MWS3-5 - MOC 20744 - SECURING WINDOWS SERVER 2016

Categoria: **Windows Server 2016**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
5 Giorni	Windows Server 2016	Microsoft Certified Trainer	Professionista IT	Microsoft

OBIETTIVI

Mettere in sicurezza Windows Server.
Sviluppare applicazioni sicure e un'infrastruttura per il bilanciamento del carico.

Gestire le baseline della sicurezza.

Configurare e gestire l'amministrazione just-enough e just-in-time (JIT).

Gestire la sicurezza dei dati.

Configurare Windows Firewall e un firewall distribuito software-defined.

Mettere in sicurezza il traffico di rete.

Mettere in sicurezza l'infrastruttura di virtualizzazione.

Gestire il malware e le minacce software.

Configurare il controllo avanzato della sicurezza.

Gestire gli aggiornamenti del software.

Gestire le minacce utilizzando Advanced Threat Analytics (ATA) e Microsoft Operations Management Suite (OMS).

PREREQUISITI

Aver completato i seguenti corsi 740, 741, e 742, o avere conoscenze equivalenti.
Avere una solida comprensione e un'esperienza pratica dei fondamenti di rete inclusi: TCP / IP, User Datagram Protocol (UDP) e Domain Name System (DNS).
Avere un'esperienza pratica dei Servizi di dominio (AD DS) e dei principi di Active Directory.
Avere un'esperienza pratica dei fondamenti di virtualizzazione Microsoft Hyper-V.
Comprendere i principi di sicurezza di Windows Server.

CONTENUTI

Module 1: Breach detection and using the Sysinternals tools
Overview of breach detection
Using the Sysinternals tools to detect breaches

Lab : Basic breach detection and incident response strategies
Identifying attack types
Using incident-response strategies
Exploring the Sysinternals tools
After completing this course, students will be able to:
Describe breach detection.
Describe how to detect a breach by using the Sysinternals tools.

Module 2: Protecting credentials and privileged access
Understanding user rights
Computer and service accounts
Protecting credentials
Understanding privileged-access workstations and jump servers
Deploying a local administrator-password solution

Lab : User rights, security options, and group-managed service accounts
Configuring security options
Configuring restricted groups
Delegating privileges
Creating and managing group managed service accounts (MSAs)
Configuring the Credential Guard feature
Locating problematic accounts

Lab : Configuring and deploying LAPs
Installing local administrator password solution (LAPs)
Configuring LAPs
Deploying LAPs
After completing this module, students will be able to:
Understand user rights.
Describe computer and service accounts.
Help protect credentials.
Understand privileged-access workstations and jump servers.
Understand how to use a local administrator-password solution.

Module 3: Limiting administrator rights with Just Enough Administration
Understanding JEA
Configuring and deploying JEA

Lab : Limiting administrator privileges by using JEA
Creating a role-capability file
Creating a session-configuration file
Creating a JEA endpoint
Connecting to a JEA endpoint
Deploying JEA by using Desire State Configuration (DSC)
After completing this module, students will be able to:
Understand JEA.
Configure and deploy JEA.

Module 4: Privileged Access Management and administrative forests

Understanding ESAE forests
Overview of MIM
Implementing JIT and Privileged Access Management by using MIM

Lab : Limiting administrator privileges by using Privileged Access Management
Using a layered approach to security
Exploring MIM
Configuring a MIM web portal
Configuring the Privileged Access feature
Requesting privileged access
After completing this module, students will be able to:
Understand enhanced security administrative environment forests.
Understand MIM.
Understand how to implement JIT and Privileged Access Management by using MIM.

Module 5: Mitigating malware and threats
Configuring and managing Windows Defender
Using software restricting policies (SRPs) and AppLocker
Configuring and using Device Guard
Using and deploying the Enhanced Mitigation Experience Toolkit

Lab : Securing applications by using AppLocker, Windows Defender, Device Guard Rules, and the EMET.
Configuring Windows Defender
Configuring AppLocker
Configuring and deploying Device Guard
Deploying and using EMET
After completing this module, students will be able to:
Configure and manage Windows Defender.
Use Software Restricting Policies and AppLocker.
Configure and use Device Guard.
Use and deploy the EMET.

