Евгений А. Басыня[1, 2]
[1] Новосибирский государственный технический университет,
просп. К. Маркса, 20, г. Новосибирск, 630073, Россия
[2] Научно-исследовательский институт информационно-коммуникационных технологий,
ул. Депутатская, 48, г. Новосибирск, 630099, Россия
e-mail: director@nii-ikt.ru, https://orcid.org/0000-0003-3916-7783

РАСПРЕДЕЛЕННАЯ СИСТЕМА СБОРА, ОБРАБОТКИ И АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

DOI: http://dx.doi.org/10.26583/bit.2018.4.04

Аннотация. Большинство сетевых инфраструктур государственных учреждений и частных предприятий функционируют на базе стека протоколов TCP/IP, обладающего существенными уязвимостями. В качестве примера стоит привести отсутствие проверки подлинности субъекта взаимодействия в базовых протоколах и технологиях данного стека. Часть уязвимостей можно устранить интеллектуальными функциями управляемого сетевого оборудования: от профилирования доступа до сегментации трафика. Немаловажным звеном защиты выступают комплексные межсетевые экраны, включающие системы обнаружения и предотвращения вторжений. Российскими и зарубежными учеными развиваются методы сигнатурного, эвристического, поведенческого, автомодельного, прогнозируемого и других способов анализа сетевого трафика и идентификации сетевых угроз. Однако предлагаемые решения не дают однозначного результата при использовании оверлейных технологий и криптографических протоколов. Также не уделяется надлежащее внимание обработке, анализу сетевого трафика и логов операционных систем Windows/Linux и приложений. Целью данной работы являлось исследование, разработка и программная реализация распределенной системы сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия. Ключевой задачей ставилось обеспечение объективного мониторинга сетевой информационной безопасности. Дополнительной задачей являлось обеспечение мониторинга работы пользователей персональных компьютеров под управлением операционных систем Windows и Linux. Для решения поставленной задачи была разработана концепция комплексной обработки трафика вычислительной сети и событий информационной безопасности как на стороне сервера, так и на стороне клиента. На обзор вынесен оригинальный сигнатурный и статистический метод составления базы знаний системы посредством тестирования и имитации известных сетевых и локальных атак с отслеживанием реакции операционных систем и приложений в среде виртуализации. Изложен подход к выполнению автоматизированного анализа коррелирующих событий с применением глубокого анализа содержимого пакетов и мониторинга локальной работы пользователей. Предложенное решение успешно апробировано и использовано в качестве одного из модулей обеспечения сетевой информационной безопасности системы интеллектуально-адаптивного управления сетевой инфраструктурой предприятия, разрабатываемой автором.

Ключевые слова: IDS, IPS, SIEM, анализ событий информационной безопасности, мониторинг работы сети и пользователей.

Для цитирования: БАСЫНЯ, Евгений А. РАСПРЕДЕЛЕННАЯ СИСТЕМА СБОРА, ОБРАБОТКИ И АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 42-51, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1160>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.04.

Evgeny A. Basinya[1, 2]
[1]Novosibirsk State Technical University,
20 K. Marx Street, Novosibirsk, 630073, Russia
[2]Research Institute of Information and Communications Technologies,
48 Deputatskaya Street, Novosibirsk, 630073, Russia
e-mail: director@nii-ikt.ru, https://orcid.org/0000-0003-3916-7783

Distributed system of collecting, processing and analysis of security information events of the enterprise network infrastructure

