kaspersky

KL 005.11:

Защита серверов Windows и встраиваемых систем

Изучаемые продукты

- Kaspersky Security для Windows Server
- Kaspersky Embedded Systems Security

Цель курса

Этот курс готовит к внедрению, настройке и обслуживанию Kaspersky Security 11 для Windows Server в средних и крупных организациях.

Курс шаг за шагом описывает действия администратора для успешного развертывания и настройки продукта в сети предприятия. Отдельно рассматриваются специфические сценарии настройки Kaspersky Security 11 для Windows Server для решения определенных задач: защита от вирусов-шифровальщиков, внедрение концепции информационной безопасности Default Deny, защита систем хранения данных.

Лабораторные работы демонстрируют актуальные методы защиты информационной системы. Администратор управляет всей инфраструктурой удаленно со своего рабочего места. Для этого используются Консоль управления Kaspersky Security Center и Консоль управления Kaspersky Security 11 для Windows Server. Практически для каждого раздела теоретической части предусмотрена лабораторная работа, чтобы продемонстрировать возможности продукта и закрепить полученные знания на практике.

Длительность

2 дня.

Требования к участникам

Понимание основ работы с Kaspersky Security Center и Kaspersky Endpoint Security. Представление о современных угрозах, типичных этапах развития атаки и типичных процедурах по расследованию инцидентов компьютерной безопасности.

Содержание

1. Введение

1.1. Основные функции Kaspersky Security для Windows Server
1.2. Системные требования Kaspersky Security для Windows Server
1.3. Компоненты защиты Kaspersky Security для Windows Server
1.4. Компоненты управления и мониторинга Kaspersky Security для Windows Server
1.5. Лицензирование
1.6. Основные функции Kaspersky Embedded System Security
1.7. Системные требования Kaspersky Embedded System Security
1.8. Компоненты защиты Kaspersky Embedded Systems Security
1.9. Компоненты управления и мониторинга Kaspersky Embedded Systems Security
1.10. Лицензирование Kaspersky Embedded Systems Security
1.11. Варианты установки Kaspersky Embedded Systems Security

2. Внедрение

2.1. Порядок внедрения
2.2. Мастер первоначальной настройки
2.3. Список установочных пакетов
2.4. Измените настройки инсталляционного пакета (опционально)
2.5. Создайте отдельную группу для KSWS (опционально)

Лабораторная работа 1. **Подготовьте Сервер Администрирования**

2.6. Способы установки Kaspersky Security для Windows Server
2.7. Результат установки
2.8. Активация Kaspersky Security для Windows Server

Лабораторная работа 2. **Установите Kaspersky Security для Windows Server и Kaspersky Embedded Systems Security**

2.9. Установка консоли Kaspersky Security для Windows Server

Лабораторная работа 3. **Установите Консоль управления Kaspersky Security для Windows Server**

3. Настройка групповых задач

3.1. Что делать после установки Kaspersky Security для Windows Server
3.2. Задача обновления баз
3.3. Задача обновления модулей программы
3.4. Задачи проверки по требованию

Лабораторная работа 4. **Настройте обновление и проверку по требованию**

4. Защита файловой системы

Лабораторная работа 5. **Настройте постоянную защиту**
Лабораторная работа 6. **Проверьте защиту Windows Subsystem for Linux**

4.1. Защита от эксплоитов

Лабораторная работа 7. **Проверьте защиту от эксплойтов**

4.2. Защита от шифрования
4.3. Как настроить защиту от шифрования
4.4. Как настроить период блокировки недоверенного устройства

Лабораторная работа 8. **Настройте защиту папок общего доступа**
Лабораторная работа 9. **Настройте компонент Защита от шифрования**

5. Защита от сетевых угроз

5.1. Как Kaspersky Security для Windows Server защищает от сетевых атак

5.2. Как настроить защиту от сетевых угроз

Лабораторная работа 10. **Настройте защиту от сетевых угроз**

6. Защита служб Удаленного Рабочего Стола

6.1. Модель угроза для служб удаленного рабочего стола
6.2. Защита сетевого трафика: Драйверный перехват
6.3. Компоненты защиты сеансов удаленного рабочего стола
6.4. Защита сетевого трафика: Перенаправление трафика
6.5. Защита сетевого трафика: Внешний прокси

Лабораторная работа 11. **Настройте компонент Защита трафика в режиме Драйверный перехват**
Лабораторная работа 12. **Настройте компонент Защита трафика для проверки почтового трафика**
Лабораторная работа 13. **Настройте компонент Защита трафика в режиме Внешний прокси-сервер**

7. Компоненты контроля сервера

7.1. Контроль запуска программ

Лабораторная работа 14. **Включите Контроль запуска программ в режиме тестирования**
Лабораторная работа 15. **Переключите Контроль запуска программ в активный режим**
Лабораторная работа 16. **Создайте разрешающие правила для установочных пакетов и обновлений**

8. Контроль устройств

8.1. Для чего нужен Контроль устройств
8.2. Как настроить контроль устройств в Kaspersky Embedded Systems Security

9. Диагностика системы

9.1. Мониторинг файловых операций
9.2. Анализ журналов

Лабораторная работа 17. **Настройте компоненты Диагностики системы**

10. Защита систем хранения данных

10.1. Возможности защиты систем хранения данных
10.2. Постоянная защита файлов для систем хранения данных

Лабораторная работа 18. **Защитите хранилище на платформе NetApp Clustered Data ONTAP**

10.3. Защита от шифрования для NetApp

Лабораторная работа 19. **Настройте компонент Защита от шифрования для NetApp**

11. Дополнительные настройки

11.1. Защита общих ресурсов кластера
11.2. Управление сетевым экраном
11.3. Интеграция с SIEM
11.4. Управление приложением
11.5. Сбор диагностической информации
11.6. Наблюдаем за состоянием защиты (Health Check)