УДК 004.056.5:004.732:65.012.8
DOI: 10.31673/2409-7292.2023.030003

Захаржевський А. Г., Таванюк Д. М., Хворостяний Р. В.

ТЕХНОЛОГІЯ СНІФІНГУ У ЛОКАЛЬНІЙ МЕРЕЖІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ WIRESHARK

В роботі наведено структура та основні показники локальної мережі підприємства, засоби аналізу захищеності та виявлення її вразливості. Проаналізовані моделі загроз та визначенні ризики які можуть виникати при передачі інформації в мережі. Проаналізовано різні засоби снiфінгу та наведено їх класифікацію. На основі проведеного аналізу та досліджень розроблено рекомендації що до застосування методів та засобів протидії снiфінгу в локальній мережі підприємства. Галузь використання – кібербезпека локальних мереж.

Ключові слова: локальна мережа підприємства, загрози, кібербезпека, захист мереж, розслідування кіберзагроз, снiфінг, мережевий трафік, мережеві протоколи.

Вступ

Комп'ютери та Інтернет стали невід'ємною частиною роботи будь-якого підприємства. Вся інформація про організацію, а також результати її діяльності зберігаються на комп'ютерах, що робить їх цікавими для зловмисників, які бажають якимось чином отримати вигоду з інформації, що зберігається на них. Тому підприємства повинні контролювати свою інформаційну систему, щоб забезпечити її захист та запобігти можливим несанкціонованим вторгненням і атакам [1].

Постановка проблеми

Програмні снiфери знайшли масове застосування через легкість встановлення у мережеву інфраструктуру. Функціональність зводиться до поділу, повторного складання та реєстрації всіх пакетів програмного забезпечення, які проходять через інтерфейс незалежно від їх адреси призначення. Такі снiфери збирають стільки трафіку, скільки проходить через фізичний мережевий інтерфейс з умовою, що інші чинники не впливають на процес. Потім дані реєструються та використовуються відповідно до налаштувань [2].

Наявність снiфера у мережі дуже складно ідентифікувати оскільки вони працюють без зміни трафіку. Найчастіше виявлення снiферів ґрунтується на помилках їхньої роботи або непрямими методами. При неправильному налаштуванні хости зі снiферами можуть видавати відповіді на пакети, що адресовані на них, та виявляти себе, у той час яку звичному режимі роботи на ці пакети вони не відповідали б. Іншою рисою снiферів, є статистична залежність [3]. Будь-якому снiферу необхідно обробляти трафік або зберігати його кудись на диск. При цьому уповільнення реакції на звичайні пакети може корелювати з підвищенням трафіку в мережі вузлів, що знаходяться в режимі прослуховування [4].

Wireshark є однією з найбільш популярних моделей снiферів. Він використовується для усунення недоліків мережі, аналізу, розробки програмного забезпечення та протоколу зв’язку, а також навчання. Wireshark дозволяє користувачеві перевести контролери мережевого інтерфейсу в promiscuous mode (якщо він підтримується контролером мережевого інтерфейсу), щоб вони могли бачити весь трафік, видимий на цьому інтерфейсі, включаючи unicast трафік якій не надісланий на MAC-адресу цього контролера мережевого інтерфейсу. Однак під час захоплення за допомогою аналізатора пакетів в promiscuous mode не весь трафік через комутатор обов’язково надсилається до порта захоплення, тому захоплення в promiscuous mode не обов’язково достатньо для перегляду трафіку всієї мережі [5].

Мета статті – дослідити можливості застосування утиліти Wireshark для аналізу трафіку та показати функціональні можливості програми захоплення трафіка для аналіза різних типів мережевих пакетів.

Дослідження мережевого трафіку з використанням пакету WireShark

Найчастіше в локальній мережі підприємства встановлюється мережеве устаткування, наприклад Ethernet комутатори, роутери, файрволли чи Linux/Unix/Windows сервери, які

також застосовуються для маршрутизації трафіку чи інших службових цілей. Застарілі моделі таких пристроїв або сервери і пристрої, що налаштовані неправильно та не захищенні можуть бути доступні для віддаленого підключення або авторизації за незахищеним протоколом telnet або rlogin. Для наочності даної вразливості при снiфінгу розглянемо наступний експеримент – перехоплення логіну та паролю при виконанні заходу на віддалений сервер за протоколом telnet [6]. Легальний користувач login: daniel здійснює підключення та авторизацію на сервер IP 142.93.99.125 (віртуальний експериментальний сервер DigitalOcean у хмарі) за протоколом telnet, представлено на рис 1.

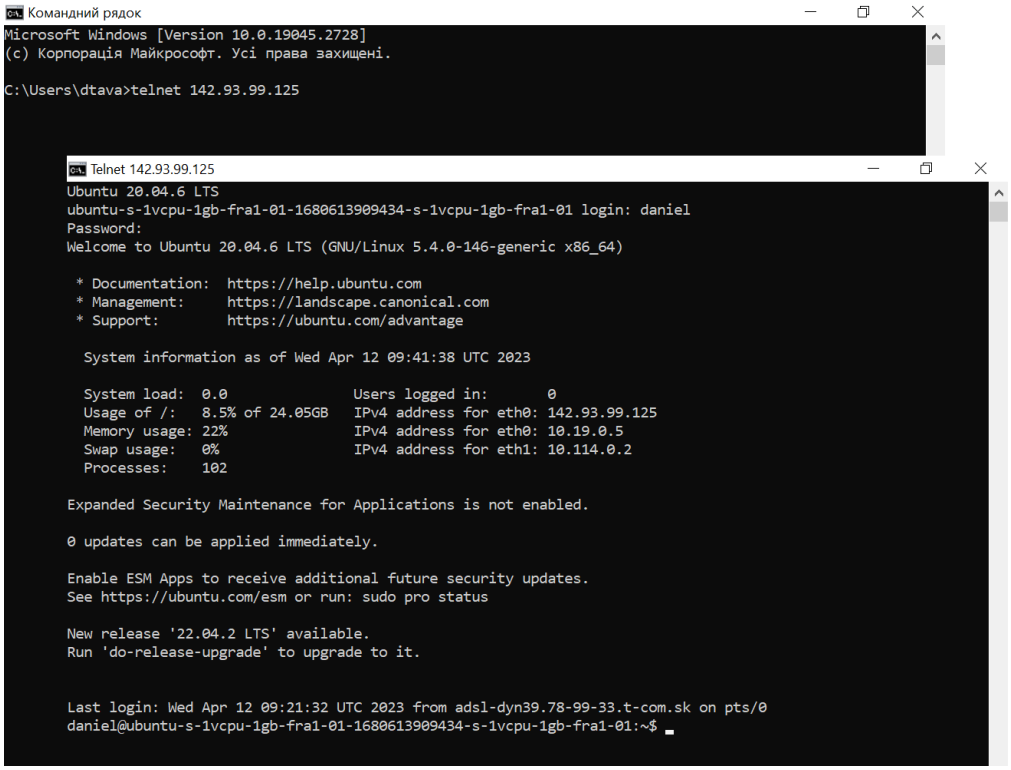

Рис. 1. Вікно консольної панелі (windows cmd)

У цей час на комп'ютері, з якого здійснюється авторизація на віддаленому сервері, що знаходиться в локальній мережі, запускаємо процес з перехоплення даних за допомогою програми Wireshark (рис. 2).

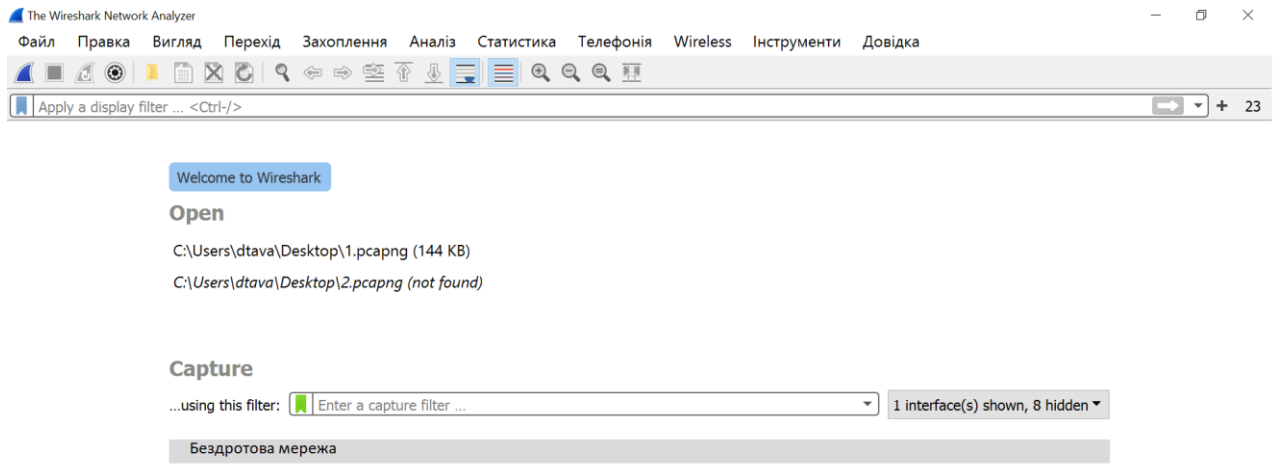

Рис. 2. Вікно «Старт»

Wireshark містить два види фільтрів – захоплення (Capture Filters) та відображення (Display Filters). Фільтр є виразом, що складається з вбудованих значень, які при необхідності можуть об'єднуватися логічними функціями (and, or, not). Також можна вибрати і заздалегідь створений фільтр. У цьому дослідженні застосовувався заздалегідь створений фільтр захоплення TCP пакетів, рис. 3.

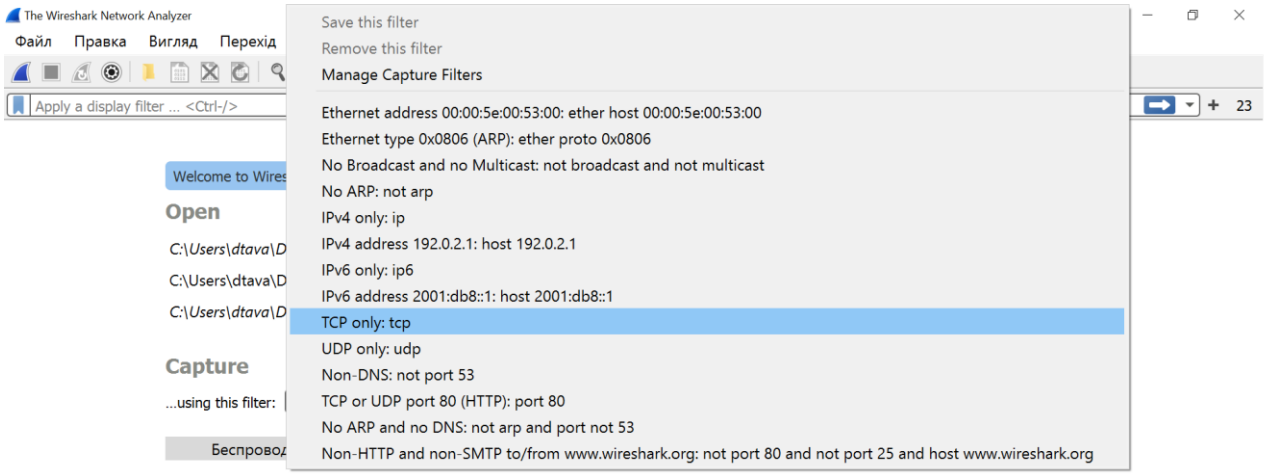

Рис. 3. Вікно «Фільтр захвату»

Після захоплення сесії процесу установки з'єднання з віддаленим сервером застосовуємо фільтр відображення обміну пакетами протоколу telnet. Фільтри відображення фільтрують лише трафік, що вже захоплено: протоколи, адреси, специфічні поля в протоколах.

У стандартній базовій конфігурації telnet сервер приймає з'єднання на TCP порту 23 будь-якої операційної системи, рис. 4.

