УДК 004.056:004.052

К. Р. Салієва

ОСОБЛИВОСТІ ЗАХИСТУ СЕРВЕРІВ, МЕРЕЖ ТА ОКРЕМИХ ЧАСТИН МЕРЕЖІ ВІД АТАКИ ТИПУ DDOS

Вінницький національний технічний університет

Анотація

Розглянуто небезпеку DDoS-атак, які загрожують нормальному функціонуванню серверів, мереж та її частин. Запропоновано методи боротьби, порядок дій при DDoS-атаках та розроблено пропозиції для запобігання подальших атак.

Ключові слова: DDoS-атака, захист, небезпека, сервери, мережі.

Annotation

The danger of DDoS-attacks that threaten the normal functioning of servers, networks and its parts is considered. Methods of struggle, the order of actions at DDoS-attacks are offered and offers for prevention of the further attacks are developed.

Keywords: *DDoS-attack, protection, danger, servers, networks.*

Вступ

На сьогоднішній день людство досягло великого прогресу у сфері технологій, яка має великий вплив на всі види діяльності, де є накопичення та оброблення даних. Кожного дня відбувається певна маніпуляція в базах даних та в інших ресурсах в мережі Інтернет. Для кожної організації важливо зберігати цілісність та, іноді, секретність своєї інформації, адже від неї залежить майбутнє стабільної роботи. Найчастіше за все даний об’єкт стає ціллю для недобросовісних користувачів – «хакерів», які направляють DDoS-атаки на жертву, щоб пошкодити або зруйнувати нормальне функціонування сайтів, мереж та її частинам задля своєї вигоди. Через такі атаки система зводиться до стану, коли вона неправильно виконує поставленні функції або не може обслуговувати інших користувачів.

Метою роботи є огляд небезпеки DDoS-атак та розроблення методу боротьби, порядок дій при небезпеці та наведено декілька універсальних порад для запобіганню подальших атак.

Результати дослідження

Distributed Denial of Service або DDoS-атака дослівно перекладається, як «розподілена відмова в обслуговуванні» або, іншими словами, це такий вид атаки, при якій «хакери» направляють, наприклад на сайт вірусний трафік для того, щоб вивести його з робочого режиму. Ціллю цієї атаки може бути як блокування проекту конкурента або популярний ресурс, так і отримання повноцінного контролю над всіма системами. Відомо три способи, щоб вивести з ладу сайт чи мережу: пропускна здатність, ресурси, використання програмних слабостей [1].

За ключовою характеристикою розрізняють такі атаки DDoS, які впливають на різні моделі взаємодії відкритих мережних систем (OSI). Перевантаження проводяться найчастіше на мережевому (Lvl. 3), транспортному (Lvl. 4), презентаційному (Lvl. 6) та прикладному (Lvl. 7) рівнях протоколів [2]. Найрозповсюджені види атак DDoS на сьогоднішній день: UPD flood, TCP flood, TCP SYN flood, Smurf-атаки, TFN та TFN2K атаки.

Після DDoS-атаки залишаються наслідки, які можуть бути руйнівними як для бізнесу, так і для інфраструктури. Атака, яка була проведено успішно, може завдати великої матеріальної шкоди організації або компанії-власнику ресурсу. До цього відноситься також втрата іміджу або поява незадоволених користувачів та клієнтів. Щоб не стати жертвою DDoS-атаки та захиститися від неї, потрібно вибудувати досить серйозний комплекс заходів. Заходи протидії можна поділити на превентивні та реакційні, пасивні

та активні. Якщо сайт піддається набагато сильнішим атакам і вони відбуваються значно частіше, то цього буде недостатньо. Тому потрібно використати такі рівні захисту [3]:

1. Доступ до сервера – віддалений ребут, при якому консоль виводиться по протоколу SSH на іншу IP-адресу, щоб була можливість скористатися нею при перевантаженому сервері.
2. ПО сервера – ретельна перевірка на предмет безпеки, щоб усі відомі «дірки» були ретельно закриті.
3. Мережа – блокування всього на стадії старту та маскування IP-адреси.
4. Провайдер – аналіз пакетів одержуваних даних і блокування IP-адрес.
5. Спеціалізоване обладнання – апаратні засоби для протистояння мережевим атакам та пропонування комплексні рішення для захисту.
6. Адміністрація сервера – використовують способи аналізу логів фаєрвола, які дозволяють вичислити IP-адреси тих машин, з яких здійснюється атака.

Якщо все-таки почалася DDoS-атака, то потрібно перш за все не панікувати, а поступово протидіяти їй. Перед початком атаки боти тільки починають «розігріватися», тому головне зловити момент і почати активні дії. У цьому допоможе постійне спостереження за маршрутизатором, підключеним до зовнішньої мережі. На сервері-жертви можна визначити початок атаки підручними засобами, але однозначно ідентифікувати DDoS-атаку складно, можна лише підтвердити свої припущення, дослідивши, чи не повторюється одна адреса декілька разів. Це дасть деякий час, щоб звернутися з проблемою до провайдера/хостеру. Є вірогідність того, що можуть не відповісти на прохання, але з серйозними атаками наодинці не впоратися.

Повністю захиститися від DDoS-атаки неможливо, але можна значно знизити її рівень ефективності. Такий алгоритм дій унеможливить постійні атаки та дасть можливість захистити об’єкт уваги хакера.

Висновки

Атаки типу DDoS довгий час тероризують сайти, мережі та їх частини. Вони технічно не вимагають серйозної підготовки, але дають руйнівний ефект для корпорацій та інтернет-структур. Кожного дня IT-ресурси страждають від DDoS-атак, які призводять до серйозних втрат та погіршення їх репутації, а хакери на цьому мають великі гроші та вигоду. Запобігти частому та серйозному впливу на об’єкт атаки можливо, але стовідсоткову гарантію не дасть будь-який досвідчений спеціаліст. Головне – це вчасне ліквідування загрози на початковій стадії та якнайкраще захистити важливу інформацію від нападу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Принцип защиты от DDoS (что такое защита от DDoS?) [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://introserv.eu/ru/info/antiddos-attack-france.
2. DDoS атаки і захист від них [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.ukraine.com.ua/uk/blog/hosting_ukraine/ddos-ataki-i-zashchita-ot-nih.html.
3. Захист сайтів від DDoS-атак [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: http://andrey.lviv.ua/blog/zahust-vid-ddos-atak.

Салієва Катерина Рустамівна - студентка групи КІТС-18б, факультет менеджменту інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: kate228778@gmail.com

Науковий керівник: ***Ткачук Людмила Миколаївна*** – к.е.н., доц. каф. МБІС, заст. декана Факультету менеджменту та інформаційної безпеки з навчально-методичної роботи Вінницького національного технічного університету, м. Вінниця, e-mail: ludatkachuk2017@gmail.com

Kateryna Salieva - student of the KITS-18b group, Faculty of Management Information Security, Vinnitsa National Technical University, Vinnitsa, email: kate228778@gmail.com

Supervisor: ***Lyudmila Tkachuk*** – PhD (Ec), Assistant Professor, Deputy dean of the Faculty of management and information security by educational work of Vinnytsia National Technical University, Vinnitsa, email : ludatkachuk2017@gmail.com.