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

8. Data Types

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

http://SecurityTube-Training.com

Fundamental Data Types

- Byte – 8 bits
- Word – 16 bits
- Double Word – 32 bits
- Quad Word – 64 bits
- Double Quad Word – 128 bits

Source: IA-32 Manual

NASM …

- Case Sensitive syntax

- Accessing memory reference with []
  - message db 0xAA, 0xBB, 0xCC, 0xDD, …
  - mov rax, message ← moves address into rax
  - move rax, [message] ← moves value into rax

http://www.nasm.us/docs.php

Defining Initialized Data in NASM

```
db    0x55                ; just the byte 0x55
db    0x55,0x56,0x57      ; three bytes in succession
db    'a',0x55            ; character constants are OK
db    'hello',13,10,'$'   ; so are string constants
dw    0x1234              ; 0x34 0x12
dw    'a'                 ; 0x61 0x00 (it's just a number)
dw    'ab'                ; 0x61 0x62 (character constant)
dw    'abc'               ; 0x61 0x62 0x63 0x00 (string)
dd    0x12345678          ; 0x78 0x56 0x34 0x12
dd    1.234567e20         ; floating-point constant
dq    0x123456789abcdef0  ; eight byte constant
dq    1.234567e20         ; double-precision float
dt    1.234567e20         ; extended-precision float
```

Source: NASM Manual Pg. 30

Declare Uninitialized Data

```
buffer:         resb    64              ; reserve 64 bytes
wordvar:        resw    1               ; reserve a word
```

Source: NASM Manual Pg. 30

Special Tokens

- $ - evaluates to the current line

- $$ - evaluates to the beginning of current section

Source: NASM Manual Pg. 37

EQU and TIMES

```
message         db      'hello, world'
msglen          equ     $-message
```

Data:

```
zerobuf:        times 64 db 0
```

Instruction:

```
times 100 movsb
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

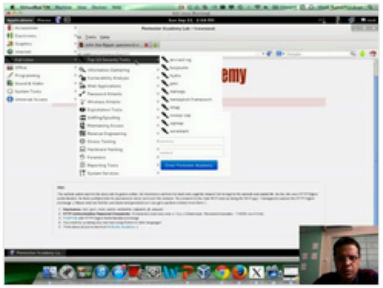
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

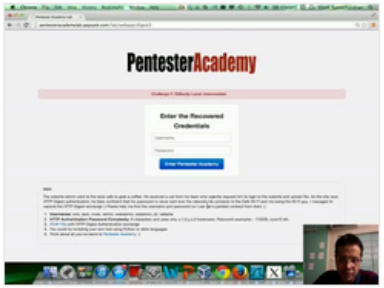
Start Learning Today!

Latest Videos

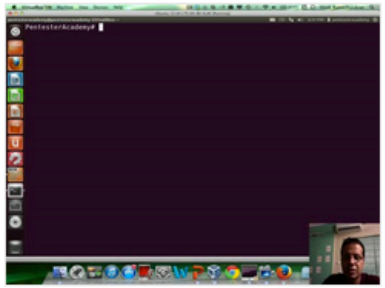
New content added weekly!



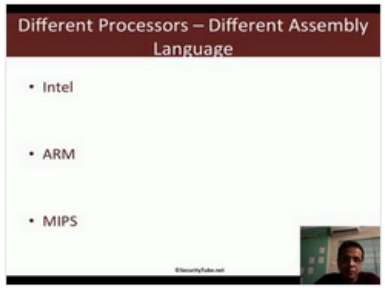
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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