Предложенная модель может быть использована для обеспечения безопасности информационных систем после формирования значений меток $p_{ij}^{1}(k)$ и $p_{ij}^{2}(k)$ с помощью обучающих алгоритмов.

Список использованных источников

1. Цветов В.П. О вложении измерительных шкал // Международная научно-техническая конференция "Перспективные информационные технологии (ПИТ-2018)". - 2018. - С. 341-344.

2. Tsvetov V. P. Dual ordered structures of binary relations // CEUR Workshop Proceedings. - 2018. - Vol. 2212. - P. 304-311

3. Tsvetov V. P. Algebras of finitary relations // CEUR Workshop Proceedings. - 2019. - Vol. 2416. - P. 119-125

Цветов Виктор Петрович, кандидат физико-математических наук, доцент, доцент кафедры безопасности информационных систем. E-mail: tsf-su@mail.ru

УДК 004.056.53, 004.056.2

СРЕДСТВО ЗАЩИТЫ ДЛЯ ОБНАРУЖЕНИЯ АТАК НА ПРОТОКОЛ EIGRP

Д.Р. Мозжухин
Московский Авиационный Институт (МАИ), г. Москва

Ключевые слова: кибербезопасность, протоколы маршрутизации, EIGRP, средство защиты информации.

Протоколы маршрутизации в сети Интернет играют очень важную роль, так как именно с помощью этих протоколов пользователи сети могут обмениваться информацией как удаленно - то есть в сети WAN, так и в сетях с маленькой площадью, например, в корпоративных сетях.

За все время существования сети Интернет пользователи разработали большое количество протоколов маршрутизации. Существуют два вида протоколов: протоколы внутридоменной и внешнедоменной маршрутизации. Как понятно из названия, протоколы внутридоменной маршрутизации используются для связи устройств внутри домена, а протоколы внешнедоменной маршрутизации используются для связи самих доменов. Их совместное использование задействуется для работы сети Интернет [1-2].

В ходе анализа открытых источников было выявлено, что наиболее популярными протоколами внутридоменной маршрутизации являются OSPF и EIGRP. При рассмотрении протокола EIGRP было обнаружено, что данный протокол имеет несколько преимуществ по сравнению с OSPF, а именно:

1. Используемый объем памяти меньше, так как хранится информация только о соседних маршрутизаторах;

2. Тонкая настройка пути, так как в формуле расчета пути используются различные коэффициенты, которые можно отключать по желанию;

3. Высокая скорость сходимости из-за передачи информации только между соседними маршрутизаторами [3].

Во время рассмотрения различных интернет ресурсов было выявлено, что EIGRP имеет низкую защищенность при проведении DDoS-атак, MITM-атак и атак типа Route Injection.

Для повышения защищенности данного протокола необходимо разработать средство защиты информации, которое будет способно обнаруживать вышеперечисленные атаки и предупреждать пользователя о них.

Чтобы обеспечить корректную защиту необходимо самостоятельно провести атаки на тестовой модели сети, в которой используется EIGRP. Во время атаки необходимо записать состояние сети, например, при помощи сниффера WireShark. Далее требуется проанализировать полученный трафик и выделить ключевые характеристики каждой атаки, чтобы корректно написать правило для детектирования атак.

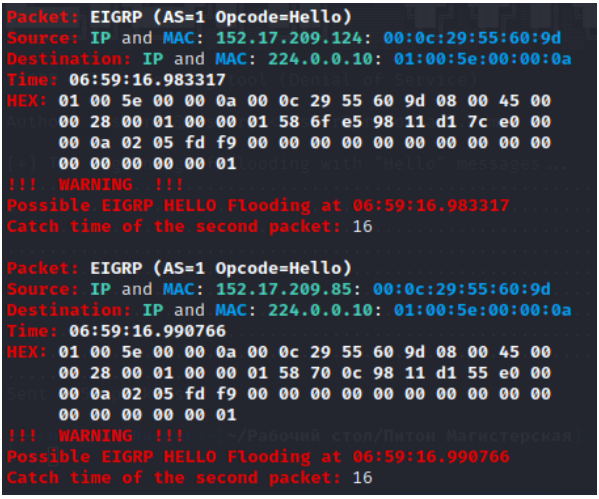

Рисунок 1 - Пример детектирования DDoS-атаки

После выполнения вышеперечисленных действий были получены следующие характеристики атак:

DDoS:

– Разрыв соединения с несуществующим маршрутом.
– Быстрорастущее число пакетов.

MITM:

– Наличие в ARP таблице двух одинаковых физических адресов.

– Наличие в трафике ARP-пакета для IP, который не входит в инфраструктуру компании.

Инъекция маршрута:

– Большое число несуществующих маршрутов в таблице маршрутизации.

– Быстрорастущее число update пакетов в dump’е трафика.

Данные характеристики помогли написать программу, представляющую собой средство защиты информации, которое использует правила, помогающие корректно детектировать атаки на протокол EIGRP. Ниже представлен пример детектирования DDoS атаки.

Исходя из вышеописанного можно сделать вывод о том, что для любой атаки, кроме атак нулевого дня, возможно создать средство защиты либо написать правило, которое поможет обнаружить злоумышленника, что поспособствует защите различной чувствительной информации. Также можно сказать, что разработанное средство детектирования атак оказалось эффективным для обнаружения атак.

Список использованных источников

1. Okonkwo Comparative study of EIGRP and OSPF protocols based on network convergence / Okonkwo, a. E. IJ, ID. — Текст : непосредственный // International Journal of Advanced Computer Science and Applications. — 2020, № 6. — С. 39-45.

2. Understand and Use the Enhanced Interior Gateway Routing Protocol. — Текст: электронный // Cisco: [сайт]. — URL: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html (дата обращения: 16.12.2023).

3. EIGRP // Cisco Learning URL: https://ciscolearning.ru/cisco-router/eigrp/ (дата обращения: 16.12.2023).

Мозжухин Даниил Ринатович, студент каф. 402 Московского Авиационного Института, danigrok3@gmail.com.

УДК 621.396:629.7

РАЗРАБОТКА ПРОТОКОЛА СВЯЗИ

А.Т. Хакимхан, Е.А. Бобина
КНИТУ-КАИ им. А. Н. Туполева, г. Казань

Ключевые слова: ультрафиолетовая связь, протокол передачи, система.

Лазеры, благодаря своей способности преобразовывать энергию в высоконаправленные лучи электромагнитного излучения, нашли широкое применение в современных оптических системах связи [1]. Основываясь на принципе возбуждения атомов или молекул в активном элементе и последующей генерации когерентного излучения, лазеры обеспечивают