Úvod

Bezpečnosť informačných systémov z pohľadu praxe

Peter Švec

>Motivácia

>binary exploitation, web, sandbox escape, shellcoding…
>**C**apture **T**he **F**lag (CTF)[1]
>prečo?
    >pochopenie ako fungujú programy/web na nízkej urovni
    >zlepšenie analytického myslenia
    >ovládanie terminálu
    >možnosť stať sa lepším programátorom

[1]https://ctftime.org/

>Vyučujúci

- > Peter Švec (reverse/shellcode/memory)
  - > peter.svec1@stuba.sk
  - > discord -> petersvec/root
- > Pavol Litauszki (system/web/exploit)
  - > qlitauszki@stuba.sk
  - > discord -> palowashere

>Predpoklady

>B-PROG1 (programovanie v Python)
>B-PROG2 (programovanie v C)
>B-API (logické operácia, hexadecimálna sústava)
>B-OS (procesy, virtuálna pamäť, zásobník, GDB, terminál)
>I-UPB (základné pojmy z bezpečnosti)
>B-DBS (základy SQL)

>Plán semestra

>0x1. Úvod + Reverzné inžinierstvo (8b) -> reverse
>0x2. Reverzné inžinierstvo konzultácia
>0x3. Shellcoding (8b) -> shellcode
>0x4. Shellcoding konzultácia
>0x5. Pamäťové zraniteľnosti (8b) -> memory
>0x6. Pamäťové zraniteľnosti konzultácia
>0x7. System hacking (8b) -> system
>0x8. System hacking konzultácia
>0x9. Webová bezpečnosť (8b) -> web
>0xA. Webová bezpečnosť konzultácia
>0xB. Exploit (10b) -> exploit
>0xC. Exploit konzultácia

>Hodnotenie

>Riešenie úloh v **dvojčlenných** tímoch
>Každý blok bude obsahovať **N** úloh
    >stupňujúca náročnosť
    >stupňujúci počet bodov za úlohu
>Celkovo 50 bodov (zápočet 25)
>Bonusové body:
    >Vyriešenie všetkých úloh v bloku +1b
    >Kreatívne riešenie +1b
    >Celkový víťaz (zlato:3, striebro:2, bronz:1)
        >1.miesto +5b
        >2.miesto +4b
        >3.miesto +3b

>Riešenie úloh

>**pwn.college** infraštruktúra na školskom cloude
>Riešenie úloh v Docker kontajneroch (vzdialený prístup cez **SSH**)
>Zraniteľný binárny súbor (suid bit - root)
>**flag** (malý textový súbor) čitateľný iba rootom
>Cieľom je nájsť exploit na binárny súbor a prečítať obsah súboru **flag**

Započítanie bodov:

>Submit správnej hodnoty flagu (náhodne generovaný)
>Na konci bloku odovzdať do AIS **dokumentáciu** a **zdrojové kódy**
>Pozor na kradnutie flagov!
>Pozor na kradnutie zdrojových kódov!
>**Pracujú OBAJA členovia tímu!!!**

>Čo spraviť dnes? (ideálne)

>Zložiť tímy
>Nahlásenie tímu (do DM na discorde/mail/osobne):
    >Názov tímu
    >Členovia tímu (skutočné meno + discord meno)
>Registrácia všetkých členov na **feictf.xyz**
>Jeden člen vytvorí tím na stránke (druhý sa pridá)
>Vyriešenie **introduction** úlohy

>Ako riešiť úlohy?

>Vygenerovanie SSH kľúča (**ssh-keygen** nástroj)
>Nastavenie verejného kľúča v profile
>Spustenie úlohy
>Pripojenie sa cez SSH:

ssh -i ./key hacker@feictf.xyz