СИСТЕМА АВТОМАТИЗИРОВАННОГО МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ OSSIM

Малюков С.А.

Волгоградский архитетурно-строительный университет, г. Волгоград

соавтор: Платонов А.А.

доцент кафедры МиИТ ВолгГАСУ, кандидат физ.-мат наук

В современном мире вопросы информационной безопасности в развитии любой отечественной компании сосредотачивают на себе большое внимание. При этом, как правило, довольно много уделяется рекомендациям и требованиям российской нормативно-методической базы в данной области. Довольно многие проблемы обеспечения информационной безопасности в настоящее время обсуждаются и решаются на страницах различных компьютерных изданий, а также в сети Интернет на форумах и специализированных сайтах. Значительное внимание в этих источниках уделяется описанию различных технических решений, анализу программных и аппаратных средств, и в меньшей степени – стратегии и тактике защиты информации, концепции и политике безопасности, планам защиты в различных условиях функционирования. Одним из современных решений вопросов безопасности, являются системы мониторинга, установленные в рабочей сети. Каждая такая система должна соответствовать определенным требованиям: непрерывность, плановость, целенаправленность, активность, надежность и универсальность, а также обязана иметь собственное обеспечение, опираясь на которое она будет выполнять свои поставленные задачи.[1] К такой системе относится OSSIM - комплексная бесплатная система с открытым исходным кодом, поддерживающей различные системы и функции, в том числе анализ, сбор и корреляция событий, мониторинг узлов сети, а также включающий в себя мощнейшую систему обмена информацией об угрозах между пользователями – OTX. Каждый из компонентов OSSIM способен работать независимо и персонально настроен для выполнения тех или иных задач. Чтобы понять, как работает система мониторинга информационной безопасности требуется разобрать за какие задачи отвечает та или иная ее составляющая.[2][3]

SIEM (Security Information and Event Management) – это система, предназначенная для анализа информации, поступающей от других систем, таких как IDS, антивирусов,

маршрутизаторов и т.д., и дальнейшего выявления отклонений от норм по каким-либо критериям. При выявлении отклонения генерируется и регистрируется инцидент. В основе SIEM лежит чистая математика и статистика, которая «сама по себе» неспособна что-то предотвращать или защищать, однако при различных ситуациях, когда внешне безобидные действия, полученные с разных источников в совокупности нанесут вред системе – этот факт не обойдет стороной SIEM. Очень важно, что при таких случаях данная система способна, используя накопленную статистику, сгенерировать инцидент и более того – предоставить необходимую доказательную базу, пригодную как для внутренних расследований, так и для суда в отношении сотрудника. Собственно говоря, это одно из главных ее предназначений. Также SIEM способна проверять подконтрольную ей сеть на соответствие стандартам(PCI DSS, COBIT и др.). Еще одной задачей, посильной этой системе является создание красивых отчетов, настроенных непосредственно для нужд пользователя или администратора, например, ежедневный отчет об инцидентах, TOP-10 нарушителей, отчет по работоспособности устройств и др. Отчеты и получатели настраиваются довольно быстро и гибко. На данный момент основными потребителями SIEM являются организации банковской сферы, потому что таковым требуется регулярно проводить аудиты соответствия. Банки работают с очень чувствительной информацией, поэтому в случае возникновения важно знать, кто и когда допустил утечку, было ли это случайное действие или злонамеренное и какие были сопутствующие факторы. Следующей категорией являются крупные предприятия, которые ежедневно генерируют миллионы событий различного свойства и отследить которые просто невозможно физически, в этом случае SIEM помогает оперативно отреагировать на возможные инциденты.[4]

