

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

3. HelloWorld Shellcode using JMP-CALL-POP

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!"
```

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



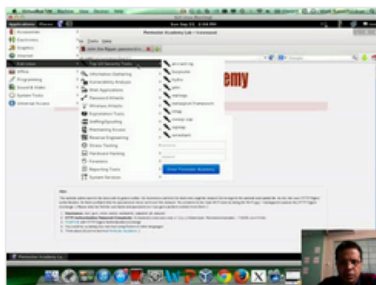
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

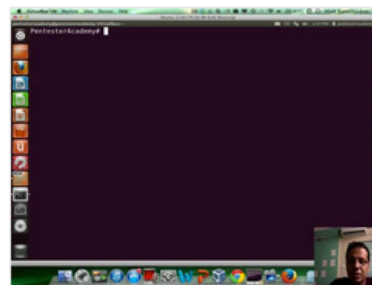
New content added weekly!



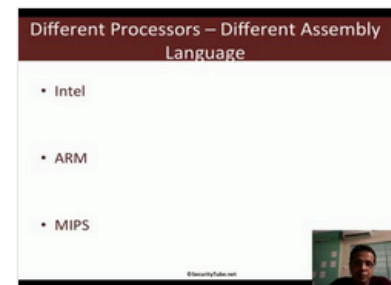
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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