БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2021. – № 4 (103). – 37–53

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056 DOI: 10.17212/2782-2230-2021-4-37-53

РАЗРАБОТКА ЛАБОРАТОРНОГО СТЕНДА ДЛЯ ИЗУЧЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ*

Н.В. КУКУШКИНА[1], А.К. НОВОХРЁСТОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистрант кафедры вычислительной техники. E-mail: kukushkina.2020@stud.nstu.ru*

[2] *634050, РФ, г. Томск, пр. Ленина, 40, Томский государственный университет систем управления и радиоэлектроники, кандидат технических наук, доцент кафедры комплексной информационной безопасности электронно-вычислительных систем. E-mail: nak@fb.tusur.ru*

Объектом исследования настоящей статьи являются сетевые и узловые системы обнаружения вторжений. В качестве цели исследования ставится получение обзора по системам обнаружения вторжений, а также построение конструктивного варианта виртуального лабораторного стенда, предназначенного для обучения студентов (изучение тестовых характеристик систем обнаружения вторжений). В статье приведена краткая справка о системах обнаружения вторжений с учетом классификации по способу мониторинга и технологии обнаружения атак. На сегодняшний день системы обнаружения вторжений являются необходимым элементом комплексной системы защиты сетей как небольших, так и крупных организаций. Они позволяют повысить безопасность сети, защищая от внешних и внутренних нарушителей. Поэтому необходимость получения навыков установки, настройки и администрирования систем обнаружения вторжений является важной частью подготовки специалистов по информационной безопасности, что обусловливает необходимость непрерывной актуализации и модернизации средств обучения. В настоящей работе предлагается виртуальный лабораторный стенд, предназначенный для изучения систем обнаружения вторжений. Описаны его архитектура и параметры функционирования. С целью выбора системы обнаружения вторжений для виртуального лабораторного стенда был проведен сравнительный анализ имеющихся на рынке бесплатных и коммерческих систем обнаружения вторжений. Отдельно были рассмотрены узловые и сетевые системы обнаружения вторжений. Для обоих видов описаны их преимущества и недостатки. В результате для выбранной по результатам анализа системы обнаружения вторжений описаны функции и механизм работы. Кроме того, рассмотрены примеры пользовательских правил обработки событий безопасности.

* Статья получена 10 ноября 2021 г.

Ключевые слова: система обнаружения вторжений, система предотвращения вторжений, лабораторный стенд, сравнительный анализ, сетевые системы обнаружения вторжений, узловые системы обнаружения вторжений, Open Source Security, мониторинг событий

ВВЕДЕНИЕ

В настоящее время достаточно остро стоит вопрос организации безопасности сетей. Согласно исследованию компании Check Point [1], в 2021 году число кибератак в мире увеличилось на 40 % по сравнению с предыдущим годом. Кроме того, около 80 % взломов осуществляется внутри организации. Поэтому появляется необходимость своевременно обнаруживать и анализировать эти атаки, чтобы оптимально организовать безопасность сети. Одним из решений данной задачи является использование систем обнаружения вторжений.

1. ОСНОВНЫЕ СВЕДЕНИЯ О СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

1.1. ОПРЕДЕЛЕНИЯ И КЛАССИФИКАЦИЯ

Система обнаружения вторжений (IDS – Intrusion detection system, аналогичный русскоязычный термин – СОВ) – это программное либо программно-аппаратное средство, которое контролирует сети, хосты или приложения на предмет несанкционированной активности [2].

СОВ относятся к детективным механизмам защиты и используются для обнаружения различных видов вредоносных действий, которые могут поставить под угрозу безопасность компьютерной системы. К таким действиям относятся сетевые атаки на уязвимые сервисы, атаки на повышение привилегий, доступ неавторизованных пользователей к критически важным файлам, а также воздействия вредоносного ПО (компьютерных вирусов, троянов и червей). В случае обнаружения подобной активности системы обнаружения вторжений отправляют оповещение администратору безопасности, который затем может предпринять необходимые действия. Кроме того, СОВ может помочь спрогнозировать атаки в будущем. Например, злоумышленник может осуществлять некоторые предварительные действия, такие как сканирование портов.

Наиболее общая классификация СОВ производится по способу мониторинга. Выделяют СОВ уровня узла (HIDS – host-based IDS) и СОВ уровня сети (NIDS – network-based IDS) [3].

Датчиками узловых СОВ (УСОВ) являются программные модули, которые устанавливаются на защищаемые компьютеры в сети. Эти модули предназначены для отслеживания событий в журналах и обнаружения признаков подозрительной деятельности. Также они могут контролировать целостность файлов конфигурации системы и наличие в них несанкционированных изменений. Одним из недостатков узловых СОВ является их повышенная ресурсоемкость, наличие на защищаемом компьютере. Такая СОВ требует использования определенных вычислительных ресурсов. Помимо этого, она отслеживает только сетевые пакеты, принятые или отправленные компьютером, на котором она установлена.

Датчики сетевых СОВ (ССОВ) выявляют несанкционированное и аномальное поведение исключительно на основании сетевого трафика. Они стратегически расположены в различных точках сети для мониторинга входящего и исходящего трафика сетевых устройств. Однако сетевые СОВ слабо защищают от внутренних атак, так как чтобы обнаружить попытку вторжения, она должна попасть в сеть и зафиксироваться СОВ. Сетевые СОВ, как правило, не влияют на производительность компьютерной сети. Они устанавливаются либо «в разрыв» и пропускают через себя трафик в защищенную сеть, либо работают в режиме «зеркалирования», так или иначе являясь пассивными устройствами. Но в сильно распределенной или нагруженной сети сетевым СОВ может быть сложно обрабатывать весь трафик, и они могут пропустить вредоносные пакеты.

Также возможно классифицировать СОВ по технологии обнаружения [4]:

– на основании сигнатуры (подписи) атаки: атака описывается в виде сигнатуры, т. е. шаблона, характеризующего некоторое содержимое сетевого трафика. Такой метод также называется сигнатурным. Для установки факта вторжения собранный трафик сравнивается с данным шаблоном. Можно выделить также синтаксический разбор пакетов. Захваченные сетевые пакеты проходят через синтаксический анализатор и проверяются на соответствие атаке с помощью регулярных выражений;

– на основании аномального трафика: при обнаружении аномалий (резко изменившийся объем трафика, взаимодействие нетипичных узлов, использование непривычных протоколов и т. д.) источники событий (логи, сетевой трафик, действия пользователей) сопоставляются с профилями поведения. Атакой считается ситуация отклонения от этого профиля. Данный метод также называют эвристическим.

Итак, СОВ может оповещать о вредоносной активности, однако часто необходимо именно предотвратить вредоносную активность на ранней стадии. Для этих целей используются системы предотвращения вторжений (IPS – Intrusion prevention system, аналогичный русскоязычный термин – СПВ).

Программное обеспечение СОВ и СПВ являются ветвями одного и того же дерева и используют аналогичные технологии. Меры защиты СПВ можно отнести к превентивным, в отличие от СОВ, выполняющей детективные функции.

Нельзя сказать, что СПВ лучше СОВ или СОВ лучше СПВ, они имеют разные задачи и возможности. Выбор в каждом конкретном случае зависит от требуемых функций защиты, топологии сети и т. д. Для обеспечения комплексной безопасности наиболее эффективен вариант совместного использования средств СОВ и СПВ.

Известно, что использование СОВ регулируется законодательно. Так, например, информационные системы персональных данных (ИСПДн), в которых необходимо для персональных данных обеспечить 1-й или 2-й уровень защищенности, должны контролироваться СОВ. Существует специальный приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) № 638, который регулирует использование СОВ в государственных информационных системах (ГИС), ИСПДн и других системах. Выделено 6 классов защиты СОВ (6-й – самый низкий) [5]. Причем СОВ, соответствующие 1–3-му классу защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну. Методические документы, описывающие профили защиты, соответствующие данным уровням, не публикуются в открытом доступе, так как сами являются сведениями, составляющими государственную тайну. Федеральная служба безопасности (ФСБ) использует термин «система обнаружения атак» (СОА) вместо СОВ и выделяет 4 класса: А, Б, В, Г. Причем Г – самый низкий, и каждый следующий класс включает все требования к предыдущим. Требования ФСБ отсутствуют в открытом доступе.

1.2. ОБЗОР СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

На данный момент существует достаточно обширный выбор СОВ. В этом разделе попытаемся дать описание некоторых популярных на рынке защитных решений исходя из документации, прилагаемой к этим системам. Рассмотрим их архитектуру, принципы работы и особенности.

А. Узловые системы обнаружения вторжений

OSSEC (сокр. от Open Source Security), возможно, является ведущей УСОВ с открытым исходным кодом, доступной сегодня. Клиент-серверная архитектура OSSEC позволяет отправлять оповещения и журналы на централизованный сервер, где в дальнейшем может выполняться анализ, а также уведомление администратора, даже если хост-система отключена или скомпрометирована [6].

В отличие от OSSEC, Tripwire доступна как с открытым исходным кодом, так и с полноценной корпоративной версией [7]. Tripwire Open Source работает только в системах Linux и Unix, поддержка Windows отсутствует, однако она доступна в коммерческой версии для предприятий. Эта СОВ хорошо подходит для небольших децентрализованных систем.

Программный комплекс (ПК) Ребус-СОВ разработан российским Научно-исследовательским институтом «Центпрограммсистем» и предназначен для обнаружения и предотвращения вторжений. Он функционирует как на уровне узла, так и на уровне сети [8]. ПК Ребус-СОВ включает в себя средство противодействия вторжениям, средство сбора данных и обнаружения вторжений, консоль управления, сервер и агента.

Samhain обеспечивает централизованный сбор данных и анализ информации, собранной каждой отдельной машиной. Samhain обладает отличительной особенностью: она скрывает свои процессы от злоумышленников при помощи стеганографии [9]. В отличие от OSSEC, обработка событий происходит на самом клиенте, что имеет определенные последствия. С практической точки зрения необходимо соблюдать осторожность, чтобы не перегружать сервер и не мешать работе. С точки зрения безопасности наличие обрабатывающего механизма на агенте предоставляет злоумышленникам дополнительную цель.

VipNet IDS HS использует сигнатуры и правила, предоставляемые российской компанией ЗАО «Перспективный мониторинг». Данная СОВ состоит из трех компонентов: агента, сервера и консоли управления [10].

Б. Сетевые системы обнаружения вторжений

ССОВ Snort была выпущена компанией Sourcefire еще в 1998 году и стала своеобразным стандартом и ориентиром для будущих СОВ. Позднее, в 2013 году, компания Sourcefire была приобретена Cisco Systems. Snort является лидером в области ССОВ, но ее все еще можно использовать бесплатно. Преимущества технологии с открытым исходным кодом сосредоточены на более низких затратах и поддержке сообщества.

Поскольку Snort был создан очень давно, с развитием современных технологий и ростом трафика в сети версия 2 оказалась не способна обрабатывать высокоскоростной трафик в силу отсутствия многопоточности. Данный недостаток компенсирован в вышедшей в 2021 году версии Snort 3 [11].

СОА «Форпост» может обнаруживать компьютерные атаки и блокировать их источники на сетевом оборудовании в ручном или автоматическом режиме [12]. «Форпост» может поставляться в качестве программного обеспечения (устанавливаться на выделенные сервера заказчика) и в качестве заранее сконфигурированного аппаратно-программного комплекса.

OpenWIPS-NG – это СОВ уровня сети с открытым исходным кодом, которая в основном предназначена для беспроводных сетей [13]. WIPS (Wireless Intrusion Prevention System) переводится на русский язык как «беспроводная система предотвращения вторжений», поэтому эта ССОВ не только обнаруживает, но еще и противодействует вторжениям. OpenWIPS-NG находится на стадии разработки. Она появилась не так давно, поэтому на данный момент эта ССОВ имеет некоторые ограничения. Каждая установка включает в себя только один датчик. Кроме того, данная СОВ не имеет официальной полной документации.

Следующим в нашем списке является продукт под названием Zeek Network Security Monitor (ранее Bro) – это бесплатная ССОВ, которая является больше чем просто системой обнаружения вторжений. Zeek действует в два этапа: регистрация трафика и его анализ [14]. Модуль анализа Zeek состоит из двух элементов. Первый – это механизм событий, который отслеживает инициирующие события, такие как сетевые TCP-соединения или HTTP-запросы. Затем события дополнительно анализируются с помощью интерпретатора сценариев политики (скриптов, использующих собственный язык программирования Zeek Script), который решает, следует ли инициировать предупреждение и запускать действие. Это характеризует Zeek еще и как систему предотвращения вторжений.

С-Терра СОВ обнаруживает сетевые атаки и может использоваться для расследования инцидентов в сфере информационной безопасности [15]. Существует три варианта исполнения: 1) отдельный программно-аппаратный комплекс, 2) в составе С-Терра Шлюз и 3) установка на отдельную виртуальную машину. Возможно интегрирование другими продуктами С-Терра.

