SecurityTube Linux Assembly Expert (SLAE^{64})

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 1: 64-Bit ASM on Linux

6. Hello World runtime analysis with GDB

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

http://SecurityTube-Training.com

Disassemble

```
PentesterAcademy# gdb -q ./HelloWorld
Reading symbols from /home/pentesteracademy/SLAE-64/HelloWorld...
 found)...done.
(gdb) set disassembly-flavor intel
(gdb)
(gdb) break _start
Breakpoint 1 at 0x4000b0
(gdb) disassemble _start
Dump of assembler code for function _start:
   0x00000000004000b0 <+0>:     movabs rax,0x1
   0x00000000004000ba <+10>:    movabs rdi,0x1
   0x00000000004000c4 <+20>:    movabs rsi,0x6000f0
   0x00000000004000ce <+30>:    movabs rdx,0x22
   0x00000000004000d8 <+40>:    syscall
   0x00000000004000da <+42>:    movabs rax,0x3c
   0x00000000004000e4 <+52>:    movabs rdi,0xb
   0x00000000004000ee <+62>:    syscall
End of assembler dump.
(gdb)
```

View Registers

```
(gdb) info registers
rax            0x0      0
rbx            0x0      0
rcx            0x0      0
rdx            0x0      0
rsi            0x0      0
rdi            0x0      0
rbp            0x0      0x0
rsp            0x7fffffffe250   0x7fffffffe250
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            0x4000b0 0x4000b0 <_start>
eflags         0x202    [ IF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
(gdb)
```

View Memory

```
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x00000000004000b0 <+0>:     movabs rax,0x1
   0x00000000004000ba <+10>:    movabs rdi,0x1
   0x00000000004000c4 <+20>:    movabs rsi,0x6000f0
   0x00000000004000ce <+30>:    movabs rdx,0x22
   0x00000000004000d8 <+40>:    syscall
   0x00000000004000da <+42>:    movabs rax,0x3c
   0x00000000004000e4 <+52>:    movabs rdi,0xb
   0x00000000004000ee <+62>:    syscall
End of assembler dump.
(gdb) x/s 0x6000f0
0x6000f0 <hello_world>:  "Hello World to the SLAE-64 Course\n"
(gdb)
```

Trace Execution

```
(gdb) disassemble
Dump of assembler code for function _start:
   0x00000000004000b0 <+0>:     movabs rax,0x1
=> 0x00000000004000ba <+10>:    movabs rdi,0x1
   0x00000000004000c4 <+20>:    movabs rsi,0x6000f0
   0x00000000004000ce <+30>:    movabs rdx,0x22
   0x00000000004000d8 <+40>:    syscall
   0x00000000004000da <+42>:    movabs rax,0x3c
   0x00000000004000e4 <+52>:    movabs rdi,0xb
   0x00000000004000ee <+62>:    syscall
End of assembler dump.
(gdb) nexti
0x00000000004000c4 in _start ()
(gdb) disassemble
Dump of assembler code for function _start:
   0x00000000004000b0 <+0>:     movabs rax,0x1
   0x00000000004000ba <+10>:    movabs rdi,0x1
=> 0x00000000004000c4 <+20>:    movabs rsi,0x6000f0
   0x00000000004000ce <+30>:    movabs rdx,0x22
   0x00000000004000d8 <+40>:    syscall
   0x00000000004000da <+42>:    movabs rax,0x3c
   0x00000000004000e4 <+52>:    movabs rdi,0xb
   0x00000000004000ee <+62>:    syscall
End of assembler dump.
(gdb)
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

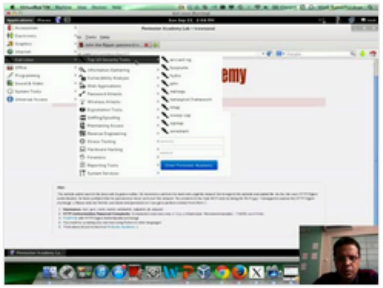
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

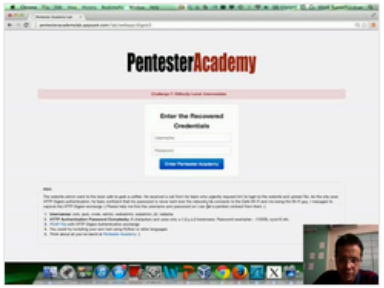
Start Learning Today!

Latest Videos

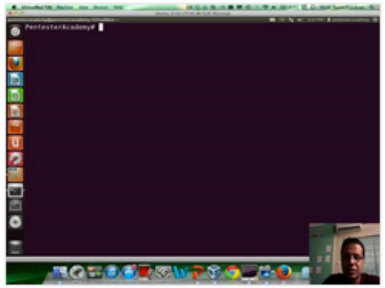
New content added weekly!



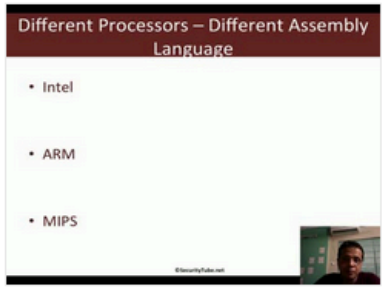
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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

Twitter and Facebook