ICS kwetsbaarheden: Appendix omtrent hardware en protocollen

Ing. Tijl Deneut
Lecturer Applied Computer Sciences Howest
Researcher XiaK, Ghent University

UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

KU LEUVEN

XiaK

Appendix?

Binnen het project is de boodschap duidelijk

Heel wat kwetsbaarheden in standaard OEMs gevonden:

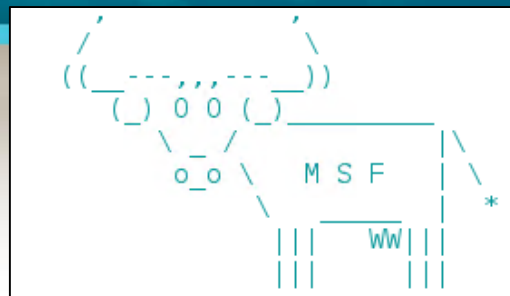
- Beckhoff: CVE-2014-9195, veiliger na update
- Siemens: CVE-2016-6204, veiliger na update
- PhoenixContact: beweging naar OpenVPN, Raspberry Pi

Recenter werk?

- Beckhoff scan script

https://github.com/tijldeneut/ICSSecurityScripts

- Siemens toegevoegd aan Metasploit
- PhoenixContact toegevoegd aan Metasploit

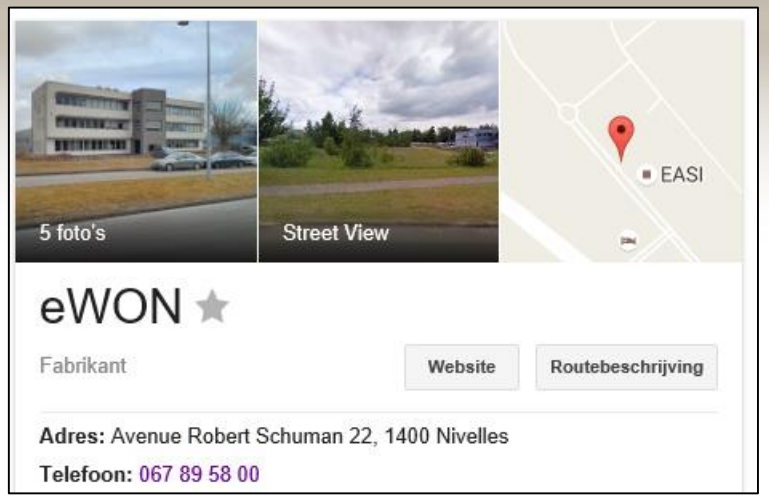



```
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.12.6-dev                          ]
+ -- --=[ 1549 exploits - 896 auxiliary - 267 post        ]
+ -- --=[ 438 payloads - 38 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search tijl

Matching Modules
================

   Name                                      Disclosure Date  Rank    Description
   ----                                      ---------------  ----    -----------
   auxiliary/admin/scada/phoenix_command     2015-05-20       normal  PhoenixContact PLC Remote START/STOP Command
   auxiliary/scanner/scada/siemens                            normal  Siemens Profinet Scanner
```

Appendix A

Op algemene aanvraag:

eWon Security Review



→ eWon Flexy Modular Router

UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

KU LEUVEN

Xiak

eWon Flexy Features

- Basis = 4 switch poorten (LAN)

  inclusief ook eigen DI's & DO's

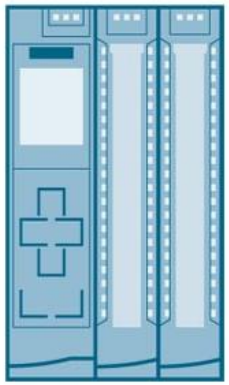
- Modulair systeem met modules voor
  - Serieel, RJ45 WAN, WiFi, 3G …

- Getest als router (WAN + LAN + VPN)
  inclusief OPC functionaliteit (Siemens S7)