2. СРАВНЕНИЕ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Перед руководителями организаций закономерно встает вопрос выбора узловой или сетевой СОВ. Надежный режим безопасности будет включать в себя обе системы. Узловая СОВ может работать совместно с сетевой, обеспечивая дополнительное покрытие для чувствительных рабочих станций и регистрируя всё, что сетевая СОВ могла пропустить. Даже если вредоносные программы смогут проскользнуть мимо сетевой СОВ, их поведение будет обнаружено узловой СОВ.

В табл. 1 и 2 показано, что СОВ могут быть очень дорогими, но, к счастью, большинство лучших СОВ на рынке можно использовать бесплатно (с возможностью приобретения платных компонентов).

Таблица 1

Table 1

Сравнение узловых СОВ

Comparison of host-based IDS

Наименование СОВ	OSSEC	Open Source Tripwire	Ребус-СОВ	Samhain	ViPNet IDS HS
Производитель	Trend Micro	Tripwire, Inc.	НИИ Центр-программ-систем	Samhain Services	ИнфотеКС
Исполнение	ПО	ПО	ПО	ПО	ПО
Стоимость	Бесплатно	Бесплатно	От 48 204 руб.	Бесплатно	От 30 860 руб.
Поддержи-ваемые платформы	Unix, Linux, Windows, macOS	Unix, Linux	Linux, Windows	Unix, Linux, macOS	Linux, Windows
Метод обнаружения атак	Сигнатурный, эвристиче-ский	Сигнатур-ный	Сигнатурный, эвристи-ческий	Сигнатур-ный	Сигнатурный, эвристиче-ский
Наличие сертификата ФСТЭК	Нет	Нет	Есть	Нет	Есть
Активный ответ на атаку	Есть	Нет	Есть	Нет	Нет
Наличие графического интерфейса	Есть	Нет	Есть	Есть	Есть
Контроль целостности файлов	Есть	Есть	Нет	Есть	Есть
Обнаружение руткитов	Есть	Нет	Нет	Есть	Есть

Таблица 2

Table 2

Сравнение сетевых СОВ

Comparison of network-based IDS

Наименование СОВ	Snort	СОА Форпост	OpenWIPS-NG	Zeek	С-Терра СОВ
Производитель	Cisco Systems	ЗАО РНК	Thomas d'Otreppe	Институт Беркли, Калифорния	С-Терра СиЭсПи
Исполнение	ПО	ПО/ПАК	ПО	ПО	ПО/ПАК
Стоимость	Бесплатно	От 194 700 руб.	Бесплатно	Бесплатно	От 117 447 руб.
Поддерживаемые платформы	Unix, Linux, Windows	Linux, Windows	Linux	Linux, FreeBSD, macOS	Linux
Метод обнаружения атак	Сигнатурный	Сигнатурный, эвристический	Сигнатурный	Сигнатурный, эвристический	Сигнатурный, эвристический
Наличие сертификата ФСТЭК	Нет	Есть	Нет	Нет	Есть
Активный ответ на атаку	Возможен при использовании расширения snort_inline	Есть	Нет	Есть	Нет
Наличие графического интерфейса	Нет	Есть	Нет	Нет	Есть
Механизм детектирования	На основании правил	На основании правил	На основании правил	На основании скриптов на собственном языке	На основании правил

В табл. 1 среди бесплатных узловых СОВ выделяется OSSEC, поскольку она использует два метода обнаружения вторжений, может осуществлять активный ответ на атаку (что позволяет ей выиграть у Samhain) и, кроме того, является кроссплатформенной. Также можно сказать, что OSSEC не уступает по функционалу Ребус-СОВ и VipNet IDS HS, которые, в свою очередь, являются коммерческими продуктами. Open Source Tripwire предоставляет довольно узкий набор возможностей, так как большинство значимых функций производитель предлагает в аналогичном коммерческом решении.

На основании данных, представленных в табл. 2, можно сделать вывод, что СОВ с открытым исходным кодом Snort и Zeek обладают примерно одинаковыми возможностями. Помимо прочего, механизм детектирования с помощью скриптов Zeek обеспечивает создание большого количества журналов, при этом не разделяя трафик на «хороший» и «плохой», что позволяет фиксировать практически все события в сети и самостоятельно интерпретировать их с помощью уже упомянутых скриптов. СОВ Open WIPS-NG является самым слабым решением из всех представленных. Это объясняется тем, что проект находится на стадии разработки и многие запланированные функции еще не реализованы.

