Бауманский учебный центр «Специалист»

Программа курса Противодействие хакерским атакам: защита, предсказание, распознавание, ответ

Код курса: **ЦНД**

Тема	Ак. часов

Модуль 1. Сетевые атаки и стратегии защиты
 	
• Основная терминология
  ◦ Активы
  ◦ Угрозы
  ◦ Нарушители
  ◦ Уязвимости
  ◦ Риски
  ◦ Атаки
• Сетевые атаки
  ◦ Рекогносцировка
  ◦ Прослушивание сети
  ◦ Атака «Человек посередине» (MITM)
  ◦ Атаки на пароли
  ◦ Повышение привилегий
  ◦ Отравление DNS
  ◦ Отравление ARP
  ◦ DHCP Атаки:
  ▪ DHCP старвация
  ▪ DHCP спуфинг
  ◦ Подмена MAC
  ◦ Отказ в обслуживании (DoS)
  ◦ Распределенная атака на отказ в обслуживании (DDoS)
  ◦ Вредоносное ПО
  ◦ Advanced Persistent Threats
• Атаки на приложения
  ◦ SQL инъекции
  ◦ Межсайтовый скриптинг (XSS)
  ◦ Подмена параметров
  ◦ Обход каталога
  ◦ Межсайтовая подделка запросов (CSRF)
  ◦ Перехват сеанса
  ◦ DoS на уровне приложений
• Социальная инженерия
• Атаки по электронной почте
• Атаки на мобильные устройства
• Атаки на облачные вычисления
• Атаки на беспроводные сети
• Методологии хакинга
  ◦ Методология CEH
  ◦ Cyber Kill-Chain
  ◦ MITRE ATT&CK
• Цели и проблемы сетевой защиты
• Стратегии защиты
• Эшелонированная защита
 	
Практическая работа
 	
• **Изучение угроз сетевой безопасности**
• **Выполнение атак сканирования, взлома паролей, SQL инъекций и XSS**
	2

Модуль 2. Административные меры безопасности
 	
• Соответствие нормативным требованиям
  ◦ Нормативно-правовая база
  ◦ Как соответствовать требованиям
• Стандарты и законодательство
  ◦ PCI-DSS
  ◦ ГОСТ Р 57580.1
  ◦ GDPR
  ◦ ФЗ № 152-ФЗ
  ◦ Другие законы и нормативные акты
• Политики безопасности
  ◦ Содержание политики безопасности
  ◦ Пример политики безопасности
  ◦ Виды политик безопасности
  ◦ Чек-лист применения политик безопасности
• Осведомленность и тренинги
• Другие административные меры
 	
Практическая работа
 	
• **Применение групповых политик в домене Active Directory**
• **Применение парольных политик в домене ALT Server**
• **Мониторинг активности сотрудников с помощью DLP**
	2

Модуль 3. Технические меры безопасности
 	
• Контроль доступа
• Контроль доступа в распределенных сетях
• Управление идентификацией и доступом
• Криптографические техники защиты
  ◦ Шифрование
  ◦ Хэширование
  ◦ Цифровая подпись
  ◦ Инфраструктура открытых ключей (PKI)
• Криптографические алгоритмы
  ◦ DES
  ◦ AES
  ◦ RC4, RC5, RC6
  ◦ DSA и RSA
  ◦ MD5
  ◦ SHA
  ◦ HMAC
• Сегментирование сети
• Решения сетевой безопасности
  ◦ Фаерволлы
  ◦ Системы обнаружения вторжений (IDS)
  ◦ Системы ловушки (Honeypots)
  ◦ Прокси серверы
  ◦ Анализаторы сетевых протоколов
  ◦ Фильтры веб содержимого
  ◦ Балансировщики сетевой нагрузки (NLB)
  ◦ UTM системы
  ◦ SIEM системы
  ◦ Системы контроля сетевого доступа (NAC)
  ◦ Виртуальные частные сети (VPN)
• Протоколы сетевой безопасности
  ◦ RADIUS
  ◦ Kerberos
  ◦ PGP
  ◦ S/MIME
  ◦ HTTPS
  ◦ IPSec
 	
