МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

«Програмно-апаратний комплекс для аналізу захищеності мережевого трафіку»

Завідувач Випускаючої кафедри — Любчак В.О

Керівник роботи — Кальченко В.В.

Студент групи КБ-81-0 — Радченко О.С.

Суми 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

Затверджую_____

Зав. кафедрою Любчак В.О.

“_____” _____2022 р.

ЗАВДАННЯ

до випускної роботи

Студента четвертого курсу, групи КБ-81-0 спеціальності «Кібербезпека» денної форми навчання Радченка Олега Сергійовича.

Тема: «Програмно-апаратний комплекс для аналізу захищеності мережевого трафіку»

Затверджена наказом по СумДУ

№_____ від _____2022 р.

Зміст пояснювальної записки: 1) Аналіз програмних та апаратних засобів для моніторингу мережевого трафіку 2) Fналіз існуючих технічних рішень network traffic access point для моніторингу мережевого трафіку 3) Розробка програмного методу та технічного рішення для аналізу захищеності мережевого трафіку

Дата видачі завдання “_____”_____2022 р.

Керівник випускної роботи _____ Кальченко В.В.

Завдання прийняла до виконання _____ Радченко О.С.

РЕФЕРАТ

Записка: стор. 40, рис. 18, табл. 0, джерел. 17

Мета роботи — аналіз методів перехоплення мережевого трафіку та розробка програмно-апаратного комплексу для оцінювання захищеності мережевого.

Об'єкт дослідження — процес перехоплення та аналізу мережевого трафіку.

Предмет дослідження – сукупність методів та заходів програмно-технічного характеру для оцінки захищеності мережевого трафіку.

Методи дослідження — методи перехоплення мережевого трафіку в інформаційно-комунікаційних системах побудованих на основі стеку протоколів TCP/IP.

Результати — проаналізовано сучасні методи перехоплення мережевого трафіку, розроблено програмно-апаратний комплекс для моніторингу та аналізу захищеності мережевого трафіку

КІБЕРБЕЗПЕКА, МЕРЕЖЕВИЙ КРАН, ПЕРЕХОПЛЕННЯ ТРАФІКУ, ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС, АНАЛІЗ ТРАФІКУ, NETWORK TAP, СТВОРЕННЯ ПРИСТРОЮ ПЕРЕХОПЛЕННЯ ТРАФІКУ

ЗМІСТ

ВСТУП

Використання глобальної мережі інтернет відкриває багато можливостей для людей у різних сферах діяльності, для студентів та школярів, це найбільша бібліотека знань, де вони можуть не тільки знаходити нову для них інформацію, а також спілкуватися та розважатися. Працівники різних сфер, які можуть не тільки працювати в інтернеті, а також підвищувати свою обізнаність у різних напрямках. Компанії, робота яких вже не може існувати без інтернету.

Все зводиться до того, що ця глобальна мережа дуже тісно пов'язана з людьми та їх повсякденністю і безпека користування мережею, завжди буде на першому місці, бо кібератаки розвиваються паралельно з мережею і засобами протидії кібератакам.

Тож щоб захиститися від кібератак людям, як основним користувачам глобальної мережі, необхідно було розробити деякі правила користування нею, найбанальніший приклад – це використання складних паролей, що у купі з різним способом захисту даних ускладнило роботу зловмисникам. Але згодом з'явився нова загроза для користувачів, не націлена на крадіжку, а націлена на відмову в обслуговуванні.

Двадцять три роки тому була вперше в історії проведена DDoS атака, що спричинила вихід з ладу мережі одного з Американських університетів. За двадцять років від дати цієї події було проведено її аналіз [1], за результатами якого можна зробити висновок, що для усунення цього виду атак, найкращим методом вирішення буде – аналіз мережевого трафіку.

РОЗДІЛ 1. АНАЛІЗ ПРОГРАМНИХ ТА АПАРАТНИХ ЗАСОБІВ ДЛЯ МОНІТОРИНГУ МЕРЕЖЕВОГО ТРАФІКУ.

1.1 Причини дня аналізу трафіку

Аналізатори трафіку (сніфери) це програма або прилад для перехвату та аналізу мережевого трафіку. Сніфер може аналізувати тільки той трафік, що проходить безпосередньо через його мережеву карту.

Є декілька способів перехвату трафіку:

- звичайне прослуховування мережевого інтерфейса,
- підключення сніферу в розрив каналу,
- відгалуження,
- аналіз побічних електромагнітних випромінювань,
- через так звані атаки MAC-спуфинг та IP-спуфинг;

Взагалі, аналізом трафіку почали користуватися хакери для захоплення логінів та паролів користувачів, на той час вони передавалися мережевими протоколами без необхідного захисту (без використання шифрування), або ж у слабко захищеному вигляді. Але треба зауважити, що сніфери використовувалися не тільки в деструктивних цілях, як приклад вони дозволяли:

- виявляти паразитний, вірусний та кільцевий трафік, що спричиняв надмірне навантаження на мережеве обладнання та канали зв'язку,
- виявляти шкідливе мережеве та недопустиме програмне забезпечення: фрудери, клієнти піринговых мереж, мережеві сканери, троянскі програми. Але це більше про спеціалізованих моніторів мережевої активності,
- перехоплення будь якої незашифрованого трафіку, а іноді і зашифрованого трафіку з метою розкриття необхідної інформації,
- для системних адміністраторів: локалізація несправності в мережах(і) та\або пошук помилок у мережевих конфігураціях;

Також призвести до прослуховування трафіку можуть підозри на атаки IP-spoofing та MAC-spoofing. Що до IP-spoofing - це тип зловмисної атаки, при якій зловмисник приховує справжнє джерело IP-пакетів, щоб важко було дізнатися, звідки вони прийшли. Зловмисник створює пакети, змінюючи вихідну IP-адресу , щоб видавати себе за іншу комп'ютерну систему, приховати особу відправника або обидва. Поле заголовка підробленого пакета для вихідної IP-адреси містить адресу, яка відрізняється від фактичної IP-адреси джерела. Кінцевим користувачам важко виявити підробку IP. Ці атаки здійснюються на мережевому рівні - рівні 3 моделі зв'язку Open Systems Interconnection. Таким чином, не буде зовнішніх ознак фальсифікації. Підроблені запити на з'єднання ззовні виглядають як законні запити на з'єднання. Однак існують інструменти моніторингу мережі, які організації можуть використовувати для аналізу трафіку на кінцевих точках мережі . Фільтрація пакетів є основним способом зробити це.

З цього виникає необхідність для аналізу трафіку для подальшої її фільтрації.

1.2 Апаратні засоби перехоплення та аналізу трафіку

Апаратні засоби аналізу трафіку, тобто пристрої для перехоплення та\або разом з аналізом цього трафіку, прикладом є Cisco RSPAN та Kismet.

Cisco RSPAN - У багатьох мережних комутаторах є можливість дзеркалювати трафік, скажімо з одного порту, на інший, або, наприклад, з VLAN зазначеного, на порт, де є аналізатор трафіку, чи якесь ПЗ. У Cisco ця технологія називається SPAN - Switch Port Analyzer та RSPAN - Remote Switch Port Analyzer (це один з способів перехоплення трафіку, що наведено у пункті 1.1 цього розділу).

В першу чергу, ця технологія необхідна для того, щоб переглянути трафік на якомусь порту для аналізу того, що передається в мережі. Так само вона може знадобитися, наприклад, для запису VOIP. VLAN Voice переправляє весь трафік на певний інтерфейс, а там розгорнуте деяке програмне

забезпечення, що має змогу записувати всі дзвінки. Окрім цього гарним прикладом є зеркалювання трафіку по аналогії системам IPS\IDS. Також RSPAN дає змогу передавати трафік до віддаленого комутатора.

Kismet – це багатофункціональна безкоштовна утиліта для роботи з бездротовими мережами Wi-Fi. В основному ця програма популярна за можливості злому чужих мереж та виявляти приховані безпровідні мережі. В арсеналі інженера інформаційної безпеки ця програма стає чудовим інструментом для спостереження та аналізу IEEE 802.11 (або ефіру 802.11). Умовно, завдання, що вирішуються за допомогою Kismet, можна розділити на дві сфери: аналітика та захист. У першому випадку накопичені відомості повинні оброблятися сторонніми програмами, а в другому Kismet працює як детектор різного роду мережевих атак, тобто як аналізатор мережевого трафіку. Ця програма підтримує багато плагінів, що розширюють її можливості [2].

Нещодавно Kismet перейшла на нове ядро, тому кількість плагінів не велика, але і серед них є гідний екземпляр - DECT Sniffer, що дозволяє використовувати Kismet для роботи з телефонними мережами, є плагін і для Bluetooth.

1.3 Програмні засоби перехоплення та аналізу трафіку

Wireshark – це відомий інструмент для захоплення та аналізу мережевого трафіку, являє собою стандартне програмне забезпечення як для освіти, так і для дорослої роботи з мережею. Ця програма допомагає мережевим адміністраторам виконувати дослідження мережевих додатків, протоколів, пакетів щоб знайти проблеми у роботі мережі, і що важливо, з'ясувати причини цих проблем. Деякі спеціалісти використовують її для пентесту, аналіз мережі на зловживання мережею, переповнення мережі та інше. Якщо дивитись на функціонал цього програмного забезпечення, то можна виділити наступне:

- Глибока перевірка сотень протоколів , які постійно додаються,
- Зйомка в реальному часі та автономний аналіз,

- Стандартний трипанельний браузер пакетів
- Мультиплатформенність: працює на Windows, Linux, OS X, FreeBSD, NetBSD та багатьох інших,
- Зняті мережеві дані можна переглядати за допомогою графічного інтерфейсу або за допомогою утиліти TShark в режимі TTY,
- Найпотужніші фільтри дисплея в галузі,
- Розширений аналіз VoIP,
- Читання/записування багатьох різних форматів файлів захоплення: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, та багато інших,
- Файли захоплення, стиснуті за допомогою gzip, можна розпакувати на льоту,
- Дані в реальному часі можна зчитувати з Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI та інших,
- Підтримка дешифрування для багатьох протоколів, включаючи IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP і WPA/WPA2,
- Правила забарвлення можна застосувати до списку пакетів для швидкого, інтуїтивно зрозумілого аналізу,
- Вихідні дані можна експортувати в XML, PostScript, CSV або звичайний текст;

З цього можна зробити висновок, що використання Wireshark є стандартом для аналізу трафіку.

