время работы с ними, а также при хранении информации на компьютере, сервере или на массивах RAID. Потеря данных может происходить в результате нарушения целостности информации (сбой программного обеспечения) и неисправности оборудования. Нарушение целостности информации означает повреждение данных, в результате которого невозможно прочитать/скопировать информацию без выполнения процедуры восстановления. При нарушении целостности возникает риск

потери всех и части данных, а также угроза работы всей компьютерной системы.

Утечки конфиденциальной информации можно разделить на две большие группы: злонамеренное похищение (включая инсайдерские риски) и утечки по неосторожности или оплошности персонала. Практика показывает, что абсолютное большинство случаев утечки конфиденциальной информации является результатом ошибок сотрудников при работе с данными. Это не значит, что инсайдерскую угрозу и промышленный шпионаж можно не рассматривать, так как доля таких происшествий очень низкая. Если говорить о конкретных каналах утечки информации, то наиболее актуальными за последние несколько лет можно назвать следующее:

- потеря незащищённого носителя данных (флешка, внешний жёсткий диск, карта памяти, диски);
- случайное инфицирование рабочей станции программами-шпионами (через незащищённый доступ в Интернет или при подключении заражённых USB-устройств);
- технические ошибки при обработке конфиденциальной информации и публикации её в сети Интернет;
- отсутствие ограничения доступа сотрудников к конфиденциальным данным;
- кибератаки на хранилища данных (хакерские атаки, злонамеренное заражение вирусами, червями и т.п.).

Серьёзной информационной угрозой можно считать фрод, то есть мошенничество при помощи информационных технологий. К данной угрозе относятся и действия по кредитной карте, и взлом онлайн-банка, и собственно внутренний фрод. Целью таких угроз является не соблюдение норм законодательства и внутренних нормативных актов компании.

В современное время угрозы происходят часто и никого этим не удивить. Известно, что такие атаки не выполняются без предварительной разведки, в этом смысл кибершпионажа.

Чтобы подробно разобраться как бороться с вышеуказанными угрозами, рассмотрим сетевые атаки и их классификации.

1.2 Сетевые атаки и их классификации

Сетевая атака - это действие, целью которого является захват контроля (повышение прав) над удалённой/локальной вычислительной системой (ВС).

Выделим следующие популярные атаки:

- переполнение буфера;
- вредоносные программы (вирусы, почтовые червы, трояны, руткиты);
- IP-спуфинг;
- атака «maninthemiddle» человек по середине;
- SQL-инъекция;

- межсайтовый скриптинг;
- отказ в обслуживании;
- подслушивание;
- перехват;
- фишинг.

Переполнение буфера происходит, когда выполняется запись или чтение данных большего объема, чем объем буфера. При этом происходит аварийное завершение или зависание программы. Если программное обеспечение работает на компьютере администратора, то через него злоумышленник получает полный контроль над всеми устройствами, управляемыми администратором.

К вредоносным программам относят любое программное обеспечение, которое не санкционировано проникает в компьютерную технику. Задача таких продуктов заключается в нарушении работы компьютера, хищению личных данных и т.д.

Вирусы — программы, которые могут добавлять вредоносный код в программы, установленные на вашем компьютере. Этот процесс называется заражением.

Основная цель вируса — распространение. В процессе распространения вирусы могут удалить файлы и даже операционную систему, испортить структуру размещения данных, заблокировать работу пользователей.

Троянями называют программы, которые выполняют несанкционированные действия пользователем. Они уничтожают информацию на дисках, приводят систему к зависанию, воруют конфиденциальную информацию. Данный класс вредоносных программ не является вирусом, которые заражают другие программы. Троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом «полезного» программного обеспечения. При этом наносимый ими вред во много раз превышает потери, чем от вируса.

Черви — это вредоносные программы, которые распространяются через сетевые ресурсы. Название этого класса было дано исходя из способности червей «переползать» с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Черви обладают очень высокой скоростью распространения. Они проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Также они могут использовать данные адресной книги почтовых клиентов.

IP-спуфинг возникает, когда злоумышленник выдает себя за легального пользователя. Он использует IP-адрес, находящийся в одной подсети организации или разрешенный внешний IP-адрес, доступный лишь некоторым сетевым ресурсам.

Кроме использования IP-спуфинга для получения логина и пароля, часто принимают способ перебирания паролей (брутфорс). Результатом

является получение прав пользователя компании. При их получении, злоумышленник способен для себя создать пути будущего доступа, даже если атакованный пользователь изменит свой логин и пароль.

Атакитипа«человек-в-середине». Для реализации атаки требуется получить доступ к сетевым пакетам. Доступ к этим пакетам имеет сотрудник провайдера, по которому передаются все сетевые пакеты. Для этого типа атак используют обычно снифферы пакетов, а также протоколы маршрутизации. Применяются для перехвата сессии к частным ресурсам, происходит анализ трафика сети и последующего внедрения атак типа отказа в обслуживании.

Отказ в обслуживании – это атака, заставляющая не отвечать сервер на текущие запросы. Отличием данной атаки является не кража информации, а остановка работы сервисов компании. Исполнение атаки проводится исключительно из одной рабочей станции, чем отличается от распределенной атаки отказа в обслуживании - DDoS.

DDoS – это атака, похожая на атаку отказа в обслуживании, но выполняется сразу с нескольких рабочих станций. Существуют процессы, где DoS может быть не эффективен. Тем самым используется DDoS, где несколько компьютеров объединившись, производят DoS атаку на компьютер сотрудника компании, его жертву.

Атаки типа SQL-инъекции изменяются параметры SQL запросов к базе данных путем добавления специального кода. В итоге запрос имеет иной характер. При недостаточной фильтрации данных, она способна привести к нарушению целостности информации, например, удалить данные или подтвердить их к изменениям.

Подслушивание. По большей части данные передаются по компьютерным сетям в незащищенном формате (открытым текстом), что позволяет злоумышленнику, получившему доступ к линиям передачи данных в сети, подслушивать или считывать трафик. Для подслушивания в компьютерных сетях используют сниффер. Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту, перехватывающую все сетевые пакеты, передающиеся через определенный домен. С помощью данной атаки можно получить имя пользователя и соответствующий пароль.

В настоящее время снифферы работают согласно законам. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые протоколы передают данные в текстовом формате (Telnet, RTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли). Предотвратить угрозу сниффинга можно с помощью применения аутентификации однократных паролей; установки аппаратных или программных средств, распознающих снифферы; применения криптографической защиты каналов связи.

Перехват. В отличие от подслушивания, перехват - это активная атака. Злоумышленник захватывает информацию в процессе ее передачи к месту назначения. Перехват имен и паролей создает большую опасность, так как

пользователи часто применяют одни и те же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а данные аутентификации передаются по сети в читаемом текстовом формате, эту информацию можно использовать для доступа к другим корпоративным или внешним ресурсам.

В самом худшем случае хакер получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает атрибуты нового пользователя, которые можно в любой момент применить для доступа в сети и к ее ресурсам.

Перехват сеанса. По окончании начальной процедуры аутентификации соединения, установленного законным пользователем - почтовым сервером, переключается злоумышленником на новый узел, а исходному серверу выдается команда разорвать соединение. В результате «собеседник» законного пользователя оказывается незаметно подмененным[2].

После получения доступа к сети у атакующего злоумышленника появляются большие возможности:

- он может посылать некорректные данные приложениям и сетевым службам, что приводит к их аварийному завершению или неправильному функционированию;

- он может также наводнить компьютер или всю сеть трафиком, пока не произойдет остановка системы в связи с перегрузкой;

- атакующий может блокировать трафик, что приведет к потере доступа авторизованных пользователей к сетевым ресурсам.

Стоит отметить, что методы внедрения сетевых атак не стоят на месте, и для этого необходимо постоянно выполнять различного рода процедуры защиты: обновлять антивирус, проверять рабочие станции, своевременно реагировать на события ИБ с помощью систем мониторинга, а также проводить аудит безопасности путем тестирования на проникновение.

2 Тестирование на проникновение

Тестирование на проникновение представляет собой метод оценки защищенности сети, который заключается в постройке модели атаки, чтобы обнаружить уязвимости в системе безопасности компании[3].

Средством тестирования является программное обеспечение, которое позволяет анализировать степень защиты систем и в дальнейшем выполнять имитации атаки на систему. С помощью тестирования можно осуществлять оценку уровня защиты сегментов и подготовить полный отчет.

Выполняется тестирование по методам «белого ящика», когда известна некоторая системная информация и «черного ящика», когда специалистам не предоставляют информацию о системе, кроме названия организации. Так же имеется понятие «серого ящика», когда используются части как из «белого ящика», так и из «черного ящика».

Процесс тестирования можно разделить на пять этапов.

Первый этап акцентируется в планировании и разведке. Он состоит в определении объема и целей тестирования, включая системы, которые должны быть рассмотрены и методы, которые будут использоваться. Сбор информации (например, сетевые и доменные имена, почтовый сервер) нужен для лучшего понимания работы цели и ее потенциальных уязвимостей.

Следующий этап (сканирование) показывает, как будет реагировать приложение на различные попытки вторжения. Обычно это делается с помощью двух видов анализа. Первый это статический анализ, в котором выполняется проверка кода приложения для оценки его поведения. Эти инструменты могут сканировать весь код за один проход. Второй динамический анализ — это проверка кода приложения в запущенном состоянии. Это более практичный способ сканирования, поскольку он обеспечивает представление работы приложения в реальном времени.

Этап получения доступа использует атаки веб-приложений, которые используются для обнаружения уязвимостей цели. Затем тестировщики пытаются использовать эти уязвимости, как правило, путем расширения прав, кражи данных, перехвата трафика и т.д., чтобы понять ущерб, который они могут причинить.

Цель следующего этапа - поддержание доступа, состоит в том, чтобы увидеть, может ли плохой субъект получить расширенный доступ. Идея заключается в том, чтобы имитировать постоянные угрозы, которые часто остаются в системе в течение нескольких месяцев, чтобы украсть наиболее конфиденциальные данные организации.

Последний этап – этап анализа. Результаты теста на проникновение заносятся в отчет с подробным описанием. В нем описаны конкретные уязвимости, а также доступ к конфиденциальным данным.

В ходе анализа тестирования выделяют методы испытания на проникновение:

- целью внешнего тестирования на проникновение являются активы компании, которые размещены в интернете, на веб-сайте, серверах электронной почты и DNS.

- внутреннее тестирование, это когда злоумышленник имитирует атаку, имея доступ к приложению за межсетевым экраном. Известным сценарием может быть сотрудник, учетные данные которого были украдены из-за фишинг-атаки.

- слепое тестирование, когда хакеру известно только название предприятия, на которое он целенаправлен. Сотрудники службы безопасности в этом случае смогут посмотреть, как в реальном времени произойдет инцидент.

- двойное слепое тестирование. Сотрудники службы безопасности не знают о предстоящей атаке, поэтому у них не будет времени подготовиться к защите.

- целевое тестирование, когда сотрудники службы безопасности и тестер проводят работу совместно друг с другом в режиме онлайн.

2.1 Анализ инструментов тестирования на проникновения

Имеется множество коммерческих и бесплатных инструментов для оценки системы информационной безопасности. Для проведения теста нужен конкретный инструмент, который ему подходит, и выбрать его не легко.

Выделяют основные четыре вида оценки безопасности: сбор данных, привязка, оценка и проникновение. Для сбора данных необходимо провести поиск сетевых устройств путем сканирования. Для привязки и оценки нужно узнать, где работает приложение, имеющее уязвимости. Проникновение - это когда уязвимости применяются для доступа к сетевым устройствам [4].

Большинство тестовых инструментов находятся в ОС KaliLinux, используются следующие программы [5]:

- сканер портов Nmap;
- сканер уязвимостей OpenVAS;
- MetasploitFramework (проведение тестирования на проникновение, содержащее в себе эксплойты);
- BurpSuiteFreeEdition (локальный прокси/сканер для анализа защищенности Web-приложений);
- THC-Hydra (утилита для подбора паролей к сетевым сервисам);
- сниффер Ettercap (перехват и анализ сетевого трафика);
- сниффер Wireshark, (перехват и анализ сетевого трафика);
- Aircrack-ng (утилита для тестирования безопасности беспроводных сетей).

После проведения аудита и предоставления отчета со списком уязвимостей, необходимо начать работу над устранением этих самых уязвимостей, собственно, и от атак в целом.

2.2 Методы защиты информации

Из-за постоянного роста угроз, появляются все новое вредоносное ПО. На каждую появившуюся угрозу создаются и используются новые защитные ПО, новые обновления по их уничтожению.

Существуют различные средства электронной защиты, к которым относятся антивирусные программы, системы защиты пользователя электронной почты от подозрительного трафика. Надо систематически обновлять пароли почтовых ящиков[6].

Анти-DDoS. В мире защита своими силами от DDoS-атак невозможна. Разработчики ПО создали услугу анти-DDoS, которая может устранить эту угрозу. Если обнаруживается в системе подозрительный трафик, IP-адреса блокируются.

Резервное копирование данных. В целях сохранности копии данных хранятся на внешних жестких дисках или в самом сервере. В нынешнее время данные компании часто хранятся в центрах обработки данных (ЦОД).

План аварийного восстановления данных похож с резервным копированием. Здесь обязательным условием является аварийный режим работы на время и после ликвидации сбоя. Данные мероприятия нужны для возобновления работы, восстановления данных в кратчайшие сроки.