Практическая работа
 	
• **Применение ролевого управления доступом с помощью JEA**
• **Применение ролевого управления доступом с помощью WAC**
• **Применение прокси-сервера Squid**
• **Установка VPN подключения с помощью OpenVPN**
	2

Модуль 4. Безопасность сетевого периметра
 	
• Фаерволлы
  ◦ Концепции
  ◦ Технологии
  ◦ Топологии
  ◦ Реализации
  ◦ Возможности
  ◦ Развертывание
  ◦ Рекомендации
  ◦ Администрирование
• Системы обнаружения вторжений (IDS)
  ◦ Концепции
  ◦ Классификации
  ◦ Типы обнаружения вторжения
  ◦ Компоненты IDS
  ◦ Развертывание
  ◦ Оповещения
  ◦ Выбор решения
  ◦ IDS решения
• Маршрутизаторы и коммутаторы
• Программно-определяемый периметр (SDP)
  ◦ Зачем программно определять периметр
  ◦ Недостатки традиционной безопасности
  ◦ Что такое SDP
  ◦ Применение SDP
  ◦ Архитектура SDP
  ◦ Инструменты SDP
 	
Практическая работа
 	
• **Блокировка доступа к сайту с помощью Ideco NGFW**
• **Закрытие портов с помощью Ideco NGFW**
• **Применение Windows Firewall**
• **Применение nft в Linux**
• **Применение IDS Suricata в Security Onion**
• **Применение IDS Suricata в Ideco NGFW**
	2

Модуль 5. Безопасность хостов Windows
 	
• Вопросы безопасности хостов Windows
  ◦ Операционные системы Windows
  ◦ Архитектура Windows
  ◦ Уязвимости хостов Windows
• Компоненты системы безопасности Windows
  ◦ Монитор ссылок безопасности
  ◦ Сервис проверки подлинности локальной системы безопасности
  ◦ Диспетчер учётных записей безопасности
  ◦ Активный каталог
  ◦ Пакеты проверки подлинности
  ◦ Диспетчер входа в систему
  ◦ Экран приветствия
  ◦ Провайдеры учетных записей
  ◦ Служба сетевого входа
  ◦ Драйвер устройства безопасности ядра
• Возможности безопасности Windows
• Основной уровень безопасности Windows
• Управление пользователями и паролями
• Установка обновлений
• Управление доступом пользователей
  ◦ Ограничение доступа к файлам
  ◦ Контроль учетных записей
  ◦ Доступ к компонентам системы
  ◦ Технология Just Enough Administration
• Техники укрепления хостов Windows
  ◦ Установка пароля на BIOS
  ◦ Хранение хэшей
  ◦ Ограничение установки программ
  ◦ Настройка системных служб
  ◦ Антивирусное ПО
  ◦ Настройка брандмауэра Windows
  ◦ Мониторинг реестра
• Укрепление Active Directory
• Укрепление сетевых служб и протоколов
  ◦ Повышение безопасности PowerShell
  ◦ Повышение безопасности RDP
  ◦ Применение DNSSEC
  ◦ Повышение безопасности SMB
 	
Практическая работа
 	
• **Выполнение базовых задач администрирования из командной строки**
• **Настройка доступа к общим ресурсам в Active Directory**
• **Анализ основного уровня безопасности с помощью MSCT**
• **Делегирование административных полномочий в Active Directory**
• **Защита паролей локальных администраторов с помощью LAPS**
	3

Модуль 6. Безопасность хостов Linux
 	
• Вопросы безопасности хостов Linux
  ◦ Архитектура Linux
  ◦ Особенности Linux
  ◦ Уязвимости хостов Linux
• Установка и обновление Linux
  ◦ Установка пароля на BIOS
  ◦ Защита загрузчика
  ◦ Управление установкой обновлений
  ◦ Контрольный список по установке и обновлениям
• Техники укрепления хостов Linux
  ◦ Настройка системных служб
  ◦ Удаление ненужных программ
  ◦ Установка антивируса
  ◦ Контрольный список по укреплению хостов Linux
• Управление пользователями и паролями
• Сетевая безопасность и удаленный доступ
• Инструменты безопасности и фреймворки
 	