Scenario

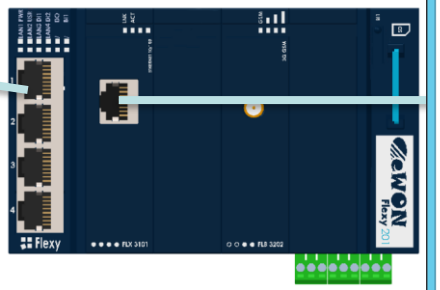
Interne kant
Intranet

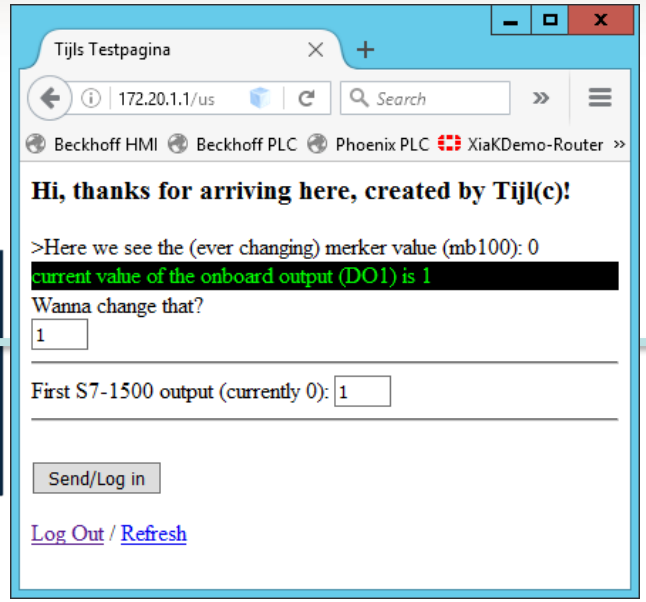
Externe kant
Internet



S7-1500

S7Comm





Webpagina
Op de router

PC

UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

KU LEUVEN

XiaK

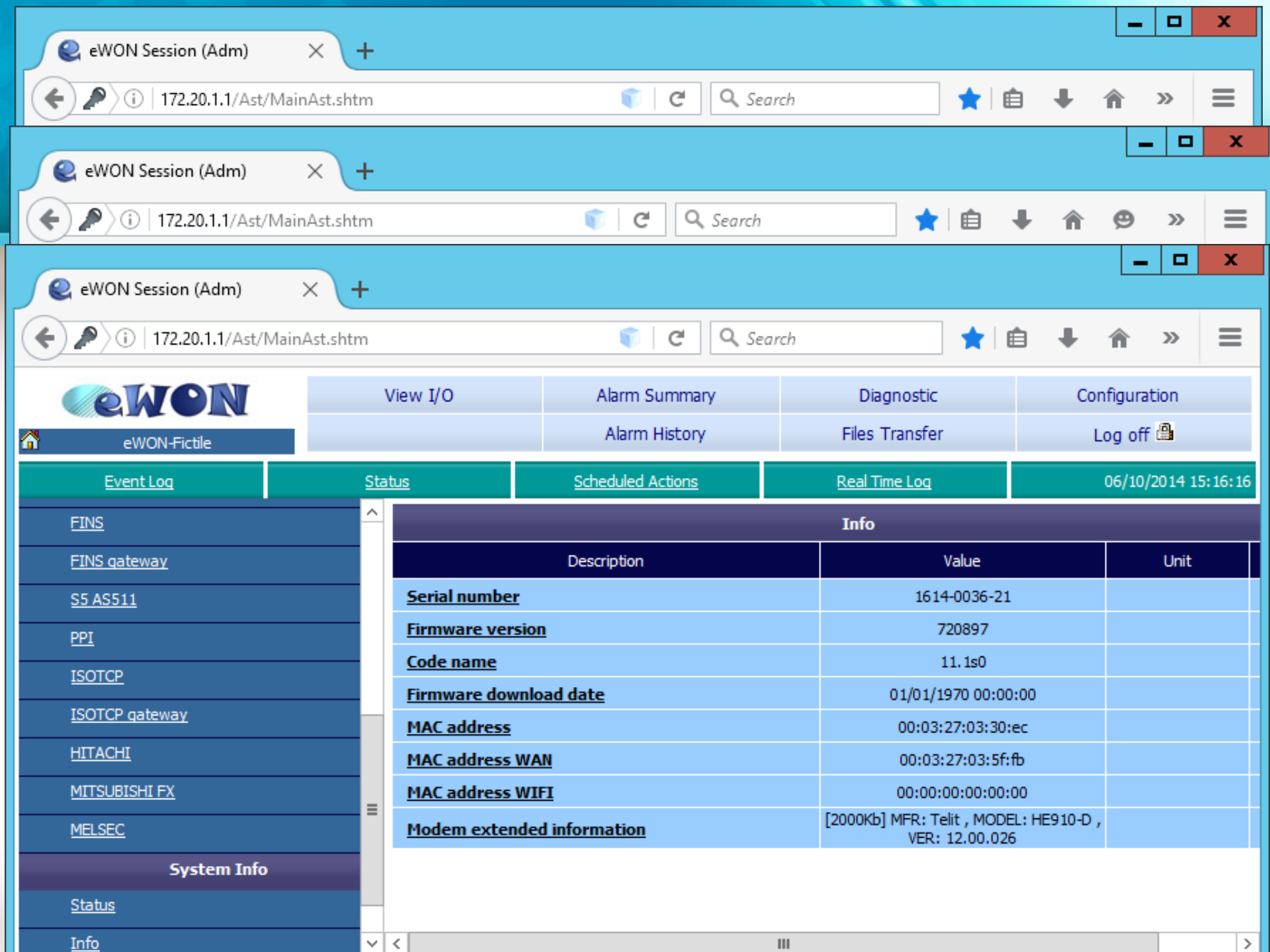
Functionele beperkingen

- Geen DHCP server functionaliteit
- Slechts één WAN-poort mogelijk
  (m.a.w. RJ45 óf 3G, niet beide)
- Eigen VPN implementatie
  (gebaseerd op OpenVPN, maar niet compatibel)

eWon security research

De zogenaamde *attack surface* is zeer groot:

- Zeer veel poorten en features, die ook nog eens open staan: FTP, SNMP, HTTP (op 2 poorten), SMTP, NTP …
- De beheerderswebsite ziet er verouderd uit en bevat tal van fouten
- Veel is afhankelijk van de veiligheid van de **zelfgemaakte** website


eWON Session (Adm)
172.20.1.1/Ast/MainAst.shtm
Search
eWON Session (Adm)
172.20.1.1/Ast/MainAst.shtm
Search
eWON Session (Adm)
172.20.1.1/Ast/MainAst.shtm
Search
eWON
View I/O
Alarm Summary
Diagnostic
