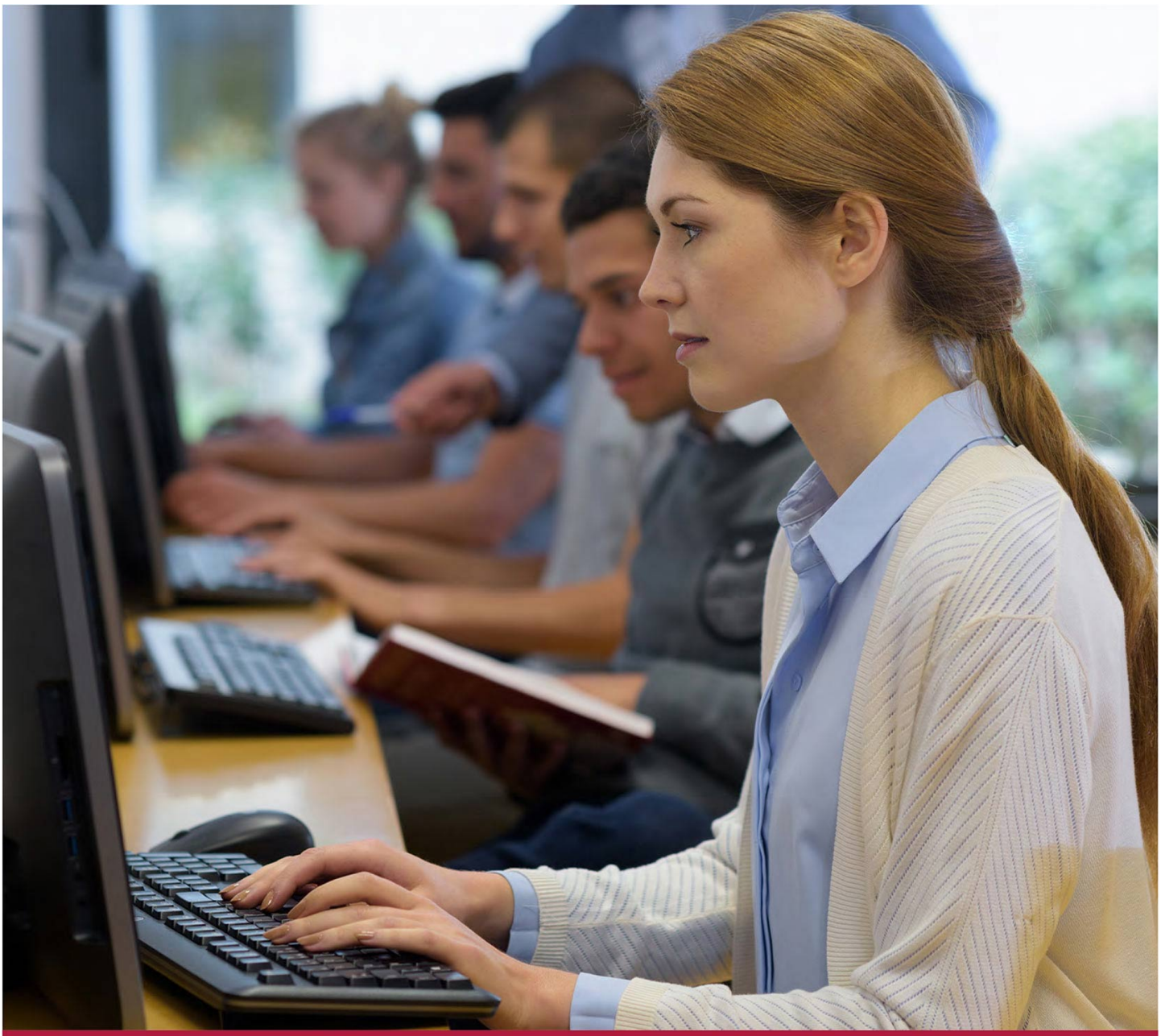
Академия АйТи
a Softline Company



Обеспечение безопасности инфраструктуры на базе ОС Linux

Код курса: LINSECURITY

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Обеспечение безопасности инфраструктуры на базе ОС Linux

Код курса: LINSECURITY

Длительность	32 ак. часа
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

В курсе освещаются актуальные вопросы обеспечения комплексной безопасности локальной и сетевой инфраструктуры, построенной на базе ОС Linux, а также рассматриваются практические аспекты безопасного конфигурирования Linux и рабочего окружения, построенного на его базе, штатные механизмы, инструменты и методики, нацеленные на защиту данных и предотвращения попыток хакерского взлома. Пройдя обучение, слушатели данного курса получат знания и практические навыки, обеспечивающие возможность безопасной настройки ОС, сетевых сервисов, web-сервера, почтового сервера, а также контроля уровня безопасности системы, своевременного обнаружения хакерских атак и осуществление превентивных мер защиты.

