Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Разработка системы обнаружения вторжений

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Михалкина Вячеслава Дмитриевича

Научный руководитель

доцент, к.п.н. _____ А.С. Гераськин

18.01.2018 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

18.01.2018 г.

Саратов 2018

ВВЕДЕНИЕ

В наши дни электронный документооборот, онлайн сервисы и приложения достигли огромного количества. Интернет все больше проникает в нашу жизнь, все большее количество конфиденциальных данных хранится в сети, что порождает повышенную опасность утечки конфиденциальной информации и, соответственно, требует повышенного внимания к безопасности таких сетей. В небольших компаниях мало обращают внимание на эту проблему и считают, что достаточно установки простейших антивирусных пакетов и разграничения прав доступа к ресурсам. Но практика показывает, что этих мер зачастую недостаточно. Большое влияние имеет человеческий фактор и проблемы возникают именно из-за недостаточности оказанного внимания техническими специалистами. По статистике большинство взломов и утечек конфиденциальных данных из серверов, обслуживающих сервисы, связанные с электронной коммерцией происходит по причине игнорирования специалистами по безопасности ошибок, которые на первый взгляд кажутся малозначительными. Но в результате оказывается, что в следствие именно этих ошибок которых конфиденциальные данные пользователей становятся доступными злоумышленникам [6].

Очень важным аспектом в обеспечении безопасности является обнаружение попыток несанкционированного доступа к серверу в реальном времени и их пресечение. Невозможно создать комплексно защищенную сеть без средств, обеспечивающих защиту от НСД.

Классические схемы построения безопасности системы представляют собой барьеры, установленные на границе сети, в которой функционирует защищаемый сервер (межсетевые экраны, фильтры пакетов и т.д.). Практика же показывает, что комплексная защита оказывается более эффективной.

Один из наиболее важных элементов комплексной системы обеспечения безопасности – это средства обнаружения вторжений. Обнаружение вторжений является процессом оценки подозрительных действий, которые происходят в контролируемой информационной системе.

Системы обнаружения вторжений очень актуальны в наше время. Рыночный спрос на них растет. [10].

Системы обнаружения вторжений контролируют весь входящий и исходящий из системы трафик, отслеживая как внутренние нарушения безопасности (обнаруживается от 70% нарушений, инициированных внутренними злоумышленниками [11]), так и внешние (процесс выявления попыток удаленных вторжений и сбора статистики как удачных, так и неудачных взломов).

Целью данной работы является реализация системы обнаружения вторжений.

Задачи дипломной работы:

1. Провести анализ технологий для выявления вторжений.
2. Провести анализ архитектуры систем обнаружения вторжений (СОВ).
3. Осуществить реализацию программного продукта, который выявляет попытки несанкционированного доступа доступа к серверу сигнатурными методами и методом поиска аномалий.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 3 приложений. Общий объем работы – 96 страниц, из них 74 страницы – основное содержание, включая 21 рисунок и 6 таблиц, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Раздел 1 озаглавлен «Теоретические основы». Он содержит в себе определения терминов, которые использованы в работе, определение систем обнаружения вторжений. Произведено теоретическое исследование СОВ: их архитектуры, классификации, возможности, цели использования, используемые методы обнаружения вторжений, виды реакций на вторжения.

Даны определения узловых и сетевых СОВ, подробно рассмотрены их схожие и отличительные черты. Для каждого из этих типов СОВ определены специфичные задачи. Выявлены преимущества и недостатки обоих видов систем.

Рассмотрены различные методы, позволяющие обнаруживать вторжения. Выделены основные их классы: обнаружение злоупотреблений и обнаружение аномалий. Для каждого из классов описаны относящиеся к ним наиболее распространенные методы. Например, статистические методы и нейронные сети для обнаружения аномалий, а так же продукционные методы и анализ изменений для обнаружения злоупотреблений. Для некоторых из описанных методов представлены реализующие их алгоритмы. Так же, для каждого метода выявлены сильные и слабые стороны, специфичные задачи, с которыми наиболее эффективно справляется конкретный метод.

Описаны возможности СОВ по реагированию на обнаруженные вторжения и атаки. Даны определения пассивным, автоматическим и автоматизированным ответным действиям СОВ. Дано определение системе предотвращения вторжений. Рассмотрены плюсы и минусы каждой из возможных реакций. Для автоматизированной реакции описаны и проанализированы две основные из возникающих проблем: проблема отказа в обслуживании и проблема доступа. Выявлены преимущества и недостатки пассивных и активных СОВ в целом.

Подробно рассмотрен процесс настройки СОВ для эффективной работы, аспекты, которым стоит уделить наибольшее внимание, например, определению пороговых значений, выбору анализируемых параметров,

определению списка обнаруживаемых атак, определению реакцию на обнаруженные вторжения.

Раздел 2 озаглавлен «Обзор существующих СОВ». В нем был произведен обзор и анализ современных СОВ, которые относительно недавно появились на рынке программных продуктов. Для каждого из рассмотренных продуктов указаны: разработчик, совместимые ОС, лицензия, по которой распространяется данный продукт, класс СОВ, методы, на основании которых производится обнаружение вторжений. Описаны классы задач, которые конкретный продукт будет решать наиболее эффективно и методы, на основании которых реализовано обнаружение вторжений. Сделаны выводы в виде плюсов и минусов каждого продукта.

Так же, данный раздел содержит в себе подраздел, посвященный недостатком современных СОВ, в котором указаны основные выявленные в процессе исследования проблемы современных СОВ, которые пока не были решены: отсутствие определенной методологии построения СОВ, недостаточная эффективность, низкая портативность, сложность модернизации, сложность установки, отсутствие общих стандартов и методов тестирования эффективности СОВ. Так же, в данном подразделе описаны недостатки изученных методов обнаружения вторжений, которые связаны в основном с невозможностью СОВ самостоятельно определять связи между атаками, высоким потреблением ресурсов и низкой скоростью обработки событий в реальном времени.

В заключении данного раздела предложены направления по улучшению СОВ, которые касаются введения общей теоретической базы, методов тестирования эффективности установленной СОВ и аппарата теории распознавания образов.

Раздел 3 озаглавлен «Реализация программного модуля». В нем описана реализация программного продукта в рамках данной дипломной работы. Описаны используемые класс СОВ, методы обнаружения вторжений и структура реализованный СОВ. Обоснован их выбор и указаны задачи, которые

должна решать реализованная СОВ. В реализованной СОВ обнаружение вторжений осуществляется двумя методами: на основании обнаружения аномалий и сигнатурного обнаружения атак. Для метода обнаружения аномалий описан алгоритм, основанный на нормальном распределении, а точнее на правиле «3-сигма». Для сигнатурного метода дан список обнаруживаемых атак: наводнение запросами (flooding), подбор пароля (brute Force), SQL-инъекции (SQL-injection), межсайтовый скриптинг (XSS) и описание сигнатур, по которым производится их обнаружение.

Представлен интерфейс работы реализованного программного модуля и произведено тестирование, в результате которого получен следующий результат: 89% вторжений были успешно обнаружены.

ЗАКЛЮЧЕНИЕ

В рамках данной работы были изучены системы обнаружения вторжений (СОВ). Рассмотрена структура современных СОВ. Выполнен анализ используемых методов и моделей структуры СОВ в соответствии с выделенными основными группами. Приведены основные недостатки существующих СОВ и обоснованы направления их совершенствования.

Был реализован программный продукт, представляющий собой хостовую СОВ (HIDS), обнаруживающий некоторые из самых распространенных атак и выписывающий рекомендации по защите от них и проведен анализ реализованной СОВ, показавший, что средний процент обнаружения вторжений полученной системой составил 89%.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Городецкий В.И. Многоагентные технологии комплексной защиты информации в телекоммуникационных системах [Электронный ресурс] / В.И. Городецкий, И.В. Котенко, О.В. Карсаев, А.В. Хабаров. СПб.: Труды, 2000. 214 с. Загл. с экрана. Яз. рус.

2. Allen J. State of Practice of intrusion detection technologies [Электронный ресурс] / J. Allen, O. Christie, W. Fithen, J. McHuge, J. Pickel, E. PITS.: Technical Report CMU/SEI-99-TR-028. Carnegie Mellon Software Engineering Institute, 2000. 143 с. Загл. с экрана. Яз. англ.

3. Denning D. An Intrusion Detection Model. [Электронный ресурс] // IEEE Transactions on Software Engineering, н. 13, 1987, с. 222-232. Загл. с экрана. Яз. англ.

4. Heady R. The Architecture of a Network Level Intrusion Detection System [Электронный ресурс] / R. Heady, G. Luger, A. Maccabe, M. Servilla. // Technical report, Department of computer since, University of New Mexico, 1990. 211 с. Загл. с экрана. Яз. англ.

