Cyber attack prevention

Course: **00168**
Filter: **Beginner**
Duration: **2 days**
Category:: **Cyber Security**
Price: **797,00 €**

About Course

Based on practical experience of penetration testing, this training course will will enable you to understand how professional hackers work as well as the techniques used and the vulnerabilities to be exploited. We will discuss the best practices to adopt in order to protect yourself.

What you'll learn

- Understand the motivations of hackers
- Understand how they operate
- Develop techniques to counter attacks

Targeted audience

- Security managers
- CSO
- CTO
- Network administrators

Pre-requisites

- Understanding basic safety vocabulary

Curriculum

Module 1: Introduction

- What will this training bring you?
- Setting the context
- Impact of a cyber attack on a company and its employees

Module 2: Put yourself in the shoes of a pentester

- This module will guide you through realistic scenarios to develop your pentester mindset
- The aim is to understand behaviour in order to train defenders rather than attackers
- Learn the essential steps of a pentest
- Developing critical and divergent thinking in the face of vulnerabilities
- Solve a realistic CTF (Capture the Flag) based on real-world scenarios
- To understand a hacker, you need to understand how they think and what their objectives are
- To protect yourself against attacks, you need to know what weapons your adversary is using

Module 3: Video game hacking experience

- Explore the techniques, tools and methodologies used to analyse and exploit video games
- This module covers the key concepts of game hacking, including debugging, memory modification and exploiting software flaws
- Understanding the basics of game hacking
- Discovering the essential techniques and tools
- How the lessons and skills learned can be applied in other areas of cyber security

Module 4: Strengthening your perimeter with open-source tools

- Discover how to secure your network perimeter using open-source tools
- Techniques and tools to prevent and detect threats

- Identifying open-source tools to strengthen perimeter security
- Implementing proactive defence strategies
- Understanding the limitations and advantages of open-source tools

Module 5: Creating a test environment

- Learn how to create and explore homelabs to develop your cybersecurity skills
- Equip participants to set up isolated and secure test environments for theory verification and debugging
- Understanding the steps involved in creating a homelab
- Identify the essential tools for configuring a homelab
- Explore practical learning scenarios

Module 6: Wrap-up

- Review of lessons learned
- How to detect an attack
- Best practices
- Recommendations for participants and companies
- Suggestions for more in-depth training courses
- Survey and feedback