

SecurityTube Linux Assembly Expert (SLAE⁶⁴)



SecurityTube Linux Assembly Expert

Training: <http://www.SecurityTube-Training.com>

Pentester Academy: <http://www.PentesterAcademy.com>

Vivek Ramachandran
SWSE, SMFE, SPSE, SGDE, SISE, SLAE^{32,64} Course Instructor

Module 2: Introduction to Shellcoding

6. HelloWorld Shellcode using Stack GDB Analysis

Vivek Ramachandran

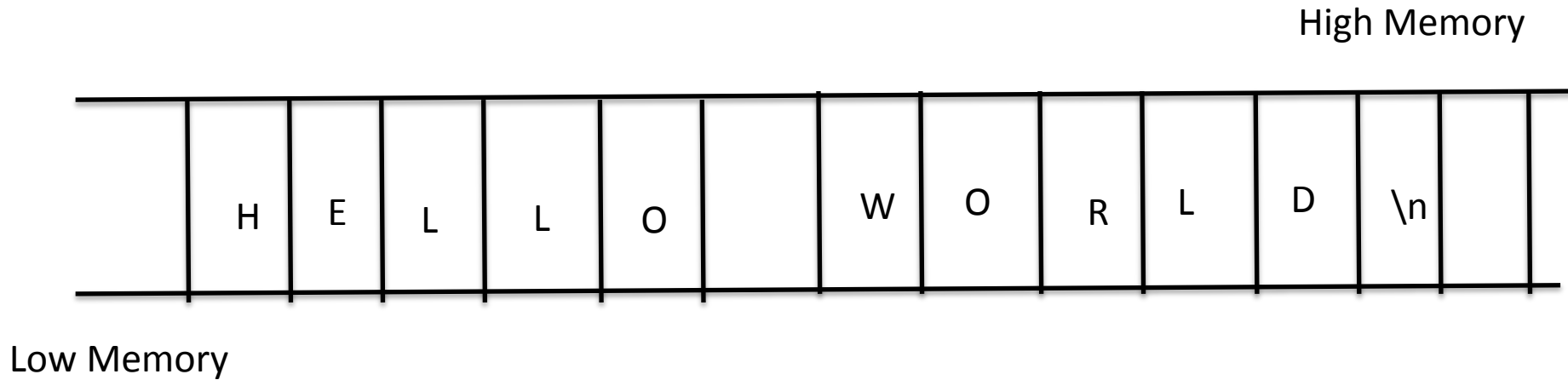
SWSE, SMFE, SPSE, SGDE, SISE, SLAE³² Course Instructor

<http://SecurityTube-Training.com>

Using the Stack

- PUSH the value of the “Hello World” string on the stack
- Get a reference using RSP
- String needs to be pushed in reverse as stack grows from High to Low memory

Stack grows from High memory to Low memory



GDB Analysis

```
pentesteracademy@pentesteracademy-VirtualBox: ~/SLAE-64/Shellcode/HelloWo... x pentesteracademy@pentesteracademy-VirtualBox: ~/SLAE-64/Shellcode/HelloWo... x
Register group: general
rax      0x0      0          rbx      0x0      0
rcx      0x0      0          rdx      0x0      0
rsi      0x0      0          rdi      0x0      0
rbp      0x0      0x0       rsp      0x7fffffff200  0x7fffffff200
r8       0x0      0          r9       0x0      0
r10      0x0      0          r11      0x200    512
r12      0x0      0          r13      0x0      0
r14      0x0      0          r15      0x0      0
rip      0x400080 0x400080 <_start>  eflags   0x202    [ IF ]
cs       0x33     51         ss       0x2b     43

B+> 0x400080 <_start> xor rax,rax
0x400083 <_start+3> add rax,0x1
0x400087 <_start+7> mov rdi,rax
0x40008a <_start+10> push 0xa646c72
0x40008f <_start+15> movabs rbx,0x6f57206f6c6c6548
0x400099 <_start+25> push rbx
0x40009a <_start+26> mov rsi,rsp
0x40009d <_start+29> xor rdx,rdx
0x4000a1 <_start+32> add rdx,0xc
0x4000a4 <_start+36> syscall

child process 4177 In: start Line: ?? PC: 0x400080
Format letters are o(octal), x(hex), d(decimal), u(unsigned decimal),
t(binary), f(float), a(address), i(instruction), c(char) and s(string).
Size letters are b(byte), h(halfword), w(word), g(giant, 8 bytes).
The specified number of objects of the specified size are printed
according to the format.

Defaults for format and size letters are those previously used.
Default count is 1. Default address is following last thing printed
with this command or "print".
(gdb) layout regs
(gdb) █
```

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS PRICING WHY SUBSCRIBE [MEMBER ACCESS](#)



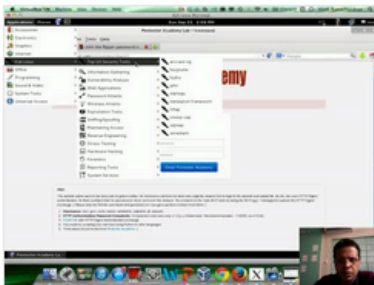
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

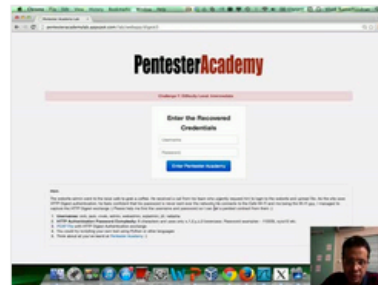
[Start Learning Today!](#)

Latest Videos

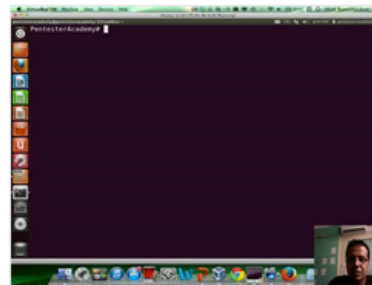
New content added weekly!



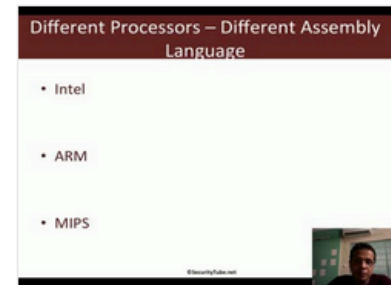
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux