OTUS

Безопасность Linux

Курс про обеспечение комплексной безопасности локальной и сетевой инфраструктуры, построенной на базе Linux

Длительность курса: 116 академических часов

1 Потенциальные цели для атаки со стороны злоумышленников

1	**Атаки на аппаратные средства и программное обеспечение**	дать теоретическое понимание, что такое ИБ. Как ИБ затрагивает процессы системного администрирования. Привести примеры внутренних и внешних угроз (инсайдеры, хакеры, бот-нет сети и т.д.)
2	**Типовые сценарии, инструменты и методики взлома серверов и сетей**	рассказать пару или тройку громких кейсов со взломом ИТ-систем, где причиной взлома явилось «неграмотное» администрирование (статьи на] [акере, Хабре)

2 Концепции безопасности Linux

1 **Обзор встроенных механизмов защиты в Linux**

четко зафиксировать в умах слушателей специфику Linux систем в сравнении с Windows, модель безопасности и философию Unix-way

Домашние задания

1 ДЗ1

создать модель безопасности для нескольких Linux компьютеров, находящимися в сети Интернет, описать угрозы, вероятные векторы атак и общий подход к обеспечению безопасности

---

2 **Управление пользователями и группами, сервисами и прикладным ПО**

3 Управление пользователями и группами

1 **Управление учетными записями и домашними каталогами пользователей**

научиться практическим аспектам управления пользователями и группами в Linux

Домашние задания

1 ДЗ 2

согласно матрице доступа создать пользовательские учетные записи и установить необходимые права для каждого пользователя

---

2 **Парольная политика и выполнение операций от имени учётной записи root**

4 Файлы, каталоги и конфигурирование прав доступа

1 **Использование атрибутов разграничения доступа - suid, sgid, sticky-bit, umask**

научиться практическим аспектам управления файлами, директориями и правами доступа к объектам файловой структуры

Домашние задания

1 ДЗ 3

согласно матрице доступа сконфигурировать права доступа к существующим каталогам и файлам для всех указанных пользователей в системе

5 Система безопасности PAM

1	**Конфигурационные файлы PAM. Примеры использования PAM**	
2	**Использование SELinux. Язык описания правил доступа**	научиться практическим аспектам Работы с SELinux

6 Списки контроля доступа (Access Control Lists)

1	**Списки контроля доступа (Access Control Lists)**	научиться практическим аспектам работы с расширенными списками доступа (ACL)

7 Пакетный фильтр Iptables

1 **Фильтрация трафика с помощью межсетевого экрана iptables**

научиться практическим аспектам Работы с сетевым фильтром для защиты от DDoS-атак и некоторых других сетевых атак

Домашние задания

1 ДЗ 4

создать цепочки фильтрации для защиты компьютера с Linux от сканирования из внешней сети Интернет

---

2 **Настройка правил фильтрации для прокси-сервера squid**

8 Безопасная настройка прокси-сервера SQUID

1 **Настройка проксирующего режима squid**

показать возможности конфигурирования SQUID как безопасного прокси-сервера (шлюза в Интернет) для корпоративной сети

Домашние задания

1 ДЗ 5

сконфигурировать правила доступа пользователей в сеть Интернет на прокси-сервере SQIUD

---

2 **Дополнительные настройки безопасности для squid**

9 Шифрование данных

1 **Пакеты openssl и stunnel**

научиться приемам шифрования отельных сетевых соединений, файлов, каталогов и партаций ОС
Примеры ПО для шифрования файлов и каталогов

Домашние задания

1 ДЗ 6

создать отельный том в структуре файловой системы и зашифровать его с использованием симметричных алгоритмов шифрования

---

2 **Использование серверных и клиентских сертификатов на примере Web-приложения на базе Apache+MySQL+PHP**

10 Система аудита и журнальные файлы

1 **Настройка системы регистрации событий в ОС Linux**

научиться приемам работы с журналами ОС в контексте поиска и анализа событий ИБ

Домашние задания

1 ДЗ 7

найти события безопасности в системном журнале, отметить критичные операции, выгрузить эти данные в текстовый файл

---

2 **Ручной и автоматический анализ журналов**

11 Квоты и лимитирование вычислительных ресурсов

1 **Управление лимитами для дисковой подсистемы и контроля вычислительных ресурсов**

научиться приемам работы для обеспечения лимитирования вычислительных ресурсов

Домашние задания

1 ДЗ 8

настроить правила выделения памяти, дискового пространства и использования центрального процессора под сетевые сервисы и ресурсы web-сервера Apache

12 Сетевые сканеры, анализаторы и системы обнаружения вторжения

1	**Инструментарий для выполнения проверок (сканеры безопасности)**	научиться приемам работы с сетевыми сканерами, анализаторами и IDS\IPS-системами Домашние задания 1 ДЗ 9 с помощью установленного сканера безопасности проверить наличие уязвимостей ПО и ядра Linux
2	**Контроль соответствия требованиям политики безопасности**	

13 Безопасная настройка сервисов

1	**Безопасность сервисов на базе Xinitd**	научиться практическим аспектам управления сервисов, обеспечивающих защиту от внешнего вторжения Домашние задания 1 ДЗ 10 на установленный web-сервер Apache подключить плагины безопасности и активировать специальные настройки безопасности для внешних пользователей
2	**Некоторые настройки безопасности для web-сервера Apache**	научиться практическим аспектам управления сервисов, обеспечивающих защиту от внешнего вторжения

14 Безопасность сетевых соединений

1 **Настройка безопасных VPN-соединений**

научиться практическим аспектам управления защищенными соединениями (SSH, VPN, VLAN, DMZ-сегментация)

Домашние задания

1 ДЗ 11

создать несколько VPN-соединений к другим компьютерам на базе Linux, находящихся в другом сегменте сети Интернет, настроить криптографические протоколы защищенного обмена

---

2 **Безопасность удаленного доступа SSH и безопасной маршрутизации**

15 Итоговая проектная работа

1	**Консультации и обсуждения проектной работы**	Домашние задания 1 Установка и настройка защищенного рабочего окружения на базе нескольких машин Linux (web-сервер Apache, прокси-сервер Squid и т.д.) с нуля
2	**Консультации и обсуждения проектной работы**	
3	**Консультации и обсуждения проектной работы**	