Следующей важной составляющей OSSIM является OSSEC – программное средство, предназначенное для выявления фактов неавторизованного доступа(вторжения или сетевой атаки) в компьютерную систему или сеть. Эта система является основополагающей, ведь любому профессиональному системному администратору важно знать что и когда происходит с его серверами. OSSEC представляет собой типичную хостовую IDS(Intrusion Detection System)-систему, призванную обнаруживать вторжения или сетевую атаку, а также прогнозировать возможное нападение , так как злоумышленнику требуется выполнить ряд действий и прощупываний безопасности системы, а это оставит след в системе мониторинга. Хостовая система обнаружения вторжений(Host-based IDS) имеет дело с информацией, собранной внутри единственного компьютера. Такое выгодное расположение позволяет ей анализировать деятельность с большой достоверностью и точностью, определяя только те процессы и пользователей,

которые имеют отношение к конкретной атаке в ОС. HIDS обычно используют информационные источники двух типов: результаты аудита ОС и системные логи. Хотя OSSEC и является HIDS, однако она имеет возможность работать по архитектуре сервер<->агенты, в отличии от других похожих продуктов, представленных на рынке.[5]

Далее рассмотрим OpenVAS - сканер уязвимостей и средство управления уязвимостями с открытым исходным кодом. OpenVAS предназначена для активного мониторинга узлов сети на предмет наличия проблем связанных с безопасностью, оценки серьезности этих проблем и для контроля их устранения. Активный мониторинг означает, что OpenVAS выполняет какие-то действия с узлом сети: сканирует открытые порты, посылает специальным образом сформированные пакеты для имитации атаки или даже авторизуется на узле, получает доступ к консоли управления, и выполняет на нем команды. Затем OpenVAS анализирует собранные данные и делает выводы о наличии каких-либо проблем с безопасностью. Эти проблемы, в большинстве случаев касаются установленного на узле необновленного ПО, в котором имеются известные и описанные уязвимости, или же небезопасно настроенного ПО. В основе работы OpenVAS-а лежит постоянно пополняемая коллекция тестов безопасности (которых уже больше 30000), а также подключение к базе, описывающей известные уязвимости. Исполнение тестов позволяет выявить уязвимость, а база обеспечивает описание проблемы и способы её решения.

За работу с беспроводными сетями Wi-Fi отвечает многофункциональная утилита Kismet. Эта система работает в «обе стороны», ведь она способна обнаруживать скрытые сети и захватывать пакеты данных. Однако в руках инженера, отвечающего за информационную безопасность, эта программа становится прекрасным инструментом для наблюдения и анализа эфира 802.11. Kismet может обнаружить и сообщить диапазон IP, используемый для конкретной беспроводной сети, а также его уровни сигнала и шума. Также данная система способна осматривать все пакеты данных для управления сетью доступной беспроводной сети. Можно использовать Kismet для поиска доступных беспроводных сетей, устранения неполадок беспроводных сетей, оптимизирования уровня сигнала для точек доступа и клиентов, а также обнаружения сетевых вторжений.

Следующей системой, входящей в OSSIM и отвечающей за мониторинг компьютерных систем и сетей, является Nagios, работающий с различными сетевыми службами(SMTP, HTTP, POP3 и т.д.). Эта программа предназначена для наблюдения, контроля состояния узлов и служб, оповещения администратора в том случае, если какие-то из служб прекращают(или возобновляют) свою работу. В возможностях Nagios стоит

отметить мониторинг состояния хостов в большинстве сетевых операционных систем, автоматическую ротацию лог-файлов и возможность организации совместной работы нескольких систем мониторинга с целью повышения надежности и создания распределенной системы мониторинга. Простая архитектура модулей расширения позволяет легко разрабатывать свои собственные способы проверки служб с использованием таких языков как Shell, Perl, Python, C++ и PHP.