DOI: http://dx.doi.org/10.26583/bit.2018.4.04

Abstract. The majority of the network infrastructures of government agencies and private enterprises operate on the basis of a TCP/IP protocol stack, which has significant vulnerabilities. For illustrative purposes, it is worth mentioning the lack of verification of the interaction subject authenticity in the basic protocols and technologies of this stack. Some of the TCP/IP stack vulnerabilities can be eliminated by the intelligent functions of managed network devices: from access profiling to traffic segmentation. Complex firewalls, which include intrusion detection and prevention systems, are also an important element of the network protection. Methods of signature, heuristic, behavioral, self-similar, predictable and other approaches for analyzing network traffic and identifying network threats are further being developed by Russian and foreign scientists. However, the proposed solutions do not give an unambiguous result when using overlay technologies and cryptographic protocols. Also, due attention is not being paid to the processing, analysis of network traffic and logs of Windows/Linux operating systems and applications. The aim of this work was the research, development and software implementation of a distributed system for collecting, processing and analyzing security information events of an enterprise network infrastructure. The key task was to ensure objective monitoring of network information security. An additional task was to ensure the monitoring of the activity of users of personal computers running Windows and Linux operating systems. In order to address this challenge, a concept for complex processing of computer network traffic and security information events both on the server and on the client sides was developed. An original signature and statistical method of compiling the knowledge base system by testing and simulating known network and local attacks with tracking the response of operating systems and applications in a virtualization environment is reviewed. The approach to performing the automated analysis of correlating events with the use of deep packets inspection (DPI) and monitoring of users' local activity is described. The reviewed solution was successfully tested and used as one of the modules for providing network information security of the system for intelligent adaptive enterprise network infrastructure management, designed by author.

Keywords: IDS, IPS, SIEM, security information events analysis, user and network activity monitoring.
For citation: BASINYA, Evgeny A. Distributed system of collecting, processing and analysis of security information events of the enterprise network infrastructure. IT Security (Russia), [S.l.], v. 25, n. 4, p. 42-51, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1160>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.04.

Введение

Одним из приоритетных направлений развития науки, технологий и техники в Российской Федерации выступают информационно-коммуникационные технологии, оказывающие существенное влияние на уровень национальной безопасности и экономической конкурентоспособности государства. Большинство сетевых инфраструктур государственных учреждений и частных предприятий функционируют на базе стека протоколов TCP/IP с использованием технологии канального уровня Ethernet, а также имеют доступ к глобальной вычислительной сети Интернет. С каждым годом возрастает количество и уровень изощренности кибернетических атак. Злоумышленники, мотивированные целью получения материальной выгоды, предпринимают попытки вывести из состояния доступности или получить несанкционированный доступ к информационным системам и вычислительным сетям, что потенциально может нанести существенный экономический ущерб компании и (в худшем случае) ущерб суверенитету, территориальной целостности, политической и социальной стабильности страны.

Соответственно, возрастает актуальность задачи обеспечения информационной безопасности сетевых инфраструктур предприятий. Стоит отметить несовершенство стека протоколов TCP/IP: так в базовых протоколах и технологиях отсутствуют проверки подлинности субъекта взаимодействия (не введены процедуры идентификации, аутентификации и авторизации). В качестве примера стоит привести возможность использования ложных ARP-ответов (англ. Address Resolution Protocol — протокол определения адреса) и фальсифицированных сообщений протоколов маршрутизации и управления сетью. Часть уязвимостей стека можно устранить интеллектуальными

функциями управляемого сетевого оборудования: от профилирования доступа до сегментации трафика. Но одним из ключевых звеньев защиты локальной вычислительной сети выступает комплексный межсетевой экран. Как правило, в его состав входит система обнаружения и предотвращения вторжений (англ. IDS/IPS, Intrusion detection system / Intrusion prevention system). Подобные системы могут функционировать на уровне приложения, хоста или сети. Сбор трафика зачастую осуществляется с каждого сегмента сети посредством агентов/датчиков, подключенных к коммутаторам/маршрутизаторам на зеркалируемый порт (англ. port mirroring). Российскими и зарубежными учеными развиваются методы сигнатурного, эвристического, поведенческого, автомодельного, прогнозируемого и других анализов сетевого трафика и идентификации сетевых угроз. Данными исследованиями занимаются: Ходашинский И.А., Мещеряков Р.В., Рубанов С.А., Тимонина А.А., Тимонина Е.Е., Половко И.Ю., Пескова О.Ю., Сычев М.П., Ефимов А.Ю., Бурлаков М. Е., Бондяков А.С. и многие другие ученые. [1 - 7]

Заслуживающими внимания положительными тенденциями являются: организация работы IDS/IPS на основе встраиваемых микропроцессорных систем и технологии data mining [8 - 9], а также консолидация IDS/IPS и систем управления безопасностью и событиями (англ. SIEM, Security information and event management) [10 - 15]. Импортозамещение иностранных технологий и продуктов в данной сфере является приоритетным направлением развития российской науки. [16]

Однако предлагаемые методики не дают однозначного результата при использовании оверлейных технологий и криптографических протоколов, а также не уделяют надлежащего внимания обработке, анализу сетевого трафика и логов операционных систем (ОС) семейства Windows/Linux и приложений.