Подробная информация

Профиль аудитории:

- ИТ\ИБ-аудиторы, занимающиеся вопросами технического обследования и тестирования безопасности ОС Linux и рабочего окружения, построенного на его основе;
- Специалисты по информационной безопасности, сетевые инженеры, технические специалисты, отвечающие за настройку безопасных конфигураций ОС Linux и рабочего окружения;
- Системные администраторы, желающие углубить свои знания в сфере обеспечения безопасности ИТ-инфраструктуры, построенной на базе ОС Linux.

Предварительные требования:

- наличие высшего или среднего профессионального образования
- наличие базового уровня компетенции в сфере информационных технологий, TCP\IP-сетях, администрировании ОС Linux
- знание основ английского языка

По окончании курса слушатели будут:

знать:

- архитектуру, принципы построения и пользовательские интерфейсы операционных систем;
- архитектуру подсистем защиты информации в операционных системах;
- программные интерфейсы операционных систем;
- сущность и содержание понятия информационной безопасности, характеристик, ее составляющих;
- источники угроз информационной безопасности и меры по их предотвращению;
- особенности источников угроз информационной безопасности, связанных с эксплуатацией программного обеспечения;
- типичные уязвимости программного обеспечения и методы их устранения;
- характерные признаки наличия вредоносного программного обеспечения;
- виды и формы функционирования вредоносного программного обеспечения;
- типовые средства защиты информации в операционных системах;
- программно-аппаратные средства и методы защиты информации в операционных системах;
- принципы функционирования средств защиты информации в операционных системах и программном обеспечении, в том числе использующих криптографические алгоритмы.

уметь:

- устанавливать программное обеспечение в соответствии с технической документацией;
- настраивать компоненты подсистем защиты информации операционных систем;
- управлять учетными записями пользователей, в том числе генерированием, сменой и восстановлением паролей;
- применять программно-аппаратные средства защиты информации в операционных системах;
- работать в операционных системах с соблюдением действующих требований по защите информации;
- устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации;
- выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации;
- контролировать целостность подсистем защиты информации операционных систем;
- противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем;
- осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения.

владеть навыками:

- установки программно-аппаратных средств защиты информации;
- контроля за соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение;
- эксплуатации программно-аппаратных средств защиты информации в операционных системах;
- настройки программно-аппаратных средств защиты информации, в том числе средств антивирусной и криптографической защиты;
- настройки программного обеспечения с соблюдением требований по защите информации;
- настройки встроенных средств защиты информации программного обеспечения по заданным шаблонам;
- проверки функционирования встроенных средств защиты информации программного обеспечения;

- обнаружения признаков наличия вредоносного программного обеспечения;
- выполнения работ по обнаружению вредоносного программного обеспечения;
- ликвидация обнаруженного вредоносного программного обеспечения и последствий его функционирования.

Программа курса

Модуль 1. Эволюция уровней информационной безопасности

- Периметровая защита (внешний и внутренний периметры)
- Четыре периметра безопасности
- Защита в глубину/Глубинная защита (Defence in Depth)
- Роль защиты узла в обеспечении ИБ организации
- Механизмы аутентификации

Модуль 2. Дискретный контроль доступа к файлам

- Возможности классических прав доступа UNIX
- Описание классических прав доступа UNIX
- Специальные права доступа и атрибуты файлов
- Возможности POSIX ACL

Модуль 3. Linux Security Modules (LSM)

- Возможности мандатного контроля доступа
- Реализация мандатного контроля доступа средствами SELinux
- Реализация мандатного контроля доступа средствами ParSec в ASTRA Linux Special Edition
- Возможности Application Security без виртуализации
- Реализация Application Security средствами AppArmor

Модуль 4. Штатные средства усиления защиты системы

- Требования к современной политике паролей
- Локальные политики безопасности (PolicyKit)
- Механизмы, основанные на SUID и SGID (su и sudo)
- Linux capabilities (man 7 capabilities)
- Подключаемые модули аутентификации (PAM)
- Настройка параметров ядра средствами sysctl

Модуль 5. Виртуализация как инструмент защиты

- Обзор технологий виртуализации
- Виртуализация средствами KVM+QEMU
- Виртуализация средствами операционной системы на базе User Mode Linux (UML)
- Виртуализация средствами операционной системы на базе OpenVZ
- Docker-контейнеры и их возможности

Модуль 6. Дополнительные инструменты защиты

- Шифрование разделов и криптоконтейнеров
- Концепции ограниченной программной среды
- Обзор Security Patches для Linux
- Защита от эксплойтов средствами модулей ядра

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru