SEMATEC
IT Professional Training Center

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 **C**ertified **E**thical **H**acker **(CEH)** معروف به **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.

هکر قانونمند کیست؟ هکر های قانونمند یا کلاه سفید افرادی هستند که از دانش خود نه برای اهداف مخرب بلکه برای ایمن کردن سیستم های رایانه ای استفاده میکنند. آنها با پیدا کردن آسیب پذیری و نقص های امنیتی و گزارش آنها باعث بر طرف شدن مشکلات امنیتی شرکت و سازمان شده و در نتیجه امنیت را بالا میبرند.

این دوره در آموزشگاه سماتک طبق آخرین ورژن رسمی آن (V10) برگزار میشود.

دوره PWK: دوره (**P**enetration **T**esting with **K**ali Linux) PWK ، یکی از دوره های شرکت Offensive Security در زمینه تست نفوذ میباشد. شرکت Offensive Security یکی از شرکت های پیشرو در زمینه آموزش امنیت سایبری میباشد. در این دوره دانشجویان با ابزار ها و روش های تست نفوذ در سیستم عامل کالی لینوکس (Kali Linux) به صورت عملی آشنا میشوند. در دوره PWK نه تنها مهارت بلکه طرز فکر لازم برای هک و تست نفوذ موفق نیز آموزش داده میشود.

این دوره در آموزشگاه سماتک طبق آخرین ورژن آن (PWK 2020) تدریس میشود.

آپدیت های ۲۰۲۰ این دوره:

مطالب اضافه شده:

- Modules
  - Active Directory Attacks
  - PowerShell Empire
  - Introduction to Buffer Overflows
  - Bash Scripting
- Labs: 3 dedicated student virtual machines (Windows 10 client, Active Directory domain controller, Debian client), more shared lab machines

- New target network to facilitate a hands-on walkthrough demonstrating a complete penetration testing exercise
- Extra mile exercises

مطالب آپدیت شده:

- All existing modules were updated, most notably:
  - Passive Information Gathering
  - Win32 Buffer Overflows
  - Privilege Escalation
  - Client-Side Attacks
  - Web Application Attacks
  - Port Redirection and Tunneling
  - The Metasploit Framework
- Updates to existing machines' OS and attack vectors

توانایی هایی که بعد از گذراندن این دوره کسب میکنید به طور خلاصه گفته شده است:

- استفاده از تکنیک های جمع آوری اطلاعات برای شناسایی اهداف کسب اطلاعاتی مانند سیستم عامل آنها
- نوشتن اسکریپت (Script) و ابزار های ساده تست نفوذ
- استفاده ، آنالیز و تغییر Exploit های مختلف
- استفاده از حملات لوکال (Local) و سمت کلاینت مانند Privilege Escalation
- آسیب پذیری های تحت وب مانند (SQLi) SQL Injection ، XSS ، RFI ، LFI
- Pivoting
- مهارت حل مسئله

مخاطبین دوره:

- تمامی علاقه مندان به یادگیری هک و تست نفوذ و امنیت
- کارشناسان تست نفوذ (Penetration Testing Experts)
- مدیران فناوری اطلاعات (IT Managers)

- تمامی علاقه مندان به یادگیری و فعالیت در حوزه جرم شناسی دیجیتال ، فارنزیک و جرایم رایانه ای (Digital Forensics)
- متخصصین و علاقه مندان SOC (**S**ecurity **O**perations **C**enter)
- مختصصین امنیت شبکه (Network Security Professionals)
- متخصصین تست نفوذ (Pentest Professionals)
- متخصصین امنیت اطلاعات (Information Security Professionals)
- آدمین های شبکه (Network Admins)

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

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
Assembling the Pieces: Penetration Test Breakdown
Trying Harder: The Labs

لینک توضیحات دوره در سایت EC-Council:

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh

لینک توضیحات دوره در سایت Offensive Security:

https://www.offensive-security.com/pwk-oscp/