УДК 004.56.5

МЕТОДИ ЗАХИСТУ МЕРЕЖЕВИХ СЛУЖБ ВІД TCP SYN-FLOOD АТАК

Нестеренко М.М., Доманчук В.С.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: nesterenko_nik@ukr.net

Methods defence of network services from TCP SYN – flood attacks

The modern methods of protecting from TCP SYN-flood attacks unadapted to the overloads and cast aside surplus queries. Development of probabilistic model, which will take into account the productivity of servers

Сучасний розвиток IT-сфери вказує на розширення спектру надання інформаційних послуг, при чому велика увага приділяється надійності роботи відповідних сервісів в умовах постійної конкуренції [1]. Особливо гостро дане питання постає при розміщенні інформаційних ресурсів та побудови інфраструктури організації в зовнішній мережі, що притаманне „хмарним технологіям". В свою чергу, платформою будь-якого сервісу є мережева операційна система на базі якої проводиться розгортання основних мережевих служб (серверів) таких, як *DNS*-, *mail*-, *FTP*- *Web*-сервер.

В зв'язку з цим, актуальність питань захисту інформаційних ресурсів та мережевих служб, які забезпечують надання інформаційних послуг кінцевим користувачам ні в кого не викликає сумнівів [2].

В наш час, набули широкого застосування та постійно удосконалюються, мережеві атаки, щодо блокування та збоїв роботи основних мережевих служб. Згідно офіційної статистики, зафіксовано велику кількість масштабних (*Distributed Denial Of Service Attack* – атака типу „відмова в обслуговуванні") *DDoS*-атак, яким важко протистояти навіть сучасним системам захисту інформації.

Нижче приведена класифікація *DDoS*-атак за предметом ураження:

- блокування каналів зв'язку і маршрутизаторів (за рахунок величезного потоку (flood) безглуздих запитів повністю забивається вся ширина каналу даних або продуктивність роботи пограничного маршрутизатора);
- атаки на рівні протоколів (обмеження устаткування за рахунок використання уразливості існуючих протоколів);
- атаки на рівні application layer (призводять до непрацездатності будь-якого додатку або ОС в цілому).

Одним з основних типів *DDos*-атак є *TCP SYN-flood*, механізм проведення якого базується на використанні вразливостей протоколу *TCP*.

На теперішній час відомі наступні методи протидії *TCP SYN-flood* атакам [3]:

- *TCP SYN Cookies* (блок управління передачею – *TCB* на сервері кодує порядковий номер і зберігає закодовану комбінацію у хеші, після чого відправляє *SYN-ACK* з закодованим *cookie* і закриває з'єднання. Якщо у відповіді клієнта *ACK cookie* співпадає то сервер відкриває *TCP* - з'єднання);

- *TCP RST Cookies* (сервер відправляє клієнту, який надіслав запит на *TCP*-з'єднання *SYN+ACK* пакет з невірними параметрами. У відповідності до специфікації протоколу *TCP* клієнт повинен надіслати *RST*-пакет. Якщо сервер отримує від клієнта даний *RST*-пакет, то сервер додає клієнта до списку легітимних користувачів);

- *Floodgate* (фізичний або програмний засіб, який випадковим чином відкидає *TCP*-з'єднання, може розміщуватись як на самому сервері так і на маршрутизаторі);

- передмаршрутизаційна фільтрація/*Blacklisting* (маршрутизатори мережі контролюють всі *IP*-адреси відправників та відфільтровують (відкидають) пакети з неіснуючими *IP*-адресами);

- *Random / Old Drop* (видаляє напіввідкриті *TCP*- з'єднання випадковим чином або ті з'єднання встановлений ліміт яких вичерпано);

- *SYN-Proxy* (використовується додатковий *proxy*-сервер, призначенням якого є обробка *SYN* пакетів. Якщо *proxy*-серверу вдалось встановити *TCP*-з'єднання з клієнтом, то клієнт допускається до ресурсів сервера);

- *Stack Tweaking* (полягає в зміні налаштувань протоколу *TCP*, а саме: таймаут перед закриттям напіввідкритого *TCP*-з'єднання, максимально допустима кількість напіввідкритих з'єднань і час очікування *ACK*-відповіді від клієнта);

- *Blacklisting* (сервер не обслуговує запити від клієнтів, які потрапили в *blacklist*);

- мережеві система виявлення вторгнень *IDS – Intrusion Detection System* (система виявлення та запобігання атак, яка комбінує в собі методи зіставлення по сигнатурам, засоби для інспекції протоколів і механізми для виявлення аномалій).