Configuration
eWON-Fictile
Alarm History
Files Transfer
Log off
Event Log
Status
Scheduled Actions
Real Time Log
06/10/2014 15:16:16
FINS
FINS gateway
S5 AS511
PPI
ISOTCP
ISOTCP gateway
HITACHI
MITSUBISHI FX
MELSEC
System Info
Status
Info
Info
Description
Value
Unit
Serial number
1614-0036-21
Firmware version
720897
Code name
11.1s0
Firmware download date
01/01/1970 00:00:00
MAC address
00:03:27:03:30:ec
MAC address WAN
00:03:27:03:5f:fb
MAC address WIFI
00:00:00:00:00:00
Modem extended information
[2000Kb] MFR: Telit , MODEL: HE910-D , VER: 12.00.026

Tekortkomingen (Deel 1)

- Out-Of-The-Box instellingen zijn **zeer** onveilig:
  - Firewall staat uit: WAN-poort laat **alle** communicatie toe naar de LAN kant. Kwestie van route in te stellen.
    → Kán aangepast worden
  - Broadcast gebaseerd detectie systeem om het toestel te configureren, zonder authenticatie
    → Kán voorzien worden van user/pass
- eWon vereist dat de PLC volledig open staat (geen verdediging mogelijk)

Tekortkomingen (Deel 2)

De website:

