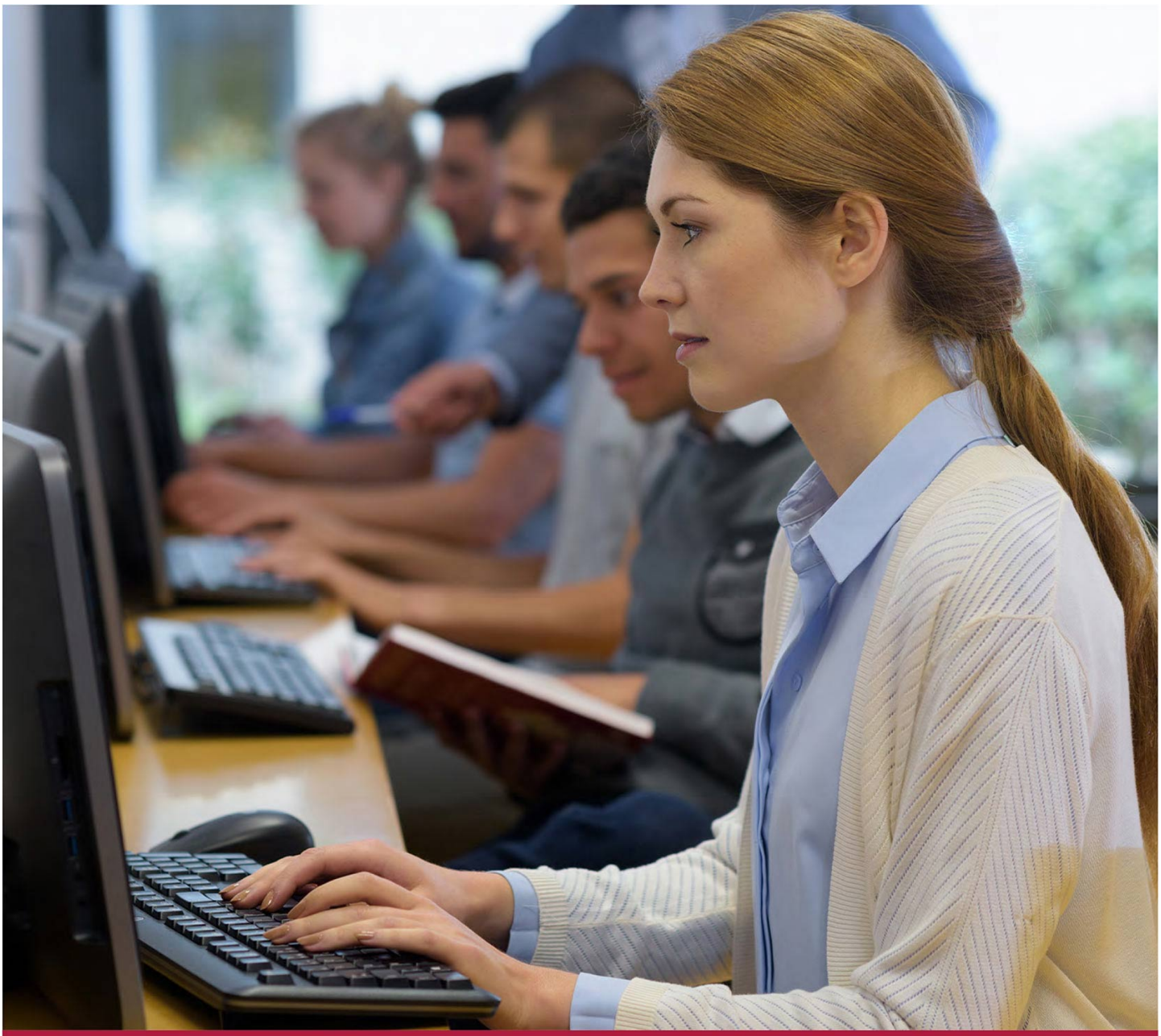
Академия АйТи
a Softline Company



Использование Linux в сетях Windows

Код курса: LINNET

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

Использование Linux в сетях Windows

Код курса: LINNET

Длительность	40 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Важнейшим фактором защиты информации в современных сетях является безопасная и прозрачная Single Sign On (SSO) идентификацией пользователей. В рамках курса рассматривается варианты решений этой задачи в сетях, объединяющих UNIX и Windows системы с использованием таких технологий как KERBEROS, LDAP, GSSAPI, NTLM и PKI. Рассматриваются открытые и коммерческие реализации этих технологий, их взаимодействие, достоинства и недостатки. Существенным отличием второй версии курса стало использование UNIX не только в качестве серверов, но и в роли рабочих станций. Кроме этого, в курсе рассмотрена организация KERBEROS сфер, позволяющая использовать UNIX в качестве полноценного сервера идентификации в смешанных Unix/Windows сетях.

Подробная информация

Успешное окончание обучения по программе данного курса позволит специалистам:

Знать:

- Максимальные ограничения по поддерживаемой операционной системой оперативной и дисковой памяти
- Принципы информационной безопасности инфокоммуникационной системы
- Модели доступа пользователей к инфокоммуникационной системе
- Основы безопасности функционирования инфокоммуникационной системы
- Типы интерфейсов дисковых подсистем
- Методы доступа к файловым системам
- Наборы утилит для работы с администрируемыми файловыми системами
- Методы восстановления данных
- Правила настройки и эксплуатации устанавливаемого системного программного обеспечения, включая лицензионные требования
- Принципы организации, состав и схемы работы операционных систем.