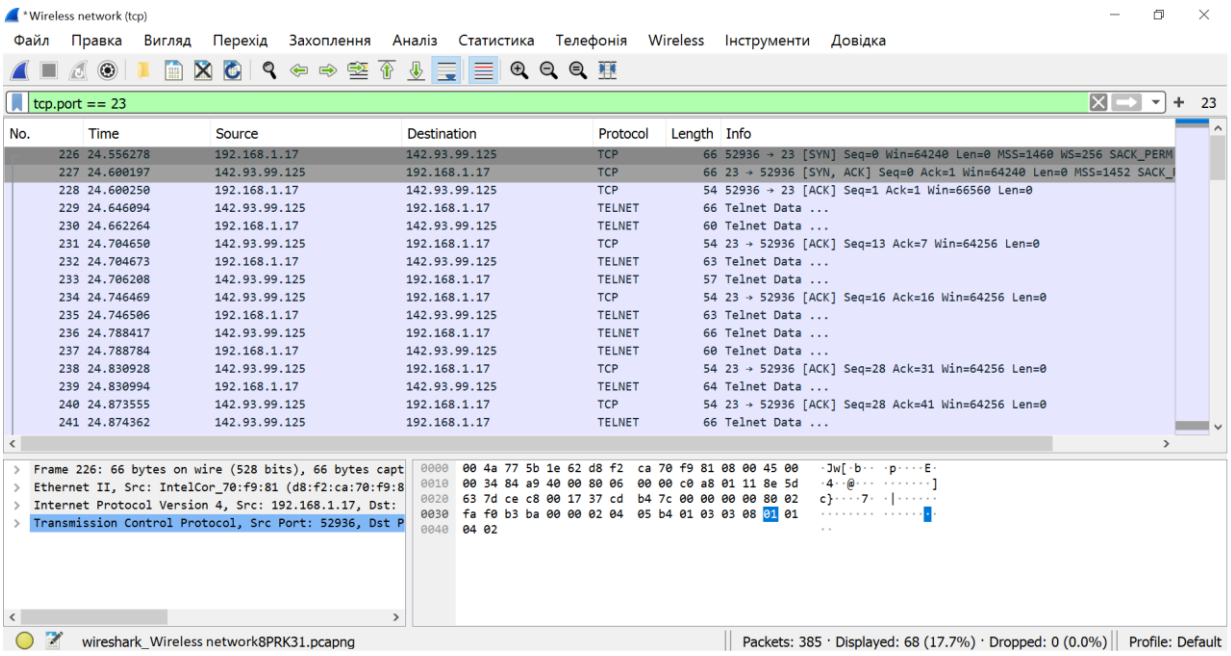

Рис. 4. Рядок фільтра для протоколу telnet

Після захоплення і фільтрації пакетів, що цікавлять нас, ми застосовуємо функцію прямування за потоком, рис. 5.

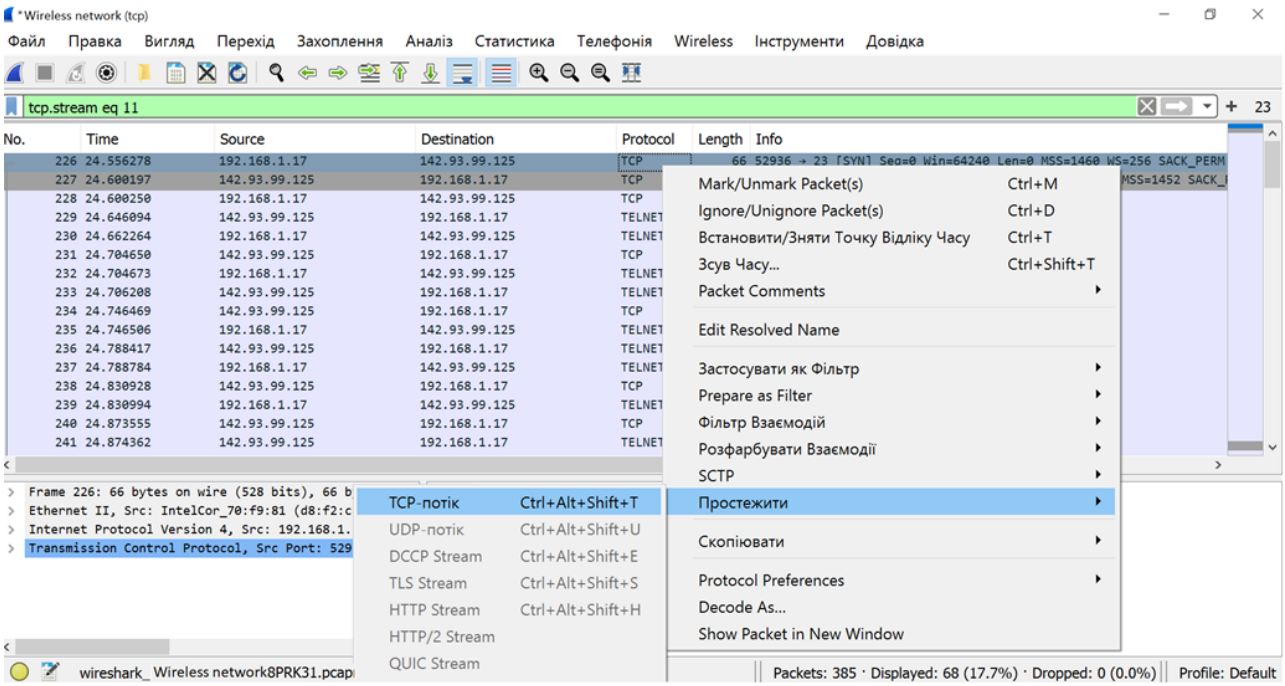

Рис. 5. Вікно «Функція прямування за потоком»

В результаті проведеного захоплення пакетів, фільтрації та прямування за потоком нам вдалося отримати таку інформацію: login, password, службову інформацію, яку передає віддалений сервер в термінальну консоль, принаймні, версію операційної системи, IP адреси та іншу системну інформацію, яку потенційний зловмисник може використовувати для атаки на інфраструктуру підприємства, рис. 6.

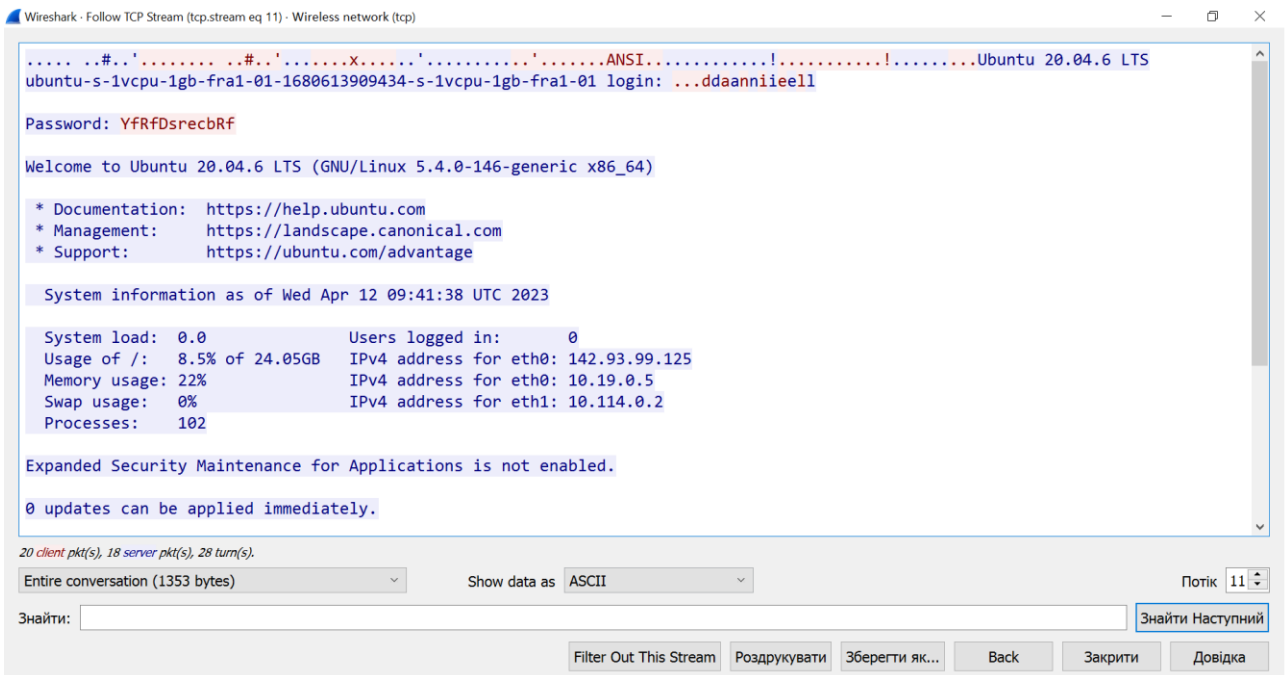

Рис. 6. Отримання інформації при дослідженні протоколу telnet

Також безумовною жертвою для сніфінгу та інтересом для зловмисників є WEB ресурси та сайти, що використовують незахищений протокол HTTP. Дуже часто в локальних мережах підприємств системні адміністратори не включають шифрування для внутрішніх

