УДК 004.056

Каплун І.С.

ПРОГНОЗУВАННЯ ТА АНАЛІЗ DDOS - АТАК НА ІНФОРМАЦІЙНІ WEB – РЕСУРСИ

Вінницький національний технічний університет

Анотація

В даній статті розглянуто існуючі атаки на конфіденційні мережеві ресурси і способи їх виявлення. В роботі наведено один з алгоритмів ідентифікації загроз несанкціонованого доступу, що базується на аналізі фактичних даних об'єму мережевого трафіку. А також розглянуто найпопулярніші, найефективніші методи боротьби з ddos - атак на інформаційні web – ресурси та підходи до ідентифікації ddos – атак.

Ключові слова: *ddos – атака, web – ресурс, мережа, алгоритми ідентифікації, несанкціонований доступ, інформація, аналіз загроз.*

Abstract

In this article the existing attacks on confidentional network resources and methods of their detection are described . In the article one of algorithms of identifying threat of unauthorized access, based on an analysis of actual data volume of network traffic is described. Also considered the most popular and effective methods of dealing with ddos - attacks on information web - resources and approaches to identification ddos - attacks.

Key words: *ddos - attacks, web - resource, network, algorithms of identification, unauthorized access, information, analysis of threats.*

Вступ

Сучасний світ не можливо уявити без використання суспільством web – ресурсів. Проте традиційною ситуацією залишається і те, що коли щось входить до широкого вжитку суспільства – потребує захисту. В даному випадку – це захист web – ресурсів від ddos – атак.

Захищати дані ресурси важливо так як вони містять велику кількість корисної інформації, частково забезпечують комунікацію громадян по всьому світу. На інформаційних ресурсах розміщують різноманітні наукові дослідження, розробки, щоденно публікують новини, завантажують фільми, фото, музику, створюють персональні сторінки та багато іншого.

В наш час програма захисту інформаційних ресурсів вкрай важлива та необхідна. Технічний прогрес не стоїть на місці, тому кваліфікаційні здібності працівників лише зростають, та поряд з цим здібності хакерів також не поступаються своєю якістю. Задля досягнення вагомих результатів в захисті інформаційних ресурсів важливо вміти прогнозувати та аналізувати ddos – атаки на них. Це дасть можливість передбачати подібні атаки, а не виправляти наслідки.

Основна частина

Загальний огляд видів ddos – атак на інформаційні web – ресури

Так як під атакою розуміється будь-яка дія порушника, яка призводить до небажаного впливу на інформаційно-обчислювальну систему шляхом використання її уразливостей , то існує багато підходів до їх класифікації, за одним з яких можна виділити види атак наступним чином [1]:

1. За характером впливу: пасивні атаки (які не впливають на функціонування системи, але порушують її політику безпеки); активні атаки (впливають на функціонування системи і порушують її політику безпеки).

2. За метою впливу: порушення конфіденційності; порушення цілісності; порушення доступності.

3. За умовою початку атаки: за запитом від об'єкта, що атакується (атакуючий очікує від об'єкта, що атакується передачі запиту певного типу, який і буде умовою початку здійснення впливу); по настанню події (атакуючий здійснює постійне спостереження за станом об'єкта атаки і при настанні визначеної події починає вплив на операційну систему об'єкта, що атакується); безумовна атака (атака здійснюється негайно і не відноситься до стану системи і об'єкта, що атакується).

4. За наявності зворотного зв'язку з об'єктом атаки: зі зворотним зв'язком (атака характеризується тим, що на деякі запити, передані на об'єкт, що атакується, атакуючому необхідно отримати відповідь, для цього між об'єктом, що атакується і атакуючим організовується зворотний зв'язок); без зворотного зв'язку (атакуючому об'єкту не вимагається реагувати на будь-які зміни, що відбуваються на об'єкті, що атакується).

5. По розташуванню щодо об'єкта атаки: внутрішньо сегментні (атакуючий об'єкт і об'єкт, що атакується знаходяться в одному сегменті мережі); зовнішньо сегментні (атакуючий об'єкт і об'єкт, що атакується знаходяться в різних сегментах мережі).

6. За рівнем моделі OSI на якому здійснюється атака: фізичний (здійснюється фізичне з'єднання між комп'ютерною системою і фізичним середовищем передачі; він визначає розташування кабельних контактів тощо); канальний (забезпечує створення, передачу і прийом кадрів даних; цей рівень обслуговує запити мережевого рівня і використовує сервіс фізичного рівня для прийому і передачі пакетів); мережевий (на цьому рівні відбувається маршрутизація пакетів на основі перетворення MAC-адрес в мережеві адреси); транспортний (ділить потоки інформації на пакети для передачі їх на мережевий рівень); сеансовий (відповідає за організацію сеансів обміну даними між кінцевими хостами); представницький (відповідає за можливість діалогу між додатками на різних хостах; цей рівень забезпечує перетворення даних прикладного рівня в потік інформації для транспортного рівня); прикладний (відповідає за доступ додатків в мережу; завданнями цього рівня є перенесення файлів, обмін поштовими повідомленнями і управління мережею).

