20744 Securing Windows Server 2016

COURSE OVERVIEW

This course teaches IT professionals how they can enhance the security of the IT infrastructure that they administer. This course begins by emphasizing the importance of assuming that network breaches have occurred already, and then teaches you how to protect administrative credentials and rights to help ensure that administrators can perform only the tasks that they need to, when they need to. This course explains how you can use auditing and the Advanced Threat Analysis feature in Windows Server 2016 to identify security issues. You will also learn how to mitigate malware threats, secure your virtualization platform, and use deployment options such as Nano server and containers to enhance security. The course also explains how you can help protect access to files by using encryption and dynamic access control, and how you can enhance your network's security.

DURATION

5 Days

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.

OBJECTIVE

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).

20744 Securing Windows Server 2016

COURSE OUTLINE

MODULE 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

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

MODULE 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 : Implementing user rights, security options, and group-managed service accounts user rights, security options, and group-managed service accounts

Lab : Configuring and deploying LAPs

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

Lab : Configuring and deploying LAPs

20744 Securing Windows Server 2016

MODULE 3	**LIMITING ADMINISTRATOR RIGHTS WITH JUST ENOUGH ADMINISTRATION** • *Understanding JEA* • *Configuring and deploying JEA* **Lab : Limiting administrator privileges by using JEA**
MODULE 3	**LIMITING ADMINISTRATOR RIGHTS WITH JUST ENOUGH ADMINISTRATION** • *Understanding JEA* • *Verifying and deploying JEA* **Lab : Limiting administrator privileges by using JEA**
MODULE 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**
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**

20744 Securing Windows Server 2016

MODULE 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**
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.**
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**
MODULE 6	**ANALYSING ACTIVITY BY USING ADVANCED AUDITING AND LOG ANALYTICS** • *Overview of auditing* • *Advanced auditing* • *Windows PowerShell auditing and logging* **Lab : Configuring advanced auditing**
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**

20744 Securing Windows Server 2016

MODULE 7	**ANALYSING ACTIVITY WITH MICROSOFT ADVANCED THREAT ANALYTICS FEATURE AND OPERATIONS MANAGEMENT SUITE** • *Deploying and configuring ATA* • *Deploying and configuring Microsoft Operations Management Suite* **Lab : Deploying ATA and Microsoft Operations Management Suite**
MODULE 8	**SECURE VIRTUALIZATION INFRASTRUCTURE** • *Guarded Fabric* • *Shielded and encryption-supported virtual machines* **Lab : Guarded Fabric with administrator-trusted attestation and shielded VMs**
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**
MODULE 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 and containers**
MODULE 10	**PLANNING AND PROTECTING DATA** • *Planning and implementing encryption* • *Planning and implementing BitLocker* **Lab : Protecting data by using encryption and BitLocker**

20744 Securing Windows Server 2016

MODULE 10	**PROTECTING DATA WITH ENCRYPTION** • *Planning and implementing encryption* • *Planning and implementing BitLocker* **Lab : Configuring EFS and 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** **Lab : Implementing DAC**
MODULE 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**
MODULE 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**
MODULE 12	**USING FIREWALLS TO CONTROL NETWORK TRAFFIC FLOW** • *Understanding Windows Firewall* • *Software-defined distributed firewalls* **Lab : Windows Firewall with Advanced Security**

20744 Securing Windows Server 2016

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 analyzing SMB traffic* **Lab : Connection security rules and securing DNS** **Lab : Microsoft Message Analyzer and SMB encryption**
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 analyzing SMB traffic* **Lab : Securing DNS** **Lab : Microsoft Message Analyzer and SMB encryption**
MODULE 14	**UPDATING WINDOWS SERVER** • *Overview of WSUS* • *Deploying updates by using WSUS* **Lab : Implementing update management**