УДК 004.491
DOI: 10.33764/2618-981X-2020-8-1-160-164

ВАРИАНТ 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 представлен вариант системы обнаружения вторжения с модулем-ловушкой. Предложенная система, состоящая из нескольких взаимодействующих модулей (IDS Snort, SIEM SAGAN, модуль-ловушка), позволяет бороться с разными межсетевыми угрозами от атак типа DoS до атак, направленных на захват контроля системой.

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

A VERSION 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 a variant of an intrusion detection system with a trap module. The proposed concept, consisting of several interacting modules (IDS Snort, SIEM SAGAN, trap module), allows dealing with various firewall threats from DoS attacks to attacks aimed at taking control of over the system.

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

В настоящее время особое внимание уделяется системам обнаружения вторжений (СОВ), которые выполняют ключевую функцию в процессе предотвращения кибератак. На рынке СОВ представлено множество решений – коммерческие, свободно распространяемые, с различными дополнительными функциями и модулями [1, 2]. Ниже представлено описание известных коммерческих систем обнаружения атак KICS for Networks от «Лаборатории Касперского» и ISIM от Positive Technologies.

Функциональные возможности обеих систем обнаружения атак предоставляют все основные функции:

– мониторинг технологической сети с возможностью поддержки технологических протоколов основных производителей автоматизированных систем управления технологическим процессом;

– автоматическое определение типа устройства;

– возможность контроля технологического процесса;

– обнаружение вторжений в технологическую сеть;

– передача зарегистрированных событий в сторонние системы мониторинга (SIEM) с возможностью их анализа;

– графическое построение карты технологической сети;

– создание и выгрузка отчетов;

– помощь в расследовании инцидентов.

Вместе с тем обе системы имеют несколько весомых недостатков:

– обе системы обнаружения атак платные;

– мониторинг обеих систем осуществляется только посредством веб-интерфейса;

– некоторые правила для обеих систем обнаружения атак возможно прописать только с помощью специалистов компаний, их распространяющих;

Вышеперечисленные системы обнаружения и предотвращения вторжений предназначены для автоматизированной производственной сети предприятия и мало подходят для защиты относительно небольших информационных сетей.

Целью работы является разработка концепции СОВ с модулем-ловушкой на базе IDS SNORT, поскольку ни одна из свободно распространяемых СОВ (OSSEC, SNORT, Suricata) 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 (KICS for Networks от «Лаборатории Касперского», ISIM от Positive Technologies) [1].

Модуль-ловушка представляет собой средство защиты информации, входящее в СОВ, направленное на затруднение взлома или иного действия, ориенти-

рованного на понижение работоспособности целевой системы и получение информации о методах работы, используемого оборудования, программного обеспечения, IP-адресов и т.д. злоумышленника. На рис. 1 представлены виды ловушек [3].

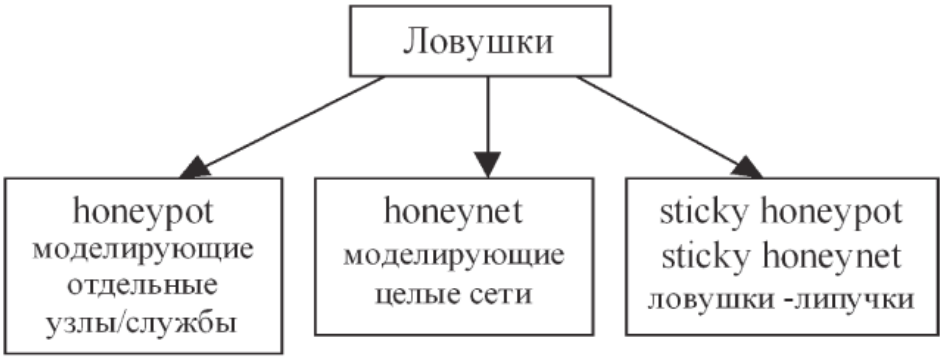

Рис. 1. Виды ловушек

Стабильная популярность атак семейства Dos-DDos (атака типа отказ в обслуживании и распределенный отказ в обслуживании), а также атак, направленных на удаленный захват контроля над системой, порождает необходимость комплексного подхода к решению данной задачи. В основе многих систем защиты локальных вычислительных сетей (ЛВС) лежит СОВ, представляющая собой программный и/или программно-аппаратный комплекс средств, направленных на анализ, выявление и предотвращение вредоносной активности (Dos-DDOS, а также атаки направленные на удаленный захват системой). Функционал данных инструментов включает превентивное воздействие на локальные источники атак, анализ вредоносной активности, а также способы противодействия атакам. Однако ни одна из существующих систем обнаружения и предотвращения атак не может обеспечить гарантированную безопасность информационной сети [4].

