Автор:
Баранов Сергій Сергійович,
студент 21 І групи
Науковий керівник:
Франчук Василь Михайлович,
кандидат педагогічних наук,
доцент кафедри комп'ютерної інженерії

УРАЗЛИВОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ. DDOS АТАКА.

Анотація. Метою дослідження є вивчення способів використання уразливостей комп'ютерних мереж зловмисником на прикладі атаки на відмову у обслуговуванні. Завданням дослідження є знайти способи повного чи часткового уникнення атаки такого типу. Об'єктом дослідження є атака на відмову в обслуговуванні. Методом дослідження є збір даних на основі досвіду вчених у галузі захисту комп'ютерних систем. Предметом дослідження є принципи роботи та стратегії застосування таких атак. Результатом дослідження є методи захисту від дій зловмисника такого типу.

Ключові слова: Комп'ютерна мережа, вразливість, атака на відмову в обслуговуванні,захист ресурсів, DDoS атака.

Вступ. З розвитком комунікаційних технологій та входженням їх у повсякденне життя вони є корисним знаряддям для навчання та іншої діяльності,але негативним наслідком цього є можливість використання зловмисником даних користувача та ресурсів його системи для власних потреб (несанкціонований доступ до даних, «зомбування» комп'ютера для створення DDoS атаки тощо)

Постановка задачі. Користувачі глобальної мережі Інтернет часто стають жертвами атак зловмисників,що використовують уразливості їх системи навіть не помічаючи цього. Тому існує проблема інформування людей про можливі атаки хакерів, їх основні класифікації,методи боротьби та профілактики.

Мета роботи. Метою дослідження є використання уразливостей системи зловмисником на прикладі атаки на відмову в обслуговуванні та методи .

Основна частина.

Уразливість – властивість комп'ютерних систем до збоїв, спричинених зовнішнім впливом чи внутрішніми недоліками.

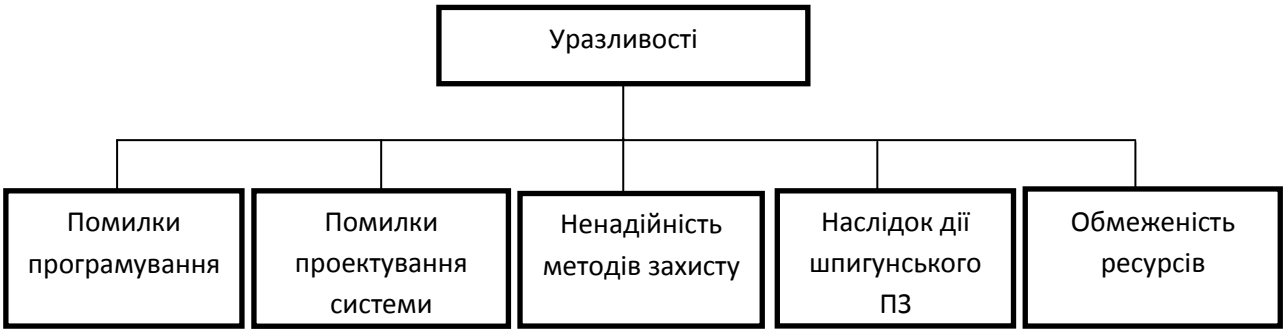

Рис. 1. Основні уразливості системи

Для виправлення більшості уразливостей, див. (рис.1) існують загальні методи їх ізоляції, зокрема використання фаєрволів, антивірусних програм,оновлення систем тощо. Найнебезпечнішими діями зловмисника може бути використання обмеженості ресурсів системи(смуга пропускання, процесорний час тощо) .

Розглянемо спосіб атаки на мережу чи окремий вузол спрямовану на відмову в обслуговуванні (Denial of service attack – DoS). Даний вид дій зловмисника полягає у

використанні усіх ресурсів системи,таким чином щоб правомірні користувачі не мали змоги отримати до них доступу.

Якщо така атака відбувається з великої кількості вузлів мережі то вона називається розподіленою(Distributed Denial of Service attack– DDoS).

Відмінність розподіленної й звичайної атаки на відмову в обслуговуванні полягає в тому, що перша складається з великої кількості DoS атак від різних вузлів мережі.Одна із негативних сторін такого виду атаки полягає у тому, що користувач може не знати про використання його ресурсів системи для здійснення цієї атаки.

