УДК 004.56.5

АНАЛІЗ МЕТОДІВ ЗАХИСТУ СЕРВЕРІВ ВІД РОЗПОДІЛЕНИХ *TCP SYN-FLOOD* АТАК

Нестеренко М.М., Романов А.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ», Україна
E-mail: nesterenko_nik@ukr.net, anton3329@gmail.com

Analysis methods of protection servers from distributed TCP SYN-flood attacks

The article presents one of the most common types of DDos-attacks on the server – TCP SYN-flood attack. The model and describes how to interact with the attacker's server during a DDos-attack. We analyzed the currently used methods of protection: TCP SYN Cookies, TCP RST Cookies, Floodgate, Random / Old Drop, SYN-Proxy, Stack Tweaking, Blacklisting.

Ефективна робота будь-якої організації не можлива без створення власної інфраструктури на базі сучасних інформаційних сервісів. Основою для реалізації відповідного сервісу є мережева операційна система на платформі якої розгортаються основні сервери такі, як *DNS*-, *mail*-, *FTP*- та *Web*-сервер. В умовах постійної конкуренції особливо гостро постає питання надання широкого спектру інформаційних послуг якість яких залежить від часу відклику та доступності серверів. Однак, останні дослідження в області комп'ютерної безпеки [1] вказують на постійний зріст та удосконалення мережевих *DDos*-атак, які в першу чергу направлені на збій в роботі (або блокування) інформаційних служб. Тому завдання оптимального конфігурування системи захисту серверів є актуальним.

Одним з основних типів *DDos*-атак є *TCP SYN-flood*, механізм проведення якого базується на використанні вразливостей протоколу *TCP*. Дана атака розрахована на обмеження кількості напіввідкритих *TCP*-з'єднань, яке задано по замовчуванню у вбудованому модулі *TCP/IP* мережевої операційної системи. Узагальнена схема проведення *TCP SYN-flood* атаки приведена на схемі рис. 1.

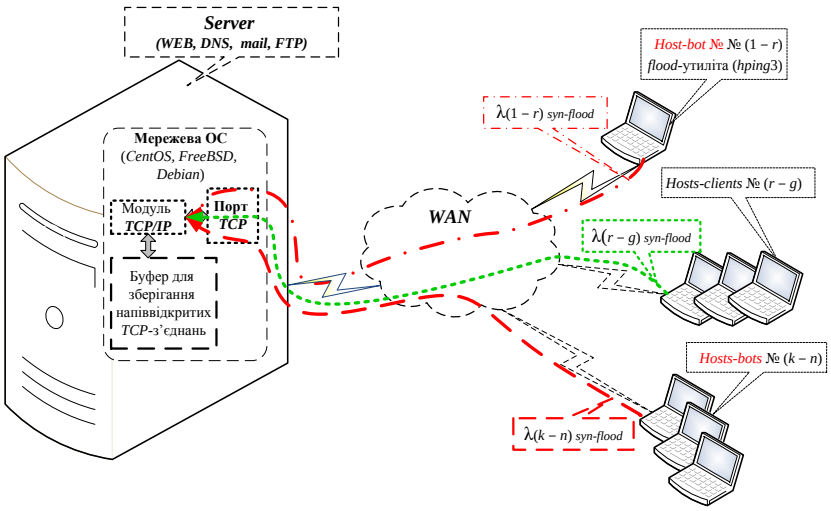

Рис. 1. Функціональна схема *TCP SYN-flood* атаки на Unix- сервер.

А саме, коли на сервер здійснюється *TCP SYN-flood* атака, то за рахунок збільшення інтенсивності *SYN*-запитів утворюється (та постійно зростає) черга з напіввідкритих *TCP*-з'єднань в стані *SYN RECEIVED* та як наслідок призводить до вичерпання ресурсу модуля *TCP/IP*, тобто сервер більше не може обробляти вхідні запити [2].

Для збільшення ефекту даного типу атаки боти використовують фіктивні *IP*-адреси для ускладнення процесу ініціалізації сервером (повторні перезапити) так, як згенерована *IP*-адреса може бути недосяжною. Дана операція також називається *SYN*-спуфінгом.

Необхідно відмітити, що деякі *TCP SYN-flood* атаки не завжди намагаються перезавантажити сервери, замість цього задачею є вичерпання всієї пропускної спроможності *Internet*-каналу [3], за рахунок повторних запитів збоку сервера при неотриманні відповіді від псевдо-клієнтів (ботів).

