

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

Зміст

Зміст	2
1 Постановка задачі	3
2 Розв'язок	4
3 Лістинг програми	5

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 усіх подій з журналу безпеки.

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

```
hacker@localhost:/home/hacker$ cat /secrets/root.pw
sh: cat /secrets/root.pw :Permission denied.
hacker@localhost:/home/hacker$ rm /home/guest
sh: rm /home/guest :Permission denied.
hacker@localhost:/home/hacker$ touch /home/guest/reverse_shell.sh
sh: touch /home/guest/reverse_shell.sh :Permission denied.
hacker@localhost:/home/hacker$ su root
Enter password for root (if any)
wrong_password
Incorrect password for user root.
hacker@localhost:/home/hacker$ su goodguy
Enter password for goodguy (if any)
wrong_password
Incorrect password for user goodguy or user doesn't exist.
```

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

```
hacker@localhost:/home/hacker$ su root
Enter password for root (if any)
qwe

Please review the below events that took place while you were away.
Registration Journal:
User goodguy registered with password - qwe.

Security Journal:
User hacker tried to perform an unauthorized command at 15-12-2021 02-40-30
cat /secrets/root.pw
User hacker tried to perform an unauthorized command at 15-12-2021 02-40-37
rm /home/guest
User hacker tried to perform an unauthorized command at 15-12-2021 02-40-48
touch /home/guest/reverse_shell.sh
Failed log in attempt for ROOT at 15-12-2021 02-40-56!.
Failed log in attempt for user goodguy at 15-12-2021 02-41-04.
Switched to root.
root@localhost:/#
```

- Фіксація блокування користувачів теж відображається в журналі:

```
guest@localhost:/home/guest$ su root
Enter password for root (if any)
qwe

Please review the below events that took place while you were away.
Registration Journal:

There are no events in journal /secrets/reg.jrn.

Security Journal:
Failed log in attempt for user hacker at 15-12-2021 02-42-57.
User hacker got banned at 15-12-2021 02-43-02!
Switched to root.
root@localhost:/#
```

3 Лістинг програми

GitHub:

<https://github.com/ldvy/infosec/tree/main/lab4>