

x0 x1 x2 x3 x4 x5 x6 x7 x8 x9 xA xB xC xD xE xF

00x 7F E L F 0A 00 9E 20 28 32 34 39 31 29 00 00

01x 02 00 3E 00 00 00 00 00 AA 00 40 00 00 00 00

02x 4A 00 00 00 00 00 00 00 B4 0E B7 00 B3 00 CD 10

03x 90 90 90 C3 40 00 38 00 01 00 60 B4 02 B7 00 B6

x0 x1 x2 x3 x4 x5 x6 x7 x8 x9 xA xB xC xD xE xF

xA .....

05x 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00

06x 00 00 X X X X X X X X 2B 00 00 00 00 00

07x 00 00 2B 00 00 00 00 00 00 00

x0 x1 x2 x3 x4 x5 x6 x7 x8 x9 xA xB xC xD xE xF

0Ax FF E8 D5 00 EB F3 61 E9 4B 01

xA .....

0Bx 11 01 40 00 B2 32 0F 05 B0 3C 66 FF C7 0F 05 52

x1 .. B G G P 2 0 2 1 G O T M

12x E T H I N K I N G S T R A N

13x G E - x c e l l e r a t o r

14x \n \r \0 \$

x0 x1 x2 x3 x4 x5 x6 x7 x8 x9 xA xB xC xD xE xF

## ELF HEADER

E\_IDENT

0+4 **EL\_MAG** **\x7F ELF**

5+1 **EL\_DATA** NONE

ELF64\_EHDR

10+2 **e\_type** **2** ET\_EXEC

12+2 **e\_machine** **0x3E** EM\_X86\_64

14+4 **e\_version** IGNORED

18+8 **e\_entry** **0x4000AA** -> 0xAA

20+8 **e\_phoff** **0x4A** -> 0x4A

34+2 **e\_shsize** **0x40**

36+2 **e\_phentsize** **0x38**

38+2 **e\_phnum** **1**

## ELF64\_PHDR (PROGRAM HEADER)

->4A+4 **p\_type** **1** LOAD

4E+4 **p\_flags** **5** XWR

52+8 **p\_offset** **0**

5A+8 **p\_vaddr** **0x400000**

6A+8 **p\_filesz** **0x2B** SHELLCODE + STRLEN

72+8 **p\_memsz** **0x2B** SHELLCODE + STRLEN

## x64 CODE

->AA+2 **mov al,** **1** WRITE

AC+3 **mov di,** **ax** STDOUT

AF+5 **mov esi** **0x400111** BUFFER-> 0x111

B4+2 **mov dl,** **0x32** STRLEN

B6+2 **syscall**

B8+2 **mov al,** **0x3C** EXIT

BA+3 **inc di** RET 2

BD+2 **syscall**

## STRING

->111+33 **String** **BGPP... \n\r\0\$**