Бауманский учебный центр «Специалист»

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

Код курса: **ЮНБЕЗ**

Тема	Ак. часов
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	**4**
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 • Аудит целостности систем • Аудит закладок • Аудит системных событий Linux (auditd)	**4**
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 POSIX capabilities • Использование системного вызова Chroot • Использование механизмов мандатного доступа сервисов к объектам системы Linux LSM • Использование технологии изоляции сервисов Linux namespaces/cgroup/Docker/LXC	**4**

Модуль 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 • 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 • Защита информации компании с использованием шифрования блочных устройств (dm-crypt) • Использование специальных решений для защиты сервисов	**4**
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) для предупреждения о попытках вторжения • Лабораторная работа: Использование решений защиты от вторжений (IPS) Fail2Ban для активной защиты периметра сети	**4**
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 OpenVPN для подключения филиалов и пользователей к сети предприятия	**4**
Аудиторная нагрузка в классе с преподавателем	**24 ак.ч. + 24 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