SolarWinds Network Bandwidth Analyzer – по своїй суті, це сімейство програмного забезпечення, що дозволяє як аналізувати трафік, так і керувати трафіком. Якщо казати більш детальніше, то ця мережева утиліта може допомагати системним адміністраторам контролювати мережеві прилади, керувати інфраструктурою, базами даних та навіть оброблювати інциденти. Фактично, ця сімейство програм може проводити всі вищевказані операції на

основі проаналізованого трафіку, що проходить через мережу. Це дуже дороге програмне забезпечення, весь його функціонал можна дізнатися лише шляхом зв'язку з компанією, яка його поставляє, вартість цього ПЗ, а скоріше модуля 449 000 гривень.

РОЗДІЛ 2. АНАЛІЗ ІСНУЮЧИХ ТЕХНІЧНИХ РІШЕНЬ NETWORK TRAFFIC ACCESS POINT ДЛЯ МОНІТОРИНГУ МЕРЕЖЕВОГО ТРАФІКУ

2.1 Аналіз мережевого трафіку

По своїй суті Аналіз мережевого трафіка є методом виявлення вірусів, використання сигнатур кібератак, виявляння кібератак у мережі , виявлення шкідливих програм різного типу та пакетів, які проходять по мережі, заснований, у першу чергу, на перевірці даних, що проходять через вузли мережі або ж по каналам передачі даних. Також визначенням аналізу мережевого трафіка можна сформулювати так: метод відстеження мережевої активності, щоб виявити проблеми з безпекою та роботою та інші порушення.

Якщо взяти у приклад поштові сервери, то спосіб мережевого аналізу даних буде найбільш ефективним, через те, що можна відстежити та нейтралізувати шкідливі пакети\програми ще до потрапляння на комп'ютери користувачів.

Для цього використовують спеціальні пристрої, що називаються Network traffic analysis (NTA), які є одним з різновидів мережевих пристроїв безпеки, що використовують мережеві комунікації в якості основного джерела даних для виявлення та розслідування загроз безпеці, аномальної чи шкідливої поведінки мережі. Ці системи захищають мережу та її інфраструктуру шляхом виявлення загроз інформаційної безпеки. Забезпечують оперативне реагування на виявлені загрози, дотримання всіх політик безпеки. Ці пристрої можуть передавати всю необхідну інформацію про події, що відбуваються, до центру моніторингу та реагування.

Взагалі, існує декілька ключових функцій мережевих аналізаторів:

- Аналіз мережевих даних як реального часу. Для забезпечення точного виявлення, розслідування та реагування протягом невизначеного періоду часу, коли загрози можуть бути дійсно небезпечними, кожен

продукт NTA повинен проводити дослідження мережі на загрози в режимі реального часу.

- Повна видимість операцій. Для того, щоб аналізатор мережного трафіку забезпечував високоточне розуміння поведінки загроз, він повинен мати можливість бачити та аналізувати фактичний зміст мережевих взаємодій. Це означає, що потрібна повна видимість, починаючи з L2 і закінчуючи рівнем L7. Поряд з цим виконується декодування прикладного протоколу та розшифровка сучасних криптографічних стандартів.
- Безпечне, контрольоване розшифрування трафіку. Наразі понад 70% веб-трафіку зашифровано, і це число швидко зростає. Однією з основних цілей інструментів NTA є надання повної видимості, що означає, що кожен продукт класу NTA має здатність розшифровувати трафік для аналізу без шкоди.
- Нормальна поведінка та виявлення аномалій. Кожен пристрій Network traffic analysis повинен мати здатність моделювати базову діяльність пристрою та активність користувача з подальшим порівнянням нових спостережень з поведінкою, яка була прийнята за нормальну. Поведінкова аналітика – це найкращий спосіб отримати дієву інформацію про стан погроз у мережі.

Не всі інструменти для моніторингу мережевого трафіку однакові. Загалом їх можна розділити на два типи: інструменти на основі потоку та інструменти глибокої перевірки пакетів (DPI). Ці інструменти мають варіанти програмних засобів для зберігання історичних даних та системи виявлення вторгнень [4].

Насамперед рішення аналізу мережевого трафіку використовуються для моніторингу корпоративних мереж. Компанії використовують аналіз мережевого трафіку для запису та аналізу закономірностей мережевого трафіку та комунікацій між активами. Потім ці дані використовуються для виявлення та

протидії загрозам безпеки. Аналіз мережевого трафіку відстежує доступність і активність мережі, а також визначає порушення в роботі та безпеці. Сучасні рішення для аналізу мережевого трафіку постійно аналізують мережеву телеметрію та записи потоків, як-от NetFlow. Сучасний аналіз мережевого трафіку об'єднує всю зібрану інформацію для виявлення нерегулярної діяльності в мережі або ненормальних моделей трафіку. Потім пристрій або ініціює автоматичну відповідь, або сповіщає команди безпеки підприємства.

Моніторинг мережевих комунікацій на предмет незвичайної активності дозволяє вчасно виявляти та запобігати загрозам кібербезпеки. Аналіз мережевого трафіку фокусується на загальному спостереженні за трафіком, а не на моніторингу окремих частин мережі або активів, підключених до мережі. Це означає, що аналіз мережевого трафіку постійно відстежує та аналізує мережевий трафік і створює орієнтири для очікуваних моделей трафіку в різних ситуаціях.

Ці моделі потім використовуються як базова лінія для виявлення аномалій. Будь-яка незвичайна пляма позначається інструментами аналізу мережевого трафіку і може бути перевірена на предмет можливих проблем безпеки, тобто ретельного дослідження загроз. У цьому процесі рішення для аналізу мережевого трафіку аналізує виявлені проміжки, щоб визначити ймовірність загрози для мережі.

Рішення для аналізу мережевого трафіку випереджають інші інструменти безпеки мережі, такі як системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS) і брандмауери. Хоча ці інструменти в основному зосереджені на трафікі в межах периметра мережі, аналіз мережевого трафіку аналізує всі типи мережевого зв'язку, включаючи традиційні пакети TCP/IP, хмарний трафік, віртуальний мережевий трафік, а також взаємодії API та SaaS.

Крім того, аналіз мережевого трафіку дає уявлення про мережеві операції, пов'язані з мережами Інтернету речей (IoT) та подібними операційними технологіями. Без аналізу мережевого трафіку ці активи можуть бути сліпою

зоною для служби безпеки. Розширені інструменти аналізу мережевого трафіку навіть здатні аналізувати зашифрований мережевий трафік.

Продукти аналізу мережевого трафіку враховують кожну сутність у мережі, від користувачів і пристроїв до місць призначення, додатків тощо.

Це забезпечує величезну цінність у порівнянні зі статичними списками IP-адрес та іншими традиційними методами безпеки мережі.

Отже аналіз мережевого трафіку визначається як метод відстеження мережевої активності для виявлення проблем із безпекою та функціонуванням, а також інших порушень.

2.2 Network Tap

Мережевий TAP – це апаратний інструмент, який дозволяє отримувати доступ до мережевого трафіку та відстежувати його. TAP одночасно передають потоки даних для надсилання та отримання по окремих виділених каналах (рисунок 2.1), забезпечуючи надходження всіх даних на пристрій моніторингу в режимі реального часу.

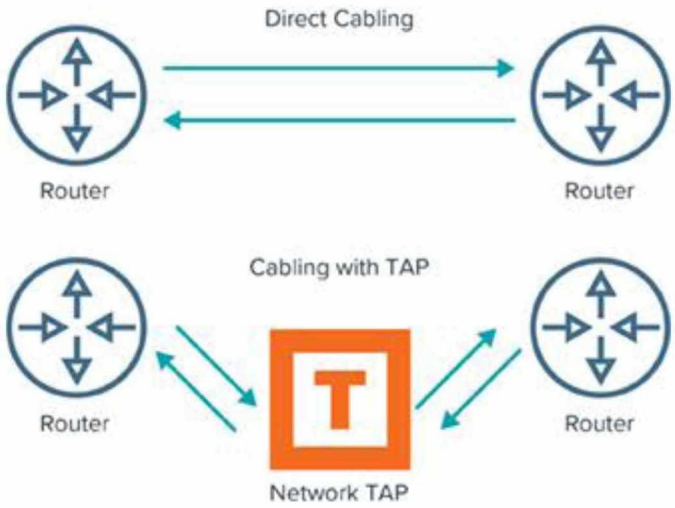

Рисунок 2.1 – принципова схема підключення Network Tap

Одною з гілок розвитку мережевого аналізатора є Network Tap (Net Tap, мережевий кран, або просто TAP), повна назва «Traffic Access Point» або «Test

Access Point», що являє собою пристрій, що встановлюється у відведене місце мережі та збирає данні для тестування і вирішення проблем. TAP (тестові точки доступу), широко відомі як Ethernet або мережеві TAP, є автономними апаратними пристроями, які створюють точну копію всього трафіку, що протікає між двома кінцевими точками в мережі. Зазвичай вони користуються перевагою, оскільки вони незалежні від мережі, що робить їх повністю настроюваними [4]. Скопійований трафік з TAP може піддаватися складним маніпуляціям з пакетами, оскільки він виводиться на різні мережеві інструменти; такі як засоби безпеки та продуктивності.

Мережні TAP, зазвичай, використовуються для систем виявлення вторгнення в мережу (NIDS), мережевих зондів, зондів віддаленого моніторингу мережі (RMON) і запису голосу через Інтернет-протокол (VoIP).

Мережні TAP поділяються на чотири основні типи:

- розривні TAP: найпростіша форма мережевих відводів, розривні TAP пристрої зазвичай складаються з двох вхідних і двох вихідних портів,
- агрегування TAP: ці TAP пристрої збирають інформацію про мережевий трафік з кількох сегментів і об'єднують її в один порт моніторингу за допомогою єдиного інструменту моніторингу,
- відводи регенерації: ці TAP пристрої збирають інформацію про трафік лише один раз з одного сегмента та надсилають її на різні пристрої моніторингу для аналізу даних,
- відводи V-Line: вони дозволяють TAP пристрою підключати віртуальний вбудований мережевий пристрій;

Мережеві TAP бувають різних форм і конфігурацій:

- пасивні TAP: підтримують позасмугові пристрої «лише прослуховування», які використовуються для інструментів моніторингу, вони прості, надійні та не потребують живлення,

- активні TAP: підтримують вбудовані пристрої, що використовуються для додатків безпеки, і включають технологію обходу або безвідмовної безпеки,
- різні типи носіїв, мідь або волокно (LC, MTP/MPO, BiDi), і можуть виконувати перетворення медіа,
- різні швидкості від 10/100/1000M аж до 400G,
- різні форм-фактори, включаючи портативні, 1/2 стійки, 1U та 2U рішення для корпусів;

Кожен тип мережевого TAP працює по-різному, залежно від вимог, які йому необхідно виконати.

