Н.П.ШАРАЕВ[1], С.Н.ПЕТРОВ[1]

ОБНАРУЖЕНИЕ ПРИЗНАКОВ СЕТЕВОЙ РАЗВЕДКИ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

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

Неотъемлемым элементом таргетированной атаки на информационную систему предприятия является сетевая разведка. Сетевая разведка – это комплекс мероприятий по получению и обработке данных об информационной системе, функционирующих в ней информационных ресурсах, средствах защиты информации и используемом программном обеспечении. В связи с тем, что сетевая разведка является первым звеном атаки и предваряет собой активные действия, ее обнаружение позволяет заблаговременно выполнить поиск возможных уязвимостей и предпринять меры по снижению рисков.

Сетевая разведка может проводиться следующим образом:

– получение информации от whois-серверов (контактные данные владельца доменного имени и список DNS-серверов, которым делегировано доменное имя);

– получение информации от DNS-серверов (связи между доменным именем и IP-адресами);

– сканирование сети (доменных имен);

– сканирование портов (определение открытых портов на компьютере или сервере и списка запущенных служб).

Наибольший интерес для обнаружения сетевой разведки представляют последние два пункта, что связано с невозможностью ограничения доступа к whois- и DNS-серверам.

В отличие от других способов обнаружения признаков сетевой разведки [1], использование нейронной сети позволит использовать максимальное число параметров, извлекаемых из сетевых пакетов или сегментов, а также избежать ограничений статистического анализа. Под использованием

максимального числа параметров подразумевается возможность добавить при обучении в нейронную сеть любого параметра сетевого пакета (сегмента) и в кратчайшие сроки узнать его влияние на комплексное обнаружение признаков сетевой разведки. Похожее исследование уже было проведено [2], однако параметры, которые использовались при обучении нейронной сети были статистические и, следовательно, подвержены тем же недостаткам, что и статистические методы.

Использование предлагаемого подхода уменьшит количество потребляемых вычислительных ресурсов ЭВМ для обучения нейронной сети.

В качестве входного тестового вектора данных (датасета) для обучения нейронной сети предлагается использовать вектор, состоящий из классических параметров: размера сетевого пакета, числа сетевых пакетов в потоке, типа сетевого протокола транспортного уровня, числа сетевых пактов протокола каждого типа, числа входящих и исходящих соединений [1]. После обучения нейронной сети на указанном датасете проводится расчет эффективности и сравнение ее с аналогами. В случае неудовлетворенности результатами предлагается добавление новых параметров в датасет для дообучения нейронной сети, в частности: флагов протокола транспортного уровня, скорости получения новых пакетов от каждого протокола и каждого хоста, время между отправкой пакетов с одного хоста и другие.

Для работы с массивами данных выбран язык программирования Python, включая библиотеку scikit-learn для извлечения признаков из набора данных. Использована база данных Redis.

ЛИТЕРАТУРА

1. Способ обнаружения аномалий в трафике магистральных сетей Интернет на основе мультифрактального эвристического анализа : пат. RU 2696296 C1 / П. Д. Зегжда, Д. С. Лаврова. – Опубл. 01.08.2019.

2. Сухов, В. Е. Система обнаружения аномалий сетевого трафика на основе искусственных иммунных систем и нейросетевых детекторов / В. Е. Сухов // Вестник РГРТУ. – 2015. – № 54, Ч. 1. – С. 84.