необхідно змінити тривіальні сигнатури, забезпечивши їх додатковими перевірками і зробивши більш точними. Ми рекомендуємо використовувати ці регулярні вирази в якості відправної точки при налаштуванні будь-якої системи виявлення вторгнень.

Список використаних джерел:

1. Cyber Attacks 2020! : URL: https://sectigostore.com/blog/cyber-attacks-2020-notable-2020-cyber-attacks/
2. Корнага Я., Базака Ю., Мар'єнко Є. Способи оптимізації SQL–запитів для поліпшення роботи з базою даних в високонавантажених системах. *Адаптивні системи автоматичного управління.* Київ, 2020. Том 2 № 37. С.26-30.

Науковий керівник: доцент Лобода Ю.Г.

ЗАСОБИ ТА МЕХАНІЗМИ ПРОТИДІЇ DDOS-АТАКАМ

Величко С.В.

студентка 1 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

DDoS-атака або атака типу «відмова в обслуговуванні» (Distributed Denial of Service) спрямована на комп'ютерну систему з метою створення несприятливих умов для використання певних ресурсів або сервісів користувачами [1]. Класифікація атак відповідає базовій еталонній моделі взаємодії відкритих систем OSI [2]. На найнижчому мережевому (третьому) рівні для атаки відбуваються дії з використанням UDP-пакетів. Ідея атаки полягає у надсиланні безлічі UDP-пакетів (як правило, великого об'єму) на обрані або випадкові номери портів віддаленої комп'ютерної системи. При цьому для кожного отриманого пакета віддалена система повинна визначити відповідний додаток, переконатися у відсутності його активності та відправити відповідне повідомлення по протоколу ICMP «адресат недоступний». В результаті атакований хост виявиться перенавантаженим: у протоколі UDP механізм запобігання перенавантаженням відсутній, тому після початку атаки шкідливий трафік швидко захопить всю доступну смугу пропускання каналу хоста, перешкоджаючи при цьому трафіку від звичайного користувача.

На транспортному (четвертому) рівні атака полягає у відправці завеликої кількості SYN (*synchronize*) - запитів на встановлення підключень за протоколом TCP. При цьому зворотні пакети від обчислювальної системи з комбінацією флагів SYN+ACK (*acknowledges*) або ігноруються, або обробляються навмисно не вірно. Таким чином у системі створюється велика кількість напіввідкритих з'єднань збільшуючи при цьому чергу на підключення.

На рівні представлення даних (шостому рівні моделі взаємодії OSI) атака полягає у зловмисному використанні протоколу SSL. Для розшифрування даних

переданих по протоколу SSL необхідно витратити певну кількість ресурсів обчислювальній системі. Найчастіше механізм атаки полягає у хижацькому використанні механізму рукостискання SSL (коли на запит з'єднання надається новий запит і так далі), відправлення сміттєвих даних на сервер SSL або порушення певних функцій, пов'язаних із процесом узгодження ключа шифрування SSL.

На прикладному (сьомому) рівні атака відбувається через надсилання великої кількості HTTP(S) POST або GET запитів. На цьому ж рівні виконується атака на DNS-структуру шляхом надсилання порожніх запитів, або запитів на декілька DNS-серверів одночасно із зміненою адресою відправника на адресу об'єкта атаки.

Протидія DDoS атакам

Методи протидії DDoS-атакам можна розділити на пасивні та активні, а також на превентивні та реакційні. Перш за все необхідно відзначити профілактичні заходи щодо попередження DDoS-атак. Зрозуміло, що цей метод є управлінським, тим не менш аналіз можливих причин імовірних DDoS-атак є першим кроком до зменшення їх руйнівних наслідків. До управлінських методів варто віднести DDoS-атаку у відповідь.

Наступні методи полягають у використанні фільтрації за списками ACL (Access Control List) та використання мережевих екранів. Такі дії дозволяють загасити атаки або навіть їх припинити. Під час атаки деякий ефект можна отримати перенаправивши трафік на атакуючі комп'ютерні системи. Такий метод не буде мати ефекту якщо для атаки використовують заражені комп'ютерні системи (ботнет).