Також в статті запропоновано розглянути пристрої на які ай частіше відбуваються ddos – атаки (наприклад, сервери, робочі станції, середовища передачі інформації і т.д.), а також наволяться способи здійснення атак найбільш розповсюджених окремих їх видів [2].

Методи виявлення ddos – атак в інформаційних web - ресурсах

Під мережевою атакою розуміється будь-яка дія зловмисника, спрямована на несанкціоноване отримання доступу до інформаційних ресурсів або порушення функціональності обчислювальної системи.

Виявлення атаки – це процес ідентифікації підозрілої діяльності, направленої на обчислювальні або мережеві ресурси, і реагування на неї. Зазвичай системи виявлення атак поділяють на два види відповідно до їх принципів роботи [3]:

- сигнатурний принцип полягає в тому, що кожна атака описується певним шаблоном. Шаблони, використані для формального опису атаки, називаються сигнатурою. Сигнатури можуть являти собою рядок символів, вираз на спеціальній мові, математичну модель тощо. Вихідні дані перевіряються на зіставлені відомим атакам шаблони, їх виявлення є свідченням атаки;

- поведінковий принцип – відбувається виділення процесів, що відрізняються від раніше спостережуваних, які можуть бути потенційними атаками. Відхилення спостережуваних характеристик від їх нормального значення називається аномалією. Таким чином, використання даного методу полягає в порівнянні поточного режиму роботи інформаційної системи з її штатним режимом функціонування, а невідповідності між ними розглядаються як атаки на дану систему.

Отже, для виявлення використовуються наступні методи: методи контекстного пошуку (сигнатурні); методи аналізу станів (сигнатурні); методи на основі статистичних моделей (поведінкові); методи продукційних правил (комбіновані); методи імітації поведінки біологічних систем. Дані методи мають свої переваги і недоліки, тому в статті запропоновано розглянути детально кожен з них, задля найбільш високої поінформованості при захисті інформаційного web – ресурсу [4].

Причини виникнення ddos – атак в інформаційних web - ресурсах

DoS–атака (Denial of Service – відмова в обслуговуванні) зазвичай характеризується як інцидент, в якому користувач або організація позбавлені очікуваного обслуговування ресурсу. Як правило, відмова в обслуговуванні – це недоступність специфічного мережевого обслуговування, наприклад, електронної пошти, або тимчасова втрата всього мережевого забезпечення зв'язку й обслуговування [5]. У гіршому випадку обслуговування може бути тимчасово повністю припинене. Подібні відмови в обслуговуванні можуть також зруйнувати файли в комп'ютерній системі. За допомогою DoS-атак зловмисник намагається перешкоджати зверненню користувачів до інформації або обслуговування. Націлившись на комп'ютер і його мережеве підключення, які використовуються, зловмисник може перешкоджати зверненням до електронної пошти, сайтів, мережевих облікових записів або інших необхідних сервісів.

Причини виникнення DoS-атак в комп'ютерній системі можна класифікувати наступним чином: помилка в програмному коді, що призводить до звернення до не використовуваних фрагментів адресного простору, виконанню неприпустимої інструкції або іншої необроблюваної виняткової ситуації, коли відбувається аварійне завершення серверного додатку; недостатня перевірка даних користувача, що призводить до нескінченного або тривалого циклу, вичерпання процесорних ресурсів, виділення занадто великого обсягу оперативної пам'яті; флуд – атака, пов'язана з великою кількістю зазвичай безглуздих або сформованих в неправильному форматі, запитів до комп'ютерної системи або мережевого обладнання, що призвела до відмови в роботі системи через вичерпання ресурсів системи – процесора, пам'яті або каналів зв'язку; атаки другого роду – атаки на системи безпеки, що призводять до їх помилкового спрацювання і недоступності комп'ютерної системи [6].

Ознакою класифікації DoS-атак може стати елемент системи, що є метою атаки: центральні процесори; оперативна пам'ять (в основному, через витоки пам'яті в додатках); запам'ятовуючі пристрої (в основному, через низьку продуктивність жорстких дисків; даний тип атак зустрічається дуже рідко, хоча і можливий); мережеве обладнання сервера; мережеве обладнання та системи безпеки, що забезпечують роботу сервера в мережі (маршрутизатори, комутатори тощо); операційна система і прикладні програми.

З наведених вище даних, можна побачити, що причини ddos – атак на інформаційні web – ресурси можуть бути найрізноманітнішими, а тому в роботі наводиться детальний аналіз найпоширеніших причин подібних загроз.