Похожей по функционалу, но иной по расположению, сетевой IDS является Suricata, отличающаяся от своих соперников на рынке многозадачностью, что в следствии приводит к высокой производительности, позволяющей обрабатывать трафик до 10Gbit на обычном оборудовании. Suricata способна отслеживать активность в реальном времени и быстро реализовывать действия по предотвращению атак. Возможные меры — блокировка потоков трафика в сети, сброс соединений, выдача сигналов оператору. Также эта система может выполнять дефрагментацию пакетов, переупорядочивать пакеты TCP для защиты от пакетов с измененными SEQ и ACK номерами. В целом Suricata — гибкий инструмент по обработке пакетов, который позволяет менять маршруты в зависимости от содержания пакета, детектировать атаки и предотвращать попадание «плохих» пакетов в систему (например подменять пакеты, пока они не дошли до WEB сервера). Возможно уже сейчас провайдеры используют Suricata в качестве DPI (технологии накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому).Прочие входящие в состав OSSIM инструменты это плагины направленные на поддержку основных систем - P0f, PADS, FProbe, Arpwatch и др.

Таким образом, нами создана система, способная защитить сеть от несанкционированного доступа на всех уровнях, обеспечить мониторинг пользователей и их действий, что позволяет обнаружить вмешательства со стороны злоумышленников и быстро реагировать на них, блокируя доступ к необходимым данным и восстанавливать их потери. Мониторинг в реальном времени способен рассказать администратору о поведении пользователей в подконтрольной сети и решать, с помощью руководства разумеется, не только вопросы информационной безопасности, но и административные. В зависимости от дополнительных задач, поставленных компанией возможна установка и использование различных программных средств, более узкоспециализированных, таких как DeviceLock FireWire, направленных на анализ работы с подключенными устройствами или Dallas Lock,работающий с различными идентификаторами(USB-ключи, Rutoken и.т.д.)

