Cheatography

Failles applicatives Cheat Sheet

by PZ. via cheatography.com/33393/cs/10372/

GDB basics

gdb -q `(prog)`	open
set disassembly-flavor `(intel)`	Intel view (AT&T = default)
dissasemble `(main)`	
r	run
b `(addr)`	breakpoint a *addr*
step	step in debug
c	continue
i r	see registers
x/100x `$esp`	see 100 char hexdump from esp
r 111	r with 111 as arg
r `$(python -c 'print "A" * 100')`	

Registres

eip `instruction pointer` : pointeur vers la prohaine instruction à exécuter

ebp `base pointer` : pointeur de base. Il permet d'acéder facilement aux arguments et aux variables

esp `stack pointer` : pointe vers le prochain emplacement libre de la pile

Organisation de l'espace utilisateur

stack est la pile du programme

.bss contient les données globales non initialisées

.data contient les données globales initialisées

.text contient le code du programme

ASCII

30 : 0 || 31 : 1 || 32 : 2..

41 : A || 42 : B || 43 : C

61 : a || 62 : b || 63 : c

Prologue

```
`
push ebp
mov ebp,esp
sub esp,0x18
push eax
`
```

Epilogue

```
`
pop eax
leave
ret
`
```

By **PZ.**
cheatography.com/pz/

Not published yet.
Last updated 30th January, 2017.
Page 1 of 1.