Silver Microsoft Partner

20744: Securing Windows Server 2016

Course Details

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**
    1. Identifying attack types
    2. Exploring the Sysinternals tools
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**
    1. Configuring security options
    2. Configuring restricted groups
    3. Delegating privileges
    4. Creating and managing group managed service accounts (MSAs)
    5. Configuring the Credential Guard feature
    6. Locating problematic accounts
    - **Lab : Configuring and deploying LAPs**
    7. Installing and configuring LAPs
    8. Deploying and testing LAPs
3. **Limiting administrator rights with Just Enough Administration**
    - Understanding JEA
    - Verifying and deploying JEA
    - **Lab : Limiting administrator privileges with JEA**

1. Creating a role-capability file
2. Creating a session-configuration file
3. Creating a JEA endpoint
4. Connecting and testing a JEA endpoint
5. Deploying a JEA configuration to another computer

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**

1. Layered approach to security
2. Configuring trust relationships and shadow principals
3. Requesting privileged access
4. Managing PAM roles

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.**

1. Configuring Windows Defender
2. Configuring AppLocker
3. Configuring Device Guard
4. Deploying and using EMET

6. Analyzing activity with advanced auditing and log analytics

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

1. Configuring auditing of file-system access
2. Auditing domain sign-ins
3. Managing advanced audit policy configuration
4. Windows PowerShell logging and 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**
    1. Preparing and deploying ATA
    2. Preparing and deploying 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**
    1. Deploying a guarded fabric with administrator-trusted attestation
    2. Deploying a shielded VM
9. **Securing application development and server-workload infrastructure**
    - Using SCM
    - Introduction to Nano Server
    - Understanding containers
    - **Lab : Using SCM**
    1. Configuring a security baseline for Windows Server 2016
    2. Deploying a security baseline for Windows Server 2016
    - **Lab : Deploying and Configuring Nano Server**
    3. Deploying, managing, and securing Nano Server
    4. Deploying, managing, and securing Windows container
10. **Planning and protecting data**
    - Planning and implementing encryption
    - Planning and implementing BitLocker
    - **Lab : Protecting data by using encryption and BitLocker**
    1. Encrypting and recovering access to encrypted files
    2. Using BitLocker to protect data
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**

1. Configuring File Server Resource Manager quotas
2. Configuring file screening and storage reports
   - **Lab : Implementing Dynamic Access Control**
3. Preparing for implementing Dynamic Access Control
4. Implementing Dynamic Access Control
5. Validating and remediating 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**

1. Creating and testing inbound rules
2. Creating and testing outbound rules
3. Creating and testing connection security rules

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 analysing SMB traffic
  - **Lab : Securing DNS**

1. Configuring and testing DNSSEC
2. Configuring DNS policies and RRL
   - **Lab : Microsoft Message Analyzer and SMB encryption**
3. Installing and using Message Analyzer
4. Configuring and verifying SMB encryption on SMB shares

14. Updating Windows Server

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

1. Implementing the WSUS server role
2. Configuring update settings
3. Approving and deploying an update by using WSUS