

# Training:

## Hardening Microsoft Environments

Date of the training: **June 27-28, 2022** in Heidelberg, Germany

Book now using the voucher code: **TR22\_HMTRAINING** and save an additional 5% of the current valid rate of any package!

### Overview

#### Day 1

- Introduction
- Relevancy and actuality of Credential Theft und Credential Reuse
- Windows Authentication
- Basics of Windows Authentication
- Security Subsystem Architecture in Windows
- Local Security Authority Subsystem Service
- Local authentication
- LM/NTLM network authentication
- Kerberos network authentication
- Credential Theft & Reuse Attacks
- Introduction into mimikatz
- Pass-the-Hash
- Pass-the-Ticket
- Overpass-the-Hash/Pass-the-Key
- Golden & Silver Ticket, Inter-Realm Ticket
- PtT in Ubuntu and Mac OS X
- Practical Exercises for All Mentioned Attack Techniques
- First Overview of Relevant Measures to Reduce Risk
- Reorganization of the Active Directory structure and best practice for administration
- Technical and Credential-Theft-specific measures
- Security monitoring & logging

## Day 2

- Detailed Examination of Relevant Measures to Reduce Risks
- Requirements
- Organizational and design measures (Admin Tiering, ESAE Forest)
- Technical measures
- Secure administration hosts
- Secure configuration of domain controllers and members
- Credential-Theft-specific measures
- Active Directory Monitoring
- Overview of Windows Event Logging
- General monitoring measures
- Centralized logging
- Basics of Advanced Audit Policy
- Specific monitoring measures
- Detection of PtH, PtT and Golden Tickets

## Who should attend this training?

- IT Security Officers
- Windows & Active Directory Administrators
- Project Managers with security focus
- Infrastructure and system architects
- System integrators
- Head of IT & Data Protection Supervisors

## Requirements

The attendees should have:

- Basic knowledge of Active Directory environments and Windows systems
- You will need to have your own Laptop and you will need to be able to establish a https connection to the workshop's AD Lab environment in order to perform the workshop's exercises

## About the Trainers:

**Heinrich Wiederkehr** is a Senior Security Consultant at ERNW Enno Rey Netzwerke GmbH and his focus lies on the assessment and evaluation of security-relevant areas in Windows-based environments, as well as the creation of related concepts and documentation. In addition to his work in audits and pentests of large enterprise networks with emphasis on Active Directory and the Windows operating system, he is also responsible for security trainings and talks. A multitude of projects for customers from different industry branches gives him a solid feeling for practical realities and an eye for essentials.

**Lennart Brauns** is a Security Consultant at ERNW Enno Rey Netzwerke GmbH and part of the Microsoft Security Team @ ERNW. In many years of working for critical infrastructure companies, Lennart has gained extensive knowledge of Microsoft Windows, Active Directory and Microsoft Azure. His focus is on research as well as design and assessment of different areas of Windows environments. In addition to security training, his work focuses on audits and pentests of enterprise networks with an emphasis on Active Directory.

## Booking

Recommended online booking of trainings through:

<https://troopers.de/tickets/>

### **Voucher code: TR22\_HMTRAINING**

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

## Contact

**Need assistance?** Don't hesitate to call us. We are fluent in English and German.  
+49 6221 480390 or [info@troopers.de](mailto:info@troopers.de)

**Booking is also possible offline through your trusted partner:**

**HM Training Solutions**, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / [info@hmtrainingsolutions.com](mailto:info@hmtrainingsolutions.com)

+49 6022 5089999 / [www.hmtrainingsolutions.com](http://www.hmtrainingsolutions.com)