УДК 371.13.001.76
Багнюк Н.В. к.т.н. доц., Мельник В.М.к.ф-м.н.доц, Клеха О.В., Невідомський І.А.
Луцький національний технічний університет

ВИДИ DDOS-АТАК ТА АЛГОРИТМ ВИЯВЛЕННЯ DDOS-АТАК ТИПУ FLOOD-ATTACK

Багнюк Н.В., Мельник В.М., Клеха О.В., Невідомський І.А. Види DDoS-атак та алгоритм виявлення DDoS-атак типу flood-attack. У статті розкрито існуючі види DDoS-атак та їх суть, а також деякі методи боротьби та протидії цим атакам з метою забезпечення надійного та постійного функціонування комп'ютерної мережі та її компонентів. Також запропоновано алгоритм протидії DDoS-атакам типу flood-атаки.
Ключові слова: DDoS-атака, види DDoS-атак, flood-атаки, функціонування комп'ютерної мережі.

Багнюк Н.В., Мельник В.М., Клеха О.В., Невидомский И.А. Виды DDoS-атак и алгоритм обнаружения DDoS-атак типа flood-attack. В статье раскрыты существующие виды DDoS-атак и их суть, а также некоторые методы борьбы и противодействия этим атакам с целью обеспечения надежного и постоянного функционирования компьютерной сети и ее компонентов. Также предложен алгоритм противодействия DDoS-атакам типа flood-атаки.
Ключевые слова: DDoS-атака, виды DDoS-атак, flood-атаки, функционирования компьютерной сети.

Bagnyuk N.V., Melnyk V., Klekha A.V., Nevidomskyy I.A. Types of DDoS-attacks and detection algorithm of such DDoS-attacks as flood-attack. The article considers the existing types of DDoS-attacks and their essence, and some methods of struggle and counter these attacks in order to ensure a reliable and continuous operation of a computer network and its components. Also, the counteractive algorithm DDoS-attacks flood-type attack.
Keywords: DDoS-attack, types of DDoS-attacks, flood-attack, computer network functioning.

Постановка наукової проблеми.

Розподілена атака на відмову в обслуговуванні – це реальна і зростаюча загроза, з якою стикаються компанії в усьому світі. Ці атаки реалізуються великою кількістю програмних агентів, розміщених на хостах, які зловмисник скомпрометував раніше. Реалізація цих атак може призвести не тільки до виходу з ладу окремих хостів і служб, а й повністю або тимчасово зупинити роботу мережі. У зв'язку з критичністю і нетривіальністю даного класу атак, побудова ефективних засобів захисту від них являє собою складну науково-технічну проблему. На рівні маршрутизаторів захист від DDoS-атак вже досить успішно реалізували компанії Cisco Systems. Але в цілому проблема DDoS-атак на сьогоднішній день як і раніше дуже гостро стоїть для більшості компаній.

Аналіз досліджень.

В обчислювальній техніці, атаки на відмову в обслуговуванні (DoS-атаки) або розподілені атаки на відмову в обслуговуванні (DDoS-атака) є спробою зробити машини або мережевий ресурс недоступним для можливих користувачів. Мотиви і цілі з DoS-атаки можуть відрізнятися, але в загальному випадку складаються із зусиль одного або декількох людей тимчасово або на невизначений термін перервати або призупинити надання послуг мережевих послуг.

Кожного дня по всьому світі відбуваються DDoS-атаки різні за масштабом (Рис.1) [7].

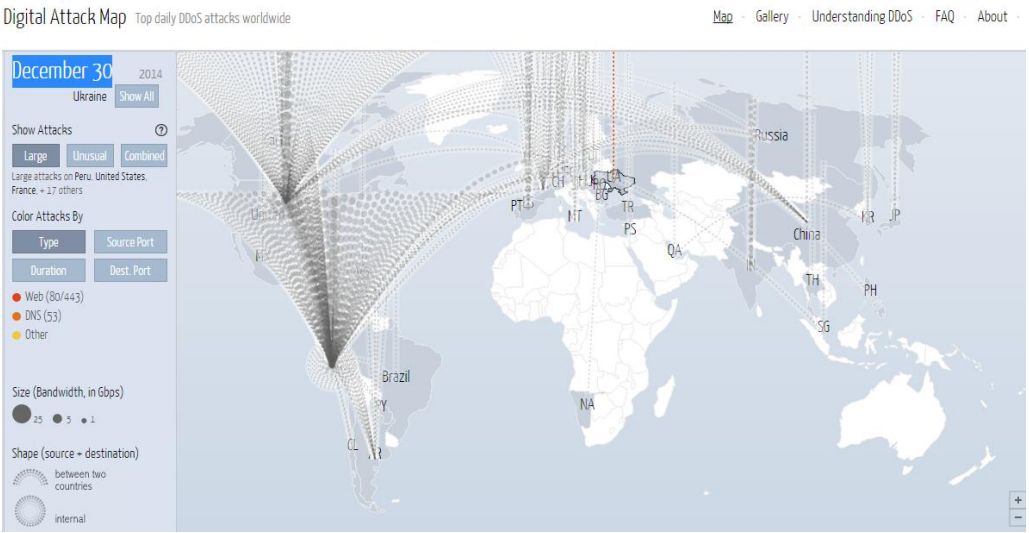

Рис.1. Цифрова карта DDoS-атак

Зазвичай використовуються такі терміни:

– Intruder: також називається нападник;
– Master: також називається оператором;
– Daemon: також званий агентом;
– Victim: завжди є жертвою.

Симптоми відмови в обслуговуванні згідно з US-CERT включають в себе:

– незвично низьку продуктивність мережі (повільне відкриття файлів або доступ до ресурсів);
– відсутність конкретного ресурсу;
– неможливість отримати доступ до будь-якого ресурсу;
– значне збільшення числа спам-листів (цей тип DoS-атаки включає в себе електронні листи з шкідливим вмістом);
– відключення бездротової мережі або доступу до мережі;
– «hit offline», тобто ціллю є позбавити вас підключення до мережі.

Відмови в обслуговуванні можуть також призвести до проблем у «гілці» мережі, в якій знаходиться фактична жертва нападників. Наприклад, пропускна здатність маршрутизатора між Інтернетом та локальною мережею може споживатися атакою, що призводить до збитків не тільки для потенційної жертви, але й для всієї мережі. Якщо атака здійснюється на досить великому масштабі – цілі географічні регіони, то через неправильно налаштоване обладнання мережевої інфраструктури, про що зловмисник міг і не знати, може бути порушена робота всієї мережі.

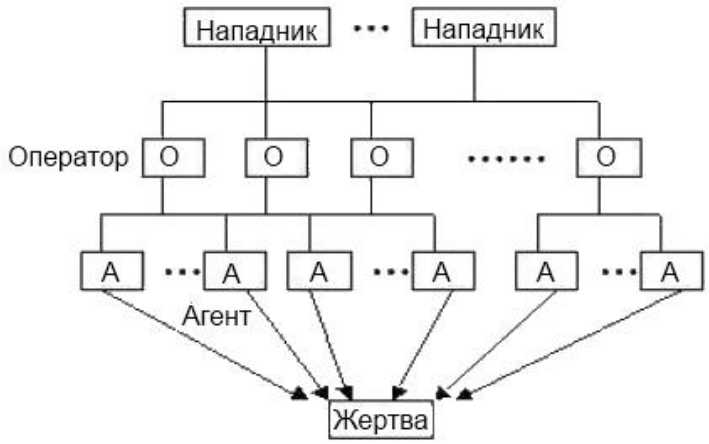

Рис. 2. Концептуальна схема DDoS-атаки

Одними з найпрогресивніших досліджень в області захисту від DDoS-атак є роботи професорів Peng T. Ong, Jaydip Sen та доктора Ashish Gupta. Структура атаки майже завжди є дуже складною, що не дозволяє в багатьох випадках відстежити нападника. Зв'язок між майстром і демонами може бути непомітним, так що стає важко знайти головний комп'ютер. Хоча деякі докази можуть існувати на одному або декількох комп'ютерах в мережі DDoS з місцем розташування майстра. Демони, як правило, автоматизовані так, що вони не є необхідними для постійного діалогу, котрий відбудеться між майстром і рештою мережі. Насправді, такі методи, які зазвичай використовуються, свідомо маскують особу і місцезнаходження господаря в мережі DDoS. Ці методи роблять процес аналізу атаки, блокування атакуючого трафіку і відстежування його до джерела надзвичайно важким.

