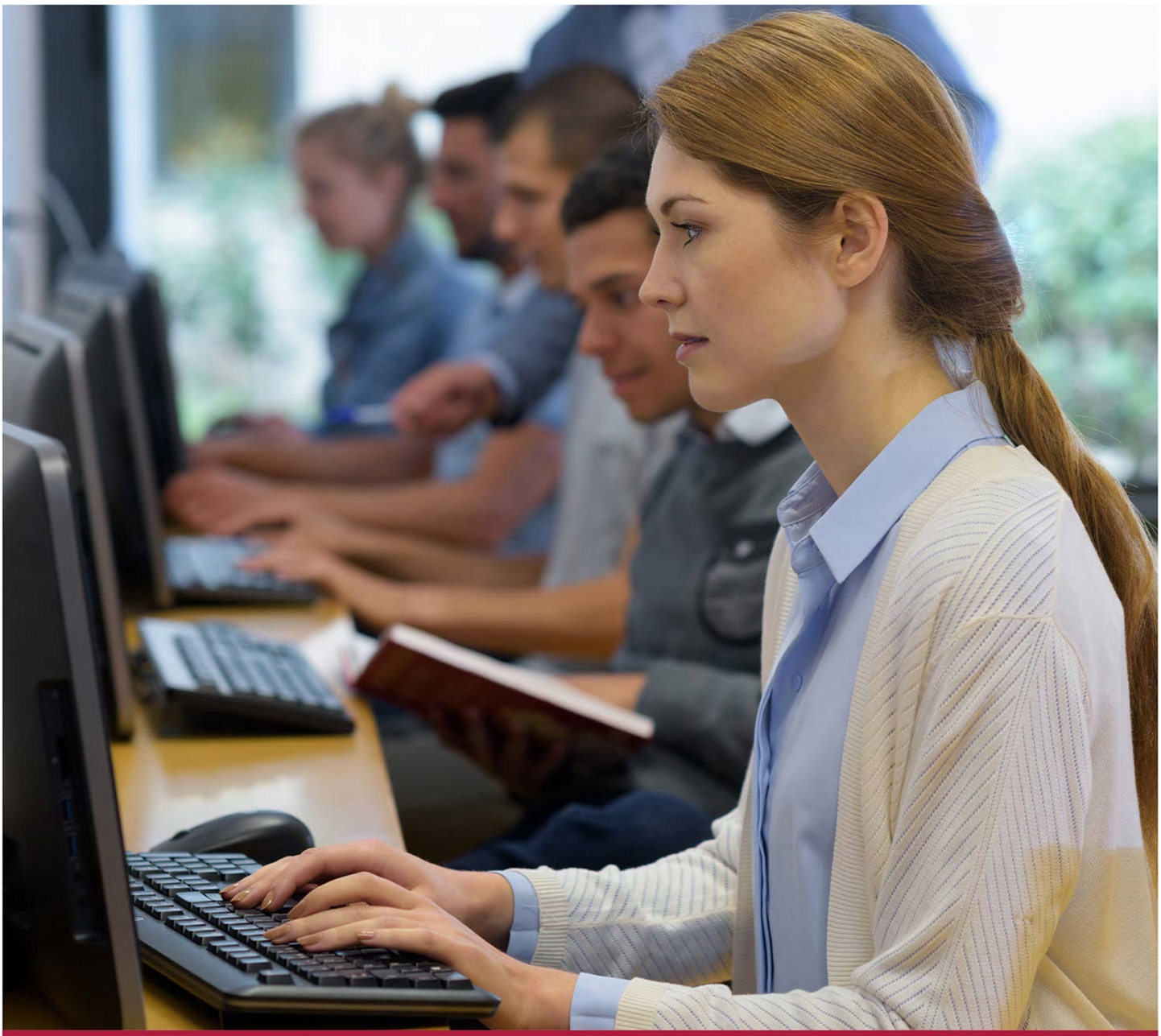
Академия АйТи
a Softline Company



Linux. Уровень 3. Обеспечение безопасности систем, сервисов и сетей

Код курса: linux3

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

Linux. Уровень 3. Обеспечение безопасности систем, сервисов и сетей

Код курса: linux3

Длительность	24 ак. часа
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Успешное окончание курса позволяет получить ключевые знания по обеспечению комплексной безопасности сетевой инфраструктуры, что позволит значительно уменьшить риск взлома сетей и сервисов предприятия и минимизировать последствия такого взлома.