Уметь:

- Проверять условия эксплуатации и выполнение требований по электропитанию оборудования

- Вычислять размер памяти для каждого тома, общую память, память, необходимую для работы самой операционной системы
- Использовать специальные процедуры для повышения производительности и восстановления в случае сбоев дисковой подсистемы
- Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
- Проверять тип файловой системы тома и ее целостность
- Выполнять настройку системного программного обеспечения в соответствии с регламентами обеспечения информационной безопасности
- Инициализировать соответствующие модули операционной системы
- Включать файловые системы в общее пространство имен
- Комбинировать имеющиеся системные средства и избегать их противоречий
- Проводить авторизацию пользователей, имеющих доступ к настройке системного программного обеспечения инфокоммуникационной системы организации

Владеть навыками / выполнять следующие трудовые действия:

- Использовать сервисы NIS, библиотек PAM и NSSWITCH для идентификации пользователей в UNIX сетях
- Использовать протокола SSH для SSO идентификации в UNIX сетях.
- Настройки KERBEROS сферы для SSO идентификации пользователей в UNIX/Windows сетях.
- Использовать LDAP каталога для хранения информации о пользователях в сети.
- Использовать Microsoft Active Directory в качестве KERBEROS сферы и LDAP каталога в UNIX/Windows сетях.
- Использовать сервера Samba в роли файлового сервера и контроллера домена.

Целевая аудитория:

Системные администраторы

Руководители IT подразделений

Необходимая подготовка:

Знания в объеме материала курсов

Администрирование Linux часть 1

Администрирование Linux часть 2

Программа курса

Модуль 1. Развертывание сети предприятия

- Обзор ретроспективы развития технологий для доменной инфраструктуры
- Настройка стенда для последующих лабораторных работ

Модуль 2. Использование пакета Samba4 в качестве контроллера домена

- Обзор развития механизмов аутентификации и авторизации в домене Windows
- Лабораторная работа: Установка PDC средствами Samba 4.x
- Лабораторная работа: Установка BDC и его связывание с PDC
- Лабораторная работа: Добавление рабочих станций в домен Samba 4.x

Модуль 3. Использование сервисов Winbind и SSSD/Realmd

- Обзор протокола Kerberos 5 и его возможностей
- Лабораторная работа: Ввод Linux в домен Active Directory средствами Samba

4.x и winbind

- Лабораторная работа: Ввод Linux в домен Active Directory средствами

SSSD/Realmd

Модуль 4. Аутентификация с использованием протокола Kerberos

- Использование keytab-файлов для аутентификации сервисов
- Лабораторная работа: Настройка прокси-сервера SQUID на использование

Kerberos-аутентификации

Модуль 5. FreeIPA как альтернатива Active Directory

- Обзор возможностей домена на основе FreeIPA
- Сравнение FreeIPA и Active Directory
- Лабораторная работа: Установка контроллера домена FreeIPA
- Лабораторная работа: Установка клиента домена FreeIPA
- Лабораторная работа: Ввод Windows в домен FreeIPA

Модуль 6. От периметровой защиты к Defence-in-Depth

- Развитие технологий периметровой защиты (сильные и слабые стороны)
- Четыре периметра безопасности (лучшее решение для периметровой защиты)
- Defence-In-Depth как наиболее зрелое решение по защите инфраструктуры

Модуль 7. Политики, процедуры и регламенты

- ISO-стандарты и ГОСТы на их основе
- Система менеджмента ИБ
- Регламент реагирования на инциденты ИБ

Модуль 8. Физическая защита

- Обзор требований к физической защите
- Требования к физической защите криптосредств (в соответствии с

требованиями ФСБ)

Модуль 9. Защита периметра

- Три поколения межсетевых экранов
- Специфика работы State Inspection Firewall
- Лабораторная работа: Настройка межсетевого экрана
- Лабораторная работа: Настройка VPN-сервера для безопасного доступа в

локальную сеть

Модуль 10. Защита внутренних сетей

- Использование безопасных протоколов AAA (Kerberos/Radius)
- Лабораторная работа: Внедрение HoneyPot для выявления сканирования

портов

Модуль 11. Защита на уровне узла сети

- Механизмы защиты от эксплойтов на уровне ядра системы
- Лабораторная работа: Использование EMET для защиты ядра Windows от

эксплойтов

- Лабораторная работа: Применение Hardened-патча для ядра Linux с целью

снижения рисков применения эксплойтов нулевого дня

- Лабораторная работа: LKRG и Tyton – модули ядра Linux для защиты от

эксплойтов

Модуль 12. Защита на уровне приложений

- Лабораторная работа: Использование сетевого суперсервера для защиты от

brute-force и dictionary-атак

- Анализ журнальных файлов для выявления попыток подбора паролей к

приложениям

- Лабораторная работа: Настройка Fail2Ban для защиты сетевых сервисов от

атак, связанных с подбором паролей

Модуль 13. Защита данных

- Лабораторная работа: Шифрование данных в Windows средствами BitLocker
- Лабораторная работа: Шифрование данных в Linux средствами LUKS

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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