Бауманский учебный центр «Специалист»

Программа курса Этичный хакинг. Техники атак и инструменты противодействия

Код курса: **CEH**

Тема	Ак. часов

Модуль 1. Введение в этичный хакинг
 	
• Обзор информационной безопасности
  ◦ Примеры и статистика утечки данных
  ◦ Основные термины безопасности
  ◦ Составляющие элементы информационной безопасности
• Угрозы информационной безопасности и векторы атак
• Концепции хакинга
  ◦ Что такое хакинг?
  ◦ Классы хакеров
  ◦ Фазы хакинга
• Концепции этичного хакинга
  ◦ Что такое этичный хакинг?
  ◦ Необходимость этичного хакинга
  ◦ Область и ограничения этичного хакинга
  ◦ Навыки этичного хакера
• Управление информационной безопасностью
  ◦ Обеспечение защиты информации
  ◦ Программа управления информационной безопасностью
  ◦ Архитектура информационной безопасности предприятия
  ◦ Зонирование сети
  ◦ Эшелонированная защита
  ◦ Политики информационной безопасности
  ◦ Моделирование угроз и управление рисками
  ◦ Управление реагированием на инциденты
  ◦ Средства управления сетевой безопасностью
• Концепции тестирования на проникновение
• Стандарты и законы по информационной безопасности
• **Практическая работа:** Изучение концепций и подготовка лаборатории
	2

Модуль 2. Сбор информации
 	
• Концепции рекогносцировки
• Методология сбора информации
  ◦ Использование поисковых систем
  ◦ Техники расширенного поиска в Google
  ◦ Google Hacking Database (GHDB)
  ◦ Поиск VoIP и VPN в GHDB
  ◦ Сбор данных из социальных сетей
  ◦ Сбор информации с веб-сайта
  ◦ Сбор информации из почтовых систем
  ◦ Конкурентная разведка
  ◦ Сбор данных, используя данные регистраторов
  ◦ Сбор данных DNS
  ◦ Сбор сетевой информации
  ◦ Социальная инженерия для сбора данных
• Инструменты сбора информации
• Меры противодействия сбору информации
• Тестирование на возможность сбора информации
• **Практическая работа:** Применение техник по сбору информации
	2

Модуль 3. Сканирование
 	
• Концепции сканирование сети
• Инструменты сканирования сети
• Техники сканиирования сети
  ◦ ICMP сканирование
  ◦ TCP Connect сканирование
  ◦ Сканирование полуоткрытыми соединениями
  ◦ Сканирование инверсными TCP флагами
  ◦ Xmas сканирование
  ◦ ACK сканирование
  ◦ Техника скрытого сканирования
  ◦ Сканирование UDP
  ◦ Сканирование SSDP
• Техники уклонения от систем обнаружения вторжений
  ◦ Фрагментация пакетов
  ◦ Маршрутизация от источника
  ◦ Маскировка IP
  ◦ Спуфинг IP
  ◦ Использование Proxy при сканировании
  ◦ Анонимайзеры
• Сбор баннеров
• Построение сетевых диаграмм
• **Практическая работа:** Сканирование компьютеров лаборатории и идентификация сервисов
	2

Модуль 4. Перечисление • Концепции перечисления • Техники перечисления • Перечисление NetBIOS • Перечисление SNMP • Перечисление LDAP • Перечисление NTP • Перечисление NFS • Перечисление SMTP • Перечисление DNS • IPSec перечисление • VoIP перечисление • RPC перечисление • Unix перечисление • Меры противодействия перечислению • **Практическая работа:** Применение техник перечисления	**2**

Модуль 5. Анализ уязвимостей
 	
• Концепции оценки уязвимостей
  ◦ Исследование уязвимостей
  ◦ Классификация уязвимостей
  ◦ Типы оценки уязвимостей
  ◦ Жизненный цикл управления уязвимостями
• Решения по оценке уязвимостей
  ◦ Подходы к оценке уязвимостей
  ◦ Типы инструментов для оценки уязвимостей
  ◦ Характеристики решений
  ◦ Выбор решения по оценке уязвимостей
• Системы оценки уязвимостей
  ◦ Common Vulnerability Scoring System (CVSS)
  ◦ Common Vulnerabilities and Exposures (CVE)
  ◦ National Vulnerability Database (NVD)
  ◦ Ресурсы для исследования уязвимостей
• Инструменты оценки уязвимостей
  ◦ Qualys
  ◦ Nessus
  ◦ GFI LanGuard
  ◦ Nikto
  ◦ OpenVAS
  ◦ Retina CS
  ◦ SAINT
  ◦ MBSA (Microsoft Baseline Security Analyzer)
  ◦ AVDS (Automated Vulnerability Detection System)
• Отчеты по оценке уязвимостей
• **Практическая работа:** Использование Nessus для инвентаризации уязвимостей компьютеров лаборатории
	1

Модуль 6. Хакинг системы
 	
• Архитектура операционной системы
• Слабые точки операционной системы
• Методология хакинга системы
• Последовательность хакинга системы
• Получение доступа к системе
  ◦ Принципы аутентификации
  ◦ Типы атак на пароли
  ▪ Не электронные атаки
  ▪ Активные онлайн-атаки
  ▪ Пассивные онлайн-атаки
  ▪ Офлайн-атаки
  ◦ Инструменты для взлома паролей
  ◦ Эксплуатация уязвимостей
  ◦ Переполнение буфера
• Повышение привилегий
  ◦ Подмена DLL
  ◦ Эксплойты на повышение привилегий
  ◦ Уязвимости Spectre a Meltdown
  ◦ Дальнейшее продвижение
  ◦ Методы защиты от повышения привилегий
• Поддержка доступа к системе
  ◦ Выполнение приложений
  ◦ Кейлоггеры
  ◦ Шпионское ПО
  ◦ Руткиты
  ◦ Альтернативные потоки данных
  ◦ Стеганография
• Скрытие следов
• **Практическая работа:** Применение техник по взлому паролей и повышению привилегий в операционных системах
	3

Модуль 7. Трояны и другое вредоносное ПО
 	
• Обзор вредоносного ПО
• Трояны
  ◦ Концепции троянов
  ◦ Как работают трояны
  ◦ Типы троянов
• Вирусы и черви
  ◦ Работа вируса
  ◦ Типы вирусов
  ◦ Компьютерные черви
• Анализ вредоносного ПО
  ◦ Методы обнаружения вредоносного ПО
• Меры противодействия
• Инструменты защиты от вредоносного ПО
• **Практическая работа:** Тестирование работы шелл-трояна, реверсного трояна, скрытого трояна
	4

Модуль 8. Снифферы
 	
• Концепции сниффинга
  ◦ Как работает сниффер?
  ◦ Типы сниффинга
  ◦ Аппаратные анализаторы протоколов
  ◦ SPAN порт
• Техники активного сниффинга
  ◦ MAC атаки
  ◦ DHCP атаки
  ◦ ARP атаки
  ◦ Спуфинг
  ◦ Отравление кэша DNS
• Инструменты сниффинга
• Меры противодействия сниффингу
• **Практическая работа:** Применение техники активного сниффинга для получения передаваемых по сети данных и подмены запросов
	2

Модуль 9. Социальная инженерия
 	
• Концепции социальной инженерии
• Техники социальной инженерии
  ◦ Без использования компьютеров
  ◦ С использованием компьютеров
  ◦ С использованием мобильных устройств
• Инсайдерские угрозы
• Имперсонация в социальных сетях
• Кража личности
• Меры противодействия социальной инженерии
• **Практическая работа:** Применение набора средств социальной инженерии SET из состава Kali Linux
	1

Модуль 10. Отказ в обслуживании
 	
• Концепции Denial-of-Service
• Что такое DDoS атака
• Техники DoS/DDoS атак
  ◦ Векторы DoS/DDoS атак
  ◦ UDP флуд
  ◦ ICMP флуд
  ◦ Ping of death
  ◦ Smurf атака
  ◦ SYN флуд
  ◦ Фрагментированная атака
  ◦ Slowloris
  ◦ Мульти-векторные атаки
  ◦ DRDoS атаки
• Бот сети
• Пример реализации DDoS атаки
• Инструменты проведения DoS атак
• Меры противодействия DoS атакам
• Инструменты защиты от DoS
• **Практическая работа:** Применение техник проведения DoS атаки для вывода из строя сервисов учебных серверов.
	1