Практическая работа
 	
• **Выполнение базовых задач укрепления Linux**
• **Установка и настройка AppArmor**
• **Настройка и использование Lynis**
• **Обнаружение векторов повышения привилегий с помощью LinPEAS**
	3

Модуль 7. Безопасность мобильных устройств
 	
• Использование мобильных устройств на предприятии
  ◦ Политика BYOD
  ◦ Политика CYOD
  ◦ Политика COPE
  ◦ Политика COBO
• Риски связанные с мобильными устройствами
• Решения по управлению мобильными устройствами (MDM)
• Руководства и практические рекомендации
• Безопасность Android
• Безопасность iOS
 	
Практическая работа
 	
• **Применение Miradore MDM**
	2

Модуль 8. Безопасность IoT устройств • Что такое Интернет Вещей • Применение IoT устройств • Архитектура Интернета Вещей • Риски использования IoT • Защита IoT окружения • Меры безопасности IoT • Инструменты защиты и рекомендации **Практическая работа** • **Анализ и настройка SSL/TLS коммуникаций интернета вещей**	**2**

Модуль 9. Безопасность приложений
 	
• Применение белых и черных списков приложений
  ◦ Политики ограниченного использования программ
  ◦ Применение AppLocker
  ◦ MangeEngine Desktop Central
  ◦ Ограничение установки приложений
  ◦ Политики эксплорера запрета запуска программ
  ◦ Инструменты применения белых и черных списков
• Применение песочниц (Sandbox)
  ◦ Песочницы в Windows
  ◦ Песочницы в Linux
  ◦ Инструменты для внедрения песочниц
• Обновление приложений
  ◦ Инструменты для обновления приложений
• Фаерволлы для веб-приложений (WAF)
  ◦ Концепции использования WAF
  ◦ WAF инструменты
 	
Практическая работа
 	
• **Применение AppLocker**
• **Применение SRP**
• **Применение Firejail Sandbox**
• **Применение URLScan WAF**
	3

Модуль 10. Безопасность данных
 	
• Концепции защиты данных
• Управление доступом к данным
• Шифрование неактивных данных
  ◦ Шифрование дисков
  ▪ Шифрование дисков в Windows
  ▪ Шифрование дисков в MacOS
  ▪ Шифрование дисков в Linux
  ▪ Шифрование дисков в Android
  ▪ Шифрование дисков в iOS
  ▪ Инструменты шифрования дисков
  ◦ Шифрование файлов
  ▪ Шифрование файлов в Windows
  ▪ Шифрование файлов в MacOS
  ▪ Шифрование файлов в Linux
  ◦ Шифрование съемных носителей
  ▪ Шифрование съемных носителей в Windows
  ▪ Шифрование съемных носителей в MacOS
  ▪ Шифрование съемных носителей в Linux
  ◦ Шифрование баз данных
  ▪ Шифрование в MS SQL
  ▪ Шифрование в Oracle
• Шифрование данных при передаче
  ◦ Шифрование между браузером и веб сервером
  ◦ Шифрование между сервером БД и веб сервером
  ◦ Шифрование почты
• Маскировка данных
  ◦ Типы и техники маскировки данных
  ◦ Маскировка данных в MS SQL
  ◦ Маскировка данных в Oracle
  ◦ Инструменты маскировки данных
• Резервное копирование и хранение данных
  • Стратегии резервного копирования
  • Выбор носителя для резервной копии
  ◦ Технология RAID
  ▪ Что такое RAID системы
  ▪ Архитектура RAID
  ▪ Уровень RAID 0: Чередование дисков	