Немаловажной функциональной проблемой комплексных межсетевых экранов выступает отсутствие возможности формирования объективных отчетов и статистики о деятельности пользователя, особенно при использовании средств анонимизации (например, сети TOR <англ. The Onion Router>). Существенным недостатком является отсутствие взаимодействия следующих решений: IDS/IPS, SIEM, систем контроля работы пользователей, систем поддержки принятия решений по вопросам администрирования и информационной безопасности, что приводит к нерентабельному избыточному потреблению вычислительных ресурсов сервера, дублированию ряда информационных блоков.

1. Постановка задачи

Целью данной работы являлось исследование, разработка и программная реализация распределенной системы сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия. Задачей ставилось обеспечение объективного мониторинга сетевой информационной безопасности и работы пользователей персональных компьютеров под управлением операционных систем Windows и Linux. Предложенное решение будет использовано в качестве модуля систем обеспечения сетевой информационной безопасности комплексного интеллектуально-адаптивного шлюза, разрабатываемого автором.

2. Теория и практика

На сегодняшний день широкое распространение получили средства сетевой анонимизации: прокси-серверы, виртуальные защищенные каналы связи и виртуальные частные сети (англ. Virtual Private Network), оверлейные сети на базе луковой и чесночной маршрутизации. Данные инструменты позволяют пользователям посещать любые информационные ресурсы в обход правил фильтрации межсетевых экранов, в том числе UTM-шлюзов безопасности (англ. Unified threat management) и NGFW (англ. Next generation firewall).

Используя оверлейную сеть TOR, пользователь может посетить целевой информационный ресурс через цепочку из трех и более случайных прокси-серверов/нодов (входного, промежуточных и выходного), с каждым из которых он обменивается ключами

и шифрует исходную информацию последовательно ключами от выходного до входного нодов, оставляя открытой лишь полезную часть заголовка пакетов для выполнения следующей трансляции информационного потока. Осуществляется многослойное шифрование и продвижение трафика по цепочке нодов, именуемое луковой маршрутизацией. Соответственно, межсетевой экран способен установить факт взаимодействия пользователя с входной нодой сети TOR, но идентифицировать целевой (посещаемый) информационный ресурс и дешифровать/проанализировать трафик не может. Тем самым пользователь может успешно обойти правила фильтрации трафика.

Одним из методов противодействия выступает механизм цифровых подписей и сертификации всех процессов операционной системы и устанавливаемых приложений. Альтернативным методом является установка корневых сертификатов в систему и ввод дополнительных средств разграничения прав доступа. Описанные подходы позволят предотвратить установку нежелательного программного обеспечения пользователями, а также дешифровывать и анализировать сетевой трафик хостов на стороне шлюза/межсетевого экрана. Стоит отметить существенный недостаток использования данных методик в гражданской сфере: работа рядового пользователя за персональным компьютером утрачивает гибкость, простоту и удобство взаимодействия с операционной системой, ограничивается по функциональности и требует постоянного вмешательства квалифицированного специалиста. Подмена корневых сертификатов в ряде стран является неэтичной и трактуется как попытка внедрения тоталитарного контроля, посягающего на свободу слова.

Задача сбора и анализа логов операционных систем и приложений может представляться тривиальной и простой. Однако стоит привести простой пример. Пользователь хоста А подключается к хосту Б с использованием протокола удаленных рабочих столов RDP (англ. Remote Desktop Protocol). Оба узла функционируют на базе операционной системы семейства Windows (версии 7 и выше). Системному администратору ставится задача установления времени пребывания пользователя хоста А на узле Б. Разумеется, специалист обращается к логам журнала событий EVTX (англ. XML EventLog, новый формат журнала Microsoft). Во вкладке «безопасность» он обнаруживает 48 событий входа/выхода пользователя в систему с идентичными кодами событий. При этом фактически пользователь находился в системе лишь один час пятнадцать минут, был произведен лишь один вход и один выход из системы с использованием протокола RDP, локальных действий не производилось. Подобных примеров можно привести большое количество, что отражает трудоемкость процесса сбора и анализа объективной информации о событиях сетевой инфраструктуры, в том числе и о работе пользователей за персональными компьютерами на базе операционных систем семейства Windows/Linux при использовании.

