Программа

№	Тема	Часы
Аутентификация		
1.	Методы обеспечения аутентификации средствами SSH-сервера Парольная аутентификация Аутентификация по публичному ключу Возможности PAM на примере одноразовых паролей Механизмы аутентификации в SQUID Одноразовые пароли Google аутентификация	4
Механизмы обеспечения целостности		
2.	Использование aide для контроля целостности системных файлов Превентивные меры по предотвращению эксплуатации уязвимостей Сборка ядра с патчами ,безопасности	2
Достоверность данных		
3.	Использование хэш-функций Применение PGP для защиты конфиденциальности Проверка контрольных сумм файлов и ее недостатки Подписание и проверка подписи исполняемого файла	2
Конфиденциальность		
4.	Механизмы ограничения доступа Помещение сервисов в chroot Применение легкой виртуализации LXC Шифрование файловой системы	2
Доступность		
5.	Механизмы контроля доступности Применение POSIX ACL для доступа к файлам Настройка LXC	4
Виртуализация		
6.	Применение виртуализации KVM Применение виртуализации LXC Основные отличия	6
Формирование отказоустойчивого кластера		
7.	Развертывание виртуальной лаборатории под кластерные решения Выбор оборудования узлов кластера и коммутация сети Предварительная настройка узлов кластера	4
Синхронизация конфигураций узлов кластера		
8.	Обзор вариантов решения задачи Использования пакета SSH, развертывание DNS сервера	4
Развертывание отказоустойчивого WWW хостинга		

9.	Обзор средств синхронизации пользовательских данных Обзор задач, стоящих перед менеджером кластера Настройка сервисов HTTP и FTP Синхронизация пользовательских данных пакетом RSYNC	4
Проверка безопасности сети и сервисов		
10.	Инструменты контроля безопасности Типы сетевых атак Перехват сессий, изменение содержимого (intercepter ng) Инструмент metasploit	8
ИТОГО:		40