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

1. Shellcoding Basics

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

http://SecurityTube-Training.com

What is Shellcode?

- Machine code with a specific purpose
  - spawn a local shell
  - Bind to port and spawn shell
  - create a new account

- Can be executed by the CPU directly – no further assembling / linking or separate compiling required

How is Shellcode delivered?

- Part of an exploit
  - Size of shellcode important (smaller size = better)
  - Bad characters a concern
    - 0x00 most common one
- Added into an executable
  - run as separate thread
  - replace executable functionality
  - Size of shellcode not a concern

Shellcode Resources

- http://www.shell-storm.org/
- http://exploit-db.com
- http://www.projectshellcode.com/

Testing Shellcode

```
#include<stdio.h>
#include<string.h>

unsigned char code[] = \
"SHELLCODE ";


main()
{

        printf("Shellcode Length:  %d\n", strlen(code));

        int (*ret)() = (int(*)())code;

        ret();

}


~
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

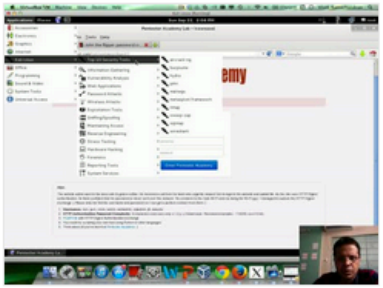
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

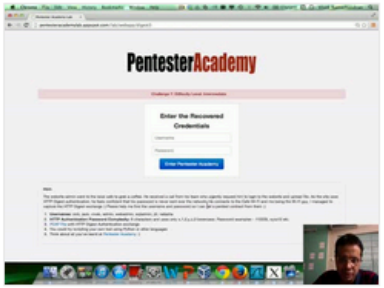
Start Learning Today!

Latest Videos

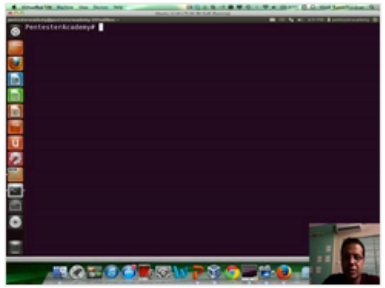
New content added weekly!



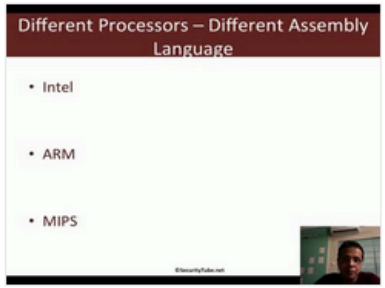
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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