Module 6: Analysing activity by using advanced auditing and log analytics
Overview of auditing
Understanding advanced auditing
Configuring Windows PowerShell auditing and logging

Lab : Configuring encryption and advanced auditing
Configuring auditing of file-system access
Auditing domain logons
Managing the configuration of advanced audit policies
Windows PowerShell logging and auditing
After completing this module, students will be able to:
Understanding auditing.
Understand advanced auditing.
Audit and log Windows PowerShell.

Module 7: Analysing activity with Microsoft Advanced Threat Analytics feature and Operations Management Suite
Overview of Advanced Threat Analytics
Understanding OMS

Lab : Advanced Threat Analytics and Operations Management Suite
Using ATA and OMS

Preparing and deploying ATA
Preparing and deploying OMS
After completing this module, students will be able to:
Understand Advanced Threat Analytics.
Understand OMS.

Module 8: Securing your virtualization an infrastructure
Overview of Guarded Fabric VMs
Understanding shielded and encryption-supported VMs

Lab : Deploying and using Guarded Fabric with administrator-trusted attestation and shielded VMs
Deploying Guarded Fabric VMs with administrator-trusted attestation
Deploying a shielded VM
After completing this module, students will be able to:
Understand Guarded Fabric VMs.
Understand shielded and encryption-supported VMs.

Module 9: Securing application development and server-workload infrastructure
Using Security Compliance Manager
Introduction to Nano Server
Understanding containers

Lab : Using Security Compliance Manager
Configuring a security baseline for Windows Server 2016
Deploying a security baseline for Windows Server 2016

Lab : Deploying and Configuring Nano Server and containers
Deploying, managing, and securing Nano Server
Deploying, managing, and securing Windows Server containers
Deploying, managing, and securing Hyper-V containers
After completing this module, students will be able to:
Understand Security Compliance Manager.
Describe Nano Server.
Understand containers.

Module 10: Protecting data with encryption
Planning and implementing encryption
Planning and implementing BitLocker

Lab : Configuring EFS and BitLocker
Encrypting and recovering access to encrypted files
Using BitLocker to protect data
After completing this module, students will be able to:

Plan and implement encryption.

Plan and implement BitLocker.

Module 11: Limiting access to file and folders
Introduction to FSRM
Implementing classification management and file-management tasks
Understanding Dynamic Access Control (DAC)

Lab : Configuring quotas and file screening
Configuring FSRM quotas
Configuring file screening

Lab : Implementing DAC
Preparing DAC
Implementing DAC
After completing this module, students will be able to:
Understand FSRM.
Implement classification management and file-management tasks.
Understand DAC.

Module 12: Using firewalls to control network traffic flow
Understanding Windows Firewall
Software-defined distributed firewalls

Lab : Windows Firewall with Advanced Security
Creating and testing inbound rules
Creating and testing outbound rules
After completing this module, students will be able to:
Describe Windows Firewall.
Understand software-defined distributed firewalls.

Module 13: Securing network traffic
Network-related security threats and connection-security rules
Configuring advanced DNS settings
Examining network traffic with Microsoft Message Analyzer
Securing SMB traffic, and analysing SMB traffic

Lab : Connection security rules and securing DNS
Creating and testing connection security rules
Configuring and testing DNSSEC

Lab : Microsoft Message Analyzer and SMB encryption
Using Microsoft Message Analyzer
Configuring and verifying SMB encryption on SMB shares
After completing this module, students will be able to:
Understand network-related security threats and connection security rules.
Configure advanced DNS settings.
Examine network traffic with Microsoft Message Analyzer.
Secure SMB traffic, and analyze SMB traffic.

Module 14: Updating Windows Server
Overview of WSUS
Deploying updates by using WSUS

Lab : Implementing update management
Implementing the WSUS server role
Configuring update settings
Approving and deploying an update by using WSUS
Deploying Windows Defender definition updates by using WSUS
After completing this module, students will be able to:
Understand WSUS.

Deploy updates with WSUS.

INFO

Materiale didattico: Materiale didattico in formato digitale
Costo materiale didattico: incluso nel prezzo del corso a Calendario
Natura del corso: Operativo (previsti lab su PC)