Є декілька режимів роботи мережевих там в залежності від конфігурацій та типу:

- проривні «звичайні» TAP: переконайтеся, що жоден пакет не буде втрачено високопріоритетними інструментами моніторингу,
- фільтрування TAP: дозволяє встановлювати правила щодо того, які дані фільтруються та надсилаються до інструментів моніторингу чи безпеки. Фільтрація запобігає переповненню портів
- агрегаційні TAP: об'єднуйте потоки трафіку в один порт моніторингу, щоб зменшити витрати пристрою, часто використовується в поєднанні з фільтруючими TAP, тобто: фільтр, зведені потоки даних,
- regeneration/SPAN TAPs: створюйте кілька копій мережевих даних для підтримки кількох пристроїв з однієї точки підключення,
- обхід TAP: запобігає вбудованим пристроям від простою мережі, якщо вони виходять з ладу або потребують оновлення;

Мережеві TAP є базовим рівнем інтелектуального доступу до мережі і можуть відстежувати різні події в локальній мережі, що означає повну видимість на всіх мережевих платформах безпеки та моніторингу, що є життєво важливим для продуктивності будь-якої мережі.

Мережевий TAP зазвичай має чотири порти. Перші два порти підключаються до двох мережевих вузлів на обох кінцях дроту, який контролює TAP. Додаткові порти підключаються до пристроїв моніторингу, які отримують дзеркальні потоки пакетів [5].

Пасивне мережеве відведення є альтернативою дзеркального відображення портів, які в Cisco називають портом аналізатора комутованого порту (SPAN), які доступні на багатьох комутаторах і маршрутизаторах . На відміну від дзеркал портів і портів SPAN, відведення не залежить від ресурсів обробки комутатора або маршрутизатора для створення дзеркального трафіку.

2.3 Переваги та недоліки TAP відгалужувачів

Найпоширенішим способом вирішення проблем моніторингу є використання технології інверсії трафіку (SPAN). Різним фахівцям потрібна копія трафіку, щоб вирішити свої проблеми: безпека, фільтрація вмісту, виявлення вторгнень, усунення несправностей, а кількість портів SPAN зазвичай обмежується одним або двома.

Крім того, SPAN (Switch Port Analyzer) має ще один недолік, який полягає в втраті пакетів у разі перевантаження порту або в разі помилок в ньому, наприклад контрольної суми. Тому, якщо працювати в швидкісних каналах зв'язку і шукати абсолютно погані пакети, то їх просто не побачимо. В результаті «некоректної роботи» спеціалісти пропускають частину трафіку користувача, що не дозволяє виявити критичні помилки в мережі, а спеціаліст з безпеки може втратити вірусний трафік або піддатися атаці зловмисника.

Деякі погані спеціалісти пропонують використовувати концентратор, але він не працює зі швидкістю 1 Гбіт/с і не працює в повному дуплексному режимі, тому це рішення для починаючих та IT-фахівців у компанії з двох осіб.

Відгалужувачі трафіку не мають описаних вище проблем, крім того, вони можуть мати ще й інтелект, що дуже корисно в сучасних мережах. Ми гарантуємо отримання 100% трафіку на будь-якій швидкості. Треба відзначити,

що пасивний розгалужувач не знижує надійність каналу, жодним чином не впливає на його навантаження, а пасивні розгалужувачі взагалі не потребують живлення. Відгалужувачі є дуже простими для користувача пристроями і не вимагають спеціального налаштування, необхідно лише підключити та почати працювати [6]. Вони підтримують швидкість передачі трафіку від 10 Мбіт/с до 100 Гбіт/с. З постійно підключеним TAP-пристроєм можна не боятися відключати мережу в ті моменти, коли інженер підключає і відключає засоби моніторингу мережі.

Також перевага TAP пристроїв - їх використання для моніторингу трафіку без будь-яких перешкод. Однак є і недоліки. Їх використання дороге, оскільки вони потребують додаткового обладнання. Для моніторингу великої мережі через мережеві TAP потрібні різні пристрої моніторингу. Крім того, розміщення мережевого відводу на короткий час також може перервати мережевий трафік, тоді як повністю пасивні мережеві відводи можуть навіть викликати збій у мережі, вводячи нові точки збою.

Якщо наводити переваги списком, то ось, які переваги його використання [N2.4]:

- TAP отримують всі дані, включаючи великі кадри та помилки,
- TAP не викликають затримок у мережі, затримок чи проблем із часом,
- TAP не змінюють тимчасові відносини кадрів, інтервал і час відгуку,
- TAP схвалені судом для розгляду справ CALEA та законного перехоплення,
- TAPS не має IP або Mac-адреси і не може бути зламаний,
- підтримки дроту, мережеві TAP доступні в 10/100M, 10/100/1000M Copper і 1G, 10G, 40G, 100G і 400G Fiber;

2.4 Пасивні мережеві TAP

Мережевий TAP — це спеціально створений пристрій, який розташовано між двома точками мережі та надсилає мережеві дані зовнішнім пристроям, не перериваючи потоків трафіку. Пасивний TAP просто робить копію мережевих даних і розповсюджує їх до сторонніх пристроїв, вони не забирають змінений трафік із пристрою та не надсилають його в мережу.

Пасивні TAP – це TAP, який не призведе до втрати зв'язку між спостережуваними пристроями у разі втрати живлення. Це досягається під час моніторингу двох пристроїв, підключених за допомогою волоконної оптики, або двох пристроїв із мідними інтерфейсами 10 або 100 Мбіт/с.

Деякі пасивні TAP не вимагають джерел живлення. Однак, якщо TAP потребує виконання додаткових послуг, крім простого копіювання та надсилання даних, їм знадобиться живлення. Незважаючи на це, пасивні мережеві TAP розроблені так, що навіть якщо середовище втрачає живлення, мережеві пристрої не втрачають зв'язок. Мережні пристрої ніколи навіть не дізнаються, що мережевий TAP втратив живлення. Принцип дії пасивного мережевного TAP відображено на рисунку 2.2.

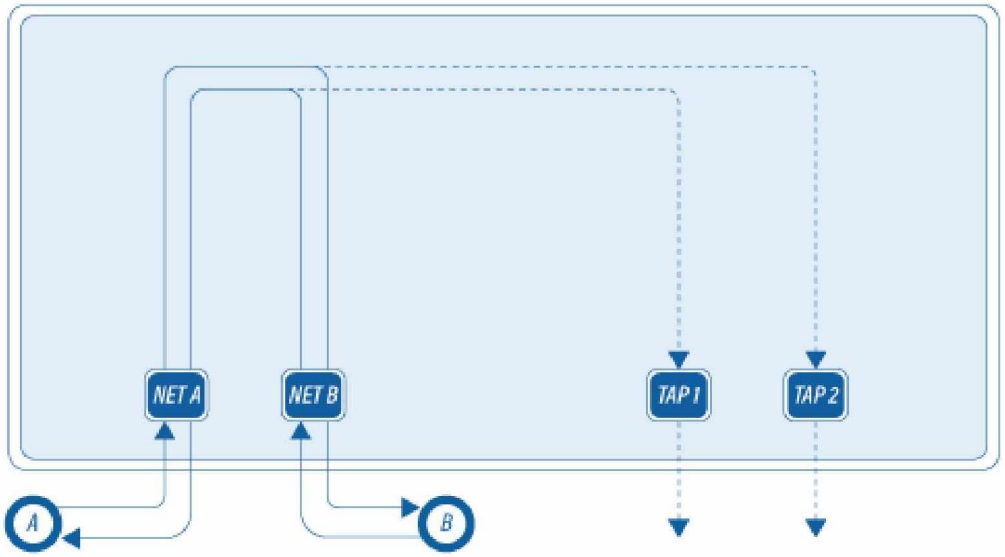

Рисунок 2.2 – Принцип дії пасивного мережевного TAP

2.5 Пасивні TAP в оптоволоконних мережах

Пасивні мережеві TAP можна використовувати в оптоволоконних мережах будь-якої швидкості (1 гігабіт, 10 гігабіт; 40 гігабіт, 100 гігабіт тощо). Якщо це все, що має робити TAP – і в волокні достатньо світла, щоб розділити його без погіршення стану мережі – немає потреби живити пасивний TAP взагалі. Для компаній із переповненими шафами електропроводки та обмеженою доступністю розеток цей дизайн мережі пропонує величезні переваги.

Однак, якщо в оптоволокні недостатньо світла або воно повинно проходити занадто далеко, щоб досягти кінцевого пункту призначення, знадобиться пасивний TAP з живленням.

Деякі мережі вимагають перетворення медіа, щоб перевести мережевий трафік до призначеної точки моніторингу. Наприклад, якщо трафік з оптоволоконної мережі потрібно надіслати на пристрій з мідними вхідними портами, TAP перетворить оптоволоконну сигналізацію на електричну, оскільки мідь є електричним інтерфейсом. Якщо мережа використовує багатомодове волокно для транспортування, і необхідно використовувати одномодове волокно для передачі трафіку до пристрою моніторингу, TAP перетворить оптичний сигнал з багатомодового в одномодовий. Хоча перетворення медіа легко виконується в пасивній мережі TAP, для цього потрібно мати живлення.

Також важливо відзначити, що стандартна пасивна мережа TAP відправляє два потоки трафіку до інструментів моніторингу. Рух зі сходу на захід і із заходу на схід. Якщо є лише один порт на інструменті моніторингу, можна використовувати один із TAP агрегації, щоб об’єднати трафік із заходу на схід і зі сходу на захід в один потік.

2.6 Пасивні TAP в мідних мережах

Пасивну мережу TAP можна використовувати в будь-якій оптоволоконній мережі, у мідних середовищах це не так просто. Пасивні TAP можна використовувати в мідних мережах, але вони завжди повинні мати живлення.

І тут виникає проблема швидкості. Пасивні мережеві TAP можуть бути розгорнуті в мережах 10/100 Base-T , але вони не можуть бути розгорнуті в середовищі мідних гігабіт. У цих мережах компанії повинні використовувати активний мережевий TAP, щоб забезпечити інструменти моніторингу з необхідною видимістю [7].

