УДК 004.056:004.052

Курінний Н.О

ЗАХИСТ СЕРВЕРІВ ВІД АТАКИ ТИПУ DDOS

Вінницький національний технічний університет

Анотація

Розглянуто небезпеку DDoS-атак, які загрожують функціонуванню серверів. Запропоновано методи захисту, порядок виконання дій при DDoS-атаках та розроблено пропозиції для уникнення подальших атак.

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

Annotation

The danger of DDoS-attacks, which threatens the functioning of servers, is considered. Methods of protection, the order of actions at DDoS-attacks are offered and offers for unification of the further attacks are developed.

Вступ

На даний момент майже кожна людина в світі має доступ до комп’ютера та мережі Інтернету, який має достатньо вагомий вплив на всі види людської та промислової діяльності, особливо на ті, в яких є наявні оброблення та накопичення даних. Кожній компанії хочеться захистити та зберегти інформацію, файли та інше, адже саме цілісність інформації забезпечує продуктивну та стабільну роботу. Саме на таку інформацію найчастіше направляють свої DDoS-атаки – «хакери», вони намагаються пошкодити або навіть зруйнувати стабільність функціонування серверів компанії. Дані атаки впливають на систему, яка обслуговує сервери, так щоб під час атаки система не могла виконувати поставленні функції або, якщо це фірма по співпраці з клієнтами то не буде змоги обслуговувати клієнтів.

Метою роботи є огляд небезпеки DDoS-атак для запобігання їх, розробка методів захисту, порядок виконання дій при захисті серверів.

Результати дослідження

Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. *DoS attack, DDoS attack, (Distributed) Denial-of-service attack*) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого сервера великою кількістю зовнішніх запитів (часто безглуздих або неправильно сформульованих), таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Взагалі відмова сервісу здійснюється:

- примусом атакованого устаткування до зупинки роботи програмного забезпечення/устаткування або до витрат наявних ресурсів, внаслідок чого устаткування не може продовжувати роботу;
- заняттям комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість сполучення перестає відповідати вимогам.[1]

Є три способи, щоб вивести з ладу сайт чи мережу: пропускна здатність, ресурси, використання програмних слабкостей.

Перша «D» в DDoS означає «distributed», розподілена атака типу «відмова в обслуговуванні». У цьому випадку мова йде про величезну масу зловмисних запитів, що надходять на сервер жертви з різних місць. Зазвичай такі атаки організовуються за допомогою бот-мереж.

Основними концепціями кібербезпеки є доступність, цілісність і конфіденційність. Атаки «відмова в обслуговуванні» (DoS) впливають на доступність інформаційних ресурсів. Відмова в обслуговуванні вважається успішним, якщо він призвів до недоступності

інформаційного ресурсу. Успішність атаки і вплив на цільові ресурси відрізняються тим, що вплив завдає жертві шкоди. Наприклад, якщо атакується інтернет-магазин, то тривала відмова в обслуговуванні може заподіяти фінансові збитки компанії. У кожному конкретному випадку DoS-активність може або безпосередньо заподіяти шкоду, або створити загрозу і потенційний ризик нанесення збитків [2].

Даний вид атак має деякі ключові характеристики, які впливають на різні сервери. Перевантаження найчастіше проводиться на мережевому, прикладному та транспортному рівнях протоколів.

Хоча атака можлива на будь-якому з рівнів, особливою популярністю користуються атаки на 3-4 і 7 рівнях моделі OSI.

DDoS-атаки на 3-му і 4-му рівні - інфраструктурні атаки - типи атак, засновані на використанні великого обсягу, потужного потоку даних (флуд) на рівні інфраструктури мережі і транспортному рівні, з метою уповільнити роботу веб-сервера, «заповнити» канал , і в кінці перешкодити доступу інших користувачів до ресурсу. Ці типи атак як правило включають ICMP-, SYN- і UDP-флуд.

DDoS атака на 7-му рівні - атака, яка полягає в перевантаженні деяких специфічних елементів інфраструктури сервера додатків. Атаки 7-го рівня особливо складні, приховані і важкі для виявлення в силу їхньої подібності з корисним веб-трафіком. Навіть найпростіші атаки 7-го рівня, наприклад, спроба входу в систему під довільним ім'ям користувача і паролем або повторюваний довільний пошук на динамічних веб-сторінках, можуть критично завантажити CPU і бази даних. Також DDoS зловмисники можуть неодноразово змінювати сигнатури атак 7-го рівня, роблячи їх ще більш складними для розпізнавання і усунення [3].

Висновок

Атаки типу DDos протягом довгого часу були серйозною загрозою для сайтів, мереж та серверів. Для їх виконання не потрібно масової підготовки та серйозної спецтехніки, але в свою чергу наносять серйозні пошкодження для серверів компанії. Дані атаки постійно приносять проблеми компаніям та шкодят їхній репутації, що, в свою чергу, різко знижує попит на продукцію даної організації, на чому й заробляють хакери. Запобігти цим атакам можливо, але стовідсоткової гарантії немає. Якщо спеціаліст зробив спробу, то її потрібно реалізувати ще на початкових стадіях, поки загроза не розповсюдилась на серверах компанії. Тому, насамперед, при захисті потрібно захищати найціннішу інформацію на серверах.

Список використаної літератури

1.DoS-атака [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/DoS.

2. The Crossfire Attack. // IEEE Symposium on Security and Privacy. – 2013. – С. 127– 142.

3. "DDoS, Machine Learning, Measures". // "Understanding Denial-of-Service Attacks". / , 2016. – (Taylor & Francis Group). – (ISBN:13: 978-1-4987-2965-9). – С. 12–34.

Курінний Назарій Олександрович – студент групи КІТС – 19б, факультету менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: nazarkyrinnoy16@gmail.com

Науковий керівник: **Шелепало Галина Василівна** – кандидат фізико-математичних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail hv.shelepalo@vntu.edu.

Kurinny Nazariy Oleksandrovych - student of KITS group - 19b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: nazarkyrinnoy16@gmail.com

Supervisor: **Shelepalo Halyna Vasylivna** - Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail hv.shelepalo@vntu.edu.ua