УДК 004.056

З. В. Окрутний

РОЗРОБКА ЗАСОБУ ДЛЯ АНАЛІЗУ ДАМПІВ ПАМ'ЯТІ ПІД ЧАС РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ

Вінницький національний технічний університет

Анотація

Дослідження описує методи роботи для розслідування інцидентів кібербезпеки на основі яких можна вважати, що з пристрою було здійснено кібератаки, або інші дії, які порушують цілісність, конфіденційність або доступність інших користувачів. Розроблено метод аналізу дампів пам'яті який допомагає виявляти дані порушення та доводити, що з пристрою справді було виконано несанкціоновані дії.

Ключові слова*:* кібербезпека, дамп пам'яті, цілісність, аналіз

Abstract

This article describes how to investigate cybersecurity incidents that suggest that a cyber attack or other activity that violates the integrity, privacy, or availability of other users may have occurred from the device. A memory dump analysis method has been developed to help detect data violations and prove that unauthorized actions were indeed performed on the device.

***K*eywords**: cybersecurity, memory dump, integrity, analysis

Вступ

Багато галузей діяльності сучасного суспільства залежать від правильного функціонування незліченної кількості програмних засобів. Тому коректна робота є чи не найголовнішою складовою кожного застосунку. Проте є низка людей, які прагнуть порушити коректність роботи або несанкціоновано отримати доступ до даних [1]. Такі випадки не повинні залишатись не покараними. Одним зі способів відслідковування таких злочинів є створення дампів пам'яті та їх аналіз, що відноситься до напряму – форензіка [2].

Результати досліджень

Дамп пам'яті [3] – це знімок частини або повного обсягу оперативної пам'яті [4] та його розміщення на енергозалежний носій (жорсткий диск). Тобто вміст оперативної пам'яті повністю або частково копіюється на носій і користувач може провести аналіз дампа пам'яті.

Існує декілька видів дампів пам'яті [3]:

- Малий дамп – зберігається мінімальний обсяг ОЗП, де знаходяться відомості з критичних помилок та компонентів, які були завантажені під час роботи системи, наприклад драйвера, програми.
- Повний дамп – зберігається повний обсяг ОЗП. Це означає, що розмір файлу дорівнюватиме обсягу оперативної пам'яті. Якщо місця на диску буде мало, буде проблематично зберегти. Цей вид використовується не часто.
- Дамп пам'яті ядра – зберігається лише інформація, що стосується ядра системи.

За допомого дампів оперативної пам'яті можна отримати також, які додатки запускались під час роботи комп'ютера, дані процесів, інтернет-трафік та іншу корисну інформацію. Аналіз захопленої інформації пам'яті пристрою (дамп пам'яті), дозволяє виявити ознаки шкідливого програмного забезпечення.

На відміну від криміналістичної експертизи жорсткого диска [5], де файлова система пристрою клонується, і кожен файл на диску може бути відновлений та проаналізований, криміналістична експертиза пам'яті зосереджується на фактичних програмах, які працювали на пристрої, коли був захоплений дамп пам'яті.

Також варто враховувати, що дамп формується з оперативного запам'ятовуючого пристрою, тобто енергозалежної пам'яті. Після вимкнення досліджуваної системи необхідні дані можуть бути втрачені назавжди. Тому важливим під час проведення розслідування є збереження цифрових доказів, а саме збереження живлення пристрою. Але в свою чергу – це може призвести до розгортання атаки, яке проводиться за допомогою того чи іншого шкідливого програмного засобу.

Найкращим підходом в даній ситуації є обмеження або ізоляція мережі. Цей метод надійно стримає та збереже цінні докази та не знищить тимчасові дані.

Здійснення дампу всієї системи може зайняти доволі багато часу і в такому разі виникає проблема перенесення копії розміром у кількасот терабайт до місця де його можна проаналізувати, що ускладнює процес дослідження. В цьому контексті аналіз дампу оперативного запам'ятовучуого пристрою є велика перевага. Його обсяг зазвичай не перебільшує 32 гігабайт та є набагато меншим за жорсткий диск хоча його аналіз має певні нюанси при аналізі. На рис.1 показана структурна схема запропонованого засобу.

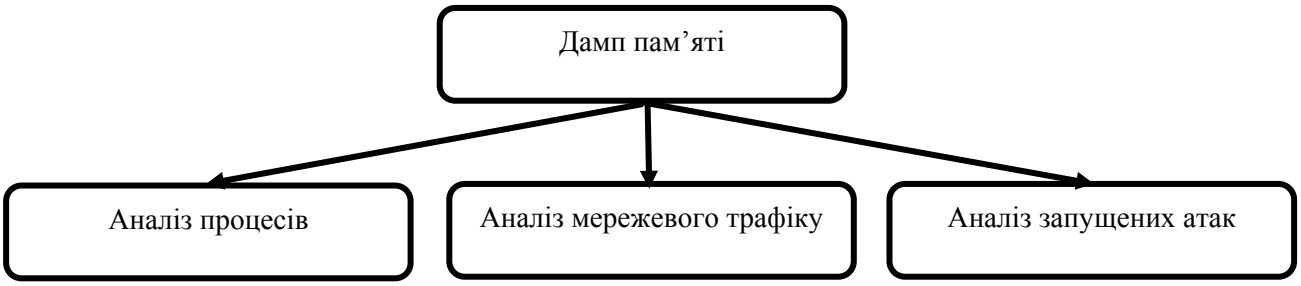

Рис. 1. Структурна схема роботи програми

Після аналізу даних кроків, буде виведено результат про можливі виявлені загрози, або ж про успішне сканування і безпечність системи. Втім немає бездоганних програм на які можна повністю покластись і якщо закрадаються хоч найменші сумніви все ж слід перевірити більш детально власноруч, адже якщо засіб автоматизований ймовірно він покриває не всі можливі варіанти загроз.

Висновки

Отже, запропонований додаток може знайти досить значне місце в аналізі дампів пам'яті та криміналістиці так як значно скорочує час на пошук та аналіз інформації яка зберігається на пристрої.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Charles J. Brooks Cybersecurity Essentials 1st edition // sybex; 1st edition 20 September 2018 p.784
2. Nhien-An Le-Khac Cyber and Digital Forensic Investigation // Springer 1st edition 26 July 2020 p.293
3. Dmitryi Vostokov Memory Dump Analysis Anthology, Volume 12 // Revised edition 28 December 2021 p.180
4. Roger Villela Mechanism and APIs Memory Management // Apress 29 November 2019 p.203
5. Nas Guide : NAS Guide PC for Network Hard disk drive // Independently 17 December 2019 p.58

Окрутний Захар Віталійович **–** студент групи 1бс-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: zaxarokrutn@gmail.com

Науковий керівник: ***Войтович Олеся Петрівна*** **–** канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет.

Zakhar Okrutnyi **–** Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : zaxarokrutn@gmail.com

Supervisor***: Voitovych Olesia*** – Cand. Sc. (Eng), Assistant Professor of information protection department, Vinnytsia National Technical University