ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2016» атты XI Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XI Международной научной конференции студентов и молодых ученых «НАУКА И ОБРАЗОВАНИЕ - 2016»

PROCEEDINGS of the XI International Scientific Conference for students and young scholars «SCIENCE AND EDUCATION - 2016»

2016 жыл 14 сәуір
Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2016» атты XI Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XI Международной научной конференции студентов и молодых ученых «Наука и образование - 2016»

PROCEEDINGS of the XI International Scientific Conference for students and young scholars «Science and education - 2016»

2016 жыл 14 сәуір

Астана

ӘӨЖ 001:37(063)
КБЖ 72:74
Ғ 96

Ғ96 «Ғылым және білім – 2016» атты студенттер мен жас ғалымдардың XI Халық. ғыл. конф. = XI Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2016» = The XI International Scientific Conference for students and young scholars «Science and education - 2016» . – Астана: http://www.enu.kz/ru/nauka/ nauka-i-obrazovanie/, 2016. – .... б. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-764-4

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

ӘОЖ 001:37(063)
КБЖ 72:74

ISBN 978-9965-31-764-4

УДК 681.3.07

СПОСОБЫ СОЗДАНИЯ СИСТЕМЫ МОНИТОРИНГА, АНАЛИЗА И ОТВЕТНОЙ РЕАКЦИИ CISCO MARS

Лубенская Светлана Николаевна
lubenskaya_svetlana@mail.ru
Магистрант 2-го курса физико-технического факультета,
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – Бурамбаева Н.А.

Cisco MARS является комплексной системой, не имеющей аналогов в обнаружении, мониторинге и управлении корпоративной системы безопасности. Система дает сетевым инженерам и систематехникам возможность выявления проблем и изолировать объекты которые нарушают политику безопасности корпоративной сети. Также система поддерживает соответствующие политики безопасности и может соответствовать различным политикам безопасности в зависимости от корпоративных нормативных документов.

MARS может обрабатывать до 10 тысяч событий в секунду. Система поддерживает масштабируемость, то есть в сетях крупных предприятий и интернет провайдеров есть возможность создать несколько уровневую архитектуру за счет использования MARS-контроллеров, к которым может подключиться несколько MARS-серверов. При использовании такой архитектуры вся сеть делится на «зоны» и каждая закрепляется за своим определенным MARS-сервером [1].

Сложность сетевой инфраструктуры влечет за собой увеличение количества средств защиты – этими устройствами могут быть отдельные межсетевые экраны, маршрутизаторы с определенным функционалом программного обеспечения, коммутаторы, различные системы IPS, IDS, HIPS-системы, а также различные антивирусные системы, почтовые прокси-серверы, web-прокси и другие подобные системы. Большое количество средств защиты рождает проблемы управления, так как возрастает количество контрольных точек, растет количество регистрируемых событий и как следствие увеличивается время необходимое для принятия решений.

Рисунок 1 – процесс принятия решения для предотвращения атаки

В связи с этим для предприятия возникает необходимость в системе более высокого уровня, способной оценить существующий уровень информационной безопасности, произведя регистрацию и корреляцию поступивших в систему событий. Система мониторинга и реагирования Cisco MARS обеспечивает выполнение данных функций. Cisco MARS представляет собой программно-аппаратное решение в серверном исполнении. Программное обеспечение системы базируется на операционной системе Linux. Основным компонентом системы является база данных Oracle, использующаяся для хранения информации.Cisco MARS имеет возможность сбора информации с различных устройств по протоколам Syslog, SNMP, NetFlow, а также имеет возможность принимать системные лог-файлы. MARS поддерживает оборудование различных вендоров таких как Cisco, IBM, Check Point, Nokia, Symantec, McAfee, Netscape и других [1].

Логика работы системы Cisco MARS базируется на запросах к базе данных. Можно выбирать информацию и уточнять её по IP-адресу источника, IP-адресу приемника, портам, типам событий, устройствам, по ключевым словам и так далее. На базе запросов базируются определенные правила, которые группируются в системе. В базе Cisco MARS содержит более 2000 правил. Можно создавать свои правила, тем самым гибко адаптировать систему к конкретным видам предполагаемых угроз.

После сохранения правила и обнаружения информации, удовлетворяющей данному правилу – формируется инцидент.

Рассматривая работу Cisco MARS можно предложить конкретный пример выполнения атаки на хост.

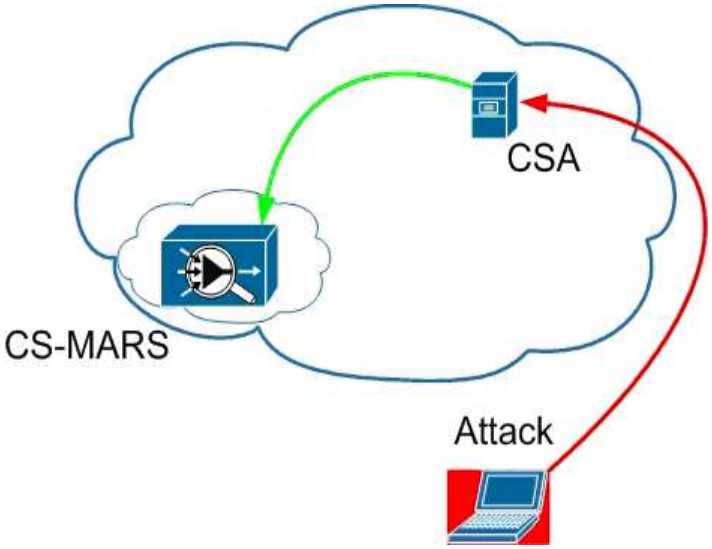

Рисунок 2 – выполнение атаки на пользователей в сети

Пример, содержащий Cisco MARS, 15 роутеров и хост с установленным продуктом Cisco Security Agent. Для эмулирования атаки выполнено сканирование сервисов хоста при помощи утилиты NMAP.

При этом события выглядят следующим образом:

- Cisco Security Agent зафиксировал сканирование портов;
- Информация об этом попала на менеджмент центр системы Cisco Security Agent, который в свою очередь отправил сообщение на MARS;
- MARS произвел синтаксический разбор и нормализацию полученого сообщения к единому виду, предусмотренному базой данных;

MARS поддерживает оборудование различных вендоров таких как Cisco, IBM, Check Point, Nokia, Symantec, McAfee, Netscape и других.

Логика работы системы Cisco MARS базируется на запросах к базе данных. Можно выбирать информацию и уточнять её по IP-адресу источника, IP-адресу приемника, портам, типам событий, устройствам, по ключевым словам и так далее.Cisco MARS имеет возможность сбора информации с различных устройств по протоколам Syslog, SNMP, NetFlow, а также имеет возможность принимать системные лог-файлы. Cisco MARS представляет собой программно-аппаратное решение в серверном исполнении. Программное обеспечение системы базируется на операционной системе Linux. Основным компонентом системы является база данных Oracle, использующаяся для хранения информации [2].