Забезпечення безвідмовної роботи Gigabit Copper TAPS:

Мережевий TAP для мідних гігабітних інтерфейсів, важливо використовувати такий, що має безпечну схему, яка відповідає стандартам ЦОД. Наприклад, безпечна релейна схема Garland, що вбудована в гігабітні мережеві TAP – у разі втрати живлення схема реле замикається менш ніж за 8 мілісекунд, забезпечуючи з'єднання між елементами мережі. Це гарантує безперервний рух пакетів в разі відключення електроенергії. [8]

Звичайно, найнадійнішим методом є розгортання всіх мережевих TAP через стійку, оснащену подвійними джерелами безперебійного живлення (UPS).

Щоб обійти потребу в живленні, деякі мережеві TAP оснащуються приєднаними літієвими акумуляторами до пасивного TAP замість того, щоб підключати його до джерела живлення. Зрозуміло, цей метод не відповідатиме стандартам ЦДК – рівень збоїв занадто високий, щоб довіряти.

2.7 Активні мережеві TAP

Підключення до мережі має вирішальне значення для будь-якого проекту безпеки або моніторингу мережі.

Активні мережеві TAP необхідні, якщо є одна з таких умов:

- розгортається вбудований пристрій безпеки, наприклад IPS або брандмауер. У цьому випадку активний TAP класифікується як обхідний TAP,
- відстежується мідний гігабітний сегмент. Гігабітна мідна мережа – це особливий випадок, який вимагає, щоб дві кінцеві точки, які контролюються, підключалися до TAP, незалежно від програми,
- буде використовуватися інструмент моніторингу, який впроваджує пакети в мережу, наприклад пакети скидання TCP;

Необхідно розглядати активний мережевий TAP як TAP, який фізично пов'язаний із контрольованими пристроями. У разі втрати живлення TAP має власну безпечну схему, яка з'єднує два контрольовані пристрої разом, щоб трафік продовжував надходити.

Активні TAP вимагають потужності для підтримки додаткових функцій, таких як агрегація та регенерація, а також розширених функцій, таких як фільтрація та обхід [9].

Суть розгортання мережевих TAP будь-якого типу полягає в тому, щоб забезпечити повну видимість для будь-яких підключених пристроїв. Ці спеціально створені пристрої вставляють безпосередньо в мережу, щоб забезпечити повний доступ до даних про трафік у джерелі. На відміну від портів SPAN комутатора або інших вторинних джерел, які можуть бути перевантажені під час стрибків трафіку, мережеві TAP передають 100% біт, байтів і пакетів, які вони бачать, безпосередньо підключеним пристроям безпеки або інструментам моніторингу мережі. На рисунку 2.3 зображено схему роботи активного мережевого TAP.

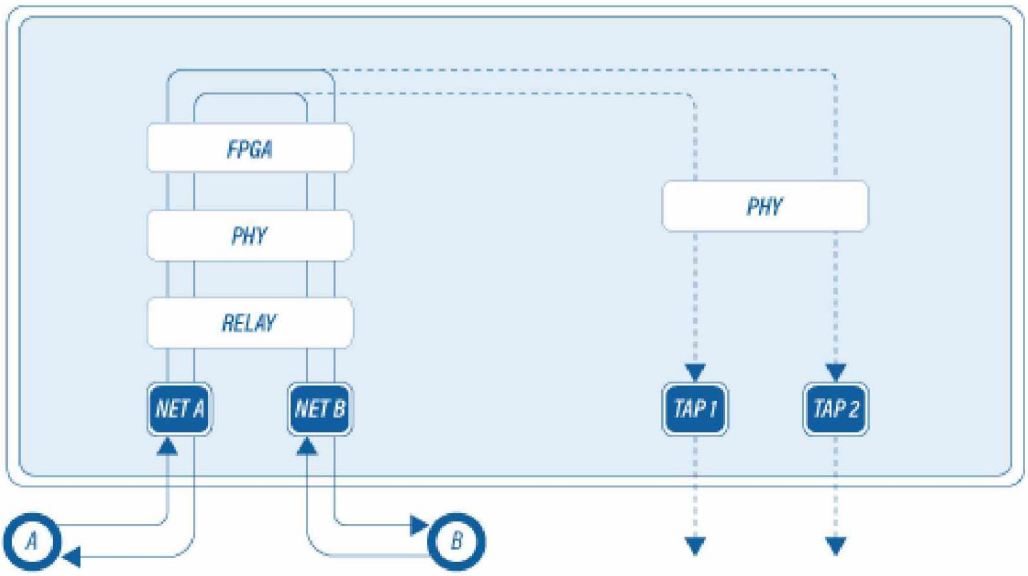

Рисунок 2.3 – Схема роботи активного мережевого TAP

Активні мережеві TAP часто розроблені для підтримки вбудованих програм безпеки, таких як брандмауери, пристрої для захисту від шкідливих програм, системи захисту від вторгнення тощо. Ці системи безпеки є унікальними, оскільки вони приймають трафік із зовнішнього світу та намагаються заблокувати підозрілі комунікації від проникнення всередину компанії. Природно, для цих пристроїв потрібен TAP, який може надавати їм мережевий трафік без втрати пакетів, але їм також потрібне рішення, здатне приймати авторизований трафік, а також повідомлення від пристрою та дозволяти їм подорожувати до цільового призначення. Тільки активний мережевий TAP може полегшити цей тип зв'язку.

Особливості активних мережевих TAP:

- усі активні мідні TAP мають безпечну функцію під назвою No Break, яка є механізмом швидкого перемикання, який активується у разі повного відключення електроенергії. На відміну від звичайних функцій безпеки на більшості TAP, функція No Break перемикається набагато швидше, тому це не призводить до повторного узгодження з'єднання з мережею. Технологія заснована на наборі реле, які залишаються відкритими під час живлення пристрою. Коли живлення вимикається, ці

реле перемикаються на прямий потік трафіку через TAP, щоб мережа продовжувала працювати,

- організації, які прагнуть забезпечити підключення для пристроїв безпеки або моніторингу мережі у високошвидкісних мідних середовищах , повинні використовувати активний мережевий TAP незалежно від того, чи є пристрій вбудованим чи позасмуговим. Пасивні TAP не можуть бути розгорнуті в гігабітних середовищах міді через те, що дані одночасно передаються та отримуються по мідних парах – кінцеві точки не отримують чіткого уявлення про те, що відбувається і що відбувається;

На відміну від деяких пасивних TAP, всі активні мережеві TAP вимагають живлення для функціонування. Це означає, що вам потрібен безпечний механізм, щоб переконатися, що ви не ввели можливу точку збою в мережі. Усі активні TAP були розроблені для розпізнавання перебоїв живлення та автоматичного замикання ланцюга реле менш ніж за 8 мілісекунд, забезпечуючи пасивне з'єднання між двома вашими елементами мережі. Це забезпечує безперебійну роботу мережі, поки адміністратори мережі вирішують проблему втрати живлення.

Незважаючи на те, що всі мережеві TAP мають однакову потребу – гарантуючи, що підключені пристрої отримують 100% даних про трафік, які їм потрібні для своєї роботи – вам потрібно вибрати той, який найкраще підходить для вашої програми та середовища.

2.8 Різниця пасивного та активного мережевого відгалужувача

Обидва типи TAP працюють по суті однаково, розділяючи частину сигналу на аналізатор мережевого трафіку, в той час як основний сигнал продовжується безперервно. Для пасивних TAP світловий промінь фізично ділиться на дві частини, тоді як для активних TAP електричний сигнал копіюється.

Отже, різниця пасивного і активного мережевого відгалужувача:

- пасивний мережевий TAP не має фізичного розділення між мережевими портами. Коли живлення пристрою буде втрачено, мережеве з'єднання буде працювати без затримки. Він не вимагає додаткового живлення,
- активний мережевий TAP має фізичне розділення між мережевими портами через реле та інші електронні компоненти всередині пристрою. Для повноцінної роботи TAP потрібне додаткове живлення;

2.9 Види мережевих відгалужувачів

Коли згадується тема мережевих TAP (тестових точок доступу або точки доступу до трафіку), люди можуть подумати про пристрій, який «підключається до мережі», щоб забезпечити видимість пакетів, надсилаючи копії трафіку на аналізатор.

Видимість мережі швидко стала основою сучасної архітектури мережі та безпеки. Хоча багато людей можуть не думати про варіанти оптимізації, TAP також надає інженерів та архітекторів, оскільки вони планують найкращий спосіб підключення до мережі.

Види мережевих TAP:

2.9.1 TAP 'Breakout'

Це типовий варіант використання, для якого люди використовують мережевий TAP. Стандартний TAP складається з чотирьох (4) портів A, B, C і D. Порти A і B є мережевими портами, а C і D — портами монітора (рисунок 2.4).

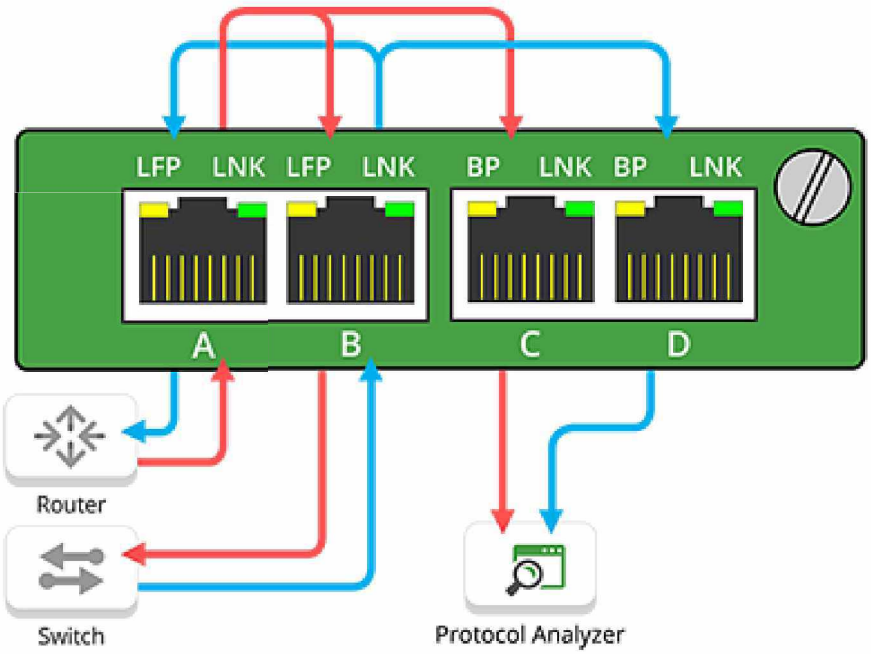

Рисунок 2.4 - TAP 'Breakout'

Проста реалізація Breakout TAP

- Східний трафік від мережевого пристрою, в даному випадку маршрутизатора, надходить у мережевий порт A і витікає з мережевого порту B на інший мережевий пристрій, у цьому випадку мережевий комутатор.
- Потім порт B надсилає його на порт C моніторингу.
- Трафік, який перетікає від мережевого порту B до мережевого порту A та надсилає його на порт D моніторингу.

