PhynxLabs Certified Security Professional

COURSE BROCHURE

INTRODUCTION

This 5-day penetration testing training course is a great place to start your journey towards becoming a professional penetration tester.

Armed with a virtual penetration testing lab environment that includes Kali Linux and series of vulnerable operating systems/web applications, the lab intensive environment gives each student in-depth knowledge and practical experience needed to research the network (information gathering), identify any vulnerabilities and execute tools, including modifying exploit code, all with the goal to compromise the systems and gain administrative access.

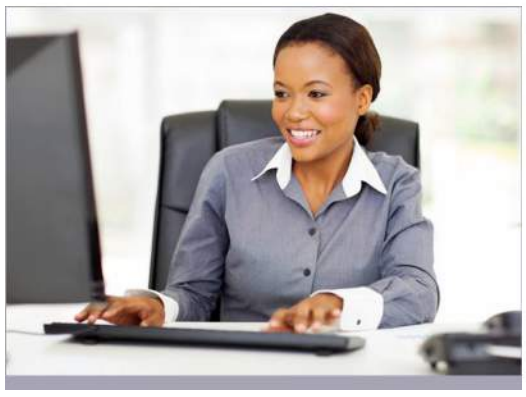
With its collection of hands-on lessons that cover key tools, techniques and strategies, this course is ideal for IT students, IT enthusiasts, web developers, IT security professionals, network engineers, Windows and Linux administrators, security engineers, database administrators and webmasters as well as anyone interested in learning basic ethical hacking techniques.

EXAM INFORMATION

At the end of the course, students will sit for the Phynxlabs Certified Security Professional (PCSP) exam which consist of a vulnerable system designed to be compromised within a 4hour period. The exam is entirely hands on and it challenges the students to prove that they have a clear practical understanding of the penetration testing process.

Who Should Attend?

- You
- IT Students
- IT personnel
- Auditors
- IT Security Enthusiasts
- Penetration testers
- IT Security Professionals
- Developers



What am I going to get from this course?

- Over 15 modules and 25 hours of content!
- A dedicated hacking lab with series of vulnerable operating systems/web applications to practice with
- How to compromise systems security (Windows and Linux Systems)
- You will learn Windows and Linux Post Exploitation Techniques
- You will learn how to crack passwords and wireless network keys with brute-forcing and wordlists
- You will learn how to find and exploit Web Application Vulnerabilities
- You will learn how to perform a comprehensive penetration test and accurately document your findings in order of priority or significance of the strengths and weaknesses.
- How to apply countermeasures to protect an organisation from exploitation.
- How to document your findings effectivel to explain them to the business.
- Be ready to sit for the exam

Complete Package Details

- Intensive Hands-on Training
- PSCP Certificate
- Detailed student Textbook
- PCSP Souvenirs
- Breakfast & Lunch

PHYNXLABS
Securing you digitally

Course Content

Introduction to Penetration Testing
- Why do we perform Penetration testing?
- Stages of Penetration tests
- Types of Penetration Tests

Setting up your Penetration testing Lab
- Installing Vmware
- Setting up Kali Linux
- Setting up target virtual machines

Information Gathering Techniques
- Internet Service Registration
- DNS Reconnaissance
- WHOIS Queries
- Ping & Trace route Network Probing

Target Scanning
- Port Scanning Basics
- Banner Grabbing
- OS Fingerprinting
- Port Scanning with NMAP

Table Of Contents

Vulnerability Assessment
- Causes of Vulnerabilities
- Finding Vulnerabilities with Nessus
- Finding Vulnerabilities with Nikto
- The NMAP Scripting Engine (NSE) Approach
- Scanning with the Metasploit Framework

Sniffing & MITM Attacks
- Introduction to Sniffing
- Capturing Traffic
- Mac Flooding
- Arp Cache Poisoning for MITM
- Intercepting SSL Traffic

The Metasploit Framework
- Msfconsole Commands
- Msfcli
- Armitage
- Using Exploits
- Generating Payloads
- Meterpreter Basics

Windows Exploitation
- Vulnerabilities Vs Exploits
- Attacking Windows
- Microsoft Windows Server Service RPC code
- Password Attacks
- Online/Offline Password Attacks
- Bruteforce Attacks
- Dictionary Attacks
- John The Ripper
- Cracking Windows Password
- Cracking Linux Password

Linux Exploitation
- Finding/Fixing Exploits
- Web Shells
- Permission Errors
- Linux Privileg

Client Side Attacks
- Client Side Exploits
- Browser specific vulnerabilities
- Adobe util.printf() Buffer Overflow
- Social Engineering
- Lab Exercise

Post Exploitation
- Post Exploitation with Metasploit
- Local Privilege Escalation
- PSExec Pass the Hash
- Enabling Remote Desktop
- Persistence
- Lab Exercise

Wireless Attacks
- Wireless Threats
- Discover WiFi Networks
- Attacking Wi-Fi Networks
- Lab Exercise

Web Application Attacks
- Cross Site Scripting
- Local File Inclusion Vulnerabilities
- Remote File Inclusion Vulnerabilities
- Command Execution
- SQL Injection
- Lab Exercise

PhynxLabs Certified Security Professional (PCSP)
- Writing a penetration testing report
- Final Lab Exam
- Closing speech by an Information Security Thought Leader

Fee: N150,000 Naira per participant

For more information, please call: +234 802 266 3120 or E-mail: pscb@phynxlabs.com or visit our website: www.phynxlabs.com