Microsoft Security Workshop: Managing Identity (40552)

- **Formato do curso:** Presencial
- **Preço:** 490€
- **Duração:** 7 horas

This 1-day Instructor-led security workshop provides discussion and practical hands-on training for Managing Identity. You will learn about some generic principles of identity management as one of the primary lines of defense against internal and external cyberattacks.

The workshop covers the most common attacks against Active Directory and countermeasures reducing the attack surface. It also contains recommendations for recovery in the event of a complete compromise. You will explore in more details the functionality of Active Directory, focusing in particular on Kerberos-based authentication, including the Windows components that play the essential role in the authentication process. The workshop covers the underlying technology which will help you with identifying the most effective approach to protecting your Active Directory environment. In addition, the workshop provides an overview of Privileged Access Management, which sample implementation is the subject of the lab of this course. The workshop will also provide an overview of Azure Active Directory (Azure AD) and illustrates how to leverage its capabilities in order to enhance identity protection and to consolidate identity management in hybrid scenarios.

This workshop is part of a larger series of Workshops offered by Microsoft on the practice of Security. While it is not required that you have completed any of the other courses in the Security Workshop series before taking this workshop, it is highly recommended that you start with the first course in the series, Microsoft Security Workshop: Enterprise Security Fundamentals.

Destinatários

This course is intended for IT Professionals that require a deeper understanding of Windows Security that wish to increase their knowledge level through a predominately hands-on experience with Active Directory DS & Azure Active Directory.

Pré-requisitos

This workshop is part of a larger series of Workshops offered by Microsoft on the practice of Security. While it is not required that you have completed any of the other courses in the Security Workshop series before taking this workshop, it is highly recommended that you start with the first course in the series, Microsoft Security Workshop: Enterprise Security Fundamentals.

This workshop requires that you meet the following prerequisites:

- Students who take this training should already have the following technical knowledge:

    - Experience with Windows Client administration, maintenance, and troubleshooting.
    - Basic experience and understanding of Windows networking technologies, to include Windows Firewall network setting, DNS, DHCP, WiFi, and cloud services concepts.
    - Basic experience and understanding of Active Directory, including functions of a domain controller, sign on services, and an understanding of group policy.
    - Knowledge of and relevant experience in systems administration, using Windows Server 2012 R2 and 2016.
- Learners who take this training can meet the prerequisites by obtaining equivalent knowledge and skills through practical experience as a Security Administrator, System Administrator, or a Network Administrator.
- Windows PowerShell will be the tool of choice when implementing features in this course. Learners should have a good foundation in accessing and using simple Windows PowerShell commands.

Objectivos

After completing this workshop, students will be able to:

- Explain the concept of Identity as the control plane
- Describe the principles of Secure Privileged Access (SPA)
- Explain the basic characteristics of AD DS
- Describe primary methods of protecting AD DS
- Describe features of Azure AD editions
- Describe core Microsoft cloud security features
- Provide an overview of MIM
- Explain the benefits of JIT administration and PAM

Programa

Managing Identity

In recent years, the range of features provided by identity solutions has been evolving in a dramatic pace in order to address continuously increasing levels of cyber threats. While facilitating authentication and authorization remain to be part of the core functionality of these solutions, modern identity management places additional emphasis on security and form one of the primary lines of defense against internal and external cyberattacks. In this module, you will learn about some generic principles of identity management that clearly demonstrate that focus.

Lessons

- Identity Management, the new Control Plane
- Securing Privileged Access (SPA)

After completing this module, students will be able to:

- Explain the concept of Identity as a control plane
- Describe the basic characteristics of Identity Management.
- Explain the premise of Securing Privileged Access (SPA)
- Identify three stages of the SPA roadmap.

Securing Active Directory

Most IT security breaches start with the compromise of a single computer. Once these entry points are compromised, the scope of the breach can expand in a rapid pace. Most commonly, exploits leverage existing vulnerabilities that have been overlooked or neglected. By identifying and eliminating the vulnerabilities that hackers leverage to propagate their exploits, organizations can minimize the impact of an initial compromise and impede lateral movement across the entire infrastructure. This approach play significant role in protecting the ultimate goal of most attacks – Active Directory domain controllers, which, once compromised, provide complete control of the organization's Active Directory Domain Services (AD DS) forests. This module presents the most common attacks against Active Directory and countermeasures reducing the attack surface. It also contains recommendations for recovery in the event of a complete compromise.

Lessons

- Introduction to Active Directory Domain Services (AD DS)
- Protecting AD DS

After completing this module, students will be able to:

- Identify primary reasons for using up-to-date operating system and antimalware software
- Recommend approach to fixing misconfigured infrastructure components
- Describe factors that contribute to reducing attack surface of Active Directory
- Advise the proper approach to auditing and monitoring Active Directory
- Explain the premise of planning for compromise
- List the best practices for maintaining a more secure environment.

Active Directory and Privileged Access Management

This module explores in more details the functionality of Active Directory, focusing in particular on Kerberos-based authentication, including the Windows components that play the essential role in the authentication process. Understanding the underlying technology will help you with identifying the most effective approach to protecting your Active Directory environment. In addition, the module provides an overview of Privileged Access Management, which sample implementation is the subject of the lab of this course.

Lessons

- Authentication and authorization in Active Directory Domain Services (AD DS)
- Privileged Access Management

After completing this module, you will be able to:

- Describe Kerberos-based authentication and authorization
- Explain the architecture and the role of Security Support Provider Interface

- Describe the sign on sequence for domain joined clients
- Identify user logon steps
- Provide characteristics of local and domain logons
- Provide characteristics of smart card logons
- Provide characteristics of biometrics logons
- Describe ESEA characteristics
- Provide an overview of MIM
- Explain the benefits of JIT administration and PAM

Azure Active Directory

This module provides an overview of Azure Active Directory (Azure AD) and illustrates how to leverage its capabilities in order to enhance identity protection and to consolidate identity management in hybrid scenarios.**Lessons**

- Introduction to Azure AD
- Microsoft cloud security components

Lab : AD Privileged Access Management (PAM) and Just In Time Administration (JIT)

- Implement PAM infrastructure
- Implement and verify functionality of PAM users, groups, and roles

After completing this module, students will be able to:

- Describe features of Azure AD editions
- List the benefits of Azure AD Identity Protection
- Describe core Microsoft cloud security features
- Explain the primary characteristics of SSO
- Explain the SSO mechanism when authenticating to cloud-based applications
- Explain the SSO mechanism when authenticating to on-premises applications
- Describe the features of Azure MFA
- Provide use cases for Azure Key Vault
- Describe the principles of RBAC
- Describe the role and components of Azure AD Connect
- Choose an Azure AD integration option most suitable in a given scenario.

Additional Reading

This workshop is part of a larger series of Workshops offered by Microsoft on the practice of Security. While it is not required that you have completed any of the other courses in the Security Workshop series before taking this workshop, it is highly recommended that you start with the first course in the series, Microsoft Security Workshop: Enterprise Security Fundamentals.