Однак, дані методи в основному працюють по принципу відсікання запитів по інтенсивності, без додаткових механізмів перевірки легітивності запитів, або вимагають складних налаштувань збоку серверного обладнання.

Також, дані методи не дозволяють адаптивне реагувати на перенавантаження або протидії *TCP/SYN flood*-атакам. Це пояснюється тим, що атака розрахована на обмеження кількості напіввідкритих *TCP*-з'єднань в модулі *TCP/IP* будь-якої мережевої операційної системи.

В наслідок цього, якість обслуговування користувачів, щодо доступності та часу відклику мережевих служб не враховується.

Особливої уваги заслуговує мережева система виявлення вторгнень *Snort*, яка може виступати основою для розгортання та удосконалення існуючих систем захисту, за рахунок можливості написання та використання власних правил обробки трафіку, можливості підключення нових модулів та гнучкої системи оповіщення про атаки (*Log*-файли, БД і т.д.).

Основні модулі *Snort* та порядок їх взаємодії приведені на рис. 1 [4].

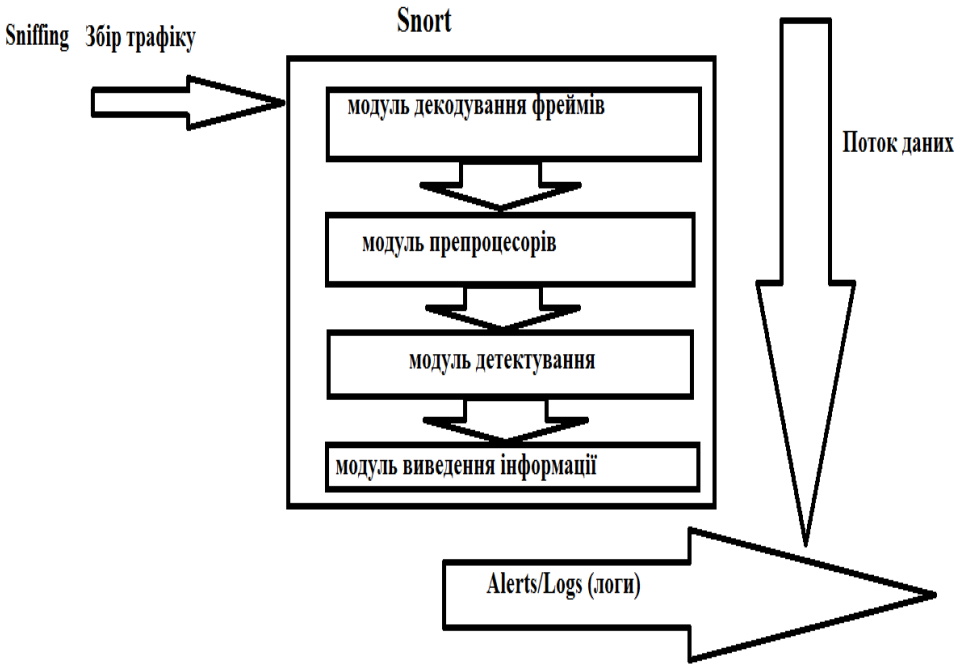

Рис. 1 Архітектура системи *IDS Snort*

На основі вище приведеного, розробка моделей та методик виявлення *flood*-атак вимагає визначення конкретних значень при конфігуруванні параметрів захисту адміністратором безпеки.

В зв'язку з цим, пропонується розробка аналітичної моделі, на базі якої буде проводитись оцінка ймовірності проведення *TCP/SYN flood*-атаки з врахуванням забезпечення якості обслуговування користувачів в залежності від продуктивності апаратних засобів та можливостей програмного забезпечення. Практичною реалізацією даної моделі може бути плагін в системі *IDS Snort.*

Література

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М.: ФОРУМ, 2013. – 416 с.
2. Белов Е. Б. Основы информационной безопасности: учеб. пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия-Телеком, 2006. – 544 с.
http://www.npk.ru/pub/presentations281010/Kaspersky_DDoS_prevention.pdf
3. Feinstein L., Schnackenberg D., Balupari R., Kindred D. Statistical Approaches to DDoS Attack Detection and Response. // DARPA Information Survivability Conference and Exposition
http://faculty.nps.edu/ncrowe/oldstudents/monteiro_thesis.htm
4. Джей Бил и др. Snort 2.1. Обнаружение вторжений. 2-е изд. Пер. с англ. - М.: ООО "Бином-Пресс", 2006;
http://rst.void.ru/papers/snort.txt