Подробная информация

Цель курса:

Формирование знаний и навыков, необходимых для обеспечения безопасности систем, сервисов и сетей

Целевая аудитория:

Системные администраторы

Программа курса

Модуль 1.Периметры безопасности и размещение сервисов в сети предприятия

- Обзор моделей безопасности и обязанностей администратора безопасности компьютерной сети.
- Выбор конфигурации сети предприятия
- Разделение сервисов сети предприятия с точки зрения аудитории
- Лабораторные работы: Развертывание шлюза и сетей предприятия.
- Настройка шлюза для подключения сети предприятия к Internet
- Развертывание сетей предприятия (DMZ, MGMT, LAN)
- Развертывание сервисов в сетях предприятия

Модуль 2.Анализ информационных систем предприятия с точки зрения безопасности

- Методы анализа безопасности сети и сервисов предприятия
- Лабораторные работы: Использование сканеров безопасности
- Оценка безопасности систем и сервисов с помощью сканеров Nmap и OpenVAS
- Оценка безопасности передачи информации по сети с помощью сканера Ettercap
- Аудит учетных данных (John the Ripper)
- Аудит целостности систем (Tripwire, AIDE, OSSEC)
- Аудит закладок (rkhunter, chkrootkit)
- Аудит системных событий Linux (auditd)

Модуль 3.Защита систем предприятия на уровне ОС

- Обзор технологий, повышающих безопасность систем на уровне ОС
- Аудит состояния систем с точки зрения безопасности
- Лабораторные работы: Аудит состояния и защита систем предприятия
- Использование списков доступа POSIX ACL
- Использование системного вызова Chroot
- Использование механизмов мандатного доступа сервисов к объектам системы Linux LSM, AppArmor, SELinux
- Использование технологии изоляции сервисов Linux namespaces/cgroup/Docker/LXC
- Использование технологий Linux Hardened/PaX/grsecurity

4.Защита сервисов предприятия

- Методы защиты сетевых сервисов от вредоносных действий
- Лабораторные работы: Защита сетевых сервисов предприятия
- Настройка сервисов с точки зрения безопасности (сокрытие «баннеров», отключение небезопасных опций, ограничение попыток входа и т.д.)
- Ограничения привилегий учетных записей пользователей сервисов
- Замена устаревших сервисов (ftp/sftp, inetd/xinetd)
- Развертывание Удостоверяющего центра (УЦ) Certificate of Authority (CA) предприятия
- Защита конфиденциальной информации передаваемой сервисам с использованием протоколов SSL/TLS
- Использование PKI для управления идентификацией и конфиденциальности пользователей
- Использование технологий Honeynet и Honeypot (portsentry)
- Защита информации компании с использованием шифрования блочных устройств (dm-crypt)
- Использование специальных решений для защиты сервисов (dhcdrop)

Модуль 5.Защита сети предприятия

- Обзор решений пассивной и активной защиты периметра сети предприятия
- Лабораторные работы: Защита периметра сети предприятия
- Лабораторная работа: Использование возможностей пакетных фильтров для активной защиты периметра сети
- Лабораторная работа: Использование систем обнаружения вторжений (IDS) Snort для предупреждения о попытках вторжения
- Лабораторная работа: Использование решений защиты от вторжений (IPS) Snort/Snortsam/Fail2Ban для активной защиты периметра сети

Модуль 6.Использование VPN в сети предприятия

- Варианты организации сетей VPN
- Лабораторные работы: Управление доступом к внутренним ресурсам сети предприятия
- Использование SSH туннелей для организации VPN
- Использование Proxy сервера Squid в качестве WebVPN
- Использование OpenVPN для подключения филиалов и пользователей к сети предприятия

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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