Межсетевой экран (файрвол) - это программно-аппаратный комплекс, который отвечает за контроль и фильтрацию сетевого трафика.

Шифрование данных при передаче информации в формате (end-to-end protection). При передаче информации с целью ее сохранности применяют шифрование. Шифрование нужно для защиты целостности информации и хранения ее на различных носителях от копирования и использования третьими лицами.

Защита от навязывания ложного маршрута. Чтобы предотвратить эту атаку, нужно настроить ОС так, чтобы сообщения были проигнорированы или применить фильтрацию о маршруте сообщения.

Защита от подмены одной из сторон. Способ защиты заключается в методе случайного подбора значения идентификатора TCP-соединения и применения в качестве протокола TCP и сетевых ОС.

Многоуровневая фильтрация сетевого трафика. Фильтрация происходит на следующих уровнях модели OSI:

- канальном (Ethernet);
- сетевом (IP);
- транспортном (TCP, UDP);
- прикладном (FTP, TELNET, HTTP, SMTP и т.д.).

Фильтрация - основная функция Firewall. Она дает право администратору проводить централизованно мероприятия по разрешению (запрету) доступа пользователям к сетевым ресурсам. При Firewall-фильтрации объектами, к которым доступ надо разграничить, могут быть транспортные протоколы и службы удалённого доступа. А субъектами могут являться IP-адреса рабочих станций пользователей.

Создание частных сетей с виртуальными IP-адресами. Если администратору безопасности надо скрыть реальную топологию внутренней IP-сети, то ему необходимо создать виртуальные сети при помощи Firewall. Для адресации во внешнюю сеть нужно применять прокси-серверы или маршрутизировать системы внешней адресации. Это результат непригодности виртуального IP-адреса. Связь с клиентами по внешней сети с действующего IP-адреса обеспечивает прокси-сервер.

Использование крипто протоколов, как основного средства защиты соединения и передаваемых данных в сети.

S-HTTP - это защищённый протокол, который действует на прикладном уровне модели OSI, обеспечивающий криптозащиту HTTP-документов на web-сервере. Недостатком S-HTTP является невозможность применения на других протоколах.

SSL - универсальный протокол защиты соединения, функционирующий на сеансовом уровне OSI. Данный протокол использует криптосистему с открытым ключом и является средством защиты для любого сетевого протокола. Дело в том, что он работает между транспортным (TCP, UDP) и прикладным (FTP, TELNET) сеансовом уровне OSI. Для отправки зашифрованных сообщений абонентами SSL-соединения применяется криптоключ.

3 Мониторинг информационных структур предприятия

Мониторингом именуется процедура исследования и наблюдения событий ресурсов. Кроме человека в роли исполнителя выступает и программное обеспечение, утилиты и прочее. Целью является состояние информационных инфраструктур (ИИ), выявленное в текущий момент времени. Суть анализа данных требуется для создания результативного решения на события, находящиеся в информационной инфраструктуре компании [7].

В ИИ предприятия входят следующие компоненты: транспортный, прикладной и физический. Транспортный состоит из сетевого оборудования и ПО. Прикладной имеет в своем составе программно-аппаратные комплексы, системное и ПО пользователей. Физический компонент имеет внешние факторы измерения и аппаратные средства сетевого оборудования.

Мониторинг ИИ включает в себя:

- сбор и регистрацию информационных ресурсов (ИР);
- хранение ИР;
- обработку ИР;
- предоставление ИР пользователям.

Для проведения анализа событий, кроме мониторинга используют сетевые сканеры.

3.1 Мониторинг и сетевые сканеры

Сетевые сканеры идентифицируют и анализируют уязвимости, проводят инвентаризацию операционной системы, программного обеспечения и устройств сети, формируют отчеты, в которых описывают способы устранения уязвимостей [8].

Различают два вида сканеров уязвимостей:

- зондирование.
- сканирование.

Зондирование запускает имитацию атаки и позволяет увидеть «дыры» в системе. Использование сканирования является быстрым, но не точным. Оно проводится с определением открытых портов и заголовков в сравнении с таблицей о сетевых устройствах. Работа сканеров имеет три этапа:

- проверка заголовков один из быстрых способов сканирования. Сканер узнает версию программного обеспечения и по этой информации делает вывод о возможных уязвимостях;

- активные зондирующие проверки. Сравняется часть программы с уязвимостью. Версия ПО не проверяется. Данный метод надежный, но медленный, по сравнению с первым;

- имитация атак — это зондирование, которое использует дыры в ПО для проверки наличия уязвимости при помощи подачи импульса в сеть.

Имитация не может применяться всегда, так как она может просто отключить узел сети.

Известны популярные сканеры уязвимостей:

- GFILanGuard;
- Nessus;
- Symantec Security Check;
- XSpider;
- FortiAnalyzer;
- NMAP.

3.2 SIEM-системы

С недавних пор крупные компании начали применять комплексное средство безопасности для анализа инцидентов в режиме онлайн и проводить мониторинг ИС для выявления событий ИБ. Такое средство именуется SIEM-системой.

Данная система выявляет различные нарушения ИБ для своевременного реагирования на события. В своей работе SIEM-система использует[9]:

- системы контроля и управления доступом;
- антивирусы;
- межсетевые экраны;
- системы обнаружения/предотвращения вторжений;
- активные сетевые устройства;
- журналы аудита СУБД.

При этом данная система дает возможность получить сведения о всех событиях ИБ, не препятствуя вредительским действиям. SIEM-система используется для осуществления сбора инцидентов безопасности, то есть консолидации данных; для хранения инцидентов ИБ; корреляции и обработки событий; предоставления инструментов для анализа и разбора событий безопасности; контекстного приобретения сведений о причастности в инцидентах безопасности бизнес-приложениям, сотрудникам; автоматического оповещения через интерфейс SIEM по электронной почте, через SMS и другие.

Кроме этого, без данной системы нельзя было бы создать системы SOC (SecurityOperationCenter), т.е. оперативные центры обеспечения информационной безопасности (ОЦИБ).

Виды типовых сценариев SIEM-системы:

- сценарий отслеживания подтверждения аккаунтов пользователей;
- сценарий отслеживания случаев заражения вредоносным ПО;
- сценарий мониторинга исходящего и передаваемого трафика;
- сценарий отслеживания системных изменений, соответствующая политике безопасности;

- сценарий отслеживания атак на веб-приложения, с использованием журналов и логов.

Мониторинг SIEM-системы предоставляет два типа интерфейсов. На рисунке 1 показан первый тип интерфейса. Он включает структуру разделов вида «иерархия» и показывает отображаемую информацию на рабочей зоне. Данный тип интерфейса имеет доступ к администрированию SIEM и управление безопасностью, чтобы владеть информацией об инцидентах.

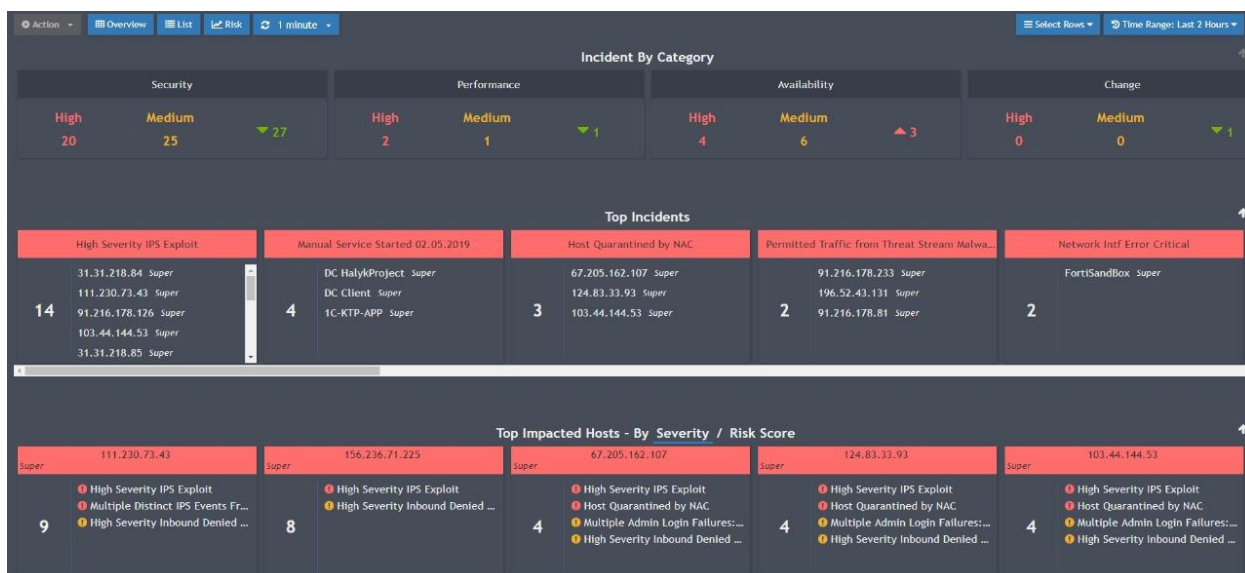


Рисунок 1–Интерфейс администратора SIEM, панель инцидентов

Второй тип интерфейса может проводить мониторинг на устройствах с плазменными панелями и огромными экранами. Как показано на рисунке 2, отображение ведется по панелям (Dashboard) или инцидентам (Incidents) и различным критериям.



Рисунок 2–Виджеты панели SIEM

На рисунке 3 показаны панели мониторинга в режиме онлайн, которые могут прокручиваться в виде слайд-шоу, показывая основные показатели:

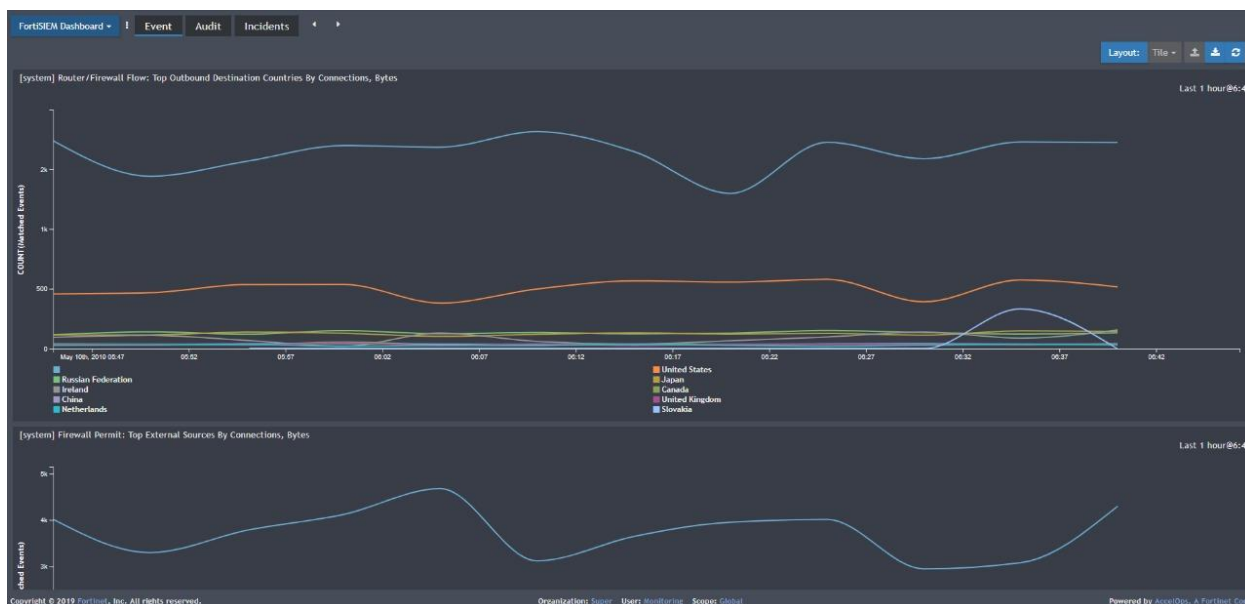


Рисунок 3– Отображение панелей мониторинга SIEM в режиме слайд-шоу

Отчет об имеющихся инцидентах ИБ, отдельно по всем устройствам, показан в рисунке 4.