У більшості випадків, системні адміністратори заражених систем навіть не знають, що демони були встановлені в ситемі. Навіть якщо вони знайшли і знищили програмне забезпечення DDoS, вони не можуть допомогти іншим користувачам визначити, чи є десь в системі ще розміщене подібне програмне забезпечення. Популярними системами для експлуатації є Web-сервери, електронна пошта, інші сервери, так як ці системи можуть мати велику кількість відкритих портів, великий обсяг трафіку, і навряд чи будуть швидко виведені з ладу, навіть при атаці на них.

DDoS-атаки завжди пов'язані з низкою систем. Типовий сценарій DDoS-атаки може відбуватись приблизно за наступними кроками:

– зловмисник знаходить одну або декілька систем в Інтернеті, які можна скомпрометувати і експлуатувати. Це зазвичай здійснюється за допомогою вкраденого облікового запису в системі з великим числом користувачів через неуважних адміністраторів чи користувачів, переважно із з'єднанням з високою пропускною здатністю до Інтернету;

– в зломану систему завантажуються будь-яка кількість таких інструментів, як сканери, детектори операційної системи, руткіти, а також програми DoS/DDoS. Ця система стає майстром DDoS. Майстер за допомогою програмного забезпечення дозволяє знайти ряд інших систем, які можна експлуатувати. Зловмисник сканує великі діапазони IP мережевих адресних блоків, щоб знайти системи, що мають вразливі місця в безпеці. Ця початкова фаза масового вторгнення використовує автоматизовані засоби, щоб віддалено зламати кілька сотень чи кілька тисяч хостів і встановити DDoS агенти в цих системах. Автоматизовані інструменти, що використовуються не є частиною інструментарію DDoS, але є способом обміну всередині груп злочинних хакерів. Ці зламані системи є початковими жертвами нападу DDoS. Згодом ці системи будуть експлуатуватись демонами DDoS, які здійснюватимуть фактичний напад;

– зловмисник має список систем, якими він може керувати, і в яких системах є демони DDoS. Фактичний напад відбувається, коли зловмисник запускає програму в головній системі, що спілкується з демонами DDoS, щоб почати атаку.

В таблиці 1 показані найпопулярніші та найвідоміші засоби для DDoS-атаки та їх основні специфікації.

Таблиця 1. Засоби DDoS-атаки та їх специфікації

Засоби DDoS-атаки	Зв'язок Intruder-to-master	Зв'язок Master-to-daemon	Зв'язок Daemon-to-master
Trinoo	27665/tcp	27444/udp	31335/udp
TFN	ICMP Echo/Echo Reply	ICMP Echo Reply	ICMP Echo/Echo Reply
Stacheldraht	16660/tcp	65000/tcp	ICMP EchoReply
Trinity	6667/tcp	6667/tcp (також 33270/tcp)	
Shaft	20432/tcp	18753/udp	20433/udp

Атака "відмова в обслуговуванні" характеризується явною спробою нападників відключити законних користувачів мережі або ресурсу від використання його доступних сервісів. Є дві основних форми DoS атак: ті, які є сервісами злому (crash services) і сервіси флуду (flood services).

Атака DoS може бути здійсненна у ряді напрямків згідно з професором. П'ятьма основними типами атак є:

– споживання обчислювальних ресурсів, таких як пропускна здатність, дисковий простір або процесорний час;

– перешкоджання доступу до інформації про конфігурацію мережі, наприклад, інформацію про маршрутизацію;

– перешкоджання доступу до інформації про стан, наприклад, небажане скидання сеансів TCP;

– перешкоджання доступу до фізичних компонентів мережі;

– перешкоджання масової комунікації між передбачуваними користувачами і жертвами, так що вони вже не можуть спілкуватися.

