

COURSE 20744: SECURING WINDOWS SERVER

Duration: 5 Days

Delivery Method: Instructor-led Classroom / Virtual Classroom

ABOUT THIS COURSE:

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.

AUDIENCE PROFILE:

This course is for IT professionals who need to securely administer Windows Server 2016 networks. 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 OUTLINE:

Here is the complete course outline.

Module 1: 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.

<p>LESSONS</p> <ul style="list-style-type: none"> Understanding attacks Detecting security breaches Examining activity with the Sysinternals tools 	<p>LAB : Basic breach detection and incident response strategies</p> <ul style="list-style-type: none"> Identifying attack types Exploring Sysinternals tools
--	--

Module 2: 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.

<p>LESSONS</p> <ul style="list-style-type: none"> Understanding user rights Computer and service accounts Protecting credentials Privileged Access Workstations and jump servers Local administrator password solution 	<p>LAB : Implementing user rights, security options, and group managed service accounts</p> <ul style="list-style-type: none"> Configuring user rights and account-security options Delegating privileges Creating group Managed Service Accounts Locating problematic accounts <p>LAB : Configuring and deploying LAPs</p> <ul style="list-style-type: none"> Installing and configuring LAPs Deploying and testing LAPs
--	---

Module 3: 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.

LESSONS

- Understanding JEA
- 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

Module 4: 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).

LESSONS

- ESAE forests
- Overview of Microsoft Identity Manager
- 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

Module 5: 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.

<p>LESSONS</p> <ul style="list-style-type: none"> Configuring and managing Windows Defender Restricting software Configuring and using the Device Guard feature 	<p>LAB : Securing applications with Windows Defender, AppLocker, and Device Guard Rules</p> <ul style="list-style-type: none"> Configuring Windows Defender Configuring AppLocker Configuring Device Guard
---	--

Module 6: 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.

<p>LESSONS</p> <ul style="list-style-type: none"> Overview of auditing Advanced auditing Windows PowerShell auditing and logging 	<p>LAB : Configuring advanced auditing</p> <ul style="list-style-type: none"> Configuring the auditing of file system access Auditing domain sign-ins Managing advanced audit policy configuration Windows PowerShell logging and auditing
--	---

Module 7: 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.

<p>LESSONS</p> <p>Deploying and configuring ATA</p> <p>Deploying and configuring Microsoft Operations Management Suite</p> <p>Deploying and configuring Azure Security Center</p>	<p>LAB : Deploying ATA, Microsoft Operations Management Suite, and Azure Security Center</p> <p>Preparing and deploying ATA</p> <p>Preparing and deploying Microsoft Operations Management Suite</p> <p>Deploying and configuring Azure Security Center</p>
--	--

Module 8: Secure Virtualization Infrastructure

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

<p>LESSONS</p> <p>Guarded fabric</p> <p>Shielded and encryption-supported virtual machines</p>	<p>LAB : Guarded fabric with Admin-trusted attestation and shielded VMs</p> <p>Deploying a guarded fabric with admin-trusted attestation</p> <p>Deploying a shielded VM</p>
---	--

Module 9: 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.

<p>LESSONS</p> <p>Using SCT</p> <p>Understanding containers</p>	<p>LAB : Using SCT</p> <p>Configuring a security baseline for Windows Server 2016</p> <p>Deploying the security baseline for Windows Server 2016</p> <p>Lab : Deploying and configuring containers</p> <p>Deploying and managing a Windows container</p>
--	--

Module 10: 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.

<p>LESSONS</p> <p>Planning and implementing encryption</p> <p>Planning and implementing BitLocker</p> <p>Protecting data by using Azure Information Protection</p>	<p>LAB : Protecting data by using encryption and BitLocker</p> <p>Encrypting and recovering access to encrypted files</p> <p>Using BitLocker to protect data</p>
---	---

Module 11: 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).

LESSONS

- File Server Resource Manager
- Implementing classification and file management tasks
- 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

Module 12: 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.

LESSONS

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

Module 13: 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.

LESSONS

Configuring advanced DNS settings

Examining network traffic with Message Analyzer

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

**FOR MORE INFORMATION ABOUT OUR TRAINING COURSES,
CALL US AT 03-6234-3883
OR VISIT OUR WEBSITE AT www.Quill.com.au**