- Enkel HTTP mogelijk (HTTPS **onmogelijk**)
- De authenticatie gebeurt via ‘Basic HTML Authentication’.
  → M.a.w. gebruiker & wachtwoord worden verstuurd met élke refresh
  – Dit betekent dat letterlijk elke link op de pagina gevaarlijk is, indien er luistervinken zijn
  – Dit betekent ook dat de gebruiker oneindig lang ingelogd blijft
- Nagenoeg elk invoerveld op de website is kwetsbaar voor XSS

```
15:16:10.568[31ms][total 31ms] Status: 200[OK]
GET http://172.20.1.1/Ast/ViewDiagStatDataAst.shtm?AST_UserId=1&AST
   Request Headers:
      Host[172.20.1.1]
      User-Agent[Mozilla/5.0 (Windows NT 6.3; WOW64; rv:49.0) Gecko
      Accept[text/html,application/xhtml+xml,application/xml;q=0.9,
      Accept-Language[en-US,en;q=0.5]
      Accept-Encoding[gzip, deflate]
      Referer[http://172.20.1.1/Ast/ViewDiagStatHeadAst.shtm]
      Authorization[Basic YWRtOmFkbQ==]
      Connection[keep-alive]
      Upgrade-Insecure-Requests[1]
   Response Headers:
      Date[Mon Oct  6 15:17:26 2014 GMT]
      Server[eWON]
      Access-Control-Allow-Origin[*]
      access-control-allow-credentials[true]
```

➔ base64(adm:adm)

eWON Session (user)