Sync	Scheduled	Name	Scope	Description
<input type="checkbox"/>	<input type="checkbox"/>	APC UPS Detailed Status	System	Detailed APC UPS status report
<input type="checkbox"/>	<input type="checkbox"/>	AWS Servers By Least Free Disk Space	System	Ranks the devices by minimum free disk space over a window
<input type="checkbox"/>	<input type="checkbox"/>	Account Lockout	System	This report ranks users getting locked out from any devices
<input type="checkbox"/>	<input type="checkbox"/>	Activity: AWS EC2 Linux Failed Privileged Command Executions	System	This report ranks the UNIX servers and their users by failed privilege command escalations (sudo) count
<input type="checkbox"/>	<input type="checkbox"/>	Activity: MS Azure Linux Failed Privileged Command Executions	System	This report ranks the UNIX servers and their users by failed privilege command escalations (sudo) count
<input type="checkbox"/>	<input type="checkbox"/>	Activity: Successful AWS EC2 Linux Servers Privileged Command Executions	System	This report ranks the UNIX servers and their users by successful privilege command escalations (sudo) count
<input type="checkbox"/>	<input type="checkbox"/>	Activity: Successful MS Azure Linux Servers Privileged Command Executions	System	This report ranks the UNIX servers and their users by successful privilege command escalations (sudo) count
<input type="checkbox"/>	<input type="checkbox"/>	Activity: Top Unix Servers, Users By Failed Privileged Command Execution Count	System	This report ranks the UNIX servers and their users by failed privilege command escalations (sudo) count
<input type="checkbox"/>	<input type="checkbox"/>	Activity: Top Unix Servers, Users By Successful Privileged Command Execution Count	System	This report ranks the UNIX servers and their users by successful privilege command escalations (sudo) count
<input type="checkbox"/>	<input type="checkbox"/>	Activity: Unix Server Privileged Command Execution	System	This report details privilege command executions (sudo) at a Unix server
<input type="checkbox"/>	<input type="checkbox"/>	Admin Logon: Failed VPN Admin Logon Detailed View	System	Provides event details for all failed VPN admin logons
<input type="checkbox"/>	<input type="checkbox"/>	Admin Logon: Successful VPN Admin Logon Detailed View	System	Provides event details for all successful VPN admin logons
<input type="checkbox"/>	<input type="checkbox"/>	Admin Logon: Top VPN Gateways, Admin Users Ranked By Failed Logon	System	Ranks the VPN Gateways and their admins by the number of failed device logons
<input type="checkbox"/>	<input type="checkbox"/>	Admin Logon: Top VPN Gateways, Admin Users Ranked By Successful Logon	System	Ranks the VPN Gateways and their admin users by the number of successful device logons
<input type="checkbox"/>	<input type="checkbox"/>	Admin Logon: VPN Admin Logon/Logoff Activity Details	System	Provides event details for all successful and failed VPN admin logons and logoffs
<input type="checkbox"/>	<input type="checkbox"/>	Airline Database Query Errors	System	Shows all database query errors. Meta data such as flight details and weight on wheels are added
<input type="checkbox"/>	<input type="checkbox"/>	Airline Database Query Execution Failures	System	Shows all database query execution failures. Meta data such as flight details and weight on wheels are added
<input type="checkbox"/>	<input type="checkbox"/>	Airline Errors	System	Counts total number of error events
<input type="checkbox"/>	<input type="checkbox"/>	Airline SSH Activity After Takeoff	System	Enumerates SSH Activity after takeoff
<input type="checkbox"/>	<input type="checkbox"/>	Airline SSH Activity Before Takeoff	System	Enumerates SSH Activity before takeoff

Рисунок 4– Отчет о событиях, наступивших на контролируемом устройстве, в интерфейсе администратора SIEM

Мониторинг SIEM оказывает поддержку обнаружения устройств, приложений и конфигураций, путем сравнения топологии физических и виртуальных инфраструктур, различных облаков, благодаря учетным данным. Для межсетевых экранов и маршрутизаторов необходимо знать интерфейсы, которые заняты и трафик, который потребляет много ресурсов.

На рисунке 5 показана панель мониторинга SIEM со статическими данными, с помощью которых администратор SIEM может выявить

загруженность интерфейса маршрутизатора, виды приложений и качество обслуживания.



Рисунок 5– Мониторинг состояний межсетевых экранов в интерфейсе администратора SIEM

Все, выявленные средствами SIEM устройства, находятся под контролем и их данные будут анализироваться. Администратору SIEM разрешено проводить настройку панели мониторинга устройства или сервиса.

Мониторинг контролируемого SIEM сервиса показан на рисунке 6.

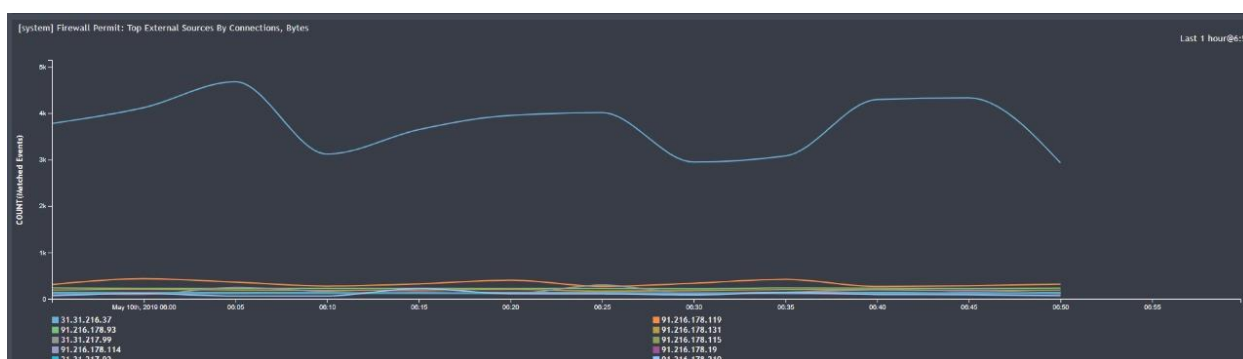


Рисунок 6 - График производительности SIEM

Путем анализа сервисов наблюдается ряд атак, а именно при DDoS-атаки, резко возрастает сетевой поток, что отражается на панели мониторинга. На рисунке 7 наблюдается отслеживание события, при сгенерированной корреляции.

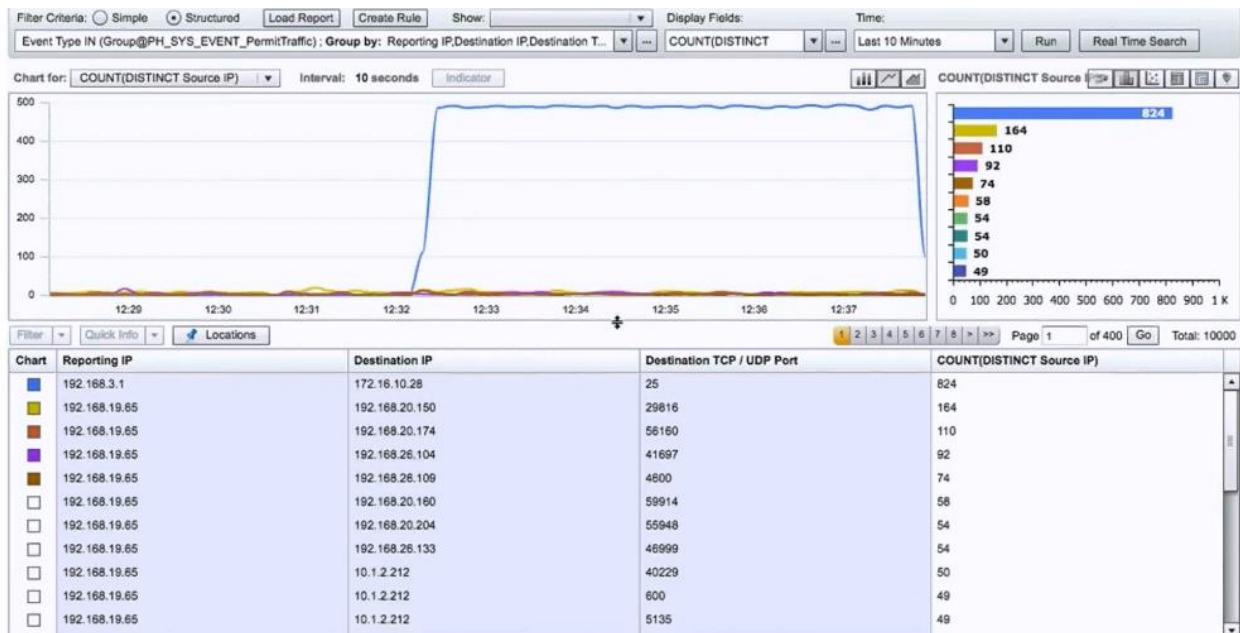


Рисунок 7 – Мониторинг DDoS-атаки средствами SIEM

Рисунок 8 показывает, как уровень риска, активность правила корреляции формирует инцидент. В данном окне администратор SIEM-системы может создать задачу (ticket), в котором указывается событие ИБ (подозрительный трафик), степень критичности события (высокий). Указывают свой идентификатор о создании задачи и указывают администраторов ИБ для ее выполнения.

Incident ID(s): 98105 Mode: Create a new ticket

Summary: Permitted Traffic from Threat Stream Malware IP List, in InternetShield_Dostyk(10.222.110.16)

State: Assigned Assignee: [Super] Monitoring (dezurnyj@)

Escalation: None Selected Priority: High

Due Date: 05/10/2019 07:02:05 Attachment:

CC:

Notes:

- Incident Name => Permitted Traffic from Threat Stream Malware IP List
- Incident Source => IP Address:196.52.43.131,
- Incident Target => InternetShield_Dostyk(10.222.110.16)
- Incident Detail =>
- Incident ID => 98105

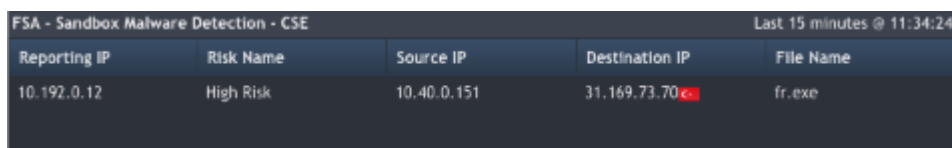
Save Cancel

Рисунок 8– Формирование правила корреляции SIEM

Возможно, написание правила построения корреляции по разным событиям, что будет являться инцидентом ИБ со своим отчетом и оповещением.

При помощи сетевой песочницы (Sandbox) можно обнаружить вредоносные программы. Она отмечает вредоносную активность, будучи

отслеживаемым SIEM устройством. События по выявлению вредоносных программ будет собрано, обновиться панель мониторинга на SIEM и автоматически образуется правило оповещения об этом инциденте, которая будет передавать команды для блокировки нежелательной активности, как показано на рисунке 9.



Reporting IP	Risk Name	Source IP	Destination IP	File Name
10.192.0.12	High Risk	10.40.0.151	31.169.73.70	fr.exe

Рисунок 9 - Оповещение инцидента на панели мониторинга SIEM

3.3 Мониторинг безопасности сети на основе сетевых сканеров

Существуют большое количество специализированных программных обеспечений, предназначенных для выявления уязвимостей путем моделирования сетевых атак. Имеется в арсенале особая операционная система, вобравшая в себя комплекс приложений, которые применяются для имитации различного рода атак, в том числе и сетевых. Такая операционная система носит название KaliLinux [10].

Для проведения тестирования был выделен ноутбук, также подключенный внутренний адрес рабочей станции. После подключения данной ОС и установки ее сетевых параметров была начата подготовка к выполнению пентеста.

На первом этапе внедрения, важно узнать, в какой подсети находится наш выделенный адрес и какие хосты подключены вместе с данным адресом. Для этого используем встроенную утилиту Nmap KaliLinux, которая выдает список хостов, находящихся рядом с нашим адресом. Данная программа выполняется в командной строке при вводе специальной команды, что показано на рисунке 10.


```
root@kali: /home/madi# nmap -sV -o 192.168.179.0/26
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-30 01:05 CDT
Nmap scan report for 192.168.179.1
Host is up (0.00052s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          (protocol 2.0)
80/tcp    open  tcpwrapped
113/tcp   closed ident
443/tcp   open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
bmit:Port22-TCP:V=7.70%I=7%D=4/30%Time=5CC7E639%P=x86_64-pc-linux-gnu%r(NULL)
SF: ,10,"SSH-2\0-YFaut0\r\n";
MAC Address: 00:09:0F:09:00:8C (Fortinet)
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (87%)
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: OpenBSD 4.0 (87%), OpenBSD 4.3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.179.5
Host is up (0.0022s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5800/tcp  open  vnc-http    RealVNC E4 (resolution: 600x250; VNC TCP port: 5900)
5900/tcp  open  vnc         RealVNC Enterprise (protocol 4.1)
MAC Address: 40:B0:34:1F:A4:F7 (Hewlett Packard)
Aggressive OS guesses: Microsoft Windows Longhorn (94%), Microsoft Windows 10 1703 (93%), Microsoft Windows 7 SP1 (93%), Microsoft Windows 8 (93%), Microsoft Windows 10 1511 (92%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 SP2 (92%), Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows 7 Enterprise SP1 (92%)
```

