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 2: Introduction to Shellcoding

12. Execve JMP-CALL-POP Shellcode GDB Analysis

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

http://SecurityTube-Training.com

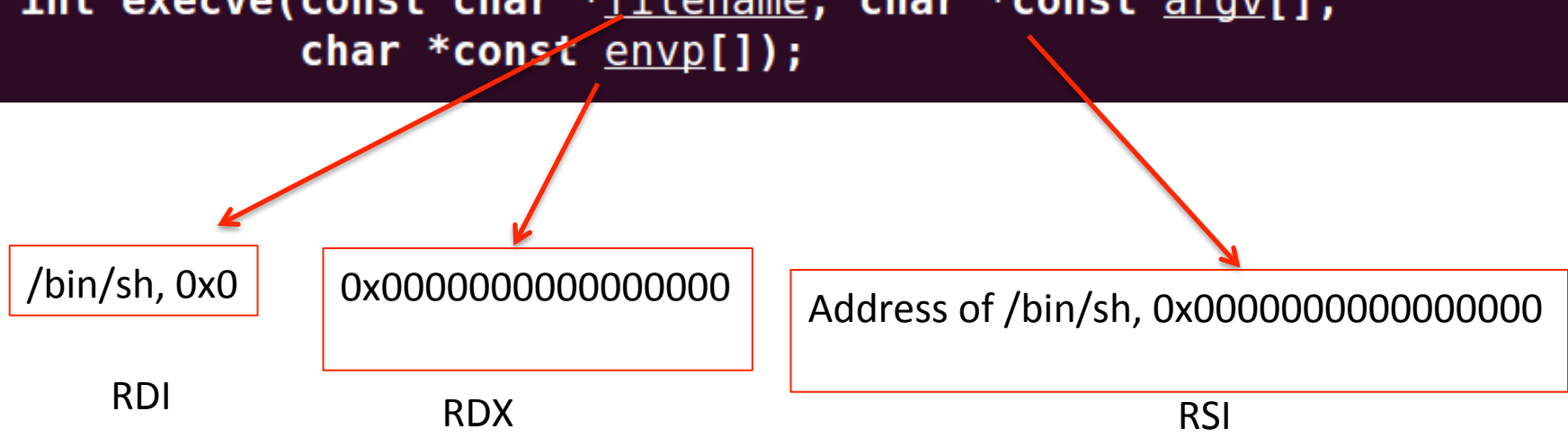
Execve

```
EXECVE(2)                          Linux Programmer's Manual

NAME
       execve - execute program

SYNOPSIS
       #include <unistd.h>

       int execve(const char *filename, char *const argv[],
                  char *const envp[]);
```



We cannot have NULLs in the Shellcode

GDB Analysis

```
B+ 0x601040 <code>          jmp    0x60105f <code+31>
   0x601042 <code+2>        xor    rax,rax
   0x601045 <code+5>        pop    rdi
   0x601046 <code+6>        mov    BYTE PTR [rdi+0x7],ah
   0x601049 <code+9>        mov    QWORD PTR [rdi+0x8],rdi
   0x60104d <code+13>       mov    QWORD PTR [rdi+0x10],rax
   0x601051 <code+17>       lea    rsi,[rdi+0x8]
   0x601055 <code+21>       lea    rdx,[rdi+0x10]
   0x601059 <code+25>       add    rax,0x3b
 > 0x60105d <code+29>       syscall
   0x60105f <code+31>       call   0x601042 <code+2>
   0x601064 <code+36>       (bad)
   0x601065 <code+37>       (bad)
   0x601066 <code+38>       imul   ebp,DWORD PTR [rsi+0x2f],0x42416873
   0x60106d <code+45>       rex.X
   0x60106e <code+46>       rex.X
   0x60106f <code+47>       rex.X
   0x601070 <code+48>       rex.X
   0x601071 <code+49>       rex.X
child process 2672 In: code
0x60106c <code+44>:     0x64    0x10    0x60    0x00    0x00    0x00    0x00    0x00
0x601074 <code+52>:     0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x60107c <code+60>:     0x00
0x0000000000601059 in code ()
0x601064 <code+36>:     0x2f    0x62    0x69    0x6e    0x2f    0x73    0x68    0x00
0x60106c <code+44>:     0x64    0x10    0x60    0x00    0x00    0x00    0x00    0x00
0x601074 <code+52>:     0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x60107c <code+60>:     0x00
0x000000000060105d in code ()
(gdb)
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

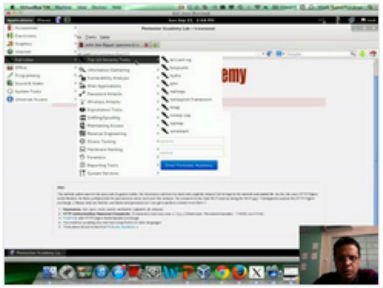
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

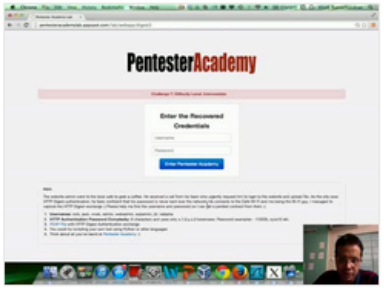
Start Learning Today!

Latest Videos

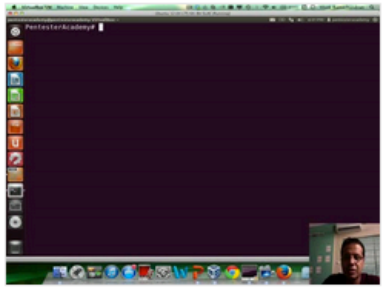
New content added weekly!



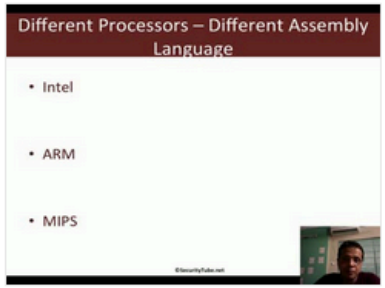
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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