https://www.scilook.eu/index.php/slif/article/view/slif17-01-036
DOI: 10.30888/2415-7538.2020-17-01-036

УДК 004.2

CONCEPTS OF DOS, DDOS-ATTACKS, BASICS OF USING, WAYS TO PROTECT

ПОНЯТТЯ DOS, DDOS-АТАК, ОСНОВИ ЗАСТОСУВАННЯ, СПОСОБИ ЗАХИСТУ

Morchenko D. N. / Морченко Д. Н.
Odessa National University, Odessa, Fontanska doroga, 10, 65029
Военная академия (г. Одесса), Одесса, Фонтанская дорога, 10, 65029
Bondarenko A. P. / Бондаренко А. П.
Odessa National University, Odessa, Fontanska doroga, 10, 65029
Военная академия (г. Одесса), Одесса, Фонтанская дорога, 10, 65029

Анотація. *У даній статті розглянуті основи DoS, DDoS-атак як інструменту протидії певним організаціям, що проводяться конкурентами, зловмисниками та іншими особами, що мають на меті завдання шкоди організації. Проаналізовані основні види флуд-атак, відмінність DoS, DDoS-атак, сфера застосування та основні заходи щодо захисту від них. Актуальність теми полягає в тому, що проведення DoS, DDoS-атак є простим, але ефективним способом протидії певній організації та можуть завдати велику матеріальну шкоду, не враховуючи авторитет серед інших організацій; часто власники ресурсів, що атакуються, не знають про такі атаки та не можуть їм протидіяти.*

Ключові слова: *DoS-атака, DDoS-атака, флуд-атака, Python, модуль TeleBot, IP-адреса, ICMP-флуд, SYN-флуд, UDP-флуд і HTTP-флуд, ACK-пакет, Overwhelming Quantity of Traffic, Maliciously Formatted Packets, ботнет.*

Вступ

Сьогодні ми майже не можемо собі уявити ту чи іншу авторитетну організацію без власного сайту, не важливо чим є ця організація, магазином, незалежними ЗМІ, представниками навчального закладу, державним урядом. Як правило, всі ми знаємо про конкуренцію, у кожного є конкурент в якійсь сфері, такі організації не стали виключенням. В процесі глобальної інформатизації з'явилися нові методи та заходи, що направлені на боротьбу з конкурентами, якщо раніше це було фізичне втручання (викрадення/псування майна, знищення/пошкодження місць дислокації цих організацій), то зараз це війна у кіберпросторі. Варто зауважити, що зараз майже кожен має доступ до інтернету та здійснює купівлю товарів, читає певну інформацію на форумах певних організацій, отримує доступ до новин на інформаційних порталах, але що буде, якщо один із сайтів не буде працювати або буде працювати з великою затримкою? Вірно, ця організація втратить споживачів, а конкуренти, які це влаштували, вірогідно, отримають нових клієнтів. Однією з форм завдання шкоди певній організації є влаштування Dos, DDoS атак, які спрямовані на створення таких умов, при яких об'єкт, що атакується виходить з ладу або просідає в продуктивності, що в кінці завдає шкоди діяльності організації, включаючи втрату клієнтів та витрату коштів на відновлення сайту.

DoS, DDos-атаки, основні поняття, їхня відмінність

Спочатку розглянемо, що таке Dos, DDoS атаки та їхню відмінність. Не слід вважати, що це щось однакове, одна літера в абревіатурі, але відмінність більша, ніж здається. У випадку DoS-атаки використовується власна IP-адреса, що стосується DDoS-атаки, то там використовуються IP-адреси заражених

обчислювальних машин користувачів, що створюють бот-мережу.