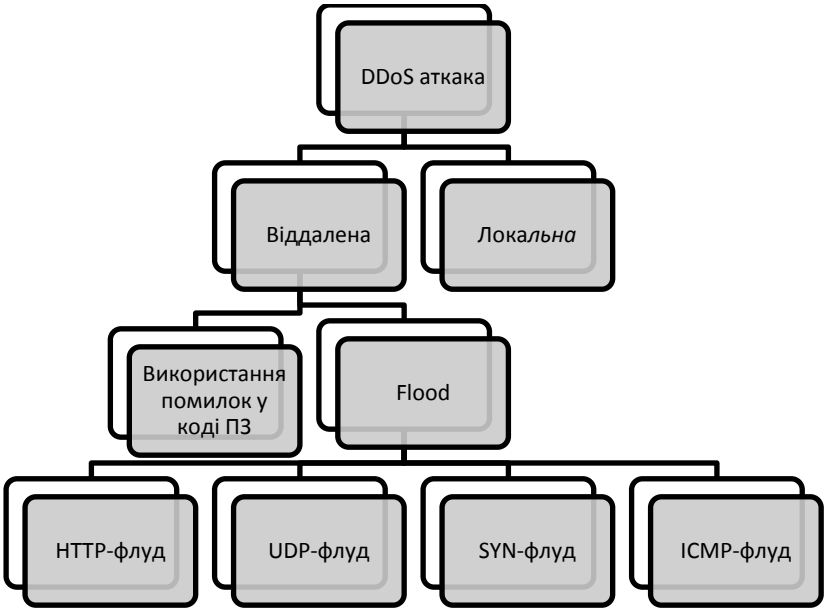

Рис. 2. Класифікація DDoS атак

Класифікувати DDoS атаки можна за наступною схемою див. (рис.2).

Локальна DDoS атака – це атака при якій зловмисник уже має доступ до системи й застосовує, для використання її ресурсів, запуск ПЗ (Програмний Засіб) який містить в собі циклічний алгоритм, що займає весь процесорний час,оперативну пам'ять тощо.

Віддалена DDoS атака – це атака з використанням помилок в коді ПЗ з метою довести його до неробочого стану і системи в цілому.

Віддалений флуд – це відправлення на адресу «жертви» величезної кількості пакетів. Метою флуду може бути канал зв'язку або ресурси комп'ютерної системи.

Атаки з використанням флуду можна класифікувати за назвами протоколів які використовуються у процесі злому.

HTTP-флуд – це вид DDoS атаки коли атакуючий відправляє HTTP-пакет, такий, щоб сервер «відповів» на нього пакетом, розмір якого в сотні разів більший. А для того, щоб відповідні HTTP-пакети не викликали відмови в обслуговуванні у системі зловмисника, щоразу підміняється власна ip-адреса на ip-адреси вузлів в мережі.

ICMP-флуд – це вид DDoS атаки коли атакуючий за допомогою підсиленої мережі за розподіленими адресами відправляє підроблені ICMP-пакети, за допомогою ping-запитів, на усі вузли,в яких замінюється ip-адреса отримувача на адресу жертви.

UDP-флуд – це вид DDoS атаки коли атакуючий відправляє echo-команди з використанням розподіленого запиту. Потім підміняється ip-адреса зловмисника на ip-адресу жертви, яка незабаром одержує безліч повідомлень-відповідей.

SYN-флуд – це вид DDoS атаки заснований на спробі ініціалізації великого числа одночасних TCP-з'єднань через з відправленням SYN-пакету з не існуючою зворотною адресою. Після кількох спроб відіслати у відповідь ACK-пакет на недоступну адресу, на більшості операційних систем вони ставляться в чергу. І лише після n-ої спроби закриваються з'єднання. Оскільки потік ACK-пакетів дуже великий, незабаром черга виявляється заповненою, і система дає відмову на спроби відкрити нове з'єднання.

Є два варіанти організації DDoS атак:

Ботнет – зараження певного числа комп'ютерів програмами, які в певний момент починають здійснювати запити до атакованого сервера.

Флешмоб – домовленість великого числа користувачів мережі,у визначений час здійснювати певні типи запитів до атакованого сервера.

Щоб не стати жертвою під час DDoS-атаки на систему, необхідно ретельно підготувати її до такої ситуації:

1. Всі сервери, які мають прямий доступ в зовнішню мережу, мають бути підготовлені до простої і швидкої віддаленої роботи. Великою перевагою буде наявність другого, адміністративного, мережевого інтерфейсу, через який можна отримати доступ до сервера при зайнятому основному каналі.
2. Програмне забезпечення, використовуване на сервері, завжди повинно знаходитися в актуальному стані. Всі дірки (уразливості) – ліквідовані, оновлення встановлені.
3. Всі мережеві сервіси, призначені для адміністративного використання, мають бути захищені брандмауером.
4. На сервері (або на першому маршрутизаторі) має бути встановлена система аналізу трафіку, використання якої дозволить своєчасно дізнатися про атаку, що починається, і вчасно виконати заходи з її запобігання [1].

Висновок. Уразливості є у кожній системі,вони можуть бути використані зловмисником для порушення прав користувача. Атака на відмову в обслуговуванні є дуже небезпечною,адже якщо помилка в ПЗ завжди може бути виправлена, то повна витрата ресурсів – ні. DoS-атаки можна класифікувати на локальні і віддалені. DDoS-атаки і їх ефективність можна істотно понизити за рахунок правильного налаштування маршрутизатора, брандмауера і постійного аналізу аномалій в мережевому трафіку.

Список використаних джерел

1. Зобнин Е.И. Устоять любой ценой / Е. И. Зобнин // Журнал Хакер. – 2009. – № 129. – С. 124.
2. Denial Of Service Attack [Electronic resource] / en.wikipedia.org/. – 2014. – Mode of access : http://en.wikipedia.org/wiki/Denial-of-service_attack