© Захаржевський, А. Г., Таванюк, Д. М., & Хворостяний, Р. В. (2023). Технологія сніфінгу у локальній мережі підприємства з використанням Wireshark. Сучасний захист інформації, 3(55), 22–31. https://doi.org/10.31673/2409-7292.2023.030003.

ресурсів і не використовують протокол HTTS з метою економії апаратних ресурсів серверів, для прискорення відгуку web сторінок і з наївною надією на те, що всередині підприємства вони більш захищені в порівнянні з публічними web ресурсами.

В експерименті, що наведено нижче, доведено зворотне і показано, наскільки просто перехопити весь незахищений потік, що йде протоколом HTTP. Наприклад, підприємство має веб сайт, що розробили за допомогою системи керування сайтами WordPress.

Заходимо на сторінку керування WordPress, яка доступна по протоколу HTTP, рис. 7.

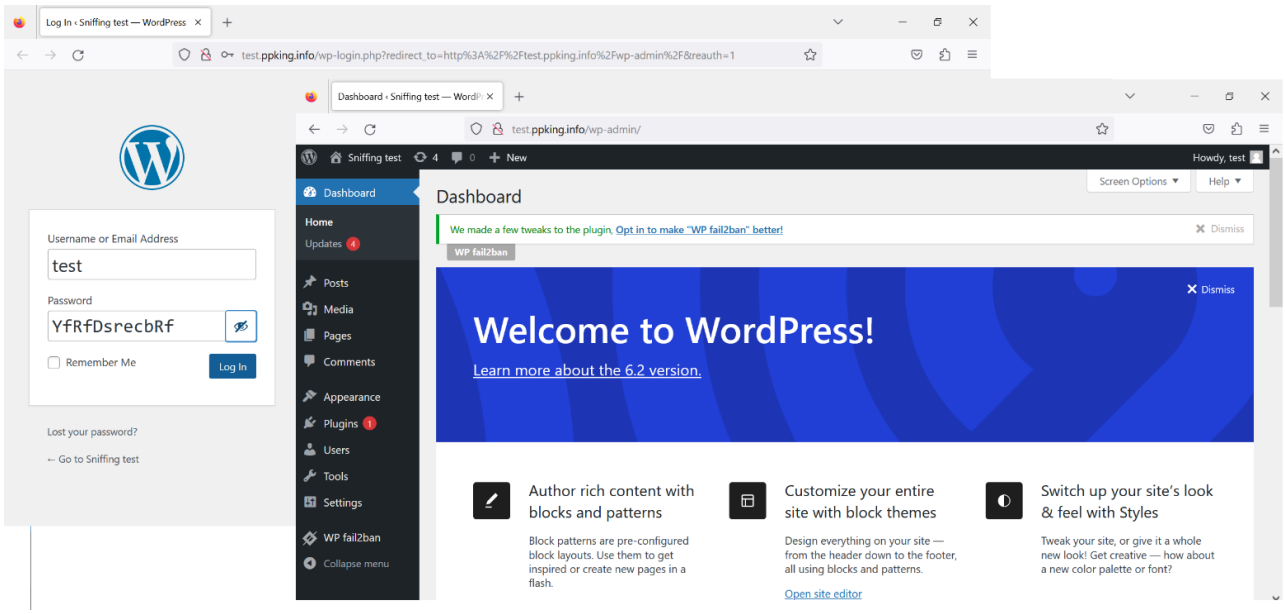

Рис. 7. Сторінка керування сайтом – WordPress

У програмі Wireshark, підключаємо фільтр захоплення протоколу TCP наведено на рис. 8, що йде на TCP порт 80 (HTTP). І робимо захоплення пакетів.

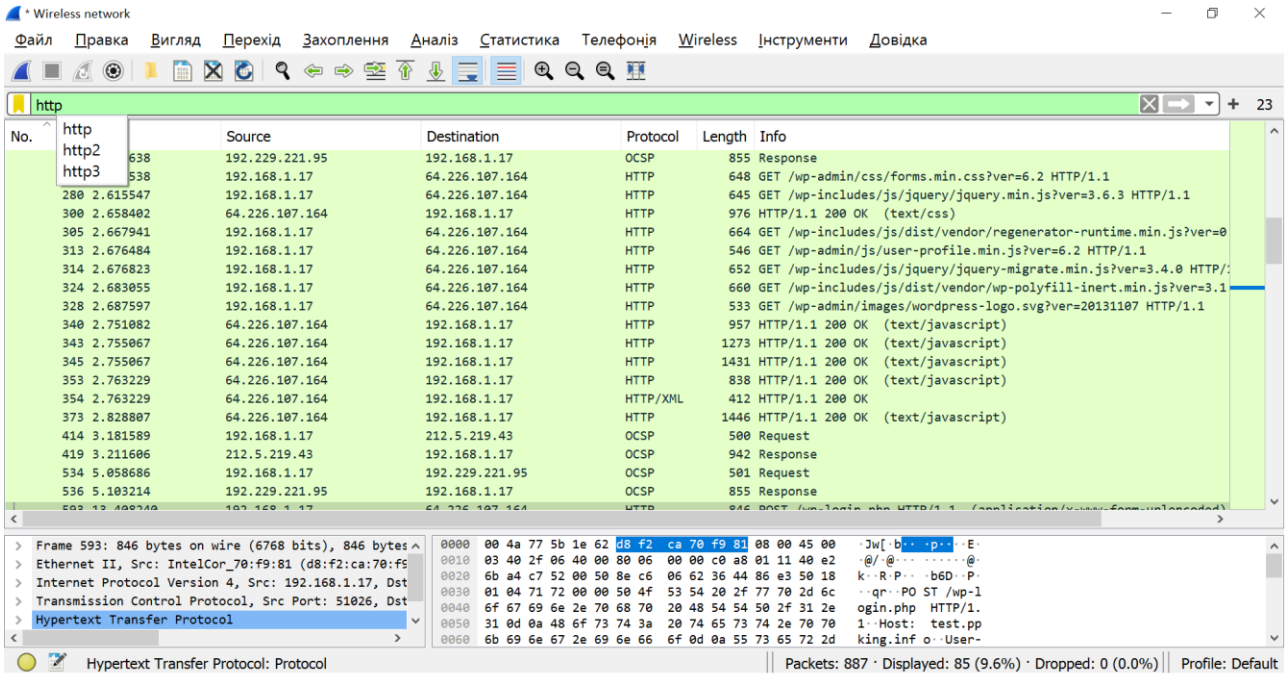

Рис. 8. Використання фільтру для протоколу HTTP

Після захоплення пакетів та застосування функції прямування за потоком (рис. 9) ми в реальному часі отримуємо висновок і можемо бачити обмін даними між клієнтом (браузером) та web-сервером.

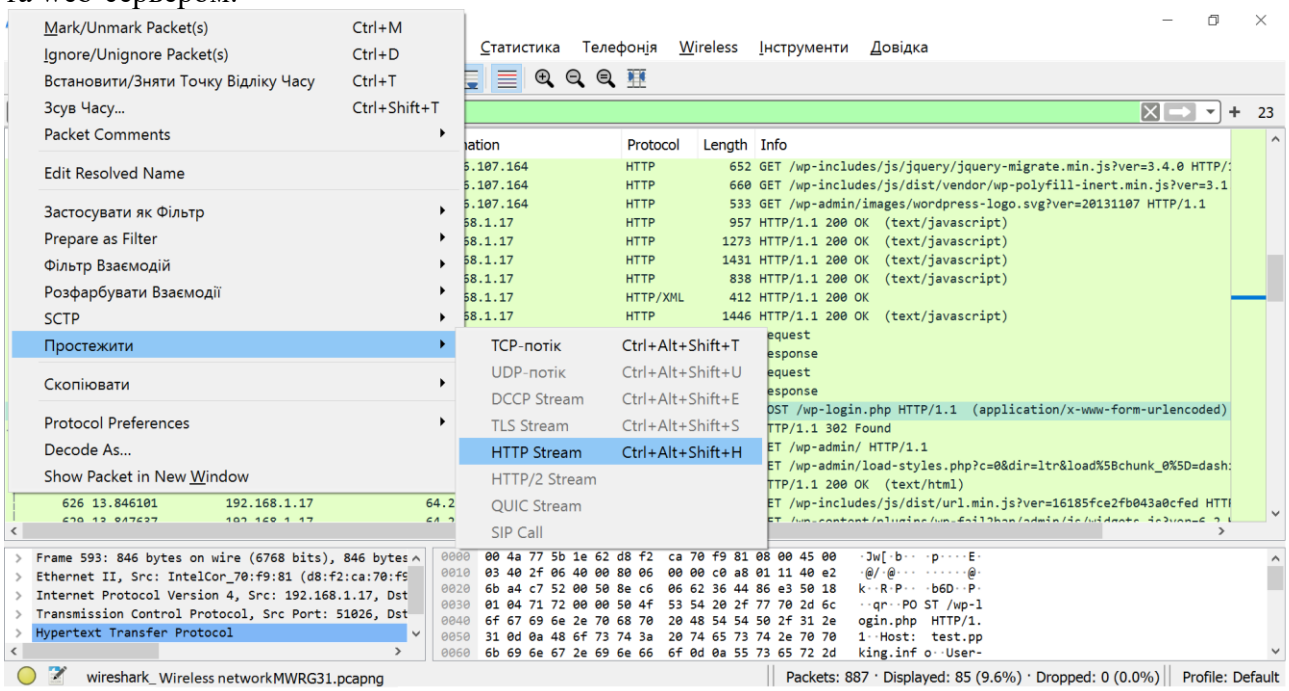

Рис. 9. Вікно прямування за потоком

На малюнку (рис. 10) можна побачити, що вдалося перехопити конфіденційну інформацію, яка використовується для заходу на панель керування сайтом.

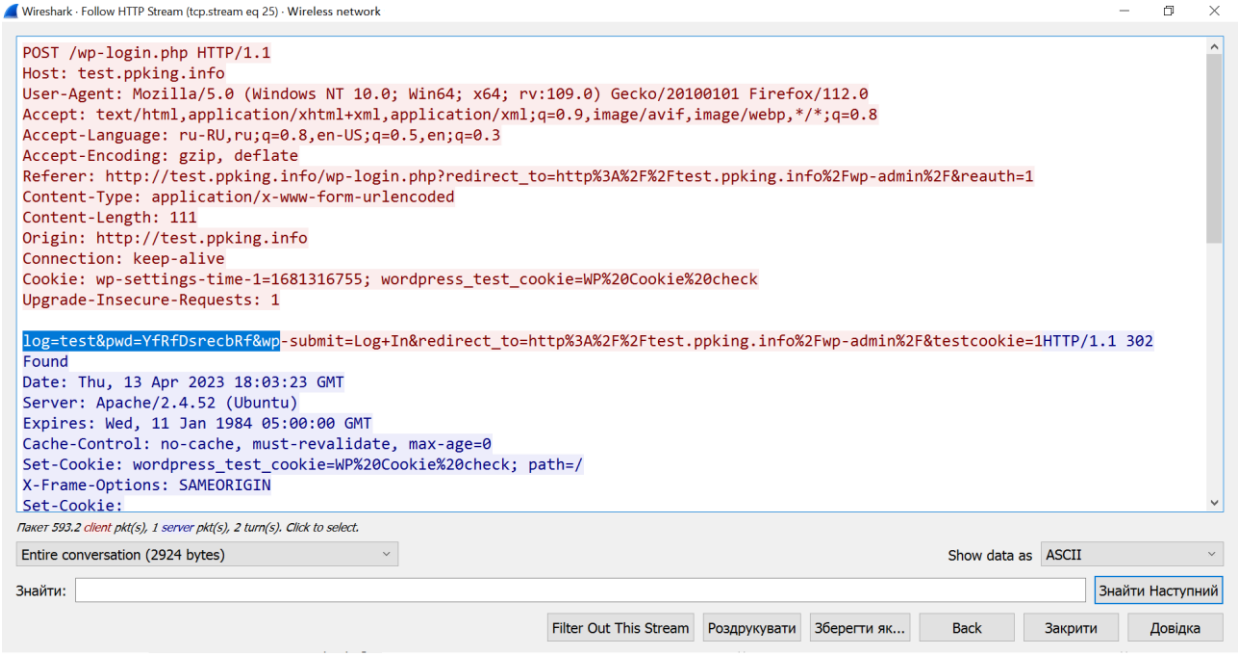

Рис. 10. Отримана інформація щодо протоколу HTTP

У випадку, наприклад, коли web сторінка містить будь-яку форму авторизації або форму з полями для введення будь-якої конфіденційної інформації, і web ресурс доступний за протоколом HTTP, можливо здійснити перехоплення та отримати конфіденційну інформацію таку як: логін та пароль користувача, персональні дані, корпоративну інформацію й так далі.

