CTF Code

Writeups

Admin

14 октября 2021 г.

Оглавление

Easy

1 Are you true admin?

Теги: Логи

<условие задачи>

Нам даны два лога подключения: по FTP и по SSH соответственно. Если их открыть FTP лог, то пароль пользователя выглядит уж слишком похожим на base64. И действительно, если прогнать, то это выглядит как кусок флага. А после в SSH логе можно заметить, что ник похож на вторую часть флага в base64. Таким образом, просто два раза по base64 и получаем флаг `oren_ctf_goto_ComRAT!`

2 Do you like black terminals with green text?

Теги: Web, шифрование, brainfuck

<условие задачи>

Нам дан сайт, который с первого взгляда абсолютно пуст. Но если посмотреть в develop-консоль, то можно увидеть, что сайт выдает туда некий base64. При расшифровке получаем:

```
Welcome aboard. Your secret phrase is "hyperion".
Maybe you will need this: ----[-->+++++<]>.------.++++.--.+++[->+++<]>.[--->+<]>-.
++[->+++<]>.[--->+<]>--.+[->+++<]>.----------.[--->+<]>++.+++++.---.[------>+<]>.
[--->++<]>+++++.[->++++++<]>+++.[->+++<]>+.+++++.-----.[----->++<]>+.+[----->+<]>.
++[---->+<]>++.|
```

Последнее очень похоже на эзотерический язык программирования brainfuck. И действительно, если выполнить эту программу любым интерпретатором, то можно получить `vptr_tbt_VtyviKzotpaz!`, что оооочень напоминает по формату флаг. Остается вспомнить, какие шифры требуют ключ. Первым, как самым популярным, на ум приходит шифр Виженера. И действительно, если прогнать через любой расшифровщик, то получаем `oren_ctf_ImageTragick!`

Medium

1 Use your head

Теги: User-agent, SHA1, requests

> <условие задачи>

При переходе по ссылке внезапно оказывается, что сайт не любит гостей. Но если посмотреть на заголовок ответа, то можно увидеть, что нам предлагают перейти по какой-то ссылке. Похоже на какой-то хеш. Если посчитать количество символов, то можно понять, что это SHA1, символов ровно 20 штук. Брут ничего не дает, поэтому можно просто перейти. Опять предложение перейти по ссылке и уже ответ, что мы забанены. Тогда можно написать простой питоновский скрипт, который просто ходит по ссылкам. В конце концов, судя по названия таска, где-то в конце будет флаг

```
from urllib.request import urlopen, Request
import sys


def get_next_message(hash_str, const):
    new_request = Request(
        url="http://{}/".format(sys.argv[1]) + hash_str,
        headers={'User-Agent': "snake3.smth + {}".format(const)}
    )
    print(hash_str)
    return urlopen(new_request).msg


i = 0
global_hash_string = get_next_message("", i)
while "oren_ctf" not in global_hash_string:
    i += 1
    print(i, global_hash_string)
    global_hash_string = get_next_message(global_hash_string.split()[-1], i)
print(global_hash_string)
```

И действительно, в конце концов получаем флаг `oren_ctf_DUHK!`

Hard

1 Just ping me

Теги: ICMP, Network analysis

> <условие задачи>

Дан единственный ICMP-запрос на хост. Но он выглядит не как стандартный ICMP - в секции данных что-то еще спрятано. Первое желение - послать такой же запрос на хост. И дейсвительно, в ответ прилетает флаг `oren_ctf_Rowhammer!`