ProTech protechtraining.com *"Charting the Course ...*

... to Your Success!"

MOC 20744 C: Securing Windows Server 2016

Course Summary

Description

This five-day, instructor-led 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.

Objectives

After taking this course, students will be able to:

- Secure Windows Server.
- Protect credentials and implement privileged access workstations.
- Limit administrator rights with Just Enough Administration.
- Manage privileged access.
- Mitigate malware and threats.
- Analyze activity with advanced auditing and log analytics.
- Deploy and configure Advanced Threat Analytics and Microsoft Operations Management Suite.
- Configure Guarded Fabric virtual machines (VMs).
- Use the Security Compliance Toolkit (SCT) and containers to improve security.
- Plan and protect data.
- Optimize and secure file services.
- Secure network traffic with firewalls and encryption.
- Secure network traffic by using DNSSEC and Message Analyzer.

Topics

- Attacks, breach detection, and Sysinternals tools
- Protecting credentials and privileged access
- Limiting administrator rights with Just Enough Administration
- Privileged access management and administrative forests
- Mitigating malware and threats
- Analyzing activity with advanced auditing and log analytics
- Deploying and configuring Advanced Threat Analytics and Microsoft Operations Management Suite
- Secure Virtualization Infrastructure
- Securing application development and server-workload infrastructure
- Planning and protecting data
- Optimizing and securing file services
- Securing network traffic with firewalls and encryption
- Securing network traffic

MOC 20744 C: Securing Windows Server 2016

Course Summary (cont'd)

Audience

This course was designed for IT professionals who want to know how they can enhance the security of the IT infrastructure that they administer.

Prerequisites

Before taking this course, students should have at least two years of experience in the IT field and should have:

- Completed courses MOC 20740 (PT10601), MOC 20741 (PT10602), and MOC 20742 (PT10603), or the equivalent.
- A solid, practical understanding of networking fundamentals, including TCP/IP, User Datagram Protocol (UDP), and Domain Name System (DNS).
- A solid, practical understanding of Active Directory Domain Services (AD DS) principles.
- A solid, practical understanding of Microsoft Hyper-V virtualization fundamentals.
- An understanding of Windows Server security principles.

Duration

Five days

ProTech protechtraining.com *"Charting the Course ... ... to Your Success!"*

MOC 20744 C: Securing Windows Server 2016

Course Outline

I. Attacks, breach detection, and Sysinternals tools

This module frames the course so that students are thinking about security in environments where the infrastructure's basis is predominantly Microsoft products. The module begins with teaching students about the "assume breach" philosophy and getting them to understand the different types of attacks that can occur, including attack timelines and vectors. Additionally, it gets students thinking about key resources, how they respond when they detect an incident, and how an organization's direct needs and legislative requirements dictate its security policy.

A. Understanding attacks
B. Detecting security breaches
C. Examining activity with the Sysinternals tools

Lab: Basic breach detection and incident response strategies

- Identifying attack types
- Exploring Sysinternals tools

II. Protecting credentials and privileged access

This module covers user accounts and rights, computer and service accounts, credentials, Privileged Access Workstations, and the Local Administrator Password Solution. In this module, students will learn about configuring user rights and security options, protecting credentials by using Credential Guard, implementing Privileged Access Workstations, and managing and deploying Local Administrator Password Solution to manage local administrator account passwords.

A. Understanding user rights
B. Computer and service accounts
C. Protecting credentials
D. Privileged Access Workstations and jump servers
E. Local administrator password solution

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

- Configuring user rights and account-security options
- Delegating privileges
- Creating group Managed Service Accounts
- Locating problematic accounts

Lab: Configuring and deploying LAPs

- Installing and configuring LAPs
- Deploying and testing LAPs

III. Limiting administrator rights with Just Enough Administration

This module explains how to deploy and configure Just Enough Administration (JEA), which is an administrative technology that allows students to apply role-based access control (RBAC) principles through Windows PowerShell remote sessions.

A. Understanding JEA
B. Verifying and deploying JEA

Lab: Limiting administrator privileges with JEA

- Creating a role-capability file
- Creating a session-configuration file
- Creating a JEA endpoint
- Connecting and testing a JEA endpoint
- Deploying a JEA configuration to another computer

IV. Privileged access management and administrative forests

This module explains the concepts of Enhanced Security Administrative Environment (ESAE) forests, Microsoft Identity Manager (MIM), and Just In Time (JIT) Administration, or Privileged Access Management (PAM).

A. ESAE forests
B. Overview of Microsoft Identity Manager
C. Overview of JIT administration and PAM

Lab: Limiting administrator privileges with PAM

- Layered approach to security
- Configuring trust relationships and shadow principals
- Requesting privileged access
- Managing PAM roles

V. Mitigating malware and threats

This module explains how to use tools such as Windows Defender, Windows AppLocker, Microsoft Device Guard, Windows Defender Application Guard, and Windows Defender Exploit Guard.