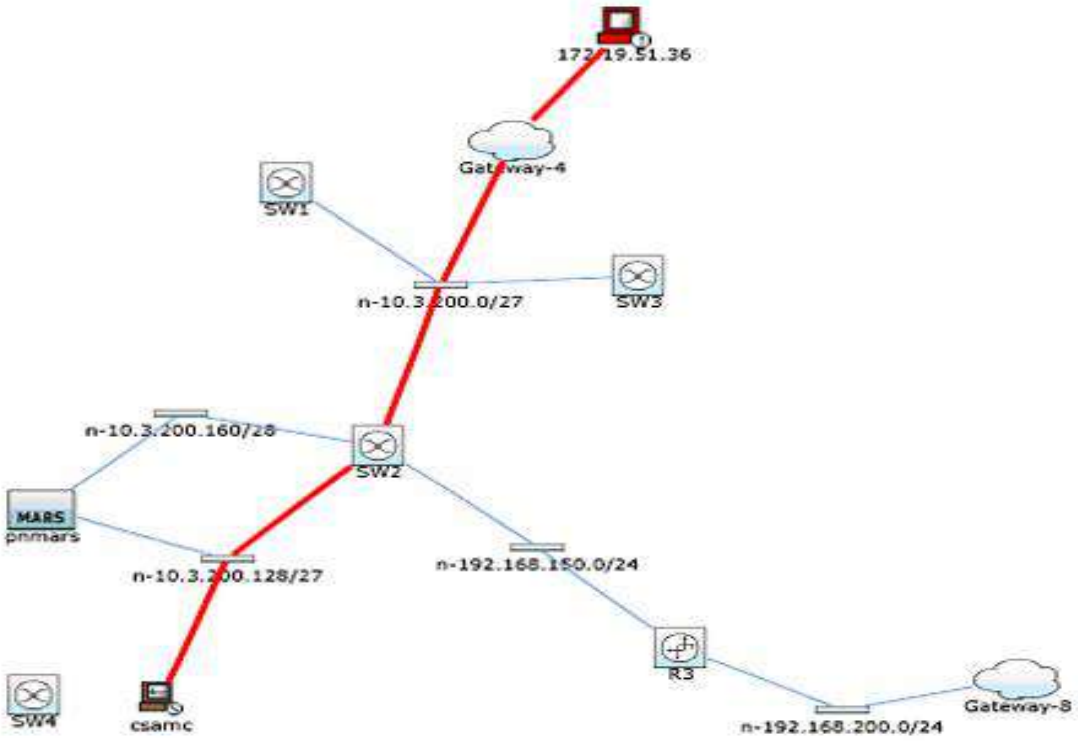

Рисунок 3 – Сетевая топология пути распространения атаки

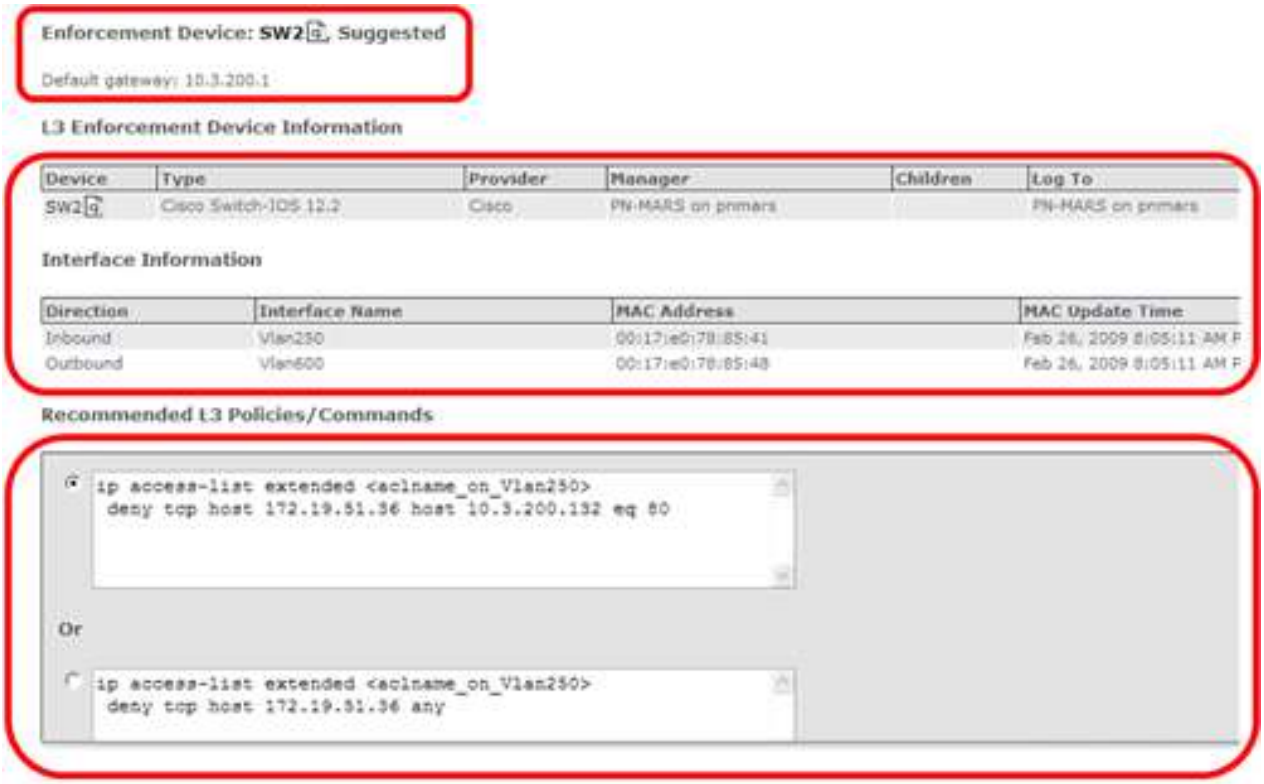

Рисунок 4 – Ответные меры для предотвращения атаки

Данное событие было проверено при помощи правил, настроенных на MARS с целью регистрации инцидентов информационной безопасности;

Также Cisco MARS имеет гибкую систему отчетов, что позволяет получать детализированные данные по всем зарегистрированным событиям. Это позволяет реализовывать принцип совершенствования защиты. Приведена рабочая область на приборной панели Web-интерфейса MARS.