Цей TAP зазвичай використовується, коли трафік на приєднаному посиланні достатньо інтенсивний, щоб спричинити перевищення підписки, якщо трафік надсилання та отримання об'єднано в один моніторний порт. Цей TAP вимагає, щоб інструмент або пристрій, до якого він підключений, вимагали двох мережевих інтерфейсних карт (NIC), щоб захоплювати потоки трафіку як на схід, так і на захід.

2.9.2 Aggregation (агрегаційні) TAPs

Щоб взяти трафік, який надходить від портів A до B і B до A, і об'єднати їх разом в один порт моніторингу. Поки об'єднаний трафік не перевищить передплату на порти монітора, TAP надсилатиме весь трафік на підключений інструмент або пристрій. Оскільки весь трафік може бути відправлений через один порт, TAP може надсилати весь трафік на два пристрої моніторингу (рис 2.5).

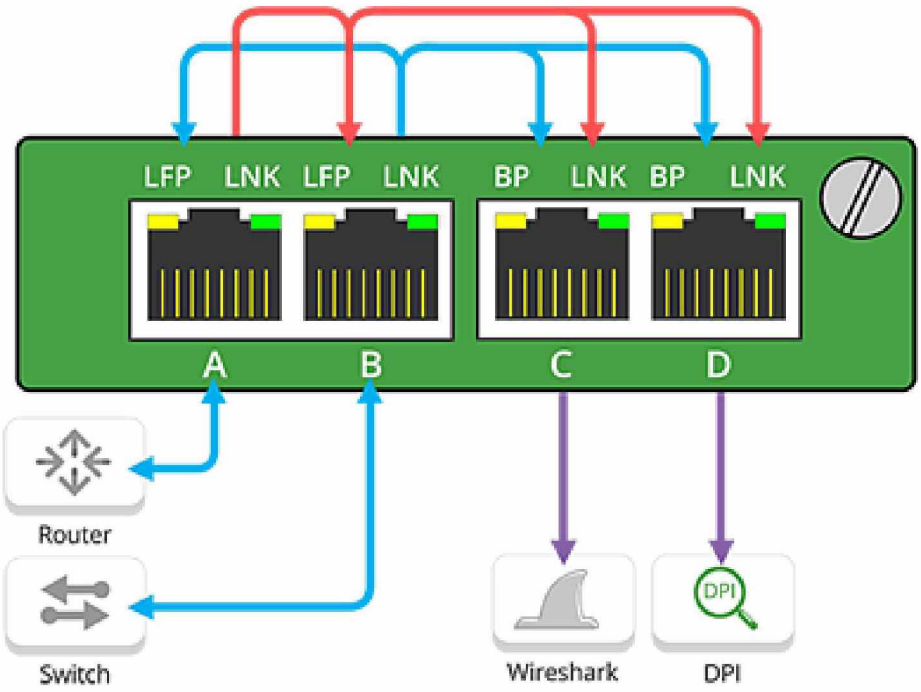

Рисунок 2.5 – Агрегаційниі TAPs

2.9.3 Replicating/SPAN (реплекаційні) TAP

Часто на мережевому маршрутизаторі чи комутаторі не вистачає портів SPAN для доступу до кількох інструментів і пристроїв аналізатора. Зручний спосіб вирішити цю проблему — надіслати SPAN або дзеркальне введення на реплікаційний TAP. Трафік на вході SPAN тепер можна розподілити на три (3) різні інструменти (рис. 2.6).

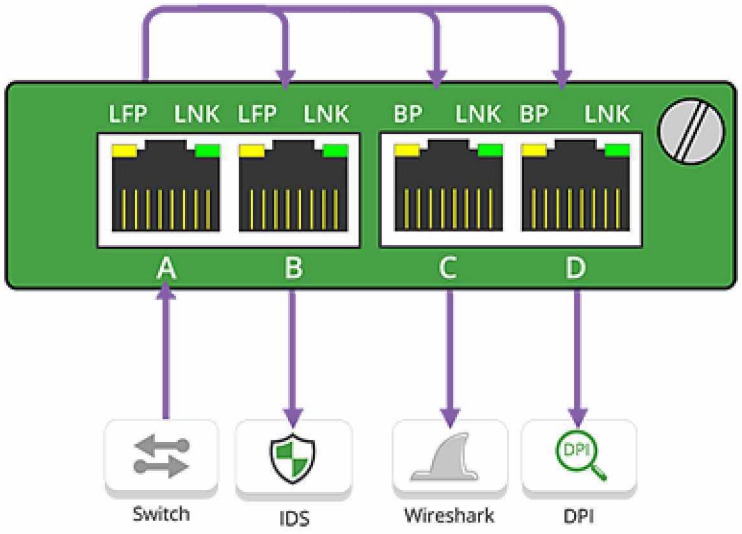

Рисунок 2.6 – Реплікаційний TAP

2.9.4 Filtering (фільтруючі) TAPs

Мережні TAP призначені для копіювання всіх ваших даних, але часто вашим інструментам не потрібно бачити «все». Ваш VoIP або Wireshark повинні бачити лише трафік, необхідний для виконання своєї роботи. Саме тут унікальна фільтрація є бажаною функцією, оскільки ви можете відфільтрувати те, що не потрібно інструменту, гарантуючи, що порти моніторингу не будуть переповнені.

Цей сценарій (нижче) показує чотири канали 1G із застосованим фільтром, який потім об’єднано разом і надіслано порт D на TAP 4 до інструменту моніторингу (рис 2.7).

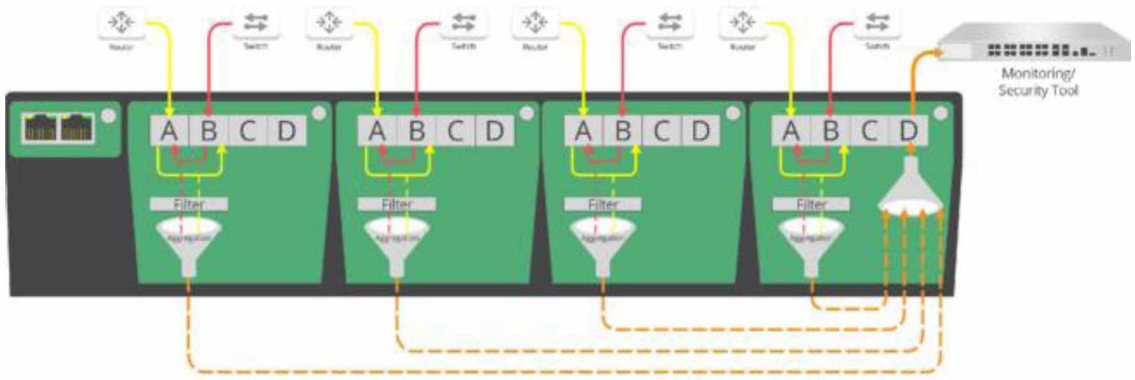

Рисунок 2.7 – Сценарій роботи фільтруючого TAP

2.9.5 Bypass (обхідні) TAP

Важливий інструмент, який дозволяє розміщувати активні вбудовані пристрої в критичну ланку без введення SPOF (єдиної точки збою). У випадку, коли ви хочете встановити вбудований пристрій , як-от брандмауер наступного покоління (NGFW) або систему запобігання вторгненням (IPS), пристрій має бути активно вбудованим, щоб виконувати свою роботу з активного блокування загроз. Проте, якщо пристрій активний, вбудована мережа може запобігти збою в мережі, якщо пристрій виходить з ладу, зв'язок переривається або вам потрібно перевести його в режим офлайн або поза смугою для оновлення або усунення несправностей.

Обхід TAP із захистом від збоїв запобіжить цьому. Обхідний TAP вставляє пакет серцевого ритму в трафік, який він відправляє на вбудований пристрій, і поки вбудований пристрій перебуває в мережі, пакет серцевих скорочень повертатиметься до TAP. TAP видалить серцевий пакет перед відправкою трафіку назад у мережу. Якщо щось піде не так з TAP або інструментом, функція захисту від збоїв TAP забезпечить протікання каналу (мережевого трафіку), принцип дії показано на рисунку 2.8.

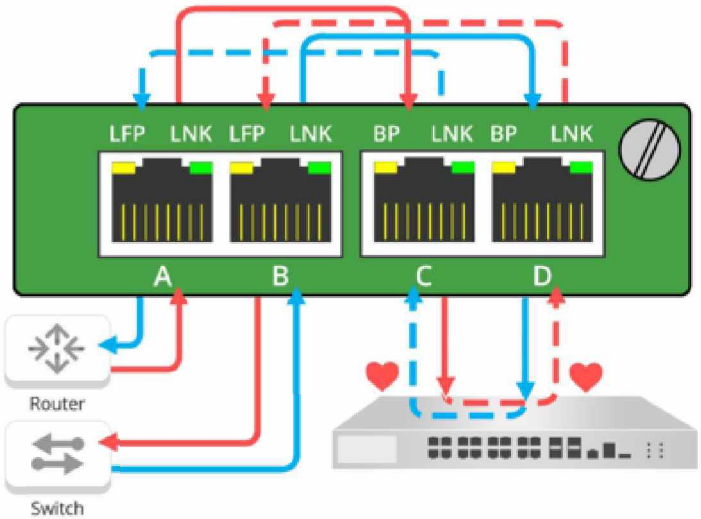

Рисунок 2.8 – принцип дії обходного TAP

2.9.6 Media Conversion (медіа-конверсійні) TAP

Є одномодове оптоволоконне мережеве з'єднання з розширеним діапазоном, яке тягнеться приблизно на 10 км. Але ваш аналізатор мережі знаходиться в двох футах від вас. Першим варіантом може бути придбання трансиверів для відповідності посиланням; однак це дорогий і неефективний підхід. Або більш поширене, перетворення оптоволоконного каналу на порти моніторингу міді, що дозволить вам все ще використовувати свої мідні інструменти та прилади. Це лише один із сценаріїв перетворення медіа з використанням мережевого TAP (рисунок 2.9).

