Ключові слова: база даних, інформаційна система, безпека.

Ключевые слова: база данных, информационная система, безопасность.

Keywords: data base, information system, security.

Науковий керівник: *к.т.н., доц. Кухаренко С.В.*

Кравченко Іван Сергійович

Національний університет «Одеська юридична академія»,

студент 3 курсу факультету кібербезпеки та інформаційних технологій

МЕТОДИ ЗАХИСТУ ВІД DDOS-АТАК

Мета атаки DDoS (Distributed Denial of Service) – домогтися відмови в обслуговуванні пристроїв які спроможні з’єднуватись з Інтернетом: обладнання мережевого контролю, різних Інтернет-магазинів, веб-сайтів та веб-додатків, інфраструктури Інтернету речей. Найбільша кількість атак у мережі розгортаються наступними кроками:

1) збір даних про цільовий об’єкт та їх аналіз з метою виявлення найбільш видимих та уразливих недоліків системи, вибір способу атаки;

2) націлюватися до атак шляхом підготовки зловмисного коду на комп'ютерах і всіх підключених до мережі Інтернет пристроях, які були перехоплені та встановлені під контроль зловмисника;

3) створення багаточисельних запитів з більшості підконтрольних пристроїв;

4) підведення підсумків атаки.

Якщо бажаний результат не був виконаний, в багатьох випадках буде проведений повторний та більш якісний аналіз, і знову повторення першого кроку.

При умовах успішної атаки на WEB-додаток, або базу даних, цільовий

ресурс буде демонструвати суттєве зниження продуктивності, або зовсім втратить можливість обробляти різні типи запитів від користувачів та серверу. Наслідками цього може бути довгі зависання ресурсу, звичайні користувачі не можуть скористатися цим ресурсом, додатком, або базою даних у потрібний для них момент. Це стає через неможливість доступу до Інтернету, та некоректно працювати. Наміри зловмисників бувають дуже різноманітними. Частіше це є недобросовісна конкуренція, або замовлення колишнього бізнес партнеру, також це може шантаж, конфлікт інтересів, поглядів, особисті переконання. Один з варіантів цих дій може бути переконання у навичках злому, так зване тренування. Також доволі часто недоброчесні програмісти використовують це з метою додаткового заробітку [1].

Для захисту крім технічних рішень, потрібно зробити дії з налаштуваннями проти DDoS-атак. Першим способом є зведення до мінімуму розміру зони яка може бути атакована. Потрібно переконатися що доступ до портів, додатків, протоколів, який не передбачений, є закритим. Основними елементами нейтралізації DDoS-атак є такі терміни як пропускна можливість і продуктивність серверу, яка достатня для поглинання атаки, правильного налаштування маршрутизатора та брандмауера. Також постійний аналіз аномалій в мережевому трафіку, і кожен раз коли є велике збільшення трафіку, при звертанні до хосту, можна використовувати максимально можливий обсяг трафіку, який хост може обробити без втрати доступності. Більш новітні методи захисту з новими можливостями дозволяють встановлювати обмеження на вхідний трафік. Для цього і подібних до цього засобів потрібно швидкі можливості Інтернету.

Проти атак, які дозволяють зловмиснику використовувати вразливість у ресурсі, наприклад проти впровадження SQL-коду чи злоякісного втручання до запиту, рекомендується використовувати Web Application Firewall. Через несхожість атак, треба самостійно нейтралізувати заборонені запити до баз даних, WEB-сервісів або інших додатків, які можуть надходити від підозрілих IP-адресів, з інших географічних регіонів [2].

Список використаних джерел:

1. Distributed Denial of Service. URL: https://stormwall.pro/knowledge-base/termin/ddos-protection

2. DDoS-атаки/ URL: https://aws.amazon. com/ru/shield/ddos-attack-protection/

Ключові слова: DDoS-атаки, ресурси, мережевий контроль, трафік, аналіз, злом, несанкціонований доступ.

Ключевые слова: DDoS-атаки, ресурсы, сетевой контроль, трафик, анализ, взлом, несанкционированный доступ.

Keywords: DDoS-attack, resource, network control, analysis, traffic, hack, unauthorized access.

Табала Ксенія Андріївна

Національний університет «Одеська юридична академія»,

студентка 2-го курсу факультету кібербезпеки та інформаційних технологій

ЦИФРОВІ ВІДБИТКИ ВЕБ-БРАУЗЕРІВ

Фінгерпрінтинг - це унікальний ідентифікатор, який створюється з застосуванням технології створення цифрового «відбитка» пристрою комунікації користувача. Ця технологія базується на аналізі інформації, яку веб-браузер відправляє на Інтернет-ресурси, якій користувач відвідує.

На основі декількох типів даних, які можна отримати завдяки запитуючому Інтернет-ресурсу, а саме: мовних налаштувань, встановлених шрифтів, часовому поясу, версії веб-браузера та його плагинів тощо - створюється унікальний «цифровий відбиток» веб-браузера. Завдяки використанню фінгерпрінтингу існує можливість розпізнати окремого користувача за створеним цифровим відбитком. Аналізуючи поведінку користувача веб-браузера в Інтернеті,