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

21. MMX XOR Decoder

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

http://SecurityTube-Training.com

Ton of instructions!

- FPU
- MMX
- SSE
- SSE2

Advantages

- Existing “popular” shellcodes hardly use them
- Probably detection rates lesser by AV and other analysis tools
- Easy to replicate existing functionality using these extensions

MMX based XOR Decoder

- SIMD – Single instruction multiple data
- Registers MM0 to MM7
- Can load 8 bytes qword
- Moving Data – movq
- XOR'ing Data – pxor
- Key Difference from the previous XOR decoder
  - Operates over 8 bytes at the same time

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

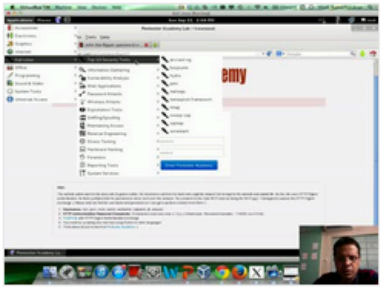
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

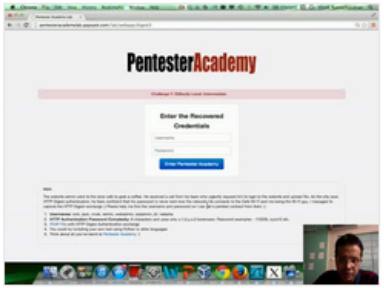
Start Learning Today!

Latest Videos

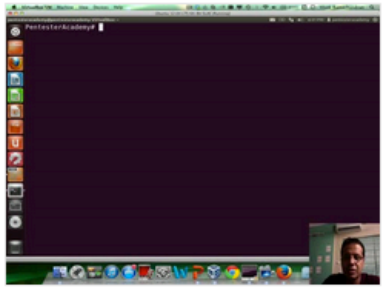
New content added weekly!



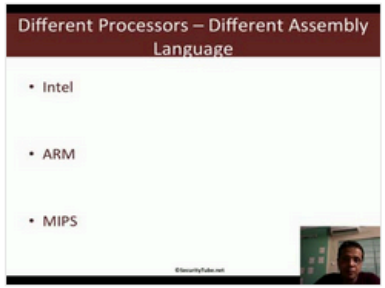
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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