TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Hardening Microsoft Environments

Date of the online training: **March 17-18, 2021**

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* or *Empire*. 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.

ERNW Enno Rey Netzwerke GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
info@ernw.de

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
BIC: GENODE61HD3
IBAN: DE43 6729 0100 0059 7891 04

Managing Directors
Florian Grunow
Michael Schaefer
VAT-ID: DE 813 376 919

Agenda

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

Prerequisites

- Basic knowledge of Active Directory environments and Windows systems.

Requirements

- A stable, wired Internet connection (preferably without a VPN connection)
- An up-to-date browser with HTML5 support (preferably Google Chrome)
- Deactivation of browser plugins that may block content from the training platform
- WebRTC support in the browser and the network configuration
- Optional: a working microphone and webcam

About the Trainers

Heinrich Wiederkehr is a Senior Security Consultant at ERNW 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.

Thomas Schlabach is a Security Consultant at ERNW GmbH and part of the Microsoft Security Team @ ERNW. His work focuses on Windows operating system security as well as security logging and monitoring. In addition to security trainings, he is involved in performing security assessments (pentests and audits) as well as conducting system analyses of clients and servers in corporate networks.

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended online booking of trainings through:

https://troopers.de/tickets/

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German. +49 6221 480390 or 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

+49 6022 5089999 / www.hmtrainingsolutions.com