ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ В ИНФОКОММУНИКАЦИОННОЙ СЕТИ ПРЕДПРИЯТИЯ, НА ОСНОВЕ КОРРЕЛЯЦИИ ДАННЫХ ПОЛУЧАЕМЫХ ИЗ РАЗЛИЧНЫХ ИСТОЧНИКОВ

В.Ф. Кулиш, Т.В. Борботько, Аль-Гбури Хуссейн Кахтан Халаф

Мероприятия по оценке защищенности инфокоммуникационных сетей основываются на анализе их уязвимостей, которые позволяют определить вероятные способы получения несанкционированного доступа к ним нарушителем, что в дальнейшем дает возможность разработать или совершенствовать систему защиты инфокоммуникационной сети. Практическая реализация таких мероприятий позволяет своевременно обнаруживать сервисы, отладочные интерфейсы и приложения, функционирующие в инфокоммуникационной сети предприятия, по ошибке администратора оказавшиеся доступными из сети Интернет.

Обнаружение уязвимостей основывается на ряде последовательных итераций позволяющих сформировать списки зарегистрированных доменных имен в анализируемой инфокоммуникационной сети, хостов и открытых на них портах. Типовой подход, используемый для получения указанных сведений, основан на сканировании сети предприятия за счет использования прикладного программного обеспечения (Nessus, Qualys и т.д.), в том числе с открытым исходным кодом (dnsmap, nmap и т.д.).

Однако с появлением таких сервисов в сети Интернет как Shodan (https://shodan.io) и Censys (https://censys.io), периодически сканирующих весь диапазон адресов протокола IP версии 4, обнаружение уязвимостей может быть реализовано за счет получения информации от указанных информационных ресурсов, сопоставления ее и преставления в удобном для оператора виде для последующего анализа. Указанные сервисы имеют интерфейсы прикладного программирования, что предлагается использовать для создания прикладного программного обеспечения для анализа уязвимостей инфокоммуникационной сети предприятия.

Разработанное программное средство получает информацию от указанных сервисов, из которой выбираются сведения, относящиеся к анализируемой инфокоммуникационной сети предприятия. На основании полученной информации от сервисов Shodan и Censys формируются два списка доступных хостов сети и открытых портах с указанием даты последнего сканирования. Полученные таким образом списки объединяются в один отчет с учетом даты последнего сканирования, который впоследствии будет анализироваться оператором.

Таким образом, разработанное программное средство позволяет получать сведения об уязвимостях инфокоммуникационной сети предприятия, без подключения к анализируемой сети, за счет корреляции данных (результатов сканирования сети) получаемых от сервисов Shodan и Censys.

ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ G-PON

Д.Н. Курбыко, Н.В. Тарченко

Основной особенностью всех xPON сетей является то, что нисходящий поток достигает всех оптических сетевых блоков (ONU), подключенных к сети. Злоумышленник после некоторых манипуляций с перепрограммированием ONU может добиться того, что будет получать информацию, адресованную другим пользователям. Система безопасности xPON сетей как раз должна уметь противостоять такого рода угрозам, как «прослушивание».

Основной алгоритм шифрования, использующийся в технологии G-PON — это расширенный стандарт криптозащиты (AES). Этот алгоритм шифрования относится к виду так называемых блочных кодов, который обрабатывает блоки данных длинной 16 байт.

Стандарт AES поддерживает несколько режимов шифрования данных, однако в технологии G-PON используется только один из них. Он получил название «шифрование со счётчиком» Counter Mode (CTR). Шифратор создает поток, состоящий из 16 байтных псевдослучайных шифроблоков. По заданному алгоритму шифроблоки взаимодействуют с входной нешифрованной информацией, в результате чего на выходе получается зашифрованная информационная последовательность. На приемной стороне происходит обратная операция, в которой участвуют те же самые шифроблоки и зашифрованная информационная последовательность. В результате получается исходная нешифрованная информационная последовательность.

