training code: BS.IT 04 / ENG AA 1d_W / EN

# Secure administrator – practical IT security workshop

## Purpose of the training

The aim of conducting workshops is preparing IT department personnel to evaluate organization's security with selected tools. This course will empower IT administrators with knowledge regarding software tools as they build or improve the security of IT infrastructure. It will also teach administrators to act as 'hunters' to identify the latest cybersecurity threat sources so they can stop breaches before complete organizational compromise occurs.

## Benefits of completing the training

- Evaluation of real corporate infrastructure security posture
- Raising the level of knowledge and skills of technical personnel responsible for system maintenance
- Acquaintance with the best practices related to IT infrastructure securities
- Acquaintance with selected tools used in IT security
- An opportunity to perform security audits on your own

## Expected Listener Preparation

- Basic computer skills

## Training Language

- Training: English
- Materials: English

## Training Includes

- 1 day of work with a trainer
- Trainer's supervision
- Contact with community
- Coursebook
- Lab environment

Training method

- lecture
- workshops

## Duration

1 days / 7 hours

## Training agenda

1. Introduction to workshops
   - Discussing basic topics related to IT security (terminology, risk and elements of Risk Management, what is system „hardening" and where to look for sources of information related to it)
2. Preparation for exercises
   - Discussing laboratory environment (VMware Workstation, network topology, operational systems)
3. OSINT (open-source intelligence) elements
   - Discussing where and what information related to company's infrastructure and employees can be found on the Internet by potential intruders
4. Network scanning and detecting details related to operational systems and services
   - Discussing tools used for OS and services discovery
5. Scanning and analysing vulnerabilities

- Discussing selected tools used to automate vulnerability scanning (OpenVAS)
- Discussing reports results

6. Hacking systems and devices
   - Discussing selected tools and methods of system hacking. Taking control over vulnerable system stealing password, intercepting webcam and keyboard input. Privilege escalation and sample Active Directory attacks.
7. Wireless network security and password cracking
   - Wireless network security analysis and intercepting traffic which will enable cracking password Discussing selected tools. Cracking WEP and WPA2 passwords.
8. Social engineering in practice
   - Discussing selected tools used in social engineering attacks, preparing environment for social engineering campaign