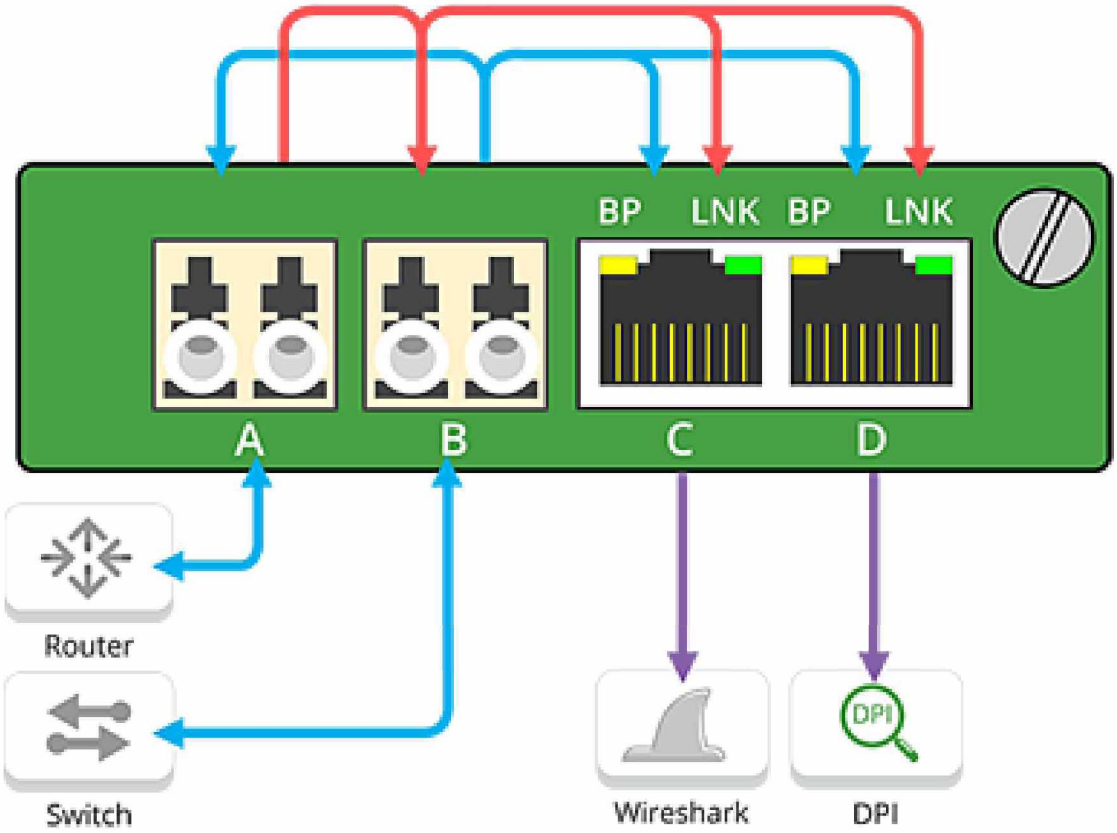

Рисунок 2.9 – Медіа конверсійний TAP

Перетворення медіа з одного режиму в SFP: перетворити одномодове волокно в багатомодове так само шляхом розгортання TAP, який має одномодові мережеві порти та порти моніторингу SFP, як показано нижче (рис 1.8).

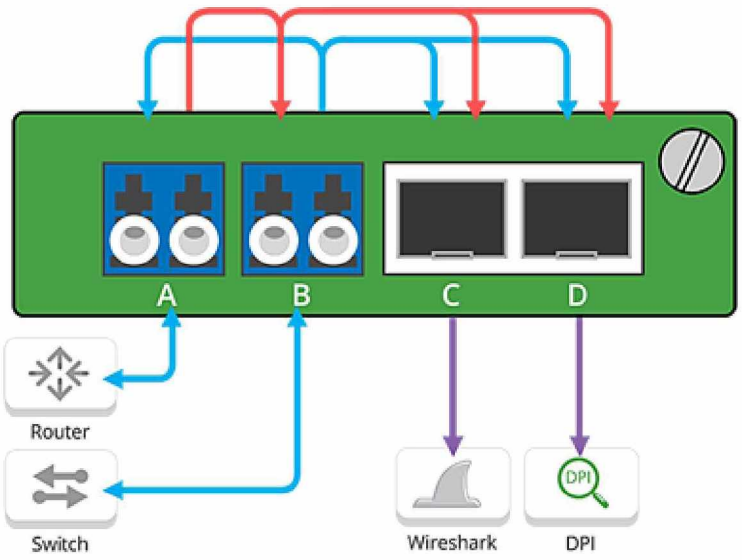

Рисунок 2.10 – Перетворення медіа з одного режиму в SFP

Перетворення медіа з міді в SFP: необхідно взяти мідний канал і перетворити його в одномодове або багатомодове волокно за допомогою TAP, який має порти мідної мережі та порти моніторингу SFP, як показано нижче (рисунок 2.11).

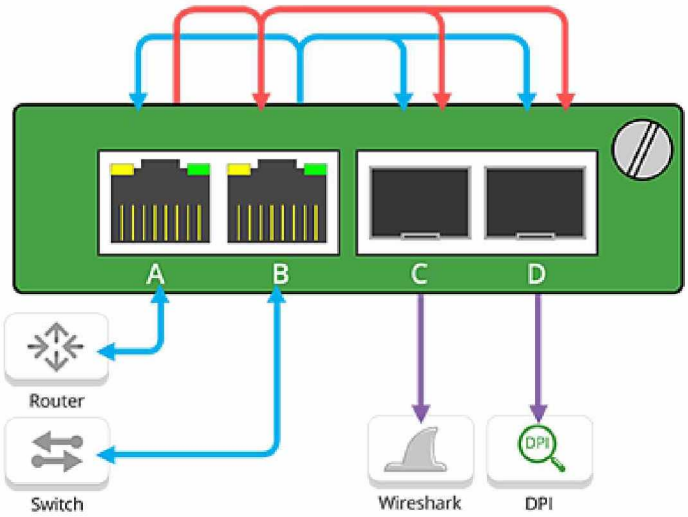

Рисунок 2.11 – Перетворення медія з міді в SFP

Окрім усіх різних типів TAP, також важливо, що TAP має бути здатним виконувати дуже важливе завдання, він не повинен створювати «точку відмови». Якщо щось піде не так з TAP, поточний трафік має продовжувати текти. А у випадку байпасного TAP, якщо щось піде не так з вбудованим приладом, зв’язок має продовжувати працювати.

РОЗДІЛ 3. РОЗРОБКА ПРОГРАМНОГО МЕТОДУ ТА ТЕХНІЧНОГО РІШЕННЯ ДЛЯ АНАЛІЗУ ЗАХИЩЕНОСТІ МЕРЕЖЕВОГО ТРАФІКУ

У цій роботі буде висвітлюватися те, як саме зібрати власний пристрій мережевого відгалужувача та підключити його до своєї власної мережі. Окрім цього буде продемонстровано, що навіть звичайний комп'ютер або ноутбук зможе стати гарним інструментом для прослуховування мережі, за допомогою якого можна буде продивится весь незахищений трафік.

3.1 Вибір та підготовка операційної системи

3.1.1 Вибір операційної системи

Під час інтернет серфінгу глобальної мережі було знайдено дві підходящі операційних систем, що могли б допомогти аналізувати трафік, а саме такі:

Ubuntu 20.04 – це гарний дистрибутив операційної системи Linux, що постійно оновлюється та має можливості встановлення всіх необхідних інструментів для аналізу трафіку.

Kali Linux – дистрибутив ОС Linux, призначений для спеціалістів із безпеки, тому поставляється з безліччю додатків для проникнення та тестування безпеки, які дозволяють його користувачам братися за роботу. Серед додатків Kali Linux є утиліти, що допоможуть проаналізувати трафік.

Так як під час навчання використовувалася Kali Linux, то у цій роботі буде показано, як проаналізувати трафік використовуючи цей дистрибутив.

3.1.2 Підготовка операційної системи

Першим кроком для встановлення операційної системи необхідно знайти флейш накопичувач об'ємом не менше ніж 8gb та встановити на комп'ютер програму для встановлення образу на флешку (rufus).

Після цього необхідно перейти на офіційний сайт Kali Linux (https://www.kali.org/get-kali/) та завантажити образ операційної системи.

Наступним кроком є встановлення образу на флешку, для цього:

- Відкрити rufus
- Підключити флеш накопичувач
- Обрати ISO образ завантаженого Kali Linux
- Обрати чекбокси: «Швидке форматування», «Створити завантажувальний диск» та «Створити розширену мітку та іконку пристрою»
- Натиснути кнопку «Старт»

Після створення завантажувальної флешки необхідно встановити операційну систему.

3.2 Створення мережевого відгалужувача

Для того, щоб зібрати власний мережевий відгалужувач, необхідно мати паяльний прилад, від двох до чотирьох метрів витої пари, чотири коннектори типу RJ-45 (або два, за умори використання накладної Ethernet розетки на два порти, які необхідно буде з'єднати меж собою) та два конденсатори 220pf.

Конденсатори необхідні для того, щоб змусити інтернет з'єднання працювати повільніше (до 100 МБ) [10] та цей пристрій зміг якісно скопіювати пакети до аналізатора (у цьому випадку комп'ютера, що буде переглядати пакети).

Під час збірки пристрою необхідно чітко дотримуватися схеми зображеної на рисунку 3.1.

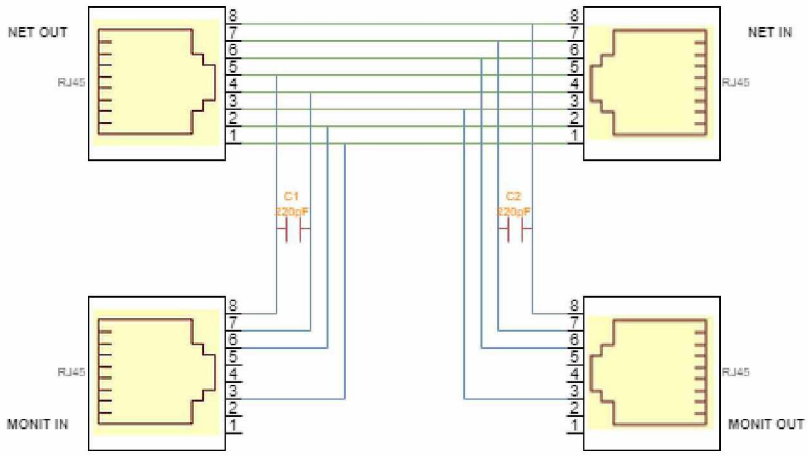

Рисунок 3.1 – Схема збірки пристрою

Якщо використовувати накладну Ethernet розетку, порти NET OUT та NET IN вже розпаяні на платі, необхідно лише додати два кабелі за схемою 2.1.

