автоматически генерируемых журналов событий. В рассматриваемом подходе задачей группы центра оперативного реагирования на инциденты в сфере информационной безопасности является ручной анализ данных из различных источников и принятие решения для какого-либо действия в зависимости от уровня критичности.

Ханипоты не могут полностью заменить такие средства защиты информации, как средства обнаружения вторжений или межсетевые экраны. Однако ханипоты являются прекрасным средством для изучения инструментария и методологии злоумышленников и улучшения систем защиты информации с помощью полученной информации. Помимо этого, благодаря возможности использования человеческих способностей для принятия решении о критичности события, ханипоты могут стать прекрасным дополнением функционирования центра оперативного реагирования на инциденты в сфере информационной безопасности (SOC).

Список литературы

1. Rahul Koul, Bakal J.W. Modern attack detection using intelligent honeypot // International research journal of engineering and technology. 2017. № 4. P. 2866–2869.

2. Назначение технологии Honeypot. [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/275420.php?R=1 (дата обращения: 02.05.2019).

ОСОБЕННОСТИ ПОДГОТОВКИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

М.В. Губич

Развитие информационного общества обусловило рост количества информации в электронном виде, подлежащей защите, и регистрируемых киберпреступлений, что в свою очередь повлекло необходимость подготовки квалифицированных кадров, обученных общим вопросам обеспечения информационной безопасности, и отдельной категории сотрудников, способных эффективно противодействовать преступлениям в сфере высоких технологий.

В связи с этим одной из основных целей профессиональной подготовки специалиста юридического профиля для правоохранительной сферы становится непрерывная компьютерная подготовка, в рамках которой должна быть сформирована готовность к использованию информационно-коммуникационных технологий (ИКТ), являющаяся базовой основой для развития компетенций в области информационной безопасности. К составляющим готовности к использованию ИКТ мы относим теоретические знания, технологические умения, навыки и профессиональные качества, личностные и мотивационные качества.

Соответственно, концепция формирования готовности к использованию ИКТ, на наш взгляд, должна быть основана на принципах обучения, способствующих овладению умениями решать профессиональные задачи и проблемы правоохранительной сферы на базовом (на уровне пользователя на основе выполнения установленных требований по информационной безопасности), углубленном (на уровне продвинутого пользователя, осуществляющего мероприятия по обеспечению информационной безопасности собственного рабочего места пользователя на основе выполнения требований технических и иных нормативных правовых актов) и специальном уровнях (умение решать служебные задачи на основе внедрения в служебную деятельность новых ИКТ, разработки собственных систем и средств обеспечения информационной безопасности рабочих мест пользователей ИКТ организации, а также противодействовать компьютерной преступности).

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ С ПОМОЩЬЮ ПОИСКОВОЙ СИСТЕМЫ SHODAN

Ш.Р. Давлатов

Shodan – это ведущая поисковая система по Интернету вещей, существующая уже более семи лет. В отличие от популярных поисковых движков (Google, Yandex, Bing и др.), которые ищут в сети информацию из обычных сайтов, система Shodan работает с теневыми каналами

Интернета. Она позволяет искать серверы, веб-камеры, принтеры, роутеры и самую разную технику, которая подключена к глобальной сети и составляет его часть. Shodan работает 24 часа в сутки, 7 дней в неделю, собирая информацию о 500 млн подключенных устройствах к сети Интернет ежемесячно. К основным фильтрам поисковой системы относятся: City/Country (фильтрация устройств, расположенных в пределах заданного города/страны, например, city:minsk); Port (вывод устройств с заданным открытым портом, например, port:443); OS (фильтрация устройств, которые работают на заданной операционной системе, например, os:linux); Geo (применяется для точного задания координат расположения устройства в формате долгота-широта, например, geo:42.9693,-74.1224); Net (используется для поиска устройств из заданного диапазона ip-адресов, например, net:216.0.0.0/16);

В данной работе представлены результаты интеграции системы Shodan с метапоисковой платформой Maltego, которая широко применяется для построения и анализа связей между различными интернет инфраструктурами (веб-сайты, dns-имена, ip-адреса и др.). Особенностями данного подхода являются визуализирование, обработка и комбинирование информации для более детального анализа данных, полученных из поискового движка Shodan. Результаты исследования могут быть использованы специалистами по информационной безопасности на начальных этапах проведения аудита автоматизированных систем (сбор первичной информации, автоматизация процесса анализа данных, тестирование объекта защиты на проникновение).

ИДЕНТИФИКАЦИЯ АКУСТИЧЕСКИХ СИГНАЛОВ МЕТКАМИ С КОДОМ БАРКЕРА

Г.В. Давыдов, В.А. Попов

Проверка защищенности речевой информации включает элемент оценки звукоизоляции помещений. Для этих целей используются как тональные сигналы, так и «белый» шум. Однако при приеме акустического сигнала за пределами помещений трудно выделить тестируемый сигнал на фоне производственных шумов.

Проанализированы методы встраивания меток в акустические сигналы, включающие тональные сигналы, «белый» шум, речевые и речеподобные сигналы, для целей определения способности акустических сигналов проходить через ограждающие элементы конструкций помещений. При этом в качестве меток широко используются коды Баркера. Коды Баркера являются оптимальными кодами, что заключается в том, что амплитуда автокорреляционной функции равна числу элементов кода, а значение боковых лепестков равно 1. Такие методы применяются для автоматического обнаружения акустических сигналов и их аутентификации [1]. Применение методов стеганографии не представляется возможным из-за того, что зондирование выполняется акустическим сигналом, а метод стеганографии предусматривает введение информации в цифровой сигнал за счет использования последних разрядов акустического цифрового сигнала.

На основании проведенного анализа разработан алгоритм встраивания меток с кодом Баркера в акустические сигналы, который включает формирование и излучение в акустическом виде в проверяемом помещении тестовых сигналов с амплитудно-импульсной модуляцией с использованием кодов Баркера для подтверждения присутствия зондирующего акустического сигнала. Предлагается использовать коды Баркера с числом разрядов 11.

Большое влияние на выбор кода и алгоритма кодирования тестового сигнала оказывает канал связи. В связи с тем, что канал связи обладает неравномерной амплитудно-частотной характеристикой, обусловленной резонансными свойствами ограждающих элементов конструкций помещений, наиболее приемлемым видом модуляции будет амплитудно-импульсная или частотная. Рассматриваются наиболее распространенные методы декодирования и обнаружения меток в тестируемом сигнале и вопросы выбора оптимальных требований для решения поставленной задачи.

Список литературы

1. Воробьев В.И., Давыдов Г.В., Лещенко Д.В. Обнаружение акустических сигналов на фоне речи // Доклады БГУИР. 2003. Т.1, №2/1. С. 48.