Модуль 11. Перехват сеанса
 	
• Концепции перехвата сеанса
• Процесс перехвата сеанса
• Типы перехвата сеанса
• Техники перехвата сеанса
  ◦ Перехват на прикладном уровне
  ▪ Сниффинг
  ▪ Предсказание идентификатора
  ▪ Атака «Человек посередине»
  ▪ Атака «Человек в браузере»
  ▪ Атаки на клиентов
  ▪ Межсайтовый скриптинг
  ▪ Межсайтовая подделка запросов
  ▪ JavaScript код
  ▪ Трояны
  ▪ Повторение сеанса
  ▪ Фиксация сеанса
  ▪ Использование прокси-серверов
  ▪ Атака CRIME
  ▪ Атака Forbidden
  ◦ Перехват на сетевом уровне
  ▪ Перехват TCP/IP
  ▪ IP спуфинг
  ▪ Подделка RST
  ▪ Перехват вслепую
  ▪ Перехват UDP
  ▪ Подделка ICMP
  ▪ ARP спуфинг
• Инструменты для перехвата сеанса
• Меры противодействия перехвату сеанса
• **Практическая работа:** Применение техник перехвата сеанса для получения доступа к ресурсам учебных серверов
	2

Модуль 12. Обход систем обнаружения вторжений, фаерволлов и систем-ловушек
 	
• Концепции IDS, фаерволлов и Honey Pot
• Системы IDS, фаерволлов и Honey Pot
• Техники уклонение от IDS
  ◦ Добавление данных
  ◦ DoS атаки
  ◦ Обфускация
  ◦ Генерация ложных срабатываний
  ◦ Разделение сеанса
  ◦ Использование Unicode
  ◦ Фрагментация
  ◦ Перекрывающиеся фрагменты
  ◦ Использование TTL
  ◦ Невалидные RST пакеты
  ◦ Флаг срочности
  ◦ Полиморфный и ASCII шелл-код
  ◦ Атаки прикладного уровня
  ◦ Десинхронизация
• Техники обхода фаерволлов
  ◦ Идентификация фаерволлов
  ◦ Спуфинг IP адреса
  ◦ Маршрутизация от источника
  ◦ Микрофрагменты
  ◦ Использование IP в URL
  ◦ Анонимайзеры
  ◦ Прокси-серверы
  ◦ Туннелирование
  ▪ ICMP туннель
  ▪ ACK туннель
  ▪ HTTP туннель
  ▪ SSH туннель
  ▪ DNS туннель
  ◦ Использование внешних систем
  ◦ Обход фаерволла посредством MITM
  ◦ Обход фаерволлов веб-приложений
• Обнаружение Honey Pot
• Инструменты обхода фаерволлов
• Противодействие обходу систем обнаружения и фаерволлов
• **Практическая работа:** Изучение возможностей уклонения от систем обнаружения
	2

Модуль 13. Хакинг веб-серверов
 	
• Концепции веб-серверов
• Типы атак на веб-серверы
• Методология атаки на веб-сервер
• Инструменты взлома веб-серверов
  ◦ Metasploit Framework
  ◦ Взломщики паролей
• Меры противодействия взлому веб-серверов
• Управление исправлениями
• Повышение безопасности веб-серверов
• **Практическая работа:** Дефейс учебного веб-сервера посредством эксплуатации уязвимости с помощью Metasploit Framework
	2

Модуль 14. Хакинг веб-приложений • Концепции веб-приложений • Угрозы веб-приложениям • Классификация OWASP Top 10 • Методология атаки на веб-приложения • Инструменты взлома веб-приложений • Веб API, хуки и шеллы • Меры противодействия взлому веб-приложений • Инструменты защиты веб-приложений • **Практическая работа:** Выполнение отраженной и сохраненной XSS атаки	**4**

Модуль 15. SQL инъекции
 	
• Концепции SQL инъекции
• Тестирование на SQL возможность инъекции
• Типы SQL инъекций
  ◦ SQL инъекция на основе ошибки
  ◦ UNION SQL инъекция
  ◦ Слепая SQL инъекция
• Методология SQL инъекции
• Примеры применения SQL инъекции
• Средства для выполнения SQL инъекции
• Скрытие SQL инъекции от IDS
• Меры противодействия SQL инъекции
• **Практическая работа:** Взлом учебного веб-сервера с помощью SQL инъекций
	2

