20744 Securing Windows Server 2016

This course teaches IT professionals how they can enhance the security of the IT infrastructure that they administer.

Length Days: 5

TARGET AUDIENCE

This course is for IT professionals who need to administer Windows Server 2016 networks securely. These professionals typically work with networks that are configured as Windows Server domain-based environments, with managed access to the Internet and cloud services.

Students who seek certification in the 70-744 Securing Windows server exam also will benefit from this course.

COURSE OBJECTIVES

After completing this course, students will be able to:

- Secure Windows Server.
- Secure application development and a server workload infrastructure.
- Manage security baselines.
- Configure and manage just enough and just-in-time (JIT) administration.
- Manage data security.
- Configure Windows Firewall and a software-defined distributed firewall.
- Secure network traffic.
- Secure your virtualization infrastructure.
- Manage malware and threats.
- Configure advanced auditing.
- Manage software updates.
- Manage threats by using Advanced Threat Analytics (ATA) and Microsoft Operations Management Suite (OMS).

COURSE OUTLINE

1 - ATTACKS, BREACH DETECTION, AND SYSINTERNALS TOOLS

- Understanding attacks
- Detecting breaches
- Examining activity with the Sysinternals tool
- Lab : Basic breach detection and incident response strategies

2 - PROTECTING CREDENTIALS AND PRIVILEGED ACCESS

- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Privileged-Access Workstations and jump servers
- Local administrator-password solution
- Lab : User rights, security options, and group-managed service accounts
- Lab : Configuring and deploying LAPs

3 - LIMITING ADMINISTRATOR RIGHTS WITH JUST ENOUGH ADMINISTRATION

- Understanding JEA
- Verifying and deploying JEA
- Lab : Limiting administrator privileges by using JEA

4 - PRIVILEGED ACCESS MANAGEMENT AND ADMINISTRATIVE FORESTS

- ESAE forests
- Overview of Microsoft Identity Manager
- Overview of JIT administration and PAM
- Lab : Limiting administrator privileges with PAM

5 - MITIGATING MALWARE AND THREATS

- Configuring and managing Windows Defender
- Restricting software
- Configuring and using the Device Guard feature
- Deploying and using the EMET
- Lab : Securing applications by using AppLocker, Windows Defender, Device Guard Rules, and the EMET.

6 - ANALYZING ACTIVITY WITH ADVANCED AUDITING AND LOG ANALYTICS

- Overview of auditing
- Advanced auditing
- Windows PowerShell auditing and logging
- Lab : Configuring advanced auditing

7 - DEPLOYING AND CONFIGURING ADVANCED THREAT ANALYTICS AND MICROSOFT OPERATIONS MANAGEMENT SUITE

- Deploying and configuring ATA
- Deploying and configuring Microsoft Operations Management Suite
- Lab : Deploying ATA and Microsoft Operations Management Suite

8 - SECURE VIRTUALIZATION INFRASTRUCTURE

- Guarded Fabric
- Shielded and encryption-supported virtual machines
- Lab : Guarded Fabric with administrator-trusted attestation and shielded VMs

9 - SECURING APPLICATION DEVELOPMENT AND SERVER-WORKLOAD INFRASTRUCTURE

- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Lab : Using Security Compliance Manager
- Lab: Deploying and Configuring Nano Server

10 - PLANNING AND PROTECTING DATA

- Planning and implementing encryption
- Planning and implementing BitLocker
- Lab : Protecting data by using encryption and BitLocker

11 - OPTIMIZING AND SECURING FILE SERVICES

- File Server Resource Manager
- Implementing classification management and file-management tasks
- Dynamic Access Control
- Lab : Quotas and file screening
- Lab : Implementing Dynamic Access Control

12 - SECURING NETWORK TRAFFIC WITH FIREWALLS AND ENCRYPTION

- Understanding network-related security threats
- Understanding Windows Firewall with Advanced Security
- Configuring IPsec
- Datacenter Firewall
- Lab : Configuring Windows Firewall with Advanced Security

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 analyzing SMB traffic
- Lab : Securing DNS
- Lab : Microsoft Message Analyzer and SMB encryption

14 - UPDATING WINDOWS SERVER

- Overview of WSUS
- Deploying updates by using WSUS
- Lab : Implementing update management