Виявлення та ідентифікація DDoS-атак

Войтович О. П. [1], Фесенко А. І. [2]

[1]Доц., к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет вул. Хмельницьке шосе 95, м. Вінниця, Україна, voytovych.op@gmail.com
[2]Студент кафедри захисту інформації, Вінницький національний технічний університет вул. Хмельницьке шосе 95, м. Вінниця, Україна, fesia.senpai@gmail.com

***Анотація* — запропоновано використовувати низку ознак атак на відмову у обслуговуванні, які враховують не тільки особливості зміни полоси пропускання, але й особливості пакетів різних протоколів, реагування з боку операційної системи та програмного забезпечення. Наведено приклад, який демонструє розбиття атаки Slowread на ознаки, за якими її можна ідентифікувати.**

Ключові слова: атака на відмову в обслуговуванні, виявлення атак, ідентифікація атак, dos, ddos.

Detection and identification of DDoS-attacks

O. P. Voytovych[1], A. I. Fesenko[2],

[1]Associate professor, senior lecturer of Department of Information Security, Vinnytsia National Technical University Khmelnytske shosse, 95, Vinnytsia, Ukraine, voytovych.op@gmail.com
[2]Student, Department of Information Security, Vinnytsia National Technical University Khmelnytske shosse, 95, Vinnytsia, Ukraine, fesia.senpai@gmail.com

***Abstract* — usage of the set of denial of service attacks signs, considering bandwidth changes, as well as different protocols packages features, operating system and software reactions is considered. The example demonstrates the stating of Slowread attack signs using which it can be identified.**

Keywords: denial of service, attack detection, attack identification, dos, ddos.

I. Вступ

Останнім часом спостерігається тенденція до підвищення кількості та потужності атак на інфраструктури обчислювальних мереж. Потужність розподілених атак на відмову в обслуговуванні (DDoS) зросла до рівня понад 100 Гбіт за секунду [1]. Незважаючи на численні дослідження та існуючі підходи до попередження та відбивання атак на відмову в обслуговуванні, питання досліджень в даному напрямку, залишається актуальним.

З ціллю мінімізації наслідків від атак на відмову в обслуговуванні надзвичайно важливими є задача їх виявлення та ідентифікації.

Якщо ще відносно нещодавно основним методом проведення DDoS-атаки був метод повного заповнення полоси пропускання [1], то тепер специфікації тяжіють до більш винахідливих рішень: відбиті атаки, slowread, slowloris, нюки, мультивекторні атаки, атаки нульового дня і т.д.

Ряд робіт [2-4], присвячені виявленню DDoS-атак та зниженню рівня помилкових реакцій. У статтях [2, 5] розглядається імітаційний механізм протидії DDoS-атакам на основі використання нейронних мереж. Запропоновані ідеї можуть бути впроваджені в використання в реальних системах. Однак, питання класифікації або взагалі не розглядається, або згадується дуже поверхнево.

Методи протидії розподілених атак на відмову в обслуговуванні можна значно оптимізувати, адаптувавши їх до певної класифікації.

Метою дослідження є виявлення універсальних ознак відомих типів атак задля вирішення задачі виявлення та ідентифікації DDoS-атак та об'єднання їх в певну класифікацію. Це дасть змогу більш ефективно реагувати на атаку не лише постфактум, але й в режимі реального часу в момент її проведення.

II. Аналіз відомих ознак атак на відмову в обслуговуванні

У ході роботи проведено дослідження ознак, за якими можна відрізнити один тип атаки від іншого. Умовно усі вони розділені на три основних рівні:

1. Рівень трафіку
2. Рівень операційної системи
3. Рівень сервісу

У свою чергу, рівень трафіку ділиться на 2 підкатегорії: кількісно та якісно. Окремо виділено протокол, за яким здійснюється атака.

Дослідивши особливості найпопулярніших розподілених атак на відмову в обслуговуванні, виділено попередній перелік ознак, які можуть визначати тип атаки на кожному з рівнів (табл. 1).

Таблиця 1 – Характерні ознаки різних видів розподілених атак на відмову в обслуговуванні

<table>
<tr><td colspan="4">Трафік (T)</td></tr>
<tr><td rowspan="6">Якісно (Q)</td><td colspan="3">Стандартний вигляд пакету (QS)</td></tr>
<tr><td rowspan="5">Пакети змінені (QCh)</td><td>Занадто великий розмір (QCh1)</td></tr>
<tr><td>Пакети пусті(QCh2)</td></tr>
<tr><td>У заголовках вказується дуже низька швидкість отримання даних (QCh3)</td></tr>
<tr><td>У заголовках вказується дуже велике значення поля «content-length» (QCh4)</td></tr>
<tr><td>Аномально низьке значення поля «Window size» (QCh5)</td></tr>
<tr><td rowspan="4">Кількісно (C)</td><td rowspan="2">Насичення смуги пропускання (CB)</td><td>Високий рівень (CB1)</td></tr>
<tr><td>В межах норми (CB2)</td></tr>
<tr><td rowspan="2">Кількість вхідних пакетів (CC)</td><td>Висока (CC1)</td></tr>
<tr><td>Низька (CC2)</td></tr>
<tr><td>Протокол (P)</td><td colspan="3">UDP (P2), ICMP(P2), TCP (P3), ethernet (P4), HTTP (P5), DNS (P6), …</td></tr>
<tr><td colspan="4">Операційна система (OS)</td></tr>
<tr><td rowspan="2">Рівень використання ресурсів (AL)</td><td colspan="3">Перевищений (AL1)</td></tr>
<tr><td colspan="3">В межах норми (AL2)</td></tr>
<tr><td colspan="4">Сервіс (S)</td></tr>
<tr><td>firewall (FW)</td><td colspan="3">Забиття ресурсів пустими або важкими пакетами (FW1)</td></tr>
<tr><td rowspan="3">networking (NW)</td><td rowspan="2">Велика кількість відповідей (NWA)</td><td>«ICMP Destination Unreachable» (NWA1)</td></tr>
<tr><td>«ICMP echo» (NWA2)</td></tr>
<tr><td colspan="2">Велика кількість напіввідкритих з’єднань (NWC)</td></tr>
<tr><td rowspan="2">web-server (WS)</td><td colspan="2">Вичерпування кількості допустимих з’єднань (WSC)</td></tr>
<tr><td colspan="2">Часті випадкові чи рекурсивні запити важких частин ресурсу (WSR)</td></tr>
<tr><td>Інші (O)</td><td colspan="3">…</td></tr>
</table>