На главной странице Cisco MARS появилась информация о том, что с сети произошел инцидент информационной безопасности, и показан путь распространения атаки.

В качестве ответных мер на возникший инцидент Cisco MARS предлагает несколько вариантов предотвращения атаки с привязкой к сетевым устройствам:

Предустановленные правила с Cisco MARS

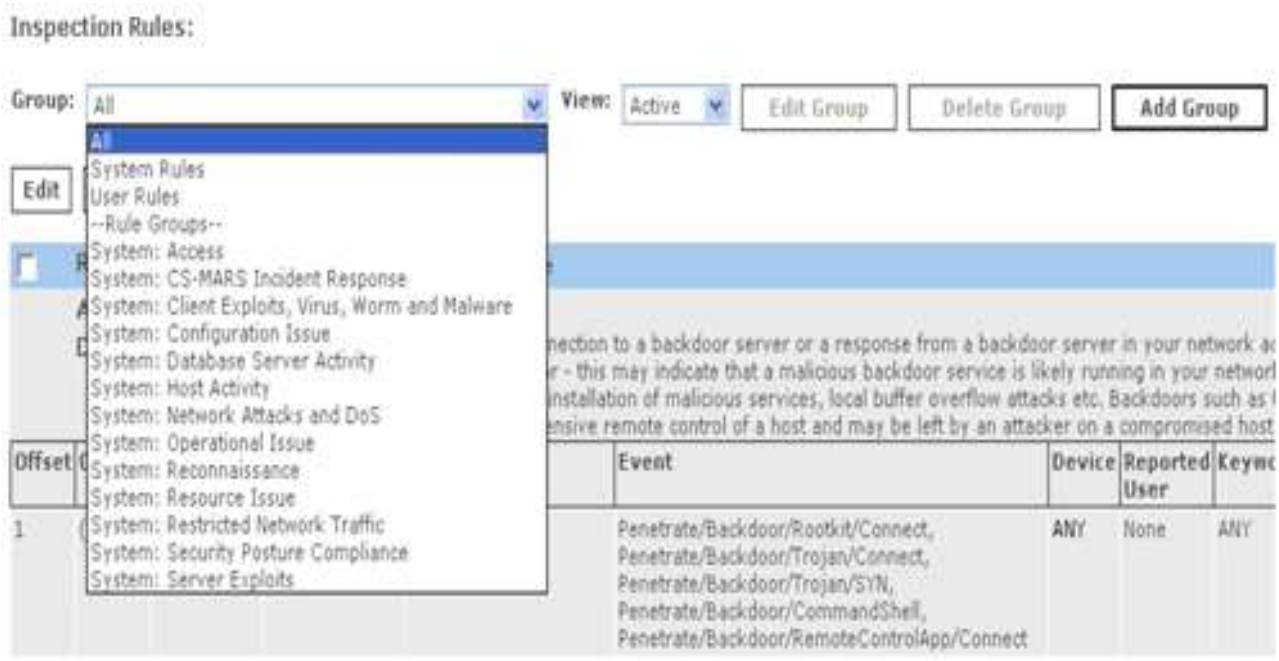

Рисунок 5 – Предустановленные правила

Для более глубокой настройки требуется в соответствии с прогнозируемыми моделями угроз составлять свои правила, которые будут анализировать поступающую информацию.

При наличии всех необходимых условий, прописанных в правиле, создается инцидент, который можно увидеть на главной панели системы. Также возможна отправка уведомления на электронную почту персонала, обслуживающего Cisco MARS

Согласно концепции информационной безопасности Республики Казахстан до 2016 года, информационная безопасность в компании должна быть на высоком уровне и уметь отслеживать и предотвращать взломы как с внешней стороны, так и внутренние угрозы.

Согласно этому в сети предприятия решено вводить так называемую систему контроля трафика и мониторинга состояния сети cisco mars. Данная система позволяет решить такие задачи как: Интеграция в сеть интеллектуальных функций для повышения эффективности механизма корреляции сетевых аномалий и событий безопасности.

Список использованных источников

1. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP- сетей. – СПб.: БХВ-Петербург, 2001, 512 с.
2. Уэнстром М., Организация защиты сетей Cisco. – Вильямс, 2005, 720 с.
3. Прицкер А., Введение в имитационное моделирование и язык СЛАМ II. – М.: Мир, 1987, 646 с.