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

©SecurityTube.net

Module 1: 64-Bit ASM on Linux

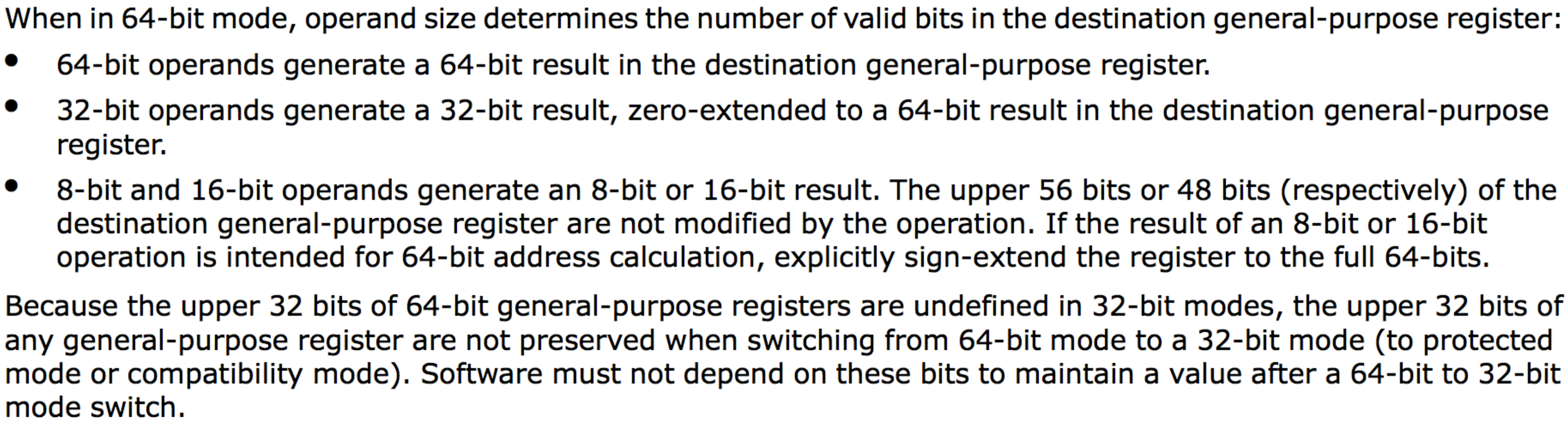
11. Moving Data

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

http://SecurityTube-Training.com

©SecurityTube.net

Super Important!



When in 64-bit mode, operand size determines the number of valid bits in the destination general-purpose register:

- 64-bit operands generate a 64-bit result in the destination general-purpose register.
- 32-bit operands generate a 32-bit result, zero-extended to a 64-bit result in the destination general-purpose register.
- 8-bit and 16-bit operands generate an 8-bit or 16-bit result. The upper 56 bits or 48 bits (respectively) of the destination general-purpose register are not modified by the operation. If the result of an 8-bit or 16-bit operation is intended for 64-bit address calculation, explicitly sign-extend the register to the full 64-bits.

Because the upper 32 bits of 64-bit general-purpose registers are undefined in 32-bit modes, the upper 32 bits of any general-purpose register are not preserved when switching from 64-bit mode to a 32-bit mode (to protected mode or compatibility mode). Software must not depend on these bits to maintain a value after a 64-bit to 32-bit mode switch.

Intel Manual 3.4.1.1

©SecurityTube.net

MOV

- Most common instruction in ASM

- Allowed Directions
  - Between Registers
  - Memory to Register and Register to Memory
  - Immediate Data to Register
  - Immediate Data to Memory

LEA

- Load Effective Address – load pointer values

- LEA RAX, [label]

