

УДК 681.324

Ігор Вікторович Рубан
Євгеній Сергійович Лошаков
Дмитро Вікторович Прибильнов

АНАЛІЗ ОСНОВНИХ АСПЕКТІВ ВПЛИВУ DoS-АТАК НА ПРАЦЕЗДАТНІСТЬ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Постановка проблеми. Аналіз останніх досліджень і публікацій

Щорічно здійснюється велика кількість атак DoS (Denial of Service – відмова в обслуговуванні), внаслідок проведення яких різні компанії в усьому світі втрачають мільйони доларів. Вони є істотною загрозою для будь-якої комп'ютерної системи. Великі збитки від реалізації даного типу атак обумовлені довготривалим непрацездатним станом системи і значним об'ємом робіт по відновленню працездатності та ідентифікації зловмисника. В цей час користувачі даної системи не мають доступу до її ресурсів, внаслідок чого компанія втрачає прибуток.

Аналіз літератури [1-8] показав, що існує декілька видів DoS-атак. Деякі з них легко виявляються, існують засоби для боротьби з ними. Але є й такі атаки, виявити які дуже складно, й засобів боротьби з ними поки що не існує.

Формулювання мети статті. Виклад основного матеріалу

Як показано на рис.1, з розвитком інформаційних технологій та мережі Інтернет йде постійне зростання кількості DoS-атак.

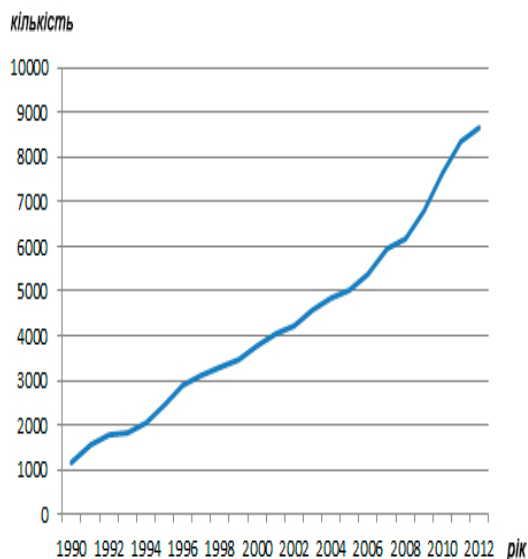


Рис.1. Статистика DoS-атак

Будь-яка DoS-атака направлена на виведення системи з працездатного стану шляхом використання тими, хто атакує, усіх її наявних ресурсів. В наслідок цього легітимні користувачі системи отримують відмову в обслуговуванні. Атака може бути реалізована як з одного комп'ютера, так і з декількох, або навіть з використанням великих мереж – так званих ботнетів (**robot network – botnet**). Така атака називається DDoS (Distributed Denial of Service – розподілена атака типу “відмова в обслуговуванні”). В залежності від вразливостей системи, які використовуються, можна виділити наступні види DoS-атак:

Атаки, що націлені на переповнення смуги пропускання;

Атаки, що використовують недостатню кількість ресурсів системи;

Атаки, що використовують помилки програмування;

Атаки DNS та маніпуляція таблицями маршрутизації;

Низькошвидкісні атаки протоколу TCP.

Одним з найбільш розповсюджених та простих видів DoS-атак є переповнення смуги пропускання. Зазвичай, зловмисник використовує флуд (англ. flood — “повінь”, “переповнення”), атаку, що пов'язана з використанням великої кількості беззмистовних або сформованих в невірній формі запитів до комп'ютерної системи чи мережного устаткування з метою вичерпання смуги пропускання каналу зв'язку. Реалізаціями даного виду DoS-атак є:

ring-флуд, який можливий тільки у тому випадку, коли канал зловмисника набагато ширший, ніж канал жертви. Таку атаку немає сенсу використовувати проти сервера, тому що він в будь-якому разі має ширший канал пропускання, ніж зловмисник.

НТТР-флуд. Ця атака використовується проти сервера. Зловмисник відправляє невеликий за об'ємом пакет, але такий, щоб сервер відповів на нього пакетом, розмір якого у декілька сотень раз більше. Навіть якщо канал пропускання сервера у декілька разів більший, ніж у зловмисника, існує

велика ймовірність його переповнення. А для того, щоб пакети-відповіді не спричинили відмову в обслуговуванні у зловмисника, він кожен раз змінює свій IP-адрес.

