***Сініцина О.В., магістрант,***
***Бродський Ю.Б., к.т.н, доцент,***
***Єфіменко А.А, к.т.н, доцент***
*Державний університет «Житомирська політехніка»*

## АЛГОРИТМ АНАЛІЗУ PCAP-ФАЙЛУ ЯК ЕЛЕМЕНТА МЕРЕЖЕВОЇ КРИМІНАЛІСТИКИ

Мережева криміналістика – це галузь кібербезпеки, що дозволяє аналізувати й відстежувати підозрілу активність у комп'ютерних мережах шляхом перехоплення трафіку.[2] Ключовим елементом цього процесу є використання PCAP-файлів, які зберігають протокольні пакети, що передаються. Аналіз PCAP-файлів надає змогу відновити події, що відбувалися у мережі, виявити ознаки атак, а також зібрати докази для подальшого розслідування.

Мета роботи полягає у розробці алгоритму аналізу PCAP-файлів для адаптації існуючих методів аналізу даних та підвищення ефективності виявлення, документування та інтерпретації мережевих артефактів.

Перед початком роботи з файлом потрібно переглянути усі метадані та отримати базову інформацію для створення загального уявлення про обсяг роботи і період збору даних. На першому етапі застосовується описовий метод, який полягає у виконанні сортування, фільтрації та візуалізації даних. Для цього обирається відповідний інструмент, наприклад, Wireshark, tshark, NetworkMiner або скрипт, написаний аналітиком. Інструменти дозволяють переглянути статистику за адресами та протоколами, що є в захоплених даних, для оцінки характеру та розподілу трафіку. Залежно від шуканої активності, потрібно визначитись з встановленням базових фільтрів за IP-адресами, портами, протоколами або часовими рамками для зменшення обсягу аналізованих даних. За потреби легітимний трафік, який не стосується розслідування, фільтрується або та видаляється для зосередження над основною задачею.[3]

На другому етапі варто виконати пошук файлів, що передаються через мережу, за допомогою функцій обраної програми з трафіку для подальшого дослідження на предмет вмісту.[2] На авторську думку, рекомендується аналізувати PCAP-файл різними інструментами, оскільки вони можуть мати більш потужний функціонал для виявлення переданих файлів.

На третьому етапі слід виконати первинне встановлення зв’язків, систематизувавши дані, отримані на попередніх кроках аналізу. Це дозволить скласти загальну картину мережевого трафіку і виділити ключові елементи для подальшого аналізу.

На четвертому етапі проводиться виявлення потенційних вразливостей, які могли бути використані зловмисниками. Основна увага приділяється виявленню відкритих портів, відсутності автентифікації, експлуатація незашифрованих протоколів (HTTP, Telnet, SMBv1).[3] Це дозволяє сформулювати рекомендації щодо посилення безпеки мережі, шляхом виявлення реалізованих та нереалізованих загроз.

На п’ятому кроці у трафіку можуть бути виявлені рідкісні чи невідомі протоколи, нестандартні команди або підозрілі обсяги даних, що передаються, шкідливе програмне забезпечення або спроби несанкціонованого доступу.

Шостий етап, а саме ретельний аналіз заголовків і вмісту пакетів дозволяє виявити маніпуляції з параметрами (фальсифікацію IP-адрес, часових міток, маніпуляції з TCP-прапорами, payload) і шкідливий вміст у пакетах (код експлойтів, команди шкідливого ПЗ).[3]

За необхідності на сьомому етапі використовуються скрипти для автоматизації відновлення файлів з захопленого трафіку, виділяють сесії або певні типи даних, проводять пошук за шаблонами (наприклад, хешами відомих шкідливих файлів). Скрипти дозволяють значно скоротити час аналізу та зменшити ризик людських помилок, забезпечуючи точність і повторюваність процесу.

На думку авторів, кожен етап аналізу важливо фіксувати, а саме дії, використані інструменти, фільтри та отримані результати. Це забезпечує прозорість, створює основу для подальших досліджень і знижує ризик помилок.[2]

Дослідження поглиблює розуміння аналізу мережевого трафіку та сприяє створенню ефективних інструментів для розслідування кіберзлочинів. Запропонований алгоритм надає систематичний підхід до аналізу PCAP-файлів, охоплюючи всі ключові етапи: від попереднього огляду до детального аналізу пакетів, та дозволяє фахівцям з мережевої безпеки швидше виявляти загрози та підвищувати якість розслідувань, забезпечуючи захищеність інформаційних систем.

**Список використаних джерел**

1. Приклади трафіку у pcap-файлі. URL: https://is.gd/FGchSK (date of access: 02.12.2024).
2. What is Digital Forensics | Phases of Digital Forensics | EC-Council. Cybersecurity Exchange. URL: https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensics/ (date of access: 02.12.2024).
3. Packet CAPture (PCAP) Analysis with WireShark. URL: https://is.gd/PWxhSi (date of access: 02.12.2024).