172.20.1.1/Ast/MainAst.shtm

Search

eWON

eWON-Fictile

Diagnostic

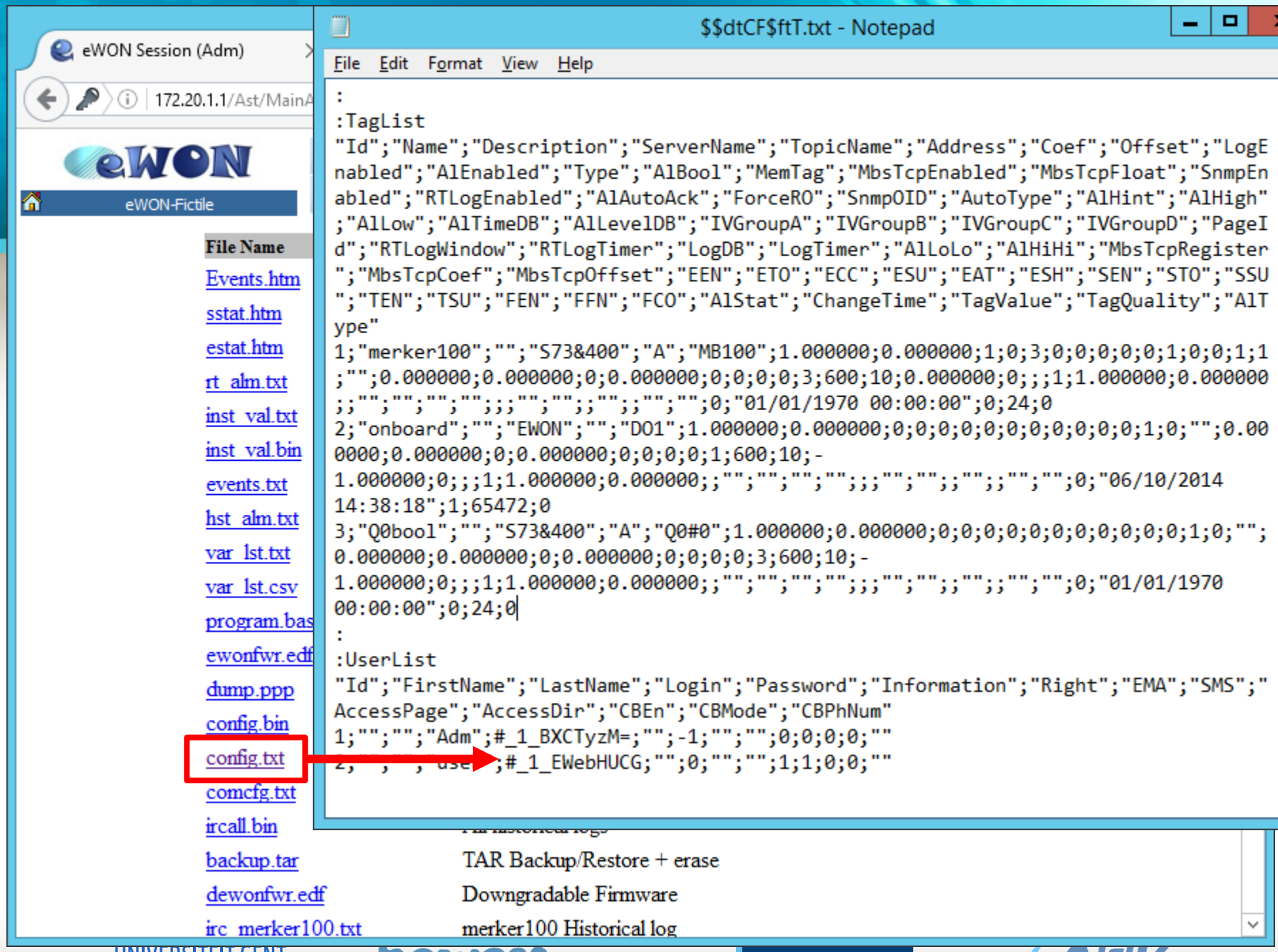
Log off

Information

User

Tekortkomingen (Deel 3)

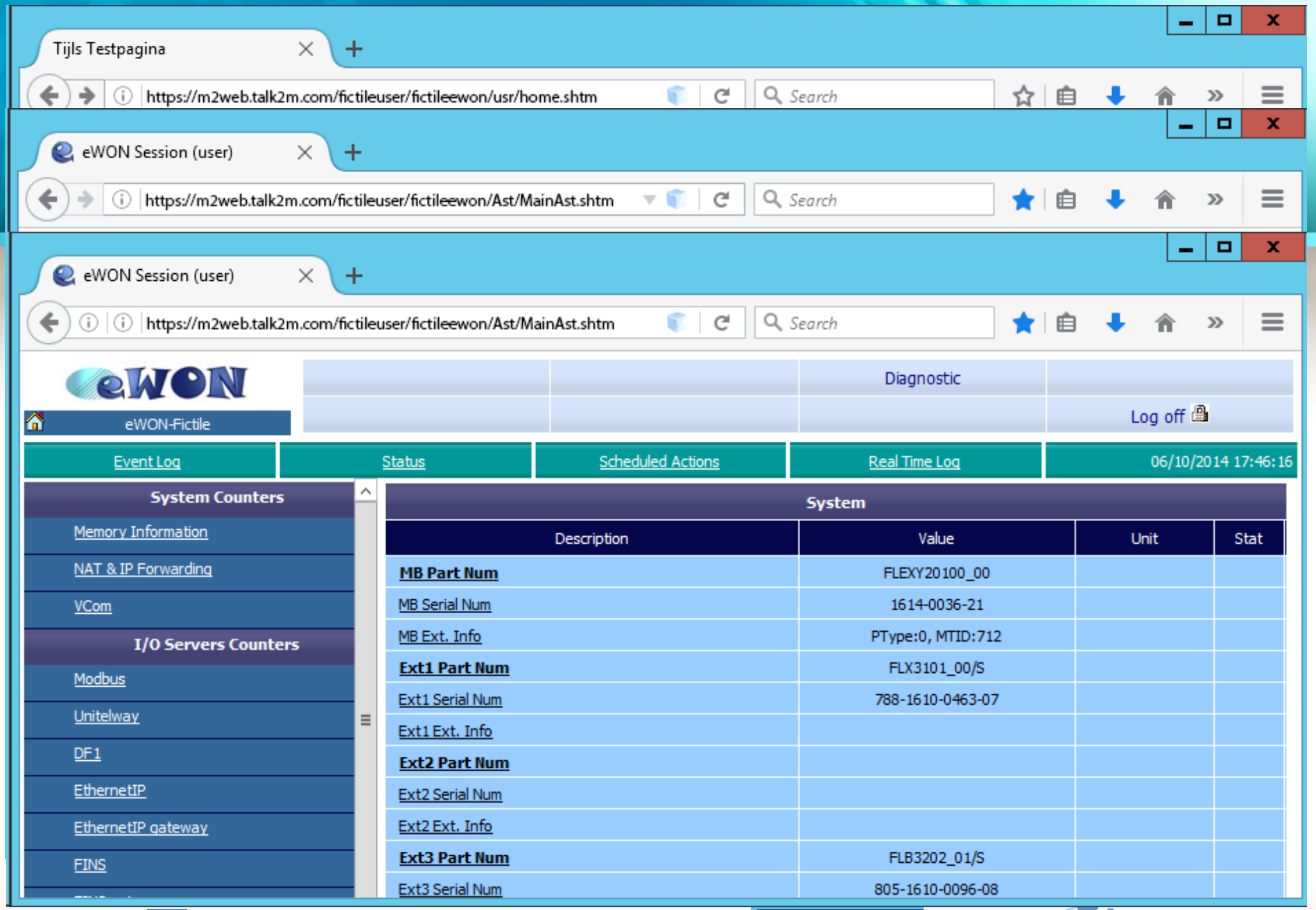
- Alle configuratie kan in één bestand gedownload worden (‘config.txt’). Dit zowel via de website als via FTP
  - Hierin zitten alle PLC gegevens en ook alle diverse wachtwoorden
    (dus ook die van 3G, VPN, FTP)
    → ’Encrypted’ volgens een **eigen** protocol.
  - Vrij eenvoudig te achterhalen (combinatie van Base64 + XOR) en dus **onveilig**


