Microsoft

Securing Windows Active Directory

WorkshopPLUS

Target Audience:

This course is an advanced course for securing Active Directory on all supported Windows Operating Systems. The course is targeted at Active Directory Administrators or Security Architects who have designed, deployed, administered and managed a Windows Active Directory infrastructure.

Active directory fundamental capabilities and behaviors will not be covered in this course, and it is expected that attendees will already possess that knowledge.

Overview

Active Directory is the backbone of every organization it is deployed in through its identity management, configuration management, and authentication services it provides. The thinking that attackers are outside your internal network is an out of date security mentality; according to researchers, the majority of attacks are from inside the network. This starts with protecting the Active Directory service. As Active Directory administrator or Active Directory security architect you have to protect the most sensitive business data and assets in your organization.

This 3-day workshop will teach students how to better secure your Active Directory Domain Controllers by reducing the attack surface, how to look for signs of compromise and how to secure the administrative and other powerful accounts. Our goal is to ensure that all students understand the importance, security mechanisms, and tasks required to secure and audit Active Directory using security recommended practices.

Key Features and Benefits

Each group of modules is organized by scenario and is designed to provide participants with in-depth skills. Attendees will have the opportunity to investigate and identify security issues in a poorly configured Active directory, and accomplish remediation through the use of freely available tools..

Technical Highlights

After completing this course, you will be able to:

- Understand typical security threats and the most effective countermeasures against them.
- Identify Security Issues & Protect Privileged Accounts on your sensitive Servers and your Active Directory partitions.
- Implement Remediation Plan and Monitoring.
- Develop skills for Security and Identity Protection for the Modern World.

Syllabus

This workshop is leveraging the Lab On Demand online platform. For closed deliveries the attendees will need an Internet connectivity to access the labs.

This workshop runs for three full days. Students should anticipate consistent start and end times for each day. Early departure on any day is not recommended.

Day 1

Module 1 – Introduction

This module presents the anatomy of attacks targeting Active Directory environment. This is the occasion to have open discussions about the presented techniques and mitigations. The module also reviews the fundamentals of information security and risk management.

Module 2 – Avenue to Compromise

This module explains the notion of initial breach targets. It includes a summary of the Windows authentication protocols as well as how they are leveraged in credential theft techniques. You will also be presented with how to identify powerful accounts and sensitive resources in your organization.

Day 2

Module 3 – Reducing the Active Directory Attack Surface

This module presents areas of security mitigation through the latest security features in Windows Active Directory and the recommended security practices. This includes the least-privilege administration model and the dedicated administrative hosts.

Day 3

Module 4 – Monitoring Active Directory for Signs of Compromise

This module provides information on the Windows auditing feature. It encompasses event log management and security monitoring of hybrid as well as on-premises environments.

Module 5 – Planning for Compromise

This last module is looking at additional techniques and processes you can deploy to secure your Active Directory service. It is the occasion to prioritize all the mitigations we have seen in accordance to our latest guidance. We also review the free tools you can use to scan and analyze your environment.

This data sheet is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY