УДК 004.491
DOI: 10.33764/2618-981X-2020-8-1-165-167

АКТУАЛЬНОСТЬ РАЗРАБОТКИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ С МОДУЛЕМ-ЛОВУШКОЙ

Мидат Олегович Максудов
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, обучающийся

Иван Евгеньевич Дорошенко
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, обучающийся

Андрей Сергеевич Грехов
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, обучающийся

Диана Георгиевна Макарова
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: kaf.ib@ssga.ru

В статье представлена актуальность разработки системы обнаружения вторжения с модулем-ловушкой. Модуль-ловушка, реализованная в рамках системы обнаружения вторжения, позволяет предоставить подробный отчет и информацию об атакующем для системы обнаружения и предотвращения атак типа SNORT.

Ключевые слова: система обнаружения вторжений, атака, модуль-ловушка, предотвращение атак, DoS-атака

RELEVANCE OF THE DEVELOPMENT OF AN INTRUSION DETECTION SYSTEM WITH A TRAP MODULE

Midat O. Maxudov
Siberian State University of Geosystems and Technologies,10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student

Ivan E. Doroshenko
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student

Andrey S. Grehov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student

Diana G. Makarova
Siberian State University of Geosystems and Technologies,10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (383)343-91-11, e-mail: kaf.ib@ssga.ru

The article presents the relevance of developing an intrusion detection system with a trap module. The trap module implemented as a part of the intrusion detection system allows providing a detailed report and information about the attacker for the intrusion detection and prevention system SNORT.

Key words: intrusion detection system, attack, trap module, attack prevention, DoS attack.

В настоящее время все больше предприятий так или иначе задумываются о сохранности информации и бесперебойной работе своих информационных систем. На рынке систем обнаружения атак представлено множество решений. Системы обладают различным функционалом, предлагают различные методы борьбы с атаками. Также наряду с коммерческими программными продуктами на рынке можно встретить и бесплатные версии систем обнаружения вторжений, которые доступны широкому потребителю.

Цель работы – проанализировать существующие на рынке предложения систем обнаружения атак и выработать общую концепцию системы обнаружения атак с модулем-ловушкой.

Самые известные системы обнаружения атак, представленные на рынке на сегодняшний день – это KICS for Networks от «Лаборатории Касперского» и ISIM от Positive Technologies, предназначены для автоматизированной производственной сети предприятия и мало подходят для защиты малых информационных сетей. [1]

Исходя из этого былсделан выбор в пользу свободно распространяемых систем обнаружения атак, однако они также имеют ряд недостатков. Ниже рассмотрены системы обнаружения и предотвращения атак OSSEC, SNORT и Suricata. В таблице представлено их сравнение, достоинства и недостатки.[2]

Сравнительная характеристика систем обнаружения вторжений

IDS/IPS	OSSEC	SNORT	Suricata
Поддерживаемые операционные системы	клиент – windows, linux, FreeBSD, Mac os, Solaris, OpenBSD	windows, linux	windows, linux, FreeBSD, Mac os, Solaris, OpenBSD
Вид IDS/IPS	Узловая	Сетевая	Сетевая
Реакция на атаки нулевого дня	Наличие модулей анализа поведения системы позволяет реагировать на атаки нулевого дня	Нет, так как система является сигнатурной	Нет, так как система является сигнатурной
Возможность реализации на одной рабочей станции	Отсутствует ввиду наличия системы клиент-сервер. При этом сервер OS Linux	Присутствует	Присутствует
Наличие возможности анализа большого количества трафика	Частично присутствует	Отсутствует	Присутствует
Наличие простого и удобного интерфейса	Присутствует при наличии дополнительных модулей	Отсутствует	Отсутствует

Исходя из данных из таблицы в качестве базовой системы обнаружения вторжения для реализации модуля-ловушки будет использована IDS SNORT. Она распространяется бесплатно и достаточно гибкая для интегрирования в нее новых модулей.

IDS SNORT является сигнатурной системой обнаружения и предотвращения атак, идеально подходит в качестве решения проблемы защиты информации на предприятии. Она бесплатна, имеет открытый исходный код, позволяет точнее настроить систему защиты информации под решение разнообразных задач путем подключения только тех модулей, которые необходимы. Благодаря этому IDS SNORT не нагружает систему лишними модулями и не выполняет лишних действий, а также способна оперативно реагировать на инциденты информационной безопасности. [3]

Ни одна из свободно распространяемых систем обнаружения и предотвращения атак, рассмотренных в данной работе, не предоставляет возможности для борьбы и перехвата инициативы с Dos-DDoS атаками и атаками, направленными на захват контроля над системой, подобно их конкурентам из платного сегмента.

Модуль-ловушка, реализованная в рамках системы обнаружения вторжения, позволяет предоставить подробный отчет и информацию об атакующем для системы обнаружения и предотвращения атак типа SNORT. Работающая система должна опираться на свободное программное обеспечение, и его настройка не должна быть осложнена ограничениями компании-поставщика.

Главная цель ловушки – затруднение взлома или иного действия, направленного на понижение работоспособности целевой системы, а также получение информации о методах работы, используемого оборудования и программного обеспечения, IP-адресов и т.д. злоумышленника [4].

Потому разработка концепции модуля-ловушки, предназначенного для сбора информации об атакующем, и для предотвращения вышеупомянутых атак в дальнейшем, является актуальной.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Сравнение промышленных СОВ: ISIM vs. KICS [Электронный ресурс]. URL: https://habr.com/ru/company/jetinfosystems/blog/450956/ (дата обращения: 20:02:20).
2. 5 open-source систем управления событиями безопасности [Электронный ресурс]. URL: https://habr.com/ru/company/cloud4y/blog/459442/ (дата обращения 20:02:20).
3. Обнаружение телекоммуникационных атак: теория и практика, Snort [Электронный ресурс]. URL: http://samag.ru/archive/article/196 (дата обращения: 20:02:20).
4. Крис Касперски "Техника сетевых атак. Приёмы противодействия. Глава 'Что такое интернет' (Архитектура интернет. Дерево протоколов. Пакеты в Internet. Назначение портов.) : СОЛОН-Р, 2001.