70-744: Securing Windows Server 2016

Course Overview

This course provides students with the knowledge and skills to secure Windows Server 2016. Students will be introduced to attacks, breaches, and detection, and learn about protecting users and workstations, managing administrative access, configuring anti-malware and patch management, auditing and advanced threat analytics, securing the infrastructure, configuring data protection, advanced file server management, and securing the network infrastructure.

Course Introduction 5m

Course Introduction

Chapter 01 - Introduction to Attacks, Breaches, and Detection 1h 11m

Topic A: Understanding Types of Attacks
Assume Breach
Methods of Attack
Attack Stages
Prioritizing Resources
Incident Response Strategy
Ensuring Compliance
Topic B: Detecting Security Breaches
Locating Evidence
Event Logs
Examining Other Configurations
Topic C: Using Sysinternals Tools
Introducing Sysinternals
Demo - Examining Sysinternals Tools
System Monitor
AccessChk
Autoruns
LogonSessions
Process Explorer
Process Monitor
Sigcheck
Demo - Using Sysinternals Tools
Chapter 01 Review

Chapter 02 - Protecting Users and Workstations 2h 22m

Topic A: User Rights and Privileges
Principle of Least Privilege
Configuring User Rights
Configuring Account Security Options
Demo - User Rights and Account Security Options

Account Security Controls
Complexity Options
Password and Lockout Policies
Demo - Configuring Account Policies in Group Policy
Configuring Fine-Grained Password Policies
Understanding PSO Application
Protected Users Security Groups
Delegating Administrative Control
Demo - Delegating Control in AD DS
Local Administrator Password Solutions (LAPS)
LAPS Requirements
LAPS Process
Configuring and Managing Passwords
Demo - Using LAPS
Topic B: Working with Computer and Service Accounts
What is a Computer Account?
Computer Account Functionality
Working with Secure Channel Passwords
Service Account Types
Group MSAs
Demo - Configuring Group MSAs
Topic C: Protecting User Credentials
Introducing Credential Guard
Credential Guard Requirements
Configuring Credential Guard
Verifying Credential Guard Operation
Credential Guard Weaknesses
NTLM Blocking
Searching AD DS for Problem Accounts
Demo - Locating Problem Accounts
Topic D: Using Privileged Access Workstations
The Need for Privileged Access Workstations
Privileged Access Workstations
Jump Servers
Securing Domain Controllers
Chapter 02 Review

Chapter 03 - Managing Administrative Access 1h 12m
Topic A: Understanding and Deploying JEA
Introduction to JEA
JEA Components
Session Configuration Files
Demo - Creating a Session Configuration File
Role Capability Files
Demo - Create a Role Capability File
JEA Endpoints
Demo - Creating a JEA Endpoint
Connecting to JEA Endpoints
Deploying JEA Endpoints

Topic B: Using Enhanced Security Administrative Environments (ESAE) Forests
ESAE Forests
Administrative Tiers
ESAE Best Practices
The Clean Source Principle
Implementing the Clean Source Principle
Topic C: Using Microsoft Identity Manager
Overview of MIM
MIM Requirements
MIM Service Accounts
Topic D: Using JIT Administration and PAM
Overview of JIT Administration
Privileged Access Management (PAM)
PAM Components
Creating an Administrative Forest
Configuring Trust Relationships
Shadow Principals
Configuring the MIM Web Portal
Managing and Configuring PAM Roles
Chapter 03 Review

<u>Chapter 04 - Configuring Anti-Malware and Patch Management</u> 1h 31m
Topic A: Configuring and Managing Windows Defender
Understanding Malware
Malware Sources
Mitigation Methods
Windows Defender
Demo - Using Windows Defender
Topic B: Restricting Software
Controlling Applications
Software Restriction Policies
Security Levels
AppLocker
Support for AppLocker
AppLocker Rules
Creating Default Rules
Demo - Using AppLocker
Topic C: Using Device Guard
Overview of Device Guard
Device Guard Features
Configuring Device Guard
Device Guard Policies
Deploying Code Integrity Policies
Control Flow Guard
Topic D: Patch Management with WSUS
Overview of WSUS
Deployment Options
Server Requirements
Configuring Clients

Administering WSUS
Approving Updates
Demo - Installing and Configuring WSUS
Chapter 04 Review

