Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Епишкин Д.С. Потребность в современных системах обнаружения вторжений по выявлению атак // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2017. – № 04 (апрель). – АРТ 66-эл. – 0,1 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056.53

Епишкин Дмитрий Сергеевич
студент 1 курса, институт заочного и дистанционного образования
ФГБОУ ВО «Московский технологический университет» МИРЭА
г. Москва, Российская Федерация
e-mail: mityai2020@mail.ru

ПОТРЕБНОСТЬ В СОВРЕМЕННЫХ СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ПО ВЫЯВЛЕНИЮ АТАК

Аннотация: В статье рассмотрена необходимость в использовании систем обнаружения вторжений.

Ключевые слова: атака, обнаружение, система обнаружения вторжений.

Yepishkin Dmitriy
1st year student, institute of correspondence and distance education
FGBOU VO «Moscow University of Tehnology» MIREA
Moscow, Russian Federation

The need for modern intrusion detection systems to detect attacks

Abstract: The article considers the need for the use of intrusion detection systems .

Keywords: attack, detection, intrusion detection system.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Современный период развития общества характеризуется сильным влиянием на него информационных технологий, которые проникают во все сферы человеческой деятельности, обеспечивая распространение информационных потоков в обществе, образуя глобальное информационное пространство. Материальное производство и другие сферы деятельности все больше нуждаются в информационном обслуживании, переработке огромного количества информации. Техническим средством обработки любой информации является компьютер, играющий роль усилителя интеллектуальных возможностей человека и общества в целом, а коммуникационные средства, использующие компьютеры, служат для связи и передачи информации.

Для передачи информации в настоящее время получили распространение как глобальные, так и локальные сети. Ими пользуются все организации, не зависимо от сферы деятельности и территориального расположения. В пределах одной организации компьютеры связываются посредством локальной сети. В свою очередь все локальные сети организации связываются через глобальную сеть интернет. Это безусловно удобно и практично, но порождает проблемы, связанные с защитой информации.

Важная информация организации может быть потеряна, украдена злоумышленником, если её руководство должным образом не отнесётся к безопасности своей корпоративной сети, что приведёт к нанесению значительного ущерба организации. Каждая угроза влечёт за собой определённый ущерб – моральный или материальный, а защита и противодействие угрозе призвано снизить его величину. Поэтому продуманная и хорошо организованная система безопасности позволяет избежать или минимизировать потерю важных данных организации.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

В связи с постоянным увеличением информационных ресурсов, использование средств защиты по выявлению угроз становится всё более необходимым и актуальным. На рынке информационных технологий существует потребность в системах для обнаружения как ранее известных, так и неизвестных атак, так как они появляются с большой скоростью.

Для достижения цели по защите информации от возможных вторжений и последующей потери важной информации необходимо рассмотреть современные системы обнаружения вторжений и проанализировать их параметры и возможности, смоделировать корпоративную сеть, настроить и подготовить систему обнаружения вторжений, смоделировать возможные вторжения для проверки работоспособности системы по их обнаружению

Система обнаружения вторжений является программной или аппаратной системой, автоматизирующая процесс просмотра событий, возникающих в компьютерной системе или сети, определяющихся как попытки компрометации конфиденциальности, целостности, доступности или обхода механизмов безопасности, и анализирует их. Подобные системы состоят из трёх функциональных компонентов: информационных источников, анализа и ответа. Система получает информацию о событии из источников информации, выполняет определяемый конфигурацией анализ данных события и затем создаёт специальные ответы, от простейших отчётов до активного вмешательства при определении проникновения.

На современном рынке существует множество различных систем обнаружения вторжений. Для понимания в какой из них есть необходимость, можно провести сравнение характеристик и изучение некоторых параметров, благодаря которым можно определить в каком продукте можно заинтересоваться, придерживаясь нужных параметров.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Сравнительная характеристика систем обнаружения вторжений.

Параметр	Bro	CATNET	OSSEC	Snort
Бесплатность	+	−	+	+
Открытость исходных кодов	+	−	+	+
Мультиплатформенность	−	+	+	+
Графический интерфейс	−	+	+	−
Тип по мониторингу системы	сетевая	сетевая	узловая	сетевая, узловая

Система Bro является сетевой с открытым исходным кодом, и является пассивной, только для пользователей unix-подобных операционных систем. Производитель данного продукта рекомендует использовать его как дополнение к уже установленной системе обнаружения вторжений.

В свою очередь система OSSEC в большинстве операционных систем, являясь узловой и масштабируемой системой. В неё интегрирован анализ логов, проверка целостности файлов, оповещение в режиме реального времени. Плюсом является то что для клиентов существует техническая поддержка.

Система CATNET является интеллектуальной, она может обнаруживать аномалии и попытки сетевых вторжений, быстрый и эффективный мониторинг сети, журнал событий для последующего анализа.

Продуктом с открытым исходным кодом для обнаружения и предотвращения вторжений является система Snort. Она способна выполнять в режиме реального времени анализ трафика и регистрацию по ip-сети.

Системы обнаружения вторжений являются мощным и гибким инструментом по выявлению сетевых атак. Использование таких систем целесообразно, так как с каждым днём количество угроз и атак стремительно возрастает. Следует отметить, что обнаружение аномалий является серьёзной

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

компонентой выявления сетевых атак, так как она позволяет выявлять подозрительное, отклонённое от нормы поведение сетевого трафика.

Список использованной литературы:

1. Жигулин Г.П. Новосадов С.Г. Яковлев А.Д. «Информационная безопасность» СПб, 2003
2. Олифер В.Г. Олифер Н.А. «Компьютерные сети» 3-е издание СПб, 2006.

Дата поступления в редакцию: 12.04.2017 г.
Опубликовано: 14.04.2017 г.