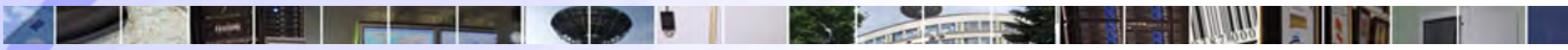
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК БЕЛАРУСИ

ОБЪЕДИНЕННЫЙ ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НЕИЗВЕСТНЫХ АТАК

При решении задач, связанных с диагностикой и защитой сетевых ресурсов, центральным вопросом является оперативное обнаружение состояние информационно-телекоммуникационной сети, приводящих к потере полной или частичной ее работоспособности, уничтожению, искажению или утечке информации, являющихся следствием отказов, сбоев случайного характера или результатом получения злоумышленником несанкционированного доступа к сетевым ресурсам, проникновения сетевых червей, вирусов и других угроз информационной безопасности. Раннее обнаружение таких состояний позволит своевременно устранить их причину, а также предотвратит возможные катастрофические последствия.

Системы обнаружения вторжений (СОВ) – это один из ключевых компонентов комплексной системы защиты информации. Они позволяют увеличить безопасность информационно-телекоммуникационной сети, контролируя все входящие и исходящие потоки трафика. Кроме того, пожалуй, это один из немногих элементов системы защиты информации, в основе которого лежит динамический принцип работы.



Эффективность СОВ во многом зависит от применяемых методов анализа полученной информации.

Существуют две технологии обнаружения вторжений: технология сигнатурного анализа и технология выявления аномального поведения трафика.

Конкретные требования к СОВ в зависимости от типа обрабатываемой информации разработаны в документе ФСТЭК РФ «Информационное письмо об утверждении требований к системам обнаружения вторжений» от 15.03.2012. ФСТЭК РФ поделила СОВ на 6 классов защиты и для каждого из них определила свои требования. Соответствие требованиям ФСТЭК РФ является важным фактором при выборе СОВ. В методическом документе «Меры защиты информации в государственных информационных системах» (Приказ ФСТЭК РФ от 11.02.2013 № 17 (утв. 11.02.2014)) представлены методы и рекомендации по использованию СОВ для обеспечения безопасности сети.

Существуют две технологии обнаружения вторжений: технология сигнатурного анализа и технология выявления аномального поведения трафика.

Метод обнаружения атак на основе сигнатур используется для обнаружения известных атак. Однако, современные технологии атак развиваются очень быстро и зачастую база сигнатур не способна покрыть все существующие на текущий момент способы атак. В связи с этим очень важным является способность информационно-телекоммуникационной сети анализировать информационные сетевые потоки с целью обнаружения и своевременного распознавания аномальных потенциально опасных в контексте атак ситуаций. Методы аномального поведения трафика в информационно-телекоммуникационной сети используются для обнаружения неизвестных атак.

Методы обнаружения атак			**СОВ**
	Сигнатурные методы		OSSEC, Snort, Suricata, Tripwire, IBM ISS, McAfee, C-Терра СОВ
	Методы, основанные на обнаружении аномалий сетевого трафика	Методы на основе нечеткой логики	Разработана исследователями из Индии Шанмагавадива Р.и Нагаражан Н.
		Методы на основе генетических алгоритмов	GA-NIDS

В настоящее время наблюдается усложнение технологий проведения атак на информационно-телекоммуникационные сети, в частности появляются новые ранее неизвестные виды атак, опасные комплексные атаки, состоящие из нескольких простых атак, использующие совокупность различных методов атак и зачастую задействующие целые группы взаимодействующих злоумышленников. Обнаружение таких комплексных распределенных атак затруднено вследствие необходимости анализа разнородных источников информации, поиска взаимосвязи между выявленными простыми атаками. Появление новых все более изощренных методов и подходов к взлому информационно-телекоммуникационных сетей, неуклонный рост профессионализма атакующих обусловливает наблюдаемые сегодня направления совершенствования и развития СОВ, в частности, создание гибридных СОВ.

В гибридных СОВ одновременно используются как сигнатурные методы, так и методы аномального поведения трафика контролируемой информационно-телекоммуникационной сети.

Нами уже разработан экспериментальный образец ПК СМСИБ, в состав которого входит СОВ, основанная на сигнатурных методах, в которой используется OSSEC – хостовая и Suricata – сетевая. Решаемые задачи СОВ:

- поиск атак в соответствии с заданными правилами;
- отображение обнаруженных атак в веб-интерфейсе консоли управления СОВ и уведомление администратора безопасности об обнаруженных атаках по e-mail;
- автоматическое сохранение обнаруженных атак для последующего анализа;
- обнаружение атак на основе динамического анализа сетевого трафика.

