А.В.САСКЕВИЧ[1], М.В.СТЕРЖАНОВ[1]

ОПРЕДЕЛЕНИЕ MITM-АТАК (MAN-IN-THE-MIDDLE) ПОСРЕДСТВОМ МАШИННОГО ОБУЧЕНИЯ

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Активное использование корпоративных сетей на предприятиях и бесплатных VPN-сервисов создает благодатную почву для MITM-атак, позволяющих перехватить и скомпрометировать

входящий и исходящий сетевой трафик. Атаки Man-In-The-Middle подразумевают разнообразный спектр атак, таких как отравление кешей сетевых устройств, атаки на SSL-сертификаты/Content-Authority сервисы, атаки на DNS сервисы и сессии [1]. В совокупности такие атаки составляют не менее 35-40% от общего числа атак на вычислительные сети и устройства [2]. Особую проблему составляет детектирование и отражение таких атак. На текущий момент готовых промышленных решений, позволяющих определять подобные атаки в режиме реального времени не существует, возможные решения имеют превентивный характер либо являются узкоспециализированными для конкретных задач и оборудования. В то же время существует достаточное количество инструментов для генерации подобных атак в академических целях. В связи с этим для решения подобной задачи требуется совершить следующие действия – сгенерировать и собрать данные для обучающей выборки, выделить необходимые характеристики для обучения модели, подготовить и обучить модель, протестировать ее на тестовых данных, интегрировать в существующую сетевую инфраструктуру. Следует отметить, что в связи с тем, что MITM-атака подразумевает несколько различных классов атак, модель и данные для каждого из классов должны подготавливаться отдельно и независимо.

Для генерации и сбора данных для обучающей выборки можно воспользоваться дистрибутивом Kali Linux – операционной системой Linux с набором инструментов и утилит для работы специалистов информационной безопасности. Посредством этой ОС возможно создание скомпрометированной виртуальной сети, анализ трафика внутри ее и генерация атак на нее [3]. Наиболее важными характеристиками, которые следует учесть при проектировании модели и сборе данных, являются время ответа, MAC/IP-адрес отправителя, последовательность посылаемых пакетов в зависимости от анализируемого сетевого протокола, адресацию в сетях и подсетях, наличие и состояние хеш-сумм и цифровых подписей [4,5]. Появление промежуточного скомпрометированного узла влияет на состояние указанных характеристик. Также важно, что сбор данных может производиться на разных сетевых уровнях модели OSI, например, сбор данных для детектирования DNS-атак может производиться на транспортном и/или сетевом уровне, детектирование атак на кеши сетевых устройств – на канальном и/или сетевом уровне, а детектирование атак на пользовательские сессии возможен на прикладном уровне (рисунок 1) [6]. Выбор уровня OSI для анализа зависит также от типа исследуемой атаки.

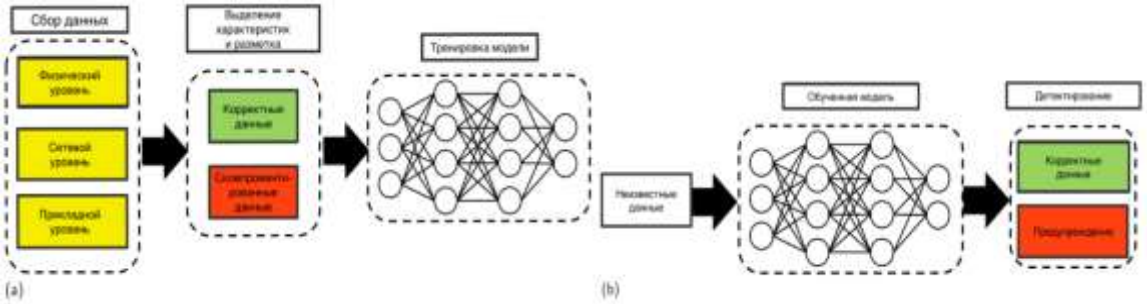

Рисунок 1 – (a) обучение CNN/RNN модели и (b) использование модели

Кроме того, сбор данных должен происходить либо в режиме обработки отдельных пакетов, либо в режиме обработки последовательностей пакетов. Это зависит от архитектуры нейронной сети, выбранной для детектирования того или иного типа атаки. Для детектирования атак в режиме реального времени на основе анализа последовательностей пакетов возможно использование рекуррентных RNN-сетей, для анализа отдельных пакетов подойдут сверточные CNN-сети [7].

Обучающий набор данных размером в 100000 пакетов и набор данных для валидации размером в 10000 пакетов, использование в качестве характеристик заголовки TCP-пакетов и рекуррентная RNN-сеть позволяют достичь точности около 75% в определении атак на DNS протокол. Аналогичных результатов можно добиться в отношении других видов MITM- атак. Изменение архитектуры сети и размер обучающей выборки на точность результата повлияли незначительно.

Таким образом, посредством машинного обучения возможно детектирование атак различного рода, например, таких как отравление кешей сетевых устройств, атаки на сессии и DNS сервисы, атаки на SSL-протокол. За активным развитием сетевых технологий собранные данные и модели могут быстро устаревать, поэтому любая модель машинного обучения должна иметь возможность итеративно доучиваться после накопления нового набора данных.

ЛИТЕРАТУРА

1. Gangan S. A review of man-in-the-middle attacks // arXiv preprint arXiv:1504.02115. – 2015.

2. Swinhoe D. What is a man-in-the-middle attack? How MitM attacks work and how to prevent them. – 2019.

3. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // ICISSp. – 2018. – Т. 1. – С. 108-116.

4. Lan H. et al. Traffic data classification to detect man-in-the-middle attacks in industrial control system //2019 6th International Conference on Dependable Systems and Their Applications (DSA). – IEEE, 2020. – С. 430-434.

5. Calvert C. et al. A procedure for collecting and labeling man-in-the-middle attack traffic //International Journal of Reliability, Quality and Safety Engineering. – 2017. – Т. 24. – №. 01. – С. 1750002.

6. Kim S., Park K. J. A Survey on Machine-Learning Based Security Design for Cyber-Physical Systems //Applied Sciences. – 2021. – Т. 11. – №. 12. – С. 5458.

7. Kozlenko, Mykola & Valerii, Tkachuk. (2019). Deep learning based detection of DNS spoofing attack. 10.5281/zenodo.4091018.