Для решения данных проблем было решено разработать распределенную систему сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия. Данная система проектировалась как модуль системы интеллектуально-адаптивного управления сетевой инфраструктурой предприятия, разрабатываемой автором (рис. 1).

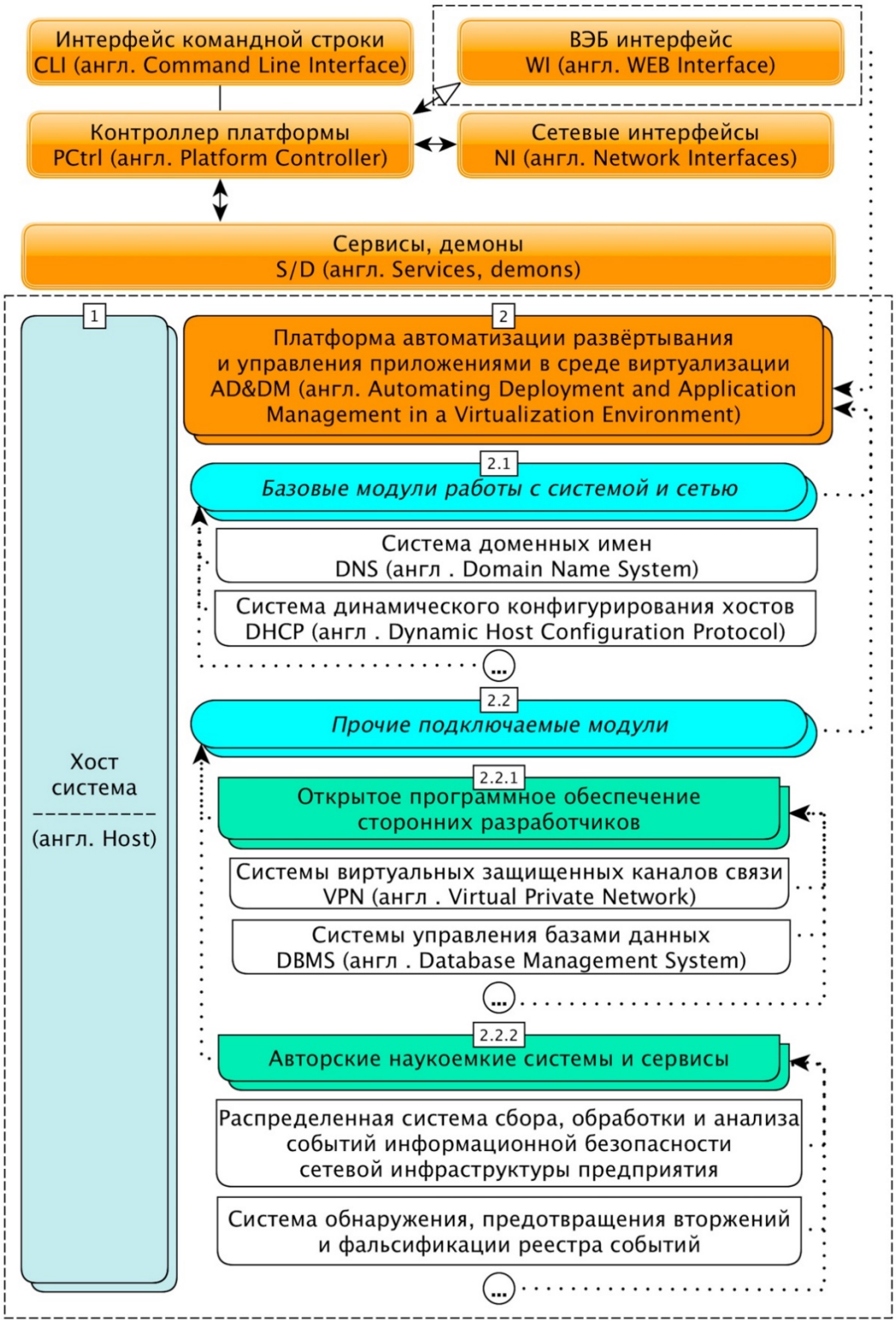

Рис. 1. Архитектура серверной части системы
(Fig. 1. Architecture of the server part of the system)

Архитектура серверной части выполнена с использованием платформы автоматизации развёртывания и управления приложениями в среде виртуализации, что обеспечивает дополнительную надежность и отказоустойчивость решения.