DoS (Denial-of-service) – «Відмова в обслуговуванні», тип мережної атаки, яка полягає у надсиланні атакованому комп'ютеру або мережевому устаткуванню безліч зовнішніх запитів. Результатом DoS-атаки є переривання роботи мережних сервісів. Як кінцевий результат сайт втрачає статус «онлайн» протягом декількох годин, днів до відновлення. Розрізняють два види DoS-атак:

1. Надсилання надмірної кількості даних (Overwhelming Quantity of Traffic), тобто надсилання великої кількості даних з такою швидкістю, що атакуємі мережі, хости втрачають здатність їх обробити. Як результат ми маємо затримку передачі даних, відгуку, відмову пристрою або аварійне завершення роботи сеансу.

2. Надсилання пакетів зловмисного формату (Maliciously Formatted Packets), тобто надсилання великої кількості пакетів зловмисного формату до хоста або програми, в результаті останні не здатні обробити запити. Наприклад, атакуючий виходить за межі стандартного алгоритму роботи серверу, відсилаючи йому такі пакеті, що не можуть бути ідентифіковані програмою, або передає неправильно відформатовані пакети. Це може викликати сповільнення роботи або відмову пристрою-отримувача. Простим прикладом може виступити наступний шматочок коду на мові програмування Python з використанням модулю TeleBot:

```
1. import config
2. from telebot import *
3. bot = TeleBot(config.token)
4. @bot.message_handler(commands=['start'])
5. def welcome(message):
6. if message.chat.id != -1001425008287 or message.chat.id != 240930282:
7. bot.send_message(message.chat.id, 'Sorry, I think that you can\'t use me because
   you are not my creator -_-')
8. else:
9. bot.send_message(message.chat.id, f'Hi, @{message.from_user.username}')
10. bot.polling()
```

На шостій строчці бачимо порівняння однакового типу даних, у разі порівняння різних типів даних наша програма проігнорує інструкцію if, але існують випади, коли різні типи даних можуть викликати помилку, наприклад непередбачена конкатенація строки та цілого числа, знаючи це зловмисник може спеціально подати неправильний тип даних, що викличе помилку TypeError:

```
1. 8 + "3"
2. Traceback (most recent call last):
3. File "<stdin>", line 1, in <module>
4. TypeError: unsupported operand type(s) for +: 'int' and 'str'
```

DoS атаки вважаються серйозною загрозою, оскільки вони можуть легко переривати сеанс та викликати значну втрату часу та грошей. Ці атаки відносно прості для виконання навіть починаючим зловмисником. IP-адреса при цьому одна, що є однією із відмінностей з DDoS атаками.

Розподілена DoS атака (Distributed DoS Attack) тобто DDoS. Вона подібна до атаки DoS, але вона походить від декількох скоординованих джерел. Принцип атакуючої дії – канал розрахований на певний об'єм вхідного трафіку. Трафік, що перевищує певну міру, виводить ресурс з ладу. Іншими словами, запит користувача не обробляється, так як кількість запитів занадто велика та потрібно довго чекати, доки веб-ресурс опрацює всі запити.

Зараженні троянами комп'ютери, що приймають участь у атаці називаються «комп'ютерами-зомбі», мережа таких комп'ютерів-зомбі називається ботнетом. Стандартний алгоритм проведення DDoS-атаки виглядає наступним чином:

- сканування мережі на предмет виявлення потенційно слабких вузлів;
- захоплення вузлів та встановлення на них троянських програм;
- відправка команд «комп'ютерам-зомбі» з метою уразити певний веб-сервер.

DoS-атаки бувають наступними:

- Віддалене користування помилками ПЗ та доведення його дон неробочого стану;
- Flood (UDP-флуд, ICMP-флуд, MAC-флуд), тобто відправлення жертві великої кількості некоректних, рідше коректних пакетів. В якості жертви можуть виступати канали зв'язку, ресурси машини. У разі атаки на канал зв'язку він забивається пакетами та втрачає можливість обробляти легальні запити. У разі атаки на ресурси машини захоплюються за допомогою багаторазового і дуже частого звернення до одного з сервісів, який виконує складну, ресурсоємну операцію. Наприклад, така атака може включати в себе тривале звернення до одного з активних компонентів (скрипту) web-сервера, тоді ресурси машини витрачаються на обробку цих запитів, а легальні запити стають у чергу на обробку.

Хоча флуд-атаки не є ефективними сьогодні, проте варто розглянути їхній різновид:

- Icmp-флуд – простий метод забивання каналу пропускання та створення навантажень на мережевий стек через постійне посилання запитів ICMP ECHO (пінг). Такий метод атаки легко виявити за допомогою аналізу потоків вхідного та вихідного трафіку: під час атаки таким методом трафіки майже ідентичні.

- SYN-флуд – один із поширених методів, який дозволяє забивати канал зв'язку та вводити мережевий стек операційної системи у стан, коли він не може приймати нові запити на підключення. Такий метод заснований на спробі ініціалізації великої кількості одночасних TCP-з'єднань через посилання SYN-пакету зі зворотною адресою, якої не існує. Через декілька спроб надіслати у відповідь ACK-пакет на неіснуючу адресу більша частина операційних систем ставлять цю спробу в чергу. Та лише після багатьох невдалих спроб закривають з'єднання. Так як потік ACK-пакетів дуже великий, черга переповнюється та ядро дає відмову на спроби відкрити нове з'єднання. Сучасні DoS-боти ще й аналізують систему на наявність відкритих життєво важливих портів, щоб атакувати лише їх. Ідентифікується така атака доволі просто, варто лише спробувати підключитися до одного з сервісів, тоді спроба не буде вдалою;

- UDP-флуд – простий та частий метод захаращення смуги пропускання. Такий метод атаки проводиться шляхом нескінченного посилання upd-пакетів на порти upd-сервісів. Така атака легко накривається шляхом ізоляції сервісів, що атакуються та встановленням ліміту на кількість з'єднань за одиницю часу до dns-сервера на стороні шлюзу;

- HTTP-флуд – один із самих популярних методів флуду. Засновується на нескінченному посиланні маленьких http-повідомлень GET на 80-й порт, що призвело би до навантаження на web-сервер. Часто жертвою є не сам сервер, а один із його скриптів, якому відводяться ресурсоємні завдання або робота з базою даних.

У класичному виконанні (один атакувальний — одна жертва) наразі дає результат перший вид атаки. Класичний флуд — не ефективний. Причина полягає в тому, що сьогодні використовуються багато заходів, що сприяли би захисту від атак, до них відносять ширину каналу, обчислювальні потужності та анти-DoS прийоми в ПЗ (як варіант, затримка при неодноразовому виконані монотонних дій). При цьому особа, яка проводить атаку втрачає свою продуктивність, не завдаючи збитку жертві, але якщо таких людей буде більше, то вони здатні з легкістю покласти сервер. Розподілена атака типу «відмова в обслуговуванні» (DDoS), зазвичай здійснювана за допомогою безлічі «комп'ютерів-зомбі», може відрізати від зовнішнього світу навіть найстійкіший сервер, і єдиним ефективним захистом є використання кластера.

Є два варіанти організації DDoS атак:

- Створення ботнету, тобто зараження певного числа комп'ютерів програмами, що за командою атакуючого починають надсилати запити до атакованого сервера;
- Організація флешмобу, тобто заздалегідь встановлений час початку атаки між декількома користувачами інтернету;

Захист від DoS, DDoS-атак

Як правило, більшість DDoS-атак достатньо важко розрізнити, так як безглузді запити нічим не відрізняються від легальних. Помилка в ПЗ може бути завжди виправлено завжди, а ось з витрата ресурсів – постійна справа. З цим стикається багато адміністраторів, коли ширини пропускного каналу (ресурсів машини) стає недостатньо, або web-сайт піддається следшот-ефекту (але це властиво сайтам з поганим (безкоштовним) хостингом), тобто на сайт несподівано та одночасно заходить велика кількість людей, як правило, це відбувається після реклами інформаційними порталами з великою аудиторією. Зменшуючи трафік та ресурси для кожного користувача, втрачається значна кількість клієнтів, але при цьому web-сайт можливо врятувати.

