

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

14. XOR Encoder GDB Analysis

Vivek Ramachandran

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

<http://SecurityTube-Training.com>

XOR Encoder GDB Analysis

```
B+> 0x601040 <code>          jmp     0x601053 <code+19>
0x601042 <code+2>          pop     rdi
0x601043 <code+3>          xor     rcx,rcx
0x601046 <code+6>          add     cl,0x3c
0x601049 <code+9>          xor     BYTE PTR [rdi],0xaa
0x60104c <code+12>         inc     rdi
0x60104f <code+15>         loop   0x601049 <code+9>
0x601051 <code+17>         jmp     0x601058 <code+24>
0x601053 <code+19>         call   0x601042 <code+2>
0x601058 <code+24>         mov     r15b,0xe2
0x60105b <code+27>         fwait
0x60105c <code+28>         push   0xfffffffffffffff5
0x60105e <code+30>         and    cl,ch
0x601060 <code+32>         lods   eax,DWORD PTR ds:[rsi]
0x601061 <code+33>         loop   0x601086 <code+70>
0x601063 <code+35>         (bad)
0x601064 <code+36>         movabs ds:0xa2dd27e2baed23e2,a1
0x60106d <code+45>         loop   0x601096
0x60106f <code+47>         std
0x601070 <code+48>         mov     edx,0x916a29e2
0x601075 <code+53>         movs   DWORD PTR es:[rdi],DWORD PTR ds:[rsi]
```

child process 2848 In: code

Line: 1

ymbols found)...done.

(gdb) break *&code

Breakpoint 1 at 0x601040

(gdb) run

Starting program: /home/pentesteracademy/SLAE-64/Shellcode/XOR-Encoder/shellcode

Breakpoint 1, 0x0000000000601040 in code ()

(gdb) █

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



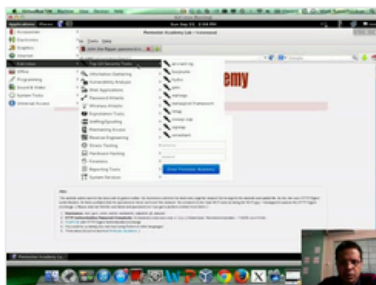
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

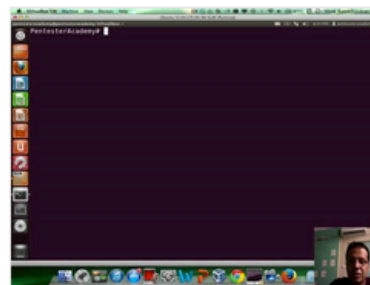
New content added weekly!



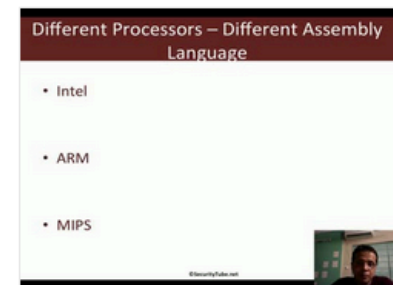
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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