Виникнення загроз можливо коли здійснюється відкриття будь-якого ресурсу в локальній мережі або мережі інтернет, наприклад веб-сайта, попередньо відбувається перетворення доменного імені в IP адресу (resolving), на якому знаходиться ресурс. Така інформація має інтерес для перехоплення, оскільки знаючи MAC і IP адреси ресурсів і пристроїв у мережі можна використовувати їх для розуміння структури мережі, спрямованого сканування для визначення наявності вразливостей пристроїв та вибору об'єктів для атак та проникнень, наприклад, DoS атаки, спуфінг-атаки.

В експерименті нижче показано, як зробити захоплення DNS протоколу і визначити, як відбувається перетворення доменного імені в IP адресу сервера, на якому знаходиться панель управління сайтом WordPress. У програмі Wireshark, підключаємо фільтр захоплення протоколу DNS, рис. 11.

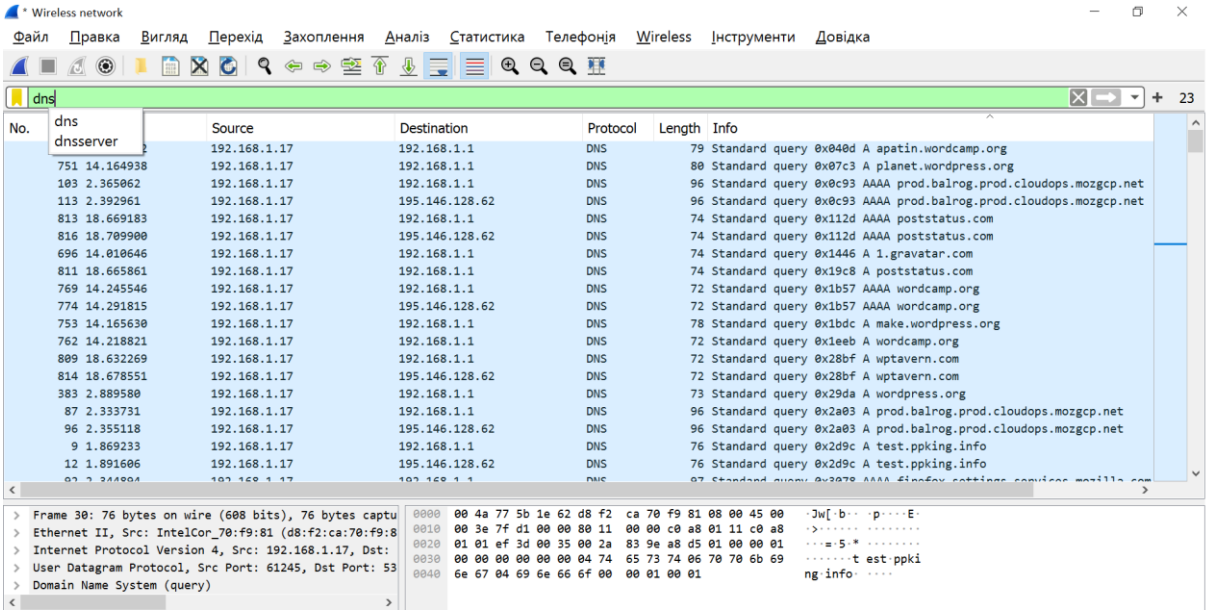

Рис. 11. Використання фільтру для протоколу DNS

Після захоплення пакетів та застосування функції прямування за потоком UDP (рис. 12) можна бачити обмін даними між клієнтом (браузером) та DNS-сервером.

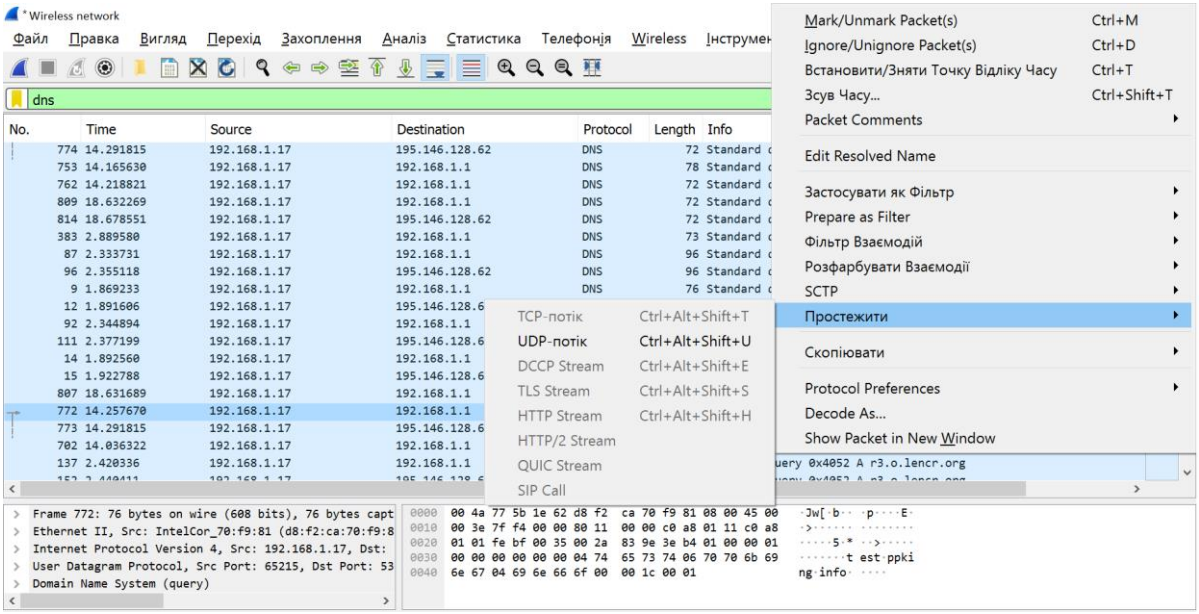

Рис. 12. Вікно прямування за потоком UDP

На рисунках 13 та 14 показано, що при запиті на відкриття сайту за адресою test.ppking.info відбулося звернення до локального DNS сервера IP 192.168.1.1, який визначив, що DNS записи домену ppking.info знаходяться у DNS сервера ajay.ns.cloudflare .com.