На российском рынке большинство СОВ поставляются вместе с аппаратной составляющей. Мощность коммерческих аппаратных решений заранее рассчитана и проверена, а внедрением занимаются специалисты. Поэтому можно легко предусмотреть запас, но вот стоят они недешево. Альтернативой служат решения open-source, зарекомендовавшие себя с хорошей стороны и при этом не требующие отчислений за программное обеспечение. Но все вопросы по внедрению ложатся на плечи системного администратора.

Для систем, где необходимо соответствие требованиям ФСТЭК и ФСБ (ГИС, ИСПДн и др.), требуется использовать сертифицированные решения, такие как VipNet IDS HS, СОА «Форпост», «Ребус-СОВ» и «С-Терра СОВ». К сожалению, бесплатных сертифицированных продуктов в России для таких систем нет. Данные СОВ могут использоваться в компаниях малого, среднего и крупного бизнеса. Они имеют широкий модельный ряд и могут быть интегрированы в различные системы.

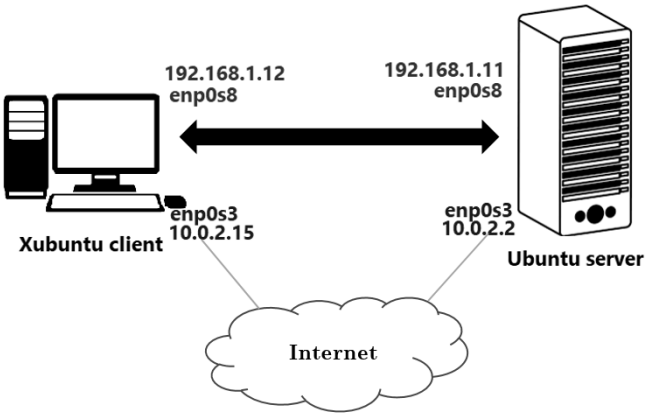
Все СОВ, перечисленные выше, имеют свои плюсы и минусы. Следовательно, лучшая СОВ для каждой отдельной организации будет зависеть от ее потребностей и обстоятельств, размера и топологии сети.

3. ОПИСАНИЕ ЛАБОРАТОРНОГО СТЕНДА

На основании сравнения, приведенного в разделе 2, предложим лабораторный стенд, использующий для демонстрации СОВ OSSEC, которая является ярким представителем семейства узловых СОВ, имеет понятный синтаксис правил, осуществляет активный ответ на атаку и может быть установлена практически в любой операционной системе. Изучение конфигурирования и основ работы с СОВ позволит получить студентам ценные профессиональные компетенции.

В процессе обучения могут использоваться различные конфигурации лабораторных стендов. Остановимся на классическом варианте виртуального лабораторного стенда, состоящего из виртуальной машины-сервера и виртуальной машины-клиента. Несмотря на свою простоту, данный стенд имеет возможность добавления разнообразных платформ для аналитики полученных событий, а также возможность реализации многозадачности: в будущем планируется добавление сетевой СОВ на сервер для демонстрации мониторинга сети.

Локальная сеть виртуального лабораторного стенда состоит из сервера и клиента, которые имеют по два адаптера: внутренняя сеть и NAT. На сервере установлена операционная система Ubuntu 18.04, а на клиенте – Xubuntu 20.04. На рисунке представлена архитектура сети для работы с СОВ OSSEC.



Конфигурация сети для СОВ OSSEC

Network configuration for OSSEC IDS

СОВ OSSEC выполняет следующие функции:

– мониторинг целостности файлов;

– мониторинг журналов (собирает, анализирует и коррелирует системные журналы);

– обнаружение руткитов;

– настраиваемые оповещения в режиме реального времени;

– интеграция с существующей инфраструктурой;

– возможен активный ответ на атаку;

– централизованный сервер для управления массовой политикой;

– агентный и безагентный мониторинг (может быть использован для мониторинга брандмауэров, маршрутизаторов и др.).

Для СОВ OSSEC возможны четыре типа установки.

1. Сервер. При данном типе установки агенты передают сообщения журнала на сервер для обработки. Правила и декодеры устанавливаются только на сервере. Оповещения генерируются и распространяются с сервера.

2. Агент. Агенты OSSEC подключают локальные файлы журнала и пересылают сообщения на сервер OSSEC. Локальные сообщения мониторинга целостности файлов также пересылаются на сервер.