При проектировании функционала клиентской части приложения, устанавливаемой на персональные компьютеры пользователей было предложено совместить в едином продукте шесть оригинальных разработок, представленных на рис. 2.

Рис. 2. Диаграмма компонентов клиентского программного обеспечения комплексного интеллектуально-адаптивного шлюза
(Fig. 2. Diagram of the client software components of the integrated intelligent adaptive gateway)

Данная диаграмма иллюстрирует пересечение функционала систем. Приведем простой пример. Система интеллектуального контроля и управления доступом к информационным ресурсам ПК блокирует подключение сторонних USB-носителей, подключение к сетям не из списка доверенных, несанкционированную отправку информации через файлообменники или почтовые сервисы, проверяет наличие секретного устройства в зоне действия локальной вычислительной сети и Bluetooth-метки, анализирует клавиатурный почерк и задействует 2d-распознавание лица.

Система мониторинга работы пользователей персональных компьютеров отслеживает активность работы пользователя в различных приложениях, анализируя нажатия клавиш, движения мыши и идентифицируя системы фальсификации деятельности пользователя. Изучает интернет-серфинг пользователя, проверяя доступность HTTPS протокола (англ. HyperText Transfer Protocol Secure) посещаемых ресурсов (в том числе отдельных блоков сайтов) и рекомендуя его использовать.

Автоматизированная система сетевого и системного администрирования ОС семейства Windows организует систему заявок между пользователем и администратором, а также в автоматическом режиме решает широкий спектр проблем. Обрабатывает логи операционных систем и приложений, мониторит сетевую активность.

Соответственно, функционал обработки, анализа логов и сетевого трафика является неотъемлемой частью всех приведенных на рис. 2 компонентов, которые должны взаимодействовать с серверной частью системы интеллектуально-адаптивного управления сетевой инфраструктурой предприятия, в том числе выполняющей функцию комплексного межсетевого экрана.

Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия выполняет следующие функции:

На стороне клиента:

1) сбор и локальную обработку логов операционной системы по сигнатурному методу;
2) сбор и локальную обработку логов установленного программного обеспечения по сигнатурному методу;
3) анализ всего трафика, обрабатываемого хостом, с использованием технологии глубокого анализа содержимого дейтаграмм DPI (англ. Deep Packet Inspection);
4) мониторинг работы пользователей в системе и различных приложениях;
5) идентификацию и блокировку приложений, фальсифицирующих активность пользователя;
6) мониторинг работы каждого запущенного процесса, изучение генерируемого им трафика;
7) составление модели поведения пользователей и процессов, задействование методов поведенческого принципа и идентификации аномалий;
8) корреляционный и статистический анализ всей собираемой информации;
9) предоставление функционала изолированной среды тестирования и изучения каждой единицы устанавливаемого программного обеспечения, так называемой песочницы;
10) работа с полученной базой знаний от сервера и формирование собственных знаний системы на основе получаемого опыта;
11) взаимодействие с серверной частью от отправки всей собранной информации до получения команд и обновления базы знаний/компонентов системы.

Под обработкой логов подразумевается не только парсинг, но и идентификация, структуризация, ранжирование и объединение событий. Так, в приведенном ранее примере удаленного подключения к хосту Б по протоколу RDP из 48 событий операционной системы было составлено 1 корректное.

Функционал «песочницы» позволяет отслеживать поведение программного обеспечения: к каким файлам, ресурсам, оборудованию и веткам реестра (в случае использования хостом ОС Windows) обращается источник, какой трафик генерирует, отправляет ли в скрытом режиме информацию, имеет ли не задекларированные правообладателем функции.