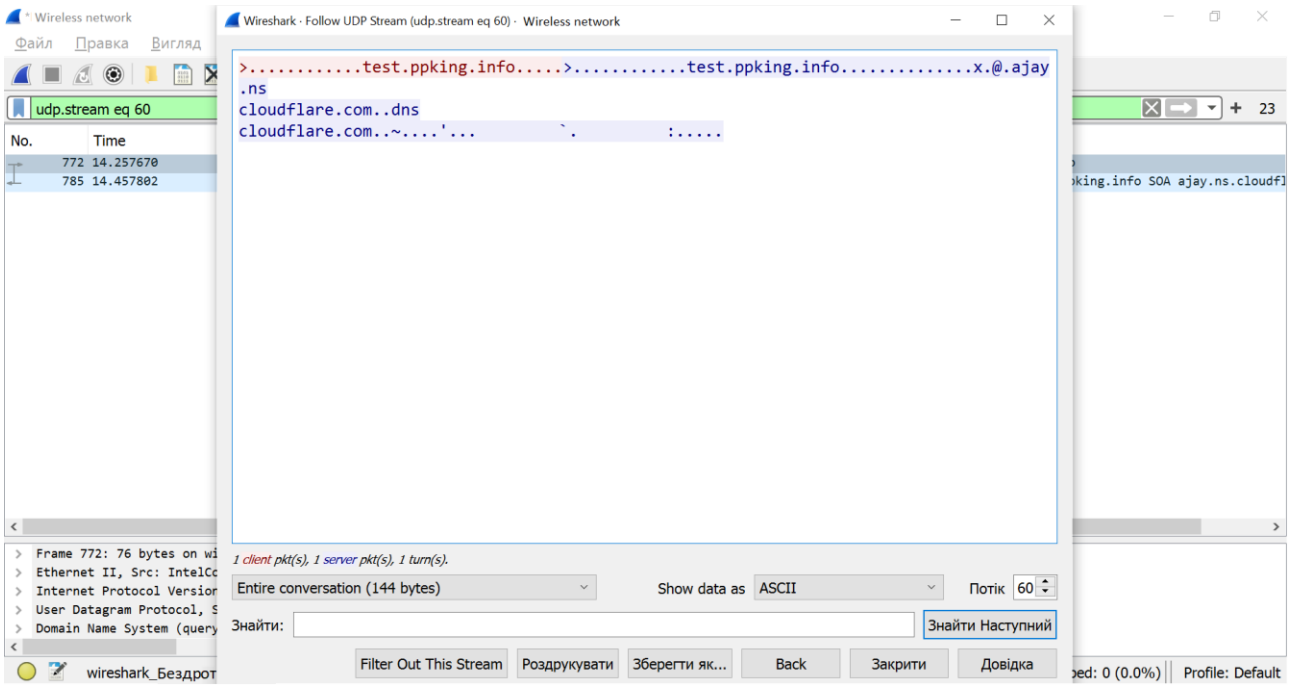

Рис. 13. Отримання інформації при дослідженні протоколу DNS

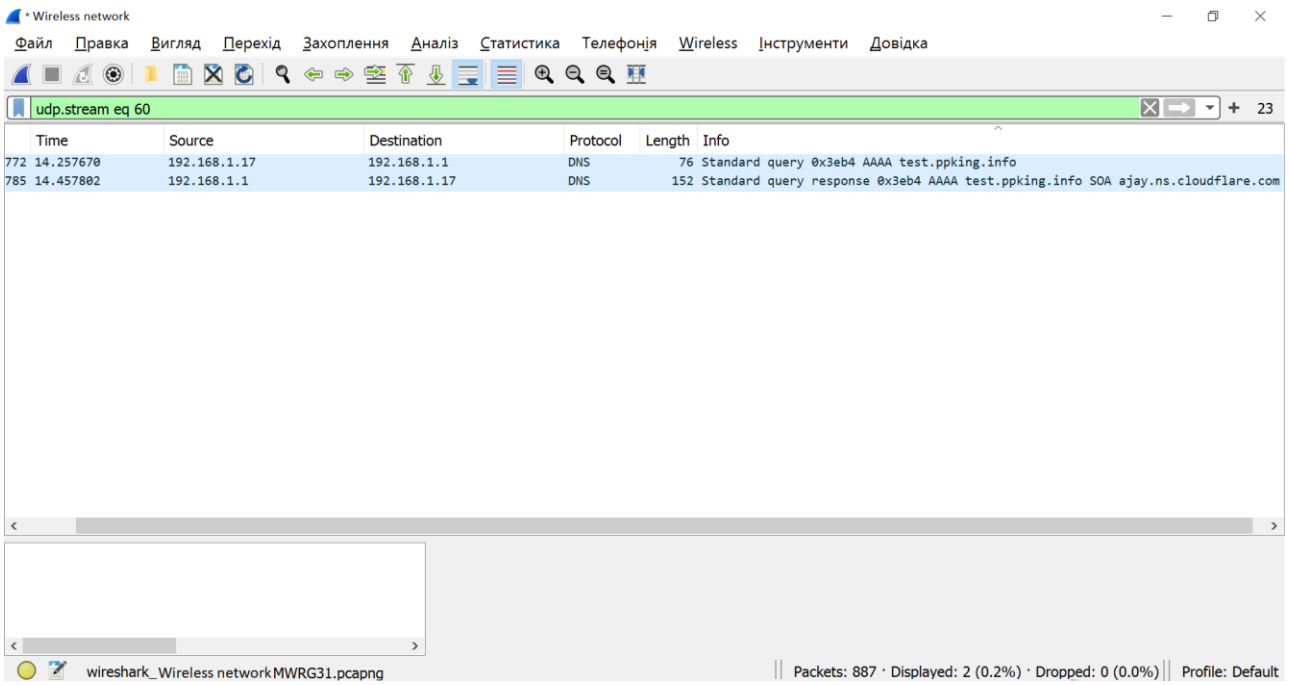

Рис. 14. Отримання інформації при дослідженні протоколу DNS – AAAA запис

На рис. 15 показано, що локальний DNS сервер IP 192.168.1.1, вочевидь після спілкування з DNS сервером, де знаходяться DNS записи домену сайту, який досліджується,

повернув відповідь відповідності доменного імені та IP адреси сайту, стався так званий resolving.