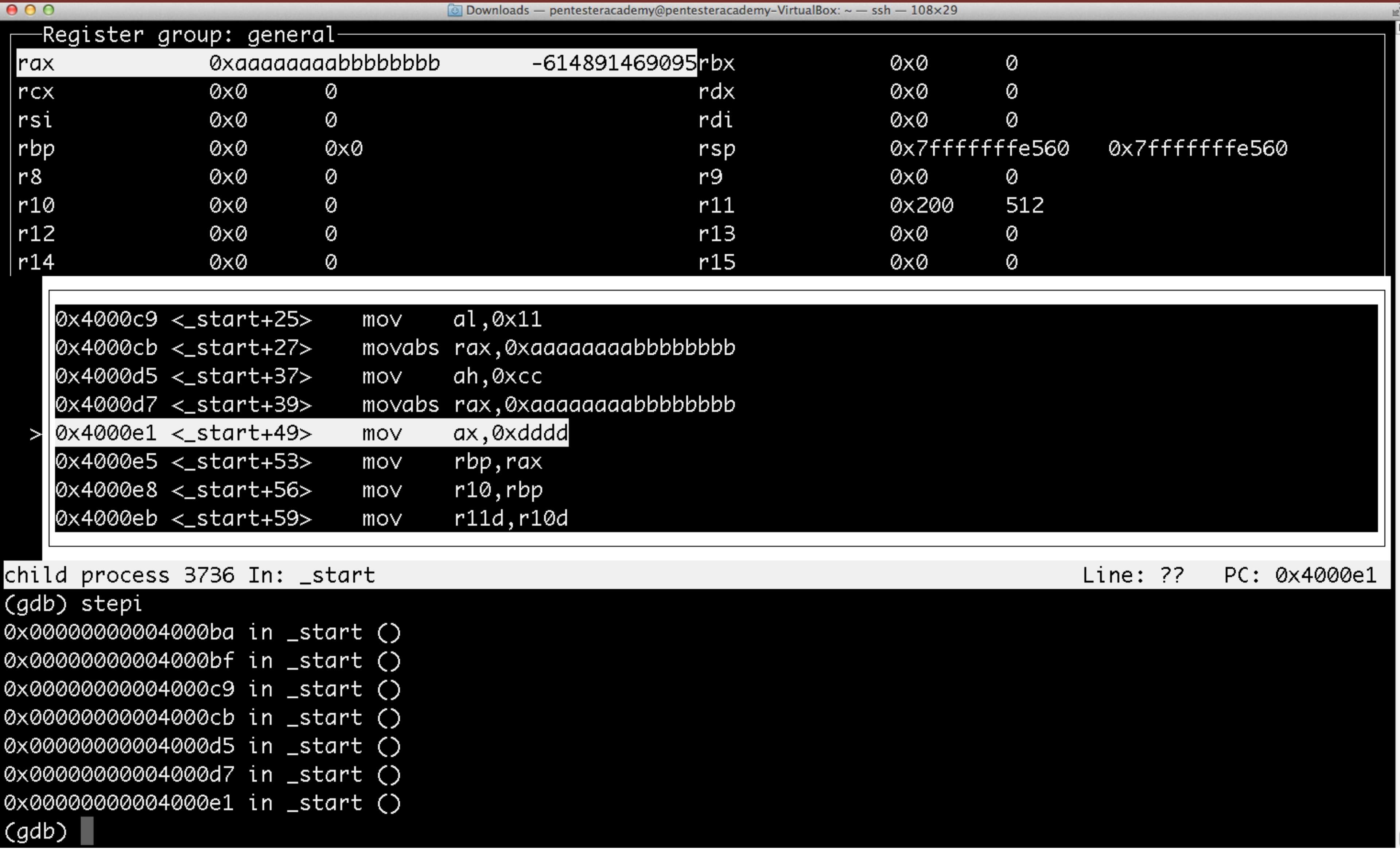
©SecurityTube.net

XCHG

- Exchanges (swaps) Values
- XCHG Register, Register
- XCHG Register, Memory

©SecurityTube.net

Moving Data Lab



Downloads — pentesteracademy@pentesteracademy-VirtualBox: ~ — ssh — 108×29

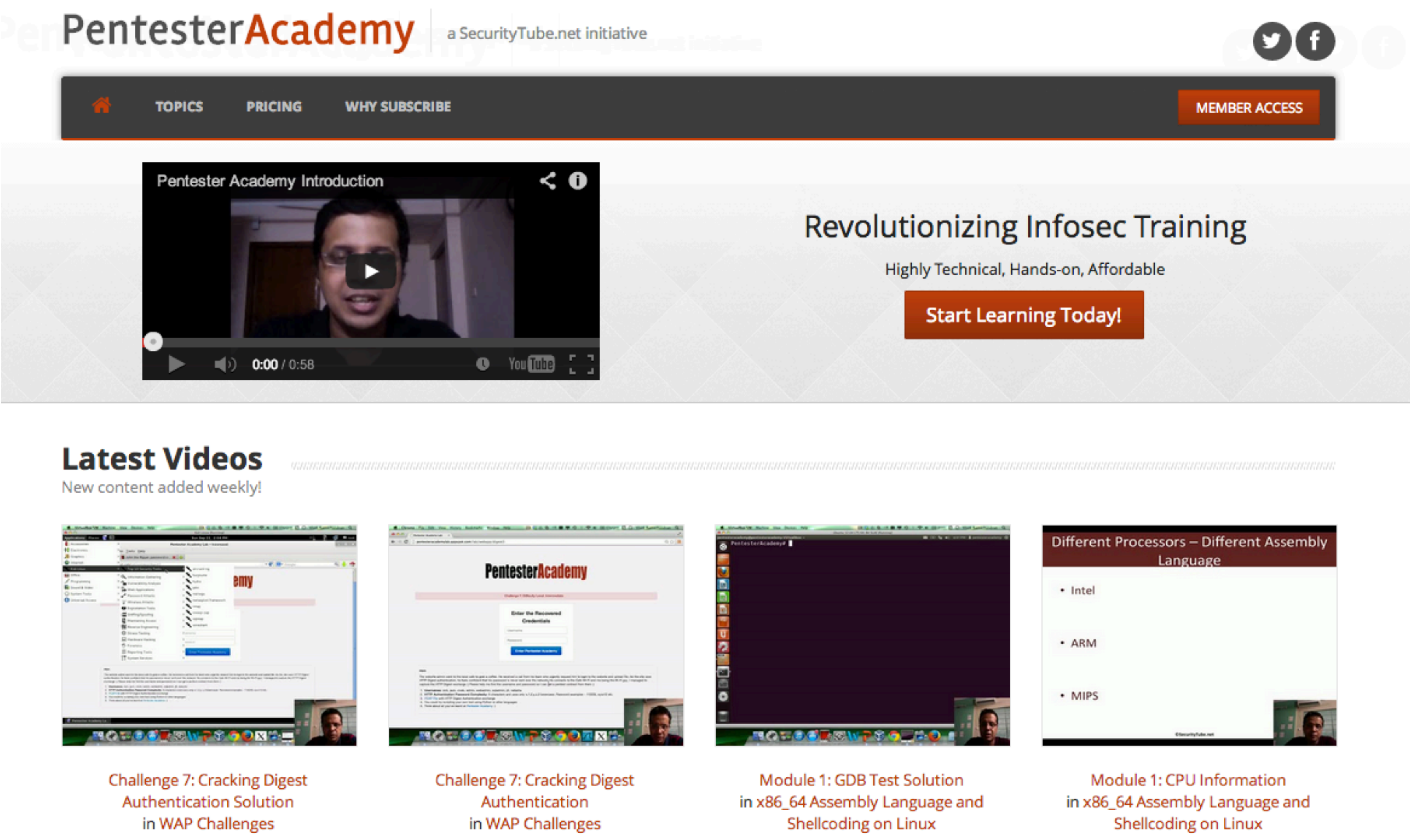
```
 Register group: general
rax            0xaaaaaaaabbbbbbbb          -6148914690950rbx            0x0      0
rcx            0x0      0                                 rdx            0x0      0
rsi            0x0      0                                 rdi            0x0      0
rbp            0x0      0x0                               rsp            0x7fffffffe560   0x7fffffffe560
r8             0x0      0                                 r9             0x0      0
r10            0x0      0                                 r11            0x200    512
r12            0x0      0                                 r13            0x0      0
r14            0x0      0                                 r15            0x0      0

   0x4000c9 <_start+25>    mov    al,0x11
   0x4000cb <_start+27>    movabs rax,0xaaaaaaaabbbbbbbb
   0x4000d5 <_start+37>    mov    ah,0xcc
   0x4000d7 <_start+39>    movabs rax,0xaaaaaaaabbbbbbbb
  >0x4000e1 <_start+49>    mov    ax,0xdddd
   0x4000e5 <_start+53>    mov    rbp,rax
   0x4000e8 <_start+56>    mov    r10,rbp
   0x4000eb <_start+59>    mov    r11d,r10d

child process 3736 In: _start                                              Line: ??    PC: 0x4000e1
(gdb) stepi
0x00000000004000ba in _start ()
0x00000000004000bf in _start ()
0x00000000004000c9 in _start ()
0x00000000004000cb in _start ()
0x00000000004000d5 in _start ()
0x00000000004000d7 in _start ()
0x00000000004000e1 in _start ()
(gdb)
```

©SecurityTube.net

Pentester Academy



PentesterAcademy | a SecurityTube.net initiative

Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Latest Videos

New content added weekly!

Different Processors – Different Assembly Language

- Intel
- ARM
- MIPS

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

©SecurityTube.net