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 **dvojclennych** timoch
>kazdy blok bude obsahovat **N** uloh
    >stupnujuca narocnost
    >pocet uloh v zavislosti od bloku (1 az **N**)
>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

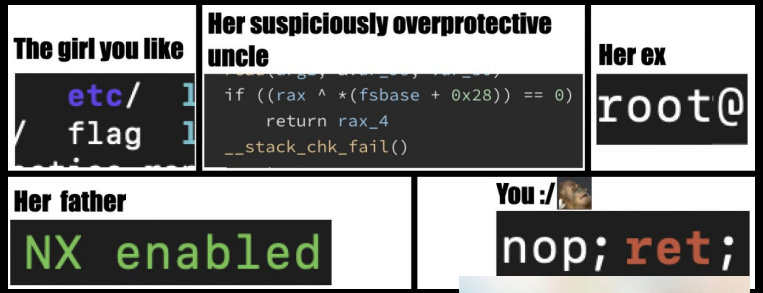
>pwn.college infrastruktura na cloude
>riesenie uloh v kontajneroch (vzdialeny pristup cez ssh)
>zranitelny binarny subor (suid bit - root)
>flag (maly textovy subor) citatelny iba rootom
>cielom je najst exploit na binarny subor a precitat obsah suboru flag

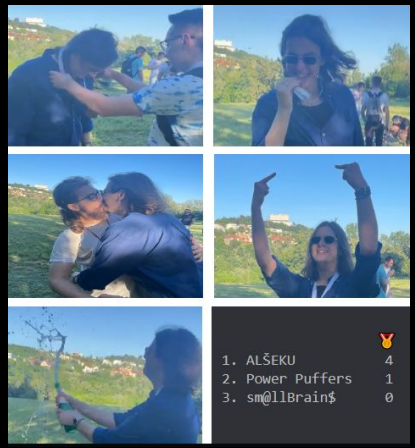
Zapocitanie bodov:
- >submit spravnej hodnoty flagu (nahodne generovany)
- >pozor na kradnutie flagov!
- >na konci bloku odovzdat do AIS zdrojove kody
- >ziadna dokumentacia!

>do dalsieho tyzdna

>zlozit timy
>nahlasenie timu (do DM alebo mail):
    >nazov timu
    >clenovia timu (skutocne meno + discord meno)
>registracia vsetkych clenov na **feictf.xyz**
>veduci timu vytvori tim na stranke (dalsi clen sa prida)
>vyriesenie **introduction** ulohy

>rocnik 2022





https://www.youtube.com/watch?v=QCSKzPZoSjI&t=1s&ab_channel=PavolSobota

0x07