

## CEH + PWK

### (پکیج هک قانونمند و تست نفوذ با کالی لینوکس)

**خلاصه دوره :** در این پکیج آموزشی دو دوره محبوب CEH از شرکت EC-Council و PWK از شرکت Offensive Security قرار داده شده است. هدف کلی این پکیج آماده ساختن دانشجویان برای شناسایی آسیب پذیری های مختلف در انواع زیر ساخت ها از جمله شبکه است تا در صورت وجود آسیب پذیری اقدامات لازم صورت گیرد.

دوره CEH: دوره **Certified Ethical Hacking** (هکر قانونمند) ، یکی از مطرح ترین دوره های هک و امنیت در جهان است. در این دوره دانشجویان به عنوان هکران کلاه سفید نحوه بازرسی از زیر ساخت های شبکه به طور قانونی در جهت یافتن آسیب پذیری های امنیتی را یاد خواهند گرفت. این دوره به شما کمک میکند تا وضعیت امنیتی یک سازمان را ارزیابی کنید تا مشخص شود آیا دسترسی غیر مجاز امکان پذیر است یا نه.

دوره PWK: دوره **Penetration Testing with Kali Linux** (تست نفوذ با کالی لینوکس) ، یک دوره گام به گام برای یادگیری تست نفوذ با سیستم عامل کالی لینوکس است. در این دوره علاوه بر ابزار و تکنیک های تست نفوذ ، طرز فکر یک هکر که برای تست نفوذ موفقیت آمیز نیاز است نیز آموزش داده میشود.

### مفایین دوره:

- علاقه مندان به یادگیری مباحث هک و نفوذ
- مدیران فناوری اطلاعات
- کارشناسان تست نفوذ

**مدت دوره:** ۶۰ ساعت

**پیشنیاز:** دوره نتورک پلاس (+Network)

### سرفصل دوره:

#### CEH:

- Module 01: Introduction to Ethical Hacking
- Module 02: Footprinting and Reconnaissance
- Module 03: Scanning Networks
- Module 04: Enumeration
- Module 05: Vulnerability Analysis
- Module 06: System Hacking
- Module 07: Malware Threats
- Module 08: Sniffing
- Module 09: Social Engineering
- Module 10: Denial-of-Service
- Module 11: Session Hijacking
- Module 12: Evading IDS, Firewalls, and Honeypots
  
- Module 13: Hacking Web Servers
- Module 14: Hacking Web Applications
- Module 15: SQL Injection



IT Professional Training Center Module 16: Hacking Wireless Networks

Module 17: Hacking Mobile Platforms

Module 18: IoT Hacking

Module 19: Cloud Computing

Module 20: Cryptography

## PWK:

Penetration Testing: What You Should Know

Getting Comfortable with Kali Linux

Command Line Fun

Practical Tools

Bash Scripting

Passive Information Gathering

Active Information Gathering

Vulnerability Scanning

Web Application Attacks

Introduction to Buffer Overflows

Windows Buffer Overflows

Linux Buffer Overflows

Client-Side Attacks

Locating Public Exploits

Fixing Exploits

File Transfers

Antivirus Evasion

Privilege Escalation

Password Attacks

Port Redirection and Tunneling

Active Directory Attacks

The Metasploit Framework

PowerShell Empire