Література:

1. Офіційний сайт Державного департаменту інтелектуальної власності МОН України. [Електронний ресурс]. - Режим доступу: www.sdip.gov.ua
2. Сіренко І. Юридична природа прав на об’єкти інтелектуальної власності // Українське право. - 2007. - С. 132-135
3. Беззуб І. Національна стратегія розвитку сфери інтелектуальної власності: оцінки експертів [Електронний ресурс]. - Режим доступу:https://uba.ua/documents/ip-strategy28082014.pdf
4. Капіца Ю. Розвиток права інтелектуальної власності в Європейському Союзі// Вісник Київського національного університету імені Тараса Шевченка. - 2006. - №33-34. - с. 45-48.

Дослідження атак на відмову в обслуговуванні інформаційно-телекомунікаційних систем

Світличний В.А.
кандидат технічних наук
доцент кафедри кібербезпеки
Харківського національного університету внутрішніх справ

Основною особливістю будь-розподіленої системи є те, що її компоненти розподілені в просторі і зв'язок між ними фізичним і програмним способами, за допомогою мережевих з'єднань і певного механізму повідомлень відповідно. Для того щоб захиститися від атак, необхідно їх вивчати і класифікувати, в зв'язку з цим не припиняються спроби, вивчити уразливості і запобігати їм. Існує безліч типів атак, але найбільше поширена і ефективна – Атака на відмову в обслуговуванні (англ. Denial-of-Service attack – DoS attack). Якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою (англ. Distributed Denial-of-Service – DDoS).). У розподіленій атаці на відмову одночасно можуть брати участь від кількох одиниць до кількох сотень тисяч, а іноді - кількох мільйонів хостів

Таким чином DDoS, це різновид втручання в роботу інформаційно-телекомунікаційної системи (ІТС), який у випадку успішної реалізації призводить до повної або часткової нездатності ІТС виконувати свої функції, тобто надавати декларовані послуги. Як правило, це проявляється у блокуванні доступу користувачів до сервісу, який надається системою, що була піддана атаці. Також зловмисники можуть скористатися нездатністю атакованої ІТС виконувати частину своїх функцій для реалізації іншої атаки (наприклад, скориставшись блокуванням певних функцій захисної системи, завантажити шкідливий програмний код).

Атаки DDoS зазвичай здійснюються з наміром зробити недоступними ресурси атакованої системи для легітимних користувачів. Прогнозованим наслідком такої атаки може бути неможливість здійснення розрахунків через Інтернет, втрата іміджу власника атакованого ресурсу або власника хостингу атакованого ресурсу, підміна заблокованого ресурсу іншим («підробленим») тощо. Крім того, метою атаки на відмову можуть бути й інші проблеми функціонування атакованої системи. Наприклад, надмірне перевантаження ресурсів певної системи може призвести до відключення її міжмережевого екрану та зробити можливою іншу атаку на цю систему (наприклад, завантаження шкідливого програмного коду тощо), або атаку на другу систему, яка при нормальному функціонуванні першої атакованої системи була недосяжною для зловмисників.

За локалізацією реалізації атаки на відмову поділяються на: локальні та віддалені. Локальні атаки (або атаки на стороні клієнта) реалізуються безпосередньо на атакованому хості. До них відносяться різні експлойти: форк-бомби і програми, що відкривають по мільйону файлів або запускають якийсь циклічний алгоритм, який перевантажує пам’ять та процесорні ресурси. Для локальної атаки на відмову необхідно мати або якимось чином отримати доступ до атакованої машини на рівні, що буде достатнім для захоплення ресурсів. Доступ можна отримати, зокрема, використовуючи вразливості програмного забезпечення атакованої системи, методи «соціальної інженерії» тощо.

Віддалені атаки на відмову реалізуються ззовні відносно атакованого хоста або атакованої мережі. В залежності від шляхів реалізації в свою чергу вони поділяються на два види: віддалена експлуатація уразливостей програмного забезпечення атакованої системи та перевантаження атакованої системи з метою вичерпання усіх наявних у атакованої системи ресурсів.