На стороне сервера выполняются следующие действия:

1) локальный сбор и обработка логов серверной операционной системы по сигнатурному методу;
2) локальный сбор и обработка логов установленного серверного программного обеспечения по сигнатурному методу;
3) анализ локального трафика, обрабатываемого сервером, с использованием технологии глубокого анализа содержимого дейтаграмм DPI;
4) сбор с клиентов обработанных логов операционной системы;
5) сбор с клиентов обработанных логов программного обеспечения;
6) сбор с клиентов информации об обработанном ими трафике;
7) сбор с клиентов выработанных знаний системы на основе полученного опыта;
8) формирование основной базы знаний системы на основе оригинального сигнатурного и статистического метода;
9) расширение базы знаний системы;
10) корреляционный и статистический анализ всей собираемой информации;
11) управление клиентами.

Полученные знания разными клиентами в штатном режиме работы вносятся в общую базу лишь при аналогичных результатах от 50 % клиентов с аналогичным

установленным программным обеспечением, при этом минимальное количество хостов составляет десять единиц.

Для составления основной базы знаний системы был разработан оригинальный сигнатурный и статистический метод, реализован фреймворк, который в свою очередь использовался для написания программы «Researcher» по тестированию систем и имитации известных сетевых и локальных атак с отслеживанием реакции операционных систем и приложений в среде виртуализации на модельных объектах.

В базу знаний программы внесены официально известные уязвимости операционных систем семейства Windows/Linux, популярных программных продуктов и вычислительных сетей, а также добавлены существующие или написанные самостоятельно эксплойты (программные реализации осуществления атаки на объект, имеющий определенную уязвимость).

Для проведения исследований на выделенном сервере устанавливается и конфигурируется гипервизор, настраивается виртуальная сетевая инфраструктура. Далее создаются модельные объекты в виде виртуальных машин с различными операционными системами и набором программного обеспечения. Для автоматизации развертки и конфигурирования решений на базе Linux с введением дополнительного слоя изоляции задействуются Docker-контейнеры и Ansible скрипты, на базе Windows – система эталонного образа и контейнеризации программ, включая «песочницы». На модельные объекты производится установка разработанного клиентского программного обеспечения. Соответственно, моделируется полноценная сетевая инфраструктура предприятия. Для восстановления начального, эталонного состояния виртуальной машины используется технология снапшотов (снимков системы).

Далее запускается программа «Researcher». Сначала со стороны виртуальной локальной сети, затем снаружи, за виртуальным межсетевым экраном. Итерационно задействуются механизмы активного и пассивного анализа трафика вычислительной сети и информационных ресурсов (сканирование, зондирование, пентестинг) по отношению к каждому модельному объекту. Клиенты модельных объектов «снимают показания» в виде логов и трафика, передают их серверу, где математический аппарат выявляет корреляцию событий по каждой атаке, составляет «слепок» поведения операционной системы и программного обеспечения в зависимости от проведенного внешнего возмущения. Количество итераций по выполнению одной процедуры (например, выполнению эксплойта) на чистый модельный объект составляет не менее 10 и может вручную задаваться администратором. Таким образом формируется основная база знаний системы.

Программная реализация серверной части была выполнена с использованием Python, Flask, C++, Bash, Docker, Ansible на ОС Alpine Linux. Клиентский модуль под ОС Windows написан на языке программирования C# с использованием native controls из .NET библиотеки Windows Forms, а под Linux использовался Python и Qt-фреймворк.

Для проверки работоспособности было выполнено ручное и автоматизированное тестирование разработанного программного продукта (клиентской и серверной части, а также их взаимодействия).

Далее был проведен эксперимент по определению эффективности предложенного подхода, объективно предоставляющего информацию даже при использовании пользователями средств анонимизации: на сотне компьютеров сотрудниками компании, принявшей участие в эксперименте, в ручном режиме были установлены и запущены: Tor и I2P браузеры, OpenVPN клиент с подключением к коммерческому VPN сервису. С использованием этих инструментов пользователи посещали различные информационные ресурсы, каждое посещение было зафиксировано разработанным клиентским программным обеспечением, информация успешно отправлялась на серверную часть. При этом сторонние комплексные межсетевые экраны с задачей не справились, т.к. не были установлены корневые сертификаты и дополнительные средства разграничения прав доступа.