Рисунок 10 – Список хостов программой Nmap

После сканирования, были определены хосты и наличие открытых портов. В итоге найдены открытые порты (443, 445, 3389) на двух рабочих станциях, с которых можно осуществить доступ (рисунок 11).


```

root@kali: /home/madi
Tue 05:41
File Edit View Search Terminal Tabs Help
root@kali: /home/madi
2 cpe:/o:microsoft:windows 8 cpe:/o:microsoft:windows 8.1
OS details: Microsoft Windows 7 SP1 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: PC-MATKASSIMOV; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.179.26
Host is up (0.00098s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open  ssl/https
445/tcp   filtered microsoft-ds
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1110/tcp  filtered nfsd-status
2869/tcp  filtered iclslap
3389/tcp  open  ms-wbt-server   Microsoft Terminal Services
19780/tcp filtered unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/su
bmit.cgi?new-service :
SF-Port443-TCP:V=7.70%T=SSL%I=7%0=4/30%Time=5CC7E6C6%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,A5,"HTTP/1.1\x20403\x20Forbidden\r\nDate:\x20Tue,\x202030\
SF:\x20Apr\x202019\x2006:09:18\x20GMT\r\nConnection:\x20close\r\nContent-Ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nX-Frame-Options:\x20DENY\r\nCont
SF:ent-Length:\x200\r\n\r\n")%r(HTTPOptions,AB,"HTTP/1.1\x20501\x20Not\x2
SF:Implemented\r\nDate:\x20Tue,\x2030\x20Apr\x202019\x2006:09:18\x20GMT\r
SF:\nConnection:\x20close\r\nContent-Type:\x20text/plain;\x20charset=utf-8
SF:\r\nX-Frame-Options:\x20DENY\r\nContent-Length:\x200\r\n\r\n")%r(Four0h
SF:FourRequest,A5,"HTTP/1.1\x20404\x20Not\x20Found\r\nDate:\x20Tue,\x2030
SF:\x20Apr\x202019\x2006:09:18\x20GMT\r\nConnection:\x20close\r\nContent-T
SF:pe:\x20text/plain;\x20charset=utf-8\r\nX-Frame-Options:\x20DENY\r\nCon
SF:tent-Length:\x200\r\n\r\n")%r(RTSPRequest,B3,"HTTP/1.1\x20400\x20Bad\x
SF:Request\r\nDate:\x20Tue,\x2030\x20Apr\x202019\x2006:09:28\x20GMT\r\nC
SF:nection:\x20close\r\nContent-Type:\x20text/html\r\nContent-Length:\x20
Tue 05:41
root@kali: /home/madi
File Edit View Search Terminal Tabs Help
root@kali: /home/madi
root@kali: /home/madi# nmap -sV -O 192.168.179.0/26
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-30 01:05 CDT
Nmap scan report for 192.168.179.1
Host is up (0.00052s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              (protocol 2.0)
80/tcp    open  tcpwrapped
113/tcp   closed ident
443/tcp   open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/su
bmit.cgi?new-service :
SF-Port22-TCP:V=7.70%I=7%0=4/30%Time=5CC7E639%P=x86_64-pc-linux-gnu%r(NULL
SF:10,"SSH-2.0-YFaut6\r\n");
MAC Address: 00:09:0F:09:00:8C (Fortinet)
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (87%)
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: OpenBSD 4.0 (87%), OpenBSD 4.3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.179.5
Host is up (0.0022s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server   Microsoft Terminal Services
5800/tcp  open  vnc-http        RealVNC E4 (resolution: 600x250; VNC TCP port: 5900)
5900/tcp  open  vnc              RealVNC Enterprise (protocol 4.1)
MAC Address: 40:B0:34:1F:A4:F7 (Hewlett Packard)
Aggressive OS guesses: Microsoft Windows Longhorn (94%), Microsoft Windows 10 1703 (93%), Microsoft Windows 7 SP1 (93%), Microsoft Windows 8 (93%), Mi
crosoft Windows 10 1511 (92%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 SP2 (92%), Microsoft Windows 8.1 Update 1 (92%),
Microsoft Windows Vista SP1 (92%), Microsoft Windows 7 Enterprise SP1 (92%)

```

Рисунок 11 – Открытые подозрительные порты

После появления возможности проведения успешной атаки в виде открытых портов, следует провести сканирование на наличие уязвимостей в данном IP-адресе. Действие будет выполнено с помощью сканера на проверку уязвимости сети, называемого OpenVas[11]. Эта программа и совершает поиск уязвимостей, что отображается на рисунке 12.

```

Applications ▾ Places ▾ Terminal ▾ Tue 05:40
root@kali: /home/madi
File Edit View Search Terminal Tabs Help

root@kali: /home/madi x madi@kali: -

root@kali: /home/madi# openvas-start
[*] Please wait for the OpenVAS services to start.
[*] You might need to refresh your browser once it opens.
[*] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● greenbone-security-assistant.service - Greenbone Security Assistant
  Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; disabled; vendor preset: disabled)
  Active: active (running) since Tue 2019-04-30 00:44:27 CDT; 1min 9s ago
  Docs: man:gsad(8)
        http://www.openvas.org/
  Main PID: 1808 (gsad)
  Tasks: 4 (Limit: 4514)
  Memory: 4.3M
  CGroup: /system.slice/greenbone-security-assistant.service
          └─1808 /usr/sbin/gsad --foreground --listen=127.0.0.1 --port=9392 --mlisten=127.0.0.1 --mport=9390
            └─1811 /usr/sbin/gsad --foreground --listen=127.0.0.1 --port=9392 --mlisten=127.0.0.1 --mport=9390

Apr 30 00:44:27 kali systemd[1]: Started Greenbone Security Assistant.
Apr 30 00:44:28 kali gsad[1808]: Warning: MHD_USE_THREAD_PER_CONNECTION must be used only with MHD_USE_INTERNAL_POLLING_THREAD. Flag MHD_USE_INTERNAL_POLLING_THREAD was added. Consider setting MHD_USE_INTERNAL_POLLING_THREAD explicitly.
Apr 30 00:44:28 kali gsad[1808]: Warning: MHD_USE_THREAD_PER_CONNECTION must be used only with MHD_USE_INTERNAL_POLLING_THREAD. Flag MHD_USE_INTERNAL_POLLING_THREAD was added. Consider setting MHD_USE_INTERNAL_POLLING_THREAD explicitly.

● openvas-scanner.service - Open Vulnerability Assessment System Scanner Daemon
  Loaded: loaded (/lib/systemd/system/openvas-scanner.service; disabled; vendor preset: disabled)
  Active: active (running) since Tue 2019-04-30 00:45:31 CDT; 5s ago
  Docs: man:openvassd(8)
        http://www.openvas.org/
  Process: 1818 ExecStart=/usr/sbin/openvassd --unix-socket=/var/run/openvassd.sock (code=exited, status=0/SUCCESS)
  Main PID: 1839 (openvassd)
  Tasks: 3 (Limit: 4514)
  Memory: 97.9M
  CGroup: /system.slice/openvas-scanner.service
          └─1839 /usr/sbin/openvassd --unix-socket=/var/run/openvassd.sock

```

Рисунок 12 – Запуск сканирования через командную строку KaliLinux

По истечении определенного времени в программе OpenVas появляется список уязвимостей, которые нужно устранить для дальнейшей безопасной работы. Как мы видим, на рисунке 13 выявлено множество уязвимостей, выделенных красным цветом.

Vulnerability	Severity	QoD	Host	Location	Actions
PHP 'php_stream_scandir()' Buffer Overflow Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP 'php_stream_scandir()' Buffer Overflow Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	443/tcp	[Icons]
PHP 'type confusion' Denial of Service Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP 'type confusion' Denial of Service Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	443/tcp	[Icons]
PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Windows)	10.0 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Windows)	10.0 (High)	80%	10.7.63.223	443/tcp	[Icons]
PHP 'com_print_typeinfo()' Remote Code Execution Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP 'com_print_typeinfo()' Remote Code Execution Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	443/tcp	[Icons]
PHP Multiple Vulnerabilities - Sep11 (Windows)	10.0 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP Multiple Vulnerabilities - Sep11 (Windows)	10.0 (High)	80%	10.7.63.223	443/tcp	[Icons]
PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)	10.0 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)	10.0 (High)	80%	10.7.63.223	443/tcp	[Icons]
PHP Multiple Vulnerabilities - 05 - Aug16 (Windows)	10.0 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP Multiple Vulnerabilities - 05 - Aug16 (Windows)	10.0 (High)	80%	10.7.63.223	443/tcp	[Icons]
PHP End Of Life Detection (Windows)	10.0 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP End Of Life Detection (Windows)	10.0 (High)	80%	10.7.63.223	443/tcp	[Icons]
PHP Multiple Vulnerabilities - Dec18 (Windows)	8.5 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP Multiple Vulnerabilities - Dec18 (Windows)	8.5 (High)	80%	10.7.63.223	443/tcp	[Icons]
PHP Denial of Service Vulnerability Jul17 (Windows)	7.8 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP Denial of Service Vulnerability Jul17 (Windows)	7.8 (High)	80%	10.7.63.223	443/tcp	[Icons]
Kerio Personal Firewall Admin Service	7.5 (High)	70%	10.7.63.223	44333/tcp	[Icons]
Kerio Winroute Firewall Admin Service	7.5 (High)	95%	10.7.63.223	44333/tcp	[Icons]
PHP Multiple Vulnerabilities - Feb19 (Windows)	7.5 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP Multiple Vulnerabilities - Feb19 (Windows)	7.5 (High)	80%	10.7.63.223	443/tcp	[Icons]
PHP Multiple Vulnerabilities - 02 - Sep16 (Windows)	7.5 (High)	80%	10.7.63.223	4080/tcp	[Icons]
PHP Multiple Vulnerabilities - 02 - Sep16 (Windows)	7.5 (High)	80%	10.7.63.223	443/tcp	[Icons]
PHP Multiple Vulnerabilities - 05 - Jul16 (Windows)	7.5 (High)	80%	10.7.63.223	4080/tcp	[Icons]

Рисунок 13 – Список уязвимостей для двух выделенных IP-адресов

3.4 Анализ инцидентов безопасности посредством SIEM-системы

Благодаря средствам SIEM у администратора всегда есть возможность просмотреть резюме инцидента, содержащее информацию о том, кто передал информацию об инциденте, какого рода этот инцидент, к какому бизнес-сервису инцидент относится, количество инцидентов. По этой информации можно сделать вывод о критичности инцидента.

SIEM основывается на поиске, отображении отчетов и правил. Поиск SIEM – это поиск в режиме онлайн, где показаны события при их возникновении. А также SIEM может выполнять исторический поиск информации по заданным временным промежуткам, находящейся в базе данных.

Рисунок 14 показывает, как оба типа могут выполнять простой поиск, на основе значений событий, а после объединять их по атрибутам.

Last Occurred	Reporting	Source	Target	Detail	Incident	Incident Status	Resolution	Count
May 10 2019, 06:11:00 AM	InternetShield_Dostyk	124.83.33.93	31.31.218.85	Component Event Type: FortiGate-Ips-signature-33106 Attack Name: MS_RDP.Connection.Brute.Force Triggered Event Count: 1	High Severity IPS Exploit	Active	Open	2
May 10 2019, 06:11:00 AM	InternetShield_Dostyk	124.83.33.93			Host Quarantined by NAC	Active	Open	2
May 10 2019, 05:59:00 AM	InternetShield_Dostyk	196.52.43.131	91.216.178.81		Permitted Traffic from Threat Stream Malware IP List	Active	Open	1
May 10 2019, 05:39:30 AM	InternetShield_Dostyk	172.104.242.173	91.216.178.44	Component Event Type: FortiGate-Ips-signature-47649 Attack Name: WINNTL.Botnet Triggered Event Count: 2	High Severity IPS Exploit	Active	Open	7
May 10 2019, 05:38:30 AM	InternetShield_Dostyk	172.104.242.173	91.216.178.46	Component Event Type: FortiGate-Ips-signature-47649 Attack Name: Joomla!.Core.Session.Remote.Code.Exe... Triggered Event Count: 2	High Severity IPS Exploit	Active	Open	7
May 10 2019, 05:37:30 AM	InternetShield_Dostyk	156.236.71.225	91.216.178.114	Component Event Type: FortiGate-Ips-signature-41851 Attack Name: Joomla!.Core.Session.Remote.Code.Exe... Triggered Event Count: 1	High Severity IPS Exploit	Active	Open	3
May 10 2019, 05:36:30 AM	InternetShield_Dostyk	156.236.71.225	91.216.178.114	Component Event Type: FortiGate-Ips-signature-47359 Attack Name: Joomla!.Core.Session.Remote.Code.Exe... Triggered Event Count: 1	High Severity IPS Exploit	Active	Open	1

Details Events Rule Auto expand

Incident ID: 98105 Incident Type: PH_RULE_FROM_THREATSTREAM_MAL... Ticket Status: None Biz Service: Security
Cleared Time: Incident Comments: Notification Recipients: Severity: 9 Impacts: 1
Cleared Reason: Incident Comments: Organization: Super First Occurred: May 10 2019, 05:59:00 AM
Reporting IP: 10.222.110.16 Ticket ID: External Cleared Time: External Resolve Time: 1
Cleared User: External Ticket State: External Ticket Type: View Status: Read
Category: 4 Subcategory: Malware Reporting Status: 2

Рисунок 14 – Исторический поиск SIEM

Администратор SIEM имея необходимые средства, может рассмотреть резюме инцидента с подробной информацией о самом инциденте. Критичность инцидента показана на рисунке 15.

