MTA Security Fundamentals Course

Session 1

Section A: Introduction

- Security Fundamentals
- Microsoft Certification Paths
- Knowledge Domains
- Taking the Exam
- Exam Prep Tips

Section B: Security Principles

- Windows Server Editions
- AAA
- Least Privilege
- Attack Surface
- Defense-in-Depth

Section C: Threats and Risks

- Threats and Risks Defined
- Personal Risk Assessment
- Internal Threats
- External Threats
- Types of Attackers
- Common Attack Methods
- Social Engineering
- Attack Phases

Section D: Authentication Fundamentals

- Authentication
- Credential Types
- Weak Authentication
- Examples of Weak Authentication
- Strong Authentication
- RADIUS Servers
- User Directories

Section E: Windows/PKI Authentication

- Windows Authentication Methods
- Kerberos Authentication
- Public Key Cryptography
- Certificates
- Public Key Infrastructure

Section F: Password Policies

- Password Policy Options
- Password Hashes
- Account Lockout Policies
- runas Option

- Resetting the User Password

Section G: User/Group Management

- Creating New User Accounts
- New User Password
- Settings/Considerations
- Managing User Account Security
- Creating New Groups
- Managing Group Memberships

Session 2

Section A: Permission Management

- Windows Permissions
- Delegating Administration Rights
- File System Permissions
- Understanding Offline Files
- Configuring NTFS Basic Permissions
- Configuring NTFS Advanced Permissions
- Overriding Inheritance Permissions
- Configuring Share Permissions
- Configuring Resource Ownership
- Understanding Permissions Inheritance

Section B: Auditing

- Auditing Defined
- Security Audit Events Spreadsheet
- Enabling Auditing in Group Policy Editor
- Configuring Advanced Auditing Policies

Section C: Physical Security Solutions

- Importance of Physical Security
- Physical Security Defined
- Physical Security Applications
- Physical Security Checklist
- Restricting Device Installation with GP
- Restricting Local Logon using GPE
- Understanding Keyloggers

Section D: Malware Protection

- Viruses Defined
- Worms Defined
- Types of Viruses
- Indications of Viral Infection
- Virus Phases
- Trojan Horses Defined
- Common Trojan Horse Programs
- Buffer Overflows Defined

Section E: Internet Explorer Security

- Internet Explorer General Options
- IT Security Zones
- Secure Web Sites
- InPrivate Filtering
- InPrivate Browsing

Section F: Encryption Basics

- Cryptography
- Simple Encryption
- Cryptography Concepts
- Uses of Cryptography
- Encryption Types
- Symmetric Encryption
- Asymmetric Encryption
- Public Key Cryptography
- PKI Applications

Section G: Windows Encryption Technologies

- Windows Encrypting File System
- EFS Benefits
- EFS Inheritance
- BitLocker Drive Encryption

Session 3

Section A: Network Perimeter Security

- Firewalls
- Network Firewalls
- Packet Filtering Firewalls
- Stateful Inspection Firewall
- Personal Firewalls
- Hardware/Software
- UTM/SCM

Section B: Network Segmentation

- Network Isolation
- VLANs
- VLAN Example
- VLAN Tagging
- Trunk Example
- Virtual Private Network
- VPN Protocols
- Perimeter Networks
- Perimeter Network Example
- NAT/Perimeter Networks
- Planning Perimeter Networks
- Honeypots
- Server/Domain Isolation

Section C: NAP

- Network Access Protection

- NAP Requirements
- NAP Implementation Methods
- NAP Architecture

Section D: Network Protocol Security

- Network Protocols
- Network Scanning
- Scanning Types
- Sniffers
- ARP Spoofing

Section E: Wireless Network Security

- Wi-Fi Vulnerabilities
- Wi-Fi Security
- Wired Equivalent Privacy
- WPA/WPA2
- 802.11i Security
- 802.1X
- 802.1X Demo
- 802.1X Deployment

Section F: Client Protection

- User Account Control Settings
- UAC Local Policies
- Run Users as Administrators
- Windows Updates
- Restriction/Control Policies

Section G: Server Protection

- Microsoft Baseline Security Analyzer
- MBSA Results
- Services
- Security Updating DNS
- NTLM

Section H: E-mail Protection

- E-mail Vulnerabilities
- E-mail Hygiene
- Protection Methods
- Junk E-mail Filtering