

УДК 004.056.53

Жигулін Д.І.¹, Головіна К.П.¹, Дячук Т.С.²

¹ студ. гр. КНТ-526 НУ «Запорізька політехніка»

² асист. НУ «Запорізька політехніка»

ВИКОРИСТАННЯ БАГАТОФУНКЦІОНАЛЬНОГО МЕРЕЖЕВОГО СНІФФЕРА “INTERCEPTER-NG” У ВІДКРИТИХ WI-FI МЕРЕЖАХ

Метою роботи є аналіз прийомів сканування трафіку відкритих точок доступу Wi-Fi, а також пошук способів самостійного захисту від рук зловмисників, що можуть вкрасти особисті дані, документи та паролі.

Interceptor-NG – це програма для виконання атак "людина-посередині". Головною особливістю, яка виділяє Interceptor-NG серед подібних програм, є те, що спочатку вона була написана для Windows і прекрасно працює саме в цій операційній системі. Також до особливостей програми можна віднести графічний інтерфейс, в якому зібрані численні функції та опції, пов'язані з атакою людина-посередині [1].

У практичному сенсі, атака людина-посередині полягає у можливості переглядати передані іншими користувачами дані в локальній мережі. Серед цих даних можуть бути логіни і паролі від сайтів. Процес аналізу переданих даних називається сніффінгом. У процесі сніффінга Interceptor-NG вміє: перехоплювати логіни і паролі для входу на веб-сайти, відновлювати передані дані (файли), перехоплювати повідомлення деяких месенджерів, та показувати відвідані користувачем адреси. Робота з програмою “Interceptor – NG” не дає стовідсоткового результату, так як є нестабільною. Це означає, що здійснення атак може погіршити швидкість з'єднання інтернету та зв'язок сніффінг-програми з користувачем (можливо атаку доведеться повторювати декілька разів до «вдалого» результату).

Завдяки атаці, званої ARP спуфінгом, комп'ютер починає вважати шлюзом не роутер, а комп'ютер атакуючого. Атакуючий отримує запити від «жертви» і передає їх у пункт призначення (наприклад, запитує вміст веб-

сайту в Інтернеті), отримавши відповідь від пункту призначення, він направляє його «жертві». У цій ситуації атакуючий стає посередником – звідси інша назва атаки людина-посередник – «атака посередника». Для реалізації атаки ARP спуфінг необов'язково розуміти її деталі [2].

За допомогою функції “Smart scan”, ми можемо відстежити пристрої, які підключені до нашої точки доступу, обрати ціль для атаки та виконувати будь-які функції Interceptor-NG.

Функція «Traffic changer» — головною метою цієї функції є отримання переходів на сторінки або рекламу, які можуть містити в собі загрозливе програмне забезпечення. Використовується для підміни слова пошукового запиту користувача на будь-яке інше слово. Недоліком цієї атаки є те, що користувач одразу помітить, що його запит був підмінений. Важливо, щоб ключове слово та слово користувача містило однакову кількість символів.

Функція «Cookie killer» — це видалення cookie-файлів користувача для повторної авторизації з метою отримання логіна та пароля. Головною метою цієї атаки є вихід з аккаунту користувача на сторінку авторизації. Повторне введення даних авторизації призведе до отримання цих даних зловмисниками. Також працює і з SSL-з'єднаннями та за допомогою функцій мережесих атак “SSL MitM” та “SSL Strip”, видаляємо “cookie-файли” з браузера користувача.

Функція «FATE» – головною метою цієї атаки є підміна оригінальної сторінки сайту на фейкову, адреса якої буде відрізнятися мінімально. Усі дані які будуть введені користувачем будуть отримані зловмисниками. Таким чином, користувач вводить на підмінну сторінку авторизації свої справжні дані та бачить помилку авторизації. На другій спробі підмінна сторінка зникає, а ми отримуємо дані які були введені на підмінній сторінці. Важливим недоліком цієї атаки є те, що адреса підмінної сторінки має відрізнятися від оригіналу. Деякі користувачі можуть запідозрити, що їх трафік відстежують.

Всі наведені вище методи отримання чужої персональної інформації були проведені лише у дослідницьких та наукових цілях, задля з'ясування способів, що можуть завдати зловмисникам у їх справах та зможуть організувати безпечне користування Інтернетом. Ці способи не передбачають використання у реальному житті, тому що викрадення персональної інформації людини може привести до несення покарання людиною, що викрала ці дані.

Є декілька простих способів, які зроблять ваше підключення максимально безпечним: підключайтеся лише до відомих мереж, не вводьте додаткову інформацію, використовуйте VPN, використовуйте двухфакторну авторизацію, використовуйте надійні та безпечні браузери, такі як Google Chrome та Mozilla Firefox.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Interceptor-NG [Електронний ресурс]. – Режим доступу: <http://sniff.su/>
2. Багатофункційний сніфер [Електронний ресурс]. – Режим доступу: <https://interceptor-ng.com/>