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

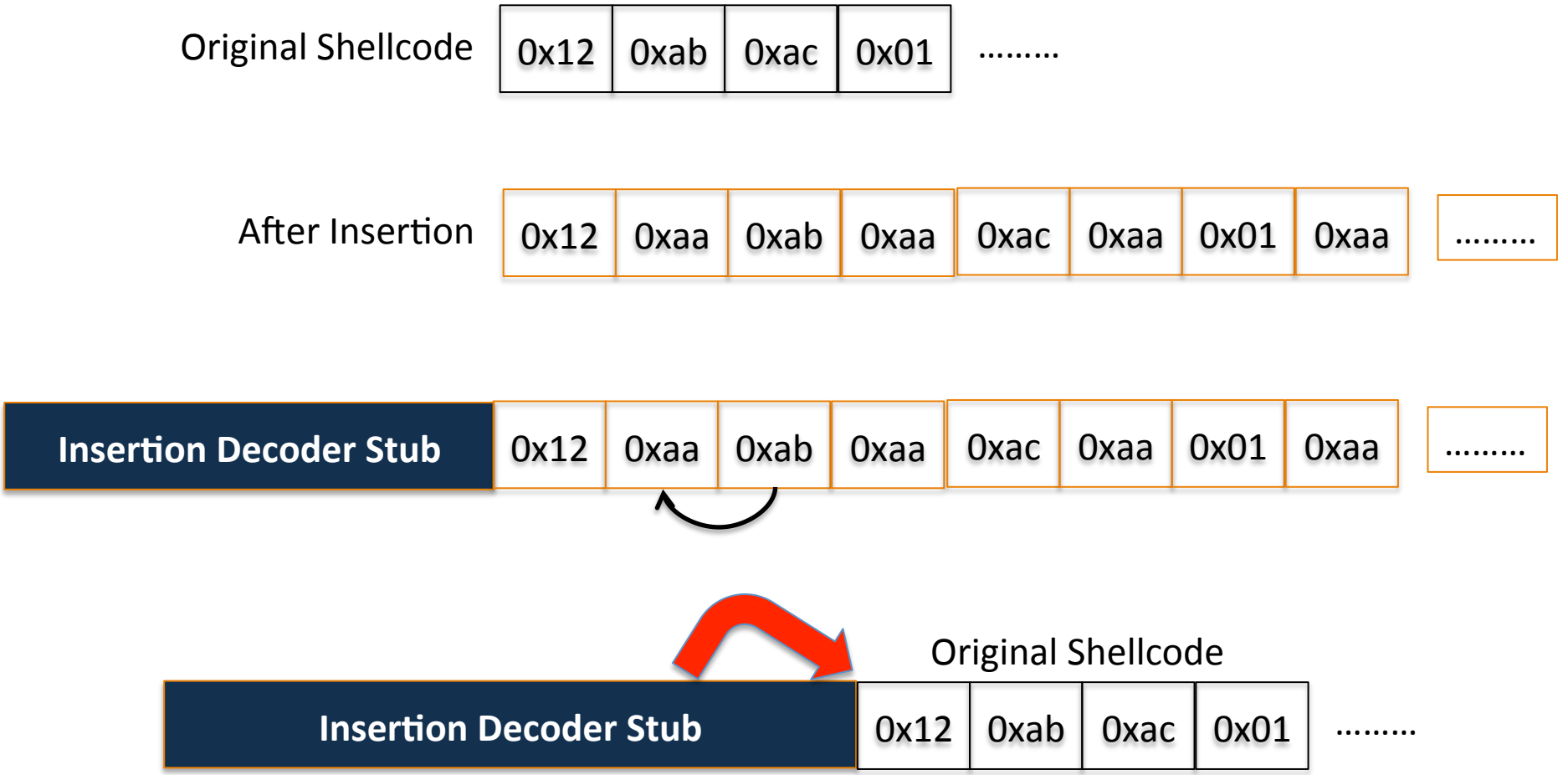
Module 2: Introduction to Shellcoding

18. Insertion Encoder GDB Analysis

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

http://SecurityTube-Training.com

Insertion Encoder?