Модуль 16. Хакинг беспроводных сетей
 	
• Концепции беспроводных сетей
• Шифрование в беспроводных сетях
• Угрозы беспроводным сетям
• Методология взлома беспроводных сетей
  ◦ Обнаружение беспроводных устройств
  ◦ Анализ трафика беспроводных сетей
  ◦ Проведение атаки на беспроводную сеть
  ◦ Взлом шифрования беспроводных сетей
• Инструменты хакинга беспроводных сетей
• Атаки на Bluetooth
• Меры противодействия атакам на беспроводные сети
• Инструменты защиты беспроводных сетей
• **Практическая работа:** Нахождение точек доступа, сниффинг, де-аутентификация, взлом ключей WEP, WPA, WPA2 и расшифровывание Wi-Fi трафика
	2

Модуль 17. Хакинг мобильных платформ • Векторы атаки на мобильные платформы • Взлом Android OS • Техники и инструменты получения прав администратора Android • Взлом iOS • Техники и инструменты джейлбрейка • Шпионское ПО для мобильных платформ • Управление мобильными устройствами • Инструменты и рекомендации по защите мобильных устройств • **Практическая работа:** Изучение инструментов для проведения атак на мобильные устройства	**1**

Модуль 18. Хакинг интернета вещей и операционных технологий
 	
• Интернет вещей
  ◦ Концепции IoT
  ◦ Атаки на IoT
  ◦ Методология хакинга IoT
  ◦ Инструменты хакинга IoT
  ◦ Меры противодействия хакингу IoT
• Операционные технологии
  ◦ Концепции OT
  ◦ Атаки на OT
  ◦ Методология хакинга OT
  ◦ Инструменты хакинга OT
  ◦ Меры противодействия хакингу OT
• **Практическая работа:** Изучение уязвимостей интернета вещей и операционных технологий
	1

Модуль 19. Облачные вычисления
 	
• Введение в облачные вычисления
• Типы облачных сервисов
• Контейнерные технологии
  ◦ Контейнеризация и виртуальные машины
  ◦ Докеры и микросервисы
  ◦ Что такое Kubernetes
  ◦ Проблемы безопасности контейнеров
  ◦ Платформы управления
• Бессерверные вычисления
• Угрозы облачных вычислений
• Атаки на облака
  ◦ Перехват сервиса с использованием социальной инженерии
  ◦ Перехват сеанса с использованием XSS
  ◦ Атаки на DNS
  ◦ SQL инъекции
  ◦ Атака wrapping
  ◦ Перехват сервиса с использованием сниффинга
  ◦ Перехват сеанса через захват сеанса
  ◦ Атака по сторонним каналам
  ◦ Атаки на криптографию
  ◦ Атаки на отказ в обслуживании
• Хакинг облачных технологий
• Безопасность в облаке
• Инструменты защиты облачных вычислений
• Тестирование на проникновение в облака
• **Практическая работа:** Изучение атак на облака и инструментов защиты облачных вычислений
	2

Модуль 20. Криптография
 	
• Концепции криптографии
• Алгоритмы шифрования
  ◦ Шифры
  ◦ Data Encryption Standard (DES)
  ◦ Advanced Encryption Standard (AES)
  ◦ RC4, RC5 и RC6
  ◦ Twofish
  ◦ DSA и схемы подписи
  ◦ Rivest Shamir Adleman (RSA)
  ◦ Diffie-Hellman
  ◦ Функции хэширования
  ▪ MD2, MD4, MD5
  ▪ SHA0, SHA1, SHA2, SHA3
  ▪ PREMID-160
  ▪ HMAC
• Криптографические средства
• Инфраструктура открытых ключей
• Шифрование почты
• Шифрование диска
• Инструменты шифрования диска
• Криптоанализ
  ◦ Методы криптоанализа
  ◦ Методы взлома ключей
  ◦ Атаки на криптографию
  ▪ Метод «грубой силы»
  ▪ Использование парадокса дней рождений
  ▪ «Человек посередине» в схемах с цифровой подписью
  ▪ Атака по побочным каналам
  ▪ Коллизия хэшей
  ▪ Атака DUHK
  ▪ Радужные таблицы
  ▪ Атака Padding Oracle
  ▪ Атака DROWN
• Средства криптоанализа
• Меры противодействия
• **Практическая работа:** Изучение алгоритмов шифрования и средств стеганографии
	2

Модуль 21. Дополнительные материалы • Руководство к выполнению лабораторных работ • Подборка сайтов посвященных этичному хакингу • Выполнение дополнительных задач на лабораторном стенде	
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