Экзамен 98-367 “Security Fundamentals”

Вопросы экзамена охватывают темы, включенные в этот список, но не ограничиваются ими.

Сведения об уровнях безопасности (25—30%)

- Сведения об основных принципах безопасности
  - Конфиденциальность; целостность; доступность; влияние угроз и рисков на принципы; принцип предоставления наименьших привилегий; социотехника; анализ направления атаки; моделирование угроз
- Сведения о физической безопасности
  - Безопасность сайта; безопасность компьютера; съемные устройства и диски; управление доступом; безопасность мобильных устройств; клавиатурные шпионы
- Сведения об интернет-безопасности
  - Параметры безопасности браузера; безопасные веб-сайты
- Сведения о безопасности в беспроводной сети
  - Преимущества и недостатки определенных типов безопасности; ключи; идентификаторы SSID; фильтры MAC-адресов

Ресурсы для подготовки

- Windows Server 2008 in an organization's defense in depth strategy
- Secure Windows Server
- Using Windows Server 2008: Controlling communication with the Internet

Сведения о безопасности операционной системы (35–40 %)

- Сведения о проверке подлинности пользователя
  - Многофакторная проверка подлинности; физические и виртуальные смарт-карты; протокол RADIUS (Remote Authentication Dial-In User Service); процедуры биометрии; использование команды "Запуск от имени другого пользователя" для выполнения административных задач
- Сведения о разрешениях
  - Разрешения файловой системы; разрешения на обмен; реестр; Active Directory; включение или отключение наследования; поведение при перемещении или копирование файлов на тот же или на другой диск; несколько групп с разными разрешениями; базовые и расширенные разрешения; смена владельца; делегирование; наследование
- Сведения о политиках паролей
  - Сложность пароля; блокировка учетных записей; длина пароля; история паролей; время между сменами паролей; принудительное использование с помощью групповых политик; распространенные способы атак; процедуры сброса пароля; защита пароля пользователя доменной учетной записи
- Сведения о политиках аудита
  - Типы аудита; что подлежит аудиту; включение аудита; что подлежит аудиту для конкретных целей; где сохранять информацию аудита; как обеспечить безопасность для информации аудита
- Сведения о шифровании
  - Шифрование файловой системы (EFS); как влияют папки с шифрованием EFS на перемещение/копирование файлов; BitLocker (To Go); TPM; шифрование на основе программного обеспечения; шифрование MAIL, регистрация в сети и другие использования; виртуальные частные сети (VPN); открытые/закрытые ключи; алгоритмы шифрования; свойства сертификатов; службы сертификации; инфраструктура PKI/служб сертификации; устройства-маркеры; настройка устройства на запуск только доверенных приложений
- Сведения о вредоносных программах
  - Переполнение буфера; вирусы, полиформфные вирусы; черви; трояны; шпионские программы; программы, требующие выкупа; рекламные программы; руткиты; пути обхода системы защиты; атака нулевого дня

Ресурсы для подготовки

- Windows authentication
- Password policy
- Audit policies

Microsoft

Learn – Practice – Certify

Сведения о сетевой безопасности (20—25%)

- Сведения о выделенных брандмауэрах
  - Типы аппаратных брандмауэров и их характеристики; когда следует использовать аппаратный брандмауэр вместо программного; проверка с отслеживанием и без отслеживания состояния брандмауэра; менеджер соответствия требованиям безопасности; базовые показатели безопасности
- Сведения о сетевой изоляции
  - Маршрутизация; система-ловушка для хакеров (honeypot); сети периметра; преобразование сетевых адресов (NAT); VPN; IPsec; изоляция сервера и домена
- Сведения о безопасности протоколов
  - Спуфинг протоколов; IPsec; туннелирование; DNSsec; сканирование сети; атаки с отказом от обслуживания (DoS); распространенные способы атак

Ресурсы для подготовки

- Windows Firewall
- Network Access Protection
- IPsec

Сведения о программном обеспечении безопасности (15—20%)

- Сведения о защите клиентов
  - Защита от вирусов; защита от установки нежелательного программного обеспечения; контроль учетных записей (UAC); поддержка обновлений операционной системы и программного обеспечения клиента; шифрование автономных папок, политики ограничения для приложений; принцип предоставления наименьших привилегий
- Сведения о защите эл. почты
  - Защита от спама, защита от вирусов, спуфинг, фишинг и фарминг; сравнение защиты клиента и сервера; записи инфраструктуры политики отправителей (SPF); записи PTR
- Сведения о защите сервера
  - Разделение служб; усиление защиты; поддержка обновлений сервера; безопасные динамические обновления службы доменных имен (DNS); отключение небезопасных протоколов проверки подлинности; контроллеры доменов только для чтения (RODC)

Ресурсы для подготовки

- What's new for operating system hardening and integrity for Windows Server 2008
- Software restriction policies
- What's new for server protection in Windows Server 2008

Learn – Practice – Certify

Варианты подготовки

Обучение под руководством инструктора

- 40032A: Networking and Security Fundamentals: Training two-pack for MTA Exams 98-366 and 98-367 (five days)

  Этот пятидневный учебный курс помогает подготовиться к экзаменам MTA 98-366 и 98-367, а также понять принципы работы сетевых инфраструктур, сетевого оборудования, протоколов и служб, уровней безопасности, безопасности операционной системы, сетевой безопасности и программного обеспечения безопасности. В этих курсах использованы те же материалы, которые приведены в Microsoft Official Academic Courses (MOAC) для этих экзаменов.

- 40367A: Security Fundamentals: MTA Exam 98-367 (three days)

  Этот трехдневный учебный курс по программе MTA помогает подготовиться к экзамену 98-367 по программе MTA, а также понять, что такое уровни безопасности, безопасность операционной системы, сетевая безопасность и программные модули безопасности. В этом курсе использованы те же материалы, которые приведены в MOAC для этого экзамена.

Практический тест

Take a Microsoft Official Practice Test for Exam 98-367

От сообщества

Find out how to advance your career in technology

Кто сдает этот экзамен?

На этом экзамене проверяются базовые знания и навыки кандидата в области безопасности. Он может послужить в качестве этапа подготовки к экзаменам на присвоение квалификации Microsoft Certified Solutions Associate (MCSA). Кандидатам рекомендуется изучить указанные ниже понятия и технологии на соответствующих учебных курсах. Экзамен рассчитан на кандидатов, имеющих практический опыт работы с Windows Server, сетями Windows, Active Directory, продуктами для защиты от вредоносных программ, брандмауэрами, сетевыми топологиями и устройствами, а также с сетевыми портами.

Microsoft

Learn – Practice – Certify

Дополнительные сведения об экзаменах

Настоящее руководство по подготовке может быть изменено в любой момент без предварительного уведомления исключительно по усмотрению корпорации Microsoft. Экзамены Microsoft могут содержать элементы адаптивного и имитационного тестирования. Корпорация Microsoft не определяет формат, в котором представлены экзамены. В каком бы формате ни проводился экзамен, пользуйтесь этим руководством по подготовке. Для подготовки к этому экзамену корпорация Microsoft рекомендует получить опыт работы с продуктом и использовать указанные учебные ресурсы. Эти учебные ресурсы не обязательно охватывают все темы, перечисленные в разделе «Оценка навыков».