Microsoft

Windows Server 2012 R2 – Securing Windows Server

Workshop*PLUS*

Target Audience:

To ensure the high-quality knowledge-transfer expected by attendees of this 4-day workshop, class size is limited to a maximum of 16 students who meet the following criteria:

- System architects and engineers responsible for security design, implementation and management.
- Windows Server (2003, 2008 or 2012) administrators with a solid understanding of network operations and management.

Overview

The Securing Windows Server 4-day WorkshopPLUS course provides students with the skills required to ensure that host servers are secure and protected from unwanted access or intrusion. This workshop covers security threats, countermeasures, and Windows Server 2012 R2 strategies, tools, and best practices for comprehensively securing servers from the file system, applications, and server communications across a network. The workshop also focuses on the use of the security-rich features of Windows Server 2012 R2 to help detect and defend against security threats that target your most valuable organizational assets.

The workshop contains Level 200+ content that covers people and process as well technical security topics. So, while it covers technical concepts it is a balance between process and technology that results in Defense in Depth. In this workshop, we outline common security risks to each layer of Security in the Defense in Depth Model, and discuss mitigations for those risks.

Please review the target-audience information and contact your Microsoft Services representative to ensure that this workshop is appropriate to the student's experience and technical expertise.

Technical Highlights

After completing this course, you will be able to:

- Understand typical security threats and the most effective Windows Server countermeasures against them.
- Protect a server against unauthorized access during and after the login and authentication processes.
- Secure a host against risks from unnecessary software and from non-secure settings.
- Properly secure applications using appropriate Windows Server 2012 R2 tools and techniques.

Syllabus

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

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

Module 1: Principles of Security, Risk Management and Defense in Depth: This module covers the high level principles of information security, including Risk Management, to ensure that students are grounded in the terms and approach. This module also discusses the use of Policies as the first layer of security.

Module 2: Physical Layer Security: This module introduces physical security considerations for Windows Server. This module discusses common threats and mitigations for physical security risks including UEFI and SecureBoot technologies.

Module 3: Perimeter Security and Windows Server: This module discusses common roles for Windows Server in the network perimeter, including Web Servers. The module also discusses common security threats and mitigations for perimeter risks.

Module 4: Network Layer Security: This module discusses common uses for Windows Server 2012 R2 to protect network communications and lightly discusses Active Directory considerations including Secure Organization Unit (OU) design and utilizing Group Policy Objects (GPO) to implement security. We also discuss Windows Firewall with Advanced Security, authentication protocols, passwords and IPsec.

Module 5: Host Security: This module covers current host security threats, and new security features of Windows Sever 2012 R2. *Pass the Hash* attacks and its mitigations are a big topic here. We also discuss managing Service Accounts and security auditing. Furthermore, we explore baseline configuration tools including Best Practice Analyzer (BPA), Security Compliance Manager (SCM) and the Security Configuration Wizard (SCW).

Module 6: Application Layer Security: This module details hardening Active Directory Domain Services (ADDS), Active Directory Certificate Services and Remote Desktop Services. We also discuss Enhanced Mitigation Experience Toolkit (EMET), AppLocker and security related group policy settings.

Module 7: Data Layer Security: This module will outline how to manage data risks from the Server technologies. The module will discuss Bitlocker as a tool to manage data security.

Microsoft