Elapsed	State	Priority	Ticket ID	Summary	Assignee	Creator	Creation Date
Overdue	Closed	Medium	7961032	Heavy TCP Host Scan On Fixed Port 29.03.2019, In In...	Monitoring	Monitoring <dezhurny@kazteleport.kz>	Apr 10 2019, 01:10:22 PM
Overdue	Assigned	Medium	4476800	Sudden Increase in Failed Logons To A Host, in dc-2.k...	SOC	admin <NursultanovB@kazteleport.kz>	May 02 2019, 12:16:20 PM
Overdue	Assigned	Medium	8911674	Sudden Increase in Network Interface Traffic, in TC...	admin	Monitoring <dezhurny@kazteleport.kz>	Apr 29 2019, 11:09:12 AM
Overdue	Closed	Medium	8511081	Account Locked: Domain, in dc.kazteleport.kz(10.22...	Monitoring	Monitoring <dezhurny@kazteleport.kz>	Apr 18 2019, 12:34:42 AM
Overdue	Assigned	Medium	8911652	Sudden Increase in Permitted Outbound Traffic To A ...	admin	Monitoring <dezhurny@kazteleport.kz>	Apr 22 2019, 09:55:26 PM
Overdue	Assigned	Medium	8911664	Sudden Increase in Permitted Inbound Traffic To A Sp...	admin	Monitoring <dezhurny@kazteleport.kz>	Apr 26 2019, 12:57:19 PM
Overdue	Closed	Medium	8511082	Account Locked: Domain, in dc.kazteleport.kz(10.22...	Monitoring	Monitoring <dezhurny@kazteleport.kz>	Apr 18 2019, 01:00:28 AM
Overdue	Closed	High	8511084	Sudden Increase in Traffic From Host, in InternetShie...	Monitoring	Monitoring <dezhurny@kazteleport.kz>	Apr 18 2019, 09:30:55 AM
Overdue	Assigned	High	8911670	Permitted Traffic from Threat Stream Malware IP Lis...	Monitoring	Monitoring <dezhurny@kazteleport.kz>	Apr 27 2019, 09:22:05 AM
Overdue	Assigned	Medium	8911662	Sudden Increase in Traffic From Host, in InternetShie...	admin	Monitoring <dezhurny@kazteleport.kz>	Apr 26 2019, 12:54:34 PM
Overdue	Assigned	High	8911668	High Severity IPS Exploit, in InternetShield_Dostyk(1...	admin	Monitoring <dezhurny@kazteleport.kz>	Apr 26 2019, 10:00:30 PM
Overdue	Assigned	High	8911659	High severity inbound Permitted IPS Exploit, in inter...	admin	Monitoring <dezhurny@kazteleport.kz>	Apr 25 2019, 02:06:51 PM
Overdue	Closed	Medium	8911657	Sudden Increase in Network Interface Traffic, in TC...	admin	Monitoring <dezhurny@kazteleport.kz>	Apr 25 2019, 01:58:04 AM
Overdue	Assigned	Medium	8911655	Sudden Increase in Traffic From Host, in InternetShie...	Monitoring	Monitoring <dezhurny@kazteleport.kz>	Apr 25 2019, 06:42:37 AM
Overdue	Assigned	Medium	8911653	Sudden Increase in Network Interface Traffic, in inte...	admin	Monitoring <dezhurny@kazteleport.kz>	Apr 23 2019, 08:28:46 AM
Overdue	Assigned	Medium	8911654	Sudden Increase in Traffic From Host, in InternetShie...	Monitoring	Monitoring <dezhurny@kazteleport.kz>	Apr 24 2019, 08:17:24 PM
Overdue	Closed	High	7961039	High Severity inbound Permitted IPS Exploit, in inter...	Monitoring	Monitoring <dezhurny@kazteleport.kz>	Apr 11 2019, 11:13:41 PM
Overdue	Closed	Medium	8511078	Sudden Increase in Traffic From Host, in InternetShie...	Monitoring	Monitoring <dezhurny@kazteleport.kz>	Apr 17 2019, 10:55:54 AM
Overdue	Closed	High	8511096	Permitted Traffic from Threat Stream Malware IP Lis...	Monitoring	Monitoring <dezhurny@kazteleport.kz>	Apr 19 2019, 12:35:44 PM
Overdue	Closed	High	8511079	Permitted Traffic from Threat Stream Malware IP Lis...	Monitoring	Monitoring <dezhurny@kazteleport.kz>	Apr 17 2019, 03:27:22 PM

Рисунок 15 – Список зафиксированных инцидентов

Для просмотра полной информации об инциденте можно наблюдать в логах событий. Дополнительно можно создать правило корреляции. Эти правила построены для корреляции большого числа критериев (рисунок 16).

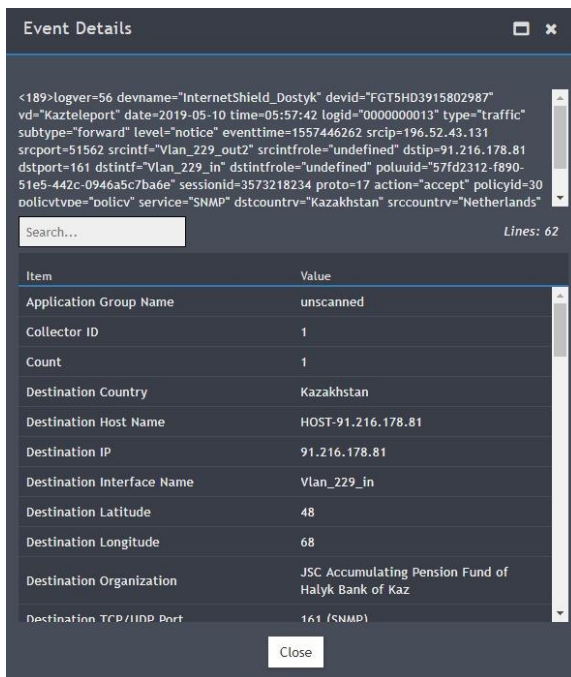


Рисунок 16 –Лог инцидента в SIEM

Администратору SIEM дана возможность исторического поиска, чтобы он мог управлять угрозами (рисунок 17). Таким образом, он контролирует тип угрозы в определенный промежуток времени. На рисунке 17 можно наблюдать, что в течении 24 часов SIEM-система выявила 222 высоких, 178 средних, 14 малых событий ИБ, распределенные по уровням критичности.

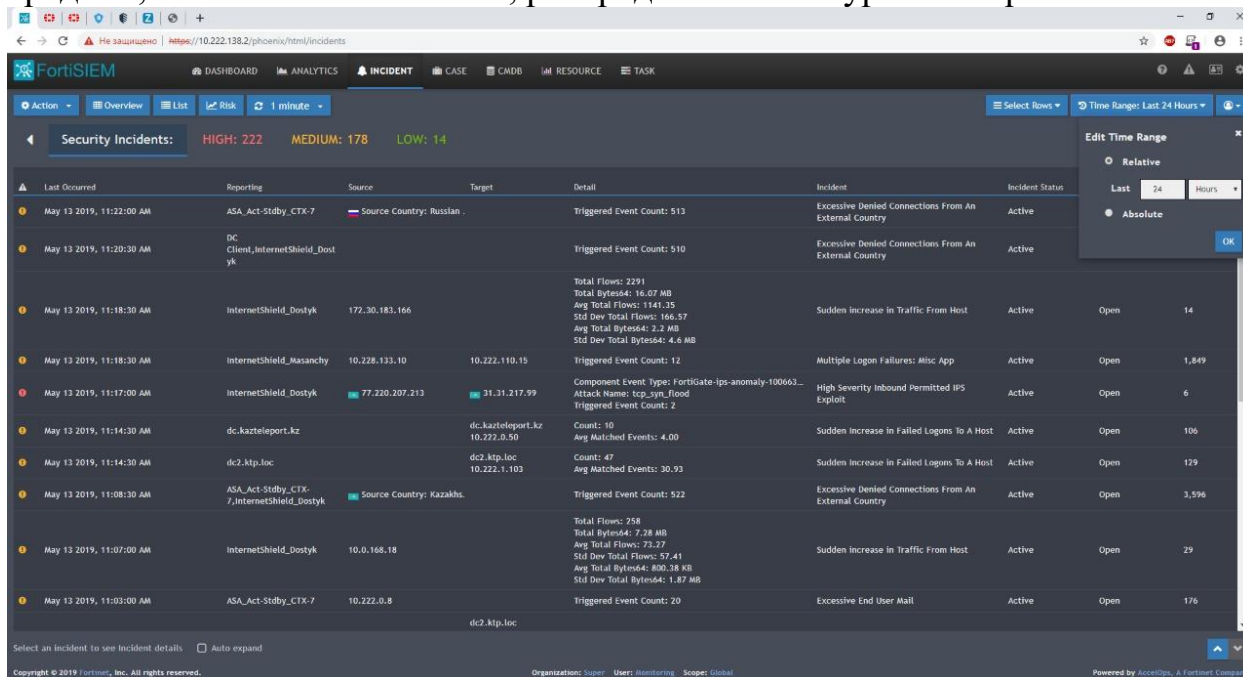


Рисунок 17 –Виджет временного диапазона

Рассмотрим инцидент с переполнением буфера на операционной системе Windows, как показано на рисунке 18. Программа OpenVas показывает, что данная уязвимость на первый взгляд является критичным. Поскольку версия используемого приложения на данной рабочей станции является устарелой, то уязвимость принимает актуальный характер.

В Операционных системах часто используются программы, которые работают с блоками данных, читаемых с носителей, из сети, или даже с клавиатуры. Для размещения этих данных, программы выделяют блоки памяти конечного размера – буфера. Переполнение буфера происходит, когда запись или чтение большого объема данных, чем вмещает сам буфер. ОС настроена так, что программы не будут пытаться занести в буфер больше, чем допустимо. Но как ни странно, переполнения буфера продолжают происходить, что может вызвать более критичный статус безопасности.

На рисунке 18 написано, что переполнение буфера может дать возможность провести атаку типа отказа в обслуживании или IP-спуфинга. Из-за этого статус безопасности в столбце (Severity) показан красным цветом, что вызывает высокий уровень угрозы.

Result: PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows)

Vulnerability	Severity	OoD	Host	Location	Actions
PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	4080/tcp	[Icons]

Summary
This host is running PHP and is prone to buffer overflow vulnerability.

Vulnerability Detection Result
Installed version: 5.2.9
Fixed version: 5.3.15/5.4.5

Impact
Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions.

Solution
Solution type: VendorFix
Upgrade to PHP 5.4.5 or 5.3.15 or later.

Affected Software/OS
PHP version before 5.3.15 and 5.4.x before 5.4.5

Vulnerability Insight
Flaw related to overflow in the _php_stream_scandir function in the stream implementation.



Vulnerability Detection Method
Details: PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803317)
Version used: \$Revision: 11865 \$

Product Detection Result
Product: cpe:/a:php:php:5.2.9
Method: PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Log: View details of product detection

References
CVE: CVE-2012-2688
BID: 54638
CERT: CB-K13/1037, CB-K13/0712, DFN-CERT-2013-2065, DFN-CERT-2013-1713, DFN-CERT-2013-1494, DFN-CERT-2013-0357, DFN-CERT-2012-1655, DFN-CERT-2012-1654, DFN-CERT-2012-1560, DFN-CERT-2012-1541, DFN-CERT-2012-1505, DFN-CERT-2012-1504, DFN-CERT-2012-1503, DFN-CERT-2012-1499, DFN-CERT-2012-1422
Other: http://www.php.net/ChangeLog-5.php
http://en.securitylab.ru/nvdi/427456.php

Рисунок 18 – Уязвимость по переполнению буфера


Стоит отметить, что попытка осуществления атаки типа отказа в обслуживании или IP-спуфинга имеет серьезную возможность. Согласно отчету OpenVas, данная уязвимость о возможном дешифровании SSL/TLS сертификатов, основанная на алгоритме шифрования Диффи-Хэллмана будет устранена в ходе последующего обновления операционной системы и программного обеспечения.

Vulnerability	Severity	QoD	Host	Location	Actions
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 Medium	80%	192.168.179.10	3389/tcp	 

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Solution type:  Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: [SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability](#), (OID: 1.3.6.1.4.1.25623.1.0.106223)
Version used: \$Revision: 12865 \$

References
Other: <https://weakdh.org/>
<https://weakdh.org/sysadmin.html>

User Tags (none)

Рисунок 19 – Уязвимость SSL/TSLсертификатов

На рисунке 19 наблюдается уязвимость SSL/TSLсертификатов, выполненная на программе OpenVas. В нем имеется название найденной уязвимости и состояние безопасности отмечено желтым цветом. Это означает, что данная уязвимость имеет среднюю критичность. Конкретизация уязвимости содержит меньшее допустимое значение временного ключа, равное 1024 бит. Данная уязвимость как мы видим на рисунке 19, может быть использована для дешифрования SSL/TSLсертификатов.

В ходе дальнейшего аудита безопасности следует повысить размерность ключа, соответствующий требованиям информационной безопасности предприятия, равный 2048 бит.

Phar-архивы аналогичны JAR-архивам Java, но учитывают нужды и гибкость PHP-приложений. Phar-архив используется для распространения законченного PHP-приложения или библиотеки в виде одного файла. Приложение, имеющее вид Phar-архива, используется в точности так же, как и любое другое PHP-приложение. Отчет сканирования можно увидеть на рисунке 20.

Согласно отчету, статус безопасности обозначен желтым цветом, что говорит средним уровнем угрозы. Успешное использование этой проблемы позволяет удаленно злоумышленникам нарушать работу ОС или потенциально раскрывать информацию.

Dashboard Scans Assets Secinfo Configuration Extras Administration Help

Result: PHP 'phar_parse_pharfile' Function Denial of Service Vulnerability - (Windows) ID: 1814750b-23d4-437f-81ae-af962dfc6ede
 Created: Mon Apr 29 09:33:59 2019
 Modified: Mon Apr 29 09:33:59 2019
 Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
PHP 'phar_parse_pharfile' Function Denial of Service Vulnerability - (Windows)	Medium	80%	10.7.63.223	4080/tcp	

Summary
 This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
 Installed version: 5.2.9
 Fixed version: 5.6.30

Impact
 Successfully exploiting this issue allow remote attackers to supply malicious archive files to crash the PHP interpreter or potentially disclose information.

Solution
Solution type: VendorFix
 Upgrade to PHP version 5.6.30 or 7.0.15, or later.

Affected Software/OS
 PHP versions before 5.6.30, 7.x before 7.0.15

Vulnerability Insight
 The flaw exists due to a buffer over-read error in the 'phar_parse_pharfile' function in ext/phar/phar.c script.

