УДК 004.7

**ТИПИ МЕРЕЖЕВИХ АТАК І СПОСОБИ ЇХ ВИЯВЛЕННЯ**

*Маляренко Олександр, КІ-17006б*

Мережеві атаки можуть бути активні і пасивні.

Активні атаки включають у себе явний вплив на систему, який змінює її стан. Наприклад, це може бути шкідливий програмний код-вірус, впроваджений в виконувану системою програму, спотворення даних на сторінках веб-сайту, блокування мережевого сервісу шляхом "бомбардування" його помилковими запитами. Відмінністю активних атак є те, що після свого завершення вони, як правило, залишають сліди.
Наприклад, змінюється вміст пам'яті, надходять дивні діагностичні повідомлення, додатки починають виконуватися неправильно, уповільнено або взагалі зависають, в характеристиках мережевого трафіку і в інших статистичних даних про роботу системи з'являються незрозумілі сплески активності. Проте ретельно підготована ​​активна атака може пройти непоміченою, якщо фахівці, що відповідають за її безпеку, погано інформовані про можливі наслідки такого роду атак.
 Пасивні атаки не порушують нормальну роботу системи: вони пов'язані зі збором інформації про систему, наприклад, вони можуть прослуховувати внутрішньо-мережевий трафік або перехоплювати повідомлення, передані по лініям зв'язку. У багатьох випадках пасивні атаки не залишають слідів, тому їх дуже складно виявити, часто вони так і проходять непоміченими.

Відмова в обслуговуванні
 DoS (відмова в обслуговуванні) і DDoS (розподілені відмови в обслуговуванні) атаки стають все більш поширеними і потужними. Атаки відмови в обслуговуванні приходять у багатьох формах, але мають спільну мету: зупиняють доступ користувачів до ресурсу, будь то веб-сторінка, електронна пошта, телефонна мережа або щось інше. Давайте розглянемо найпоширеніші типи атак на веб-цілі, і як DoS може стати DDoS. За своєю суттю, атака "відмова в обслуговуванні" зазвичай виконується шляхом затоплення сервера, наприклад, сервера веб-сайту, настільки, що він не може надавати свої послуги законним користувачам. Існує декілька способів, якими можна скористатися, найпоширенішими є атаки затоплення TCP і атаки DNS.

Спуфінг
 При проведенні атак зловмисникові важливо не тільки досягти своєї мети, яка полягає в заподіянні шкоди атакованому об'єкту, але і знищити всі сліди своєї
діяльності. Одним з основних прийомів, використовуваних зловмисниками для "замітання слідів", є підміна вмісту пакетів, або спуфінг (spoofing). Зокрема, для приховування місця знаходження джерела шкідливих пакетів зловмисник змінює значення поля адреси відправника в заголовках пакетів. Оскільки адреса відправника генерується автоматично системним програмним забезпеченням, зловмисник вносить зміни в відповідні програмні модулі так, щоб вони давали йому можливість відправляти  зі свого комп'ютера пакети з будь-якими IP-адресами.

Сніфери пакетів
 Сніффер пакетів являє собою прикладну програму, яка використовує мережеву карту, що працює в режимі promiscuous mode (у цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додатку для обробки). При цьому сніффер перехоплює усі мережні пакети, які передаються через певний домен.

Атаки Man-in-the-Middle

Для атаки типу Man-in-the-Middle хакеру потрібний доступ до пакетів, що передаються по мережі. Такий доступ до всіх пакетів, що передаються від провайдера в будь-яку іншу мережу, може, приміром, отримати співробітник цього провайдера. Для атак цього типу часто використовуються сніффери пакетів, транспортні протоколи та протоколи маршрутизації. Атаки проводяться з метою крадіжки інформації, перехоплення поточної сесії і отримання доступу до приватних мережевих ресурсів, для аналізу трафіку та отримання інформації про мережу та її користувачів, для проведення атак типу DoS, спотворення переданих даних і введення несанкціонованої інформації в мережеві сесії, Ефективно боротися з атаками типу Man-in-the-Middle можна тільки за допомогою криптографії.

Фрагментація даних

При передачі пакету даних протоколу IP мережі може здійснюватися поділ цього пакету на декілька фрагментів. Згодом, при досягненні адресата, пакет відновлюється з цих фрагментів. Зловмисник може ініціювати надсилання великої кількості фрагментів, що призводить до переповнення програмних буферів на приймальній стороні і, в ряді випадків, до аварійного завершення системи.

 Атака Ping flooding

 Ping-флуд — тип атаки на мережеве обладнання, ключовою особливістю якої є можливість здійснення атаки програмами і утилітами, що входять до складу домашніх/офісних версій операційних систем. ICMP-повідомлення обробляється мережевим обладнанням третього (і вище) рівня. У більшості випадків це обладнання використовує програмні засоби маршрутизації і обробки пакетів. В результаті, при формальному збереженні невеликого трафіку, виникає перевантаження по кількості пакетів, і пристрій починає втрачати інші пакети (з інших інтерфейсів чи протоколів), що і є метою атаки.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

Типи і приклади мережевих атак URL: https://holodoks.blogspot.com/2017/12/blog-post.html (дата звернення: 25.04.2021).

Фрагментація даних URL: https://web.posibnyky.vntu.edu.ua/fitki/11petuh\_bazdanyh\_movy\_zalitiv/32.htm (дата звернення: 25.04.2021).

Захист локальної мережі URL: https://sites.google.com/site/zahistlokalnoiemerezi/tipi-atak (дата звернення: 25.04.2021).