СПОСОБИ ЗАХИСТУ ВІД DDOS АТАК ЗАСОБАМИ BGP

Войтенко Є. Д., ст. (гр. КВ-81мн, ФПМ КПІ ім. Ігоря Сікорського)

Анотація: В даній роботі розглядаються різні методи захисту ресурсів від DDoS атак. Приведені плюси і мінуси, а також методи організації null routing, фільтрації каналу зі сторони провайдера та BGP Black hole.

Ключові слова: протокол граничного шлюзу,розподілена атака на відмову в обслуговуванні, метод повної фільтрації, метод «чорної діри», захист інформації.

Abstract: In this paper we consider different methods of protecting resources from DDoS attacks. Advantages and disadvantages, as well as methods of organization of null routing, channel filtering from the provider and BGP Black hole are presented.

Keywords: border gateway protocol, distributed denial of service attack, null routing method, «Black hole» method, information protection.

DDoS атака (від англ. Distributed Denial of Service, розподілена атака типу «відмова в обслуговуванні») – це хакерська атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, за яких потрібно викликати відмову в обслуговуванні великої компанії або урядової організації, в результаті чого вони не можуть отримати доступ до системних ресурсів (серверів), або цей доступ ускладнений.

Сьогодні DDoS-атаки найбільш популярні, так як дозволяють довести до відмови практично будь-яку систему, не залишаючи юридично значимих доказів. Кожен адміністратор публічного ресурсу хоч раз стикався з різноманітними DDoS атаками. Ціллю нападу можуть бути, як окремі ресурси розміщені на серверах, так і самі сервера чи увесь майданчик в цілому. За статистикою з кожним місяцем кількість, складність і потужність атак зростає. Боротися з такими атаками необхідно силами всієї команди хостингу. Мережеві адміністратори також повинні мати засоби боротьби з такими атаками на мережевому рівні.

На жаль, ще не винайшли універсального засобу захисту. Найбільш ефективним і часто вживаним є null routing (нульова маршрутизація) – повна фільтрація трафіку по IP-адресі, що піддається атаці [1]. Після того, як вузол піддався фільтрації, можна при відносно спокійних обставинах перенести ресурс на іншу IP-адресу чи навіть змінити DNS ім’я, або просто змиритися з тимчасовою недоступністю одного ресурсу, при цьому зберігти працездатність інших. Але, здавалося б такий простий спосіб фільтрації, зовсім не такий простий.

По-перше, більша частина маршрутизаторів з вбудованими допоміжними технологіями не витримують потоку навантаження, що утворюється в даному випадку.

По-друге, за умови відсутності безлімітного доступу, за завантаження гігабіт інформації доведеться сплатити чималу суму. І, по-третє, завантаження

фізичного каналу заважає нормальній роботі легітимних клієнтів, що теж не є добре [2].

Тут нам на допомогу приходить просте обмеження вже існуючого рішення. Ми повинні фільтрувати трафік якомога ближче до джерела, тобто, у кросоверного порту. Це робиться звичайним дзвінком у техпідтримку провайдера з проханням фільтрувати трафік на їхньому боці каналу.

Проте на такі дії йде багато часу, особливо при роботі з декількома провайдерами. Крім того, цей метод повністю залежить від роботи людини, тобто не є автоматизованим чи динамічним [3].

У гонитві за автоматизованістю процесу ми повертаємося до необхідності використання динамічної маршрутизації. Тому розглянемо модифікацію null routing – BGP Black hole («чорної діри»), що описується в RFC 3882. Він дозволяє повністю припинити потік трафіку на сервер, що піддається атаці, та зняти навантаження з каналів автономної системи та провайдера.

Як випливає з назви, для роботи методу необхідно BGP-сусідство з провайдером. І звісно він вимагає невеликої додаткової конфігурації з обох сторін. Технічно це виглядає як BGP-анонс префікса/32 позначеного спеціальною групою [4].

У класичній схемі метод передбачає виставлення next-hop для анонсованого маршруту на IP-адресу з приватної мережі. Оскільки у магістральних провайдерів маршрути до приватних мереж, здебільшого, мають бути спрямовані в Null0 за термінологією Cisco, в Juniper – discard, пакети з адресою призначення цієї мережі буду автоматично відкидатися – потрапляти в «чорну діру» ще в мережі провайдера.

На жаль, в реальних мережах магістральних провайдерів не завжди встановлені маршрути приватних мереж в Null0, бо самі провайдери використовують ці адреси для маршрутизації або просто не дотримуються рекомендацій робочої пропозиції.

Для встановлення «чорної діри», найчастіше, використовуються розширені можливості управління маршрутами BGP – BGP community. Метод реалізується шляхом створення спеціальної групи (community) для маршрутів, трафік яких необхідно направити в «чорну діру». В момент початку атаки у мережевого адміністратора автономної системи, що атакується, буде можливість передати маршрут з довжиною маски /32 підкріпивши його цим community, тим самим повідомивши маршрутизаторам провайдера про те, що пакети до цієї IP-адреси повинні відкидатися.

Фільтрація пакетів на стороні провайдера може здійснюватися як за допомогою ACL, так і за допомогою Null інтерфейсу, але найбільш правильний підхід передбачає рекурсивну «чорну діру».

Висновки. Є кілька універсальних порад, які допоможуть підготувати систему до DDoS-атаки:

– всі сервери, які мають доступ у зовнішню мережу, повинні бути підготовлені до віддаленого аварійного перезавантаження, є бажаною наявність

другого мережевого інтерфейсу, через який по ssh-з'єднанню можна швидко отримати доступ до сервера;

– програмне забезпечення, яке встановлено на сервері, має бути останньої модифікації задля безпеки системи;

– всі мережеві сервіси повинні бути захищені брандмауером.

Атрибут BGP community широко використовується магістральними провайдерами для класифікації трафіку та оперативного управління. Багато провайдерів надають цілий набір community, які дозволяють не тільки відправляти певні адреси в blackhole, але і управляти трафіком, що надходить в їх автономні системи, тобто ще на каналах провайдера.

Аналіз community провайдерів дозволяє адміністратору розробити схему боротьби з DDoS атаками, а іноді й автоматизувати процес ліквідації атак [5].

В умовах надання послуг віртуального хостингу високої доступності цей метод є крайнім заходом, але залишається ефективним засобом для боротьби з великими DDoS атаками, коли іншими засобами впоратися не вдається.

Науковий керівник: Землянська О. В., ст. викл. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Література

1. Parkhurst W. R. Cisco BGP-4 Command and Configuration Handbook / William R. Parkhurst. – Indianapolis: Cisco Press, 2001. – 401 с.

2. Мак-Ферсон Д. Принципи маршрутизації та основні способи захисту в Internet / Д. Мак-Ферсон, С. Хелеби. – Торонто: Вильямс, 2001. – 448 с.

3. McPherson D. Practical BGP / D. McPherson, S. Sangli, R. White. – Boston: Addison-Wesley Professional, 2005. – 434 с.

4. Семенюк О. BGP протокол (перевод на русский) [Електронний ресурс] / Олег Семенюк. – 1996. – Режим доступу до ресурсу: https://www.opennet.ru/docs/RUS/bgp_rus/.

5. A Border Gateway Protocol (BGP) [Електронний ресурс]. – 1989. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc1105.