



仙台CTF2018 セキュリティ技術競技会(CTF)

問題解説 OT/IoT

平成30年11月10日

仙台CTF推進プロジェクト

目黒 有輝

戸羽 秀人

Q1. HMIとPLC間の制御プロトコルを特定して下さい

- sshでEWSにログインし、tcpdumpでパケットをスニフ。pcap形式で保存。
- pcapファイルをscp等でコピーした後、Wiresharkで開いてプロトコルを確認。

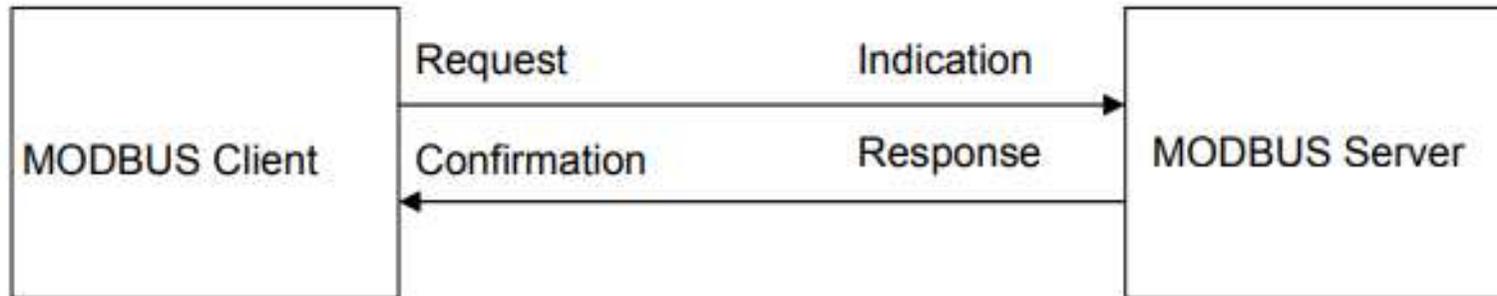
適用します

Source	Destination	Protocol	Length	Info
192.168.30.110	192.168.30.6	Modbus/TCP	64	Response: Trans: 690...
192.168.30.6	192.168.30.110	Modbus/TCP	66	Query: Trans: 690...
192.168.30.110	192.168.30.6	TCP	60	502 → 47635 [ACK] Seq...
192.168.30.110	192.168.30.6	Modbus/TCP	64	Response: Trans: 690...
192.168.30.6	192.168.30.110	Modbus/TCP	66	Query: Trans: 690...
192.168.30.110	192.168.30.6	TCP	60	502 → 47635 [ACK] Seq...
192.168.30.110	192.168.30.6	Modbus/TCP	64	Response: Trans: 690...
192.168.30.6	192.168.30.110	Modbus/TCP	66	Query: Trans: 690...

FLAG「modbus/tcp」

(参考)Modbus/TCPとは

- Modbusとは米Modicon社により開発された、PLC用のネットワークプロトコル。
- 仕様は公開されており、制御システムで汎用的に採用されている。



http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

Q2. 照明機能を制御するためのPLCレジスタを特定して下さい

- Modbus/TCPプロトコルのパケットを観察すると、1種類のレジスタに対して連続的にRead命令が行われていることが分かる。
- QueryのReference Numberを確認する。

```
▷ Internet Protocol Version 4, Src: 192.168.30.6, Dst: 192.168.30.110
▷ Transmission Control Protocol, Src Port: 47635, Dst Port: 502, Seq: 13, Ack: 21, Len: 12
▾ Modbus/TCP
  Transaction Identifier: 6903
  Protocol Identifier: 0
  Length: 6
  Unit Identifier: 1
▾ Modbus
  .000 0001 = Function Code: Read Coils (1)
  Reference Number: 3048
  Bit Count: 1
```

FLAG「3048」



Q3. 照明機能を復旧させ、復旧させた様子を監視カメラで確認して下さい

- ヒントファイルを参考に、Pythonで簡易Modbusクライアントを作成。
- 宛先IPアドレスはPLC、宛先ポート番号は502番、ペイロード部分には、Write Single Coilのパケット(Q2のヒントファイルに記載されていたペイロード)を転記。
- 作成したPythonプログラムを実行させると照明が3秒間点灯し、明るくなったことで監視カメラ越しに見えたQRコードを読み込むとフラグが確認できる。

```
import socket

client = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
client.connect(("192.168.30.110", 502))
client.send(b"\x00\x03\x00\x00\x00\x06\x01\x05\x0b\xe8\xff\x00")
modbus_client.py (END)
```



FLAG「OK_GOOGLE_DENKI_WO_TSUKETE」