

Exploiting Simple Buffer Overflows on Win32

Vivek Ramachandran

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

Certifications: <http://www.securitytube-training.com>

Pentester Academy: <http://www.PentesterAcademy.com>

Course Introduction

Exploit Research

Platforms
Windows XP – SP1, SP2 ...
Windows Vista – SP...
Windows 7 – 8...
Windows Server 2003, 2008 ...
Linux
Mac OSX

Exploitation Techniques
Simple Buffer Overflows
SEH, SafeSEH
NX, DEP
ASLR
Stack Cookies
....

What will this course cover?

- Buffer Overflows (emphasis on Stack Based)
- In Absence of Protection Mechanisms like DEP, ASLR etc.
- 32-bit Windows

Emphasis on Practice

- 10+ Real World and Staged Applications
- Very detailed and thorough
- Practice! Practice! Practice!

Software Requirements

- Windows XP SP3
- Immunity Debugger
- Virtualbox/Vmware
- Metasploit

Knowledge Requirements

- Assembly Language Basics (32-bit)
- <http://www.pentesteracademy.com/course?id=3>

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



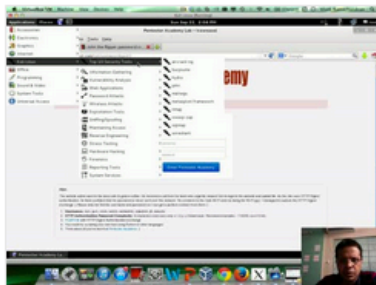
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

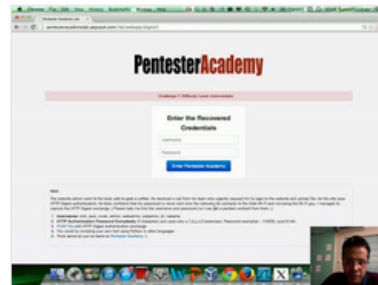
Start Learning Today!

Latest Videos

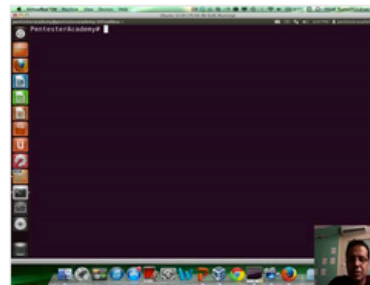
New content added weekly!



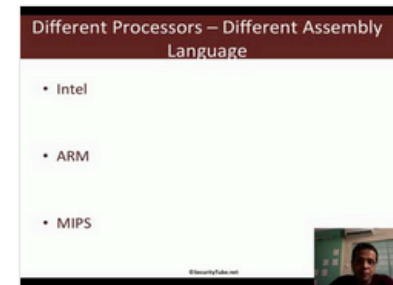
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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