3. Гибрид. Гибридная установка – это и сервер, и агент. Как сервер, он обрабатывает журналы для нескольких агентов, а как агент – отправляет предупреждения на другой сервер.

4. Автономная установка. Это означает, что машина, на которую установлен OSSEC, не связана с сервером или агентами. Декодеры и правила также будут храниться на данном компьютере.

Для рассматриваемого лабораторного стенда использованы первые два типа установки для сервера и клиента соответственно.

СОВ OSSEC располагает собственным стандартным веб-интерфейсом, он достаточно скромен, но позволяет удобнее отслеживать события. На данный момент его разработка остановлена. Разработчики рекомендуют использовать для этих целей Kibana, Splunk или другие. В рамках же образовательного процесса данного веб-интерфейса вполне достаточно.

Правила OSSEC предоставляют собой мощный способ настройки оповещений. Каждый файл правил содержит несколько определений правил для различных приложений. В сочетании с правилами существуют декодеры, предназначенные для извлечения данных из необработанных событий, что позволяет OSSEC коррелировать разрозненные события, полученные из нескольких источников.

Используя правила OSSEC, мы можем настроить правила на основе имени пользователя, IP-адреса, имени хоста источника, URL-адреса, имени файла, времени суток, дня недели, совпавших правил, частоты и времени с момента последнего предупреждения.

В реальных системах также используется несколько способов работы с правилами:

– игнорирование правил (игнорирование определенных IP-адресов);

– повышение уровня значимости правила;

– изменение частоты появления некоторого правила до срабатывания связанного с ним правила;

– написание правил для пользовательских приложений;

– игнорирование событий изменения целостности определенных каталогов и др.

Для примера можно создать два правила, иллюстрирующих обработку событий неуспешной аутентификации (листинг 1). Правило 2501 захватывает событие, а правило 100100 будет срабатывать, если 5 раз выполнится правило 2501 в течение пяти минут для одного и того же пользователя.

Листинг 1 – Правила для обработки событий неуспешной аутентификации

```
<rule id="2501" level="8" overwrite="yes">
    <pcre2>FAILED LOGIN |authentication failure|</pcre2>
    <pcre2>Authentication failed for|invalid password
for|</pcre2>
    <pcre2>L0GIN FAILURE|auth failure: |authentication er-
ror|</pcre2>
    <pcre2>authinternal failed|Failed to authorize|</pcre2>
    <pcre2>Wrong password given for|login failed|Auth: Login
incorrect|</pcre2>
    <pcre2>Failed to authenticate user</pcre2>
    <decoded_as>fauth</decoded_as>
    <group>authentication_failed,</group>
    <description>User authentication failed.</description>
</rule>

<rule id="100100" level="10" frequency="5" timeframe="300">
    <if_matched_sid>2501</if_matched_sid>
    <same_user />
    <description>5 failed passwords within 5 minutes by same
user</description>
</rule>
```

OSSEC позволяет осуществлять активный ответ на события с помощью настройки секции <active-response> в конфигурационном файле. Используя

<active-response>, можно заблокировать пользователя, который вызвал срабатывание вышеописанного правила на 5 минут (листинг 2).

Листинг 2 – Конфигурация активного ответа

```
<active-response>
    <disabled>no</disabled>
    <command>disable-account</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>300</timeout>
</active-response>
```

Когда будет выполняться активный ответ на правило 100100, пользователь, который его вызвал, даже при вводе правильного пароля не сможет войти до истечения срока блокировки.

ЗАКЛЮЧЕНИЕ

По результатам сравнительного анализа можно сделать вывод, что эффективное решение для обеспечения безопасности должно включать возможность активного ответа на атаку, быть масштабируемым, кроссплатформенным и сочетать в себе разные методы обнаружения атак.

Статистика говорит, что трафик пользователей увеличивается каждый год на 50 %. К такой нагрузке следует быть готовым заранее. В том числе к обработке большого сетевого потока должны быть готовы системы обнаружения / предотвращения вторжений.

На самом деле сейчас редко используются решения СОВ в чистом виде. Чаще всего их интегрируют с СПВ, межсетевыми экранами и антивирусами. Следующим этапом развития подобных систем стало появление межсетевых экранов нового поколения (NGFW, Next Generation Firewall), которые выигрывают за счет параллельного анализа одного и того же трафика всеми средствами защиты.