Vulnerability Detection Method
 Checks if a vulnerable version is present on the target host.
 Details: PHP 'phar_parse_pharfile' Function Denial of Service Vulnerability - (Windows) (OID: 1.3.6.1.4.1.25623.1.0.811483)
 Version used: \$Revision: 11982 \$

Product Detection Result
 Product: cpe:/a:php:php:5.2.9
 Method: PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
 Log: View details of product detection

References
 CVE: CVE-2017-11147
 CERT: CB-K17/1575, CB-K17/1461, CB-K17/1358, DFN-CERT-2018-0835, DFN-CERT-2017-1647, DFN-CERT-2017-1529, DFN-CERT-2017-1420
 Other: http://www.php.net/ChangeLog-5.php

Рисунок 20 – Уязвимость отказа в обслуживании на Phar-архивах

По итогам сканирование рабочей станции сотрудника компании наблюдается уязвимость в Phar-архивах на различных PHP-приложениях. Данная уязвимость позволяет создать инцидент информационной безопасности посредством атаки отказа в обслуживании. Решение в устранении данной уязвимости состоит в обновлении приложения с 5.2.9 на 5.6.30.

Следующей уязвимостью данной рабочей станцией является возможность использования атаки «человек-по-середине» на сертификаты OpenSSL. Успешное использование этой проблемы позволяет хакерам получать конфиденциальную информацию, проводя атаку «человек посередине». OpenSSL не ограничивает должным образом обработку сообщений шифровального изменения, что позволяет злоумышленникам «посередине» инициировать использование мастер ключа нулевой длины в определенных обменах openSSL-to-OpenSSL и, следовательно, перехватывать сеансы или получать информацию через созданное рукопожатие TLS. Данная уязвимость показана на рисунке 21. Статус безопасности имеет значение (Medium).

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Result: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability Modified: Mon Apr 29 09:37:57 2019
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	Medium	70%	10.7.63.223	44333/tcp	

Summary
OpenSSL is prone to security-bypass vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

Vulnerability Insight
OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS injection' vulnerability.

Vulnerability Detection Method
Send two SSL ChangeCipherSpec request and check the response.
Details: [SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability \(OID: 1.3.6.1.4.1.25623.1.0.105042\)](#)
Version used: \$Revision: 12865 \$

References
CVE: [CVE-2014-0224](#)
BID: [67899](#)
CERT: [CB-K15/0567](#), [CB-K15/0415](#), [CB-K15/0384](#), [CB-K15/0080](#), [CB-K15/0079](#), [CB-K15/0074](#), [CB-K14/1617](#), [CB-K14/1537](#), [CB-K14/1299](#), [CB-K14/1297](#), [CB-K14/1294](#), [CB-K14/1202](#), [CB-K14/1174](#), [CB-K14/1153](#), [CB-K14/0876](#), [CB-K14/0756](#), [CB-K14/0746](#), [CB-K14/0736](#), [CB-K14/0722](#), [CB-K14/0716](#), [CB-K14/0708](#), [CB-K14/0684](#), [CB-K14/0683](#), [CB-K14/0680](#), [DFN-CERT-2016-0388](#), [DFN-CERT-2015-0593](#), [DFN-CERT-2015-0427](#), [DFN-CERT-2015-0396](#), [DFN-CERT-2015-0082](#), [DFN-CERT-2015-0079](#), [DFN-CERT-2015-0078](#), [DFN-CERT-2014-1717](#), [DFN-CERT-2014-1632](#), [DFN-CERT-2014-1364](#), [DFN-CERT-2014-1357](#), [DFN-CERT-2014-1350](#), [DFN-CERT-2014-1265](#), [DFN-CERT-2014-1209](#), [DFN-CERT-2014-0917](#), [DFN-CERT-2014-0789](#), [DFN-CERT-2014-0778](#), [DFN-CERT-2014-0768](#), [DFN-CERT-2014-0752](#), [DFN-CERT-2014-0747](#), [DFN-CERT-2014-0738](#), [DFN-CERT-2014-0715](#), [DFN-CERT-2014-0714](#), [DFN-CERT-2014-0709](#)
Other: <https://www.openssl.org/news/secadv/20140605.txt>

Рисунок 21 – Уязвимость OpenSSL сертификатов

Решение данного инцидента заключается в установке центра распределения сертификатов на сетевых устройствах и рабочих станциях. После распределения соответствующих требованиям сертификатов данная уязвимость будет устранена.

ЗАКЛЮЧЕНИЕ

В данном дипломном проекте, темой которого является мониторинг сетевых угроз на основе тестирования на проникновение, было выполнено выявление различных сетевых угроз с помощью мониторинга сетевых ресурсов предприятия. В процессе выполнения работы выполнено моделирование сетевых атак посредством ОС KaliLinux и специальных утилит. Проведено выявление инцидентов при помощи мониторинга и анализ событий при помощи SIEM-системы.

В ходе выполнения дипломного проекта был проведен анализ сетевых угроз и их источников, рассмотрена классификация сетевых атак, выполнен обзор инструментов тестирования на проникновение, проанализированы функции SIEM-системы.

Выполнено моделирование сетевых атак с помощью утилит KaliLinux (Nmap, OpenVas), в результате чего были выявлены открытые порты и уязвимости.

Выполнен анализ следующих инцидентов безопасности с использованием SIEM-системы:

- переполнение буфера;
- дешифрование SSL/TSL сертификатов;
- человек-посередине.

Для устранения уязвимостей предложены определенные методы защиты.

Работа выполнялась на конкретном, реальном предприятии и можно сделать вывод, что при имитации атак, сканировании системы не было выявлено критических уязвимостей. Это говорит о том, что предприятие, а точнее отдел информационной безопасности тщательно введет обновление и работу над безопасностью внутренней сети компании.

Мониторинг обеспечивает своевременное оповещение о событиях, происходящих в системе, а также предоставляет оператору возможность вовремя принять решение по реакции на эти события. Взаимодействие с информационной инфраструктурой, мониторинг предполагает следующие этапы:

- обнаружение события;
- степень важности;
- варианты реакции на события;
- реакция на события.

В качестве реакции на события может быть бездействие или формирование и отправка сообщения определенному набору адресатов. Дальнейшая обработка событий является функцией не системы мониторинга, а оператора, принявшего сообщение. Оператором при этом может быть, как человек, так и информационная система.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Муханова А.А. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах, 2013.
2. Лаборатория Касперского. Вредоносные программы. // Электронная версия на сайте: <https://www.kaspersky.ru/resource-center/preemptive-safety/faq>.
3. Information Supplement: Penetration Testing Guidance. PCI Security Standards Council. 2015. - 40 с.
4. Официальная документация по KaliLinux на сайте // Электронная версия на сайте: <https://docs.kali.org/policy/kali-linux-network-service-policies>.
5. «KaliLinux- любимец хакеров» на сайте <https://prostolinux.ru/kali-linux>.
6. Касперски К. Техника сетевых атак. Приемы противодействия. — М.: Солон.М.Р., 2015. — 397 с.
7. Федотов А.М., Ревнивых А.В. Мониторинг информационной инфраструктуры организации, 2012.
8. Инструменты тестирования KaliLinux. Сетевой сканер Nmap // Электронная версия на сайте <https://kali.tools/?p=1317>.
9. Что такое SIEM-системы и для чего они нужны? // Электронная версия на сайте: <https://www.antimalware.ru/analytics>.
10. Kali Linux Official Documentation // Электронная версия на сайте <https://www.docs.kali.org>.
11. Сканер уязвимостей OpenVas // Электронная версия на сайте: <https://www.kali.org/penetration-testing/openvas-vulnerability-scanning>.

ПРИЛОЖЕНИЕ А

В приложении (А) показан подробный отчет SIEM-системы, которые выявили события, проведенные во время тестирования на проникновения. В ходе сканирования сети на уязвимости, программой OpenVas были выявлены возможные «дыры» в системе безопасности.

Rank	Event Receive Time	Reporting IP	Event Name	Raw Event
1	4/3/19 9:31:05 AM	10.222.110.16	Apache.Expect.Header.XSS	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=09:31:04 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554262264 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740410376 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Expect.Header.XSS" srcport=40853 dstport=80 direction="outgoing" attackid=15229 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID15229" incidentserialno=1762863056 msg="web_server: Apache.Expect.Header.XSS," crscore=10 crlevel="medium"
2	4/3/19 9:31:09 AM	10.222.110.16	HTTP.GET.Request.Directory.Traversal	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=09:31:06 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554262266 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740411096 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.GET.Request.Directory.Traversal" srcport=40915 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=14088 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID14088" incidentserialno=1762863188 msg="misc: HTTP.GET.Request.Directory.Traversal," crscore=10 crlevel="medium"

Продолжение приложения А

Event Receive Time	Reporting IP	Event Name	Raw Event	
3	4/3/19 9:31:47 AM	10.222.110.16	Apache.Expect.Header.XSS	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=09:31:44 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554262304 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740426574 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Expect.Header.XSS" srcport=41365 dstport=443 direction="outgoing" attackid=15229 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID15229" incidentserialno=1294407883 msg="web_server: Apache.Expect.Header.XSS," crscore=10 crlevel="medium"
4	4/3/19 9:32:10 AM	10.222.110.16	HTTP.URI.Script.XSS	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=09:32:07 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554262327 severity="low" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740434684 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.URI.Script.XSS" srcport=41770 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=10574 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10574" incidentserialno=992533908 msg="web_server: HTTP.URI.Script.XSS," crscore=5 crlevel="low"
5	4/3/19 9:33:43 AM	10.222.110.16	Cisco.IOS.HTTP.Remote.Command.Execution	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=09:33:42 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554262422 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740472443 action="dropped" proto=6 service="HTTP" policyid=99 attack="Cisco.IOS.HTTP.Remote.Command.Execution" srcport=49973 dstport=80 direction="outgoing" attackid=30478 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID30478" incidentserialno=1762874725 msg="misc: Cisco.IOS.HTTP.Remote.Command.Execution," crscore=50 crlevel="critical"
6	4/3/19 9:34:22 AM	10.222.110.16	FortiGate-ips-signature-44187	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=09:34:19 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554262459 severity="high" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740488465 action="dropped" proto=6 service="tcp/11001" policyid=99 attack="Java.Debug.Wire.Protocol.Insecure.Configuration" srcport=52738 dstport=11001 direction="outgoing" attackid=44187 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID44187" incidentserialno=992543753 msg="misc: Java.Debug.Wire.Protocol.Insecure.Configuration," crscore=30 crlevel="high"
7	4/3/19 9:34:48 AM	10.222.110.16	Cisco.IOS.HTTP.Remote.Command.Execution	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=09:34:45 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554262485 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740499747 action="dropped" proto=6 service="HTTP" policyid=99

Продолжение приложения А

Rank	Event Receive Time	Reporting IP	Event Name	Raw Event
			Command.Execution	<pre> devid="FGT5HD3915802987" vd="Kazteleport" date=2019- 04-03 time=09:35:48 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554262548 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740524947 action="dropped" proto=6 service="HTTP" policyid=99 attack="Cisco.IOS.HTTP.Remote.Command.Execution" srcport=59015 dstport=80 direction="outgoing" attackid=30478 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID30478" incidentserialno=1294426206 msg="misc: Cisco.IOS.HTTP.Remote.Command.Execution," crscore=50 crlevel="critical" </pre>
9	4/3/19 9:38:44 AM	10.222.110.16	FortiGate-ips- signature- 44544	<pre> <185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019- 04-03 time=09:38:42 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554262722 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740587896 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Tomcat.JSP.File.Information.Disclosure" srcport=33107 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=44544 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID44544" incidentserialno=1294437232 msg="web_server: Apache.Tomcat.JSP.File.Information.Disclosure," crscore=10 crlevel="medium" </pre>
10	4/3/19 9:41:46 AM	10.222.110.16	FortiGate-ips- signature- 44544	<pre> <185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019- 04-03 time=09:41:43 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554262903 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740654821 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Tomcat.JSP.File.Information.Disclosure" srcport=33365 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=44544 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID44544" incidentserialno=992574027 msg="web_server: Apache.Tomcat.JSP.File.Information.Disclosure," crscore=10 crlevel="medium" </pre>
11	4/3/19 9:45:46 AM	10.222.110.16	FortiGate-ips- signature- 44544	<pre> <185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019- 04-03 time=09:45:43 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554263143 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740740841 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Tomcat.JSP.File.Information.Disclosure" srcport=33415 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=44544 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID44544" incidentserialno=1762923372 msg="web_server: Apache.Tomcat.JSP.File.Information.Disclosure," crscore=10 crlevel="medium" </pre>

Продолжение приложения А

Rank	Event Receive Time	Reporting IP	Event Name	Raw Event
			signature-44544	<pre> devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=09:52:43 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554263563 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740895349 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Tomcat.JSP.File.Information.Disclosure" srcport=33503 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=44544 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID44544" incidentserialno=992618850 msg="web_server: Apache.Tomcat.JSP.File.Information.Disclosure," crscore=10 crlevel="medium" </pre>
14	4/3/19 9:55:47 AM	10.222.110.16	FortiGate-ips-signature-44544	<pre> <185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=09:55:44 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554263744 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2740967986 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Tomcat.JSP.File.Information.Disclosure" srcport=33541 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=44544 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID44544" incidentserialno=1762966446 msg="web_server: Apache.Tomcat.JSP.File.Information.Disclosure," crscore=10 crlevel="medium" </pre>
15	4/3/19 9:59:47 AM	10.222.110.16	FortiGate-ips-signature-44544	<pre> <185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=09:59:44 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554263984 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2741058734 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Tomcat.JSP.File.Information.Disclosure" srcport=33586 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=44544 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID44544" incidentserialno=1294525743 msg="web_server: Apache.Tomcat.JSP.File.Information.Disclosure," crscore=10 crlevel="medium" </pre>
16	4/3/19 10:02:47 AM	10.222.110.16	FortiGate-ips-signature-44544	<pre> <185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=10:02:44 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554264164 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2741124096 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Tomcat.JSP.File.Information.Disclosure" srcport=34176 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=44544 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID44544" incidentserialno=992663012 msg="web_server: Apache.Tomcat.JSP.File.Information.Disclosure," crscore=10 crlevel="medium" </pre>

