Національний технічний університет України «КПІ ім. Ігоря Сікорського»
Факультет Інформатики та Обчислювальної Техніки
Кафедра Автоматизованих Систем Обробки Інформації та Управління

Лабораторна робота №4

з дисципліни «Системи Безпеки Програм і Даних»

Виконав:
студент гр. ІС-91
Мягков Герман

Київ – 2021

Зміст

1 Постановка задачі

Лаб. Робота 4. Розробка програми моніторингу безпеки для виявлення небезпечних або аномальних дій користувачів. Програма забезпечує ведення операційного журналу (ОЖ) реєстрації всіх дій користувачів при зверненні до логічних дисків, файлів, службовим програмам. У ОЖ фіксується час і виділяються особливі події - звернення до системних таблиць, зашифрованих файлів, а головне фіксуються всі відмови в доступі: куди звертався і коли отримав відмову. За даними ОЖ формується список небезпечних або аномальних дій кожного користувача і шаблони їхньої нормальної роботи.

2 Розв’язок

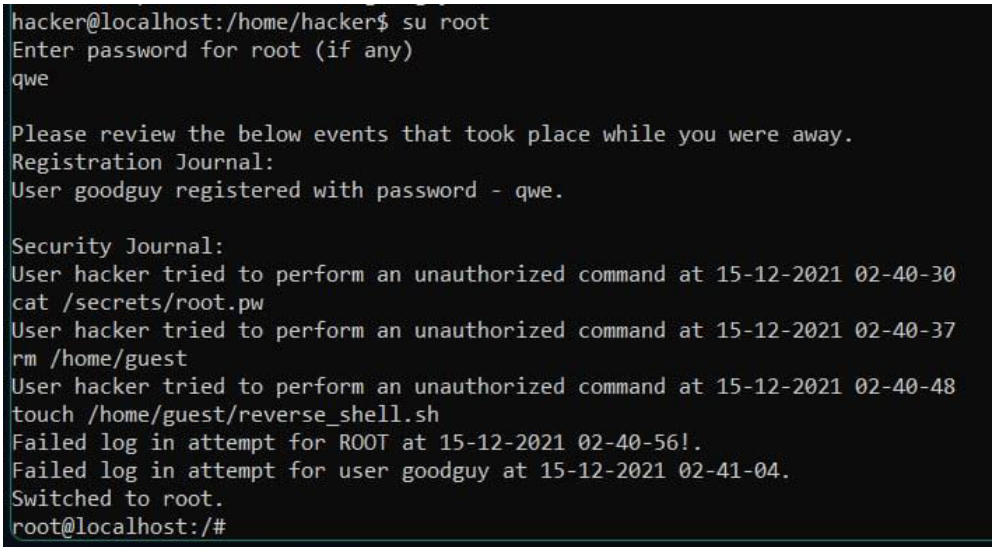
Реалізація завдання цієї лабораторної роботи базується на механізмі журналів із попередньої роботи.

На захищеному носію створюється ще один допоміжний журнал – sec.jrn. Цей файл фіксує усі відмови в доступі, неавторизовані команди користувачів, час коли користувач викликав цю команду, та події блокування користувачей.

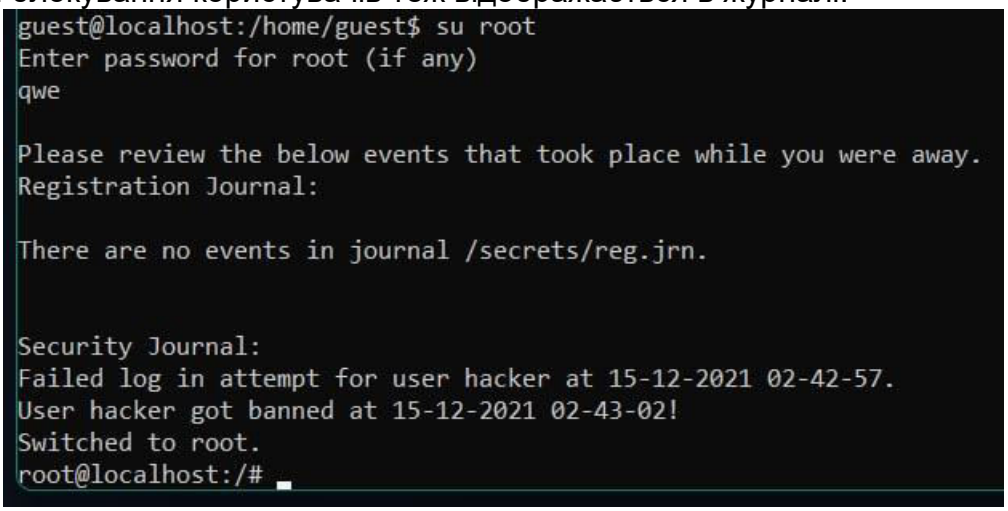
При вході адміністратора у свій обліковий запис («root»), програма надає список усій подій з журналу безпеки.

- Користувач hacker виконує декілька небезпечних команд та отримує відмову в доступі на кожну з них:

- Усі ці відмови фіксуються в журналі та надаються адміністратору при вході в його обліковий запис:



- Фіксація блокування користувачів теж відображається в журналі:



3 Лістинг програми

GitHub:
https://github.com/ldvy/infosec/tree/main/lab4