

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

10. Execve Shellcode Stack Method GDB Analysis

Vivek Ramachandran

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

<http://SecurityTube-Training.com>

GDB Analysis

```
B+ 0x400080 <_start>      xor    rax,rax
    0x400083 <_start+3>   push  rax
    0x400084 <_start+4>   movabs rbx,0x68732f2f6e69622f
    0x40008e <_start+14>  push  rbx
    0x40008f <_start+15>  mov    rdi,rsp
    0x400092 <_start+18>  push  rax
    0x400093 <_start+19>  mov    rdx,rsp
    0x400096 <_start+22>  push  rdi
    0x400097 <_start+23>  mov    rsi,rsp
    0x40009a <_start+26>  add    rax,0x3b
> 0x40009e <_start+30>  syscall
    0x4000a0          add    BYTE PTR [rsi],ch
    0x4000a2          jae   0x40011d
    0x4000a4          ins   DWORD PTR es:[rdi],dx
    0x4000a5          je    0x400108
    0x4000a7          (bad)
    0x4000a8          add    BYTE PTR [rsi],ch
```

```
child process 2285 In:  start
```

```
(gdb) x/s $rsp
```

```
0x7fffffffef1f0:  "/bin//sh"
```

```
(gdb) stepi
```

```
0x0000000000400092 in  _start ()
```

```
0x0000000000400093 in  _start ()
```

```
0x0000000000400096 in  _start ()
```

```
0x0000000000400097 in  _start ()
```

```
0x000000000040009a in  _start ()
```

```
0x000000000040009e in  _start ()
```

```
(gdb) █
```

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



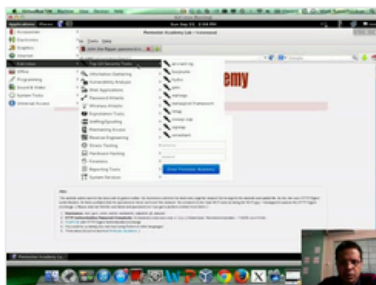
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

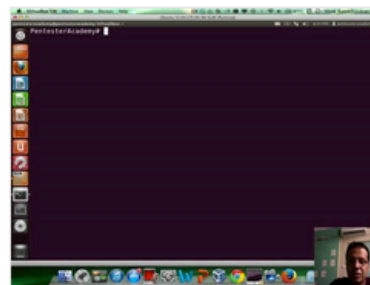
New content added weekly!



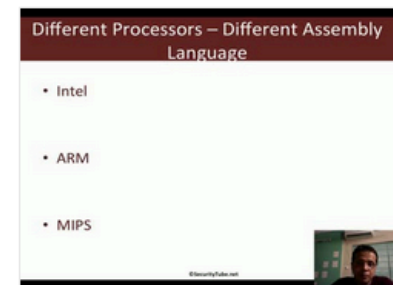
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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