Buy tickets: https://romhack.io/buy-tickets/

AZURE AD SECURITY TRAINING

Dirk-jan Mollema

COURSE OBJECTIVES

This training explains how organizations use Azure AD to manage modern cloud-based or hybrid environments and what security challenges this brings. It is the result of many years of research into the protocols and internals of Azure AD. It will give you the knowledge to analyze, attack, and secure Azure AD and hybrid setups from modern attacks. The training is technical and deep-dives into core protocols such as OAuth2 and application concepts. It includes many hands-on exercises and labs, set up as challenges, to gain access to accounts and elevate privileges. The training focuses on Azure AD's use as an identity platform. The training does not cover Azure Resource manager abuses, except the parts where it intersects with Azure AD. While a range of (open source) tools are used during the training, the goal is to provide understanding of the inner workings, not just on knowing how to run tools.

TRAINING OUTCOMES

Immersive learning of concepts and techniques to understand the inner workings of Azure AD, which can be applied during Azure AD pentests and red teams in hybrid environments.

WHO SHOULD ATTEND?

Red teamer, blue teamer, penetration tester, security architect, IT professionals

ABOUT THE TRAINER

Dirk-jan Mollema is a hacker and researcher of Active Directory and Azure AD at Outsider Security. Amongst the open-source tools published to advance the state of (Azure) AD research are aclpwn, krbrelayx, mitm6 and the Azure AD ROADtools framework. He blogs at dirkjanm.io, where he publishes about new Active Directory attack chains, which included the discovery of the PrivExchange vulnerability. He presented previously at TROOPERS, DEF CON, Black Hat, RomHack and BlueHat and was part of the MSRC most valuable researchers 2018 to 2020 through his Azure AD research.

WHAT TO BRING

Laptop with a virtualization platform (such as VMWare) with a virtual machine that can be used for the labs in the training. Most labs can be done on both Windows and Linux virtual machines, but some require the use of Windows. Note that not all required tools will work on Windows on ARM, having a x64 virtual machine is preferred.

Training page: https://romhack.io/training/azure-ad-security/
RomHack Training 2023: https://romhack.io/training/

Buy tickets: https://romhack.io/buy-tickets/

WHAT WILL BE PROVIDED?

Trainees will receive the training materials (slides) in PDF form. The online labs will be available for a short period after the training, but not all exercises will be available due to the changing configuration of the lab.

PARTICIPANT SKILL SET

The students should have some degree of existing knowledge of Windows, Active Directory, web based technologies such as REST API's, and be familiar with command line based tools, virtual machines and HTTP inspection/crafting tools.

CLASS SYLLABUS [1]

Tuesday, 12 September 2023 - Day 1

Lecture 1 - Introduction

> What is Azure, differences between Azure IaaS, Azure AD and Microsoft 365
> Terminology, components and their connection
> The modern Microsoft workplace way of working
> Identities: users, groups and devices

Lecture 2 - Azure AD components: Administrator roles and privileges

> Different roles and role types
> Privilege separation per role
> Privilege escalation in Azure AD

Wednesday, 13 September 2023 - Day 2

Lecture 3 - Azure AD components: data interfaces

> Data gathering in Azure AD
> Portal, API, PowerShell modules and the differences

Lecture 4 - Azure AD components: applications

> Apps and how they work
> Privilege model
> Apps and Oauth2 principles
> Breaking and securing applications

Thursday, 14 September 2023 - Day 3

Lecture 5 - Primary refresh tokens and device identity

> Interacting with primary refresh tokens via SSO
> Stealing and using primary refresh tokens for lateral movement

Using device identities to comply with conditional access policies

Lecture 6 - Identity security: Conditional Access

> CA policies and settings

[1] Schedule of lectures on the specified days may be subject to changes

- CA best practices and bypasses

Friday, 15 September 2023 - Day 4

Lecture 7 - Hybrid environments

- Different integration types with on-premises AD
- Access paths to the cloud from on-prem
- Azure AD connect abuse