Система поиска несанкционированных пользователей информационной системы

Е. Г. Самончик
Белорусский государственный университет информатики и радиоэлектроники, Минск, Республика Беларусь
Научный руководитель: Дворникова Т.Н. – старший преподаватель, магистр техн. наук каф. ИРТ

Аннотация

Система поиска несанкционированных пользователей (далее СПНП) на базе языка *Python* реализована в виде веб-приложения, а также разработана модель нейронной сети для обнаружения DoS и PortScan атак.

Ключевые слова: *DoS*, *PortScan*, *Python*, технические требования, схема структурная, алгоритм.

Введение

Объемы информации, циркулирующие в локальных вычислительных сетях (ЛВС), увеличиваются с каждым днём, также расширяется спектр задач, решаемых с помощью информационных систем, а значит увеличивается число угроз и уязвимостей информационных ресурсов. В связи с этим возрастают требования к системам защиты ЛВС, которые должны обеспечивать не только пассивное блокирование несанкционированного доступа (НСД) к внутренним ресурсам сети предприятия из внешних сетей, но и осуществлять обнаружение успешного НСД.

Раннее обнаружение НСД к ИС позволит своевременно устранить их причину, а также предотвратить возможные катастрофические последствия, в следствии вторжений из внешних сетей.

1. Описание принципа работы системы поиска несанкционированных пользователей информационной системы

В общем случае СПНП состоит из подсистемы сбора информации, подсистемы анализа данных и подсистемы представления данных.

Структурная схема СПНП представлена на рисунке 1:

Рис. 1. Структурная схема СПНП

Sniffer пакетов отвечает за перехват пакетов, поступающих на сетевую карту до того, как они попадут в стек протоколов для последующей их передачи на препроцессор и декодер пакетов.

Декодер пакетов занимается разбором заголовков захваченных пакетов, поиском аномалий и исключением отдельных протоколов из дальнейшего анализа и другой аналогичной работой.

Если декодер разбирает трафик на втором и третьем уровне эталонной модели, то препроцессор предназначен для более детального анализа и нормализации протоколов на третьем, четвертом и седьмом уровнях.

Детектор имеет два режима работы: режим обучения и режим тестирования. При обучении, на вход детектора попадают заранее подготовленные данные, предназначенные для

обучения и тестирования, и при помощи алгоритма обучения проводится обучение нейронной сети. При тестировании детектор использует модель полученную при обучении и определяет степень аномальности захваченных пакетов сетевого трафика.

После обнаружения атаки модуль вывода может выдать (записать или отобразить) соответствующее сообщение в различных форматах – текстовый файл, *Syslog*, *ASCII* и т. д.

2. Разработка программной части автоматизированной системы управления

Для разработки программной части СПНП использовалась интегрированная среда разработки *PyCharm,* представляющая собой графический инструмент, который позволяет импортировать все необходимые библиотеки для языка *Python.*

В качестве модуля для захвата трафика выбрана программа *CICFlowMeter*. Выходные данные приложения представляют собой формат файла *CSV*.

Обучение нейросети происходило на базе библиотек *TensorFlow* и *Keras.*

В качестве информации для обучения выступает набор данных CICIDS2017, содержащий современные распространённые атаки, похожие на реальные.

Представление данных осуществляется веб-приложением, осуществлённым на базе подключаемой библиотеки *Aiohttp* для *Python Asyncio.*

Заключение

В работе представлена сетевая система обнаружения вторжений с применением нейросетевых технологий при помощи языка программирования *Python*.

Использование нейронных сетей позволило анализировать искаженные данные и увеличить скорость обработки данных.

Список литературы

[1] **Вострецова, Е. В.** Основы информационной безопасности: учебное пособие для студентов вузов – Екатеринбург: изд-во Урал. ун-та, 2019. – 204 с.

[2] **Лукацкий А. В.** Обнаружение атак. – СПб: БХВ-Петербург, 2001. – 624 с.

[3] ИНТУИТ. Основы теории нейронных сетей [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/studies/courses/88/88/info.

The search system for unauthorized users of the data system

Y. G. Samonchyk

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Scientific supervisor: Dvornikova T.N. - senior lecturer, master of tech. Sciences

department: IRT

Annotation

The Python-based search system for unauthorized users (hereinafter referred to as the SPNP) is implemented as a web application, and a neural network model has been developed to detect DoS and PortScan attacks.

Keywords: DoS, PortScan, Python, technical requirements, structural scheme, algorithm.