Атака DoS може включати в себе використання шкідливих програм, призначений для:

– використання процесора на максимум, запобігаючи будь-якій новій роботі машини;

– помилки тригера в мікрокодах машини;

– помилки тригера в послідовності інструкцій, з тим, щоб змусити комп'ютер працювати в нестабільному стані або припиняти його роботу;

– використовувати помилки в операційній системі, тобто використовувати всі наявні засоби, щоб реальна робота не виконувалась або відбувся збій самої системи;

– збій самої операційної системи.

Рисунок 3 ілюструє тип широкосмугової атаки, котрий називається відбиваючою розподіленою відмовою в обслуговуванні (DRDOS-атакою). Метою DRDOS-атаки є приховати джерела трафіку атаки за допомогою третіх осіб (маршрутизаторів або веб-серверів) для передачі трафіку атаки до жертви. Ці безневинні треті особи називаються відбивачами. Будь-яка машина, яка відповідає на вхідний пакет може стати потенційним відбивачем. Напад DRDOS складається з трьох етапів. Перший етап являє собою типову DDoS-атаку, де нападники відправляють велику кількість пакетів до хоста жертви. Тим не менш, на другому етапі, після того як нападник отримав контроль над певною кількістю «зомбі», замість інструктажу «зомбі» для відправки трафіку атаки жертвам безпосередньо, «зомбі» наказано вислати третім особам фальшиві пакети з IP-адресом жертви в якості джерела IP-адресу. На третьому етапі, треті особи будуть надсилати відповідь до жертви, яка являє собою атаку DDoS. У порівнянні з традиційною DDoS-атакою, трафік від нападу DRDOS збільшений за допомогою третіх осіб. Це робить напад більш ширшим а, отже, і процес зупинення атаки буде більш важким. Крім того, джерела IP-адрес атаки є безневинними третіми особами. Це робить процес простеження джерела атаки вкрай складним. Нарешті, DRDOS атаки мають здатність посилювати трафік атаки, що робить атаку ще більш потужною.

Рис. 3. DR-DoS-атака

HTTP flood відноситься до атаки, що бомбардує веб-сервери HTTP-запитами. HTTP flood спільна риса в більшості ботнетів програмного забезпечення. Для відправлення запиту HTTP потрібне підключення TCP, який вимагає справжнього IP-адресу. Зловмисники можуть підставити його за допомогою IP-адреси бота. Крім того, зловмисники можуть сформувати HTTP запити різними способами для того, щоб або збільшити силу атаки або уникнути виявлення. Наприклад, зловмисник може доручити ботнету відправляти HTTP-запити на скачування великих файлів від цілі. Так ціль повинна зчитати файл з жорсткого диска, зберегти його в пам'яті, завантажити його в пакети, а потім відправити пакети назад в ботнет. Таким чином, простий запит HTTP може спричинити значні витрати ресурсів процесору, пам'яті, пристроїв вводу/виводу і вихідних інтернет-з'єднань.

SYN flood-атака використовує уразливість TCP, а саме трьох ступінчатий запит, тому сервер повинен виділити велику структуру даних для всіх вхідних SYN пакетів, незалежно від його достовірності. Під час SYN flood-атаки, атакуючий посилає SYN пакети з вихідними IP-адресами, які не існують або не використовується. Коли сервер заносить інформацію запиту в стек

пам'яті, він буде чекати підтвердження від клієнта, який відправив запит. У той час як запит очікує підтвердження, він буде залишатися в стеку пам'яті. Оскільки IP-адреса джерела, використовуваного в ході SYN flood-атаки може виявитися помилковою, сервер не отримає пакета з підтвердженням запитів. Кожне напіввідкрите з'єднання буде залишатися в стеку пам'яті до закінчення часу запиту. Це призводить стек пам'яті до переповнення. Таким чином, ніякі запити, в тому числі потрібні, не можуть бути оброблені і послуги системи будуть відключені. SYN flood-атака залишаються одним з найбільш потужних методів флуду.