Як такого алгоритму 100% захисту немає, однак наслідки DoS, DDoS-атак та їхня ефективність може бути знижена правильним налаштуванням маршрутизатора, брандмауера та постійним аналізом аномалії в мережовому трафіку.

Використання фільтрувальної мережі як один з методів захисту, який базується за прийманні трафіку на себе, його фільтрація, в результаті до цільового серверу доходить перевірений і якісний трафік від реальних

користувачів.

Отже, існує два типи DoS/DDoS-атак, і найпоширеніша з них заснована на ідеї флуда, тобто надсилання жертві великої кількості пакетів. Флуд буває різним: ICMP-флуд, SYN-флуд, UDP-флуд і HTTP-флуд. Більшість сучасних DoS-ботів використовують всі ці види атак одночасно, це варто враховувати при побудові системи захисту.

Основними видами захисту від цих атак є:

- фільтрація та блекхолінг;
- зворотній DDoS;
- виправлення вразливостей;
- нарощування ресурсів;
- розосередження;
- ухилення;
- використання спеціального ПО.

Використання превентивних заходів дозволить вам не опинитися в безвихідній ситуації під чат таких атак. Для цього слід використовувати наступні заходи:

- Кожен сервер, що має прямий доступ до зовнішньої мережі, повинен мати доступ до швидкої та простої віддаленої роботи. Як ефективний варіант, наявність другого, адміністративного, мережевого інтерфейсу, щоб мати змогу отримати доступ до серверу з вільного каналу;

- ПЗ, що використовується на сервері, має бути останньої версії та здатними до адекватної роботи. Всі дірки слід пропатчити, завантажити та встановити останні оновлення, це дає змогу захиститися від DoS-атак та багів у сервісах;

- Доступ до всіх слухаючих мережевих сервісів, що призначені для адміністративного користування, повинні буди приховані від осіб, для яких вони не призначені, брандмауером. Це не дає можливість використати їх для проведення DoS-атаки чи брутфорсу (взлом чогось шляхом перебирання великої кількості паролів, взятих зі словника).

- На найближчому маршрутизаторі повинна бути встановлена система аналізу трафіку, яка дозволила би своєчасно дістати інформації про атаку, що починається, що дає змогу виконати заходи з її запобігання;

- Варто зауважити, що превентивні заходи направлені лише на зниження ефективності від DDoS-атак, щ оставлять метою втрату ресурсів машини. Від флуду захиститися практично неможливо, єдиним правильним заходом захисту є позбавлення атаки сенсу. У разі наявності достатньо широкого каналу, який пропустить весь трафік, що призначений для атаки, сервер вважається практично захищеним. Є більш ефективний спосіб захисту, але й одночасно більш складний у виконанні, він полягає у розподіленні обчислювальної мережі, що включає велику кількість дублюючих серверів, які підключені до різних каналів. Це робиться для того, щоб у раз втрати обчислювальної або пропускної спроможності каналу, перенаправити клієнтів на інший сервер, або поступово розподілити навантаження між усіма серверами. Така система вважається найбільш захищеною та одночасно дуже дорогою.

