Задание 1:

Написать небольшую программу демонстрирующую работу с операторами языка Си, работу с адресной арифметикой, вызов функций. Скомпилировать под архитектуры ARMv7 и ARMv8. Проанализировать полученные программы с использованием IDA Pro или Ghidra и разобраться в какие ассемблерные инструкции скомпилировался код. В качестве решения необходимо предоставить:

1. Исходный код программы
2. Название компилятора/среды разработки и описание того, как производилась сборка программы, а также непосредственно скомпилированную программу
3. Небольшой отчет с описанием того, во что скомпилировался исходный код (сопоставление кода и ассемблерным инструкциям)

Задание 2:

Написать небольшую программу, в которой будет функция, реализующая пузырьковую сортировку массива целых чисел. Скомпилировать под архитектуры ARMv7 и ARMv8. Проанализировать полученные программы с использованием IDA Pro или Ghidra. Пропатчить функцию сортировки, заменив её на функцию, которая просто умножает все элементы массива на 8. В качестве решения необходимо предоставить:

1. Исходный код программы
2. Название компилятора/среды разработки и описание того, как производилась сборка программы, а также непосредственно скомпилированную программу
3. Пропатченную программу и небольшой отчет с описанием того, как производился патчинг

Задание 3:

Для прошивки/восстановления/диагностики Android устройств на базе SoC MediaTek (MTK) есть специальная утилита SP Flash Tool. При подключении выключенного MTK устройства к ПК на одну секунду появляется COM-порт и если за это время к нему подключится, то становится возможным взаимодействие с устройством по низкоуровневому протоколу через COM-порт. SP Flash Tool на вкладке Readback позволяет вызвать функцию чтения ROM. Необходимо настроить сниффер COM-порта и захватить трафик взаимодействия с устройством в процессе чтения первых 0x10000 байтов ROM. Затем необходимо написать программу на Python, которая повторит все действия SP Flash Tool и прочитает первые 0x10000 байтов ROM. То есть необходимо просто захватить трафик COM-порта и просто повторить последовательность на Python.

Устройство для выполнения задания предоставляется компанией. В качестве решения необходимо предоставить:

1. Захваченный трафик
2. Первые 0x10000 байтов ROM
3. Python скрипт
4. Небольшой отчет с описанием хода выполнения задания, что было сделано, какие возникли трудности и как они решались