УДК 004.047

**РОЗРОБЛЕННЯ, АНАЛІЗ ТА ПРОЕКТУВАННЯ ПЛАТФОРМИ RASPBERRY PI ТА KALI LINUX ДЛЯ РОБОТИ ТА ТЕСТУВАННЯ WI-FI МЕРЕЖІ УНІВЕРСИТЕТУ.**

**ЧАСТИНА 2: ТЕХНІЧНА РЕАЛІЗАЦІЯ**

*Ломако О. О., науковий керівник Лахно В. А., завідувач кафедри комп'ютерних систем і мереж, д.т.н., професор*

З розвитком світу також дуже стрімко розвиваються технології, зокрема інформаційні. Тому зараз інформація є дуже цінним активом, і як сказав Натан Ротшильд: «Хто володіє інформацією, той володіє світом». Паралельно з цим зловмисники теж удосконалюють свої методи, щоб заволодіти нею і використовувати у власних цілях, в основному в незаконних.

Як сказано вище, з розвитком світу, розвиваються і технології. Раніше основним методом передачі інформації була тільки мова, потім до неї додалось письмо. А в епоху науково-техніної революції з’явився зв'язок за допомогою дротів: телеграф, телефон і т. д.. Коли стало можливим передавати інформацію на великі відстані, стало питання про її захист від конкурентів та зловмисників. Особливо гостро це питання стало з появою бездротових тейнологій, таких як Bluetooth та Wi-Fi. Тепер зловисникам навіть не потрібен фізичний контакт з об’єктом атаки. Тому, щоб запобігти їх проникненню, потрібно правильно налаштовувати маршрутизатори та власноруч перевіряти їх на можливість несанкціонованого проникнення.

Основною метою цього проекту є створення пристрою для тестування на можливість проникнення у Wi-Fi мережу університету. Так званий «етичний» (або «білий») хакінг[1], коли організація сама винаймає хакерів, які імітують дії зловмисників, а після виконання роботи складають звіт з можливими проблемама та способоми їх вирішення.

Основою даного пристрою виступає одноплатний мікрокомп’ютер Raspberry Pi 4 model B з встановленою на нього операційною системою Kali Linux, яка спеціалізується на безпеці комп’ютерних мереж. Сам пристрій невеликий за розміром, завбільшки як пачка цигарок, який матиме автономне джерело живлення(наприклад павербанк), та можливість підключення до нього за допомогою SSH, що дасть змогу виконувати майже всі операції за допомогою смартфону.

Основні інструменти для роботи з Wi-Fi та роутерами[2]:

Aircrack-ng: найпопулярніший інструмент для хакінгу паролів WEP, WAP, WPA2. Він перехоплює пакети з мережі, аналізує їх. Має консольний інтерфейс. Виконує стандартну FMS-атаку разом з кількома оптимізаціями, щоб прискорити процес.

Hydra: інструмент для атаки «грубою силою» (Bruteforce) для взлому практично будь-якої служби аутентифікації. Підтримує швидкий перебір по словнику для більш, ніж 50 протоколів (telnet, https, ftp…).

Nmap: інструмент для виявлення мереж та перевірки їх безпеки.

John the Ripper: ще один популярний інструмент для взлому. Має налаштовуваний зламувач, може автоматично виявляти хеш паролів, проводити атаки типу Bruteforce та атаки по словнику.

Kismet Wireless: інструмент для вторгнень, мережевий сканер та аналізатор паролів, має можливість розширювати функціонал за допомогою плагінів.

Hashcat: один з найвідоміших та найшвидший інструмент для взлому паролів та відновлення. Має механізм обробки правил в ядрі, більш, ніж 200 типів хешів і вбудовану систему тестування на продуктивність.

Fern Wifi Cracker: інструмент захисту в Wi-Fi мережах. Призначений для аудиту вразливостів в мережі. Може зламувати і відновлювати ключі WEP, WPA, WPS, а також може виконувати атаки на мережі Ethernet.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. «Пентест (pentest) – внешний аудит безопасности» [електронний ресурс]/

Алексе Кузин. – 18.07.2019. - Режим доступу до ресурсу:

<https://itglobal.com/ru-kz/company/blog/penetration-testing/>

1. «The Best 20 Hacking and Penetration Tools for Kali Linux» [електронний ресурс]/ Divine Okoi. - 22.04.2019. – Режим доступу до ресурсу:

<https://www.fossmint.com/kali-linux-hacking-and-penetration-tools/>