УДК 621.396:004.7.056

ТЕСТУВАННЯ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ У СЕРЕДОВИЩІ KALI LINUX

Кияниця О.М. Холодило О.В.
Науковий керівник – ст. викладач Медведєв. Є.О.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ
м. Харків, Україна

This paper investigates the security of wireless networks using the Kali Linux software environment. Cracking networks involves several stages, with success depending on the speed of key decryption–the most labor-intensive phase. The advantage of Kali Linux lies in its extensive set of tools for vulnerability analysis and ethical hacking.

Бездротові мережі стали невід'ємною частиною сучасного світу. Вони використовуються у різних сферах життя – вдома, на роботі та в громадських місцях, забезпечуючи зручний доступ до Інтернету для виконання як професійних, так і особистих завдань. Попри численні переваги, що спрощують повсякденну діяльність, існують певні ризики, пов'язані з безпекою. Уразливість бездротових мереж призводить до серйозних загроз, включаючи кібератаки на фінансові установи, комерційні компанії та державні органи. Кількість таких інцидентів продовжує зростати, оскільки не всі адміністратори мереж застосовують надійні методи захисту. Вразливості бездротових мереж можна використати для несанкціонованого доступу, і цей процес можна здійснити за допомогою операційної системи Kali Linux, який буде детально розглянуто далі.

Тестування безпеки бездротових мереж у Kali Linux. Загальна процедура тестування бездротових мереж у Kali Linux складається з кількох кроків [1], [2], [3]:

- підключення зовнішнього бездротового адаптер до USB-порту ноутбука;
- створення інтерфейсу моніторингу. Для цього необхідно перевести бездротовий адаптер у режим моніторингу;
- використання інструментів **Kali Linux** для пошуку всіх найближчих бездротових мереж (із перехопленням і захопленням пакетів) і обирання цілі для спроби злому.

Атака відключення (Deauthentication Attack). Цей тип атаки використовується для відключення будь-якого пристрою від будь-якої мережі в межах робочого діапазону, навіть якщо мережа захищена ключем. Хакер надсилає пакети відключення (deauthentication packets) до маршрутизатора, прикидаючись цільовим пристроєм (шляхом підміни його MAC-адреси). Одночасно хакер надсилає пакети до цільового пристрою (вдаючи, що він є маршрутизатором), повідомляючи, що пристрою необхідно повторно пройти аутентифікацію.

Для відключення всіх клієнтів у конкретній мережі необхідно скористатися наступною командою:

aireplay-ng --deauth [кількість пакетів] -a [AP] [ІНТЕРФЕЙС]

Для відключення конкретного клієнта в мережі:

aireplay-ng --deauth [кількість пакетів відключення] -a [AP] -c [ціль] [інтерфейс]

Створення фальшивої точки доступу (Honeypot). Фальшиві точки доступу (AP) можуть бути корисними в багатьох ситуаціях. Створення відкритої точки доступу – один із прикладів. Таким чином можна привабити багато клієнтів, і що ще важливіше, багато з них автоматично підключаться до неї. Оскільки це відкрите з'єднання, трафік не буде зашифрованим, що дає можливість перехоплювати весь трафік, створений клієнтами, які підключаються до цієї точки.

Для цього потрібні дві карти: одна – підключена до Інтернету, а друга – Wi-Fi карта, яка виступає як точка доступу.

Клієнт (жертва) надсилає запити до Wi-Fi карти хакера (атакувальника), а хакер налаштовує свою машину так, щоб кожен запит, який надходить від Wi-Fi карти, перенаправлявся на другу карту, підключену до Інтернету. Відповідь повертається від другої карти через машину хакера до Wi-Fi карти, яка передає її клієнту, що надіслав запит.

Для реалізації описаного процесу підключення до цільової мережі не є обов'язковим. Однак, якщо підключитися до цільової мережі, можна отримати точнішу інформацію та проводити більш ефективні атаки. Відкрита мережа дозволяє підключитися до неї без пароля та виконувати подальші дії.

Проблема виникає, якщо цільова мережа використовує ключ, тобто застосовує певний тип шифрування. Існує три основних типи шифрування: WEP, WPA та WPA2.

WPA2 – це технологія мережевої безпеки, яка широко використовується в бездротових Wi-Fi мережах. Вона є вдосконаленням оригінальної технології WPA, яка була розроблена як заміна старішого та значно менш безпечного WEP. WPA2 застосовується на всьому сертифікованому Wi-Fi обладнанні з 2006 року і базується на стандарті технології IEEE 802.11i для шифрування даних.

Коли WPA2 увімкнене з найсильнішим варіантом шифрування, інші особи в межах діапазону мережі можуть бачити трафік, але він буде зашифрований за найсучаснішими стандартами шифрування .

Хоча WPA2, WPA та WEP схожі за назвами, вони відрізняються за рівнем безпеки. WEP – найменш безпечний, легко зламується через однаковий ключ для всіх пакетів, що дозволяє знайти його за допомогою програм за кілька хвилин, тому його краще уникати. WPA використовує TKIP для шифрування, що робить його безпечнішим за WEP. WPA2, заснований на AES, є найнадійнішим, особливо з ключами WPA2-PSK (64 шістнадцят-

кові цифри), які часто застосовуються в домашніх мережах під назвою "WPA2 Personal". Враховуючи рівень шифрування, можна зробити висновок, що найменш безпечним є WEP, за ним іде WPA, а найбільш безпечним є WPA2.