Вместе с развитием технологий безопасности развиваются и кибератаки. Их становится сложно прогнозировать и предотвращать. Однако появляется возможность эффективно бороться с сетевыми атаками и обеспечивать дополнительный уровень безопасности компьютерных систем с помощью правильного инструмента СОВ, поддерживающего бизнес и IT-инфраструктуры.

БЛАГОДАРНОСТИ

Выражаем искреннюю благодарность доктору технических наук, профессору Виктору Матвеевичу Белову за высказанные замечания и оказанную поддержку при подготовке данной статьи.

СПИСОК ЛИТЕРАТУРЫ

1. Check Point Blog: web-сайт. – URL: https://blog.checkpoint.com/ (accessed: 03.12.2021).

2. *Andress J.* Foundations of information security: a straightforward introduction. – San Francisco: No Starch Press, 2019. – 248 p.

3. *Шелухин О.И., Сакалема Д.Ж., Филинова А.С.* Обнаружение вторжений в компьютерные сети (сетевые аномалии). – М.: Горячая линия – Телеком, 2018. – 220 с.

4. *Акбарова Ш.А., Ганиев А.А.* Классификация IDS // Молодой ученый. – 2017. – № 15 (149). – С. 1–3. – URL: https://moluch.ru/archive/149/41931/ (дата обращения: 03.12.2021).

5. Информационное письмо об утверждении требований к системам обнаружения вторжений / Федеральная служба по техническому и экспортному контролю. – ФСТЭК России, 2012. – 3 с.

6. OSSEC HIDS: website. – URL: https://www.ossec.net/about/ (accessed: 03.12.2021).

7. Tripwire: website. – URL: https://github.com/Tripwire/tripwire-open-source (accessed: 03.12.2021).

8. Программный комплекс обнаружения вторжений «Ребус-СОВ»: web-сайт. – URL: https://rebus-sov.ru/ (дата обращения: 03.12.2021).

9. The Samhain file integrity/intrusion detection / Samhain Labs. – URL: https://la-samhna.de/samhain/s_documentation.html (дата обращения: 03.12.2021).

10. ViPNet IDS HS – Система обнаружения компьютерных атак: web-сайт. – URL: https://infotecs.ru/product/vipnet-ids-hs-versiya-1.html#docs (дата обращения: 03.12.2021).

11. Snort Overview: website. – URL: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node2.html (accessed: 03.12.2021).

12. Система обнаружения атак «Форпост» версии 3.0 / Комапания «РНТ» Российские наукоемкие технологии. – URL: https://www.rnt.ru/ru/production/detail.php?ID=689 (дата обращения: 03.12.2021).

13. OpenWIPS-ng: website. – URL: https://openwips-ng.org/index.html (accessed: 03.12.2021).

14. Zeek: website. – URL: https://docs.zeek.org/en/lts/intro/index.html (accessed: 03.12.2021).

15. С-Терра СОВ. Версия 4.2: web-сайт. – URL: https://doc.s-terra.ru/rh_output/4.2/IDS/output/index.htm#t=mergedProjects%2F1main%2FFirst_Topic.htm (дата обращения: 03.12.2021).

Кукушкина Надежда Викторовна, магистрант кафедры вычислительной техники Новосибирского государственного технического университета. Область научных интересов – информационная безопасность автоматизированных систем. E-mail: kukushkina.2020@stud.nstu.ru

Новохрёстов Алексей Константинович, кандидат технических наук, доцент кафедры комплексной информационной безопасности электронно-вычислительных систем Томского государственного университета систем управления и радиоэлектроники. Область научных интересов – безопасность вычислительных сетей. E-mail: nak@fb.tusur.ru

DOI: 10.17212/2782-2230-2021-4-37-53

Development of the laboratory bench for studying intrusion detection systems*

N.V. Kukushkina[1], A.K. Novokhrestov[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, master's student of the Computer Science Department. E-mail: kukushkina.2020@stud.nstu.ru*

[2] *Tomsk State University of Control Systems and Radioelectronics, 40 Lenin Avenue, Tomsk, 634050, Russian Federation, candidate of technical sciences, Associate Professor of the Department of Integrated Information Security of Electronic Computing Systems. E-mail: nak@fb.tusur.ru*

The research object of this article is network-based and host-based intrusion detection systems. The aim of the study is to obtain an overview of intrusion detection systems, as well as to build a constructive version of a virtual laboratory bench intended for teaching students (studying the test characteristics of intrusion detection systems). The article provides a brief reference on intrusion detection systems, taking into account the classification by the method of monitoring and the technology of detecting attacks. Today, intrusion detection system is a necessary element of a comprehensive network protection system for both small and large organizations. They improve network security by protecting against external and internal intrud-