На цій схемі зображено порти с використанням стандарту T568B (рисунок 3.2), що є найрозповсюдженішим у наш час [11].

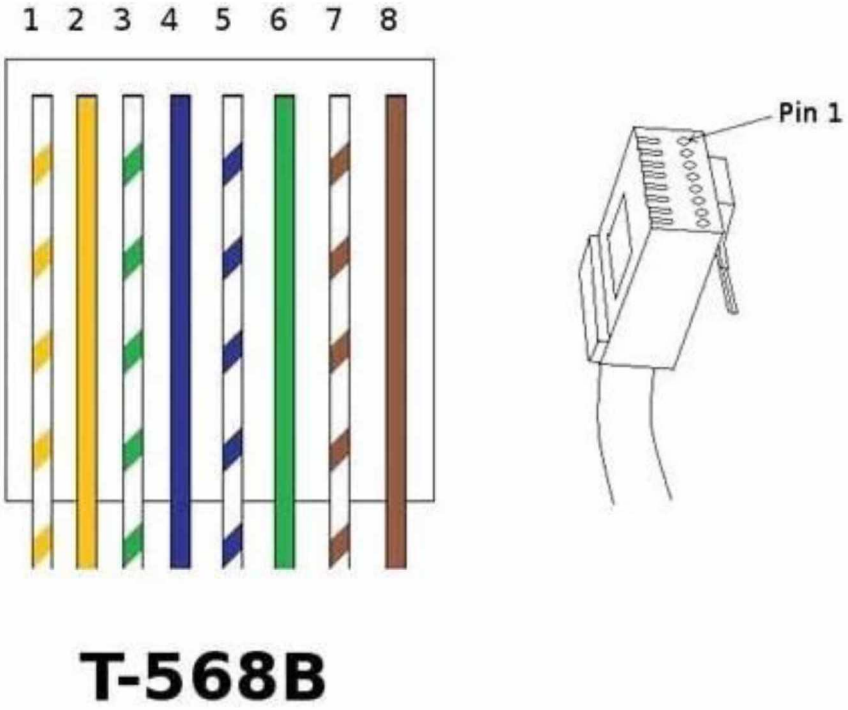

Рисунок 3.2 – Стандарт T568B

Невелике пояснення до пронумерованих провідників:

(1) Помаранчево білий: Надсилання дані +

(2) Помаранчевий: Надсилання даних -

(3) Білий і зелений: отримання дані +

(4) Синій: двонаправлені дані +

(5) Білий і синій: двонаправлені дані-

(6) Зелений: отримання дані-

(7) Білий і коричневий: двонаправлені дані +

(8) Коричневий: двонаправлені дані-

Насправді, для мережевого кабелю 100 М використовуються лише 1, 2, 3 і 6. Поки порти RX двох мережевих кабелів підключені до RX і TX цільового мережевого кабелю відповідно, усі дані можна прослуховувати. 4, 5, 7 і 8 в

гігабітному мережевому кабелі використовуються для двосторонньої передачі даних і схвалення даних. Саме тому необхідно використовувати два конденсатори 220pF, щоб перешкоджати комунікації, тому гігабітний мережевий кабель вважає, що якість зв'язку погана, і знижує від гігабіту до 100 МБ.

У випадку використання накладної Ethernet розетки на два порти схема залишається такою ж, але необхідно з'єднати два конектори один до одного 8-8, 7-7 і так далі. На рисунку 3.3 зображено фотографію готового пристрою в корпусі Ethernet розетки на два порти.

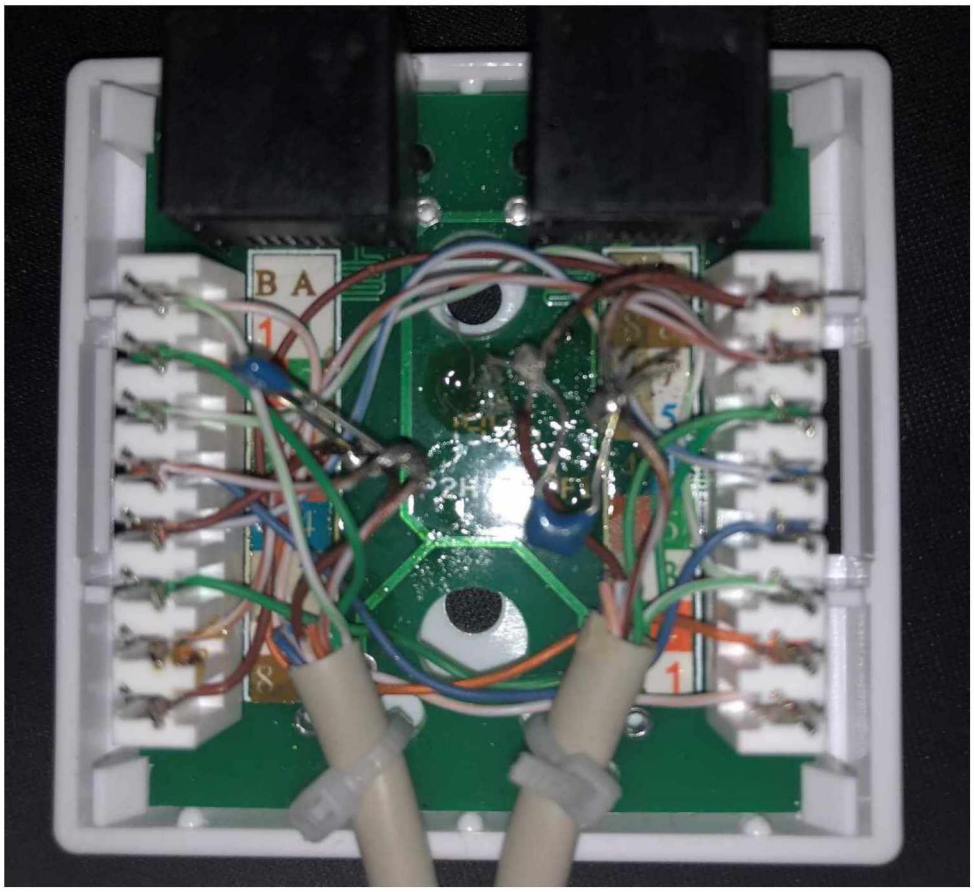

Рисунок 3.3 – Фотографія готового пристрою в корпусі

Така проста схема дозволить бути у мережі і не бути видим для пристроїв моніторингу мережі, бо цей пристрій фізично не може мати ні IP, ні MAC адрес.

Якщо дивитися з економічної точки зору, то саморобний пристрій коштує набагато дешевше. Всі компоненти доступні, дешеві та відказовідмовні.

Цей пристрій складається з:

- 4 метри мідної витої пари, середня ціна за один метр – 8 грн
- 2 Конденсатори 220pF – 16 грн
- Накладна Ethernet розетка (опціонально) – 75 грн
- Коннектори типу RJ45 (2-4 од) – 2 грн\од = 4 грн\ 8 грн

Як можна бачити , саморобний пристрій являє собою найдешевше рішення, що може зробити спеціаліст в край швидкий час у порівнянні з найдешевшими заводськими аналогами, його ціна варіюється від 56 до127 гривень.

3.3 Приклад роботи пристрою

3.3.1 Перевірка роботи пристрою

Для початку перехвату трафіку необхідно під'єднати пристрій в розрив з'єднання цільової мережі до глобальної мережі як показано на рисунку 3.4.

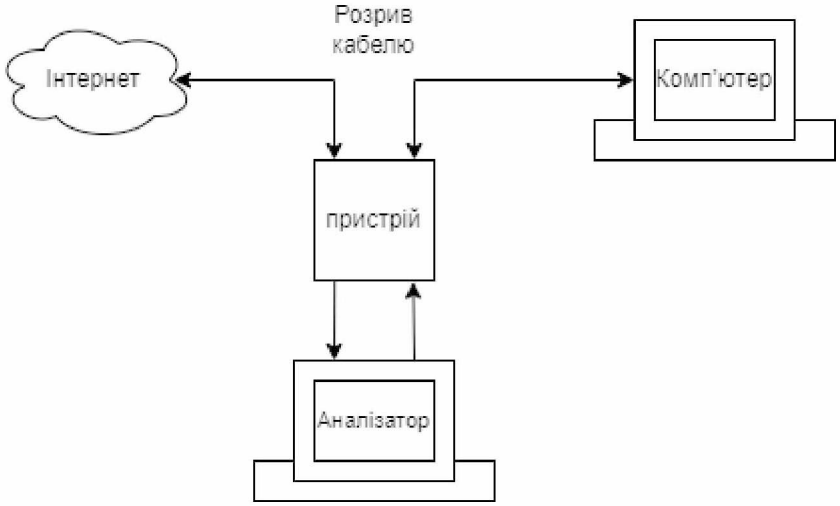

Рисунок 3.4 – Схема під'єднання пристрою до мережі

Після під'єднання для перевірки необхідно відкрити термінал на системі, яка буде копіювати трафік та вписати таку команди в два різні термінали:

```
sudo tcpdump -i eth0 -s 0 -w pingdump1.pcap
sudo tcpdump -i eth1 -s 0 -w pingdump2.pcap
```

Використовуючи вмонтовану в систему утиліту tcpdump можна прослуховувати мережеві інтерфейси та записувати весь трафік що проходить

по ним, тож ця команда забезпечить одночасний запуск двох синхронних процесів запису мережевого трафіку до двох різних файлів. Але можна і використати утиліту wireshark минаючи крок з використанням утиліти tcpdump, розпочавши перехоплення трафіку одразу у двох вікнах, кожне з яких перехоплює трафік по різним мережевим портам eth0 та eth1. У цій роботі буде використовуватися утиліта tcpdump для прикладу, але для відтворення ходу роботи можна нею не користуватися.

Отже почавши прослуховування, для перевірки необхідно запустити команду:

```
ping 8.8.8.8
```

Після виконання якої необхідно завершити прослуховування трафіку на пристрої копіювання.

Як результат, потоки входу та виходу, які записані до різних файлів, вміст фалів вихідного трафіку відображений на рисунку 3.5, а вхідного трафіку на рисунку 3.6.

