academy

Pentesting with Kali Linux (PWK) - OSCP

Partner Training

Training code	TSTOCP-CE
Spoken Language	English
Language Materials	English
Dayparts	10
Price	€5.495,00 excl. VAT No extra costs.

What is OSCP - Pentesting with Kali Linux (PWK)

Penetration Testing with Kali Linux (PWK) is an advanced penetration test training, developed for pentesters, network administrators and security professionals who want to take a serious step in the world of professional pen testing.
In this unique training you use the most up-to-date ethical hacking tools and techniques in challenging, virtual pen testing labs that simulate a full penetration test from start to finish. You will receive a target-rich, diverse and vulnerable network environment for this purpose.
An OSCP is able to identify existing vulnerabilities and conduct organized attacks on them in a controlled and focused manner, write simple Bash or Python scripts, modify existing exploit code to its advantage, perform network pivoting and data exfiltration.

Who should attend OSCP - Pentesting with Kali Linux (PWK)

This training is interesting for students with various backgrounds and personal goals:

- Security Professionals,
- Penetration testers,
- Ethical Hackers,
- Network administrators

and any experienced IT specialist who wants to learn to look out-of-the-box to the security of an IT environment.

Prerequisites

With regard to the level of the training, knowledge or experience at CEH level is an absolute advantage. At least a good understanding of TCP / IP, networking and a reasonable skill with Linux are required. Not required but nice to have familiarity with Bash scripting and basic Perl or Python knowledge

academy

Objectives

Objectives are:

- Use multiple information gathering techniques to identify and enumerate targets running various operating systems and services
- Write basic scripts and tools to aid in the penetration testing process.
- Analyze, correct, modify, cross-compile, and port public exploit code.
- Successfully conducting both remote and client side attacks.
- Identify and exploit XSS, SQL injection, and file inclusion vulnerabilities in web applications.
- Deploy tunneling techniques to bypass firewalls.
- Demonstrate creative problem solving and lateral thinking

If a third-party copyright applies to this course, you will find the copyright on https://academy.capgemini.nl/en/topic/trademarks/

Capgemini Academy's general terms and conditions are applied to all products and services mentioned within this document. For the latest version please check https://academy.capgemini.com/. The rates of products and services mentioned in this document are subject to change. For the most recent rates, please also visit our website.

About Capgemini Academy

Capgemini Academy's professionals offer what people in IT need. Our professionals have a keen eye for motivation, talent and are aware of specific contexts and circumstances. They move people to move. Programmes and courses that originate from daily experience of our both didactical and substantively strong trainers, light a fire within the individual IT professionals.
Real life stories of our professionals' experience that tell how to solve problems and work with the people around it, do the rest.

An organization, like ours, helps people and their organizations day by day to get the best out of themselves and each other. We prepare them to defy tomorrow's challenges. We stimulate learning and curiosity. In order for individual IT professionals and their employers, to build better, longer and more intensive relationships. For mutual benefit.

Capgemini Academy. We transform IT professionals
academy.capgemini.nl

IN/3A-018.18