Одним из возможных способов реализации оптимального уровня защиты информационной сети является введение злоумышленника в заблуждение, или же попытка установить истинного злоумышленника атаки посредством создания модуля-ловушки. Его использование заставит нарушителя выполнить больший объем действий и позволит администратору предпринять меры к предотвращению атаки и идентификации атакующего.

Предлагаемая концепция СОВ с модулем-ловушкой основывается на возможности получения более подробного отчета и информации об атакующем для СОВ SNORT. Предлагаемая концепция СОВ должна опираться на свободное программное обеспечение (open source), а также его настройка не должна быть осложнена ограничениями компании поставщика. Концепция реализации СОВ указана на рис. 2.

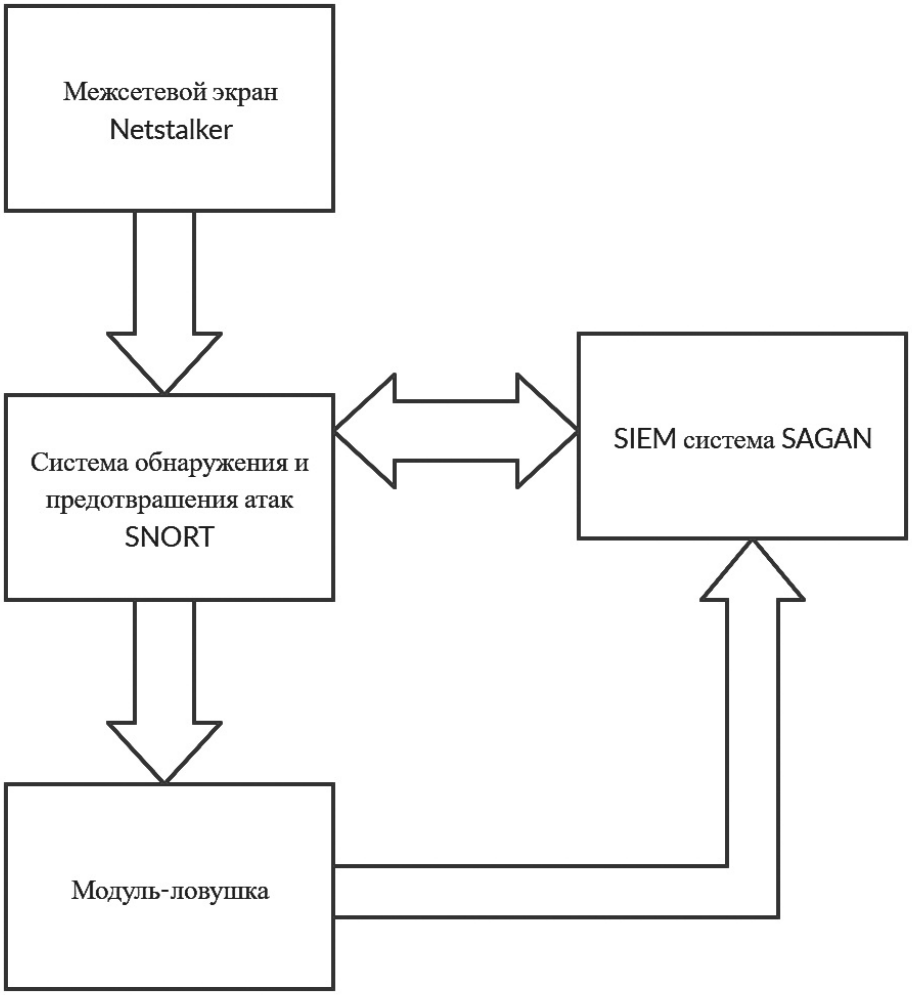

Рис. 2. Схема разрабатываемой системы

Составные части блок-схемы:

– IDS-IPS SNORT, являющийся частью целевой ИС (информационной системы);

– SIEM система Sagan, входящая в состав образа linux, установленная дополнительно;

– межсетевой экран Netfilter;

– модуль-ловушка, или система реакции и деанонимизации нарушителя.

