МАТЕРІАЛИ V МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ ТА ВПРОВАДЖЕННЯ МІЖДИСЦИПЛІНАРНИХ НАУКОВИХ ДОСЯГНЕНЬ

9 ЧЕРВНЯ 2023 РІК

М. ІВАНО-ФРАНКІВСЬК, УКРАЇНА

OPEN ACCESS

DOI 10.36074/mcnd-09.06.2023
ISBN 978-617-8126-35-3

МАТЕРІАЛИ
V МІЖНАРОДНОЇ
НАУКОВОЇ КОНФЕРЕНЦІЇ

Міжнародний Центр Наукових Досліджень

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ ТА ВПРОВАДЖЕННЯ МІЖДИСЦИПЛІНАРНИХ НАУКОВИХ ДОСЯГНЕНЬ

9 ЧЕРВНЯ 2023 РІК
м. Івано-Франківськ, Україна

Вінниця, Україна
«Європейська наукова платформа»
2023

УДК 001 (08)
П 78

https://doi.org/10.36074/mcnd-09.06.2023

Організація, від імені якої випущено видання:
ГО «Міжнародний центр наукових досліджень»

Голова оргкомітету: Рабей Н.Р.

Верстка: Зрада С.І.
Дизайн: Бондаренко І.В.

Конференцію зареєстровано Державною науковою установою «УкрІНТЕІ» в базі даних науково-технічних заходів України та бюлетені «План проведення наукових, науково-технічних заходів в Україні» (Посвідчення № 64 від 17.01.2023).

П 78 **Проблеми та перспективи реалізації та впровадження міждисциплінарних наукових досягнень**: матеріали V Міжнародної наукової конференції, м. Івано-Франківськ, 9 червня, 2023 р. / Міжнародний центр наукових досліджень. — Вінниця: Європейська наукова платформа, 2023. — 290 с.

ISBN 978-617-8126-35-3
DOI 10.36074/mcnd-09.06.2023

Викладено матеріали учасників V Міжнародної спеціалізованої наукової конференції «Проблеми та перспективи реалізації та впровадження міждисциплінарних наукових досягнень», яка відбулася 9 червня 2023 року у місті Івано-Франківськ.

УДК 001 (08)

ISBN 978-617-8126-35-3

СЕКЦІЯ XVII.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

СЕКЦІЯ XVIII.
ФІЛОЛОГІЯ ТА ЖУРНАЛІСТИКА

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТІ БЕЗДРОТОВИХ МЕРЕЖ

Колесник Едуард Андрійович
здобувач вищої освіти, Факультет інформаційних
радіотехнологій та технічного захисту інформації
Харківський національний університет радіоелектроніки, Україна

Науковий керівник: Алфьоров Микола Євгенович
Старший викладач кафедри радіотехнологій
інформаційно-комунікаційних систем, старший викладач
Харківський національний університет радіоелектроніки, Україна

Актуальність проекту:

Мережі Ethernet призначені для надання нового спектру комерційних послуг передачі даних як для корпоративних, так і для домашніх користувачів. Але технології постійно розвиваються й у 1998 році було створено технологію бездротової локальної мережі, вона отримала назва WiFi. Технологію створено на основі стандартів IEEE 802.11.

Ця технологія, що дозволяє реалізувати доступ до мережі Ethernet, без використання проводів, при цьому втрати швидкості доступу будуть мінімальними. Також технологія має достатній запас зростання для розвитку. Приблизно з 2009 року мережі WiFi набули широкої популярності як у домашніх користувачів, так і у компаній [1].

Все це дозволило технології WiFi зайняти лідируючі місця у сфері бездротових технологій зв'язку. Крім удосконалення швидкості та дальності WiFi сигналу також важливою складовою є безпека бездротових мереж.

Вразливість Wi-Fi-мережі у тому, що з передачі використовується повітря. Це означає, що будь-яка людина, яка знаходиться поблизу вашої бездротової мережі, може спробувати отримати до неї доступ.

Щоб наочно продемонструвати вразливості бездротових мереж, дослідники мережевої безпеки з проекту Sophos, відомі як «warbiking», їздять центральними вулицями найбільших мегаполісів у світі на велосипедах, обладнаних спеціалізованими антенами, у пошуках мережевих уразливостей, сканують десятки тисяч Wi-Fi., що потрапляють у зону видимості їх устаткування.