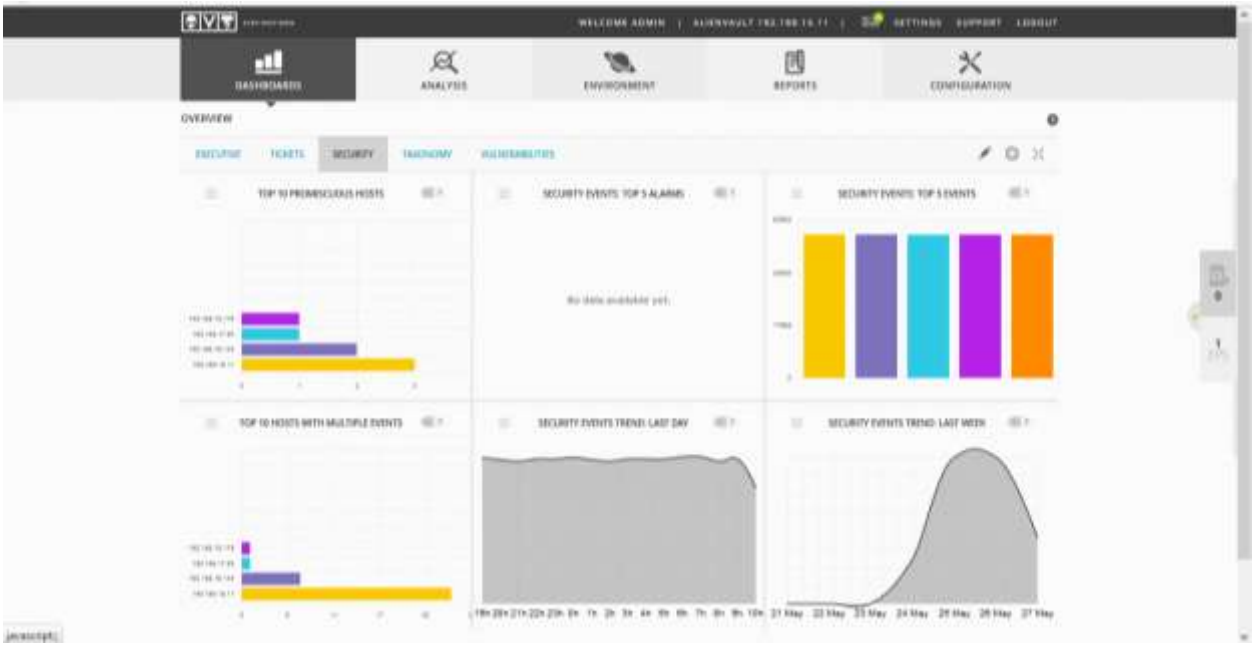

Рис. 1. Главное окно OSSIM

Рис. 2. Показания мониторинга трафика сети

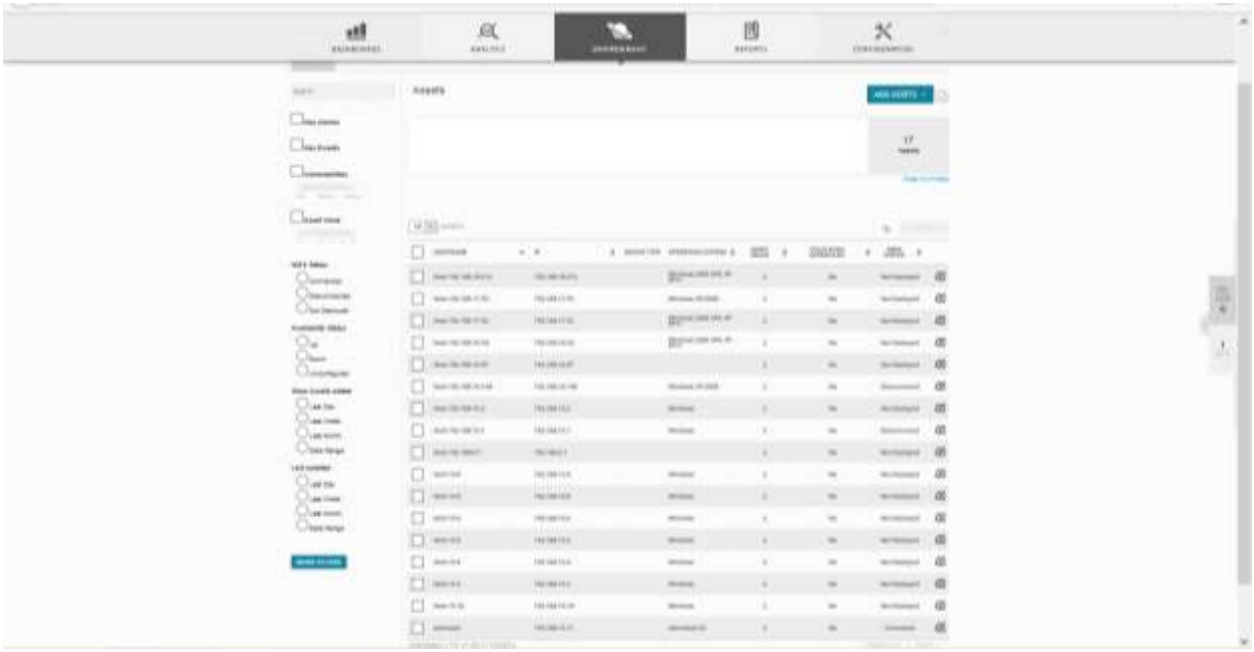

Рис. 3. Компьютеры, включенные в сеть

Рис. 4. Работа SIEM в реальном времени

Список литературы

1. Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия: Учебное пособие. 2-е изд. М.: Издательско-торговая корпорация Дашков и К°, 2005.
2. Computer Safety, Reliability, and Security. 30th International Conference, SAFECOMP 2011, Naples, Italy, September 19-22, 2011.
3. OSSIM v5 Deployment Guide // URL:
4. SIEM: ответы на часто задаваемые вопросы, 2013 / / URL: https://habrahabr.ru/post/172389/
5. OSSEC: Большой Брат наблюдает за тобой, 2013 // URL: https://habrahabr.ru/post/192800/
6. USM v5. Deployment Guide // URL: https://www.alienvault.com/documentation/usm-v5-deployment-guide.htm