Exploit

Bezpecnost informacnych systemov z pohladu praxe

Peter Svec

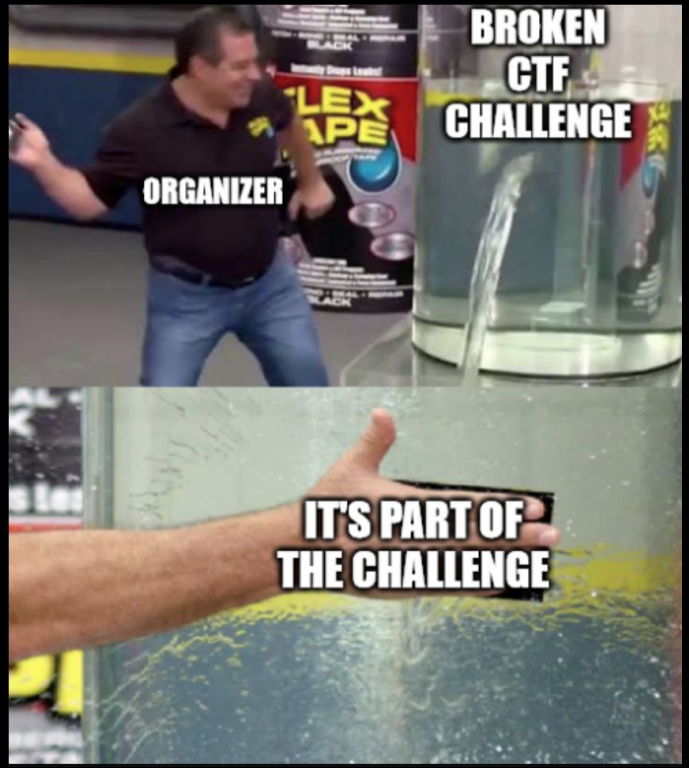
>rop vysledky

All Time Rankings

Rank		Hacker	Score
#1		ALŠEKU	35
#2		Power_Puffers	35
#3		Team7	33
#4		FIIT_Dropouts	32
#5		tichoslapos_divocakos	31

>uvod

>koniec practice prikladom
>ulohy podobne skutocnym CTF uloham
>dalsie exploit koncepty:
    >jmp2shellcode
    >stack pivoting
    >format string



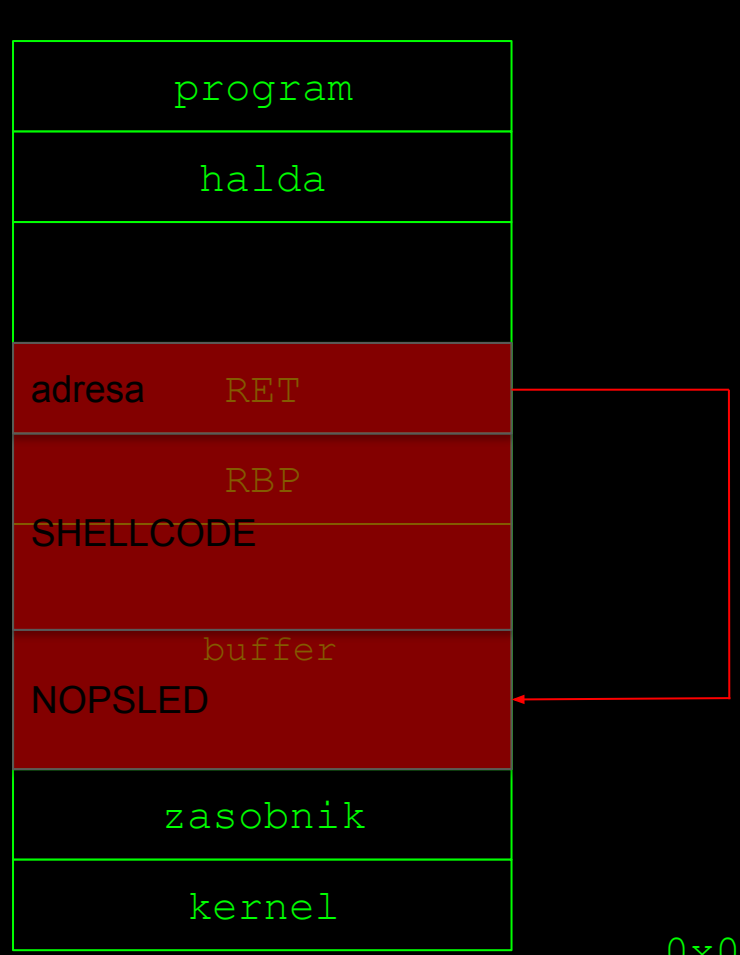
>jmp2shellcode

>popularna technika v 90s
>namiesto AAAAAA… vlozit shellcode a navratovu adresu prepisat adresou buffra
>NX vsak zabrani spusteniu takeho kodu (unless…)

>jmp2shellcode

>ako najst adresu?
    >ASLR ON - information leak
    >ASLR OFF - GDB
>preco nopsled?
    >zarovnanie zasobnika je
     rozne pri kazdom spusteni
     (premenne prostredia)

    >nopsled zabezpeci, ze aj ked
     nevieme presnu adresu, tak
     sa dostaneme ku shellcodu



>stack pivoting

>co ked mame iba limitovany overflow a vieme zapisat iba par bajtov? (malo miesta na rop chain)
>vyrobime si novy stack!

```
pop rsp
ret
```

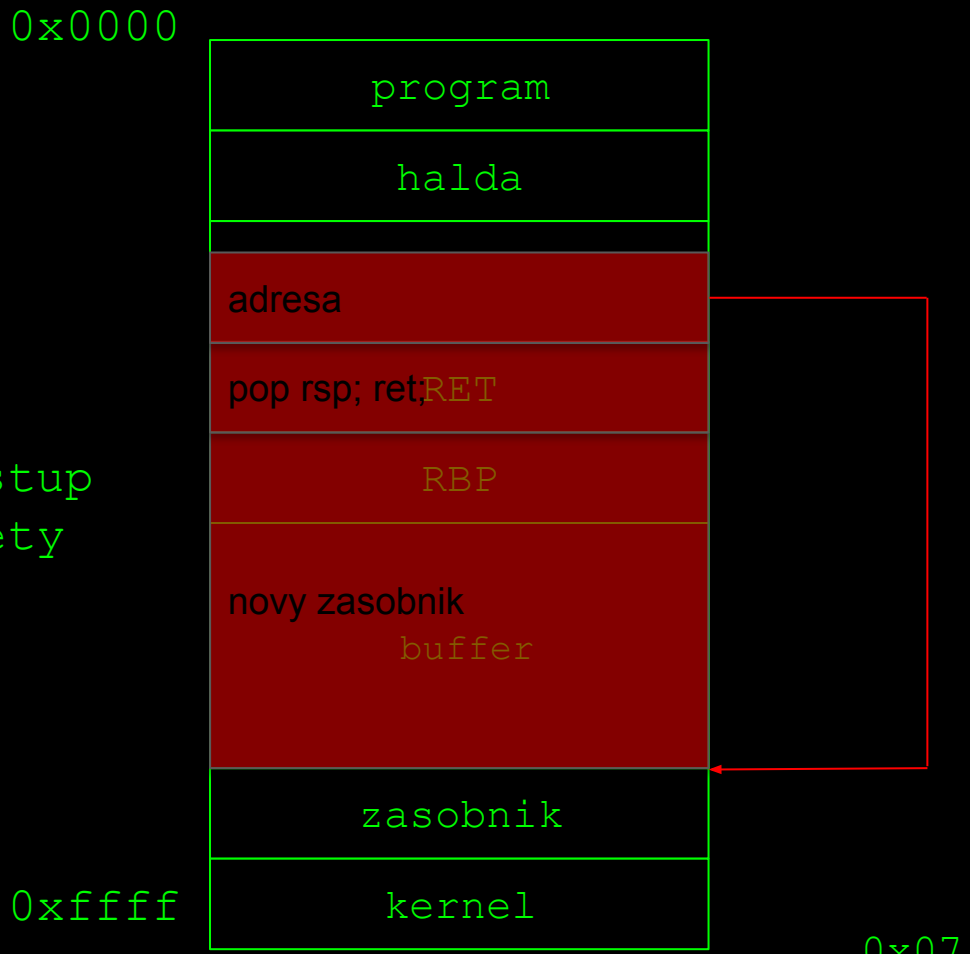
```
xchg rax, rsp
ret
```

>stack pivoting

>miesto na spustenie jedneho gadgetu

>vytvorime novy zasobnik v pamati kde sa nachadza nas vstup a umiestnime tam zvysne gadgety

>musime vsak poznat adresu (leak)



>format string

>zranitelnost patriaca do minulosti (obcas sa vsak vyskytne, najma ako information leak)
>zvykne sa objavit aj na CTFkach
>je mozne dosiahnut aj arbitrary write (nielen read)

```
char buffer[80];
printf(buffer);
```

vstup: '%p %p %p %p'
vystup: 0x7fd449f65723 (nil) 0x7fd449e860a7 0x1b

>format string

>ked chceme priamo pristupit k n-temu parametru (napr. 4ty)

printf("%p %p %p **%p**"); vypise vsetky 4 hodnoty
printf("%**4**$**p**"); vypise iba 4tu hodnotu

>ked chceme zapisat na do adresy na 4 pozici hodnotu 100
>formatovaci retazec %n -> na adresu, ktoru poskytneme, zapise pocet doposial zapisanych bajtov

// na 4 adresu zo stacku zapise hodnotu 100
printf("A"*100 + "%4$**n**");

>riesenie uloh

>vyskusat binarku ako funguje, otestovat rozne vstupy
>skontrolovat ochrany voci exploitacii
>zreverzovat binarku za ucelom zistenia ako funguje interne
>navrhnut plan ako riesit exploit
>implementacia exploitu
>ide? idem na dalsiu ulohu
>nejde? GDB!

zaver bispp

19.5. 18:00 pred A (po skuske)
-grilovanie
-odovzdanie cien
-aperol, pivo, vino,...
-atd…