About This Exam Review Kit

Microsoft Technology Associate Certification Exam Review Kit: 98-367 Security Fundamentals

Exam Review Kit Description

- This Microsoft® Technology Associate (MTA) Certification Exam Review Kit is a series of 20 review lessons intended to reinforce concepts in preparation for the *MTA Certification Exam: 98-367 Security Fundamentals* and/or serve as a resource and guide for teachers and faculty to create their own additional student learning experiences.
- It is assumed that students taking an MTA certification exam have completed and/or are currently taking academic courses and/or job experiences that address the exam objective domain.
- The MTA Exam Review Kits:
    - Are intended to supplement (not supplant) existing academic courses.
    - Are not intended to serve as foundational content for academic courses.
    - Are directly and closely tied to the objective domain of each individual MTA exam.
    - Are platform-specific or -agnostic in accord with the objective domain of each MTA exam.
- Because each certification exam has approximately 20 objectives, this MTA Exam Review Kit includes twenty 50-minute review lessons.
- The build of materials for each review lesson includes a lesson plan, lesson delivery materials, and student activity documents.
- MTA exams test breadth of technical knowledge and help students explore career options before choosing a specialized career path with minimal investment of time and money. MTA certifications measure and validate the fundamental technology skills that are in demand today and provide an essential foundation to build a career in technology. Earning MTA certification provides students with a credential that validates fundamental technology industry knowledge and motivates them to succeed in continued studies, compete on admissions, and prepare for a career in technology. The MTA certifications enable students to prove their commitment to technology and connect with a community of more than five million Microsoft Certified Professionals (MCPs).
- Teachers and faculty can easily integrate the new MTA certification exams into existing schedules and curricula, and deliver exams right in the classroom, on their own schedules.

Audience

- This Exam Review Kit is intended for students age 15–24 years who have an interest in technology and technology careers and are preparing for the *MTA Certification Exam: 98-367 Security Fundamentals*, and seeking to prove introductory knowledge of and skills with security concepts and technologies.

- It is recommended that exam candidates be familiar with the concepts of and have hands-on experience with the technologies described here either by taking relevant training courses or by working with tutorials and samples available on MSDN®. Although minimal hands-on experience with the technologies is recommended, job experience is not assumed for these exams.
- Candidates for this exam are in the process of expanding their knowledge and skills in the following areas:
    - Windows Server®
    - Windows®-based networking
    - Active Directory®
    - Anti-malware products
    - Firewalls
    - Network topologies and devices
    - Network ports

Student Prerequisites

This course requires that you meet the following prerequisites:

- It is assumed that students taking an MTA certification exam have completed and/or are currently taking academic courses and/or have job experiences that address the exam objective domain.
- It is expected that students have had experience with Windows Server and security technologies.

Exam Review Kit Objective Domain

This Exam Review Kit provides lessons that reinforce previous learning in the following objectives:

1. Understanding Security Layers

1.1. Understand core security principles.

This objective may include but is not limited to: confidentiality; integrity; availability; how threat and risk impact principles; principle of least privilege; social engineering; attack surface.

1.2. Understand physical security.

This objective may include but is not limited to: site security; computer security; removable devices and drives; access control; mobile device security; disable Log On Locally; keyloggers.

1.3. Understand Internet security.

This objective may include but is not limited to: browser settings; zones; secure websites.

1.4. Understand wireless security.

This objective may include but is not limited to: advantages and disadvantages of specific security types; keys; SSID; MAC filters.

2. Understanding Operating System Security

2.1. Understand user authentication.

This objective may include but is not limited to: multifactor; smart cards; RADIUS; Public Key Infrastructure (PKI); understand the certificate chain; biometrics; Kerberos and time skew; using Run As to perform administrative tasks; password reset procedures.

2.2. Understand permissions.

This objective may include but is not limited to: file; share; registry; Active Directory; NTFS vs. FAT; enabling or disabling inheritance; behavior when moving or copying files within the same disk or onto another disk; multiple groups with different permissions; basic permissions and advanced permissions; take ownership; delegation.