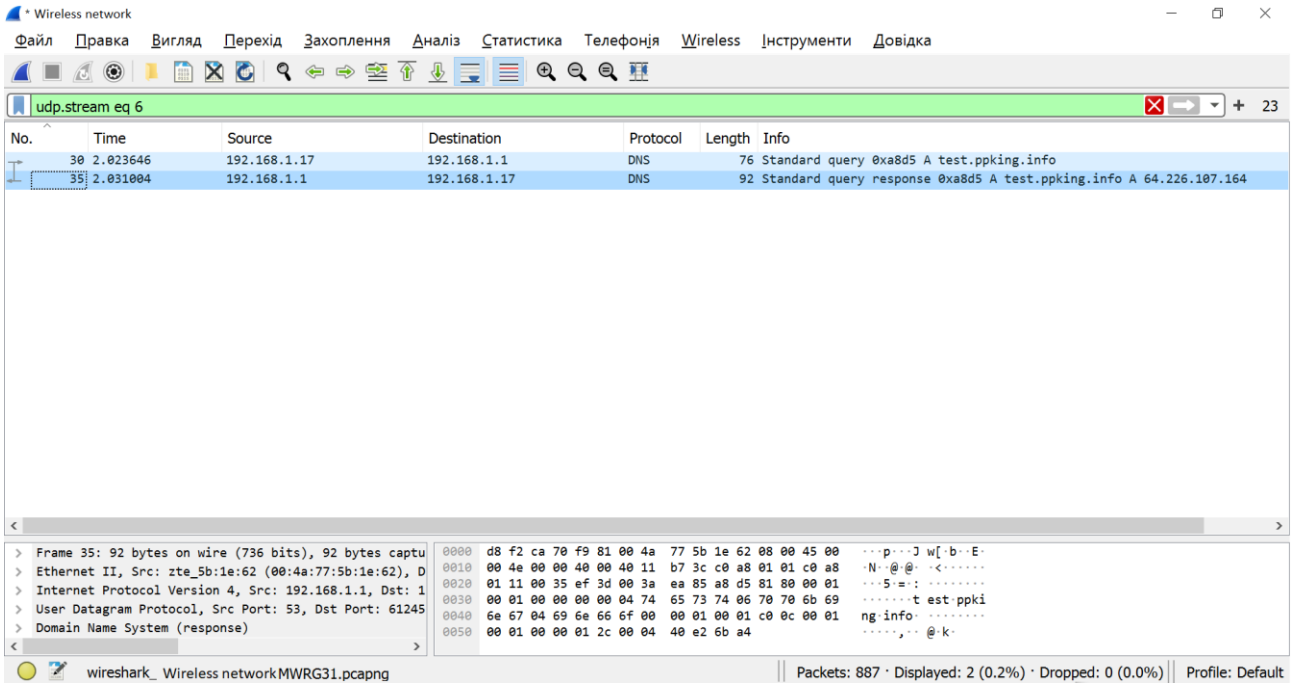

Рис. 15. Отримання інформації при дослідженні протоколу DNS – A запис

Існує кілька способів боротьби зі сніферами. Одним з них є їх виявлення за допомогою антисніферів. Серед таких програмних засобів, що ловлять сніфери в мережі, можна назвати: AntiSniff, CPM (Check Promiscuous Mode), neped, sentinel. Однак добре налаштований сніфер знайти ними неможливо. Пошук невиявлених засобів можливий лише непрямими способами, наприклад, шляхом створення пасток та генерації хибного трафіку до них. Хост, який скористався неправдивою інформацією, буде значним джерелом інформації для успішного пошуку сніфера. Використання засобів шифрування трафіку (криптографії) не запобігає можливості перехоплення повідомлень і не розпізнає роботу сніферів, проте є дієвим засобом боротьби зі сніферами. На сьогодні існують різні реалізації цього способу з різним ступенем надійності. Криптографія деяких пристроїв Cisco на мережевому рівні базується на протоколі IPSec, який є стандартним методом захищеного зв'язку між пристроями за допомогою протоколу IP. До інших криптографічних протоколів, які можна використовувати для боротьби зі сніфінгом, можна віднести SSH (Secure Shell) та SSL (Secure Socket Layer). Безперечно, що боротися зі сніферами краще запобіжними засобами, зводячи ефективність їх використання до нуля.

Якщо сніфер використовується порушником, це вважається атакою. Якщо сніфер санкціоновано використовується адміністратором мережі, це потужний засіб аналізу роботи мережі. Є чотири сфери, де використовують сніфер у добрих намірах: мережеві інженери (щоб оптимізувати мережу, вони мають слідкувати за трафіком), системні адміністратори (їм необхідно спостерігати за трафіком, щоб збирати дані про показники на кшталт пропускної спроможності мережі), фахівці з кібербезпеки (вони можуть помітити підозрілу активність у мережі, відстежуючи її). Роботодавці можуть використовувати програмне забезпечення для відстеження своїх співробітників.

© Захаржевський, А. Г., Таванюк, Д. М., & Хворостяний, Р. В. (2023). Технологія сніфінгу у локальній мережі підприємства з використанням Wireshark. Сучасний захист інформації, 3(55), 22–31. https://doi.org/10.31673/2409-7292.2023.030003.

Висновки

З досліджень із перехоплення мережного трафіку за допомогою Wireshark можна зробити такі висновки. Можливе перехоплення будь-яких даних, що передаються через мережу, якщо дані, які передаються, не в зашифрованому вигляді, якщо сервери та пристрої не використовують зашифрований протокол для віддаленого керування, наприклад SSH. Або якщо, наприклад, корпоративні web ресурси відкриті для доступу по відкритому протоколу HTTP, а не використовую шифрування SSL і протокол HTTPS, або якщо корпоративні поштові служби використовують не захищені поштові протоколи без SSL шифрування SMTP, POP3, IMAP.

Тому найкращим способом протидії сніфінгу та крадіжки облікових та корпоративних даних є впровадження протоколів шифрування на всіх пристроях мережі та для всіх сервісів підприємства. Але не завжди підприємство має можливості впровадити повне шифрування всіх ресурсів, не завжди є можливість навчити співробітників безпечної поведінки в мережі і особливо в мережі Internet. Так само іноді буває досить важко і дорого забезпечити фізичний захист периметра підприємства від проникнення сторонніх чи не авторизованих осіб, що також є ризиком для крадіжки даних за допомогою сніфінгу мережного трафіку.

Важливо регулярно перевіряти свою локальну мережу на наявність вразливостей, які можуть бути використані для сніфінгу, та вживати заходів щодо їх усунення. Знання основних принципів роботи мережевих протоколів та програмного забезпечення для аналізу трафіку, такого як Wireshark, може допомогти у виявленні сніфінгу та захисті від нього.

Перелік посилань

1. Жилін А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
2. Аналізатори [Електронний ресурс] – Режим доступу до ресурса: https://thk.kz/index.php/informatsiya/stati/318-20-besplatnykh-programm-administratora
3. 11 найкращих нюхачів WiFi - бездротові нюхачі пакетів у 2021 році. [Електронний ресурс] – Режим доступу до ресурса: https://uk.myservername.com/11-best-wifi-sniffers-wireless-packet-sniffers-2021
4. Що таке сніфер? [Електронний ресурс] – Режим доступу до ресурса: https://www.avg.com/en/signal/what-is-sniffer
5. Chris Sanders. Practical packet analysis using Wireshark то Solve Real-World network problems, 3-rd edition: San Francisco - No Starch Press, 2017 – 368 p.
6. Wireshark. [Електронний ресурс] – Режим доступу до ресурса: http://www.wireshark.org/

Надійшла: 16.07.2023 Рецензент: д.т.н., професор Гайдур Г.І.