III. МОДЕЛЮВАННЯ

Для прикладу, проведемо розбір ситуації, коли на об’єкт захисту була направлена атака типу slowread [6]. Ця атака заснована на відомій особливості TCP-протоколу, при якій клієнт може виставити значення поля Window Size, що означає розмір даних, які він готовий прийняти на своїй стороні, рівним нулю. У цьому випадку сервер буде підтримувати з'єднання, «прослуховуючи» клієнта до його готовності прийняти ненульовий буфер невизначено велику кількість часу. У простому випадку атаки буде вичерпуватися серверна черга з'єднань, але все можна значно ускладнити, якщо запитати у сервера великий ресурс, який не вміщується в його буфері для пересилання - додатково до всього буде споживатися серверна пам'ять при кожному подібному запиті. В кінці кінців ліміт одночасних підключень на атакованому сервері доволі швидко закінчується і він перестає приймати легітимні запити.

Отже, моніторинг ситуації показує:

– рівень насичення смуги пропускання (CB) залишився в нормі (CB2);
– networking (NW) - аномально велика кількість відкритих з’єднань (NWC);
– web-server (WS) - веб-сервер не функціонує або функціонує з відхиленням від норми (WSC);
– Рівень використання ресурсів (AL) - ОС працює у звичайному режимі (AL2).

Отже, атака типу Slowread може бути ідентифікована за такими ознаками:

$$A_{Slowread}=\{CB2; P5; NWC; WSC; AL2\}$$

Перерахований список можна продовжувати, ввівши додаткові критерії класифікації, однак навіть маючи такий набір можна, проаналізувавши його, зробити висновок про ідентифікацію атаки типу Slowread.

Не завжди можна подібним чином однозначно ідентифікувати тип атаки, однак задача ідентифікації зводиться до збільшення достовірності таких прийнятих рішень.

Інший випадок виникає при ненавмисній DDoS-атаці. Власне, у такому випадку це і атакою назвати не можна. Цей вид DDoS відбувається тоді, коли посилання на який-небудь сайт потрапляє на сторінки, наприклад, топового ресурсу новин або популярного блогу. Це спричинює різкий зріст відвідуваності, до якого сайт-жертва виявляється не готовим. У такому випадку система фіксує велику кількість відкритих TCP-з’єднань, деградацію сервісу, насичення полоси пропускання. Такі ситуації складно спрогнозувати, вони вимагають додаткового аналізу втручання адміністратора.

IV. ВИСНОВКИ

Запропоновані класифікація та ознаки для ідентифікації DDoS-атак, що дозволить більш ефективно реагувати на появу таких атак та проводити аналіз атак, що відбулися.

В подальшому планується розширити список ознак з врахуванням параметрів атак, які можна отримати з різних джерел.

[1] DDoS в 100 Гбит/с - репортаж с линии фронта от очевидца [Електронний ресурс] – Режим доступу: http://blogerator.ru/page/ddos-v-100-gbits-reportazh-s-linii-fronta-ot-ocevidca – Назва з екрану

[2] Tewani R. A Novel Methodology for Implementing a DDos Attack and Prevention / Rachna Tewani, Saumya Singh, Arun Kumar Dubey // International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5149-5152

[3] Сліповичев І. І. ОБНАРУЖЕНИЕ DDoS АТАК НЕЧЕТКОЙ НЕЙРОННОЙ СЕТЬЮ / И.И. Слеповичев, П.В. Ирматов, М.С. Комарова, А.А. Бежин // Известия Саратовского университета. – 2009

[4] Терновий О.С. Снижение ошибки обнаружения ddos атак статистическими методами при учете сезонности / О. С. Терновий, А. С. Шатохін // Перспективы развития информационных технологий. – Новосибирск, изд. «Сибпринт», С. 2012 – 212

[5] Котенко І. В. Имитационное моделирование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода “Нервная система сети” / Труды СПИИРАН. Випуск 3 (22) – 2012

[6] Security Labs Are you ready for slow reading [Електронний ресурс] – Режим доступу: https://community.qualys.com/blogs/securitylabs/2012/01/05/slow-read – Назва з екрану