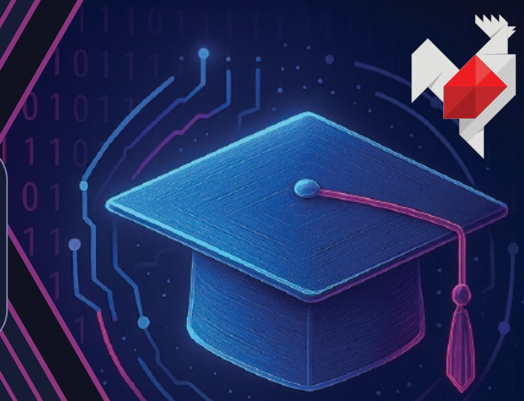
securITum

Netsecurity **Master** from sekurak



Learn how to effectively secure your IT infrastructure by exploring the techniques used by attackers!

Language course: Polish

11 live training sessions, each 4 hours long, in an accessible format

MODULE 1

SIX LIVE SESSIONS

2800 PLN NET

MODULE 2

FIVE LIVE SESSIONS

2200 PLN NET

COMBINE AND BENEFIT

MODULE 1 and MODULE 2

~~5000~~ PLN NET

3990 PLN NET

WHY THIS COURSE IS SO GOOD

- Over 40 hours of practical, hands-on training
- The minimum necessary theory, with real-life examples of network vulnerabilities and effective ways to eliminate them
- Knowledge delivered by experienced IT system administrators/auditors
- Access to a dedicated training platform and network lab
- Access to recordings of all training sessions

BENEFITS FOR THE COMPANY AND TEAM

- More effective identification of potential attacks on the company's network infrastructure
- Ability to apply learned protection methods against attacks
- Skills to independently conduct penetration tests
- Increased team awareness of the consequences of cybercrime
- Improved security within the company

netsec.sekurak.pl

AGENDA

MODULE 1

Session 1: Network Reconnaissance and Vulnerability Scanning:

- Port scanning. How do port scanners work? Which services run on which ports? Use of advanced filters and network scanning techniques (including very large networks).
- Practical methodology for managing scan results. How to effectively scan huge networks without getting lost?
- Fuzzing of web application directories.
- Introduction to OSINT. Searching for domains, subdomains, organizational IP addresses, cloud resources, and collecting additional data based on the organization's name and partial information.
- Hands-on lab for self-practice.

Session 2: Exploiting Network Services. Email Security:

- Methods for finding exploits online. Creating and modifying your own exploits. Identifying so-called "low-hanging fruits".
- Metasploit: a tool for exploitation, but also for managing scanning of large networks.
- Techniques for gaining and maintaining control over a compromised device (persistence). Explanation of terms: reverse shell, bind shell, web shell, staged shell, stageless.
- Common security issues related to SMTP services.
- Hands-on lab for self-practice.

Session 3: Moving Within a Local Network:

- Analyzing a local device after gaining access. Gathering key information about the LAN and the device itself.
- Port forwarding, network pivoting. How to move between subnets?
- How to stealthily scan an internal LAN without having a port scanner available on the compromised device?
- Hands-on lab for self-practice.

Session 4: Wi-Fi Security. Antivirus Evasion Techniques:

- WPA2-PSK, WPA2-Enterprise, WPA3, or even WEP? Clarifying the theory.
- Reconnaissance of local Wi-Fi networks.
- Practical attacks on modern Wi-Fi networks: from WPA2-PSK attacks, through Evil Twin, to WPA3 downgrade attacks.
- Overview of static and dynamic malware analysis techniques.
- Sample antivirus/EDR evasion techniques.
- Introduction to Command and Control concepts.
- Searching for C&C servers online.

Session 5: IDS/IPS:

- Fundamentals of IDS/IPS systems.
- Introduction to configuring Snort and Wazuh.
- Detecting specific traffic signatures in a local network using Snort.
- Hands-on lab for self-practice.

Session 6: Multi-Stage Practical Task Summarizing the Training Module

MODULE 2

Session 1: Security Issues in Linux Systems:

- Gathering information about the local system and services on the network.
- Common privilege escalation techniques on the device.
- Hiding backdoors.
- Hardening and defense against attacks (SELinux, AppArmor, sandboxing, principle of least privilege, minimizing attack surface, kernel hardening, data-at-rest encryption).
- Hands-on lab for self-practice.

Session 2: Security Issues in Windows Systems:

- Gathering information about the local system and services on the network.
- Attacks on user accounts and passwords.
- Common privilege escalation techniques on the device.
- Hiding backdoors. Obfuscation and evading detection.
- Hardening and defense against attacks (hardening Windows protocols, securing local accounts, minimizing attack surface, data-at-rest encryption).

Session 3: Active Directory Basics from a Pentester's Perspective:

- Techniques for easily obtaining credentials of additional devices after gaining access to the LAN.
- Active Directory enumeration and identifying common vulnerabilities.
- Proven methods for easily acquiring credentials of key users and the domain controller.

Session 4: Basics of Docker and Kubernetes Security:

- Attacks on Docker/Kubernetes containers and daemons.
- Fundamental principles for securely configuring Docker and Kubernetes.
- Hands-on lab for self-practice.

Session 5: Multi-Stage Practical Task Summarizing the Training Module

TRAINERS

Marek Rzepecki

Tomasz Turba

Kamil Jarosiński

securITum

FOR WHOM

- IT administrators
- SOC employees
- Security department employees
- Pentesters
- Individuals responsible for implementing security measures in companies

REGISTRATION AND DETAILS

netsec.sekurak.pl

Additional questions: e-mail: szkolenia@securitum.pl
phone: +48 (12) 352 33 82