Smurf-атака або ICMP-флуд. Для реалізації цієї атаки зловмиснику необхідна підсилююча мережа. Він використовує широкомовну розсилку ring-запитів для виявлення працездатних вузлів цієї мережі. Після цього їм широкомовно відправляється ICMP-пакет, в якому IP-адрес відправника змінюється на адрес жертви. В наслідок чого, канал пропускання серверу переповнюється ICMP-пакетами від усіх працездатних вузлів мережі.

Fraggle-атака (аналогічна Smurf-атаці, тільки замість ICMP-пакетів використовуються UDP-пакети), SYN-флуд (відправлення жертві SYN-пакетів з неіснуючими IP-адресами, які ставляться в чергу і вичерпують усі ресурси системи).

При реалізації DoS-атак, що використовують недостатню кількість ресурсів системи, зловмисник намагається захопити такі системні ресурси, як оперативна і фізична пам'ять, процесорний час та інші. Як правило, такі атаки проводяться, якщо зловмисник вже володіє певною кількістю ресурсів. Метою атаки є захоплення додаткових ресурсів. Зловмисник намагається максимально навантажити центральний процесор сервера, заповнити усю вільну оперативну або фізичну пам'ять, в наслідок чого виникає відмова в обслуговуванні. Шляхами реалізації даного виду атак є:

відправлення пакетів, розмір яких значно перевищує стандартний. Вони не переповняють смугу пропускання серверу, але, обробляючи такі пакети, його процесор може не впоратись зі складними обчисленнями, і виникне збій. Як наслідок – відмова в обслуговуванні.

якщо системний адміністратор невірно налаштував на сервері систему логування (документування дій користувачів та програм), не визначивши певний ліміт, зловмисник може скористуватися цим. Він буде відправляти на сервер пакети з помилками. Факт отримання цих пакетів буде записуватися у лог-файл. Таким чином, через короткий проміжок часу буде використана уся наявна пам'ять, що призведе до відмови в обслуговуванні.

на будь-якому сервері застосовується CGI (Common Gateway Interface – загальний інтерфейс шлюзу). Це програма, що зв'яже зовнішню програму з веб-сервером. Якщо зловмисник отримає доступ до CGI, у нього буде можливість написати скрипт, який задіє значну кількість системних ресурсів. І якщо на сервері не налаштована система квотування, то скрипт за малий проміжок часу займе усі наявні ресурси сервера.

ініціювання хибного спрацювання системи захисту, що призводить до відмови в обслуговуванні користувачів.

Більш професійні зловмисники не використовують такий примітивний спосіб атаки, як переповнення смуги пропускання. Вони вивчають структуру системи жертви і, повністю з нею розібравшись, пишуть спеціальні програми – експлойти, які допомагають атакувати складні системи. Частіше за все зловмисниками використовуються помилки в програмному коді, що призводять до звернень до фрагменту адресного простору, що не застосовується, виконанню недопустимої інструкції або іншої виняткової ситуації, що не оброблюється, в наслідок чого виникає аварійне завершення програми-сервера. Розповсюджені реалізації цієї атаки:

зловмисники шукають помилки у програмному коді операційної системи чи якоїсь програми та примушують її обробляти такі виняткові ситуації, які вона обробляти не може. В наслідок чого виникають помилки і відмова в обслуговуванні.

зловмисник змінює якусь програму таким чином, що вона після цього записує дані більшого розміру, ніж розмір буферу, що їй виділяється. Виникає помилка в наслідок переповнення буферу, що призводить до відмови в обслуговуванні.

Широко застосовуються DoS-атаки, що спрямовані на маніпуляцію таблицями маршрутизації та на службу DNS. Як відомо, деякі протоколи маршрутизації, такі як RIPv1 та BGP, не мають взагалі або мають слабкі алгоритми аутентифікації. Це дає можливість зловмиснику отримати доступ до маршрутизатору. Підключившись до нього, зловмисник вносить зміни до таблиці маршрутизації. Він змінює маршрут руху інформації, що призначена для користувачів таким чином, що вона направляється в неіснуючу мережу. В наслідок цього, користувачі системи перестають обслуговуватися. При реалізації атаки, що спрямована на сервери DNS, зловмисник змінює в кеш-пам'яті сервера IP-адресу ресурсу, що атакується, на такий, якого не існує. Внаслідок чого, сервер DNS, який виконує зворотній пошук IP-адреси по доменному імені, повертає неіснуючу адресу, що призводить до відмови в обслуговуванні.