Smurf-атака типу ICMP flood, де зловмисники використовують ICMP-пакети echo-запитів, спрямованих до широкомовних IP адресів з віддалених місць, щоб згенерувати відмову в обслуговуванні. Є три особи таких нападів: зловмисник, посередники та жертви. По-перше, зловмисник посилає один ICMP echo-запит пакет на широкомовний адрес мережі і запит направляється на всі вузли в межах посередницької мережі. По-друге, всі хости в межах посередницької мережі, відправляють ICMP echo-відповіді, що йдуть на адрес жертви. Рішення проти Smurf-атаки включає відключення IP спрямованих на послуги широкомовної передачі в посередницькій мережі. В даний час, Smurf-атаки досить рідкісні в Інтернеті, бо захиститися від таких атак не складно.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження.

Загальна схема протидії DDoS-атакам представлена на рис.4.

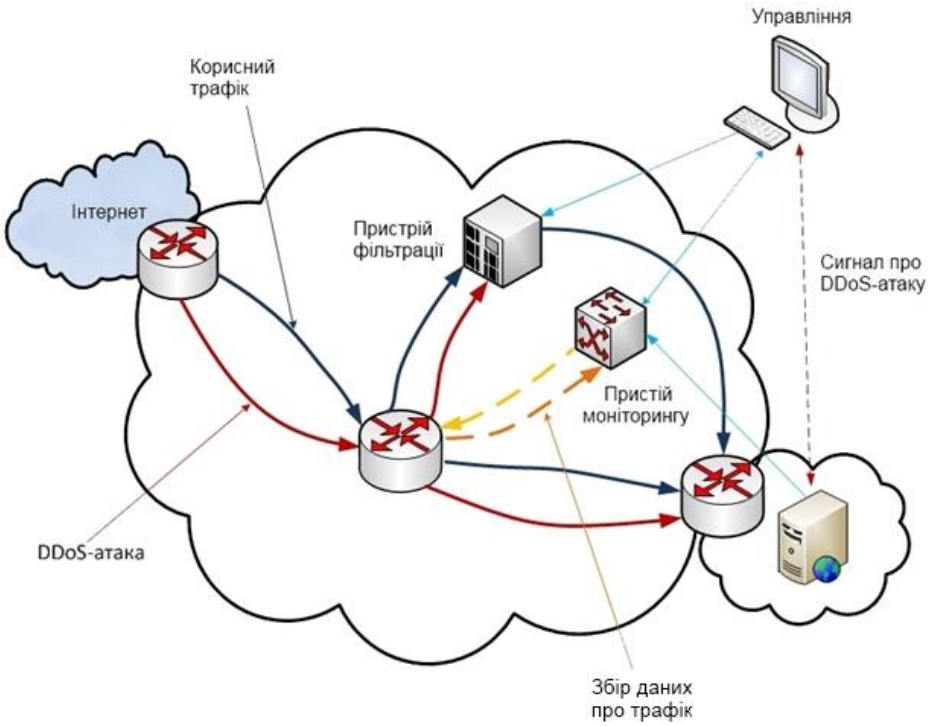

Рис. 4. Схема протидії DDoS-атаки

Технічна реалізація даного рішення передбачає наявність у мережі двох додаткових пристроїв, один з яких здійснює моніторинг вхідного трафіку і виявляє чи відбувається DDoS-атака, а другий фільтрує(очищає) зовнішній трафік.

У нормальному режимі роботи дані пристрої не повинні чинити жодного впливу на трафік що проходить. У разі ж атаки пристрій «очищення» затримує трафік, ідентифікований як DDoS-пакети, не допускаючи її потрапляння у відносно вузькосмугові клієнтські канали і на клієнтські ресурси, тим самим не перериваючи надання клієнту основної послуги.

Пристрій моніторингу на сервері виконує чотири дії з метою виявлення атаки DDoS та джерела атаки. Ці чотири дії виконуються послідовно в тому ж порядку, як вони вказані:

1) виявлення нападу;
2) ідентифікації джерел атак;
3) зупинення трафіку, що надходить від джерел атаки;
4) тестування, чи атаку успішно зірвано.

