SETC Training Corporate Logo

IT Security Training: Offensive & Defensive Hack Proofing (PENCP, 4 jours)

Description

The course Offensive & Defensive Hack Proofing (IT Security Training) is an introduction to white hat hacking. The course teaches you how to perform every stage of the hacking process so that you may protect your environment. The training includes tools for information gathering & target scoping, target discover & enumeration, vulnerability mapping & social engineering. You are taught how to use the Metasploit Framework to perform target identification & exploitation so that you may stop it from happening to you. The progressive & hands-on practical lab allow you to execute a hack from initial identification to privilege escalation & maintenance. Stop hackers in their tracks today!

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Linux Kali: The Bare Essentials

- Setting up Linux Kali
- A Note on Lab Configuration
- A Quick Intro to the Linux Command Line
- Touring the Linux File System
- Mastering User Privilege and SELinux
- All about File Permissions
- Editing Files with VIM

Linux Kali: A Few Useful Topics

- About Runlevels and Boot
- Managing Packages with apt-get
- Managing Processes and Services
- Setting up and Understanding IP Addresses and Hostnames
- Mastering Netcat
- Mastering the Firewall
- A Quick Tour of TCPDump

BASH Scripting and Other Programming

- More on VIM Editing
- Setting up your Profile
- Working with Quotes
- Working with Variables
- Implementing Conditional Logic
- Implementing Repeating Logic
- A Few More Advanced Concepts
- Writing Python Scripts: A Quick Tour
- Introduction to C Compilers
- Writing and Compiling C Code

Power Tools: The Metasploit Framework

- What is the Metasploit Framework?
- Starting and Updating Metasploit
- Finding Metasploit Modules

Web Attacks
Mass Email Attacks
Multipronged Attacks

Bypassing Antivirus Applications

Trojans
How Antivirus Applications Work
Microsoft Security Essentials
Getting Past an Antivirus Program
Hiding in Plain Sight

After the Exploit

Introduction to Meterpreter
Working with Meterpreter Scripts
All about Metasploit Post-Exploitation Modules
Local Privilege Escalation
Local Information Gathering
Lateral Movement
Pivoting
Persistence

Web Application Testing

Working with ZAP Attack
SQL Injection
XPath Injection
Local File Inclusion
Remote File Inclusion
Command Execution
Cross-Site Scripting
Cross-Site Request Forgery
Web Application Scanning with w3af

Wireless Attacks

Setting Up
Monitor Mode
Capturing Packets
Open Wireless
Wired Equivalent Privacy
Wi-Fi Protected Access
WPA2
Wi-Fi Protected Setup

Mobile Hacking

About the Smartphone Pentest Framework
Mobile Attack Vectors
The Smartphone Pentest Framework
Remote Attacks
Client-Side Attacks
Malicious Apps
Mobile Post Exploitation

Advanced Exploits (If TIme Permits)

Understanding Buffer Overflows
Creating the Exploit Code
Compiling the Exploit Code
Uploading the Payload