2.3. Understand password policies.

This objective may include but is not limited to: password complexity; account lockout; password length; password history; time between password changes; enforce by using group policies; common attack methods.

2.4. Understand audit policies.

This objective may include but is not limited to: types of auditing; what can be audited; enabling auditing; what to audit for specific purposes; where to save audit information; how to secure audit information.

2.5. Understand encryption.

This objective may include but is not limited to: EFS; how EFS-encrypted folders impact moving and copying files; BitLocker® (To Go); Trusted Platform Module (TPM); software-based encryption; MAIL encryption and signing and other uses; VPN; public key and private key; encryption algorithms; certificate properties; certificate services; PKI/certificate services infrastructure; token devices.

2.6. Understand malware.

This objective may include but is not limited to: buffer overflows; worms; Trojans; spyware.

3. Understanding Network Security

3.1. Understand dedicated firewalls.

This objective may include but is not limited to: types of firewalls and their characteristics; when to use a hardware firewall instead of a software firewall; stateful vs. stateless inspection.

3.2. Understand Network Access Protection (NAP).

This objective may include but is not limited to: purpose of NAP; requirements for NAP.

3.3. Understand network isolation.

This objective may include but is not limited to: VLAN; routing; honeypot; perimeter networks; NAT; VPN; IPsec; Server and Domain Isolation.

3.4. Understand protocol security.

This objective may include but is not limited to: protocol spoofing; IPsec; tunneling; DNSsec; network sniffing; common attack methods.

4. Understanding Security Software

4.1. Understand client protection.
This objective may include but is not limited to: anti-virus; User Account Control (UAC); keeping client operating system and software updated; encrypting offline folders; software restriction policies.

4.2. Understand e-mail protection.
This objective may include but is not limited to: anti-spam; anti-virus; spoofing, phishing, and pharming; client vs. server protection; SPF records; PTR records.

4.3. Understand server protection.
This objective may include but is not limited to: separation of services; hardening; keeping server operating system and software updated; secure dynamic DNS updates; disabling unsecure authentication protocols; Read-Only Domain Controllers; separate management VLAN; Microsoft Baseline Security Analyzer (MBSA).

Review Kit Timing

Each of the 20 Review Lessons in this collection is intended to be used in a single 50-minute class period.

Review Kit Materials

The following materials are included in this Exam Review Kit:

- Review lessons: A plan for teacher and student activities in reviewing the learning objectives and providing the key points that are critical to the success of the in-class review experience.
- Microsoft PowerPoint® presentations: A structure for classroom lectures and discussions.
- Student activities: A hands-on platform for applying the knowledge and skills reviewed in the lesson.
- Student activity answer keys: solutions to student activities.
- Additional resources: Various resources to expand the reviewing and learning opportunities.

Software Requirements

The following software is suggested for this series of review lessons:

- Windows XP or Windows 7
- Windows Server 2008

Instructional Preparation Activities

It is highly recommended that you complete the following instructional preparation activities:

- Familiarize yourself with the objectives of each lesson.
- Walk through each Exam Review Lesson presentation slide deck and read the corresponding Instructor Notes (located in the notes view of the presentation slide deck) for the lesson. *Note that additional hidden slides are used in each slide deck to accommodate the amount of Instructor Notes information for a given topic.*

- Familiarize yourself with the student activity.
- Practice presenting each module.
- Identify the key points and must-know information for each topic.
- Perform each demonstration and hands-on lab.
- Anticipate the questions that students might have.
- Identify examples, analogies, impromptu demonstrations, and additional delivery tips that will help to clarify module content and provide a more meaningful learning experience for your specific audience.
- Customize and enhance your instructor notes.
- Review the updated information about the Microsoft Certification Program on the Microsoft Learning Certifications website (*http://www.microsoft.com/learning/en/us/certification/cert-default.aspx*).