* *Received 10 November 2021.*

ers. Therefore, the need to acquire skills in installing, configuring and administering intrusion detection systems is an important part of training information security specialists, which necessitates continuous updating and modernization of training tools. In this paper, we propose a virtual laboratory bench designed to study intrusion detection systems. Its architecture and functioning parameters are described. In order to select an intrusion detection system for a virtual laboratory bench, a comparative analysis of free and commercial intrusion detection systems on the market was carried out. Network-based and host-based intrusion detection systems were considered separately. For both types, their advantages and disadvantages are described. As a result, the functions and operation mechanism are described for the intrusion detection system selected based on the analysis results. In addition, examples of custom rules for handling security events are discussed.

Keywords: intrusion detection system, intrusion prevention system, laboratory bench, comparative analysis, network-based intrusion detection systems, host-based intrusion detection systems, Open Source Security, event monitoring

REFERENCES

1. Check Point Blog: website. Available at: https://blog.checkpoint.com/ (accessed 03.12.2021).

2. Andress J. *Foundations of information security: a straightforward introduction*. San Francisco, No Starch Press, 2019. 248 p.

3. Shelukhin O.I., Sakalema D.Zh., Filinova A.S. *Obnaruzhenie vtorzhenii v komp'yuternye seti (setevye anomalii)* [Detection of intrusions into computer networks (network anomalies)]. Moscow, Goryachaya liniya – Telekom Publ., 2018. 220 p.

4. Akbarova Sh.A., Ganiev A.A. Klassifikatsiya IDS [IDS classification]. *Molodoi uchenyi = Young Scientist*, 2017, no. 15 (149), pp. 1–3. (In Russian). Available at: https://moluch.ru/archive/149/41931/ (accessed 03.12.2021).

5. *Informatsionnoe pis'mo ob utverzhdenii trebovanii k sistemam obnaruzheniya vtorzhenii* [Intrusion detection system requirements statement letter]. Federal Service for Technical and Export Control, 2012. 3 p.

6. *OSSEC HIDS*: website. Available at: https://www.ossec.net/about/ (accessed 03.12.2021).

7. *Tripwire*: website. Available at: https://github.com/Tripwire/tripwire-open-source (accessed 03.12.2021).

8. *Programmnyi kompleks obnaruzheniya vtorzhenii "Rebus-SOV"* [Intrusion detection software "Rebus-SOV"]. Available at: https://rebus-sov.ru/ (accessed 03.12.2021).

9. *The Samhain file integrity/intrusion detection*. Samhain Labs. Available at: https://la-samhna.de/samhain/s_documentation.html (accessed 03.12.2021).

10. *ViPNet IDS HS*: website. (In Russian). Available at: https://infotecs.ru/product/vipnet-ids-hs-versiya-1.html#docs (accessed 03.12.2021).

11. *Snort Overview*: website. Available at: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node2.html (accessed 03.12.2021).

12. *"Forpost" version 3.0*. RNT Company. (In Russian). Available at: https://www.rnt.ru/ru/production/detail.php?ID=689 (accessed 03.12.2021).

13. *OpenWIPS-NG*: website. Available at: https://openwips-ng.org/index.html (accessed 03.12.2021).

14. *Zeek*: website. Available at: https://docs.zeek.org/en/lts/intro/index.html (accessed 03.12.2021).

15. *S-Terra SOV. Versiya 4*.2: website. (In Russian). Available at: https://doc.s-terra.ru/rh_output/4.2/IDS/output/index.htm#t=mergedProjects%2F1main%2FFirst_Topic.htm (accessed 03.12.2021).

Для цитирования:

Кукушкина Н.В., Новохрёстов А.К. Разработка лабораторного стенда для изучения систем обнаружения вторжений // Безопасность цифровых технологий. – 2021. – № 4 (103). – С. 37–53. – DOI: 10.17212/2782-2230-2021-4-37-53.

For citation:

Kukushkina N.V., Novokhrestov A.K. Razrabotka laboratornogo stenda dlya izucheniya sistem obnaruzheniya vtorzhenii [Development of the laboratory bench for studying intrusion detection systems]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2021, no. 4 (103), pp. 37–53. DOI: 10.17212/2782-2230-2021-4-37-53.