Затем в рамках этой же сетевой инфраструктуры была исследована загрузка каналов связи предложенной системы в сравнении со стандартным методом сбора логов системами обнаружения и предотвращения вторжений, системами управления безопасностью (Snort, Suricata, Bro, OSSEC, ELK, LightSIEM и др.). Длительность эксперимента составила два месяца. Уменьшение загрузки каналов связи трафиком рассматриваемых продуктов при прочих условиях составило 12–47 % при использовании разработанной системы (при этом информативность была улучшена). Однако существенным недостатком выступило использование больших вычислительных мощностей: от 16 до 39 %. При этом важно отметить, что функционал системы значительно шире в сравнении с существующими решениями в комплексе. Работа по оптимизации системы продолжается.

Заключение

В рамках данного исследования была разработана и программно реализована система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия, функционирующая на основе оригинального сигнатурного и статистического метода по составлению базы знаний системы посредством тестирования и имитации известных сетевых и локальных атак с отслеживанием реакции операционных систем и приложений в среде виртуализации на модельных объектах. Изложен подход к выполнению автоматизированного анализа коррелирующих событий в совокупности с модулями глубокого анализа содержимого пакетов DPI (англ. Deep Packet Inspection) и мониторинга локальной работы пользователей. Предложена концепция комплексной обработки трафика вычислительной сети и событий информационной безопасности как на стороне сервера, так и на стороне клиента. Недостатком программной реализации предложенного решения является потребление вычислительных мощностей на стороне клиента на 16–39 % больше в сравнении с альтернативными продуктами. Что выступает ценой за расширенный функционал и использование языка программирования Python. Предложенное решение использовано в качестве одного из модулей обеспечения сетевой информационной безопасности системы интеллектуально-адаптивного управления сетевой инфраструктурой предприятия, разрабатываемой автором.

СПИСОК ЛИТЕРАТУРЫ:

1. Ходашинский И.А., Мещеряков Р.В., Рубанов С. А. Гибридная система обнаружения вторжений на базе нечеткого классификатора с использованием жадного и генетического алгоритмов // Вопросы защиты информации. 2013. № 4(102). С. 67 – 72.
2. Тимонина А.А., Тимонина Е.Е. Атаки на централизованные системы обнаружения вторжений // Системы и средства информатики. 2013. Т. 23. № 1. С. 33 – 42.
3. Половко И.Ю., Пескова О.Ю. Анализ функциональных требований к системам обнаружения вторжений // Известия ЮФУ. Технические науки. 2014. № 2(151). С. 86 – 92.
4. Обоснование архитектуры перспективной системы обнаружения и предотвращения вторжений / М.П. Сычев [и др.] // Инженерный журнал: Наука и инновации. 2013. № 2 (14). С. 23.
5. Ефимов А.Ю. Проблемы обработки статистики сетевого трафика для обнаружения вторжений в существующих информационных системах // Программные продукты и системы. 2016. № 1. С. 17 – 21.
6. Бурлаков М. Е. Модель многослойной универсальной системы обнаружения вторжений // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2(32). С. 214– 218.
7. Бондяков А. С. Основные режимы работы системы предотвращения вторжений (IDS/IPS SURICATA) для вычислительного кластера // Современные информационные технологии и ИТ-образование. 2017. Т. 13. № 3. С. 31 – 37.
8. Булдакова Т. И., Джалолов А. Ш. Выбор технологий DATA MINING для систем обнаружения вторжений в корпоративную сеть // Инженерный журнал: Наука и инновации. 2013. № 11(23). С. 36.
9. Доценко С.М., Владыко А.Г., Летенко И.Д. Системы обнаружения вторжений на основе встраиваемых микропроцессорных систем // Телекоммуникации. 2013. № S7. С. 15 – 18.
10. Котенко И.В., Саенко И.Б., Полубелова О.В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 2013. № 2(25). С. 113 – 134.
11. Lavrova D.S. An approach to developing the SIEM system for the internet of things // Automatic control and computer sciences. 2016. Vol.50. №8. P. 673 – 681.

12. Анализ методов корреляции событий безопасности в SIEM-системах часть 1 / А.В. Федорченко, Д.С. Левшун, А.А. Чечулин, И.В. Котенко // Труды СПИИРАН. 2016. № 4(47). С. 5 – 27.
13. Грани SIEM / С. А. Графов, А. Ю. Белявцев, Д. А. Воронов, А. А. Трофимов // Защита информации. Инсайд. 2017. № 1(73). С. 56 – 62.
14. Графов А.Ф. Развитие российских SIEM-систем: Security Capsule // Защита информации. Инсайд. 2013. № 5(53). С. 84 – 86.
15. Шабуров А.С., Борисов В.И. Разработка модели защиты информации корпоративной сети на основе внедрения SIEM-Системы // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2016. № 19. С. 111–124.
16. Петренко С.А., Цирлов В. Л. Импортозамещение решений IDS и SIEM // Защита информации. Инсайд. 2017. № 5(77). С. 46 – 51.

