TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Hardening Microsoft Environments

Date of the training: **March 18–19, 2019** in Heidelberg, Germany

Book Now using the voucher code: **TR19_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

Credential theft attacks can be described as a technique in which account logon credentials are captured from a compromised computer, and then used to authenticate to other systems on the network. Attack techniques which fall in the categories of “Credential Theft” or “Credential Reuse” have grown in the last few years into one of the biggest threats to Microsoft Windows environments.

In 2015 and 2016, this development was significantly promoted by a considerable improvement and increasing distribution of hacking and attack tools, such as /mimikatz/ and /Windows Credential Editor/ and frameworks for attacking Active Directory environments such as /PowerSploit/. This led to theoretical attacks being actually possible in real world scenarios with the application of the aforementioned methods. Once an attacker gains initial foothold on a single system in the environment it takes often less than 48 hours until the entire Active Directory infrastructure is compromised.

But how can such a threat be handled?

In this intensive two-day seminar, we will present various technical and organizational measures to protect both individual critical Microsoft Windows systems, as well as the entire Active Directory. The goals in mind are to prevent credential theft in the first place, but also to protect

against and detect unauthorized use of stolen credentials as early as possible and to provide important hardening guideline information.

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

Requirements

- Basic knowledge of Active Directory environments and Windows systems.
- You will need to bring your own Laptop with an up-to-date RDP client and you will need to be able to establish an RDP connection to the workshop's AD Lab environment in order to perform the workshop's exercises.

About the Speaker: Florian Gattermeier

Florian Gattermeier is a Security Analyst at ERNW and part of the Microsoft security team. He focuses on research and assessment in various areas of Windows-based environments. Apart from security trainings, his work concentrates on audits and pentests of large-scale enterprise networks with emphasis on Active Directory. A vocational training before studies and a wide variety of projects for different customers and give him a solid awareness of the practical realities and hands-on experience. Florian holds a bachelor's degree in computer engineering at University of Applied Sciences Mannheim.

About the Speaker: Nina Matysiak

Nina Matysiak is a Security Analyst at ERNW and part of the Microsoft security team. She focuses on assessments of Azure and Active directory environments. Several projects for different customers give her a solid awareness of the practical realities and obstacles in these areas.

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended Online Booking of Trainings Through:

Sign-Up Form https://troopers.de/tickets/

Voucher code: **TR19_HMTS**

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code up until March 11th, 2019 or until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German.

Zögern Sie nicht uns zu kontaktieren. Wir sprechen fließend Englisch und Deutsch.

Troopers Organization Team

+49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner from:

HMTS HM Training Solutions

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com