Способи виявлення ddos – атак на інформаційні web - ресурси

Загалом виділяють два методи виявлення DoS-атак – аналіз інформаційного мережевого потоку і аналіз журналів реєстрації операційної системи або додатків. Перший підхід до виявлення атак є більш ефективним з причини реагування в реальному масштабі часу. Тому основні дослідження зараз спрямовані на розробку способів і процедур виявлення атак в мережевому трафіку. Тут основним завданням є ідентифікація шкідливого трафіку. Більшість атак в даний час важко відрізнити від звичайних дій користувачів, у той же час, зворотне твердження так само справедливо – часто діяльність користувачів викликає ефекти, ідентичні ефекту від проведення розподіленої атаки відмови в обслуговуванні. [7]

В роботі розглянуто найбільш ефективні способи виявлення ddos - атак на основі аналізу трафіку, такі як визначення профілю активності; точки зміни стану; хвильовий аналіз (вейвлет-аналіз) [8]. Проте, не дивлячись на позитивні характеристики даних методів виявлення, існують наступні проблеми по знаходженню ddos – атак,а саме такі як проблема варіювання умов тестування; проблема оцінки природної мережевої активності; проблема визначення параметрів детектування; проблема раннього прогнозу атаки. Таким чином, проблема виявлення DoS-атак на основі аналізу мережевого трафіку у даний час є досить актуальною.

Висновки

Отже, в даній статті проаналізовано основні види атак на інформаційні web - ресурси, зокрема мережеві атаки. Був проведений огляд методів виявлення атак на комп'ютерні мережі, їх переваги та недоліки. Найбільш розповсюдженим типом атак на конфіденційні мережеві ресурси є відмова в обслуговуванні, тому були розглянуті причини їх виникнення і проведена класифікація видів DoS-атак. Також були проаналізовані основні способи виявлення атак цього виду та їх проблеми, тому

актуально розробити алгоритм виявлення DoS-атак на основі аналізу і прогнозування мережевого трафіку.

Таким чином, можна зробити висновок, що розробки в даній галузі є достатньо актуальними та вартими подальшої розробки. Інформаційні web – ресурси мають досить високий попит у сучасному світі, а тому їх захист потребуватиме постійного вдосконалення. Так як, вміння завчасного прогнозування ddos – атак – досить необхідне, в статті описано найрізноманітніші методи виявлення та захисту web - ресурсів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Котенко И.В., Степашкин М.В., Дойникова Е.В. Анализ защищенности автоматизированных систем с учетом социоинженерных атак // Проблемы информационной безопасности. Компьютерные системы. 2011 – №3 – С.40–57.

2. Игнатенко Е.Г., Дегтяренко И.В., Червинская Н.В., Яремко И.Н. Методика краткосрочного прогнозирования трафика телекоммуникационных сетей. – Збірник наукових праць ДонІЗТ. 2011 №28 – 102-107 с.

3. Крюков Ю.А., Чернягин Д.В. Модель прогнозирования значений трафика // Информационные технологии и вычислительные системы – 2011 – №2 – с.41–49.

4. Дубовой В.М. Прогнозування доцільної кількості повторень циклічного технологічного процесу / В.М. Дубовой, І.В. Пилипенко, Р.С. Стець // Вінниця: Видавництво Вінницького національного технічного університету (Вісник ВПІ), 2015. – ст.86-91.

5. Ibrahimov B. G. Research and estimation characteristics of terminal equipment a part of multiservice communication networks / B. G. Ibrahimov // Automatic Control and Computer Sciences. – 2010. – Vol.48. – No.6. – P. 54-59.

6. А.П., Кортко. Види ddos - атак та алгоритм виявлення ddos – атак типу flood – attack / Кортко. А.П.. // науковий журнал «Комп'ютерно – інтегровані технології: освіта, наука, виробництво». – 2015. – 18. – С. 18-25.

7. Н.Р., Кондратенко. Виявлення аномалії на основі стохастичної нейротехнології / Кондратенко. Н.Р., Никитюк. О.М.. // Вінницький національний технічний університет. – 2015. – 15. – С. 23-27.

8. Я.В., Тарасов. Методи виявлення низько інтенсивних ddos – атак на основі гібридної нейронної сітки / Тарасов. Я.В.. // Науково - технічний журнал. – 2015. – 34. – С. 43-57.

Ірина Сергіївна Каплун – студентка групи УБ-14б, факультет менеджменту, Вінницький національний технічний університет, м. Вінниця, e-mail: irka_kaplun@mail.ru

Iryna Serhiivna Kaplun - student of UB-14b group, faculty of management, Vinnitsa technical university, Vinnitsa, e-mail: irka_kaplun@mail.ru