На даний момент найбільш ефективними та такими, які важко виявити, є низькошвидкісні DoS-атаки. Можливість реалізації даної атаки обумовлюється особливостями роботи протоколу TCP, а саме механізму тайм-ауту та повторної передачі пакету. Цей механізм працює наступним чином: після відправлення пакету очікується пакет-відповідь протягом інтервалу часу RTO (Retransmission TimeOut). Якщо пакет-відповідь не приходить у продовж цього інтервалу часу, виконується повторна передача пакету, а RTO збільшується в два рази. Якщо знову пакет-відповідь не приходить у продовж інтервалу часу RTO, ще раз виконується повторна передача, а RTO збільшується ще у два рази. І так далі. Цю особливість використовує зловмисник для

реалізації атаки. Він відправляє імпульс трафіку в необхідний момент часу, а саме в кінці інтервалу RTO. В наслідок цього, канал зв'язку переповнюється в момент, коли очікуються пакети-відповіді. В зв'язку з цим вони не отримуються, а інтервал часу RTO збільшується в два рази. Далі зловмисник повторює свої дії. Пакети-відповіді знову не отримуються. Таким чином, виникає стійка непрацездатність системи і відмова в обслуговуванні легітимних користувачів.

Висновки

Таким чином, існує декілька видів DoS-атак. Найпростішим з них є переповнення полоси пропускання. Реалізації цього виду атак відомі давно, вони легко виявляються, існує багато засобів ефективного захисту від них. Атаки з використанням недостатньої кількості ресурсів системи можливі лише у разі її невірної налаштування системним адміністратором, тому також є неефективними. Більш суттєвий результат дають атаки DNS та маніпуляції з таблицею маршрутизації. Але при правильному налаштуванні системи та використанні засобів

виявлення та захисту від атак, вони не становлять істотної загрози. Але існує такий вид DoS-атак, який є достатньо ефективним і простим у реалізації. Це низькошвидкісні DoS-атаки. Для реалізації такої атаки зловмисник використовує особливості роботи протоколу TCP, а саме механізм тайм-ауту та повторної передачі пакета. Цей механізм необхідний для стабільної роботи протоколу TCP, але, на ряду з цим, він дає зловмиснику можливість реалізувати атаку. Йому лише необхідно в певні моменти часу відправляти імпульси трафіку, які переповнюють канал пропускання серверу на короткий проміжок часу, що зриває отримання сервером пакетів-відповідей. Таким чином, зловмисник створює тривалий час відмову в обслуговуванні легітимних користувачів. При цьому виявити таку атаку досить складно. На теперішній час не існує ефективних засобів виявлення та захисту від низькошвидкісних DoS-атак. Тому розробка методу виявлення і захисту від даного типу DoS-атак, а також ідентифікації зловмисника є актуальною науковою задачею.

Література

1. Касперски Крис Техника сетевых атак / К. Касперски. – М.: СОЛОН-Р, 2001. – 304 с. **2. Крис Касперски.** Компьютерные вирусы изнутри и снаружи. – СПб.: Питер, 2006. – 526 с. **3. Медведовский И.Д.** Атака из Internet / И.Д. Медведовский, Б. В. Семьянов, Д. Г. Леонов, А. В. Лукацкий. – М.: СОЛОН-Р, 2002. – 368 с. **4. Петренко С.А.,** Политики безопасности компании при работе в интернет / С.А. Петренко, В.А. Курбатов – М.: ДМК Пресс, 2011. – 396 с. **5. Жуков Юрий** Основы веб-

хакинга. Нападение и защита / Ю. Жуков – СПб.: Питер, 2006. – 208 с. **6. Столлингс Вильям** Основы защиты сетей. Приложения и стандарты / В. Столлингс – М.: Вильямс, 2002. – 432 с. **7. Норткати Стивен** Обнаружение нарушений безопасности в сетях / С. Норткати Н. Джуди – М.: Вильямс, 2003. – 448 с. **8. Эрикссон Джон** Хакинг: искусство эксплойта / Д. Эрикссон, 2-е издание. – М.: Символ Плюс, 2009. – 510 с.

В статье проанализированы основные виды DoS-атак. Рассмотрены пути их реализации для атак компьютерных сетей и возможности защиты от них.

Ключевые слова: DoS-атака, компьютерная система, эксплойт, протокол, канал пропускания.

Analysis of the main types of DoS-attacks has carried out. The ways of their realization for attacks of computer networks and possibilities of protection against them have considered.

Key words: DoS-attack, computer system, exploit, protocol, transmission channel.