УДК 004.424

МЕРЕЖЕВІ АТАКИ В ІНТЕРНЕТ СЕРЕДОВИЩІ: ICMP FLOOD АТАКА

В.В. Дутчак, Н.С. Назарчук, В.В. Гурак, Т.В. Дитко

Івано-Франківський Національний Технічний Університет Нафти і Газу
Україна, 76000, м. Івано-Франківськ, вул. Карпатська, 15, vasuldutschak@mail.ru

На сьогоднішній час найважливішою проблемо в області ІТ є забезпечення цілісності і захисту даних. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Підвищення інтересу до TCP/IP-мереж обумовлено бурхливим зростанням мережі Internet. Однак це змушує замислитися над тим, як захистити свої інформаційні ресурси від атак із зовнішньої мережі. Якщо ви підключені до Internet, Ваша система може бути атакована. Протоколи сімейства IP є основою побудови мереж Intranet і глобальної мережі Internet. Незважаючи на те, що розробка TCP/IP фінансувалася Міністерством оборони США, TCP/IP не володіє абсолютною захищеністю і допускає різні типи атак, розглянуті в даній главі. Для здійснення подібних атак потенційний зловмисник повинен мати контроль хоча б над однією з систем, підключеної до Internet. Одним з підходів до аналізу загроз безпеці комп'ютерних систем є виділення в окремий клас загроз, властивих тільки комп'ютерним мережам [1]. DoS-атака (Denial of Service – відмова в обслуговуванні) – атака на розрахункову систему з метою вивести її з ладу, тобто створити умови, щоб користувачі не могли отримати доступ до системи.

Виділяють такі види DdoS атак:

1 UDP Flood – Мережева атака яка використовує безсеансовий режим протоколу UDP. Полягає у відправці безлічі UDP-пакетів (як правило великого обсягу) на певні або випадкові номери портів віддаленого хоста. [2]

2 ICMP Flood– Мережева атака яка використовує протокол ICMP який компенсує недоліки протокола IP і гарантовано надсилає дані [3]

Управління Інтернет повідомленнями протоколу ICMP здійснюється без встановлення з'єднання, що використовується для IP операцій, діагностики та помилок [4]. Так само, як з UDP Flood, ICMP Flood (або Ping Flood) є прикладом незахищеності від основного нападу; тобто, він не покладається на будь-яку конкретну помилку, наприклад, досягнути відмови в обслуговуванні. ICMP Flood може включати будь-який тип наприклад ICMP повідомлення запиту або луни. ICMP Flood відправляє трафік на цільовий сервер, він стає перевантажений від спроб обробляти кожен запит, в результаті чого відбувається відмова в обслуговуванні. ICMP Flood є об'ємною атакою, вимірюється в Мбіт (пропускна здатність) і PPS (пакетів в секунду).

Організувати атаку можна за допомогою програми Anonymous DoSer. Програма проста у використанні потрібно вказати адресу сайту або його ip і час який пакет буде надсилатись.

```
Website [URL/IP]: адреса.сайту
Time [SECONDS]: 15
```

Для ідентифікації атакуючого трафіку застосовуються апаратні засоби, які аналізують сигнатуру, статичні і поведінкові дані для кожного типу захищаючого сервісу. Перевіряється зберігання вимог специфікацій протоколів, що використовуються.

Відкинувши трафік «широкої смуги» на рівні додатку (L5-L7) створюється інтелектуальна фільтрація, де проводиться аналіз атак на протоколи HTTP, HTTPS (див. Схему на Рис.1). В результаті послідовної фільтрації до клієнтів доходить тільки легітимний трафік.[5, 6]

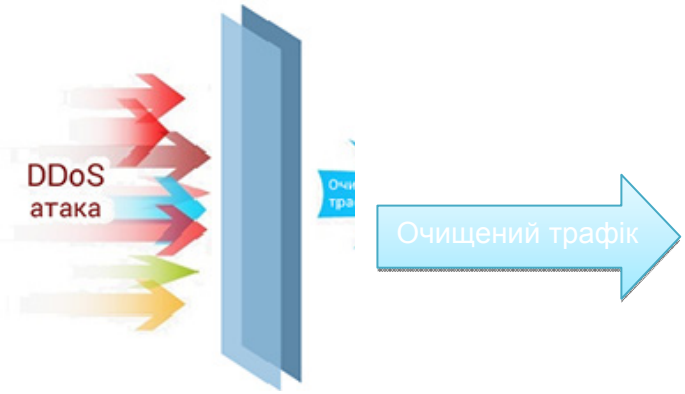

Рисунок 1 - Схематичне зображення смуг для здійснення фільтрації

Також існує можливість програмного захисту але це дуже примітивний метод забивання смуги пропускання і створення навантажень на мережевий стек через монотонну посилку запитів ICMP ECHO (пінг). Легко виявляється за допомогою аналізу потоків трафіку в обидві сторони: під час атаки типу ICMP-флуд вони практично ідентичні. Наприклад:

```
ping -i 0 -s 10000 -l 100 -q ya.ua
```

В роботі проведене дослідження мережевої ICMP Flood атаки, наведені приклади застосування та способи боротьби з даним різновидом атак.

Інформацію про мережеві атаки, перечислено види DDos атак та їхні можливі причини. Детально розглянуто тип ICMP Flood атаки, а також було розглянуто метод захисту від ICPM Flood атаки..

Література

1 Мережеві атаки і дещо ще [Електронний ресурс]. Джерело доступу: http://uk.shram.kiev.ua/hacker/net_attacks.shtml – Назва з екрану. – Дата звернення: 16.09.2015.

2 UDP – Flood визначення мережевої атаки [Електронний ресурс]. Джерело доступу: https://ru.wikipedia.org/wiki/UDP-флуд – Назва з екрану. – Дата звернення: 16.09.2015.

3 ICMP протокол і дещо ще [Електронний ресурс]. Джерело доступу: http://habrahabr.ru/post/157207/– Назва з екрану. –Дата звернення: 16.09.2015.

4 Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. –СПб.: Наука и техника, 2004.

5 Грязнов Е., Панасенко С. Безопасность локальных сетей – Электрон. журнал "Мир и безопасность" №2, 2003.

6 Фільтрація Ddos атак [Електронний ресурс]. Джерело доступу: https://ddos-lab.com/protection – Назва з екрану. – Дата звернення: 16.09.2015.