УДК 004

Дробот Т. С. студентка гр. 125-20-1
Науковий керівник: Олішевський І.Г., асистент кафедри БІТ
(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

ВРАЗЛИВОСТІ WI-FI МЕРЕЖІ. ЧОМУ НЕ МОЖНА ПІДКЛЮЧАТИСЯ ДО ЗАГАЛЬНИХ ТОЧОКДОСТУПУ

Основна ідея: показати на практиці наскільки може буде вразливий електроний девайс,якщо підключатиметься до відкритих Wi-Fi мереж.

Вступ

На даний момент часу в усьому світі вкрай поширений стандарт широкосмугового доступу Wi-Fi. Практично в кожному відвідуваному закладі - кафе, ресторані, кіно, освітньому закладі, аеропорту, вокзалі тощо, в кожній квартирі, є доступ в інтернет черезWi-Fi.

Підключаючись до точки доступу, найчастіше користувачі заходять на сайти, соціальні мережі та поштові сервіси, здійснюють онлайн-покупки за допомогою електронних гаманців і банківських карток, вводячи свої персональні дані та дані авторизації. Середньостатистичний користувач анітрохи не замислюється про безпеку своїх даних, довірених їм мережі Wi-Fi.

Зловмисник, який отримав доступ до мережі Wi-Fi або сам створив таку точку доступу, отримує доступ до всіх даних, переданих під'єднаними пристроями.

Тому сьогодні розберу деякі сценарії того, як зловмисник може отримати доступ до мережі Wi-Fi, розберемо сценарій перехвату «Hand-shake», щоб отримати пароль до закритої мережі Wi-Fi, також розглянемо сценарій «людина по середині» з перехватом та модифікацією трафіку, отримання доступу до налаштування маршрутизатора та які ризики це має, та те, як забезпечити собі безпеку при роботі з Wi-Fi.

Модуляція ситуації

Для початку моделюємо ситуацію, наприклад, маємо деяку «жертву» (далі ціль), і того, хто хоче заволодіти особистими даними «жертви»(далі зловмисник), зловмисник хоче отримати дані від банківського профілю цілі, та його сайту швидкої їжі, бо ціль, постійно працює в одному з кафе недалеко від дому, тому що там є безкоштовний Wi- Fi.

Інструменти для роботи

Ноутбук, операційна система mac OS або Linux. Деякі скрипти та програмне забезпечення.

Прямого доступу навіть до Wi-Fi мережі не будемо мати, все з самого нуля.

Отримання доступу до Wi-Fi мережі де є користувач

Для виконання цього будемо приводити приклад атаки «Hand-shake».

Для отримання пароля WPA2 WiFi треба в першу чергу перевести мережевий адаптер у режим моніторингу. Командою ifconfig моніторимо нашу систему, знаходимо бездротовий адаптер wlan0, та переводимо його в режим моніторингу. Знаходимо необхідну мережу. Тепер робимо від’єднання всіх користувачів у цій мережі, та паралельно вмикаємо моніторинг перехвату пакетів Hand-shake. Після успішного виконання ми отримаємо надпис в консолі WPA Handshake: 50:D4:F7:E5:66:F4. Де після «:» йде BSSID мережі.

Тепер виконуємо розшифрування Hand-shake, по словнику, який складаємо самостійно виходячи з зовнішніх факторів, які можуть у собі мати пароль.

Отримаємо 2000 можливих паролів та додаємо їх до словника базових паролів і

маємо файл на 960 тис. паролів, виконуємо розшифрування, в мене на це витратило 40 хвилин.

Тепер маємо пароль від мережі.

Перехват пакетів

Для перехоплення пакетів мережі виростаємо програму Wireshark. Попередньо налаштуємо протокол IEEE 802.11 як Enable decryption. Щоб трафік шов частково вже розшифрований.

Вмикаємо програму, та чекаємо деякий час. Далі зберігаємо файл та починаємо йогоаналізувати за допомогою POST, GET та DNS запитів.

З POST ми отримаємо відкриті дані які передаються, через Get зашифровані для більш детального аналізу. А з DNS ми отримаємо ті сайти куди заходив користувач.

Виходячи з цього, що маємо: з POST отримали почтову адресу жертви, номер телефону,повне ім'я та прізвище, з DNS запитів отримали те, що користувач заходив на сайт швидкої їжі (те, що шукаємо), покупку білетів та подорожі.

Підміна DNS

Тепер зробимо підміну DNS сайту для того, щоб жертва зайшла на наш сайт прицьому нічого не запідозривши.

Для цього робимо сайт-обманку, яка буде красти паролі та

логіни.Заходимо в налаштування роутера, тут є два випадки.

1. Роутер має заводські налаштування і тому витрачається менше часу
2. Роутер має більш сильні налаштування, але дозволяють під'єднатись по бездротовій мережі.

Спочатку розберемо другий випадок, тут маємо зробити як з паролем від Wi-Fi підбір пароля далі йти як описано нижче.

Розглядаємо випадок, коли пароль стандартний, просто заходимо на сайт та робимозаміну DNS, (заздалегідь треба знати ip адресу сайту, який будемо заміняти)

Перезавантажуємо роутер, та чекаємо.

Тут також треба розуміти, що якщо це підміна загальних сайтів, то будемо отримувати всі данні людей, які будуть заходити на них.

А ще через таку підміну можемо встановлювати застосунки на пристрій користувачів під видом, наприклад оновлення.

Як забезпечити безпеку для себе

Розглянувши приклади атак через бездротову мережу виникає питання - як забезпечити власну безпеку.

Найбанальніша рекомендація - не користуватись загальними мережами. Але є випадки коли це необхідно робити без винятку.

Тому перше, що треба зробити це забезпечити шифрування свого трафіку, для цьоготреба використання VPN.

Уважно слідкуйте як працює сайт, де будете вводити свої дані, зазвичай якщо потрапили на фальш-сторінку, вона працює за протоколом HTTP (це можна зрозуміти по сірому замочку біля пошукової стрічки), якщо замочок є зелений, то це протокол HTTPS і він є безпечний.

Якщо володієте роутером, часто робіть оновлення прошивки, також змініть налаштування зміни стандартного логіну та пароль. А ще вимкніть можливість підключення до налаштування роутера через wi-fi, або зробіть вайт-лист тих хто може це зробити.

Перелік посилань:

1. https://us.norton.com/blog/privacy/public-wifi - Автор: Клер Стауффер, співробітник NortonLifeLock, 15 вересня 2022 року
2. https://www.rd.com/article/dangers-of-public-wifi/ - Автор: Лорі Будгар, 26жовтня 2022 року
3. https://www.computerworld.com/article/2577244/top-10-vulnerabilities-in-today- s-wi-fi-networks.html - Автор: Сандіп Сінгхал, 15 липня 2002 року