На рисунку 5 представлена блок схема виявлення та зупинення DDoS-атаки. З самого початку перевіряється чи йде збільшення числа з'єднань до сервера, ніж це відбувається зазвичай. Якщо ж все-таки є їх перевищення, то це є підставою для перевірки чи йде атака на наш сервер.

Перш за все перевіряється чи знаходяться IP адреси в списку виключень, тобто доступ до мережі вони не повинні мати.

Після цього підраховується кількість з'єднань з кожного IP адресу до нашого сервера. Коли їх більше, ніж n, то це є підставою вважати, що йде DDoS-атака. Щоб припинити атаку варто заблокувати дані IP адреси на 5 хвилин. За цей час буде зупинено атаку.

Дана схема є дієвою для всіх flood-атак. Єдина різниця що для кожного типу атаки буде відрізнятися число n.

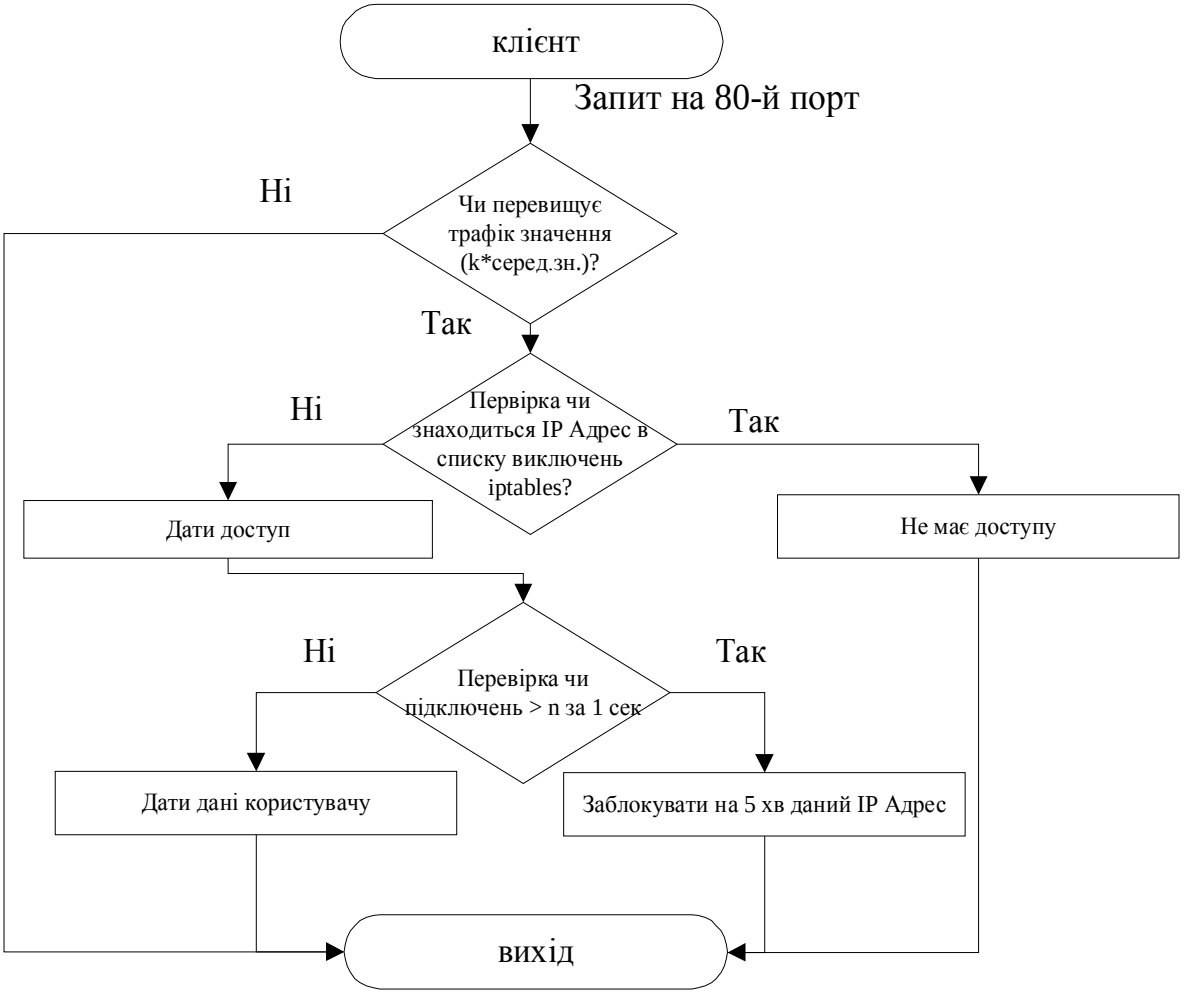

Рис. 5 – Блок схема виявлення та зупинення DDoS-атаки

Коли є підозра, що йде DDoS-атака всі дані про з'єднання записуємо в окремий текстовий файл. Ключовими полями в файлі, котрі нас цікавлять є час та вхідний IP-адрес з'єднання. Ці два поля за допомогою циклу в Python поміщаємо до словника (dictionary):

```
for i in range(len_line-1):    //len_line – кількість рядків в файлі
        item = my_file.readline()
        item = string.split(item, " ")
        d[item[2]]=item[3]        // d – dictionary, в котрий поміщаємо наші дані
        l+= [item[2]]
```

Тепер опрацьовуємо dictionary в відповідності чи є перевищення кількості з'єднань число n за 1 секунду за допомогою дано коду:

```
for i in range (t+1):
        l2=[]
```

```
for item in l:
        if (float(item) > i) and (float(item) < (i+1)):
                l2.append(d[item])
    l3+=[x for x in set(l2) if l2.count(x)>n]
l3 = [e for i,e in enumerate(l3) if e not in l3[:i]]
```

В списку l3 містяться всі IP-адреси, з котрих йде DDoS-атака. Тому всі вони блокуються на 5 хвилин в iptables.