Віддалена експлуатація уразливостей програмного забезпечення представляє собою використання помилок, недоробок чи інших слабкостей у програмному забезпеченні атакованої системи з метою довести його до неробочого стану. Реалізується частіш за все шляхом пересилки

спеціально сформованих шкідливих пакетів. Прикладом такої атаки може слугувати так званий «ping of death» - тип мереженої атаки, під час якої атакований комп'ютер отримує особливим чином сформований echo-запит (ping), після якого він перестає відповідати на запити взагалі.

Перевантаження атакованої системи з метою вичерпання усіх наявних у атакованої системи ресурсів полягає у використанні величезної кількості безглуздих (рідше - осмислених) пакетів для завантаження ресурсів системи, необхідних для обробки запитів легітимних користувачів. Цей вид атаки також має назву флуд, що походить від англомовного терміну flood - повінь.

В залежності від напрямку реалізації флуд-атаки бувають: спрямовані на ресурси атакованої системи та спрямовані на канал зв'язку, що з'єднує атаковану систему з іншою частиною мережі.

Під час флуд-атаки, спрямованої на ресурси системи, ці ресурси захоплюються за допомогою багаторазового і дуже частого звернення до якого-небудь сервісу, що виконує складну операцію. Це може бути, наприклад, тривале звернення до одного з активних компонентів (скриптів) web-сервера. Сервер витрачає всі ресурси машини на обробку атакуючих запитів, а легітимним користувачам доводиться чекати.

Якщо ж флуд-атака спрямована на канал зв'язку, потік флуд- пакетів займає весь пропускний канал. Завдяки цьому більшість легітимних пакетів не досягають цільової системи, що піддається атаці. Крім того, сама атакована система, будучи зайнятою обробкою флуд-пакетів, не має можливості обробляти легальні запити.

Як видно з визначення, грань між двома описаними вище напрямками флуд-атак є досить умовною, оскільки в багатьох випадках величезна кількість трафіку займає як ресурси атакованої системи, так і канал зв'язку.

Також атаки на відмову класифікуються в залежності від рівня мережевої моделі, на якому вони реалізуються. Мережева взаємодія є складним процесом, який відбувається на кількох рівнях.

В залежності від рівня мережевої моделі Transmission Control Protocol та Internet Protocol (TCP/IP), на якому реалізується атака на відмову, виділяють:

- рівень доступу до середовища передачі даних;
- мережевий рівень;
- транспортний рівень;
- прикладний рівень.

В залежності від рівня мережевої моделі Open Systems Interconnection (OSI), на якому реалізується атака на відмову, виділяють:

- перший рівень - фізичний;
- другий рівень - канальний;
- третій рівень - мережевий;
- четвертий рівень - транспортний;
- п'ятий рівень - сеансовий;
- шостий рівень - представлення;
- сьомий рівень - прикладний.

За схемою атаки, тобто в залежності від того, якими шляхами здійснюється доставка шкідливого трафіка від атакуючого комп'ютера до атакованої ІТС, виділяють наступні атаки на відмову:

- пряма, під час якої пересилка трафіку здійснюється безпосередньо з одного або багатьох хостів;
- віддзеркалена, під час якої пересилка трафіка здійснюється через третіх осіб;
- прихована, під час якої зловмисний трафік ховається в «законному» трафіку.

Таким чином, розподілена атака на відмову характеризується тим, що здійснюється одночасно кількома атакуючими. Існують наступні варіанти організації розподілених атак на відмову: ботнет - зараження певного числа комп'ютерів програмами, які в певний момент починають надсилати атакуючі запити; флешмоб - домовленість великого числа користувачів Інтернету почати здійснювати певні типи запитів до атакованого сервера; смурфінг - атака з використанням широкомовних адрес та підробки IP-адреси відправника.

Все сказане дозволяє зробити висновок, що різні види атак можуть залишити різні цифрові сліди, а отже буде легше зрозуміти, де їх шукати.