сушіння, відновлення, випробувань ізоляції електрообладнання суден суттєво впливають на тривалість перебування суден в ремонті і після ремонту надійність відремонтованого суднового електрообладнання.

В роботі виконано аналіз способів сушіння зволожених обмоток ССГ (самозбуджувальних і безщіткових) в експлуатаційних умовах на судах, виявлені переваги та недоліки розглянутих способів та представлено порівняльну характеристику (табл. 1).

Висновок. Всі розглянуті в роботі способи сушіння в принципі дають позитивний результат, проте на практиці в суднових експлуатаційних умовах доцільно використовувати ті із способів сушіння вологих обмоток, для яких можна застосувати наявні на судах джерела електроенергії, тобто можна практично легко і ефективно здійснити ці методи сушіння в суднових експлуатаційних умовах.

Список використаних джерел:

[1] Приходько, В.М. (2015). Математическая модель судовых асинхронных двигателей при сушке изоляционных систем по энергосберегающей технологии. *Морской вестник,* №2 (54), 67 – 69.

[2] Приходько, В.М. (2013). Эффективность методики прогнозирования электропотребления судоремонтным предприятием. *Морской вестник*., №3 (47), 51-56.

[3] Мелкауи, Х. (2012). Методы и средства комплексных испытаний электрооборудования по энергосберегающей технологии в судостроении и судоремонте: дис. канд. техн. наук: 05.08.04/Хассан Мелкауи. Санкт-Петербург.

DOI 10.36074/24.04.2020.v2.16

ВИКОРИСТАННЯ ОСОБЛИВОСТЕЙ ЗАВАНТАЖУВАЧА «GRUB» ДЛЯ ОТРИМАННЯ ДОСТУПУ ДО ІНФОРМАЦІЇ, ЗАХИЩЕНОЇ МЕТОДАМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ЗА СПЕЦИФІКАЦІЄЮ «LUKS»

ORCID: 0000-0002-2180-0969 **Пташкін Роман Леонідович**
заступник завідувача відділу комп'ютерно-технічних та телекомунікаційних досліджень
Черкаський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України

Обруч Юрій Юрійович
завідувач відділу комп'ютерно-технічних та телекомунікаційних досліджень
Черкаський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України

УКРАЇНА

В сучасності досить популярним сімейством операційних систем є сімейство Unix-подібних операційних систем. Станом на початок 2020 року Unix-подібні операційні системи є найпопулярнішими системами для web-серверів – згідно статистичних даних W3Techs майже 70% всесвітньої мережі Інтернет працює на операційних системах цього типу, з них понад 32% – операційні системи сімейства Linux [1].

Ріст популярності операційних систем Linux призвела до збільшення випадків використання її й злочинцями. В ході аналізу кількості та виду досліджених речових доказів, працівниками Черкаського науково-дослідного експертно-криміналістичного центру МВС України встановлено, що за останні роки значно збільшилась кількість випадків використання можливостей Linux-подібних операційних систем для створення робочих станцій, захищених криптографічними засобами захисту інформації. Найтиповішим випадком є шифрування даних методами криптографічного захисту за специфікацією «LUKS» з використанням можливості автоматичного (без введення паролю) розшифрування даних після завантаження операційної системи. Такий підхід практично унеможливлює дослідження носія інформації й одночасно не потребує від кінцевого користувача знання паролю.

Метою даної роботи є висвітлення деяких особливостей завантажувача «GRUB», що в окремих випадках дозволяють отримати доступу до інформації, захищеної методами криптографічного захисту за специфікацією «LUKS».

Досліджуючи носій інформації з ознаками криптографічного захисту, судовому експерту за напрямком комп'ютерно-технічних досліджень необхідно не тільки зчитати вміст носія, а й дослідити внутрішні процеси й алгоритми, які виконуються під час функціонування системи та прикладного програмного забезпечення загалом, тобто поряд з класичним дослідженням варто застосувати експертний експеримент – дослідження працюючої системи в повністю контрольованому середовищі.

Одним з варіантів такого середовища є Oracle VM VirtualBox – програмний засіб віртуалізації для операційних систем, перевагою якого є кросплатформність, підтримка різних форматів образів носіїв інформації та вільне використання, тобто програмний засіб є безкоштовним.

Відтак, враховуючи той факт, що завантажувач «GRUB» дозволяє користувачеві при завантаженні задавати довільні параметри і передавати їх в ядро операційної системи для подальшої обробки, можливо ініціювати «паузу» в завантаженні операційної системи та здійснити вхід до інтерфейсу командного рядка [2,3]. Для виконання вищезазначеного алгоритму необхідно завантажити досліджуваний образ носія інформації в середовищі програмного засобу Oracle VM VirtualBox. Відразу після запуску завантажувача необхідно перервати процес завантаження та перейти (зазвичай натисканням клавіші «E») в режим редагування параметрів завантаження (рис. 1).

Рис 1**. Вигляд параметрів завантаження**

Отримавши доступ до режиму редагування параметрів завантажувача необхідно провести їх модифікацію – змінити режим роботи з носієм та ініціювати вхід до інтерфейсу командного рядка «bash» (рис. 2). Варто зауважити, що ініціалізацію командної оболонки «bash» необхідно вказувати останнім параметром [4].