В свою чергу, процес повторної передачі буде ініціалізуватись з боку сервера за допомогою *SYN-ACK* запитів, до моменту отримання *ACK*-відповіді від клієнта. Тобто, пакет з флагом *ACK* з боку клієнта є підтвердженням на встановлення *TCP*-з'єднання з сервером (рис. 2 а).

Якщо сервер на який здійснюється атака не отримує відповідь від віддаленого хоста-клієнта, то він повторно робить перезапит (*SYN+ACK*-запит) до тих пір поки не наступить тайм-аут, а потім видаляє це напіввідкрите *TCP*-з'єднання з черги (рис. 2 б).

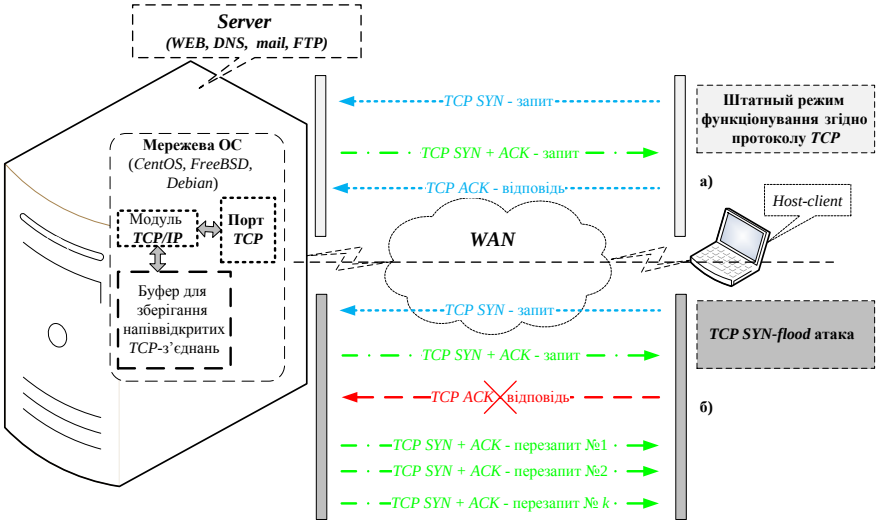

Рис. 2. Порядок проведення *TCP SYN-flood* атаки
при використанні вразливості протоколу *TCP*

На теперішній час відомі наступні методи протидії *TCP SYN-flood* атакам [4]:

- *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 *ACK* клієнта *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 легітивних користувачів);

- *Floodgate* (фізичний або програмний засіб, який випадковим чином відкидає *TCP*-з'єднання);

- передмаршрутизаційна фільтрація/*Blacklisting* (маршрутизатори мережі контролюють всі *IP*-адреси відправників та відфільтровують 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,* як правило використовується з передмаршрутизаційною фільтрацією);

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

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

В подальшому симуляцію атаки на *Web*-сервер (Apache) було проведено за допомогою утиліти *hping3*, яка дозволяє генерувати *SYN-flood* від неіснуючих *IP*-адрес, що обираються випадковим чином. В результаті перевірки завантаженості сервера було з'ясовано: процесор майже не задіяний, вільної оперативної пам'яті більше половини, отже фізичні ресурси сервера не були вичерпані, проте черга потоків в модулі *TCP/IP* була повністю зайнята, що призвело до непрацездатності сервісу на 80 порту.

На основі вище приведеного, розробка моделей та методик виявлення *flood*-атак вимагає визначення конкретних значень параметрів системи захисту при її конфігуруванні. А саме, динамічну зміну заданих по замовчуванню стекових змінних по протоколу *TCP/IP* у відповідних модулях мережевих операційних систем в залежності від кількості *SYN*-запитів.

Література

1. http://expert.com.ua/100780-issledovateli-check-point-otmetili-rost-ddos-atak-v-yanvare-2016-goda.html.
2. Инструменты безопасности с открытым исходным кодом /Хаулет Т. – М.: НОУ „Интуит" 2016. – 556 с.
3. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М.: ФОРУМ, 2013. – 416 с.
4. Feinstein L., Schnackenberg D., Balupari R., Kindred D. Statistical Approaches to DDoS Attack Detection and Response. // DARPA Information Survivability Conference and Exposition.