Висновок

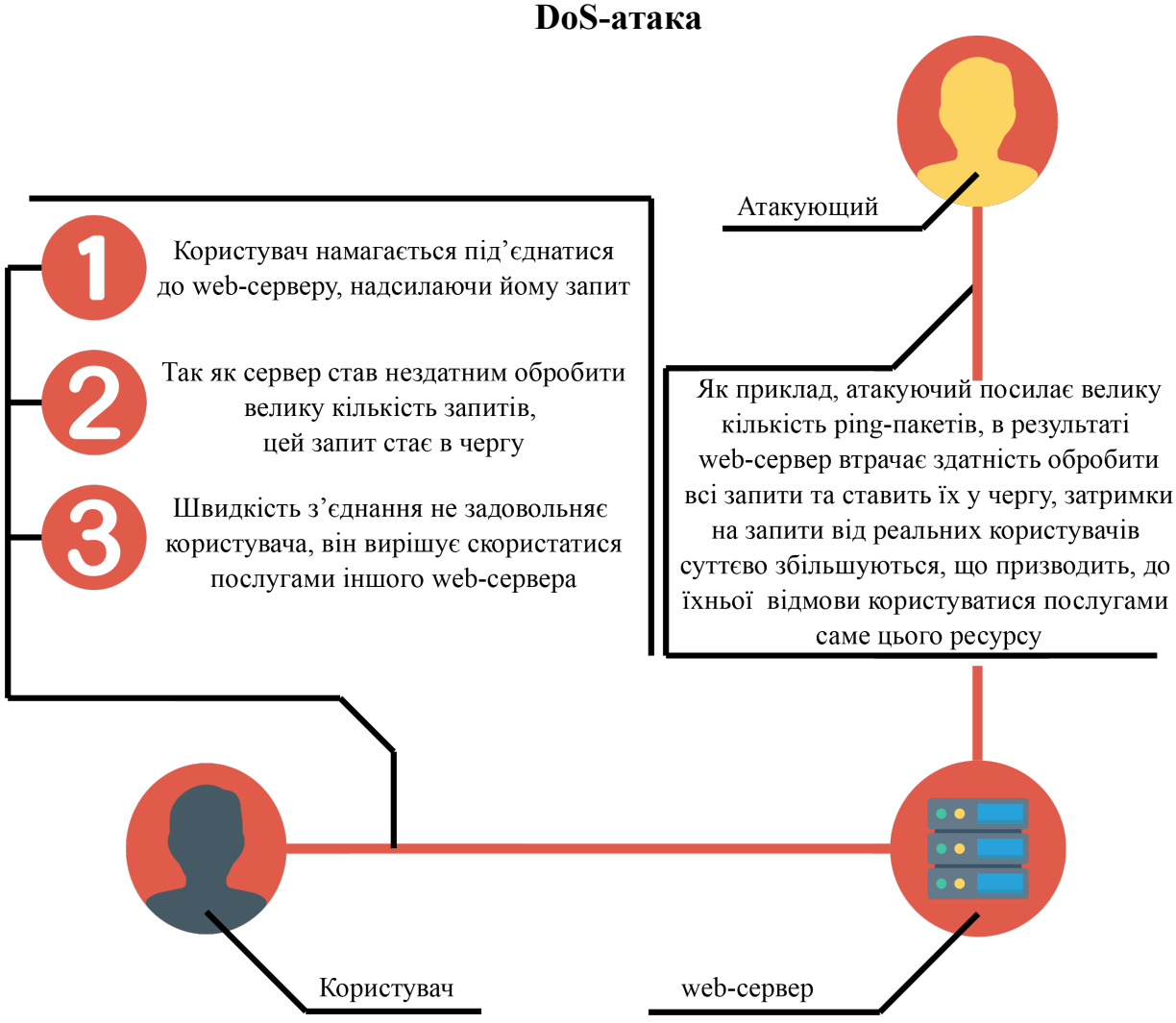
З інформатизацією суспільства з'являється все більше та більше можливостей завдати збитків тій, чи іншій організації. Багато коштів витрачається на усунення наслідків та ще більше витрачається на захист від проведених атак. У даній статті було розглянуто основні способи проведення DoS, DDoS-атак та шляхи захисту від них. Розглянута інформація буде корисна, як власникам сайтів, так і тим особам, які беруть участь у тому, щоб технічно забезпечити роботу цього сайту.

