Бауманский учебный центр «Специалист»

Программа курса Настройка безопасности в Windows Server 2022/2019/2016

Код курса: **M20744AC**

Тема	Ак. часов
Модуль 1. Обнаружение нарушений и использование инструментов Sysinternals В этом модуле объясняется, как обнаружить нарушения, определить тип атаки и векторы вторжения киберпреступности, а также как анализировать активность системы, используя инструменты Sysinternals. **Темы** • Обзор возможностей обнаружения нарушений • Использование инструментов Sysinternals для выявления нарушений **Лабораторная работа: Основные обнаружения нарушений и стратегии реагирования на инциденты** • Выявление типов атак • Применение стратегии реагирования на инциденты • Изучение средств Sysinternals	**3**
Модуль 2. Защита учетных данных и привилегированный доступ В этом модуле объясняется, как настроить права пользователя и параметры безопасности, защитить учетные данные пользователей с помощью Охранника учетных данных (credential guard), осуществлять привилегированный доступ к рабочим станциям, управлять и разворачивать решения для управления паролем локального администратора. **Темы** • Понимание работы прав пользователя • Учетные записи компьютера и служб • Защита учетных данных • Понимание привилегированного доступа к рабочим станциям и серверам • Развертывание решения для управления паролем локального администратора **Лабораторная работа: Права пользователя, параметры безопасности и групповые управляемые сервис аккаунты** • Настройка параметров безопасности • Настройка групп с ограниченным доступом • Делегирование привилегий • Создание и управление групповых управляемых сервис аккаунтов • Настройка функций Охранника учетных данных (Credential Guard) • Обнаружение проблемных учетных записей **Лабораторная работа: Настройка и развертывание решений управления паролем локального администратора (local administrator password - LAPS)** • Установка решений управления паролем локального администратора (LAPS) • Настройка решений LAPS • Развертывание решений LAPS	**3.5**

Модуль 3. Ограничение прав администратора с помощью функции Just Enough Administration В этом модуле объясняется, как развернуть и настроить Just Enough Administration. **Темы** • Понимание Just Enough Administration • Настройка и развёртывание Just Enough Administration **Лабораторная работа: Ограничение прав администратора с помощью функции Just Enough Administration** • Создание файла с перечнем возможностей • Создание файла конфигурации сеанса • Создание точки подсоединения Just Enough Administration • Подключение к точке подсоединения Just Enough Administration • Развертывание Just Enough Administration с помощью Desire State Configuration (DSC)	**2.5**
Модуль 4. Управление привилегированным доступом и администрирование леса В этом модуле объясняются концепции расширенной административной среды безопасности (Enhanced Security Administrative Environment - ESAE) леса, Microsoft Identity Manager (MIM), функционал Just In Time (JIT) Administration и привилегированный доступ к управлению. **Темы** • Понимание расширенная административная среда безопасности леса • Обзор MIM • Реализация Just In Time (JIT) Administration и управление привилегированным доступом с помощью MIM **Лабораторная работа: Ограничение прав администратора с помощью управления привилегированным доступом** • Использование многоуровневого подхода к безопасности • Изучение MIM • Настройка веб-портала MIM • Настройка функции привилегированного доступа • Запрос привилегированного доступа	**2.5**
Модуль 5. Противодействие вредоносным программам и угрозам В этом модуле описывается настройка Защитника Windows, AppLocker и Device Guard. **Темы** • Настройка и управление Защитником Windows • Использование политик ограничения программного обеспечения (SRP) и AppLocker • Настройка и использование Device Guard • Использование и развертывание Enhanced Mitigation Experience Toolkit (EMET) **Лабораторная работа: Защита приложений с помощью AppLocker, защитника Windows, правил Device Guard и EMET** • Настройка Защитника Windows • Настройка AppLocker • Настройка и развертывание Device Guard • Развертывание и использование EMET	**2.5**

