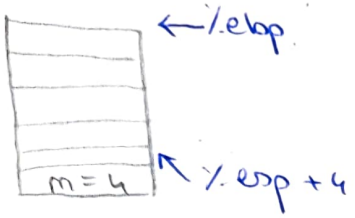
05.12.2023

Tutoriat

- stivă



Dacă adunăm bytes la %esp, stiva scade și o să pointeze mai sus

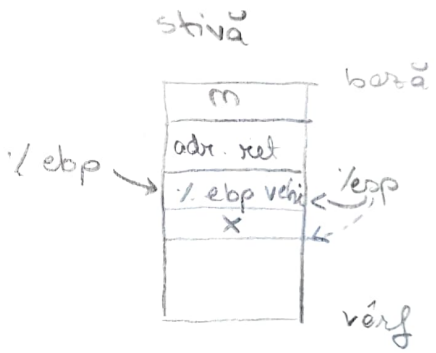
Dacă scădem — " —, stiva crește și o să pointeze mai jos

- data
- text

```
proc
-----
ret
```

- global main

```
main:
    push m
    call proc
    popl %eax
proc:
    pushl %ebp
    movl %esp, %ebp
    push x
    -----
    pop %eax
    popl %ebp
    ret
```



%ebp pointează mereu sus la prima adresă

%esp pointează la ultima valoare adăugată în jos.

→ când mutăm %ebp în %esp, practic îi spunem că de la adresa unde era %esp începe stiva. (pagă devine cuma ultima val/adresă adăugată)

→ revine înapoi la adresa inițială pt a vedea cât de mare e stiva (cred)

- Structura procedurii:

```
proc:
    pushl %ebp
    movl %esp, %ebp
    -----
    popl %ebp
    ret
```

%eax, %ecx, %edx nu se garantează salvarea

%ebx, %esp, %ebp, %esi, %edi se salvează

Dacă instalezi gdb peda, ca să rămâi la gdb normal: gdb -- mx ex
↳ numele fișier