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

13. XOR Encoder

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

http://SecurityTube-Training.com

XOR

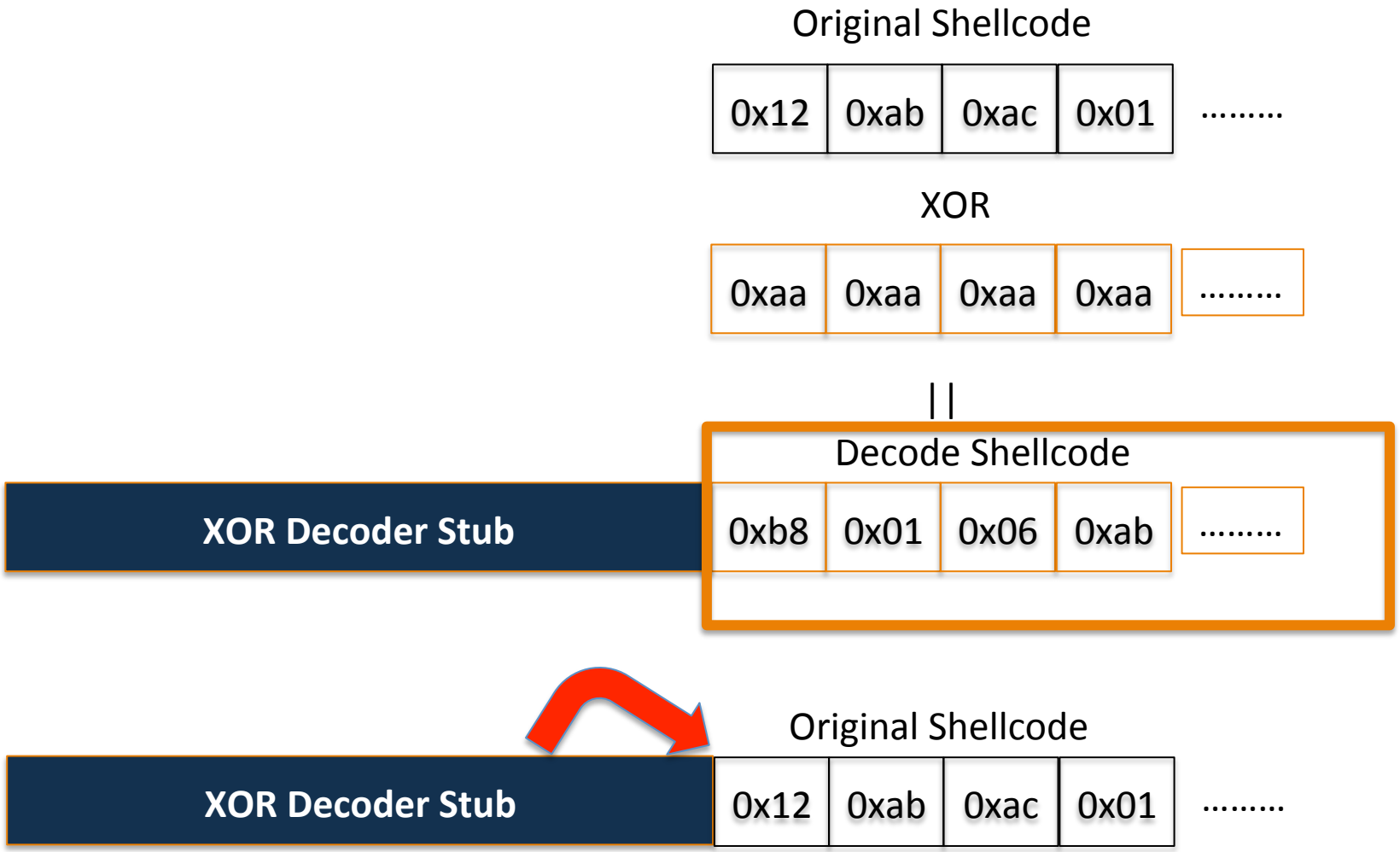
A	B	A xor B
0	0	0
1	1	0
1	0	1
0	1	1

Interesting: (A xor B) xor B = A

What does this mean for us?

- Select an encoder byte e.g. 0xAA
- XOR every byte of Shellcode with 0xAA
- Write a decoder stub which will XOR the encoded shellcode bytes with 0xAA and recover original shellcode
- Stub then passes control to decoded shellcode

Too much text can kill a concept ☺



Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

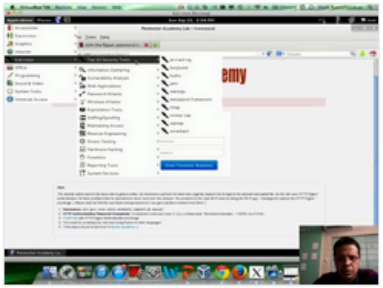
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

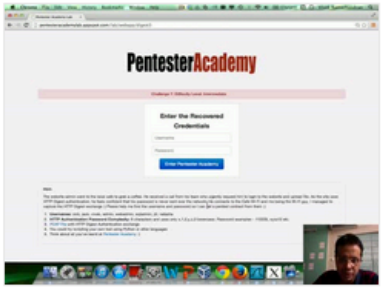
Start Learning Today!

Latest Videos

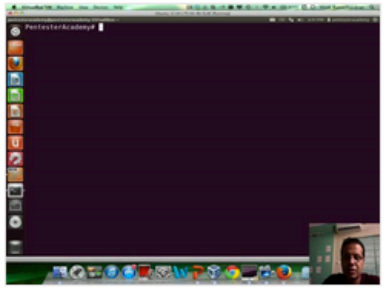
New content added weekly!



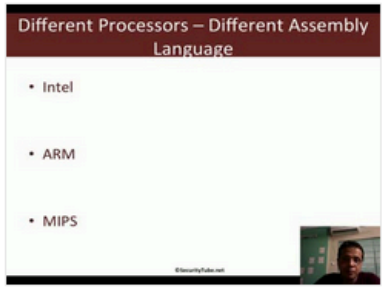
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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