Результати їх досліджень вражають. Так, наприклад, із 81743 бездротових мереж, просканованих кілька років тому в Лондоні, 29,5 % взагалі не мають жодного захисту або використовують алгоритм WEP (Wired Equivalent Privacy), що вже понад 15 років вважається вкрай вразливим. Більше того, ще 52% відсканованих мереж використовували Wi-Fi protected Access (WPA), який також не рекомендується використовувати спеціалістами в сфері інформаційної безпеки[2].

Вигода даної теми:

–розробка методик захисту інформації в бездротових мережах;

–дослідження вразливостей бездротових мереж сприяє розвитку нових методів захисту, що можуть бути використані для подальшого покращення безпеки та захисту мереж;

–вибір інструментів для тестування Wi-Fi мереж.

Основне дослідження:

–аналіз вразливостей стандартних протоколів бездротового зв'язку;

–розробка нових методів виявлення та захисту від атак, що специфічні для бездротових мереж;

–експериментальне дослідження реальних бездротових мереж з метою визначення слабких місць та пропозицій щодо покращення їх безпеки;

–розробка рекомендацій щодо захисту бездротових мереж для користувачів.

Дослідження вразливості WPS.

Wi-Fi Protected Setup, WPS – стандарт (і однойменний протокол) напівавтоматичного створення бездротової мережі Wi-Fi, створений Wi-Fi Alliance. Офіційно запущено 8 січня 2007 року.

Метою протоколу WPS є спрощення процесу налаштування бездротової мережі, тому спочатку він називався Wi-Fi Simple Config. Протокол покликаний надати допомогу користувачам, які не мають широких знань про безпеку в бездротових мережах, і як наслідок мають складнощі при здійсненні налаштувань.

WPS автоматично позначає ім'я мережі та задає шифрування для захисту бездротової Wi-Fi-мережі від несанкціонованого доступу до мережі, при цьому немає необхідності вручну задавати всі параметри[3].

Метою представленої роботи є перевірка точок доступу на вразливість Pixie Dust. Перевірити цю вразливість можна за допомогою Kali Linux та інструменту Wifite, який вже встановлений у системі за замовчуванням.

Цей інструмент дуже простий у використанні, має велику кількість функцій, і всі його процеси автоматизовані, що значно полегшує процес перевірки вразливості.

Основні особливості програми можна знайти в Інструменти для тестування бездротових мереж Kali Linux.Після запуску програма автоматично переводить бездротовий адаптер у режим моніторингу. У цьому режимі він пасивно спостерігатиме за всіма пакетами доступних бездротових мереж у радіусі своєї зони дії.

Далі Wifite автоматично розпочне пошук усіх Wi-Fi мереж у зоні досяжності. Зупинити пошук можна примусово, натиснувши певне сполучення клавіш. В результаті сканування можна побачити наступну інформацію про бездротові мережі.

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	TP-LINK_30D29	12	WPA	59db	yes	1
2	pers	2	WPA	32db	lock	
3	DIR-615	9	WPA	25db	no	
4	ASUS	10	WPA	21db	yes	1
5	Dom-30_19	3	WPA	21db	yes	
6	Keenetic-35	11	WPA	17db	yes	
7	WiFi-25	1	WPA	16db	yes	
8	WiFi-42	11	WPA	15db	yes	
9	Kvartira 22	11	WPA	14db	yes	
10	Keenetic-4241	8	WPA	14db	lock	2
11	DOM 34-111	9	WPA	14db	yes	
12	DIR-300	1	WPA	14db	no	

Рис. 1.1. **Інформація про бездротові мережі Wifite**

Після ознайомлення зі списком точок доступу вибирається та, яку потрібно перевірити.