▪ Уровень RAID 1: Зеркалирование дисков ▪ Уровень RAID 3: Чередование дисков с четностью ▪ Уровень RAID 5: Распределенная четность ▪ Уровень RAID 10: Дублирование и параллельная обработка ▪ Уровень RAID 50: Распределенная четность и повышенная производительность ▪ Выбор подходящих уровней RAID ▪ Аппаратные и программные RAID ▪ Практические рекомендации по использованию RAID ◦ Сеть хранения данных (SAN) ▪ Практические рекомендации и инструменты ◦ Сетевые хранилища (NAS) ▪ Типы NAS ▪ Интегрированная система NAS ▪ Шлюз системы NAS ▪ Выбор подходящего метода резервного копирования ▪ Выбор правильного места для резервного копирования ▪ Типы резервного копирования ▪ Полное резервное копирование ▪ Обычное резервное копирование ▪ Разностное резервное копирование ▪ Добавочное резервное копирование ▪ Выбор лучшего решения для резервного копирования ▪ Программное обеспечение для резервного копирования ▪ Резервное копирование баз данных ▪ Резервное копирование электронной почты ▪ Резервное копирование веб-сервера ▪ Политика хранения данных ◦ Безвозвратное удаление данных ▪ Инструменты безвозвратного удаления данных ◦ Предотвращение утечек данных (DLP) ▪ Решения DLP ▪ Рекомендации по внедрению DLP **Практическая работа** ◦ **Шифрование данных с использованием VeraCrypt** ◦ **Шифрование баз данных MS SQL** ◦ **Применение OpenSSL** ◦ **Архивация данных в Windows** ◦ **Восстановление удаленных данных**	**3**
Модуль 11. Защита виртуальных сетей • Виртуальное окружение • Концепции виртуализации • Виртуальные сети • Атаки на VLAN • Безопасность VLAN • Программно-конфигурируемые сети (SDN) • Виртуализация сетевых функций (NFV) • Безопасность виртуализации ◦ Контейнеры ◦ Докеры ◦ Kubernetes • Руководства и рекомендации по безопасности **Практическая работа** • **Аудит безопасности докера с помощью сканера Trivy** • **Аудит безопасности докера с помощью Docker-Bench-Security**	**2**

Модуль 12. Безопасность облачных вычислений • Концепции облачных вычислений • Безопасность в облаке • Провайдеры облачных сервисов • Безопасность облака Amazon (AWS) • Безопасность облака Microsoft Azure • Безопасность облака Cloud.ru • Рекомендации и инструменты по безопасности **Практическая работа** • **Управление доступом в облаке** • **Управление ключами в облаке** • **Защита хранилища в облаке**	**2**

Модуль 13. Wi-Fi. Защита беспроводных сетей
 	
• Основные термины
• Беспроводные сети
• Беспроводные стандарты
• Беспроводные топологии
  ◦ Ad-hoc
  ◦ Инфраструктура
• Использование беспроводных сетей
  ◦ Расширение проводной сети
  ◦ Несколько точек доступа
  ◦ Маршрутизируемые беспроводные сети
  ◦ 3G Hotspot
• Компоненты беспроводной сети
  ◦ Точка доступа
  ◦ Сетевой адаптер
  ◦ Модем
  ◦ Мост
  ◦ Ретранслятор
  ◦ Маршрутизатор
  ◦ Шлюзы
  ◦ USB-адаптер
  ◦ Антенна
• Типы шифрования в беспроводных сетях
  ◦ WEP
  ◦ WPA
  ◦ WPA2
  ◦ WPA3
• Методы проверки подлинности
  ◦ Открытая система
  ◦ Аутентификация по общему ключу
• Использование сервера централизованной аутентификации
• Меры повышения безопасности беспроводных сетей
  ◦ Инвентаризация устройств
  ◦ Размещение точек доступа
  ◦ Выключение трансляции SSID
  ◦ Применение надежного шифрования
  ◦ Фильтрация MAC адреса
  ◦ Мониторинг беспроводного трафика
  ◦ Обнаружение поддельных точек доступа
  ◦ Настройка параметров точки доступа
 	
Практическая работа
 	
• **Настройка параметров безопасности беспроводной точки доступа**
	1

Модуль 14. Мониторинг и анализ сетевого трафика
 	
• Введение в мониторинг и анализ трафика
• Расположение сенсоров для мониторинга трафика
• Примеры сигнатур сетевого трафика
  ◦ Сигнатуры нормального трафика
  ◦ Сигнатуры сетевых атак
  ◦ Техники анализа сигнатур сетевых атак
  ▪ Контентный анализ
  ▪ Контекстный анализ
  ▪ Композитный анализ
  ▪ Анализ одного пакета
• Сниффер N1: Wireshark
  ◦ Компоненты Wireshark
  ◦ Фильтры отображения и захвата
  ◦ Мониторинг и анализ трафика
• Обнаружение сетевых атак
  ◦ Примеры обнаружения сетевых атак
• Концепции мониторинга производительности сети
 	