GDB Analysis

```
(gdb) disassemble
Dump of assembler code for function code:
   0x0000000000601040 <+0>:     jmp    0x601085 <code+69>
=> 0x0000000000601042 <+2>:     xor    rax,rax
   0x0000000000601045 <+5>:     push   rax
   0x0000000000601046 <+6>:     movabs rbx,0x68732f2f6e69622f
   0x0000000000601050 <+16>:    push   rbx
   0x0000000000601051 <+17>:    mov    rdi,rsp
   0x0000000000601054 <+20>:    push   rax
   0x0000000000601055 <+21>:    mov    rdx,rsp
   0x0000000000601058 <+24>:    push   rdi
   0x0000000000601059 <+25>:    mov    rsi,rsp
   0x000000000060105c <+28>:    add    rax,0x3b
   0x0000000000601060 <+32>:    syscall
   0x0000000000601062 <+34>:    mov    DWORD PTR [rdx-0x55af5519],ebp
   0x0000000000601068 <+40>:    rex.W stos BYTE PTR es:[rdi],al
   0x000000000060106a <+42>:    mov    DWORD PTR [rdx-0x55a8551e],ebp
   0x0000000000601070 <+48>:    rex.W stos BYTE PTR es:[rdi],al
   0x0000000000601072 <+50>:    mov    DWORD PTR [rdx-0x55b7551a],ebp
   0x0000000000601078 <+56>:    sub    DWORD PTR [rdx-0x55c45540],0xf
   0x000000000060107f <+63>:    stos   BYTE PTR es:[rdi],al
   0x0000000000601080 <+64>:    add    eax,0xbbbbbbbb
   0x0000000000601085 <+69>:    lea    rsi,[rip+0xfffffffffffffb6]
   0x000000000060108c <+76>:    lea    rdi,[rsi+0x1]
   0x0000000000601090 <+80>:    xor    rax,rax
   0x0000000000601093 <+83>:    mov    al,0x1
   0x0000000000601095 <+85>:    xor    rbx,rbx
   0x0000000000601098 <+88>:    mov    bl,BYTE PTR [rsi+rax*1]
   0x000000000060109b <+91>:    xor    bl,0xaa
   0x000000000060109e <+94>:    jne    0x601042 <code+2>
   0x00000000006010a0 <+96>:    mov    bl,BYTE PTR [rsi+rax*1+0x1]
   0x00000000006010a4 <+100>:   mov    BYTE PTR [rdi],bl
   0x00000000006010a6 <+102>:   inc    rdi
   0x00000000006010a9 <+105>:   add    al,0x2
   0x00000000006010ab <+107>:   jmp    0x601098 <code+88>
   0x00000000006010ad <+109>:   add    BYTE PTR [rax],al
End of assembler dump.
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

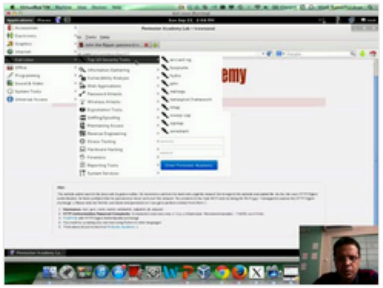
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

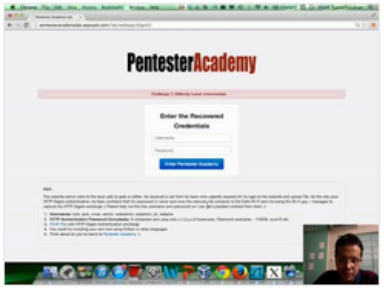
Start Learning Today!

Latest Videos

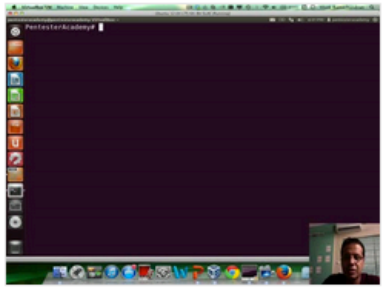
New content added weekly!



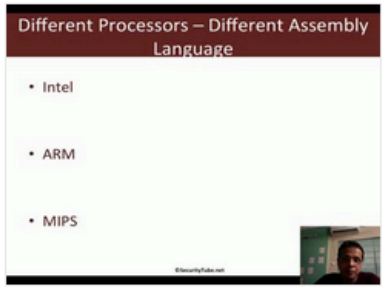
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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