Chapter 05 - Auditing and Advanced Threat Analytics 1h 28m

Topic A: Configuring Auditing for Windows Server 2016
Overview of Auditing
The Purpose of Auditing
Types of Events
Auditing Goals
Auditing File and Object Access
Demo - Configuring Auditing
Topic B: Advanced Auditing and Management
Advanced Auditing
Advanced Auditing Subcategories
Dynamic Auditing
Event Log Subscriptions
Audit Collection Services (ACS)
Demo - Configuring Event Forwarding
Auditing with Windows PowerShell
Demo - Using PowerShell with Audit Logs
Transaction Logging
Module Logging
Script Block Logging
Demo - Configuring PowerShell Logging
Topic C: Deploying and Configuring ATA
Overview of ATA
Usage Scenarios
Deployment Requirements
ATA Gateways
Port Mirroring
Configuring ATA Center
Topic D: Deploying and Configuring Operations Management Suite
Introduction to Operations Management Suite
Deployment Overview
OMS Solutions
Installing OMS
OMS Solutions
Chapter 05 Review

Chapter 06 - Securing the Infrastructure 44m

Topic A: Secure the Virtualization Infrastructure
Introduction to Guarded Fabric
Host Guardian Service
Preparing HGS Nodes
Installing and Configuring HGS
Attestation and Encryption
Attestation Methods

Initializing HGS
Configuring HGS Clients
Topic B: Deploying Security Baselines
Security Compliance Manager (SCM)
SCM Requirements
Demo - Installing SCM
Demo - Configuring and Deploying Security Baselines
Topic C: Deploying Nano Server
Planning for Nano Server
Understanding Nano Server Roles
Installing Nano Server Roles
Nano Server Installation
Installation Steps
Chapter 06 Review

Chapter 07 - Configuring Data Protection 1h 4m
Topic A: Planning and Implementing File Encryption
Introducing Encrypting File System
EFS Features
Encryption and Decryption
Recovering EFS Files
Demo - Using EFS
Topic B: Planning and Implementing BitLocker
Overview of BitLocker
BitLocker and TPMs
BitLocker Requirements
Tools for Configuring and Managing BitLocker
Deploying BitLocker
Demo - Deploying BitLocker
BitLocker on Hyper-V VMs
BitLocker and CSVs
Enabling BitLocker for CSV
Network Unlock
Network Unlock Process
BitLocker Recovery
Microsoft BitLocker Administration and Monitoring (MBAM)
Chapter 07 Review

Chapter 08 - Advanced File Server Management 1h 55m
Topic A: Using File Server Resource Manager
Capacity Management
Storage Management
Introduction to FSRM
Storage Management with File Server Resource Manager
Overview of FSRM
Installing and Configuring FSRM
Demo - Installing and Configuring FSRM
Quota Management
Demo - Create and Manage Quotas

File Screening
Using File Groups
Exceptions and Templates
Demo - Implementing File Screening
Storage Reports
Report Tasks
Demo - Generating Storage Reports
Automatic File Management
Topic B: Implementing Classification and File Management Tasks
File Classification
Classification Rules
Demo - Configure File Classification
File Management Tasks
Topic C: Working with Dynamic Access Control
Overview of Dynamic Access Control
Dynamic Access Control Scenarios
DAC Technologies
Understanding Identity
Understanding Claims
Types of Claims
Central Access Policies
Policy Components
DAC Prerequisites
Demo - Implementing DAC
Chapter 08 Review

Chapter 09 - Securing the Network Infrastructure 2h 14m

Topic A: Using the Windows Firewall with Advanced Security
Types of Firewalls
Well-Known Ports
Host-Based Firewall
Network Profiles
Configuring the Windows Firewall
Demo - Working with the Windows Firewall
Topic B: Datacenter Firewall
Network Controller
Datacenter Firewall
Network Security Groups
Scenarios for Datacenter Firewall
Topic C: Utilizing IP Security
Overview of IP Security
IPSec Protocols
IPSec Usage Scenarios
IPSec Configuration Tools
Connection Security Rules
Understanding Rule Types
Rule Endpoints
Authentication Settings
Authentication Methods

Encryption Settings
Monitoring Connections
Demo - Implementing IPSec
Topic D: Configuring Advanced DNS Settings
Managing DNS Services
Optimizing DNS Name Resolution
The GlobalNames Zone
Implementing DNS Security
DNS Security (DNSSEC)
Implementing DNSSEC
Demo - Configuring DNSSEC
Introducing DNS Policies
Implementing DNS Policies
RRL Feature
Demo - Configuring DNS Policies
Topic E: Monitoring Network Traffic
Microsoft Message Analyzer
Demo - Using Microsoft Message Analyzer
Topic F: Securing SMB Traffic
SMB 3.1.1 Protocol Security
SMB Encryption Requirements
Encrypting SMB Shares
Disabling Support for SMB 1.0
Chapter 09 Review
Course Closure

Total Duration: 13h 46m