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: Certification Exam

The Grand Finale

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

http://SecurityTube-Training.com

Exam Format

- 7 Assignments of varying difficulty
- Post solutions to your personal blog
  - wordpress.com, Blogger or your own domain
- Store code in a Github account

Assignment #1

- Create a Shell_Bind_TCP shellcode
  - Binds to a port
  - Needs a “Passcode”
  - If Passcode is correct then Execs Shell
- Remove 0x00 from the Bind TCP Shellcode discussed

Assignment #2

- Create a Shell_Reverse_TCP shellcode
  - Reverse connects to configured IP and Port
  - Needs a “Passcode”
  - If Passcode is correct then Execs Shell

- Remove 0x00 from the Reverse TCP Shellcode discussed

Assignment #3

- Study about the Egg Hunter shellcode
- Create a working demo of the Egghunter
- Should be configurable for different payloads

Assignment #4

- Create a custom encoding scheme like the "Insertion Encoder" we showed you

- PoC with using execve-stack as the shellcode to encode with your schema and execute

Assignment #5

- Take up at least 3 shellcode samples created using Msfpayload for linux/x86_64
- Use GDB to dissect the functionality of the shellcode
- Document your analysis

Assignment #6

- Take up 3 shellcodes from Shell-Storm and create polymorphic versions of them to beat pattern matching
- The polymorphic versions cannot be larger 150% of the existing shellcode
- Bonus points for making it shorter in length than original

Assignment #7

- Create a custom crypter like the one shown in the “crypters” video
- Free to use any existing encryption schema
- Can use any programming language

Blog post must mention

This blog post has been created for completing the requirements of the SecurityTube Linux Assembly Expert certification:

http://www.securitytube-training.com/online-courses/x8664-assembly-and-shellcoding-on-linux/index.html

Student ID: SLAE64-XXXXX

Evaluation Criteria

- Originality of Shellcode
- Quality of Explanation – detailed and insightful
- Each Assignment carries 10 marks
- Certification Criteria: > 50 out of 70 marks

Extra Points ☺

- Posting additional new shellcodes beyond the assignments (10 points)

- Shellcode submitted to and accepted by:

  – Shell-Storm.org
  – Exploit-db.com

  (10 points)

- Community Interaction (5 points)
  – Chatter on Twitter, Facebook
  – Comments on Blog posts

Submission Format

- Email to feedback@binarysecuritysolutions.com
- Subject: SLAE64 Exam Blog Posts
- Email contains:
  - Links to all 7 blog posts
  - Link to Gitgub account where code is stored
  - Link to Shell-Storm / Exploit-db submissions
  - Link to Twitter / Facebook if posted there
- Around 5 working days for result

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

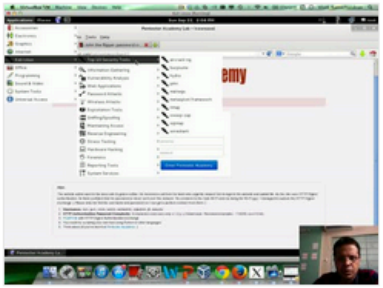
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

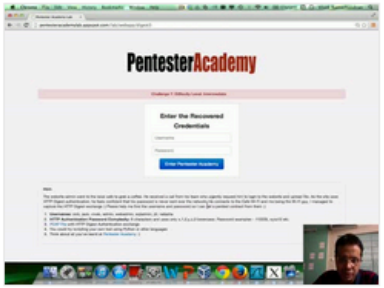
Start Learning Today!

Latest Videos

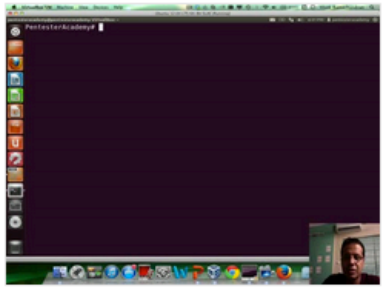
New content added weekly!



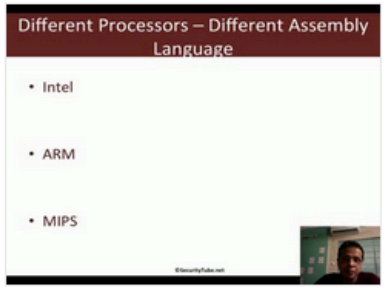
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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