Uvod

Bezpecnost informacnych systemov z pohladu praxe

Peter Svec

>motivacia

>binary exploitation
>**C**apture **T**he **F**lag (CTF)[1]
>preco?
    >pochopenie ako funguju programy na nizkej urovni
    >zlepsenie analytickeho myslenia
    >ovladanie terminalu
    >moznost stat sa lepsim programatorom

[1]https://ctftime.org/

>predpoklady

>PROG-1, PROG-2, AP, OS, UPB
>C, python
>zaklady prikazoveho riadku
>ladenie v GDB

>plan

>0x1. Uvod + Jazyk symbolickych instrukcii (assembler)
>0x2. Shellcoding (10b)
>0x3. Shellcoding
>0x4. Reverzne inzinierstvo (10b)
>0x5. Reverzne inzinierstvo
>0x6. Pamatove zranitelnosti (10b)
>0x7. Pamatove zranitelnosti
>0x8. Navratovo orientovane programovanie (10b)
>0x9. Navratovo orientovane programovanie
>0xA. Exploitacia (10b)
>0xB. Exploitacia
>0xC. .*

>hodnotenie

>riesenie uloh v mensich timoch (1-3)
>kazdy blok bude obsahovat **N** uloh
    >stupnujuca narocnost
    >pocet uloh v zavislosti od bloku (1-10)
>kazda vyriesena uloha za 10/**N** bodov
>celkovo 50 bodov (zapocet 25)
>prve **3** timy, ktore najrychlejsie vyriesia blok ziskavaju bonus (1.5b - 1b - 0.5b)
>najlepsie **3** timy na konci semestra ziskaju fyzicke ceny :O
>bonus za tematicky **meme**

>riesenie uloh

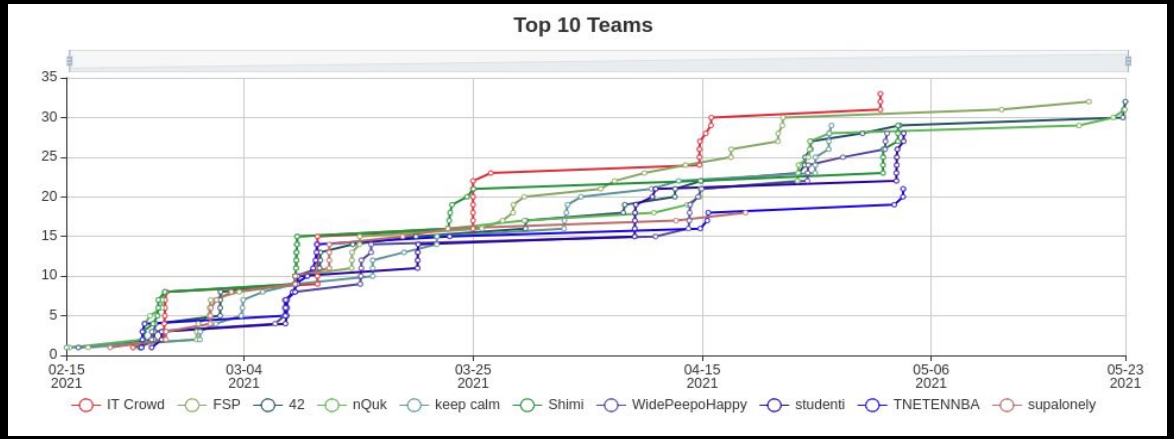
>pwn.college infrastruktura na cloude
>riesenie uloh v kontajneroch (vzdialeny pristup cez ssh)
>zranitelny binarny subor (suid bit - root)
>flag (maly textovy subor) citatelny iba rootom
>cielom je najst exploit na binarny subor a precitat obsah suboru flag

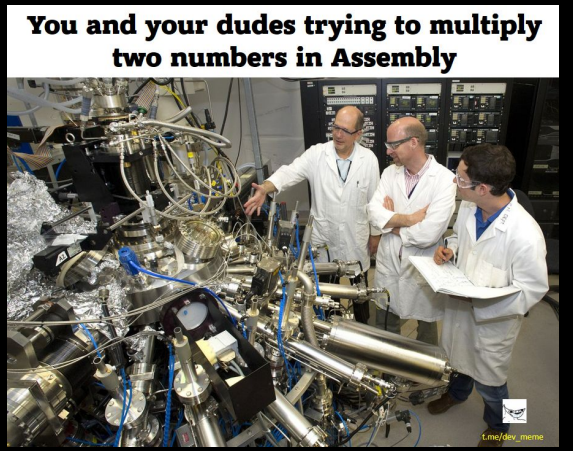
Zapocitanie bodov:
- >submit spravnej hodnoty flagu (nahodne generovany)
- >na konci bloku odovzdat do AIS zdrojove kody
- >ziadna dokumentacia!

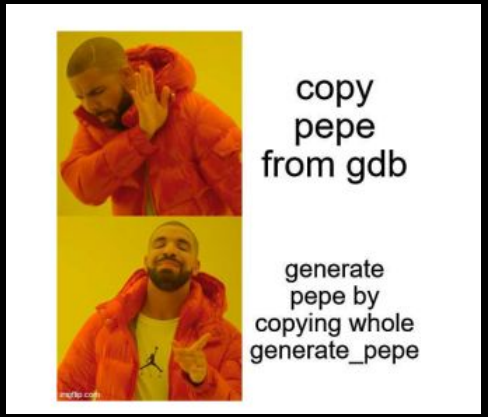
>do dalsieho tyzdna

>zlozit timy
>nahlasenie timu (do DM alebo mail):
    >nazov timu
    >clenovia timu (skutocne meno + discord meno)
>po zverejneni stranky (najneskor v pondelok):
    >veduci timu vytvori konto s nazvom timu + SSH kluce
    >konto bude zdielane v ramci timu

>rocnik 2021


Top 10 Teams
35
30
25
20
15
10
5
0
02-15 2021
03-04 2021
03-25 2021
04-15 2021
05-06 2021
05-23 2021
IT Crowd
FSP
42
nQuk
keep calm
Shimi
WidePeepoHappy
studenti
TNETENNBA
supalonely


You and your dudes trying to multiply two numbers in Assembly
t.me/dev_meme


copy pepe from gdb
generate pepe by copying whole generate_pepe


I think I forgot something.
If you forgot, then it wasn't important.
Yeah, you're right.


After all these years
Finally I have them all


ITS OVER...
ITS FINALLY OVER...