eWON Session (Adm)
172.20.1.1/Ast/MainA
eWON
eWON-Fictile
File Name
Events.htm
sstat.htm
estat.htm
rt_alm.txt
inst_val.txt
inst_val.bin
events.txt
hst_alm.txt
var_lst.txt
var_lst.csv
program.bas
ewonfwr.edf
dump.ppp
config.bin
config.txt
comcfg.txt
ircall.bin
backup.tar
dewonfwr.edf
irc_merker100.txt
TAR Backup/Restore + erase
Downgradable Firmware
merker100 Historical log
$$dtCF$ftT.txt - Notepad
File Edit Format View Help
:
:TagList
"Id";"Name";"Description";"ServerName";"TopicName";"Address";"Coef";"Offset";"LogEnabled";"AlEnabled";"Type";"AlBool";"MemTag";"MbsTcpEnabled";"MbsTcpFloat";"SnmpEnabled";"RTLogEnabled";"AlAutoAck";"ForceRO";"SnmpOID";"AutoType";"AlHint";"AlHigh";"AlLow";"AlTimeDB";"AlLevelDB";"IVGroupA";"IVGroupB";"IVGroupC";"IVGroupD";"PageId";"RTLogWindow";"RTLogTimer";"LogDB";"LogTimer";"AlLoLo";"AlHiHi";"MbsTcpRegister";"MbsTcpCoef";"MbsTcpOffset";"EEN";"ETO";"ECC";"ESU";"EAT";"ESH";"SEN";"STO";"SSU";"TEN";"TSU";"FEN";"FFN";"FCO";"AlStat";"ChangeTime";"TagValue";"TagQuality";"AlType"
1;"merker100";"";"S73&400";"A";"MB100";1.000000;0.000000;1;0;3;0;0;0;0;0;1;0;0;1;1;"";0.000000;0.000000;0;0.000000;0;0;0;0;3;600;10;0.000000;0;;;1;1.000000;0.000000;;"";"";"";"";;;"";"";;"";;"";"";0;"01/01/1970 00:00:00";0;24;0
2;"onboard";"";"EWON";"";"DO1";1.000000;0.000000;0;0;0;0;0;0;0;0;0;0;0;0;1;0;"";0.000000;0.000000;0;0.000000;0;0;0;0;1;600;10;-1.000000;0;;;1;1.000000;0.000000;;"";"";"";"";;;"";"";;"";;"";"";0;"06/10/2014 14:38:18";1;65472;0
3;"Q0bool";"";"S73&400";"A";"Q0#0";1.000000;0.000000;0;0;0;0;0;0;0;0;0;0;0;0;1;0;"";0.000000;0.000000;0;0.000000;0;0;0;0;3;600;10;-1.000000;0;;;1;1.000000;0.000000;;"";"";"";"";;;"";"";;"";;"";"";0;"01/01/1970 00:00:00";0;24;0
:
:UserList
"Id";"FirstName";"LastName";"Login";"Password";"Information";"Right";"EMA";"SMS";"AccessPage";"AccessDir";"CBEn";"CBMode";"CBPhNum"
1;"";"";"Adm";#_1_BXCTyzM=;"";-1;"";"";0;0;0;0;""
;#_1_EWebHUCG;"";0;"";"";1;1;0;0;""

