## Лабораторна робота № 12

Дослідження стійкості точок доступу бездротової мережі Wi-Fi

***Мета***: дослідити стійкість паролів точок доступу бездротової мережі та надати рекомендації стосовно оптимізації парольної політики для доступу до таких мереж.

***Обладнання***: Персональний комп'ютер (ноутбук) з бездротовим доступом до мережі Інтернет.

***Програмне забезпечення***: операційна система Linux (Kali, Ubuntu etc.), Windows (XP, 7, 8, 10); утиліти wifite, besside-ng, aircrack-ng або аналогічні програмні засоби. Для перевірки стійкості паролів знадобиться John The Ripper (Linux) або Elcomsoft Wireless Security Auditor (Windows). Можна використати інше аналогічне ПЗ.

### Теоретичні відомості

Злам паролів точок бездротового доступу та подальше використання захищених ресурсів небезпечне не лише з економічної точки зору. Зловмисник, проникнувши до корпоративної мережі, не тільки зможе виконувати дії від імені Вашої мережі, а й деструктуризувати корпоративні ресурси. Тому в таких мережах необхідно дотримуватися усіх правил парольної політики та слідкувати за тим, щоби стійкість паролів доступу була максимальна. Дослідження стійкості паролів точок доступу бездротової мережі підприємства — один з основних обов'язків адміністратора безпеки.

Комп'ютер, що підключається до бездротової мережі, обмінюється з точкою доступу так званими handshake-пакетами (пакетами "рукостискання", авторизації), які може перехопити зловмисник з подальшим зламом кодів доступу програмами-брутфорсерами. Для перехоплення пакетів авторизації wi-fi-модуль ноутбука переводиться програмним чином у режим прослуховування, а пакети, які вдається перехопити, утиліта прослуховування копіює у файл. Оскільки коди доступу передаються у зашифрованому вигляді, цей файл подається утиліті-кракеру. Час зламу коду доступу безпосередньо залежить від його складності. Таким чином, знаходження слабких кодів доступу — основна задача досліджень стійкості wi-fi-мережі.

### Практична частина

1. Знаходячись у середовищі Kali Linux (або аналогічному), захопіть handshake-пакети точки доступу, що досліджується (або кількох одночасно, які "бачить" Ваш wi-fi-модуль). Для цього використайте утиліти wifite, aircrack, besside або аналогічні. Звичайно, точки доступу, пакети з яких Ви намагаєтеся перехопити, повинні належати Вашому закладу і знаходитися під Вашим або Вашого підрозділу підпорядкуванням. У крайньому випадку Ви повинні отримати у власника чужої точки доступу дозвіл на виконання цих дій.
2. Здійсніть парольну атаку на отриманий файл за допомогою John The Ripper Linux, Windows) або Elcomsoft Wireless Security Auditor (Windows). Можна використати інше ПЗ з аналогічним функціоналом.

3. Відзначте, скільки часу знадобилося на здійснення парольної атаки (повним перебиранням або за словником) на різні паролі, виділіть серед них слабкі, та замініть їх сильними паролями.
4. З’ясуйте формат handshake-пакетів та протоколи підключення до точок доступу.
5. Сформулюйте вимоги до парольної політики та правила вибору сильних паролів, які на Вашу думку, зроблять парольні атаки неефективними.
6. Підготуйте звіт з лабораторної роботи. Для цього запишіть відеопротокол Ваших дій з екрану комп’ютера та озвучте його. Основний наголос у відеозвіті повинен бути на розгляд формату handshake-пакетів та протоколів підключення, а також на ефективність запропонованих Вами сильних паролів.

**Питання до лабораторної роботи**

1. Які небезпеки загрожують інформації в корпоративній мережі в разі проникнення зловмисника через точку доступу wi-fi?
2. Яким способом можна запобігти цим загрозам?
3. Яка структура пакету handshake при підключені до точки доступу бездротового зв’язку? Продемонструйте це на основі отриманих Вами даних.
4. Які протоколи використовуються при підключенні до точки доступу? Охарактеризуйте їх особливості, переваги та недоліки.
5. Які слабкі паролі Ви знайшли при скануванні? Чому вони виявилися слабкими?
6. Сформулюйте вимоги до парольної політики та правила вибору сильних паролів, які на Вашу думку, зроблять парольні атаки неефективними.