

[Оглавление]

Введение в курс

1. О чем это курс
2. Начальные требования
3. Чему вы научитесь
4. Вкратце по всем главам

Подготовка рабочего окружения

1. Kali linux
2. Знакомство со средой
3. Раскатка уязвимых образов

Общая теория

1. Что такое пентест
2. Что такое аудит
3. Фазы пентестинга (сбор информации, пассивный анализ, активный анализ, подготовка отчетов, устранение)
4. Основы понимания механизмов веб окружения. (HTTP)
 - 4.1 *****
 - 4.2 *****
 - 4.3 *****
 - 4.4 *****
 - 4.5 *****
 - 4.6 *****
5. Классификаторы уязвимостей OWASP, WASC, CVE, CVSS
6. Методологии пентеста: NIST, ISSAF, PTF и др.
7. Экскурс в мир хека (реверсинг, бинарщина, веб, ИнфарПентест, АСУТП, вардрайвинг и др.)
8. Сети и протоколы. Стеки OSI, TCP/IP. Основные сетевые протоколы.
9. Вирусы. История, типы распространения, типы нагрузки.

1. *****
2. *****
- *****
10. *****
11. *****

1. *****
2. *****

Уязвимости

1) Инъекции

1. Sql injection
2. Server Side Template Injection

3. XXE

4. CMD Injection

5. Php injection

6. *****
7. *****
8. *****
9. *****
10. *****
11. *****
12. *****
13. Python, Ruby и Perl
14. File Upload tricks

2) Уязвимые компоненты

3) Обход Авторизации

1. *****
2. *****
3. *****
4. *****
5. *****
6. *****

4) Мисконфигурейшены

1. *****
2. *****

3. *****

5) Клиентские атаки

1. *****

1.1. *****

1.2. *****

1.3. *****

1.4. *****

1.5. *****

2. CSRF

3. Bypass CSP

4. CSTI

5. Open Redirect

6. CSS INjection

6) Системные уязвимости

7) SSRF

1. *****

2. *****

3. *****

Инструментальные средства

1. Kali linux

2. Утилиты

3. Метасплоит

4. PowerSploit

5. BurpSuite

1. *****

2. *****

3. *****

Сертификация и литература

1. OSCP, OSCE, СЕН

2. Сети

3. Программирование

4. Книги по хакингу НАОЕ