CTF Code

Writeups

Forensics

8 октября 2021 г.

Оглавление

Easy

1 <Название>

Теги:

> <условие задачи>

2 Just log in

Теги: Виртуальная машина, сброс пароля, дамп памяти

> <условие задачи>

Нам дается запароленная виртуалка с Windows 7. Хакер, который ее использовал был явно не самым аккуратным человеком, это видно, стоит только зайти. Ну кто будет хранить флаги на рабчоем столе? По сути, вся задача сводится к гуглингу "как сбросить пароль на Windows 7"или, более умный путь решения, знания из которого пригодятся в последней задачи ветки - вытащить из данного дампа памяти с помощью Volatility и плагина mimikatz.
Флаг: `oren_ctf_Shellshock!`

Medium

1 <Название>

Теги:

<условие задачи>

2 <Название>

Теги:

<условие задачи>

Hard

1 <Название>

Теги:

<условие задачи>

Real life

1 <Название>

Теги:

<условие задачи>