almond INSTITUTE

Training sheet
Hacker techniques
How to protect yourself

CONTACT FOR THIS TRAINING

Miora RAHARINIRINA
Almond Institute coordinator
almond.institute@almond.eu
07 64 42 71 56

→ Version 1.0
→ 08/12/2023

Hacker techniques - How to protect yourself

Course overview

This training program aims to raise awareness among IT teams about IT risks and their consequences. This module presents the techniques commonly used by hackers, while popularizing the subject for a non-technical audience. It details the best practices to adopt to protect against most attacks.

01. **Raising awareness among IT teams** about IT risks and their consequences

02. **Presentation of techniques commonly used by hackers** by popularizing the subject for a non-technical audience

03. **Detailing the best practices** to adopt to protect against most attacks

Hacker techniques - How to protect yourself

Useful informations

Who should attend?

- IT team
- CISO
- IT Support team
- System administrator
- Network administrator

Entry requirements

- Computer basics: network (protocols, OSI model, etc.) and system (Linux or Windows, server management, etc.).

Method of assessment

Production of a final online questionnaire covering all the concepts learned.

How and when to acces

The participant is considered registered when:

- The prerequisites and needs are identified and validated
- The training agreement is signed

Registration requests can be sent up to 10 working days before the start of the training.

To go further

This training course is a preparation for the following training course:

- Secure IT development techniques

Accessibility

Whether you are recognized as having a disability or not, making our training accessible to everyone is part of our commitment. If you need compensation or adaptation for the content, the supports, the "venue", the material used, the schedules, the rhythm, **we are at your disposal**.

READ MORE

Hacker techniques - How to protect yourself

Face-to-face and distance learning

Course overview

Introduction	Web application security	Equipment weakness	Security for mobile devices	Active Directory Security	Social engineering	WIFI networks
→ Cybersecurity context (CNIL, threats, attackers, data leaks, the black market in vulnerabilities, etc.). → MITRE ATT&CK matrix	→ OWASP → Authentication/Password storage → HTTP (Burp Suite presentation)	→ Risks of USB equipment → Recommendations	→ The risks of nomadism → Data encryption and erasure → Recommendations	→ NTLM authentication and relay → Password management → Privilege management → Security tools	→ How to detect it? → Fraud by email, telephone, to the president → Recommendations	→ Wireless network protection

Training benefits

- Training by an offensive safety expert
- Operating recommendations
- Practical tools
- Real case studies

Price and informations

- **Duration:** 7 hours
- **Price:** Contact us
- **Financing:** OPCO support

→ READ MORE