На рис. 3 представлена схема реализации модуля-ловушки для локальной вычислительной сети. В случае атаки будет осуществлен обмен данными с SIEM системой, уведомление администратора и соответствующая реакция на атаку. Система реакции не просто запишет ip-адрес нарушителя в соответствующий список, но и введет его в заблуждение посредством инструментов Delude и Chaos, а также вычислит его примерное местоположение посредством инструментов Geoip и piGeoip.

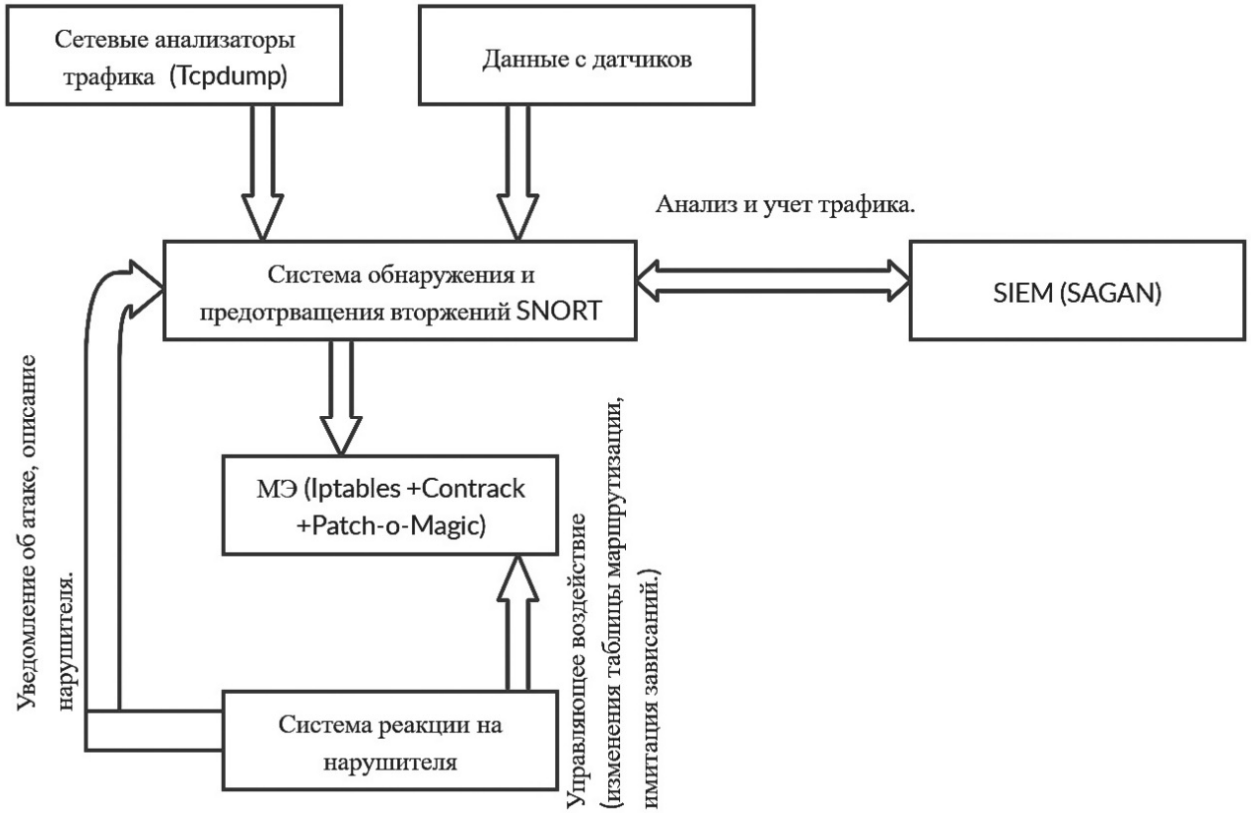

Рис. 3. Схема реализации модуля-ловушки

Предложенная концепция СОВ с модулем-ловушкой, состоящая из нескольких взаимодействующих модулей (IDS Snort, SIEM SAGAN, модуль-ловушка), позволяет бороться с разными межсетевыми угрозами от атак типа DoS до атак, направленных на захват контроля системой. Особенностью предлагаемой системы является возможность деанонимизировать злоумышленника. Преимуществом такой концепции является простота ее реализации, а также возможность использования свободно распространяемого программного обеспечения.

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.