

0x00000000

execve stack allocation on stack-growing-down machines (x86, arm, ...)

ep_minsaddr

ep_ssize

initial stack pointer

Userland program stack

argc

*argv[]

\0

*env[]

\0

auxinfo

arg / env strings

ASLR gap

sigcode

ps_strings

STACK_PTHREADSPACE

copied by copyargs()

copied by elf_copyargs()

ps_strings passed via register argument

0xffffffff

(VM_MAXUSER_ADDRESS)

ps_argvstr
ps_nargvstr
ps_envstr
ps_nenvstr