5. Anderson D. Next Generation Intrusion Detection Expert System (NIDES). [Электронный ресурс] // Software Design, Product Specification and Version Description Document, Project 3131, SRI International, July 11, 1994. Загл. с экрана. Яз. англ.

6. Терехов С.А. Байесовы сети [Электронный ресурс] // Научная сессия МИФИ – 2003, V Всеросийская научно - техническая конференция «нейроинформатика-2003»: лекции по нейроинформатике. Часть 1. М.:МИФИ, 2003. 188с. Загл. с экрана. Яз. рус.

7. Debar H. A neural network component for intrusion detection systems [Электронный ресурс] / H. Debar, M. Becker, D. Siboni. // In proceeding of

the 1992 IEEE Computer Society Symposium on Research in Security and Privacy. с. 240 – 250. Oakland. 2012. Загл. с экрана. Яз. англ.

8. Cheng K. An Inductive engine for the Acquisition of temporal knowledge. [Электронный ресурс] / Ph. D. Thesis // Department of computer science, university of Illinois at Urbana-Champain. 2004. Загл. с экрана. Яз. англ.
9. Porras P.A. Event Monitoring Enabling Response to Anomalous Live Disturbance [Электронный ресурс] / P.A. Porras, P.G. Neumann. // Proceeding of the IEEE Symposium on Research in Security and Privacy. Oakland. 2009. 132 с. Загл. с экрана. Яз. англ.
10. Ilgun K. State Transition Analysis: A Rule-Based Intrusion Detection System [Электронный ресурс] / K. Ilgun, R.A. Kemmerer, P.A. Porras // IEEE Trans. Software Eng. vol. 21, н. 3. 2007. Загл. с экрана. Яз. англ.
11. Ilgun K. A Real-time Intrusion Detection System for UNIX [Электронный ресурс] // Proceeding of the IEEE Symposium on Research in Security and Privacy. Okaland. 2015. 112 с. Загл. с экрана. Яз. англ.
12. Heberlein T. A network security monitor [Электронный ресурс] / T. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood. // In Proceeding of the 1990 IEEE Symposium on Research in Security and Privacy. 1990. с. 296 – 304. Загл. с экрана. Яз. англ.
13. Garvey T.D. Model-based Intrusion Detection [Электронный ресурс] / T.D. Garvey, T.F. Lunt. // Proceeding of the 14 th Nation computer security conference. Baltimore. 1991. Загл. с экрана. Яз. англ.
14. Anderson J.P. Computer Security Threat Monitoring and Surveillance [Электронный ресурс] // James P. Anderson Co., Fort Washington, PA, April. 1980. Загл. с экрана. Яз. англ.
15. Sandeep K. An application of pattern matching in intrusion detection, Eugene H. Spafford. [Электронный ресурс] // Technical Report CSD-TR-94-013, The

COAST Project, Dept. Of Computer Sciences, Purdue University, West Lafayette. 2013. Загл. с экрана. Яз. англ.

16. Vern P. A system for detection network intruders in real time [Электронный ресурс] // Proceeding of the 7th USENIX Security Symposium, San Antonio. 1998. Загл. с экрана. Яз. англ.

17. Карве А. Обнаружение атак как средство контроля за защитой сети. [Электронный ресурс] / HackZone. [Электронный ресурс] : [сайт]. URL: http://www.iss.net/products-services/enterprise-protection/rsserver/protector (дата обращения: 30.10.2017). Загл. с экрана. Яз. рус.

18. Evaluating an Intrusion Detection Solution. A Strategy for a Successful IDS Evaluation. [Электронный ресурс] / Internet Security Systems [Электронный ресурс] : [сайт]. URL: https://www.symantec.com/connect/articles/evaluating-network-intrusion-detection-signatures-part-one (дата обращения: 25.11.2017). Загл. с экрана. Яз. англ.

19. Stop Hacker Attacks at the OS Level. [Электронный ресурс] / Internet Security Advisor Magazine. [Электронный ресурс] : [сайт]. URL: http://academy.delmar.edu/Courses/ITSY2430/ (дата обращения: 12.11.2017). Загл. с экрана. Яз. англ.

20. Аудит и мониторинг сети. Адаптивное управление безопасностью. [Электронный ресурс] / Лаборатория сетевой безопасности. [Электронный ресурс] : [сайт]. URL: http://ypn.ru/511/security-monitoring-and-auditing/ (дата обращения: 05.10.2017). Загл. с экрана. Яз. рус.