Когда датаграмма отправляется OLT или принимается ONU, то в ней содержится информация о первом байте заголовка. В первом байте заголовка находится значение криптосчетчика. Для конкретной датаграммы это значение используется в качестве начального значения счетчика

шифроблоков. Для последующих шифроблоков в той же датаграмме счетчик увеличивается на 1 для каждого последующего. Такая организация счетчиков приводит к тому, что значение счетчика никогда не повторяется два раза. 46-ти битное значение блока криптосчетчика управляет 128 битами AES последовательности по следующему алгоритму: 46 бит повторяются 3 раза, в итоге получается 138-битная последовательность, 10 первых бит которой отбрасываются. Полученные 128 бит информации подвергаются обработке AES алгоритма, в результате чего получается случайная шифропоследовательность, которая потом взаимодействует с блоками данных.

Использование стандарта шифрования AES позволяет повысить безопасность личной информации конечных пользователей. Стандарт AES использует 128-битовые ключи и имеет высокую скорость работы, кодируя за один цикл 128-битный блок.

Литература

1. Эксперт: Телекоммуникации вчера, сегодня, завтра. [Электронный ресурс]. — Режим доступа: http://rfcmd.ru/book_07/h5_5. — Дата доступа: 13.05.2016.

МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ПОИСКА АНОМАЛИЙ В ЗАДАЧАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

А.А. Левчук

Методы анализа, используемые в большинстве современных систем детектирования вторжений, направлены на обнаружение известных и формально описанных типов воздействий, но зачастую оказываются не в состоянии обнаружить модификации или новые типы аномалий, что делает их использование не всегда эффективным.

В работе была поставлена задача: на основе изучения алгоритмов поиска аномалий, спроектировать и реализовать отдельные элементы интеллектуальной системы на основе нейронных сетей для применения в задачах обнаружения вторжений.

Для решения задачи был предложены архитектурные решения обнаружения аномалий с использованием нейросетевых моделей. В исследованиях были получены 4 варианта нейросетей, спроектированных путём комбинирования рециркуляционных нейронных сетей и многослойных персептронов.

Чтобы оценить эффективность предложенного подхода обнаружения вторжений, был проведён ряд экспериментов. База данных KDD Cup 99 использовалась для обучения и тестирования нейросетевых моделей. В базе KDD-99 представлены 22 типа атак, разделенных на четыре основных категории: DoS, U2R, R2L и Probe. Наилучший результат распознавания аномалий разработанной системой был достигнут для атак класса DoS и Probe, несколько хуже определяются U2R и R2L.

Таким образом, в работе подтверждено, что модели нейронных сетей могут успешно применяться в задачах обнаружения вторжений. В ходе эксперимента проведён сравнительный анализ спроектированных систем на основе нейронных сетей. Для сравнения были использованы такие показатели эффективности, как доля обнаруженных атак, доля распознанных атак по каждому классу и число ложных срабатываний.

РЕШЕНИЕ ЗАДАЧИ ЦЕЛЕРАСПРЕДЕЛЕНИЯ В ИНФОРМАЦИОННОЙ ПОДСИСТЕМЕ КОМПЛЕКСА СРЕДСТВ АВТОМАТИЗАЦИИ ЗЕНИТНОЙ РАКЕТНОЙ БРИГАДЫ С УЧЕТОМ КЛАССА ЦЕЛЕЙ

А.Ю. Липлянин, Е.И. Михненок, Е.И. Хижняк

В основе эффективного управления боевыми средствами системы войск противовоздушной обороны лежит качественное управление огневыми средствами, решаемое в управляемой подсистеме комплексов средств автоматизации. Одним из факторов успешного функционирования управляющей подсистемы является эффективное решение задачи целераспределения. В настоящее время в комплексах средств автоматизации зенитной ракетной бригады имеется совокупность решаемых задач, в которые входят задачи боевого управления. Одним из типов таких задач является задача распределения усилий между группами зенитных ракетных дивизионов и целераспределение между зенитными ракетными дивизионами. На сегодняшний день эффективность зенитной ракетной бригады оценивается математическим ожиданием количества уничтоженных целей, которая в свою очередь обладает достаточно низкой коррелированностью с действительными результатами боевых действий [1]. Поскольку целью зенитной ракетной бригады при отражении удара воздушного противника является минимизировать ущерб объекту обороны, то и в качестве показателя