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

23. Crypters

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

http://SecurityTube-Training.com

Crypters

- Encrypt Executable / Shellcode
- Decrypt at runtime and run
- For powerful crypto techniques like RC4, AES etc. a lot of assembly code
- Shellcode size too large to be useful

RC4

- Symmetric Stream Cipher
- 2 Step process:
  - Key Scheduling Algorithm
  - Pseudo Random Number Generation
- Full Details: http://en.wikipedia.org/wiki/RC4

Writing an RC4 Shellcode Crypter in C

- Encryption Phase:
  - For a given key, encrypts shellcode
- Decryption Phase:
  - For the same key, decrypts shellcode
  - Executes it

RC4 in Assembly

- https://thunked.org/programming/rc4-in-assembly-t23.html
- http://youritguy.wordpress.com/2010/06/13/adler-32-and-rc4-in-inline-assembly/
- http://nayuki.eigenstate.org/page/rc4-cipher-in-x86-assembly

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

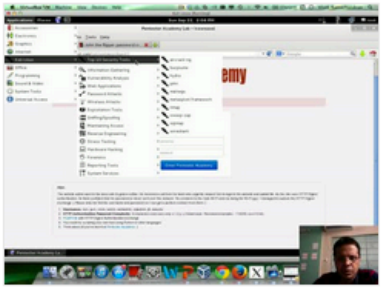
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

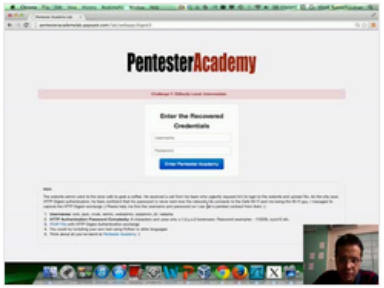
Start Learning Today!

Latest Videos

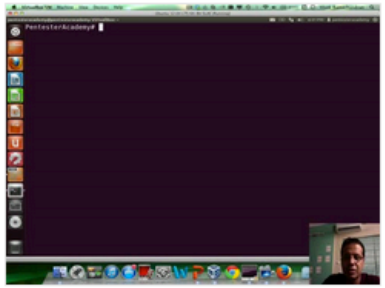
New content added weekly!



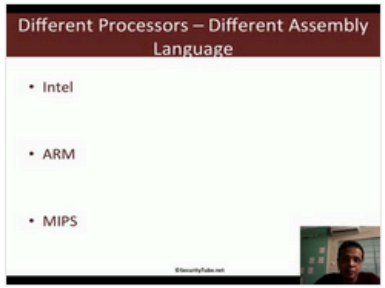
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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