Для протидії DDoS-атакам на сьомому рівні моделі OSI компанія Cloudflare (https://www.cloudflare.com/) пропонує послуги з пом'якшення шкідливих дій. Служби Cloudflare працюють в якості посередника між відвідувачем вебсервісу та хостинг-провайдером Cloudflare, який, при цьому, виконує роль зворотного проксі. Для клієнтів компанія Cloudflare пропонує режим «Under Attack». Cloudflare стверджує, що це може пом'якшити розширені DDoS атаки 7-го рівня, представивши для цього обчислювальну задачу JavaScript, яку необхідно завершити браузером користувача, перш ніж користувач зможе отримати доступ до вебсайту. Окрім того, Cloudflare пропонує безкоштовну авторизовану систему доменних імен (DNS) для всіх клієнтів [3].

Не менш діючим є механізм оновлення системного та прикладного програмного забезпечення з можливістю повернення до попередньої версії. Варто розглянути в якості прикладного та системного програмного забезпечення вільне та відкрите програмне забезпечення [4], адже виявлення та виправлення недоліків серед цього класу програмного забезпечення проходить достатню кількість перевірок фахівцями різного рівня та спеціалізацій.

Сучасні захисні рішення забезпечують моніторинг трафіку, його фільтрацію, сприяють виявленню мережевих DDoS-атак різного типу. Вони блокують шкідливі пакети у трафіку, не перешкоджаючи доступу реальних користувачів, відстежують наявність аномалій, а у разі їх виявлення інформують хостера про можливу DDoS-атаку. Використання такого програмно-апаратного комплексу дозволяє підтримувати якість послуг, безперервність бізнес-процесів, а також знизити ризики для клієнтів.

Особливо ефективні є системи розподіленого захисту. Відповідне обладнання встановлюється у магістральних операторів, і якщо аналізатор атак фіксує напад на хост, або сервер, що захищається, він моментально транслює адреси атакуючих хостів іншим вузлам по всій мережі, і мережа починає працювати проти атакуючих хостів. Подібна система здатна відбити DDoS-атаки великої потужності.

Найбільш високопродуктивним і ефективним вважається застосування апаратних систем розподіленого захисту [5]. На приклад A10 Networks Thunder Threat Protection System володіє такими характеристиками як: автоматичний розрахунок фільтрів блокування та аналіз без попереднього налаштування або ручного втручання з подальшим блокуванням аномальної поведінки; 5-рівнева адаптивна ескалація політики, захист на основі машинного навчання; інтелектуальне виявлення сервісів з автоматичним призначенням політики пом'якшення наслідків; захист застосунків від DDoS-атак, що не вимагає спеціальної підготовки для застосунків і серверів; понад чотири десятки джерел інформації про загрози безпеки для миттєвого розпізнавання і блокування шкідливого трафіку.

Результатом використання сервісів захисту від DDoS-атак буде своєчасне виявлення та запобігання DDoS-атак, безперервність функціонування сайту та його постійна доступність для користувачів, мінімізація фінансових та репутаційних втрат від простоїв сайту чи порталу.

Список використаних джерел:

1. Захаров М. Як компаніям захиститися від DDoS-атак: пояснюють кіберексперти. З технічного боку. URL: https://cutt.ly/QHdBV0J
2. What is a DDoS Attack?. AWS. : URL: https://aws.amazon.com/shield/ddos-attack-protection/?nc1=h_ls.
3. Cloudflare DNS. *CLOUDFARE*. URL: https://www.cloudflare.com/dns/
4. Вільне та відкрите програмне забезпечення. URL: https://cutt.ly/uHdKnu4
5. A10 THUNDER TPS. URL: https://iitd.com.ua/tag/zashchita-ot-ddos-atak/

Науковий керівник: доцент Задерейко О.В.