УДК: 004.056
Онищук В. А – ст. гр. 11 – БГм
Кременецька обласна гуманітарно-педагогічна академія ім. Тараса Шевченка

СТРАТЕГІЯ АТАКИ НА МЕРЕЖУ SYN-FLOOD ПРИ ІНСТРУМЕНТІ HPING3

Науковий керівник: к.с.-г. н. Тригуба О. В.

Onyshchuk V. A.
Kremenets regional humanitarian and pedagogical academy named after Taras Shevchenko

SYN-FLOOD NETWORK ATTACK STRATEGY WITH HPING3 TOOL

Supervisor: Triguba O. V.

Ключові слова: інфокомунікаційна система, пентестер, DOS-атака, трафік, ACK.
Keywords: information communication system, pentester, DOS attack, traffic, ACK.

У світі інформаційних технологій важливе місце надається безпеці мережі. Цей аспект потребує постійної уваги, вивчення та захисту. Інфокомунікаційна система (ІКС) – сукупно складається із електронних та інформаційних комунікаційних систем, які у процесі обробки та аналізу інформації діють як єдине ціле [1]. Сьогодні у світі використання ІКС є однією із складових процесу роботи із потоками інформації, прогрес людства характеризується новітніми інфокомунікаційними технологіями. На даний момент існує безліч атак на комп'ютерні системи. За дослідженнями ізраїльської компанії Check Point Research, кількість кібератак в тиждень на корпоративні мережі збільшилася на 50 % у 2021 році у порівнянні із 2020 роком [2].

В Україні потужними навчальними закладами які займаються дослідженням ІКС та хакерських атак є Тернопільський національний технічний університет імені Івана Пулюя, Київський університет імені Ігоря Сікорського та Харківський політехнічний інститут.

Однією із найпоширеніших є DOS-атака – хакерська атака на обчислювальну систему з метою сильного перевантаження та її відмови, тобто довести до такої критичної точки коли справжні користувачі не зможуть отримати доступ до певних ресурсів.Хостинг може виявитись повним «шлаком», який не протистоїть тим, хто заповнює пропускний канал «брудним трафіком». Деякі не чесні хостери, не попереджають що вони не надають захист від DoS-атаки. Для них головне SMM реклама (найнижчі ціни, підтримка), але немає найважливішого – надання стабільної роботи інтернет ресурсів. Така атака небезпечна багатьма факторами, наприклад під час неї буде важкий доступ не лише в клієнтів, а й в власника ресурсу. Вона може відволікати від серйознішої атаки.

Одним з поширених видів атак DoS – SYN-Flood. Такий флуд відбувається на транспортному рівні моделі OSI. Це є своєрідний спосіб атаки, суть якого відправлення дуже великої кількості SYN запитів в супер малий термін. Для кращого розуміння

варто пригадати «трьохкратне рукостискання». SYN-запит – певний запит до протоколу TCP, що знаходиться в транспортному рівні. Користувач відправляє пакет, на якому є позначка SYN, тоді система розуміє що він хоче під'єднатися. SYN-позначка є в заголовку частини TCP, який синхронізовує номери сесій прийому та передачі. Якщо все успішно, тоді сервер має відправити зустрічний пакет на яких є позначки SYN-ACK. Після отримання клієнт підтверджує відповідь сервера і з'єднання є стійким та стабільним. Традиційний SYN Flood можна створити з одного комп'ютера або тоді коли є в наявності інші «заражені» машини на різних серверах і вони атакують жертву.

Зловмисник посилає SYN пакети та переповняє жертву цими запитами. Головною умовою є ігнорування SYN-ACK пакетів. Можливий такий варіант, коли відбувається підробка власного адресу та відповідні пакети просто відправляються на неіснуючі адреси. У сервера з'являються не закриті з'єднання, такі які потребують відповіді від клієнта. Після закінчення певного часу, вони зникають, але хакер або пентестер відправляє нові запити, що постійно збільшуються. Для звичайних користувачів підключитись до такого сервера дуже важко, їм потрібно зловити певний таймінг, що є практично не реально.

Для того щоб навчитись захищати мережу, потрібно відточити майстерність з атаки. Найпростішим інструментом є hping3. Команда для установки в Kali Linux – # sudo apt-get install hping3». Після установки інструменту такою командою починають атаку на певну ціль – «# hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source (адреса жертви)». Тепер трішки детальніше про цю команду – ми відправляємо 15000 пакетів («-c 15000»), розміром 120 байт («-d 120»). Потрібно вказати що позначка SYN («-S»), має бути включена, а розмір TCP вікна – «-w 64», порт – 80 («-p 80»), та позначаємо флуд («--flood»). Важливою умовою для маскування та уникнення відповіді від сервера є створення дуже багатьох підробних IP-адресів («--rand-source»). Отже, на таку атаку існує багато методів боротьби, наприклад використання Wireshark для моніторингу трафіку, але вона залишається небезпечною. Пентестери вивчають не тільки методи захисту, але й вплив на жертву.

Хоча існують та оновлюються інструкції з безпеки, але зловмисники постійно шукають нові способи здійснення цих атак, або відбувається поєднання їх для кращої ефективності. Підтримка безпеки мережі та постійне оновлення заходів захисту є важливим для запобігання небезпеки. Наприклад потрібно використовувати firewall, та IPS чи IDS, також існують ще дуже багато інших інструментів. Але варто запам'ятати що повністю бути в безпеці неможливо, навіть при дотриманні найкращих практик та заходів захисту. Найслабшим елементом є людина, на яку легко подіяти соціальною інженерією.

Список використаних джерел

1. Верховна Рада України, Закон України «Про захист інформації в інформаційно-комунікаційних системах», 1994. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення 10.04.2024).
Check Point Blog, Check Point Research: Cyber Attacks Increased 50% Year over Year». 2021. URL: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year (last accessed 10.04.2024).