Аудит безопасности - Часть 1

Код: SECR-002

Длительность: 40 ч.

Описание:

В рамках данного курса слушатели получат представление о разных способах и методах атак на корпоративные сети и другие информационные ресурсы; рассматривается сама концепция взлома и защиты от него в рамках различных технологий и инструментов, применяемых PEN-тестерами (аудиторами безопасности).

Данный курс рассчитан на системных администраторов и специалистов по информационной безопасности компаний, которые хотят получить комплексную картину по инструментам вторжения и защите от него, подготовив свою компанию к внутреннему аудиту безопасности.

Цели:

Курс знакомит слушателей с концепциями, технологиями и инструментами, применяемыми при тестировании на проникновение хакера и для выявления инсайдерской активности.

Разбираемые темы:

Введение

- Компетенции аудитора безопасности
- Виды хакерской активности
- Эволюция хакинга
- Что атакуют?

Сбор информации

- Утечки
- Поиск через сервисы Whois
- Сбор данных через DNS
- Использование расширенного поиска Google
- Противодействие сбору данных
- Лабораторная работа №1 — Утечки
- Практическое задание — сбор данных о человеке из открытых источников
- Семинар по противодействию сбору данных

Социальная инженерия

- Методы социальной инженерии
- Обратная социальная инженерия
- Противодействие социальной инженерии
- Семинар по методам социальной инженерии

Сканирование

- Цели сканирования сети
- Методы сканирования
- Определение топологии сети
- Определение доступных хостов и получение списка сервисов для каждого из них
- Определение операционной системы для каждого из доступных узлов сети
- Поиск потенциально уязвимых сервисов
- Противодействие сканированию
- Использование TOR
- Другие техники туннелирования
- Лабораторная работа №2 — Сканирование

Перечисление

- DNS zone transfer
- SNMP
- Пользователи Windows
- Группы Windows
- Противодействие перечислению

Переполнение буфера

- Stack-based Buffer Overflow
- Heap-Based Buffer Overflow
- Overflow using Format String
- Противодействие переполнению буфера
- DEP (Data Execution Preventer)
- ASLR (Address Space Layout Randomization)
- PAX + GRSecurity
- Лабораторная работа №3 — Переполнение буфера

Отказ в обслуживании (DoS и DDoS)

- Цель DoS-атаки
- Как проводится DDoS-атака
- Ботнеты
- Признаки DoS-атаки
- Обнаружение DoS-атак
- Противодействие DDoS/DoS-атакам
- Противодействие ботнетам

Вирусы и Черви

- Признаки вирусной атаки
- Полиморфные вирусы
- Противодействие вирусам

Трояны и бэкдоры

- Проявления активности троянов
- Определение троянов
- Противодействие троянам

Снифферы

- Цели применения снифферов
- Протоколы, уязвимые для прослушивания
- Противодействие прослушиванию
- Лабораторная работа №4 — Снифферы
- Лабораторная работа №5 — Протоколы, уязвимые для прослушивания

Перехват сеанса

- Атака «Человек посередине»
- Hijacking
- Spoofing
- Сравнение Hijacking и Spoofing
- Захват сеанса
- Противодействие перехвату

SQL-инъекция

- Как работают web-приложения
- SQL-инъекция
- Тестирование защиты от SQL-инъекций
- Лабораторная работа №6 — SQL-инъекция

Криптография

- Стандарты шифрования
- Симметричные криптоалгоритмы
- Ассиметричные шифры
- Криптографические хэш-функции
- Инфраструктура открытых ключей (PKI)
- SSL/TLS
- SSH
- ЭЦП
- Взлом шифрования

Хакинг системы

- "Домашняя работа" перед взломом
- Проникновение в корпоративную сеть
- Методы взлома паролей
- Прослушивание сессии
- Противодействие взлому
- Лабораторная работа №7 — Атака по словарю и перебором

Хакинг Web-серверов

- Особенности web-серверов
- Использование сообщений об ошибках
- Эксплойты
- Атаки на стороне клиента
- Защита web-серверов
- Лабораторная работа №8 - Эксплойты

Хакинг Web-приложений

- Специфика Web-приложений
- Межсайтовый скриптинг
- Использование обработчиков ошибок
- Некриптостойкое хранение
- Управление сессией и аутентификацией
- Атаки на web-сервисы
- Взлом Web App
- Анализ уязвимостей web-приложений
- Защита web-приложений

Хакинг беспроводных сетей

- Стандарты беспроводной связи
- Типы шифрования беспроводных соединений
- Прослушивание IP-адресов
- Противодействие взлому беспроводных сетей

Обход IDS и Honeypot

- Система обнаружения вторжений (IDS)
- Определение типа брандмауэра
- Техники обхода брандмауэров
- Обход брандмауэра через Proxy
- Honeypot

Тестирование на проникновение

- Оценка безопасности и уязвимостей
- Тестирование на проникновение
- Порядок тестирования
- Методы тестирования
- Что тестируется
- Тестирование web-приложений
- Лабораторная работа №9 — Тестирование на проникновение

Целевая аудитория:

Системные администраторы и специалисты по защите информации.

Предварительная подготовка – общее:

Курсы по администрированию Windows и Unix-систем или аналогичный опыт.

Рекомендуемые дополнительные материалы, источники:

Раздаются на курсе