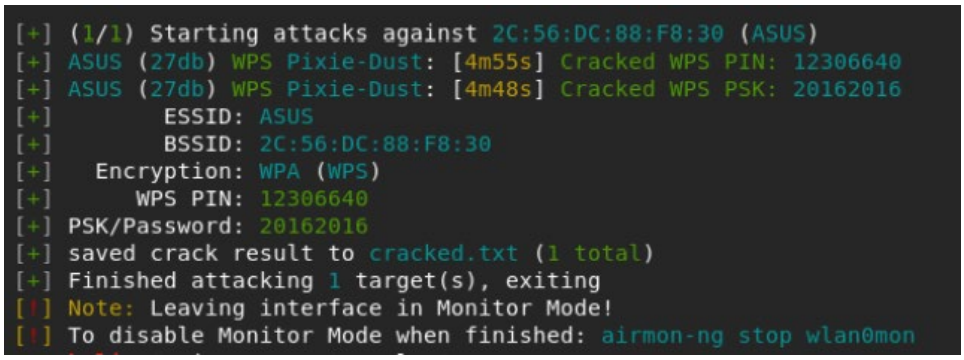

Рис. 1.2. **Результати перевірки точки доступу на вразливість**

Відображаються параметри бездротової мережі, що розглядається, у тому числі і WPS PIN, завдяки якому Wifite підключився до точки доступу і отримав пароль від бездротової мережі:

–ESSID – назва точки доступу,

–BSSID – MAC адреса точки доступу,

–Encryption – тип шифрування ключа точки доступу,

–WPS PIN – пін-код WPS точки доступу, що розглядається,

–PSK/Password - пароль точки доступу.

Для перевірки на вразливість точок доступу в межах міста було проведено дослідження у місцях з високою щільністю бездротових мереж: спальний район [5].

Нижче наводяться дані для однієї з них (з метою збереження конфіденційності даних, SSID точки доступу та її MAC-адреса частково приховані): У спальному районі з кожних 10 точок доступу 6 схильні до вразливості, що перевіряється. Дані однієї з них представлені нижче (частково приховані):

psk: tek889nj,

bssid: 8C:7B:**:1D:**:58

pin: 63167767,

essid: WiFi-**

тип: WPS.

Висновок:

Підсумовуючи, слід зазначити, що не всі точки доступу схильні до вразливості PixieDust. Найбільше схильні точки доступу фірми ZyXEL модель Keenetic. З іншого боку, можна сказати, що у половині випадків SSID мережі не змінювався, тобто залишився за назвою фірми-виробника, заданого за умовчанням. А функція WPS була включена менш ніж у половині точок доступу.

Найбільша частка вразливих точок доступу знаходиться в спальному районі, тому що звичайні користувачі домашніх бездротових мереж не вникають у суть налаштувань безпеки мережі та залишають ті, що прописані за умовчанням в устаткуванні. Загалом рекомендації щодо захисту бездротових мереж 802.11 такі:

–найголовніший і найпростіший метод захисту – це відключення функції WPS у налаштуваннях маршрутизатора;

–придумати унікальне ім'я (SSID) для бездротової мережі та зробити її прихованою. Без точної назви точки доступу не можна підключитися до неї;

–додати перевірку за MAC-адресою. Зловмисник навіть за наявності пароля від мережі не зможе підключитись до неї в цьому випадку;

–зменшити радіус сигналу бездротової мережі, щоб зловмисник не міг працювати в ній здалеку;

–увімкнути шифрування. Використовувати по можливості новий протокол

шифрування WPA3, у якому поки що не знайдено вразливості;

–найрадикальніший метод – це користуватися провідним Інтернетом.

Список використаних джерел:

1. "Hacking Exposed Wireless: Wireless Security Secrets & Solutions" - Johnny Cache, Joshua Wright, Vincent Liu. McGraw-Hill Education. - 512 ст.
2. "Wi-Foo: The Secrets of Wireless Hacking" - Andrew Vladimirov, Konstantin Gavrilenko, Andrei Mikhailovsky. Addison-Wesley Professional. - 528 ст.
3. "Wireless Security: Models, Threats, and Solutions" - Randall K. Nichols. McGraw-Hill Education. - 432 ст.
4. "The Mobile Application Hacker's Handbook" - Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse. Wiley. - 784 ст.
5. "Security Engineering: A Guide to Building Dependable Distributed Systems" - Ross J. Anderson. Wiley. - 1080 ст.
6. "Cryptography and Network Security: Principles and Practice" - William Stallings. Pearson. – 752 ст.