Модуль 6. Анализ активности с помощью расширенного аудита и журналов аналитики В этом модуле объясняется, как использовать расширенный аудит и отчёты Windows PowerShell. **Темы** • Обзор технологий аудита • Понимание расширенный аудит • Настройка аудита в Windows PowerShell и ведение журнала **Лабораторная работа: Настройка шифрования и расширенный аудит** • Настройка аудита доступа к файловой системе • Аудит входа в систему домена • Управление конфигурацией расширенной политики аудита • Протоколирование и аудит в Windows PowerShell	**3**
Модуль 7. Анализ активности с помощью Microsoft Advanced Threat Analytics и Operations Management Suite В этом модуле объясняется, как использовать инструменты Microsoft Advanced Threat Analytics и Microsoft Operations Management suite (OMS), как настраивать через них мониторинг и проводить анализ безопасности развертывания Windows Server. **Темы** • Обзор Advanced Threat Analytics • Понимание OMS **Лабораторная работа: Microsoft Advanced Threat Analytics и OMS** • Использование Microsoft Advanced Threat Analytics и OMS • Подготовка и развертывание Microsoft Advanced Threat Analytics • Подготовка и развертывание OMS	**2.5**
Модуль 8. Защита виртуальной инфраструктуры Этот модуль объясняет, как настроить защищённую фабрику виртуальных машин (ВМ), обеспечить требования по экранировании и поддержка шифрования ВМ. **Темы** • Обзор защищённой фабрики виртуальных машин • Понимание требований экранирования и поддержка шифрования ВМ **Лабораторная работа: Развертывание и использование защищенной фабрики с доверенной проверкой администратора и экранированием ВМ** • Развертывание защищенной фабрики ВМ с доверенной проверкой администратора • Развертывание экранированных ВМ	**3.5**

Модуль 9. Настройка безопасности при разработке приложений для серверной инфраструктуры Этот модуль объясняет, как применять диспетчер проверки на соответствие требованиям безопасности (Security Compliance Manager), как настраивать, управлять и проверять базовые планы. Также в модуле рассмотрены развертывание и настройка режима Nano Server, Microsoft Hyper-V и контейнеров Windows Server. **Темы** • Использование Security Compliance Manager • Введение в Nano Server • Понимание концепции контейнеров **Лабораторная работа: Использование Security Compliance Manager** • Настройка базового плана по безопасности для Windows Server 2016 • Развертывание базовой плана по безопасности для Windows Server 2016 **Лабораторная работа: Развертывание и настройка Nano Server и контейнеров** • Развертывание, управление и обеспечение безопасности Nano Server • Развертывание, управление и обеспечение безопасности контейнеров Windows Server • Развертывание, управление и обеспечение безопасности контейнеров Hyper-V	**5**
Модуль 10. Защита данных с помощью шифрования В этом модуле описывается настройка шифрования диска с помощью BitLocker и защита файлов с помощью шифрованной файловой системы (EFS). **Темы** • Планирование и реализация шифрования • Планирование и реализация BitLocker **Лабораторная работа: Настройка EFS и BitLocker** • Шифрование и восстановление доступа к зашифрованным файлам • Использование BitLocker для защиты данных	**3.5**
Модуль 11. Ограничение доступа к файлам и папкам Этот модуль объясняет, как оптимизировать файловые службы путем настройки диспетчера ресурсов сервера файлов (FSRM) и распределенной файловой системы (DFS). В модуле рассмотрены способы защиты данных и шифрования устройств с помощью BitLocker, а также показано, как управлять доступом к общим файлам путем настройки динамического контроля доступа (DAC). **Темы** • Введение в Диспетчер ресурсов файлового сервера • Реализация управления классификацией и задачи управления файлами • Понимание динамического контроля доступа (DAC) **Лабораторная работа: Настройка квот и блокировки файлов** • Настройка квот FSRM • Настройка блокировки файлов **Лабораторная работа: Внедрение DAC** • Подготовка DAC • Реализация DAC	**3**

Модуль 12. Использование брандмауэров для контроля сетевого трафика Этот модуль объясняет, как настроить брандмауэры, встроенные в Windows Server. **Темы** • Общие сведения о брандмауэре Windows • Распределенные программные брандмауэры **Лабораторная работа: Брандмауэр Windows в режиме повышенной безопасности** • Создание и тестирование правил входящих подключений • Создание и тестирование правил исходящих подключений	**3**
Модуль 13. Обеспечение безопасности сетевого трафика В этом модуле объясняется, как обеспечить безопасность сетевого трафика и как использовать Microsoft Message Analyzer, шифрование SMB и DNSSEC. **Темы** • Угрозы безопасности сети и правила безопасного подключения • Настройка дополнительных параметров DNS • Анализ сетевого трафика с Microsoft Message Analyzer • Обеспечение безопасности трафика SMB и анализа трафика SMB **Лабораторная работа: Правила безопасного подключения и обеспечение безопасности DNS** • Создание и тестирование правила безопасного подключения • Настройка и тестирование DNSSEC **Лабораторная работа: Шифрование SMB и Microsoft Message Analyzer** • Использование Microsoft Message Analyzer • Настройка и проверка шифрования SMB на общих папках	**2.5**
Аудиторная нагрузка в классе с преподавателем	**40 ак.ч. + 40 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru