Аудит безопасности - Часть 2

Код: SECR-003

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 является логическим продолжением 1 части и предназначен для практического закрепления полученных навыков и уверенного их применения в своей работе.

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:

Практическое закрепление знаний, полученных на курсе SECR-002 «Аудит безопасности - Часть 1», и способность уверенно их применять.

Разбираемые темы:

Внимание! Весь курс сугубо практический, вся теория и инструменты изучаются в 1-й части курса, а потому она строго обязательна.

Подготовка и настройка виртуальных машин

- Настройка Windows Server 2008 R2
- Настройка Backtrack/Kali Linux
- Импорт и развертывание жертвы для взлома на платформе Linux
- Импорт и развертывание жертвы для взлома повышенной сложности (используется для взлома виртуальной корпоративной сети)

Взлом хоста на платформе Linux

- Сканирование

- Проверка на наличие Web-приложений
- Проверка на возможность взлома Web-приложений
- Выявление потенциально уязвимых сервисов
- Использование Metasploit для проверки существующих уязвимостей
- Подготовка отчета о результатах тестирования
- Подготовка рекомендаций по устранению найденных недостатков
- Разбор полетов в режиме семинара

Защита хоста на платформе Linux

- Применение сетевого суперсервера для ограничения доступа к сервисам
- Использование политик безопасности SELinux/AppArmor в Linux, MAC во FreeBSD
- Виртуализация серверов с использованием технологий OpenVZ/LXC в Linux и Jail во FreeBSD
- Виртуализация приложений путем совмещения помещения сервисов в Chroot и применения к ним политик безопасности

Взлом сетевого узла на платформе Windows

- Сканирование
- Выявление потенциально уязвимых сервисов
- Использование Metasploit для проверки существующих уязвимостей
- Подготовка отчета о результатах тестирования
- Подготовка рекомендаций по устранению найденных недостатков
- Разбор полетов в режиме семинара

Защита сетевого узла на платформе Windows

- Усиление политик безопасности там, где не требуется совместимость с предыдущими версиями Windows
- Виртуализация серверов с использованием технологии Hyper-V
- Виртуализация приложений с использованием технологии App-V (ранее SoftGrid)
- Использование службы управления правами (AD RMS)

Проникновение в локальную сеть компании

- Сбор данных с сайта компании

- Проверка корпоративного сайта на подверженность веб-уязвимостям
- Тестирование на возможность раскрытия данных с сайта компании
- Сканирование доступных ресурсов компании
- Выявление потенциально уязвимых сервисов
- Проверка потенциально уязвимых сервисов на предмет возможности эксплуатации уязвимостей
- Проникновение через найденные уязвимости
- Использование полученного доступа для дальнейшего проникновения
- Повторение этого списка шагов, пока не будет получен полный доступ ко всем сетевым узлам корпоративной сети
- Подготовка отчета о результатах тестирования
- Подготовка рекомендаций по устранению найденных недостатков
- Разбор полетов в режиме семинара

Практическая работа — Установка и настройка EMET (Enhanced Mitigation Experience Toolkit) на Windows 2008 R2

Бонус (для быстрых групп слушателей):

- Практическая работа — сборка Сборка и настройка ядра Linux с патчами GRSecurity и Pax

Целевая аудитория:

Системные администраторы и специалисты по защите информации, окончившие курс SECR-002 «Аудит безопасности - Часть 1» и решившие на практике закрепить полученные знания.

Рекомендуемые дополнительные материалы, источники:

Раздаются на курсе