В разрабатываемой СОВ будут одновременно использоваться как сигнатурные методы, так и методы аномального поведения трафика.

Методы аномального поведения трафика, которые будут использоваться в разрабатываемой СОВ:

- статистические методы;

- методы, основанные на вейвлет-анализе;
- спектральные методы;
- методы на основе нейронных сетей;
- методы на основе иммунных систем.

Следует отметить, что каждый метод имеет как достоинства, так и недостатки. Совместное использование различных методов увеличит вероятность обнаружения неизвестных атак. В качестве примера приведем достоинства и недостатки статистических методов обнаружения неизвестных атак. К статистическим методам обнаружения неизвестных атак относятся:

- цепи Маркова;
- метод хи-квадрат ($\chi 2$);
- метод среднеквадратических отклонений;
- анализ распределений интенсивности передачи/приема пакетов;
- анализ временных рядов;
- пороговый анализ.

Статистические методы	Достоинства	Недостатки
Цепи Маркова	Возможность получения вероятности атаки. Сохранение промежуточных состояний для дальнейшего анализа вредоносных действий. Возможность применения упреждающих действий по ликвидации следующих шагов развития	Экспоненциальное увеличение числа состояний модулируемой цепи с ростом ее порядка. Необходимость в периодическом изменении параметров моде - ли с целью ее адаптации к изменяющемуся поведению легитимного пользователя

Статистические методы	Достоинства	Недостатки
Метод χ 2	Высокая теоретическая точность обнаружения в случае нормально распределенных случайных величин (99.7% для 95%-го доверительного интервала)	Предположение о нормальном распределении векторов наблюдаемых измерений, соответствующих трафику без аномалий. Необходимость задания наиболее полной выборки измерений нормального трафика

Статистические методы	Достоинства	Недостатки
Метод средне-квадратических отклонений	Наличие адаптивной способности, позволяющей подстраиваться под изменения сетевого окружения	Возможность постепенного переобучения системы со стороны злоумышленника с целью ее введения в заблуждение о нормальном поведении пользователя. Необходимость создания репрезентативной выборки нужного размера, представленной исключительно легитимным трафиком

Статистические методы	Достоинства	Недостатки
Анализ распределе-лений интенсивности передачи/приема пакетов	Возможность наглядного визуального представления аномалии в сети с помощью графиков и гистограмм	Зависимость качества обнаружения от выбора величины допустимого изменения параметров

Статистические методы	Достоинства	Недостатки
Анализ временных рядов	Возможность динамического и долгосрочного прогнозирования трендов, задающих изменения нормального функционирования системы. Возможность обнаружения постепенных, но значительных отклонений от нормального поведения	Сложность выбора прогнозирующей функции. Усложнение описательной модели для учета сезонности наблюдаемого временного ряда. Низкая эффективность обнаружения атак для случая рядов, не обладающих свойством стационарности

Статистические методы	Достоинства	Недостатки
Пороговый анализ	Простота реализации и настройки. Отсутствие этапа предварительного обучения. Простота интерпретации полученных результатов, свидетельствующих о нормальности/ аномальности событий в сети	Необходимость тонкого задания числового порога, требующего знаний эксперта и напрямую влияющего на качество обнаружения. Отсутствие адаптивных механизмов для автоматического выбора порога. Необходимость тщательного анализа полученных результатов вследствие возможных пропусков атак и ложных срабатываний


Внешний канал передачи данных
Клиентская часть/
Мультифункциональные распределенные агенты
Модуль захвата данных
Модуль предобработки и формирования данных
Модуль шифрования
Модуль формирования и передачи пакета
Модуль логирования
Модуль ответа на вторжения
Локальная БД
Локальный канал передачи данных
Административная часть/Консоль администратора
Модуль управления клиентской частью
Модуль управления серверной частью
Модуль загрузки и обновления данных в БД
Локальный канал передачи данных
Серверная часть/распределенная серверная часть
Модуль дешифрации и предобработки
Модуль формирования очереди
Модуль логирования
Модуль анализа/ансамбль классификаторов
Сигнатурные методы
Статистические методы
Методы вейвлет-анализа
Спектральные методы
Нейронные сети
Иммунные системы
Модуль ответа
Модуль хранения состояния
БД

СПАСИБО ЗА ВНИМАНИЕ