CTF Code

Writeups

Admin

24 октября 2021 г.

Оглавление

Easy

1 Are you true admin?

Теги: Логи

> Мы почти поймали злостного хакера haxor! Даже получили логи его подключения на серверы по SSH и FTP. Но не можем понять, что именно он хочет... Вся надежда только на вас! Эти логи определенно как-то связаны, нужно только понять, как именно.

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

> Мы обнаружили, что haxor работает не один! Даже нашли сайт его группировки. Кажется, где-то там есть флаг

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

> По следам группировки haxor'a мы пришли на какой-то сайт, который очень сильно не хочет взаимодействовать с нами. Возможно, у вас получится что-то достать оттуда?

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

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

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


def main():
    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],

    print(global_hash_string)


if __name__ == "__main__":
    main()
```

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

2 Bash escape

Теги: BASH jail escape

> Кажется, это один из серверов, с которых их группировка проводит атаки на пользователей. Но только шелл какой-то очень странный. Какие-то коровы и никаких флагов.
> nc ctf-edu-t.orb.ru 1893

После попадания на сервер становится понятно, что либо что-то не так с переменной `PATH` (или, возможно, сделаны алиасы для комманд на чтение), либо все пропатченно. После попытки сделать `/bin/ls` становится понятно, что патчей нет, а просто сделаны алиасы или измененна переменная `PATH`, что не так уж важно. Прямо в нашей дирректории лежит флаг. Делаем `/bin/cat flag.txt` и получаем флаг `oren_ctf_Drupalgeddon!`

Hard

1 Too many files

Теги: Find file, diff the files

> Окей. В их сети обнаружился еще один сервер. На этот раз с шеллом все в порядке, даже удалось сбрутить праоль одного из пользователей. Но вот колчество файлов там поражает. Возможно, есть какой-то способ быстро найти нужный?..
> P.S. Пароль от user1 - find32
> ssh user1@ctf-edu-t.orb.ru -p 1653

Заходим на сервер с данным нам паролем и видим некоторое количество дирректорий, в которых еще больше файлов. Ручками все это перебирать невозможно. Попробуем погрепать, возможно, что-то красивое действительно сможем найти:

```
$ grep -irs oren_ctf
........grep -irs oren_ctf_not_the_flag!{user2:AAE976A5232713355D58584CFE5A5}.......
```

Выглядит как пароль пользователя. Попробуем зайти под этого пользователя. На этот раз количество файлов куда меньше, но количество строк не сильно уменишлось. Первое желание в такой ситуации - продиффать файлы, больше все равно ничего не остается. И действительно, все файлы одинаковые, кроме одного:

```
$ diff adgsfdgasf.js sadsas.tx
42391a42392
> Rowhammer
```

Попробуем обернуть в `oren_ctf_!` и сдать. Действительно, это и есть искомый флаг.

Real life

1 Just read the flag

Теги: Escape chroot, ssh keys

> Все, конец им! Мы нашли главный сервер. Но вот шелл там просто ужас - не выдает ошибок и нужного файла нигде не видно. Как же найти флаг?
> nc ctf-edu-t.orb.ru 1934

Мы можем исполнять все команды, но вот флага нигде нет. Тогда на ум приходит в идея, что мы находимся в chroot и нужно как-то выйти из него. Если немного побродить по файловой системе, то можно увидеть, что в `.ssh` домашней дирректории рута лежит ssh-ключ, по которому так же можно логиниться. Логинимся `ssh -i /root/.ssh/id_rsa -o StrictHostKeyChecking=no root@localhost` и получаем в ответ флаг `oren_ctf_NAME:WRECK!`