Практическая работа
 	
• **Анализ сетевого трафика с помощью Wireshark**
• **Обнаружение атак посредством анализа сетевого трафика**
• **Анализ сетевого трафика с помощью ntop-ng**
	2

Модуль 15. Мониторинг и анализ сетевых журналов
 	
• Концепции ведения журналов
  ◦ Форматы журналов
  ◦ Типы журналирования
• Анализ журналов Windows
• Анализ журналов Linux
• Анализ журналов Mac OS
• Анализ журналов фаерволлов
• Анализ журналов маршрутизаторов
• Анализ журналов веб-серверов
• Централизованное ведение журналов
  ◦ Инструменты для централизованного ведения журналов
 	
Практическая работа
 	
• **Анализ журналов Windows**
• **Анализ журналов веб-сервера**
	1

Модуль 16. Управление реагированием на инциденты • Реагирование на инциденты • Состав команды: Роли и обязанности • Оперативное реагирование на инцидент ◦ Первые шаги по реагированию для сетевых администраторов • Процесс обработки и реагирования на инцидент • Последовательность действий при обработке инцидента • Расследование инцидента информационной безопасности **Практическая работа** • **Обработка инцидентов информационной безопасности**	**2**

Модуль 17. Непрерывность бизнеса и восстановление после сбоев • Концепции непрерывности бизнеса и восстановления после сбоев • Деятельность по обеспечению непрерывности и восстановления • Планы по обеспечению непрерывности и восстановления • Стандарты по обеспечению непрерывности и восстановления **Практическая работа** • **Применение технологии NLB в Windows Server**	**2**

Модуль 18. Управление рисками
 	
• Концепции управления рисками
  ◦ Роли и ответственности при управлении рисками
  ◦ Ключевые индикаторы риска
• Программа управления рисками
• Фазы управления рисками
  ◦ Идентификация рисков
  ◦ Оценка риска
  ▪ Уровни риска
  ▪ Матрица рисков
  ◦ Обработка риска
  ◦ Пересмотр риска
• Фреймворки по управлению рисками
  ◦ Вендоры ERM решений
  ◦ Рекомендации по эффективному управлению рисками
• Управление уязвимостями
  ◦ Обнаружение
  ◦ Расстановка приоритетов
  ◦ Оценка уязвимостей
  ◦ Составление отчетов
  ▪ Примеры отчетов
  ◦ Устранение уязвимостей
  ◦ Проверка
• Сканирование и инвентаризация уязвимостей
 	
Практическая работа
 	
• **Проведение аудита безопасности сети с помощью OpenVAS**
• **Проведение аудита безопасности веб сайта с помощью OWASP ZAP**
	2

Модуль 19. Определение угроз и анализ поверхности атаки • Что такое анализ поверхности атаки • Визуализация поверхности атаки • Идентификаторы воздействия (IoE) • Симуляция атаки (BAS) ◦ Вендоры решений по симуляции атак • Снижение поверхности атаки • Анализ поверхности атаки для облачных вычислений и IoT **Практическая работа** • **Анализ поверхности атаки с использованием Windows Attack Surface Analyzer** • **Анализ поверхности атаки веб приложения с использованием OWASP Attack Surface Detector** • **Составление карты поверхности атаки с помощью Amass**	**1**

Модуль 20. Анализ киберугроз
 	
• Роль анализа киберугроз (CTI) в сетевой защите
• Типы сведений об угрозах
• Индикаторы киберугроз
  ◦ Индикатор компрометации (IoC)
  ◦ Индикатор атаки (IoA)
• Уровни киберугроз
• Платформы анализа угроз
• Сопротивление киберугрозам
 	
Практическая работа
 	
• **Изучение фидов угроз**
	1

Аудиторная нагрузка в классе с преподавателем	**40 ак.ч. + 40 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