A. Configuring and managing Windows Defender
B. Restricting software
C. Configuring and using the Device Guard feature

MOC 20744 C: Securing Windows Server 2016

Course Outline (cont'd)

Lab: Securing applications with Windows Defender, AppLocker, and Device Guard Rules

- Configuring Windows Defender
- Configuring AppLocker
- Configuring Device Guard

VI. Analyzing activity with advanced auditing and log analytics

This module provides an overview of auditing, and then goes into detail about how to configure advanced auditing and Windows PowerShell auditing and logging.

A. Overview of auditing
B. Advanced auditing
C. Windows PowerShell auditing and logging

Lab: Configuring advanced auditing

- Configuring the auditing of file system access
- Auditing domain sign-ins
- Managing advanced audit policy configuration
- Windows PowerShell logging and auditing

VII. Deploying and configuring Advanced Threat Analytics and Microsoft Operations Management Suite

This module explains the Microsoft Advanced Threat Analytics tool and the Microsoft Operations Management suite (OMS). It also explains how you can use them to monitor and analyse the security of a Windows Server deployment. You will also learn about Microsoft Azure Security Center, which allows you to manage and monitor the security configuration of workloads both on-premises and in the cloud.

A. Deploying and configuring ATA
B. Deploying and configuring Microsoft Operations Management Suite
C. Deploying and configuring Azure Security Center

Lab: Deploying ATA, Microsoft Operations Management Suite, and Azure Security Center

- Preparing and deploying ATA
- Preparing and deploying Microsoft Operations Management Suite
- Deploying and configuring Azure Security Center

VIII. Secure Virtualization Infrastructure

This module explains how to configure Guarded Fabric VMs, including the requirements for shielded and encryption-supported VMs.

A. Guarded fabric
B. Shielded and encryption-supported virtual machines

Lab: Guarded fabric with Admin-trusted attestation and shielded VMs

- Deploying a guarded fabric with admin-trusted attestation
- Deploying a shielded VM

IX. Securing application development and server-workload infrastructure

This module describes the SCT, which is a free, downloadable set of tools that you can use to create and apply security settings. You will also learn about improving platform security by reducing the size and scope of application and compute resources by containerizing workloads.

A. Using SCT
B. Understanding containers

Lab: Using SCT

- Configuring a security baseline for Windows Server 2016
- Deploying the security baseline for Windows Server 2016

Lab: Deploying and configuring containers

- Deploying and managing a Windows container

X. Planning and protecting data

This module explains how to configure Encrypting File System (EFS) and BitLocker drive encryption to protect data at rest. You will also learn about extending protection into the cloud by using Azure Information Protection.

A. Planning and implementing encryption
B. Planning and implementing BitLocker
C. Protecting data by using Azure Information Protection

Lab: Protecting data by using encryption and BitLocker

- Encrypting and recovering access to encrypted files
- Using BitLocker to protect data

MOC 20744 C: Securing Windows Server 2016

Course Outline (cont'd)

XI. Optimizing and securing file services

This module explains how to optimize file services by configuring File Server Resource Manager (FSRM) and Distributed File System (DFS). Students also will learn how to manage access to shared files by configuring Dynamic Access Control (DAC).

A. File Server Resource Manager
B. Implementing classification and file management tasks
C. Dynamic Access Control

Lab: Quotas and file screening

- Configuring File Server Resource Manager quotas
- Configuring file screening and storage reports

Lab: Implementing Dynamic Access Control

- Preparing for implementing Dynamic Access Control
- Implementing Dynamic Access Control
- Validating and remediating Dynamic Access Control

XII. Securing network traffic with firewalls and encryption

This module explains how you can use Windows Firewall as an important part of an organization's protection strategy. It explains the use of Internet Protocol security (IPsec) to encrypt network traffic and to establish security zones on your network. You will also learn about the Datacenter Firewall feature that you can use to help protect your on-premises virtual environments.

A. Understanding network-related security threats
B. Understanding Windows Firewall with Advanced Security
C. Configuring IPsec
D. Datacenter Firewall

Lab: Configuring Windows Firewall with Advanced Security

- Creating and testing inbound rules
- Creating and testing outbound rules
- Creating and testing connection security rules

XIII. Securing network traffic

This module explores some of the Windows Server 2016 technologies that you can use to help mitigate network-security threats. It explains how you can configure DNSSEC to help protect network traffic, and use Microsoft Message Analyzer to monitor network traffic. The module also describes how to secure Server Message Block (SMB) traffic.

A. Configuring advanced DNS settings
B. Examining network traffic with Message Analyzer
C. Securing and analyzing SMB traffic

Lab: Securing DNS

- Configuring and testing DNSSEC
- Configuring DNS policies and RRL

Lab: Microsoft Message Analyzer and SMB encryption

- Installing and using the Message Analyzer
- Configuring and verifying SMB encryption on SMB shares