САИБ

Базовые методы тестирования на проникновение

+7 (383) 255 32 55 info@saib.biz saib.biz

saib.biz
info@saib.biz
+7 (383) 255 32 55

Аннотация

На сегодняшний момент хороший специалист в области защиты информации, помимо обеспечения защиты корпоративных ресурсов организации, должен и уметь осуществлять взлом информационных систем – так называемое тестирование на проникновение, с целью моделирования действий злоумышленника. Это необходимо для понимания актуальной ситуации по существующим изъянам и уязвимостям в своей системе, своевременного реагирования на них и модернизации системы защиты информации.

Данный курс направлен на изучение специалистами наиболее популярных инструментов тестирования на проникновения с целью получения практического опыта их использования в собственной инфраструктуре.

Материла курса состоит из презентационного материла и видеозаписей, с рассмотрением наиболее популярных векторов атак при использовании изучаемых, в рамках курса, инструментов тестирования.

saib.biz
info@saib.biz
+7 (383) 255 32 55

Содержание курса

Поиск информации в открытых источниках
В этом разделе вы ознакомитесь с понятием Open Source Intelligence, получите знания об открытых источниках информации. Ознакомитесь с инструментами, которые используют специалисты при поиске информации в открытых источниках.

Поиск учетных записей, почтовых адресов
В данном разделе мы рассмотрим инструменты для автоматизации поиска учетных записей и почтовых адресов организации, такие как hunter.io и harvester.

Поиск поддоменов, анализ структуры организации
Вы научитесь проводить первичный анализ структуры организации, работать с утилитами DNS Recon, dnsdumpster.com, выявлять наиболее уязвимые узлы и составлять первичные векторы атак.

Поиск информации с помощью поисковых запросов
Этот раздел включает в себя общую информацию о запросах в поисковых системах, методологию работы с Google Dork Queries, а также разбор баз данных запросов google-hacking-database.

САИБ

Базовые методы тестирования на проникновение

saib.biz
info@saib.biz
+7 (383) 255 32 55

Сканирование уязвимостей

В ходе этого курса мы рассмотрим эксплуатацию, установку, разбор результатов наиболее популярного сканера уязвимостей - Nessus.

Поиск уязвимостей в WEB приложениях

В данном курсе мы изучим методики обнаружения уязвимостей в WEB приложениях. Ознакомимся с популярным сканером WEB приложений OWASP ZAP, а также рассмотрим узконаправленные инструменты wpscan, joomscan и их аналоги.

Утилиты для работы с паролями и словарями

Данный подкурс объясняет, как работать с инструментами составления словарей, с инструментами перебора логинов и паролей для авторизации. В ходе этого курса будут рассмотрены следующие инструменты: Crunch, Patator, Hashcat, JohnTheRipper.

Metasploit framework

Обзор популярного фреймворка для поиска и эксплуатации уязвимостей. В ходе этого курса мы рассмотрим установку, основные команды, результаты и разберем популярные способы использования этого инструмента.

САИБ

Базовые методы тестирования на проникновение

saib.biz
info@saib.biz
+7 (383) 255 32 55

Covenant

Covenant - современный пост-эксплутационный фреймворк, использующий возможности .NET и написанный на C#. Covenant, как и любой C2-фреймворк, используется для стадии закрепления, повышения привилегий и дальнейшего продвижения в сети, но при этом не использует PowerShell и обладает возможностью динамической компиляции своей полезной нагрузки.
В данном курсе рассматриваются основные возможности фреймворка, модули и их эксплуатация для повышения привилегий и разведки в сети Active Directory.

Социальная инженерия

В данном курсе вы научитесь проводить первоначальный анализ структуры организации на наличие в ней слабых звеньев, которые будут использоваться в будущих векторах атак. Мы рассмотрим способы подбора доменного имени, варианты фишинговых сообщений, а также доставку и маскировку полезной нагрузки.


САИБ