Uvod

Bezpecnost informacnych systemov z pohladu praxe

Peter Svec

>motivacia

>binary exploitation, web, sandbox escape, race conditions…
>**C**apture **T**he **F**lag (CTF)[1]
>preco?
- >pochopenie ako funguju programy/web na nizkej urovni
- >zlepsenie analytickeho myslenia
- >ovladanie terminalu
- >moznost stat sa lepsim programatorom

[1]https://ctftime.org/

>vyucujuci

- > Peter Svec (reverse/memory/exploit)
  - > peter.svec1@stuba.sk
  - > discord -> petersvec/root
- > Palo Litauszki (web/system/exploit)
  - > discord -> palowashere

>predpoklady

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

>plan

>0x1. Uvod + Jazyk symbolickych instrukcii (assembler)
>0x2. Reverzne inzinierstvo (10b) -> reverse
>0x3. Reverzne inzinierstvo
>0x4. Pamatove zranitelnosti (10b) -> memory
>0x5. Pamatove zranitelnosti
>0x6. Webova bezpecnost (10b) -> web
>0x7. Webova bezpecnost
>0x8. Sandbox/Race conditions (10b) -> system
>0x9. Sandbox/Race conditions
>0xA. Exploitacia (10b) -> exploit
>0xB. Exploitacia
>0xC. .*

>hodnotenie

>riesenie uloh v **trojclennych** 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 (3b - 2b - 1b, moze sa vsak menit)
>celkovy vitaz - olympijsky system (zlato:3, striebro:2, bronz:1)
>najlepsie **3** timy na konci semestra ziskaju fyzicke ceny :O

>riesenie uloh

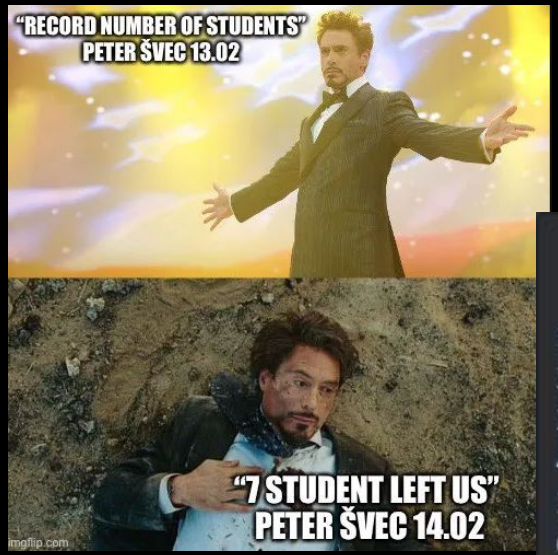
>pwn.college infrastruktura na cloude
>riesenie uloh v kontajneroch (vzdialeny pristup cez ssh)
>zranitelny binarny subor (suid bit - root)
>flag (maly textovy subor) citatelny iba rootom
>cielom je najst exploit na binarny subor a precitat obsah suboru flag

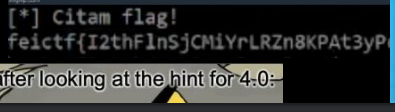
Zapocitanie bodov:
- >submit spravnej hodnoty flagu (nahodne generovany)
- >na konci bloku odovzdat do AIS dokumentaciu a zdrojove kody
- >pozor na kradnutie flagov!
- >pozor na kradnutie zdrojovych kodov!

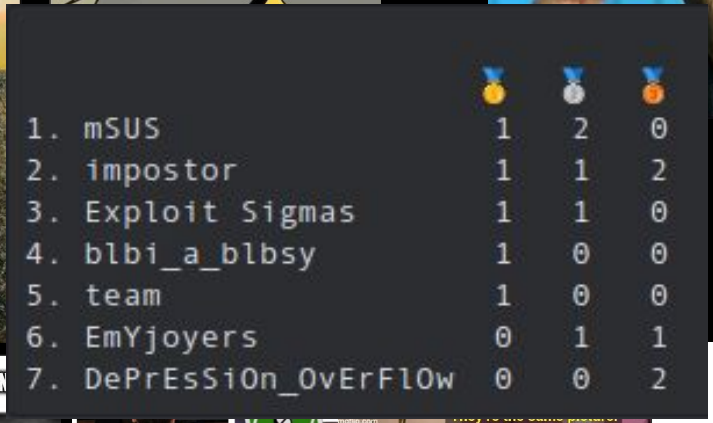
>do dalsieho tyzdna

>zlozit timy
>nahlasenie timu (do DM na discorde 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 2023







		🥇	🥈	🥉
1.	mSUS	1	2	0
2.	impostor	1	1	2
3.	Exploit Sigmas	1	1	0
4.	blbi_a_blbsy	1	0	0
5.	team	1	0	0
6.	EmYjoyers	0	1	1
7.	DePrEsSiOn_OvErFlOw	0	0	2

0x09