ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОГЛЯДУ ТА ВИЛУЧЕННЯ ОКРЕМИХ СЕРВЕРНИХ КОМП'ЮТЕРНИХ СИСТЕМ ЗБЕРІГАННЯ ДАНИХ

Сергій Олександрович БИЧКОВ,

заступник завідувача відділу комп'ютерно-технічних та телекомунікаційних досліджень Харківського науково-дослідного експертно-криміналістичного центру МВС України

Однією із загальних проблем при проведенні дослідження серверів віртуальних контейнерів, файлових серверів, серверів баз даних є відсутність розуміння судовим експертом їх початкової конфігурації, взаємодії у локальній мережі та підключенні між собою окремих компонентів таких систем у місці, де проводиться їх вилучення. Фіксація такої інформації як мережеві налаштування маршрутизаторів, IP-адреси серверів (якщо налаштовано на статичну IP-адресу) може суттєво спростити дослідження для таких серверних систем, як мережеві дискові масиви, а також мережеві дискові масиви розширення. Такі системи зазвичай мають можливість підключення до них через мережевий інтерфейс (веб-інтерфейс, або спеціальне програмне забезпечення). Виготовлення файлів-образів з таких систем не завжди є можливим через значну кількість задіяних в неї носіїв інформації, що в свою чергу дає значний розмір виготовлених файлів-образів, який не можливо розмістити в пам'яті обладнання судового експерта. Крім того, такі системи зберігання даних не завжди використовують стандартні технології віртуалізації типу RAID, що призводить до неможливості визначення конкретного рівня віртуального RAID-масиву та об'єднання виготовлених файлів-образів у віртуальний RAID-масив за допомогою програмного забезпечення судового експерта.

Існує велика різниця в дослідженні звичайних системних блоків персональних комп'ютерів (СПБК) та деяких серверних систем, як наприклад, мережеві дискові масиви. Вона полягає у тому, що загальними методами описаними в методиках проведення досліджень для СПБК провести дослідження мережевих дискових масивів практично неможливо. Загальні методи досліджень СПБК передбачають виготовлення файлів-образів з носіїв інформації СПБК та їх подальше дослідження програмними засобами експерта. Виготовити файли-образи безпосередньо з носіїв інформації мережевих дискових масивів частіше за все неможливо в зв'язку з особливостями специфіки контролерів до яких вони під'єднані та самих інтерфейсів під'єднання. Наявне апаратне обладнання не завжди може відтворити певний контролер, що унеможливлює фізичне підключення носія інформації до робочої станції експерта. Виготовлення файлів- образів шляхом завантаження в оперативну пам'ять мережевих дискових масивів спеціальних завантажувальних операційних систем на базі ядра Linux, до складу яких входить програмне забезпечення для виготовлення файлів-образів з носіїв інформації також неможливий в

зв'язку зі специфікою архітектури мережевих дискових масивів та відсутністю відповідних інтерфейсів під'єднання зовнішніх носіїв інформації.

Підключення та робота з мережевими дисковими масивами здійснюється через спеціальне програмне забезпечення, яке ідентифікує у локальній мережі дисковий масив, здійснює його конфігурацію, надає доступ до користування певним користувачам та виконує інші сервісні операції зі сховищем. Таким чином, відсутність зазначених мережевих налаштувань, які вносяться під час ініціалізації дискового масиву унеможливлює отримання будь-якого доступу до інформації, яка в ньому збережена.

Окремо необхідно зазначити про фіксацію підключення між собою дискових процесорів та дискових масивів розширення. Дисковий масив розширення не може виступати як окремий об'єкт дослідження, оскільки він призначений для розширення існуючого дискового масиву і може досліджуватись тільки в сукупності з дисковими процесорами та іншими дисковими масивами розширення, які об'єднані між собою у конкретну послідовність за допомогою спеціальних кабелів через зовнішні роз'єми SAS. В такій системі дисковий процесор є керуючим пристроєм та конфігурує через мережевий інтерфейс всі інші пристрої об'єднані в загальну систему збереження даних. Тому для проведення повного дослідження таких систем вкрай важливо розуміти їх підключення на момент проведення вилучення зазначеної техніки. Рекомендується залучати до проведення вилучання спеціалістів з знаннями у певній галузі комп'ютерних мереж та систем.

Також при можливості слід фіксувати конфігурацію контролерів віртуальних RAID-масивів з метою розуміння кількості задіяних дисків у окремих масивах, а також специфікації безпосередньо самого RAID-масиву (RAID0, RAID1, RAID5, …. тощо). Фіксація конфігурацій налаштованих RAID-масивів серверних систем, також може суттєво полегшити проведення дослідження таких систем та спростити відтворення віртуального RAID-масиву у робочому середовищі експерта.

Слід зауважити і про те, що доступ безпосередньо до даних, які зберігаються у таких мережевих сховищах, якщо він відбувається за допомогою веб-інтерфейсу або спеціального програмного забезпечення, може бути обмежений за допомогою логіну та паролю облікового запису користувачів таких мережевих сховищ. Якщо існує можливість отримати такі авторизаційні дані їх також необхідно зафіксувати у протоколі слідчої дії.

Не менш важливим є фіксування налаштувань мережевого обладнання (роутери, маршрутизатори), яке використовується для об'єднання комп'ютерних систем, що будуть вилучатись. Розуміння того, чи було налаштоване статичне отримання IP-адреси (якщо так, необхідно зафіксувати конкретний IP-адрес присвоєний пристрою), чи динамічно за протоколом DHCP (у цьому випадку необхідно розуміти діапазон IP- адрес, що виділяються, а також підмережу) може надати можливості в ході

проведення дослідження під'єднатися до мережевого сховища, використавши конкретну IP-адресу.

Сукупність та послідовність наведених дій при проведенні слідчої дії, метою якої є вилучення окремих серверних систем із залученням спеціаліста, що володіє знаннями у певній галузі знань комп'ютерних систем та мереж, дозволять у подальшому провести більш повне та результативне дослідження.