УДК 681.12

Е.І. Колібабчук
О.П. Войтович

ЗАСІБ ДЛЯ ВИЯВЛЕННЯ DOS-АТАК

Вінницький національний технічний університет

Анотація
Запропоновано програмний засіб для виявлення атак на відмову в обслуговуванні. Проведено моделювання атак типу TCP Syn Flood, Slowloris, SSL DoS.
Ключові слова: відмова в обслуговуванні, хакерська атака, кібербезпека, система виявлення DoS-атак

Abstract
Software for detection of denial-of-service attacks is dedeloped. Modelling of TCP Syn Flood, Slowloris and SSL DoS attacks is performed.
Keywords: denial of service, cyberattack, cybersecurity, denial-of-service detection system.

Вступ

В даний час, важко собі уявити успішну компанію, яка не використовує для організації діловодства досягнення науки і техніки у сфері інформаційних технологій. Для полегшення виявлення та захисту від подібних атак необхідно мати чітку класифікацію за різними критеріями [1].

Результати дослідження

Відповідно до існуючої класифікації [2] було розроблено програмний засіб, який дозволяє за допомогою вхідного потоку трафіку дозволяє фахівцю визначити певний тип атаки [2].

Було протестовано декілька атак, таких як SYN Flood, Slowloris та SSL DOS. Для атаки SYN Flood можна побачити стрімке зростання кількості пакетів [3] та збільшення співвідношення кількості SYN пакетів до кількості SYN+ACK-пакетів.

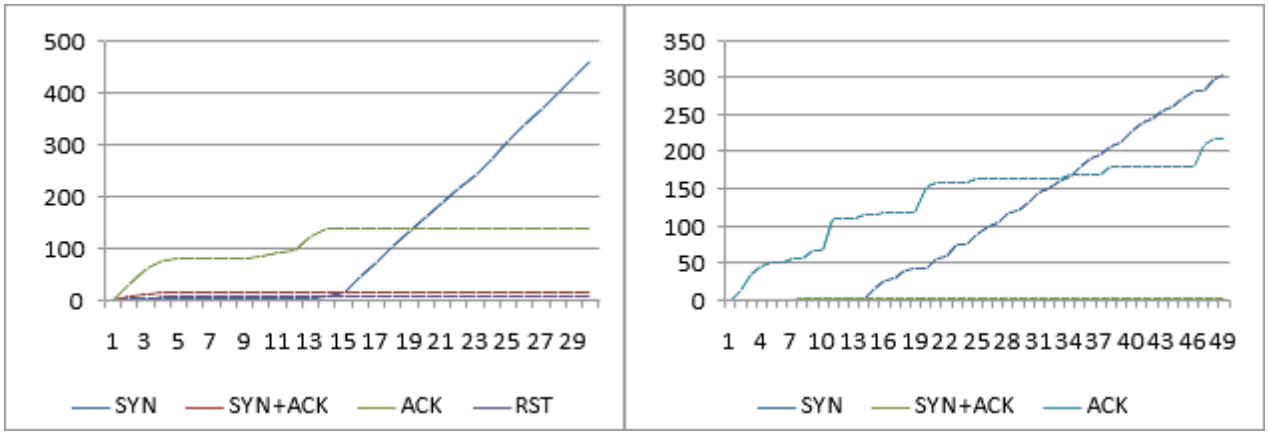

Рисунок 1 - Графіки атак типу TCP SYN Flood та Slowloris

Атака типу Slowloris може бути виявлена за зростанням кількості TCP-пакетів та припиненні нормальної роботи веб-сервера без створення істотного навантаження. Також після заповнення буфера веб-сервера помітно зростає кількість втрат SYN+ACK-пакетів [4].

Для атаки типу SSL DOS характерне більшення кількості потоків створює та вагоме навантаження на комп'ютер-зловмисника. Атаку можна виявити по ступінчастому зростанню TCP-пакетів та об'єму трафіку, постійному максимальному навантаженню центрального процесора та поступовому зростанню використання оперативної пам'яті.

Рисунок 2 - Графік атак типу SSL DoS

Висновки

Розробений програмний засіб дозволяє здійснювати моніторинг пакетів мережевого трафіку та на його основі дозволяє визначати наявність та тип атаки відповідно до запропонованої класифікації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Mirkovic J. A taxonomy of DDoS attack and DDoS defense mechanisms / J J Mirkovic, P Reiher // ACM SIGCOMM Computer Communication. – 2004. – Режим доступу до ресурсу

2. Voytovych O. P. Denial-of-service attacks investigation / Voytovych O. P., Kolibabchuk E. I. // Тези доповідей Четвертої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації» м. Вінниця, 19-21 квітня 2016 року. - Вінниця: ВНТУ, 2016. - 74-76 с

3. Voytovych O. P. Denial-of-service attack research / Voytovych O. P., Kolibabchuk E.I. // Матеріали статей Міжнародної науково-практичної конференції «Інформаційні технології та комп’ютерне моделювання» м. Івано-Франківськ - Яремче, 23-28 травня 2016 року. - Івано-Франківськ: Супрун В. П., 2016. - 111-112 с.

4. Voytovych O. P. Denial-of- Service attacks investigation / Voytovych O. P., Kolibabchuk E. I., Kupershtain L. M. // Вісник ХНУ : серія Технічні науки. - №3. -2016. - С. 129-133.

Колібабчук Едуард Ігорович — студент групи 1БС-16м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: ekolibabchuk4@gmail.com

Науковий керівник Войтович Олеся Петрівна — канд. техн. наук, доцент, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Kolibabchuk Eduard I. — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : ekolibabchuk4@gmail.com

Voitovych Olesya. P. — Cand. Sc. (Eng.), Assistant Professor of Information Security Department, Vinnytsia National Technical University, Vinnytsia