Exploit

Bezpecnost informacnych systemov z pohladu praxe

Peter Svec

>rop vysledky

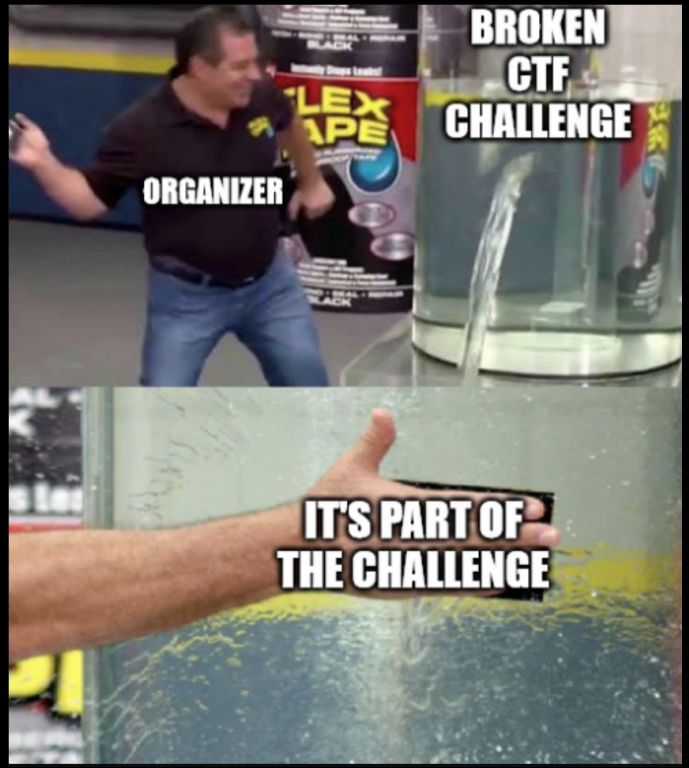
Rank	Team	Score
#1	mSUS	8
#2	impostor	8
#3	DePrEsSiOn_OvErFlOw	8
#4	EmYjoyers	8
#5	Exploit Sigmas	8

celkovy stav ->

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

>uvod

>koniec practice prikladom
>ulohy podobne skutocnym CTF uloham
>dalsie exploit koncepty:
    >jmp2shellcode
    >race condition



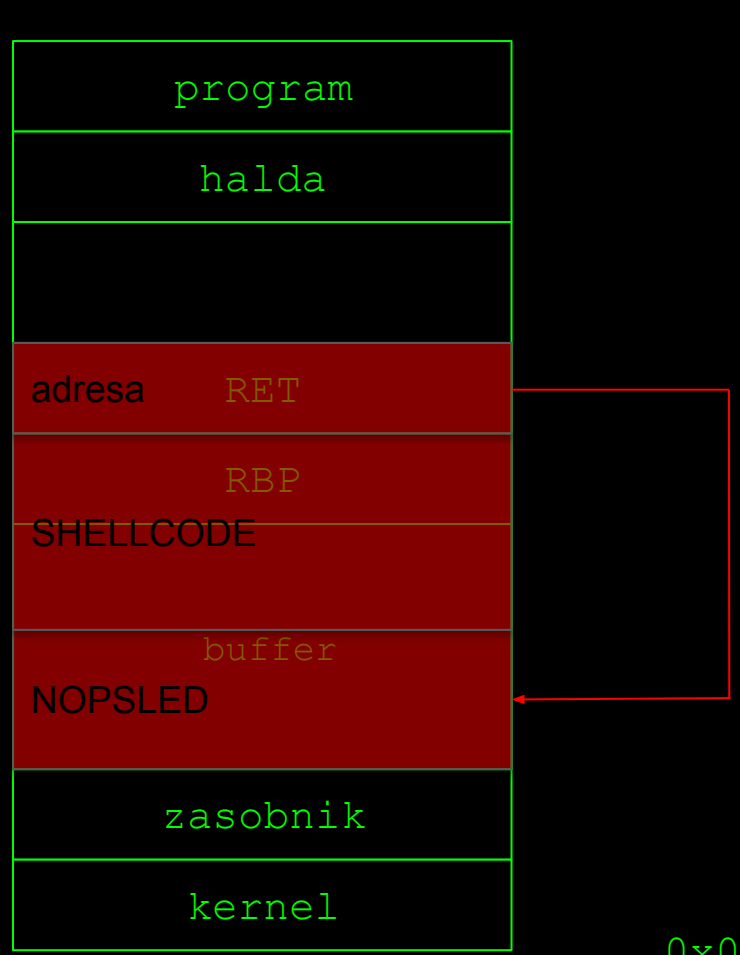
>jmp2shellcode

>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)

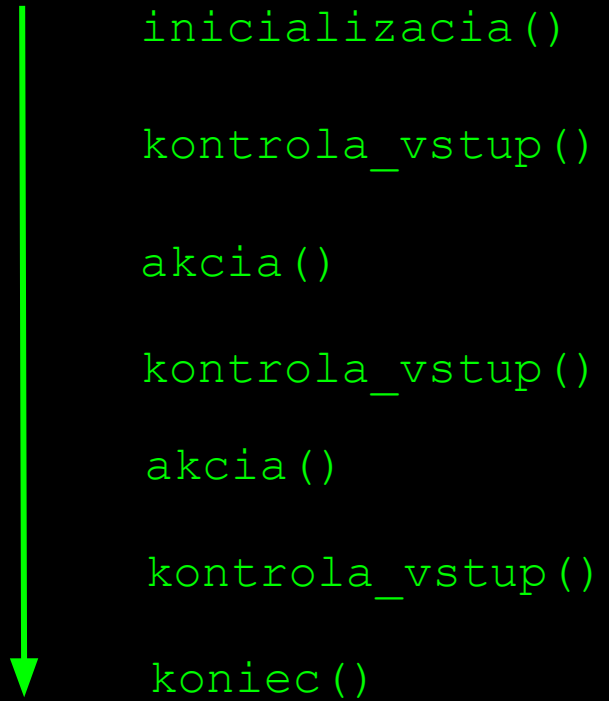
    >nopsled zabezpeci, ze aj ked
     nevieme presnu adresu, tak
     sa dostaneme ku shellcodu



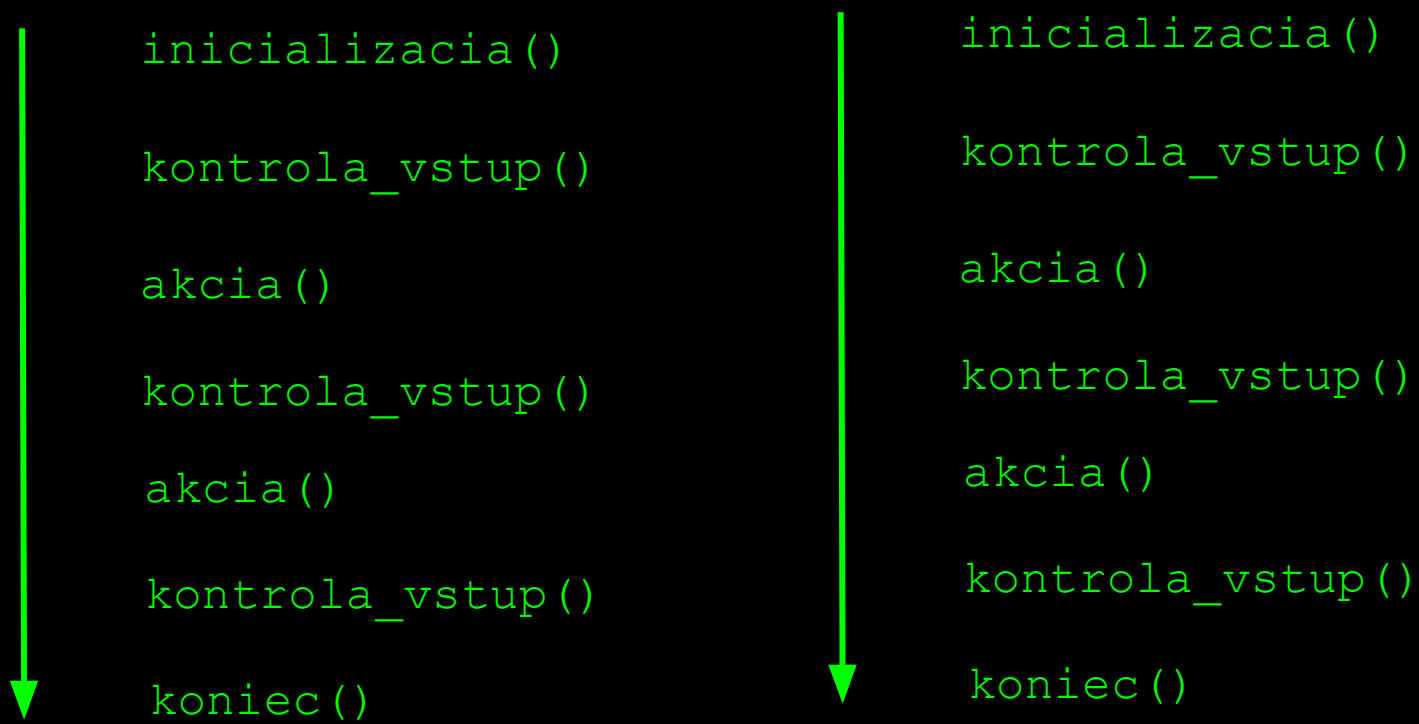
>race condition

>chyby vznikajuce pri paralelnom vykonavani operacii
>TOCTOU chyby (Time of Check - Time of Use)
>subehy na suborovom systeme, vlaknach, pamati…

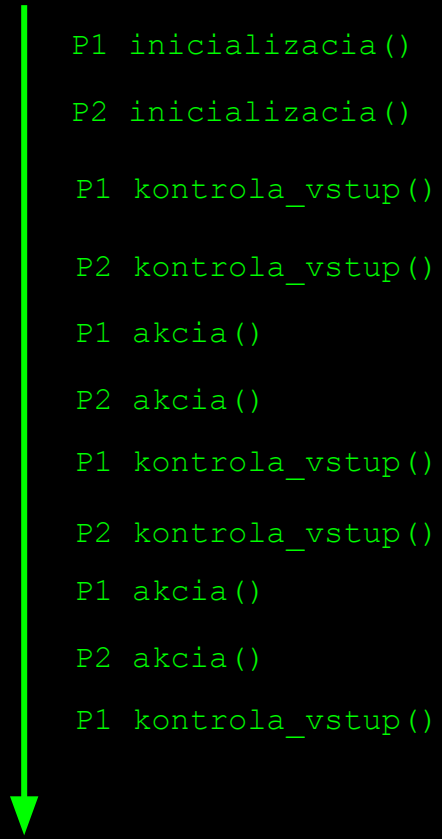
>proces


inicializacia()
kontrola_vstup()
akcia()
kontrola_vstup()
akcia()
kontrola_vstup()
koniec()

>proces


P1
inicializacia()
kontrola_vstup()
akcia()
kontrola_vstup()
akcia()
kontrola_vstup()
koniec()
P2
inicializacia()
kontrola_vstup()
akcia()
kontrola_vstup()
akcia()
kontrola_vstup()
koniec()

>proces


P1 inicializacia()
P2 inicializacia()
P1 kontrola_vstup()
P2 kontrola_vstup()
P1 akcia()
P2 akcia()
P1 kontrola_vstup()
P2 kontrola_vstup()
P1 akcia()
P2 akcia()
P1 kontrola_vstup()

>proces

>mozne usporiadania vykonania procesov:

```
P1 inicializacia()
P2 inicializacia()
P1 kontrola_vstup
P2 kontrola_vstup
P1 akcia()
P2 akcia()
P1 kontrola_vstup
P2 kontrola_vstup
P1 akcia()
P2 akcia()
P1 kontrola_vstup
P2 kontrola_vstup
P1 akcia()
P2 akcia()
P1 koniec()
P2 koniec()
```

```
P1 inicializacia()
P1 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 koniec()
P2 inicializacia()
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 koniec()
```

```
P1 inicializacia()
P1 kontrola_vstup
P2 inicializacia()
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 koniec()
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 koniec()
```

```
P1 inicializacia()
P2 inicializacia()
P1 kontrola_vstup
P2 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 koniec()
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 koniec()
```

```
P2 inicializacia()
P1 inicializacia()
P1 kontrola_vstup
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 akcia()
P2 akcia()
P1 kontrola_vstup
P2 kontrola_vstup
P1 akcia()
P2 akcia()
P1 koniec()
P2 koniec()
```

0x0A

>proces

>...niektore mozu viest ku chybam

```
P1 inicializacia()
P2 inicializacia()
P1 kontrola_vstup
P2 kontrola_vstup
P1 akcia()
P2 akcia()
P1 kontrola_vstup
P2 kontrola_vstup
P1 akcia()
P2 akcia()
P1 kontrola_vstup
P2 kontrola_vstup
P1 akcia()
P2 akcia()
P1 koniec()
P2 koniec()
```

```
P1 inicializacia()
P1 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 koniec()
P2 inicializacia()
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 koniec()
```

```
P1 inicializacia()
P1 kontrola_vstup
P2 inicializacia()
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 koniec()
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 koniec()
```

```
P1 inicializacia()
P2 inicializacia()
P1 kontrola_vstup
P2 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P1 koniec()
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P2 akcia()
P2 koniec()
```

```
P2 inicializacia()
P1 inicializacia()
P1 kontrola_vstup
P2 kontrola_vstup
P2 akcia()
P2 kontrola_vstup
P1 akcia()
P1 kontrola_vstup
P1 akcia()
P2 akcia()
P1 kontrola_vstup
P2 kontrola_vstup
P1 akcia()
P2 akcia()
P1 koniec()
P2 koniec()
```

>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!