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 The thinking that attackers are outside your internal network is an out of date security mentality; according to researchers, the majority of attacks are from inside the network.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

Contact your TAM if hardware is to be provided. If you are attending an Open enrollment workshop, the hardware will be provided for you.

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: Security Issues / Threats & Myths and Reality

This module details Active Directory security threats and current Top 10 security issues illustrated by demos. This is also an opportunity for open discussion about Security Myths and Reality.

Module 2: Identify & Protect Privileged Accounts – Part 1

In this module, you will be presented with how to identify powerful accounts and sensitive resources in your organization; how to identify security hygiene issues, where and how credentials are stored; authentication protocol mechanism and an overview of risk management.

Day 2

Module 3: Protect Privileged Accounts – Part 2

This module presents areas of security mitigation through the latest security features in Windows Active Directory and the recommended security practices..
A lab put attendees in a real condition where they have to identify security issues in Active Directory using provided list of tools.

Module 4: Protect your Servers and your Active Directory partitions

This module covers how to mitigate security risks for sensitive servers such as Domain Controllers, Active Directory Certificate Services (ADCS), Admin Workstations and check security settings on Active Directory Partitions. You will see security features that can be implemented to reduce the attack surface.

Day 3

Module 5: Remediation Plan and Monitoring

A lab will put attendees in a real scenario where they have to implement remediation to mitigate security issues in Active Directory using provided and freely available tools. This module focuses on how to setup a plan for detecting abnormal activities in Active Directory using a list of tools and methods.

Module 6: Security and Identity Protection for the Modern World

This module provides information about security mechanisms in Windows Azure Active Directory (AAD), security threats with Bring Your Own Device (BYOD) and covers new security features provided by Windows 10 such as Next Generation Credentials.

Microsoft