REFERENCES:

[1] Xodashinskij I.A., Meshheryakov R.V., Rubanov S. A. The construction of fuzzy intrusion detection classifiers based greedy and genetic algorithms. Voprosy` zashhity` informacii. 2013. № 4(102). pp. 67 – 72. (in Russian).
[2] Timonina A.A., Timonina E.E. Attacks on the centralized systems of intrusion detection. Sistemy` i sredstva informatiki. 2013. V. 23. № 1. pp. 33 – 42. (in Russian).
[3] Polovko I.Yu., Peskova O.Yu. Analysis of the functional requirements for intrusion detection systems. Izvestiya YuFU. Texnicheskie nauki. 2014. № 2(151). pp. 86 – 92. (in Russian).
[4] Proposal of perspective architectural intrusion detection and prevention system M.P. Sy`chev [i dr.]. Inzhenerny`j zhurnal: Nauka i innovacii. 2013. № 2(14). pp. 23. (in Russian).
[5] Efimov A.Yu. Problems of collecting and analyzing network traffic statistics to detect intrusion in information systems. Programmny`e produkty` i sistemy`. 2016. № 1. pp. 17 – 21. (in Russian).
[6] Burlakov M. E. The common model of intrusion detection syste. Doklady` Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioe`lektroniki. 2014. № 2(32). pp. 214 – 218. (in Russian).
[7] Bondyakov A. S. The basic modes of the intrusion prevention system (ids/ips suricata) for the computing cluster. Sovremenny`e informacionny`e texnologii i IT-obrazovanie. 2017. V. 13. № 3. pp. 31 – 37. (in Russian).
[8] Buldakova T. I., Dzhalolov A. Sh. Choice of the Data Mining technologies for intrusion detection systems into a corporate network. Inzhenerny`j zhurnal: Nauka i innovacii. 2013. № 11(23). pp. 36. (in Russian).
[9] Docenko S.M., Vlady`ko A.G., Letenko I.D. Intrusion detection systems based on embedded microprocessor systems. Telekommunikacii. 2013. № S7. pp. 15 – 18. (in Russian).
[10] Kotenko I.V., Saenko I.B., Polubelova O.V. Perspective data storage systems for security information monitoring and management. Trudy` SPIIRAN. 2013. № 2(25). pp. 113 – 134. (in Russian).
[11] Lavrova D.S. An approach to developing the SIEM system for the internet of things. Automatic control and computer sciences. 2016. Vol.50. №8. pp. 673 – 681. (in Russian).
[12] An Analysis of Security Event Correlation Techniques in Siem-Systems. Part 1. A.V. Fedorchenko, D.S. Levshun, A.A. Chechulin, I.V. Kotenko. Trudy` SPIIRAN. 2016. № 4(47). pp. 5 – 27. (in Russian).
[13] SIEM-profile. S. A. Grafov, A. Yu. Belyavcev, D. A. Voronov, A. A. Trofimov. Zashhita informacii. Insajd. 2017. № 1(73). pp. 56 – 62. (in Russian).
[14] Grafov A.F. Development of Russian SIEM-systems: Security Capsule. Zashhita informacii. Insajd. 2013. № 5(53). pp. 84 – 86. (in Russian).
[15] Shaburov A.S., Borisov V.I. developing model information protection corporate network based on the implementation of siem-system. Vestnik Permskogo nacional`nogo issledovatel`skogo politexnicheskogo universiteta. E`lektrotexnika, informacionny`e texnologii, sistemy` upravleniya. 2016. № 19. pp. 111 – 124. (in Russian).
[16] Petrenko S.A., Cirlov V. L. Import Substitution Solutions IDS and SIEM. Zashhita informacii. Insajd. 2017. № 5(77). pp. 46 – 51. (in Russian).

Поступила в редакцию – 30 августа 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – August 30, 2018. The final version – November 01, 2018.