Джерела

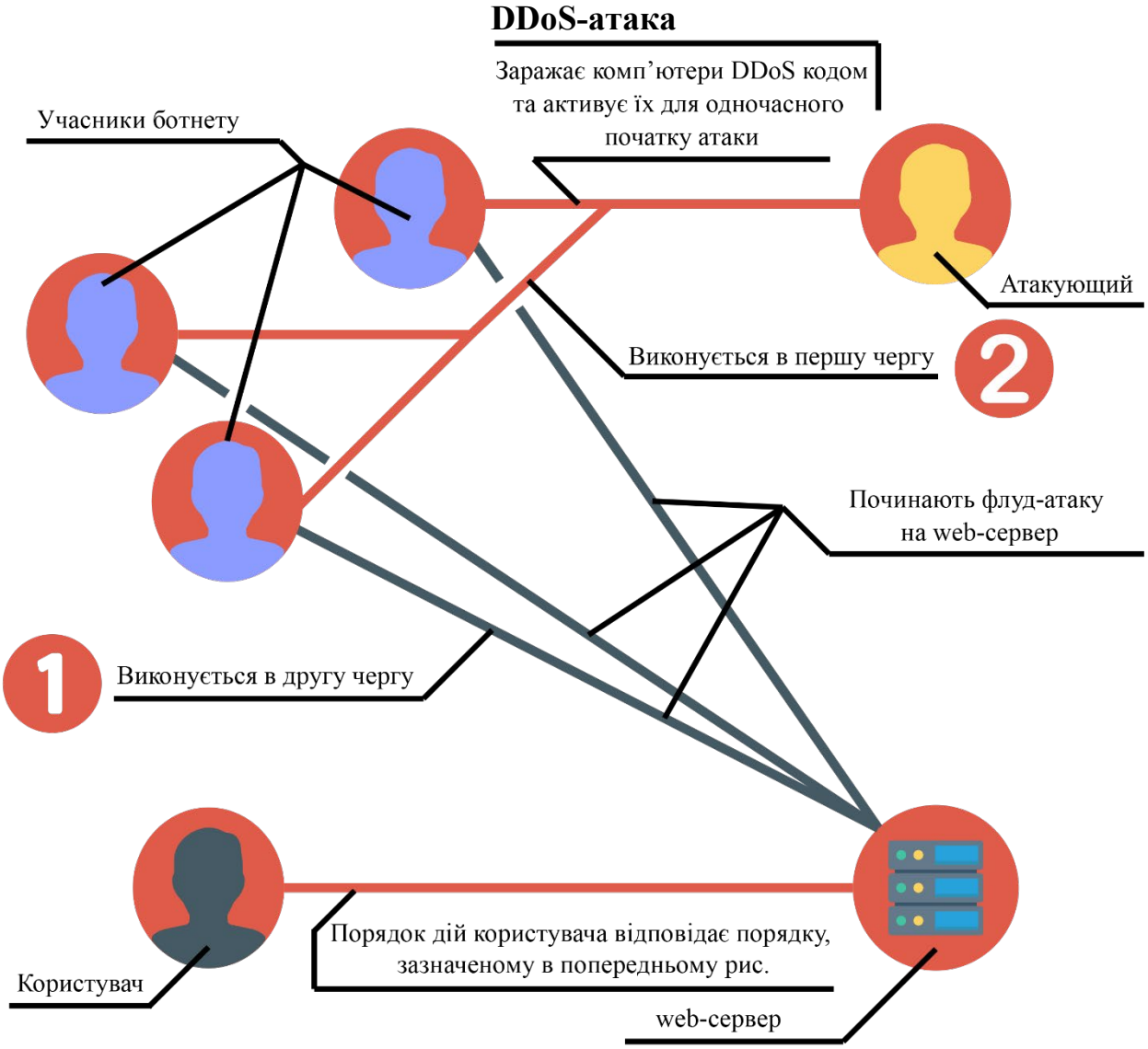
1. DoS-атака // uk.wikipedia.org URL: https://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0 (дата звернення: 23.03.2020).

2. Методи боротьби з Dos або DDos атаками // wiki.tntu.edu.ua URL: https://wiki.tntu.edu.ua/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8_%D0%B1%D0%BE%D1%80%D0%BE%D1%82%D1%8C%D0%B1%D0%B8_%D0%B7_Dos_%D0%B0%D0%B1%D0%BE_DDos_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0%D0%BC%D0%B8 (дата звернення: 23.03.2020).

Додаток 1



Мал 1.



мал 2.

Науковий керівник: Бондаренко А. П.
Стаття відправлена: 09.04.2020 г.