Продолжение приложения А

Rank	Event Receive Time	Reporting IP	Event Name	Raw Event
				<pre>date=2019-04-03 time=11:10:32 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268232 severity="low" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742799383 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.URI.Script.XSS" srcport=46236 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=10574 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10574" incidentserialno=992997852 msg="web_server: HTTP.URI.Script.XSS," crscore=5 crlevel="low"</pre>
19	4/3/19 11:10:49 AM	10.222.110.16	FortiGate-ips-signature-43745	<pre><185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019- 04-03 time=11:10:45 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268245 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742804819 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Exec ution" srcport=46275 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=992998999 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical"</pre>
20	4/3/19 11:10:59 AM	10.222.110.16	FortiGate-ips-signature-43745	<pre><185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019- 04-03 time=11:10:57 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268257 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742810116 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Exec ution" srcport=46285 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=1294876670 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical"</pre>
21	4/3/19 11:11:13 AM	10.222.110.16	FortiGate-ips-signature-43745	<pre><185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019- 04-03 time=11:11:09 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268269 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742815566 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Exec ution" srcport=46296 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=1763337770 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical"</pre>

Продолжение приложения А

Rank	Event Receive Time	Reporting IP	Event Name	Raw Event
23	4/3/19 11:11:35 AM	10.222.110.16	FortiGate-ips-signature-43745	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:11:33 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268293 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742825769 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution" srcport=46316 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=1763339893 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical"
24	4/3/19 11:11:49 AM	10.222.110.16	FortiGate-ips-signature-43745	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:11:46 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268306 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742830599 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution" srcport=46323 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=1763340835 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical"
25	4/3/19 11:12:00 AM	10.222.110.16	FortiGate-ips-signature-43745	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:11:57 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268317 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742835346 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution" srcport=46335 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=1294881931 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical"
26	4/3/19 11:12:12 AM	10.222.110.16	FortiGate-ips-signature-43745	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:12:10 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268330 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742841004 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution" srcport=46344 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=1294883050 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical"

Продолжение приложения А

Rank	Event Receive Time	Reporting IP	Event Name	Raw Event
				resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=1294883939 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execu tion," crscore=50 crlevel="critical"
28	4/3/19 11:12:37 AM	10.222.110.16	FortiGate-ips-signature-43745	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:12:34 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268354 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742850534 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execu tion" srcport=46357 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=1763344688 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical"
29	4/3/19 11:12:49 AM	10.222.110.16	FortiGate-ips-signature-43745	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:12:46 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268366 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742855538 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execu tion" srcport=46363 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=1763345731 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical"
30	4/3/19 11:13:00 AM	10.222.110.16	FortiGate-ips-signature-43745	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:12:58 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268378 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742860973 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execu tion" srcport=46367 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=993010560 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical"
31	4/3/19 11:13:13 AM	10.222.110.16	FortiGate-ips-signature-43745	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:13:10 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268390 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742867256 action="dropped" proto=6 service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execu tion" srcport=46372 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=1763348334 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical"

Продолжение приложения А

Rank	Event Receive Time	Reporting IP	Event Name	Raw Event
33	4/3/19 11:13:38 AM	10.222.110.16	FortiGate-ips-signature-45331	<pre> service="HTTP" policyid=99 attack="Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution" srcport=46379 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=43745 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43745" incidentserialno=993013175 msg="applications3: Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution," crscore=50 crlevel="critical" <185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:13:35 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268415 severity="high" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742878538 action="dropped" proto=6 service="HTTP" policyid=99 attack="EmbedThis.GoAhead.Web.Server.CGI.Remote.Code.Execution" srcport=46386 dstport=80 hostname="91.216.178.115:" direction="outgoing" attackid=45331 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID45331" incidentserialno=993014297 msg="web_server: EmbedThis.GoAhead.Web.Server.CGI.Remote.Code.Execution," crscore=30 crlevel="high" </pre>
34	4/3/19 11:13:48 AM	10.222.110.16	FortiGate-ips-signature-45331	<pre> <185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:13:47 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268427 severity="high" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742883211 action="dropped" proto=6 service="HTTP" policyid=99 attack="EmbedThis.GoAhead.Web.Server.CGI.Remote.Code.Execution" srcport=46395 dstport=80 hostname="91.216.178.115:" direction="outgoing" attackid=45331 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID45331" incidentserialno=1294891833 msg="web_server: EmbedThis.GoAhead.Web.Server.CGI.Remote.Code.Execution," crscore=30 crlevel="high" </pre>
35	4/3/19 11:14:01 AM	10.222.110.16	FortiGate-ips-signature-45631	<pre> <185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:13:59 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268439 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2742888023 action="dropped" proto=6 service="HTTP" policyid=99 attack="Adobe.Coldfusion.BlazeDS.Java.Object.Deserialization" srcport=46399 dstport=80 hostname="91.216.178.115:80" direction="outgoing" attackid=45631 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID45631" incidentserialno=1294892816 msg="applications3: Adobe.Coldfusion.BlazeDS.Java.Object.Deserialization," crscore=50 crlevel="critical" </pre>

Продолжение приложения А

Rank	Event Receive Time	Reporting IP	Event Name	Raw Event
				0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268749 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2743023086 action="dropped" proto=6 service="HTTP" policyid=99 attack="Web.Server.Password.Files.Access" srcport=46488 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=43336 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43336" incidentserialno=1294920746 msg="applications3: Web.Server.Password.Files.Access," crscore=10 crlevel="medium"
38	4/3/19 11:21:16 AM	10.222.110.16	HTTP.Request.URI.Directory.Traversal	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:21:15 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268875 severity="high" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2743072330 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.Request.URI.Directory.Traversal" srcport=46615 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=10604 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10604" incidentserialno=1763390323 msg="web_server: HTTP.Request.URI.Directory.Traversal," crscore=30 crlevel="high"
39	4/3/19 11:22:20 AM	10.222.110.16	HTTP.Request.URI.Directory.Traversal	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:22:18 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554268938 severity="high" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2743098576 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.Request.URI.Directory.Traversal" srcport=46710 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=10604 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10604" incidentserialno=993059264 msg="web_server: HTTP.Request.URI.Directory.Traversal," crscore=30 crlevel="high"
40	4/3/19 11:23:24 AM	10.222.110.16	FortiGate-ips-signature-43336	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:23:22 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554269002 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2743125908 action="dropped" proto=6 service="HTTP" policyid=99 attack="Web.Server.Password.Files.Access" srcport=46735 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=43336 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43336" incidentserialno=1294941906 msg="applications3: Web.Server.Password.Files.Access," crscore=10 crlevel="medium"
41	4/3/19 11:41:43 AM	10.222.110.16	FortiGate-ips-signature-43336	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=11:41:39 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554270099 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2743060643 action="dropped" proto=6 service="HTTP" policyid=99 attack="Web.Server.Password.Files.Access" srcport=56700 dstport=80 hostname="91.216.178.115" direction="outgoing"

Продолжение приложения А

Rank	Event Receive Time	Reporting IP	Event Name	Raw Event
43	4/3/19 12:05:31 PM	10.222.110.16	HTTP.Request.URI.Directo ry.Traversal	<p>0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554270162 severity="medium" srcip=64.39.102.135 srcountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2743634747 action="dropped" proto=6 service="HTTP" policyid=99 attack="Web.Server.Password.Files.Access" srcport=56920 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=43336 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43336" incidentserialno=1295043335 msg="applications3: Web.Server.Password.Files.Access," crscore=10 crlevel="medium"</p> <p><185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019- 04-03 time=12:05:28 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554271528 severity="high" srcip=64.39.102.135 srcountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2744214739 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.Request.URI.Directory.Traversal" srcport=41252 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=10604 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10604" incidentserialno=1763616790 msg="web_server: HTTP.Request.URI.Directory.Traversal," crscore=30 crlevel="high"</p>
44	4/3/19 12:08:39 PM	10.222.110.16	HTTP.Request.URI.Directo ry.Traversal	<p><185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019- 04-03 time=12:08:38 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554271718 severity="high" srcip=64.39.102.135 srcountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2744297264 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.Request.URI.Directory.Traversal" srcport=41448 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=10604 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10604" incidentserialno=1295174040 msg="web_server: HTTP.Request.URI.Directory.Traversal," crscore=30 crlevel="high"</p>
45	4/3/19 12:10:45 PM	10.222.110.16	FortiGate-ips-signature- 43336	<p><185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019- 04-03 time=12:10:44 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554271844 severity="medium" srcip=64.39.102.135 srcountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2744354807 action="dropped" proto=6 service="HTTP" policyid=99 attack="Web.Server.Password.Files.Access" srcport=41524 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=43336 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID43336" incidentserialno=1295185467 msg="applications3: Web.Server.Password.Files.Access," crscore=10 crlevel="medium"</p>

Продолжение приложения А

Rank	Event Receive Time	Reporting IP	Event Name	Raw Event
				0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554271931 severity="medium" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2744390963 action="dropped" proto=6 service="HTTP" policyid=99 attack="NetworkActiv.Web.Server.XSS" srcport=41578 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=34971 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID34971" incidentserialno=1295192576 msg="web_server: NetworkActiv.Web.Server.XSS," crscore=10 crlevel="medium"
48	4/3/19 12:13:55 PM	10.222.110.16	HTTP.Request.URI.Directory.Traversal	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=12:13:53 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554272033 severity="high" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2744436007 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.Request.URI.Directory.Traversal" srcport=41640 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=10604 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10604" incidentserialno=1763661197 msg="web_server: HTTP.Request.URI.Directory.Traversal," crscore=30 crlevel="high"
49	4/3/19 12:14:59 PM	10.222.110.16	HTTP.Request.URI.Directory.Traversal	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=12:14:56 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554272096 severity="high" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2744465897 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.Request.URI.Directory.Traversal" srcport=41676 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=10604 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10604" incidentserialno=1295207607 msg="web_server: HTTP.Request.URI.Directory.Traversal," crscore=30 crlevel="high"
50	4/3/19 12:15:22 PM	10.222.110.16	HTTP.Request.URI.Directory.Traversal	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=12:15:21 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554272121 severity="high" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2744477521 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.Request.URI.Directory.Traversal" srcport=41694 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=10604 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10604" incidentserialno=1763669764 msg="web_server: HTTP.Request.URI.Directory.Traversal," crscore=30 crlevel="high"

Продолжение приложения А

Rank	Event Receive Time	Reporting IP	Event Name	Raw Event
				date=2019-04-03 time=12:20:12 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554272412 severity="high" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2744616115 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.Request.URI.Directory.Traversal" srcport=41861 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=10604 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10604" incidentserialno=1763696772 msg="web_server: HTTP.Request.URI.Directory.Traversal," crscore=30 crlevel="high"
58	4/3/19 12:21:18 PM	10.222.110.16	HTTP.Request.URI.Directory.Traversal	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=12:21:15 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554272475 severity="high" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2744642506 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.Request.URI.Directory.Traversal" srcport=41888 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=10604 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10604" incidentserialno=1763701825 msg="web_server: HTTP.Request.URI.Directory.Traversal," crscore=30 crlevel="high"
59	4/3/19 12:22:21 PM	10.222.110.16	Bsguest.RemoteCommand Execution	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=12:22:18 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554272538 severity="critical" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2744670751 action="dropped" proto=6 service="HTTP" policyid=99 attack="Bsguest.RemoteCommandExecution" srcport=42004 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=12461 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID12461" incidentserialno=1763707605 msg="web_app: Bsguest.RemoteCommandExecution," crscore=50 crlevel="critical"
60	4/3/19 12:24:28 PM	10.222.110.16	HTTP.Request.URI.Directory.Traversal	<185>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802987" vd="Kazteleport" date=2019-04-03 time=12:24:25 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" eventtime=1554272665 severity="high" srcip=64.39.102.135 srccountry="Switzerland" dstip=91.216.178.115 srcintf="Vlan_229_out2" srcintfrole="undefined" dstintf="Vlan_229_in" dstintfrole="undefined" sessionid=2744724115 action="dropped" proto=6 service="HTTP" policyid=99 attack="HTTP.Request.URI.Directory.Traversal" srcport=42250 dstport=80 hostname="91.216.178.115" direction="outgoing" attackid=10604 profile="KTP IPS Policy for web resources" ref="http://www.fortinet.com/ids/VID10604" incidentserialno=1763718313 msg="web_server: HTTP.Request.URI.Directory.Traversal," crscore=30 crlevel="high"

Классификация тестирования на проникновение по источнику анализа:

- внешний – источник анализа системы за пределами защищаемого периметра;
- внутренний – источник анализа системы внутри защищаемого периметра;
- Shadow IT – источники анализа, выпадающие из поля зрения информационных технологий (IP-телефоны или системы видеонаблюдения и т.д.).

В результате проведения тестирования уведомление или отчет должен содержать:

- границы проведения тестирования;
- использованные методы и средства в ходе проведения тестирования;
- описание уязвимостей с оценкой рисков;
- всевозможные сценарии проникновения;
- оценка информационной безопасности компании;
- рекомендации и советы по устранению найденных уязвимостей.

