Кейс 1: Сканирование сетей и выявление открытых портов

Задание:

1. Использовать инструмент Nmap для сканирования заданного IP-диапазона.
2. Определить активные устройства и открытые порты.

Ожидаемый результат:

- Сканирование выполнено, активные устройства и открытые порты выявлены и задокументированы.

Кейс 2: Поиск уязвимостей с помощью Nessus

Задание:

1. Установить и настроить Nessus на локальной машине.
2. Выполнить сканирование уязвимостей на заданном сервере.
3. Проанализировать результаты и задокументировать найденные уязвимости.

Ожидаемый результат:

- Сканирование выполнено, уязвимости выявлены и задокументированы.

Кейс 3: Эксплуатация уязвимостей с Metasploit

Задание:

1. Использовать Metasploit для выполнения атак на найденные уязвимости.
2. Выполнить успешную эксплуатацию одной из уязвимостей и получить доступ к системе.

Ожидаемый результат:

- Уязвимость успешно эксплуатирована, доступ к системе получен.

Кейс 4: Тестирование веб-приложений на уязвимости

Задание:

1. Использовать инструмент Burp Suite для анализа безопасности веб-приложения.
2. Выполнить тестирование на уязвимости, такие как SQL-инъекции, XSS и CSRF.

Ожидаемый результат:

- Уязвимости в веб-приложении выявлены и задокументированы.

Кейс 5: Атаки на пароли

Задание:

1. Использовать инструмент Hydra для выполнения брутфорс-атаки на службу SSH.
2. Попытаться получить доступ к системе с помощью подобранного пароля.

Ожидаемый результат:

- Атака выполнена, доступ к системе получен или подтверждено, что пароли надежны.

Кейс 6: Социальная инженерия

Задание:

1. Разработать фишинговую атаку, направленную на получение учетных данных пользователя.
2. Провести симуляцию атаки и проанализировать результаты.

Ожидаемый результат:

- Фишинговая атака разработана и проведена, результаты проанализированы.

Кейс 7: Обход антивирусного ПО

Задание:

1. Создать вредоносное ПО, которое может обойти антивирусные системы (с использованием Veil или аналогичных инструментов).
2. Проверить успешность обхода на тестовой системе с установленным антивирусом.

Ожидаемый результат:

- Вредоносное ПО создано и успешно обошло антивирусное ПО.

Кейс 8: Анализ логов и выявление атак

Задание:

1. Использовать инструмент ELK Stack (Elasticsearch, Logstash, Kibana) для сбора и анализа логов с сервера.
2. Проанализировать логи и выявить возможные атаки.

Ожидаемый результат:

- Логи проанализированы, атаки выявлены и задокументированы.

Кейс 9: Создание безопасной инфраструктуры

Задание:

1. Спроектировать и настроить безопасную сетевую инфраструктуру с использованием брандмауэров и VPN.
2. Провести тестирование безопасности созданной инфраструктуры.

Ожидаемый результат:

- Сетевая инфраструктура настроена, тестирование безопасности проведено.

Кейс 10: Защита от DDoS атак

Задание:

1. Смоделировать DDoS атаку на веб-сервер.
2. Реализовать меры защиты и смягчения последствий атаки (например, с использованием Cloudflare).

Ожидаемый результат:

- DDoS атака смоделирована, меры защиты реализованы и протестированы.