Злам WPA. У WPA кожен пакет шифрується унікальним тимчасовим ключем. Це означає, що кількість зібраних пакетів даних не має значення. WPA та WPA2 подібні – єдина відмінність полягає в тому, що WPA2 використовує алгоритм під назвою CCMP.

Злам WPA/WPA2 через вразливість WPS. WPS – це функція, яка дозволяє користувачам легко підключатися до мереж із увімкненим WPS, використовуючи кнопку WPS або просто активуючи цю функцію. Аутентифікація відбувається за допомогою 8-значного PIN-коду. Це означає, що кількість можливих комбінацій PIN-коду відносно невелика, і за допомогою атаки грубої сили (brute force) ми можемо вгадати PIN-код менш ніж за 10 годин.

Інструмент під назвою Reaver може потім відновити ключ WPA/WPA2 із цього PIN-коду.

Примітка: Ця вразливість притаманна функції WPS, а не самому WPA/WPA2, але вона дозволяє нам зламати будь-яку точку доступу WPA/WPA2 без використання списку слів (wordlist) і без наявності клієнтів.

Для зламу точок доступу з WPS ми використаємо інструмент wash, щоб провести сканування на та виявити точки з увімкненим WPS.

wash -i [інтерфейс]

Потім ми застосуємо інструмент reaver, щоб за допомогою атаки грубої сили визначити WPS PIN-код і розрахувати WPA-ключ.

reaver -i [інтерфейс] -b [MAC цільової точки доступу] -c [цільовий канал] -vv

Треба зауважити, захоплення пакетів WPA не є корисним, оскільки вони не містять інформації, яку можна використати для злому ключа. Єдині пакети, які містять дані, що допомагають нам зламати пароль, – це пакети рукостискання (handshake). Щоразу, коли клієнт підключається до точки доступу, між клієнтом і точкою доступу відбувається чотиристоронє рукостискання (four-way handshake). Захопивши рукостискання, ми можемо використати aircrack-ng для запуску атаки за списком слів (wordlist attack) проти рукостискання, щоб визначити ключ.

Для злому точки доступу WPA/WPA2 із відключеним WPS потрібно дві речі: захоплення рукостискання (handshake) та список слів (wordlist).

Захоплення рукостискання. Пакети рукостискання надсилаються щоразу, коли клієнт підключається до цільової точки доступу. Щоб захопити його, ми виконаємо наступне:

Запустимо airodump-ng на цільовій точці доступу:

airodump-ng --channel [канал] --bssid [bssid] --write [ім'я-файлу] [інтерфейс]

Чекаємо, поки клієнт підключиться до точки доступу, або відключимо підключеного клієнта (якщо такий є) на дуже короткий період часу, щоб його система автоматично перепідключилася.

aireplay-ng --deauth [кількість пакетів відключення] -a [AP] -c [ціль] [інтерфейс]

Створення списку слів. Друга річ, необхідна для злому WPA/WPA2, – це список паролів для вгадування. Кожен може завантажити готовий список слів із Інтернету або створити власний за допомогою інструменту crunch.

crunch [мін. довжина] [макс. довжина] [символи] -o [файл]

Злам ключа. Для зламу ключа ми використаємо aircrack-ng. Цей інструмент комбінує кожен пароль із списку слів із назвою точки доступу (ESSID), щоб обчислити головний парний ключ (Pairwise Master Key, PMK) за допомогою алгоритму pbkdf2. Потім PMK порівнюється з файлом рукостискання.

aircrack-ng [файл рукостискання] -w [список слів] [інтерфейс]

Процес зламу ключа може буди достатньо довгим и дуже сильно залежить від потужності комп'ютера.

Висновки. Kali Linux забезпечує потужний набір інструментів для етичного хакерства та аналізу мереж, що дозволяє користувачу не лише тестувати, а й захищати своє оточення. У доповіді описано процес тестування на проникнення, підкреслено, що успіх цього етапу значною мірою залежить від ефективності інструменту для розкриття ключа чи пароля, причому саме цей етап є найчасовитратнішим порівняно з іншими. Також проведено поверхневий аналіз систем шифрування, на основі якого можна зробити висновок про доцільність використання сучасних алгоритмів шифрування, що зробить вірогідність зламу мінімальним.

Список використаних джерел:

1. Ramachandran V, Buchanan C, Kali Linux Wireless Penetration Testing Learn to Penetrate Wi-Fi and Wireless Networks to Secure your System from Vulnerabilities, 2nd Edition, Packt Publishing, 2015, ISBN-10: 1783280417

2. Broad J, Bindner A, Hacking with Kali – Practical Penetration Testing Techniques, Elsevier, 2014., ISBN: 978-0-12-407749-2.

3. McClure S, Scambray S J, Kurtz G, Hacking Exposed: Network Security Secrets & Solutions, Chapter Wireless Hacking, Computing McGraw-Hill, 2012, ISBN-10: 0072121270

4. The 10 Top Hacking Tools in Kali Linux, Hacking Tutorials (2015, July 16).