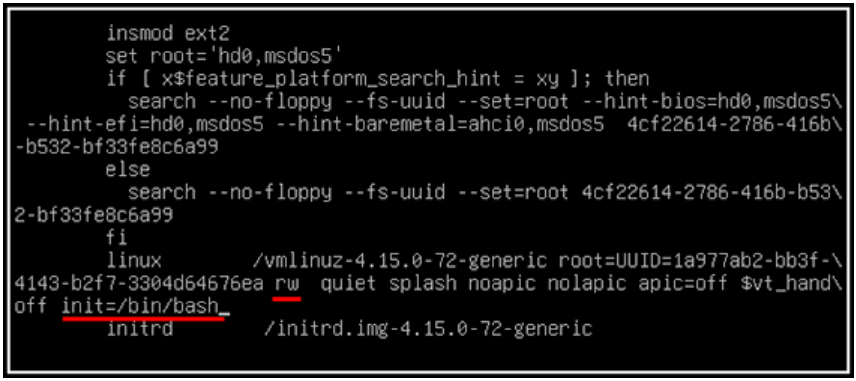

Рис 2. **Вигляд параметрів завантаження**

По закінченню редагування варто продовжити завантаження з заданими параметрами. Відразу після запуску завантажувача він здійснить передачу зазначених параметрів ядру операційної системи, яка в свою чергу здійснить ініціалізацію інтерфейсу командного рядка «bash».

Варто зазначити, що в окремому випадку, котрий розглядається в даній роботі та найчастіше зустрічається працівникам Черкаського НДЕКЦ МВС за напрямком комп'ютерно-технічних досліджень, дешифрування розділів здійснюється програмним засобом «cryptsetup» в автоматичному режимі безпосередньо перед завантаженням операційної системи. Тобто на етапі ініціалізації командного рядка «bash» захищені розділи вже знаходяться в дешифрованому вигляді (рис. 3).

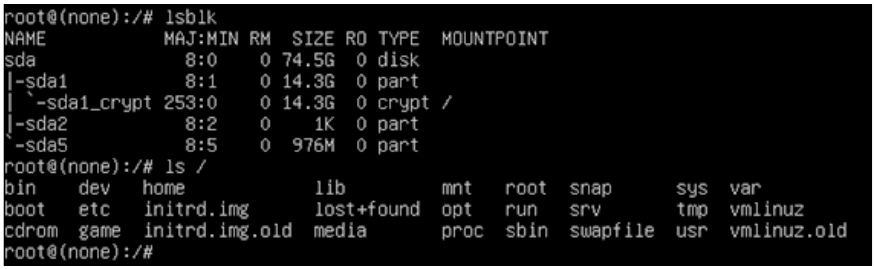

Рис 3. **Вигляд блокових пристроїв та вмісту кореневого каталогу**

В рамках подальшого дослідження, судовий експерт може застосувати будь-які навички чи інструменти, що зазвичай застосовуються до носіїв інформації без ознак криптографічного захисту інформації. Один з шляхів

подальшого дослідження – копіювання декодованого носія інформації на носій інформації експерта (наприклад засобом «dd», що встановлений за замовчуванням в більшості UNIX-подібних операційних систем) та проведення подальшого дослідження класичними методами.

Як один з подальших шляхів дослідження, можна запропонувати проведення аналізу конфігураційних файлів операційної системи та програмного забезпечення з метою виявлення параметрів декодування – ключової послідовності, паролю, тощо. В першу чергу варто провести аналіз налаштувань програмного засобу «cryptsetup», адже саме цим засобом проводиться декодування розділів, захищених методами криптографічного захисту за специфікацією «LUKS».

Також на даному етапі можна провести зміну паролю суперкористувача «root», що дозволить отримати доступ до системи в ході її функціонування. Отримавши доступ до системи, відкривається можливість проведення досліджень запущених процесів, тимчасових файлових систем, змонтованої структури файлів та каталогів, результуючих конфігураційних файлів, тощо.

Підсумовуючи вищевикладене можна сказати, що в експертній практиці все частішими є випадки, коли дослідження внутрішніх алгоритмів функціонування працюючої системи є ключовим аспектом в можливості проведення подальших досліджень. Адже отримати доступ до даних, що захищені методами криптографічного захисту за специфікацією «LUKS», практично не можливо без дослідження операційної системи в динаміці.

Розглянутий алгоритм дозволяє отримати доступ до даних, захищених методами криптографічного захисту за специфікацією «LUKS», без використання парольних фраз, ключів, тощо. В рамках проведення експертного експерименту, застосовуючи описаний алгоритм модифікації параметрів завантажувача «GRUB» можливо не тільки декодувати зашифровані дані, а й дослідити внутрішні процеси вже працюючої операційної системи, отримати доступ до динамічних файлових систем, тощо.

Також варто зазначити, що вищезазначений алгоритм успішно апробовано при проведенні досліджень працівниками відділу комп'ютерно-технічних та телекомунікаційних досліджень Черкаського науково-дослідного експертно-криміналістичного центру МВС України. Неодноразовим практичним застосуванням описаного алгоритму модифікації завантажувача «GRUB» для отримання доступу до захищеної інформації, підтверджено його працездатність, детермінованість та ефективність.

Список використаних джерел:

[1] Usage Statistics and Market Share of Linux for Websites, April 2020. (2020). Вилучено з: https://w3techs.com/technologies/details/os-linux;

[2] Уорд, Б. (2016). Внутреннее устройство Linux. СПб.: Питер. ISBN 978-5-496-01952-1

[3] Negus, C. (2015). Linux Bible, Ninth Edition. Indianapolis, IN: John Wiley & Sons, Inc. ISBN: 978-1-118-99987-5;

[4] Кетов, Д. В. (2017). Внутреннее устройство Linux. СПб.: БХВ-Петербург. ISBN 978-5-9775-3580-9.