Методы тестирования:

- BlackBox – это метод тестирования без использования аутентификации, без дополнительной информации о web-приложении;
- WhiteBox – это первый метод с дополнением аутентификационной и дополнительной информации предоставляемых компанией (стандартные права доступа);
- GreyBox с результатами прошлого метода – это метод использующий информацию в отчете прошлого аудита, при этом углубленно изучается архитектура, топология сети.

Векторы атаки:

- физический вектор – это атаки с физическим доступом к периметру корпоративной сети;
- сетевой вектор – это атаки задействующие сетевые протоколы, ресурсы;
- беспроводные сети – это атаки на беспроводные сети и протоколы;
- электронная почта – это атаки на электронную почту (задействованы элементы социальной инженерии);
- мобильные устройства/приложения – это атаки на мобильные устройства и приложения;
- приложения – это атаки на приложения заказчика (web-приложения, web-портал и т.д.);
- социальная инженерия – это атаки основанные на социальной инженерии.

Основные этапы тестирования на проникновение:





- подготовительный – это заключение договора между сторонами. В этом этапе разъясняется цель тестирования, к каким данным предоставляется доступ, в каком виде будет представлен отчет и т.д.;
- сбор необходимой информации – это сбор необходимой информации о сетевой инфраструктуре, информации о всевозможной защите, стоящей по периметру и не только, разведданные и т.д.;
- анализ уязвимостей – это выявление уязвимостей и их эксплуатация;
- этап эксплуатации – это этап эксплуатации, а именно полученные данные собираются, мониторятся и выстраивается план действий;
- формирование отчета – это этап обобщения всей информации со всех предыдущих этапов, с добавлением результатов тестирования и решений по их закрытию.

Метрики/оценки уязвимостей:

- базовая метрика – это отображение базовой характеристики уязвимости (не зависящей от времени и среды);
- временная метрика – это отображение временных характеристик (не зависящих от среды);
- контекстная метрика – это уникальные характеристики в контексте (зависящие от пользовательской среды).

Внешний пентест делится на категории:

- сетевые сканеры;
- эксплойтинг;

					Дипломный проект		
					Лист	Масса	Масштаб
Изм.	Лист	Ф.И.О	Подп.	Дата	Тестирование на проникновение		
Разработал	Тазабеков.Ш.		13.05				
Нормоконтр	Зиро А.		13.05				
Руководитель	Айтхожаева Е.		13.05				
Зав. каф.	Сейлова Н.		13.05	Тема: Мониторинг безопасности сети на основе тестирования на проникновение			
					Лист 1	Листов 4	
					КазНИТУ ИИиТТ КБОиХИ 5В100200		

Лог инцидента в SIEM

Event Details

```
<189>logver=56 devname="InternetShield_Dostyk" devid="FGT5HD3915802967"
wi="kazteleport" date=2019-05-10 time=05:57:47 logid="000000013" type="traffic"
subtype="forward" level="notice" eventtime=1557446262 srcip=196.52.43.131
srcport=51562 srcintf="Vlan_229_out2" srctnrole="undefined" dstip=91.216.178.81
dstport=161 dstintf="Vlan_229_in" dstnrole="undefined" poluid="57fd2312-fb90-
51e8-442c-0946a5c7b4de" sessionid=3573218234 proto=17 action="accept" policyid=30
policytype="policy" service="SMB" dstcountry="Kazakhstan" srccountry="Netherlands"
```

Search... Lines: 62

Item	Value
Application Group Name	unscanned
Collector ID	1
Count	1
Destination Country	Kazakhstan
Destination Host Name	HOST-91.216.178.81
Destination IP	91.216.178.81
Destination Interface Name	Vlan_229_in
Destination Latitude	48
Destination Longitude	68
Destination Organization	JSC Accumulating Pension Fund of Halyk Bank of Kaz
Destination TYP//IPC Port	T41 (SMB)

Close





Виджет временного диапазона

Security Incidents: HIGH: 222 MEDIUM: 178 LOW: 14

Time Range: Last 24 Hours

Last Occurred	Routing	Source	Target	Detail	Incident	Incident Status
May 13 2019, 11:22:02 AM	ASA_Acl-500by_CTK-7	Source Country: Russia		Triggered Event Count: 513	Excessive Denied Connections From An External Country	Active
May 13 2019, 11:20:30 AM	DC_Client-InternetShield_Dostyk			Triggered Event Count: 510	Excessive Denied Connections From An External Country	Active
May 13 2019, 11:18:30 AM	InternetShield_Dostyk	177.30.183.166		Total Flows: 2291 Total Bytes: 16.07 MB Avg Total Flows: 1141.35 Std Dev Total Flows: 164.57 Avg Total Bytes: 2.3 MB Std Dev Total Bytes: 4.6 MB	Sudden Increase in Traffic From Host	Open 14
May 13 2019, 11:16:30 AM	InternetShield_Masachy	10.228.133.10	10.222.118.15	Triggered Event Count: 12	Multiple Login Failures: Misc App	Open 1,849
May 13 2019, 11:17:00 AM	InternetShield_Dostyk	77.220.207.213	31.31.217.99	Component Event Type: Fortigate-ips-anomaly-100663 Attack Name: C02_SMB_Host Triggered Event Count: 2	High severity inbound permitted IPS Exploit	Open 6
May 13 2019, 11:14:30 AM	dc.kazteleport.kz		dc.kazteleport.kz 10.222.0.50	Count: 10 Avg Matched Events: 4.00	Sudden Increase in Failed Logins To A Host	Open 106
May 13 2019, 11:14:30 AM	dc2.kip.loc		dc2.kip.loc 10.222.1.103	Count: 47 Avg Matched Events: 30.93	Sudden Increase in Failed Logins To A Host	Open 179
May 13 2019, 11:08:30 AM	ASA_Acl-500by_CTK-7;InternetShield_Dostyk	Source Country: Kazakh		Triggered Event Count: 522	Excessive Denied Connections From An External Country	Open 3,596
May 13 2019, 11:07:00 AM	InternetShield_Dostyk	10.0.108.18		Total Flows: 258 Total Bytes: 7.78 MB Avg Total Flows: 75.27 Std Dev Total Flows: 57.41 Avg Total Bytes: 800.28 KB Std Dev Total Bytes: 1.87 MB	Sudden Increase in Traffic From Host	Open 29
May 13 2019, 11:02:00 AM	ASA_Acl-500by_CTK-7	10.222.0.8		Triggered Event Count: 29	Excessive End User Mail	Open 176

Copyright © 2019 Palo Alto Networks, Inc. All rights reserved. Organization: Topnet Users: admin@topnet.kz Topnet Global Powered by Arc42, A Palo Alto Networks Company

<h1>Дипломный проект</h1>							
					Лист	Масса	Масштаб
Изм.	Лист	Ф.И.О	Подп.	Дата	Функциональные возможности SIEM-системы Тема: Мониторинг безопасности сети на основе тестирования на проникновение		
	Разработал	Тазабеков.Ш.		13.05			
	Нормоконтр	Зиро А.		13.05			
	Руководитель	Айтхожаева Е.		13.05			
	Зав. каф.	Сейлова Н.		13.05	Лист 2		Листов 4
					КазНИТУ ИИиТТ КБОУХИ 5В100200		

Запуск сканирования через командную строку Kali Linux

```

root@kali: /home/madi
root@kali:/home/madi# openvas-start
[*] Please wait for the OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● greenbone-security-assistant.service - Greenbone Security Assistant
   Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2019-04-30 08:44:27 CDT; 1min 9s ago
     Docs: man:gsad(8)
           http://www.openvas.org/
   Main PID: 1808 (gsad)
     Tasks: 4 (limit: 4514)
    Memory: 4.3M
   CGroup: /system.slice/greenbone-security-assistant.service
           └─1808 /usr/sbin/gsad --foreground --listen=127.0.0.1 --port=9392 --mlisten=127.0.0.1 --mport=9398
           └─1811 /usr/sbin/gsad --foreground --listen=127.0.0.1 --port=9392 --mlisten=127.0.0.1 --mport=9398

Apr 30 08:44:27 kali systemd[1]: Started Greenbone Security Assistant.
Apr 30 08:44:28 kali gsad[1808]: Warning: MHD USE THREAD PER CONNECTION must be used only with MHD_USE_INTERNAL_POLLING_THREAD. Flag MHD_USE_INTERNAL_POLLING_THREAD was added. Consider setting MHD_USE_INTERNAL_POLLING_THREAD explicitly.
Apr 30 08:44:28 kali gsad[1808]: Warning: MHD USE THREAD PER CONNECTION must be used only with MHD_USE_INTERNAL_POLLING_THREAD. Flag MHD_USE_INTERNAL_POLLING_THREAD was added. Consider setting MHD_USE_INTERNAL_POLLING_THREAD explicitly.

● openvas-scanner.service - Open Vulnerability Assessment System Scanner Daemon
   Loaded: loaded (/lib/systemd/system/openvas-scanner.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2019-04-30 08:45:31 CDT; 5s ago
     Docs: man:openvassd(8)
           http://www.openvas.org/
   Process: 1818 ExecStart=/usr/sbin/openvassd --unix-socket=/var/run/openvassd.sock (code=exited, status=0/SUCCESS)
   Main PID: 1839 (openvassd)
     Tasks: 3 (limit: 4514)
    Memory: 97.9M
   CGroup: /system.slice/openvas-scanner.service
           └─1839 /usr/sbin/openvassd --unix-socket=/var/run/openvassd.sock
    
```

Список уязвимостей для двух выделенных IP-адресов

Vulnerability	Severity	QoD	Host	Location	Actions
PHP [php_stream_scandir()] Buffer Overflow Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	4080tcp	
PHP [php_stream_scandir()] Buffer Overflow Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	443tcp	
PHP 'type confusion' Denial of Service Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	4080tcp	
PHP 'type confusion' Denial of Service Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	443tcp	
PHP [php_fix_filepath()] Function Stack Buffer Overflow Vulnerability - Mar15 (Windows)	10.0 (High)	80%	10.7.63.223	4080tcp	
PHP [php_fix_filepath()] Function Stack Buffer Overflow Vulnerability - Mar16 (Windows)	10.0 (High)	80%	10.7.63.223	443tcp	
PHP [com_print_typeinfo()] Remote Code Execution Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	4080tcp	
PHP [com_print_typeinfo()] Remote Code Execution Vulnerability (Windows)	10.0 (High)	80%	10.7.63.223	443tcp	
PHP Multiple Vulnerabilities - Sep11 (Windows)	10.0 (High)	90%	10.7.63.223	4080tcp	
PHP Multiple Vulnerabilities - Sep11 (Windows)	10.0 (High)	80%	10.7.63.223	443tcp	
PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)	10.0 (High)	80%	10.7.63.223	4080tcp	
PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)	10.0 (High)	80%	10.7.63.223	443tcp	
PHP Multiple Vulnerabilities - 05 - Aug16 (Windows)	10.0 (High)	90%	10.7.63.223	4080tcp	
PHP Multiple Vulnerabilities - 05 - Aug16 (Windows)	10.0 (High)	80%	10.7.63.223	443tcp	
PHP End Of Life Detection (Windows)	10.0 (High)	90%	10.7.63.223	4080tcp	
PHP End Of Life Detection (Windows)	10.0 (High)	80%	10.7.63.223	443tcp	
PHP Multiple Vulnerabilities - Dec18 (Windows)	10.0 (High)	80%	10.7.63.223	4080tcp	
PHP Multiple Vulnerabilities - Dec18 (Windows)	10.0 (High)	80%	10.7.63.223	443tcp	
PHP Denial of Service Vulnerability Jul17 (Windows)	10.0 (High)	90%	10.7.63.223	4080tcp	
PHP Denial of Service Vulnerability Jul17 (Windows)	10.0 (High)	80%	10.7.63.223	443tcp	
Kerio Personal Firewall Admin Service	7.9 (High)	70%	10.7.63.223	4433tcp	
Kerio Winroute Firewall Admin Service	7.9 (High)	75%	10.7.63.223	4433tcp	
PHP Multiple Vulnerabilities - Feb19 (Windows)	7.9 (High)	80%	10.7.63.223	4080tcp	
PHP Multiple Vulnerabilities - Feb19 (Windows)	7.9 (High)	80%	10.7.63.223	443tcp	
PHP Multiple Vulnerabilities - 02 - Sep16 (Windows)	7.9 (High)	80%	10.7.63.223	4080tcp	
PHP Multiple Vulnerabilities - 02 - Sep16 (Windows)	7.9 (High)	80%	10.7.63.223	443tcp	
PHP Multiple Vulnerabilities - 05 - Jul16 (Windows)	7.9 (High)	80%	10.7.63.223	4080tcp	

Дипломный проект

						Лист	Масса	Масштаб
Изм.	Лист	Ф.И.О	Подп.	Дата	Сканирование сетевыми сканерами			
Разработал		Тазабеков.Ш.	<i>[Signature]</i>	13.05				
Нормоконтр		Зиро А.	<i>[Signature]</i>	13.05				
Руководитель		Айтхожаева Е.	<i>[Signature]</i>	13.05		Лист 3	Листов 4	
Зав. каф.		Сейлова Н.	<i>[Signature]</i>	13.05				
					Тема: Мониторинг безопасности сети на основе тестирования на проникновение			КазНИТУ ИИиТТ КБоиХИ 5В100200