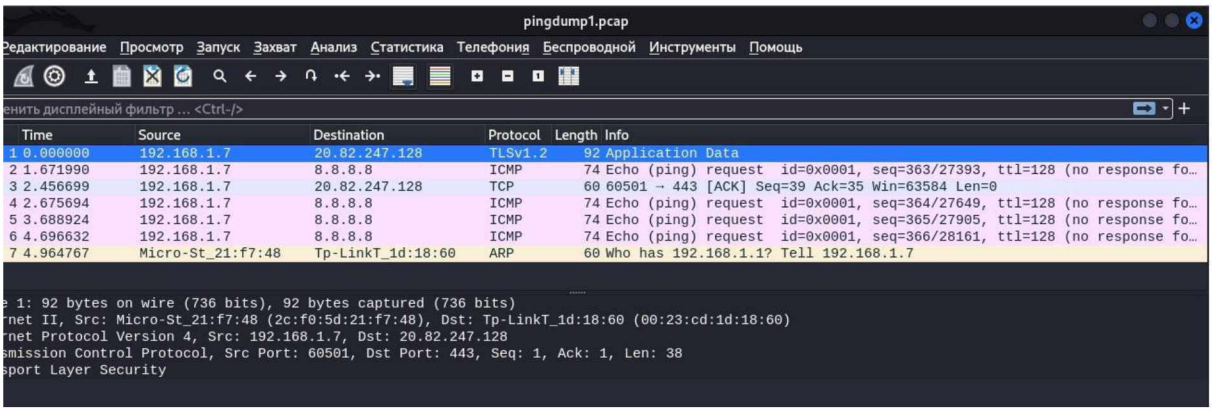

Рисунок 3.5 – Перевірка роботи пристрою. Вихідний трафік.

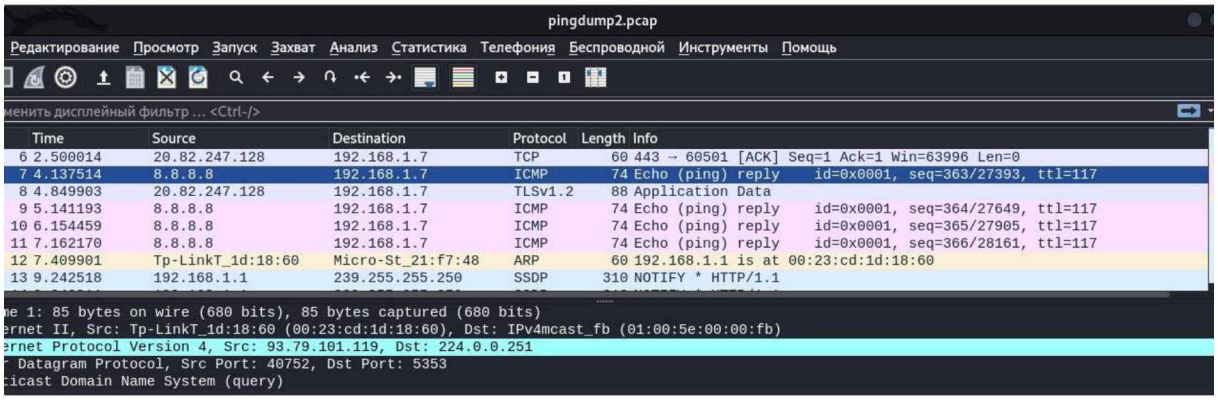

Рисунок 3.6 – Перевірка роботи пристрою. Вхідний трафік.

Як можна бачити на рисунку 3.5 та рисунку 3.6, канали входу та виходу записані у два різні файли, на першому зображено вихідний трафік, а саме те, що виходить з цільової мережі, колонка Sourse вказує на адресу комп'ютера, що відправив пакет, Destination – куди прямує пакет, в сусідній колонці вказано, який протокол було використано. У вхідному трафіку данні в колонках Sourse та Destination поміняні місцями.

На скріншотах видно, яка інформація міститься в цих пакетах, чітко можна побачити, що «Ping request» та «Ping reply» записані у різні потоки (файли), з чього можна сказати, що пристрій працює справно.

3.3.2 Перехват даних авторизації користувача по протоколу HTTP

Для перехвату даних авторизації користувача по протоколу HTTP достатньо пере авторизацією запустити команди (аналогічно з командами пункту 2.2.1):

```
sudo tcpdump -i eth0 -s 0 -w httpdump1.pcap
sudo tcpdump -i eth1 -s 0 -w httpdump2.pcap
```

Після запуску команди необхідно пройти авторизацію на сайті з протоколом http, як приклад http://www.altoromutual.com/login.jsp, а після авторизації завершити перехват трафіку.

Результат перехвату даних авторизації зображено на рисунку 3.7.

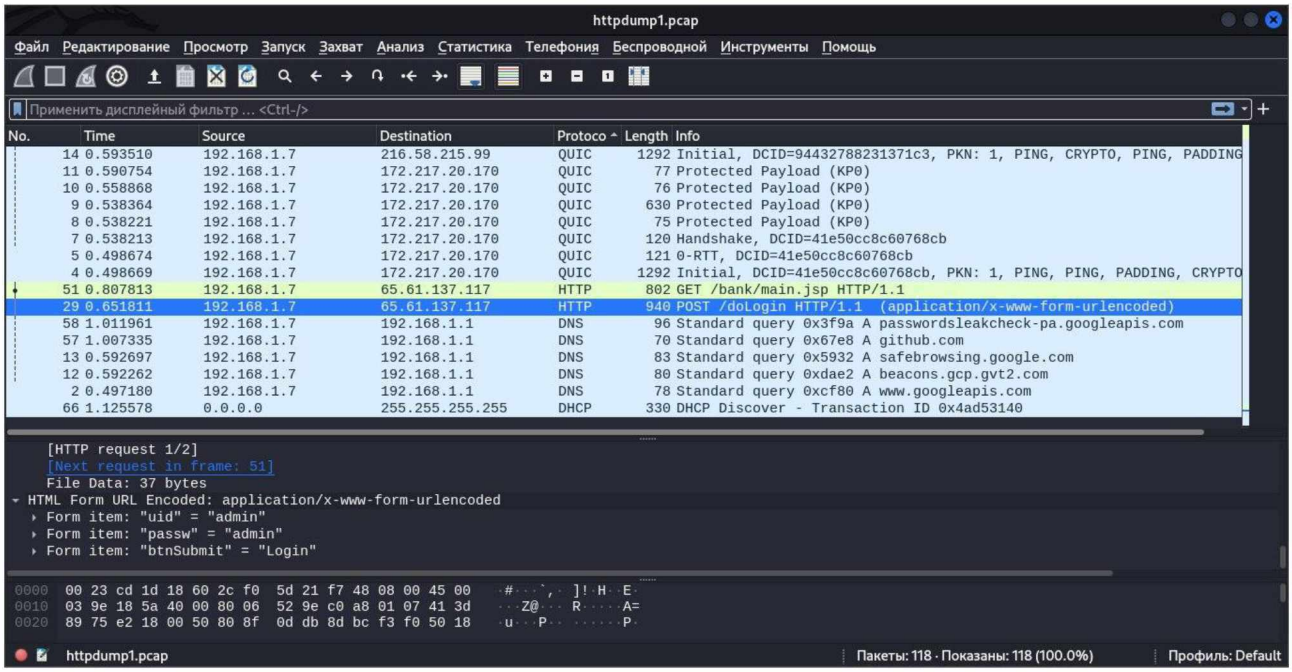

Рисунок 3.7 – Перехват даних авторизації.

На скріншоті 2.7 можна бачити спілкування цільової мережі з глобальною мережею, деякі захищенні данні (protected payload), а також інформацію, яка була відправлена методом POST протоколу HTTP, це свідчить про незахищений трафік, а назва сторінки, з якої було відправлено пакет – про спробу авторизації. Якщо продивитися зміст цього пакету, можна бачити данні авторизації, а саме: login: admin, password: admin та іншу менш корисну інформацію.

ВИСНОВОК

В ході цієї роботи було проаналізовано сукупність методів, приладів та програмного забезпечення для перехоплення, зберігання та аналізу мережевого трафіку після аналізу якого було розроблено прилад для його відгалуження на пристрій, що може зберігати цей трафік та в кінці частично проаналізувати отриману інформацію.

Кінцевою точкою роботи було продемонстровано роботу саморобного пристрою перехоплення трафіку, за допомогою якого можна переглядати трафік обраного користувача або мережі. Продемонстровано уразливість незахищених з'єднань між користувачами, які можуть недбало ставитися до захисту кабелю, що дає можливість зловмисникам підключитися до їх з'єднання та «читати» трафік, який надходить до та від цільової мережі.

На основі роботи можна розробити більш детальний аналіз цієї проблемі, що може стати у нагоді для майбутніх студентів, тобто служити підґрунтям для іншої випускної роботи або ж стати лабораторною роботою для студентів спеціальності «Кібербезпека», що дасть змогу студенту на практиці зрозуміти як саме виконується перехоплення трафіку та подальший його аналіз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Анализ первой в мире DDoS атаки [Електронний ресурс] – режим доступу https://medium.com/mit-technology-review/the-first-ddos-attack-was-20-years-ago-this-is-what-weve-learned-since-94a0b6e7f5fc

2 Kismet [Електронний ресурс] - режим доступу https://www.kismetwireless.net/

3 Що таке аналіз мережевого трафіку? [Електронний ресурс] – режим доступу https://www.toolbox.com/tech/networking/articles/network-traffic-analysis/

4 Розуміння мережевих TAP [Електронний ресурс] – режим доступу https://www.networkcritical.com/network-taps

5 мережевий кран [Електронний ресурс] – режим доступу https://www.techtarget.com/searchnetworking/definition/Network-tap

6 Переваги TAP-відповідачів та їх види [Електронний ресурс] – режим доступу https://iron-harry.ua/tap-otvetviteli-trafika-i-agregatory-chto-eto-takoe-i-kak-vybrat/

7 Переваги використання мережевого TAP [Електронний ресурс] – режим доступу https://www.garlandtechnology.com/2013/11/15/what-is-a-tap-anyway

8 пасивні мережеві TAP [Електронний ресурс] – режим доступу https://www.garlandtechnology.com/blog/the-101-series-passive-network-taps

9 Активні мережеві TAP [Електронний ресурс] – режим доступу https://www.garlandtechnology.com/blog/the-101-series-active-network-taps-where-when-and-how

10 Початок про мережеві TAP [Електронний ресурс] – режим доступу https://www.garlandtechnology.com/2014/01/17/a-test-access-point-tap-primer

11 Схема побудови NET TAP [Електронний ресурс] – режим доступу https://forum.90sec.com/t/topic/217