Висновки та перспективи подальшого дослідження. Таким чином, DDoS-атаки є реальною загрозою для функціонування будь-якої мережевої комп'ютерної системи. Хоча часто важко виявити і реагувати на розумно сплановані і підготовлені атаки. Після рекомендації, що містяться в цій статті буде легше захистити жертву, максимально знизивши при цьому вплив потенційно небезпечних атак.

1. Chen, E.Y. Detecting DoS Attacks on SIP Systems. In: Proceedings of the 1st IEEE Workshop on VoIP Management and Security, pp 53 – 58.
2. Forristal, J.Fireproofing against DoS Attacks. URL: http://www.networkcomputing.com/1225/1225f3.html, Network Computing.
3. Matsure, K., Imai, H. Protection of Authenticated Key-Agreement Protocol against a Denial-of-Service Attack. In Proceedings of 1998 International Symposium on Information Theory and its Applications (ISITA'98), pp. 466 – 470, Oct. 1998.
4. Park, K., Lee, H. "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internet. In Proceedings of ACM SIGCOMM'01, San Diego, CA, August 2001, pp. 15 – 26.
5. Park, K., Lee, H. On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack. In Proceedings of IEEE INFOCOM'01, Anchorage, Alaska, 2001, pp. 319 – 347.
6. Paxson, V. An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks. ACM Computing Communication Review, Vol. 31, No. 3, pp. 38 -47, 2001.
7. Paxson, V. An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks. ACM Computing Communication Review, Vol. 31, No. 3, pp. 38 -47, 2001.
8. Peng, T., Leckie, C., Ramamohanarao, K. Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems. ACM Computing Surveys, Vol. 39, No. 1, April 2007.
9. Ramanathan, A.: WesDes: A Tool for Distributed Denial of Service Attack Detection. Thesis at Texas A&M University, August 2002.
10. Sen, J. A Novel Mechanism for Detection of Distributed Denial of Service Attacks. In Proceedings of the 1st International Conference on Computer Science and Information Technology (CCSIT 2011) – 2011, pp. 247 – 257
11. Top daily DDoS attacks worldwide. URL: http://www.digitalattackmap.com.