Training:

Hardening Microsoft Environments

Date of the training: June 24th – 25th, 2024 in Heidelberg, Germany

Book now using the voucher code: **TR24_HMTRAINING** 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.

Since 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.

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
- Practical Exercises for All Mentioned Attack Techniques
    - Trojan / RAT
    - Practical Exercises for All Mentioned Attack Techniques
    - 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.

- Notebook to establish a browser-based HTTPS connection to the AD lab environment of the workshop.

About the Trainers:

Friedwart Kuhn is a renowned expert for Active Directory security. He knows AD since the beginning and has performed a large number of projects, both in the assessment field (audits, pentests) and in the concept/design space of large enterprise AD environments. He likes to transfer his knowledge in trainings and conferences. Friedwart is the team lead of the Microsoft Security Team@ERNW.

René Mathes is a longstanding auditor and penetration tester. For more than 10 years of his work as IT security analyst he gives advice to a diverse portfolio of customers: Mid-tier companies, city authorities to true global players, advertisement to heavy industry. As tutor he develops workshops that he holds throughout Germany for example for attendees from the financial world.

Booking

Recommended online booking of trainings through:

https://troopers.de/tickets/

Voucher code: TR24_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

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany
+49 6022 508200 / info@hm-ts.de
+49 6022 5089999 / https://hm-ts.de