Домашнее задание

Дисциплина	Технологии детектирования атак и управления инцидентами
Тема	Тестирование на проникновение LAN и Wi-Fi-сетей
Форма проверки	**Самопроверка. Студент выполняет задание и самостоятельно проверяет его с помощью чек-листа. Домашнее задание является факультатиыным и не будет учитываться в итоговой оценке за дисциплину**
Имя преподавателя	Геннадий Шастин
Время выполнения	120 минут
Цель задания	Получение навыков в использовании утилит Wifite2 и пакета aircrack-ng для реализации атак на Wi-Fi-сети
Инструменты для выполнения ДЗ	Google Docs / Яндекс документы, Kali Linux, домашний Wi-Fi-роутер, Wi-Fi-адаптер, Wifite2, airmon-ng, airodump-ng, aireplay-ng, aircrack-ng
Правила приёма работы	1. Выполните все пункты задания. 2. Подготовьте отчёт о тестировании домашней Wi-Fi-сети 3. Загрузите файл с отчётом на Google Диск / Яндекс диск и прикрепите ссылку на файл с выполненным заданием в личный кабинет. Важно: убедитесь, что по ссылке есть доступ. Название файла должно содержать фамилию и имя студента, номер ДЗ
Критерии оценки	**Задание считается выполненным, если:** прикреплена ссылка на файл с выполненным заданием; доступ к материалам открыт; выполнены требования чек-листа самопроверки. **Задание не выполнено, если:** файл с заданием не прикреплён или отсутствует доступ по ссылке
Дедлайн	Срок сдачи — 7 рабочих дней после вебинара

Описание задания

Перед выполнением задания:

- посмотрите запись вебинара по теме 9 «Тестирование на проникновение LAN и Wi-Fi-сетей»;
- установите утилиты wifite2 и пакет утилит aircrack-ng отдельно или в составе дистрибутива Kali Linux: wifite2, aircrack-ng, Kali Linux;
- потребуется внешний USB Wi-Fi-адаптер, если Kali Linux установлен как виртуальная машина.

Задание 1
Преднастройки: на домашнем Wi-Fi-роутере включите WPS (если выключено).

Заказчик попросил вас выполнить тестирование служебной Wi-Fi-сети в ресторане. Вы приехали на место и выяснили, что на роутере включена авторизация при помощи WPS.

Необходимо:

1.1. При помощи утилиты Wifite2 выполнить атаку на домашнюю сеть с WPS и успешно к ней подключиться, используя атаку Pixie Dust или подбор PIN.

1.2. Подготовить отчёт с описанием выполненных действий, скриншотами и рекомендациями по повышению защищённости Wi-Fi-сети.

Важно: в отчёте обязательно опишите риски: чем опасно для организации использование WPS и какие действия необходимо выполнить для отключения WPS. Приложите скриншоты.

Задание 2
Преднастройки: на домашнем Wi-Fi-роутере для Wi-Fi-сети включите WPA/WPA2 и установите простой PSK-ключ, например, «qwerty123» или «1234567890».

Заказчик снова попросил вас выполнить тестирование служебной Wi-Fi-сети в ресторане, чтобы проверить, насколько эффективно были реализованы рекомендации по повышению защищённости Wi-Fi-сети. Вы обнаружили, что ваши рекомендации были выполнены и WPS на роутере выключен. Вы принимаете решение о дальнейшем тестировании сети.

Необходимо:

2.1. При помощи набора утилит airmon-ng, airodump-ng, aireplay-ng и aircrack-ng перехватить хендшейк — авторизацию клиента на точке доступа.

Важно: для этого может потребоваться отправка deauth-пакетов и затем PSK к

сети при помощи aircrack-ng.

2.2. Подготовить отчёт с описанием выполненных действий и рекомендациями по повышению защищённости Wi-Fi-сети.

Чек-лист самопроверки

№ п/п	Критерии выполнения задания	Отметка о выполнении
1.1	Выполнены преднастройки: на домашнем Wi-Fi-роутере включён WPS	
1.2	Запущена утилита Wifite2, в качестве фильтра указано «только сети с поддержкой WPS»	
1.3	Запущена атака на сеть из пункта 1.1 и получен результат	
1.4	При успешной атаке удалось получить PIN и успешно подключиться к домашней Wi-Fi-сети из пункта 1.4	
1.5	Подготовлен отчёт: ● описаны действия, выполненные для реализации атаки на домашнюю сеть; ● Представлены скриншоты результатов атаки; ● Предложены рекомендации по улучшению защищённости Wi-Fi-сети	
2.1	Выполнены преднастройки: на домашнем Wi-Fi-роутере для Wi-Fi-сети включён WPA/WPA2 и установлен простой PSK-ключ	
2.2	Wi-Fi-адаптер переведён в неразборчивый режим	
2.3	Запущен airodump-ng и выполнен перехват пакетов для вашей сети из пункта 2.1	
2.4	С помощью aireplay-ng отправлен deauth-пакет выбранному клиенту. Например, на свой	

	мобильный телефон, подключённый к сети из пункта 2.1	
2.5	С помощью aircrack-ng получен ключ (PSK) для доступа в сеть из пункта 2.1	
2.6	При помощи ключа (PSK) выполнено успешное подключение к сети из пункта 2.1	
2.7	Подготовлен отчёт: ● описаны действия, выполненные для реализации атаки; ● представлены скриншоты результатов атаки; ● предложены рекомендации по улучшению защищённости Wi-Fi-сети	
3.1	В личном кабинете прикреплена ссылка на файл с отчётом	
3.2	Файл доступен для просмотра другим пользователям, название файла содержит фамилию и имя студента, номер ДЗ	