

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

4. HelloWorld Shellcode GDB Analysis

Vivek Ramachandran

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

<http://SecurityTube-Training.com>

Modifying Hello World

- Replace all 0x00 opcode instructions
- No hardcoded addresses
 - dynamically figure out address of “Hello World” string

JMP-CALL-POP

JMP Call_shellcode:

shellcode:

```
    pop rsi
```

```
    ....
```

```
    ...
```

```
    ...
```

Call_shellcode:

```
    call shellcode:
```

```
    HelloWorld db "Hello World!"
```

GDB Analysis

```
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      0x7fffffff210 0x7fffffff210
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>      jmp     0x4000a0 <call shellcode>
0x400082 <shellcode>     pop     rsi
0x400083 <shellcode+1>   xor     rax,rax
0x400086 <shellcode+4>   mov     al,0x1
0x400088 <shellcode+6>   mov     rdi,rax
0x40008b <shellcode+9>   mov     rdx,rdi
0x40008e <shellcode+12>  add     rdx,0x22
0x400092 <shellcode+16>  syscall
0x400094 <shellcode+18>  xor     rax,rax
0x400097 <shellcode+21>  add     rax,0x3c

child process 2728 In: start Line: ?? PC: 0x400080
Reading symbols from /home/pentesteracademy/SLAE-64/Shellcode/HelloWorld/HelloWorld...(no debugging symbols found)...done.
(gdb) break _start
Breakpoint 1 at 0x400080
(gdb) run
Starting program: /home/pentesteracademy/SLAE-64/Shellcode/HelloWorld/HelloWorld

Breakpoint 1, 0x0000000000400080 in _start ()
(gdb) █
```

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



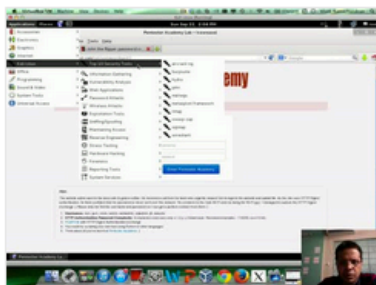
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

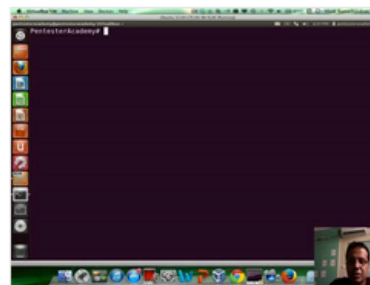
New content added weekly!



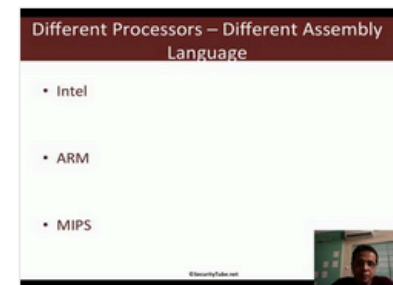
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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