Tekortkomingen (Deel 4)

VPN

- Gaat altijd via het Datacenter van eWon (FR)
- Vereist eCatcher software (VPN client)
  - Verschillende beveiligingsniveaus mogelijk
- Alle beveiligingsniveaus laten de diagnostics pagina toe
  - Oók clientless *m2web* methode
- Bijgevolg: volledig afschermen niet mogelijk



UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

KU LEUVEN

XIAK

eWon / Bintz

- eWon wordt (werd?) in België exclusief via Bintz Technics verkocht
- Werden op 14 Juni 2016 op de hoogte gebracht
- Alles werd bevestigd … (door Bintz)
- (Nog) geen officiële reactie (na aandringen)

eWon Conclusie

- Heel wat aandachtspunten …
  - Al had het erger gekund, gezien de functionaliteiten lijst
- Goede nieuws: de standaard instellingen zijn onveilig, maar zijn wel veilig te maken
  - Al hangt alles af van het scenario en doelpubliek

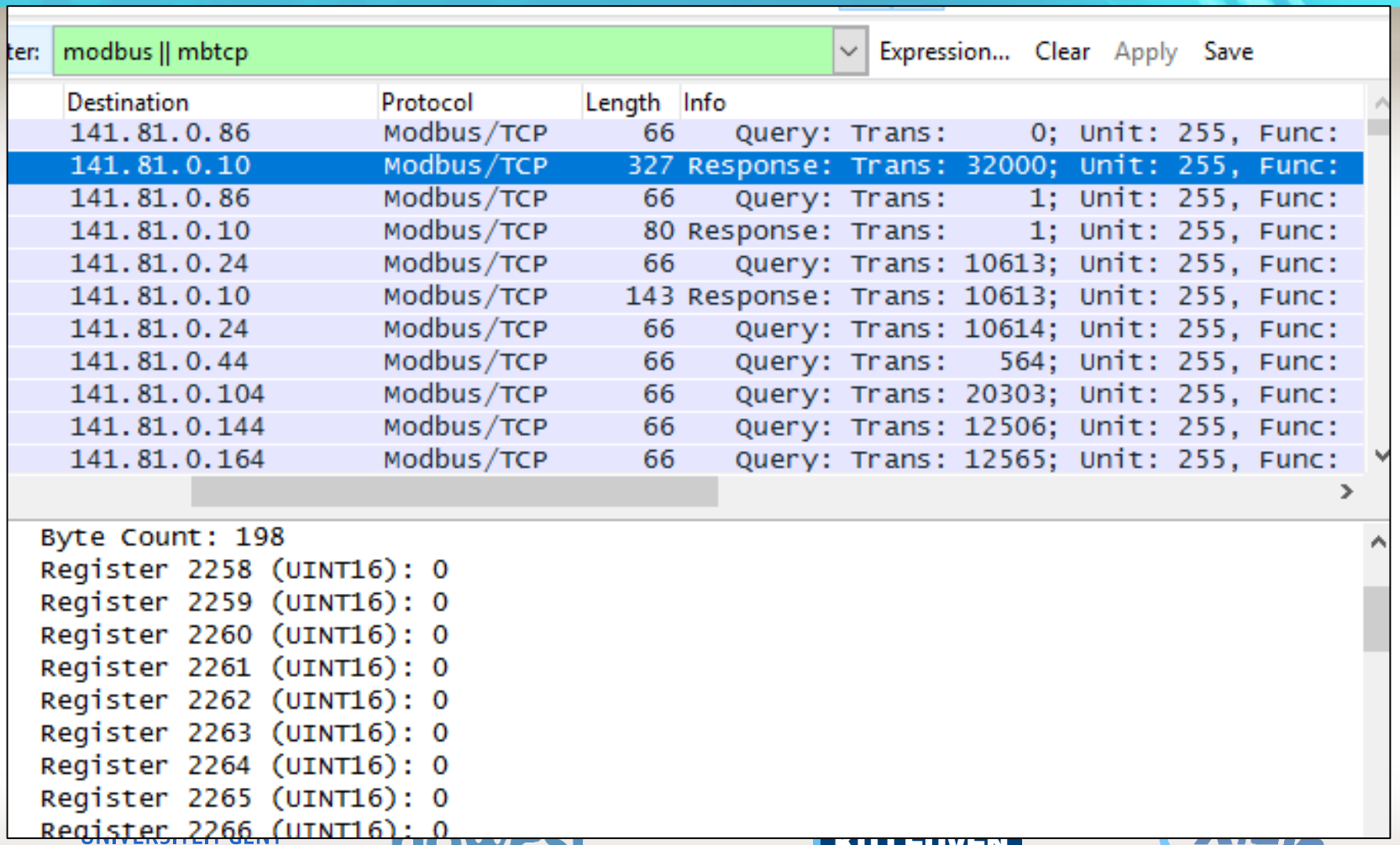
Appendix B

- Het meest ‘algemene’ protocol
- Ondersteund door de meeste vendors
- Modbus TCP
  → Geen authenticatie mogelijk

ModBus TCP

- Protocol volledig reverse engineered
- Dissector aanwezig in Wireshark
  - Modbus/TCP sinds versie 1.0.0 (2008)
  - Modbus sinds versie 1.8.0 (2012)

ModBus TCP


ter: modbus || mbtcp
Expression... Clear Apply Save
Destination Protocol Length Info
141.81.0.86 Modbus/TCP 66 Query: Trans: 0; Unit: 255, Func:
141.81.0.10 Modbus/TCP 327 Response: Trans: 32000; Unit: 255, Func:
141.81.0.86 Modbus/TCP 66 Query: Trans: 1; Unit: 255, Func:
141.81.0.10 Modbus/TCP 80 Response: Trans: 1; Unit: 255, Func:
141.81.0.24 Modbus/TCP 66 Query: Trans: 10613; Unit: 255, Func:
141.81.0.10 Modbus/TCP 143 Response: Trans: 10613; Unit: 255, Func:
141.81.0.24 Modbus/TCP 66 Query: Trans: 10614; Unit: 255, Func:
141.81.0.44 Modbus/TCP 66 Query: Trans: 564; Unit: 255, Func:
141.81.0.104 Modbus/TCP 66 Query: Trans: 20303; Unit: 255, Func:
141.81.0.144 Modbus/TCP 66 Query: Trans: 12506; Unit: 255, Func:
141.81.0.164 Modbus/TCP 66 Query: Trans: 12565; Unit: 255, Func:
Byte Count: 198
Register 2258 (UINT16): 0
Register 2259 (UINT16): 0
Register 2260 (UINT16): 0
Register 2261 (UINT16): 0
Register 2262 (UINT16): 0
Register 2263 (UINT16): 0
Register 2264 (UINT16): 0
Register 2265 (UINT16): 0
Register 2266 (UINT16): 0

Modbus Software

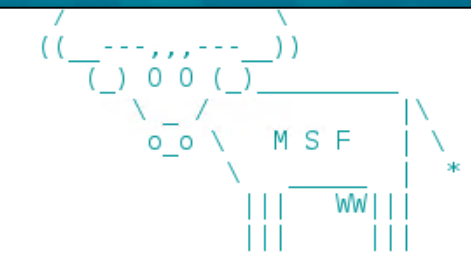
- Vrij voor iedereen te vinden:
  - Perl script: mbtget.pl

```
root@kali:~/mbtget/scripts# ./mbtget 1
values:
  1 (ad 00000):     55
  2 (ad 00001):      1
  3 (ad 00002):     33
```

  - Modules in Metasploit:
    modbusclient, modbusdetect,
    modbus_findunitid …

- Alsook gratis simulator: modbuspal (Java)

Metasploit Framework



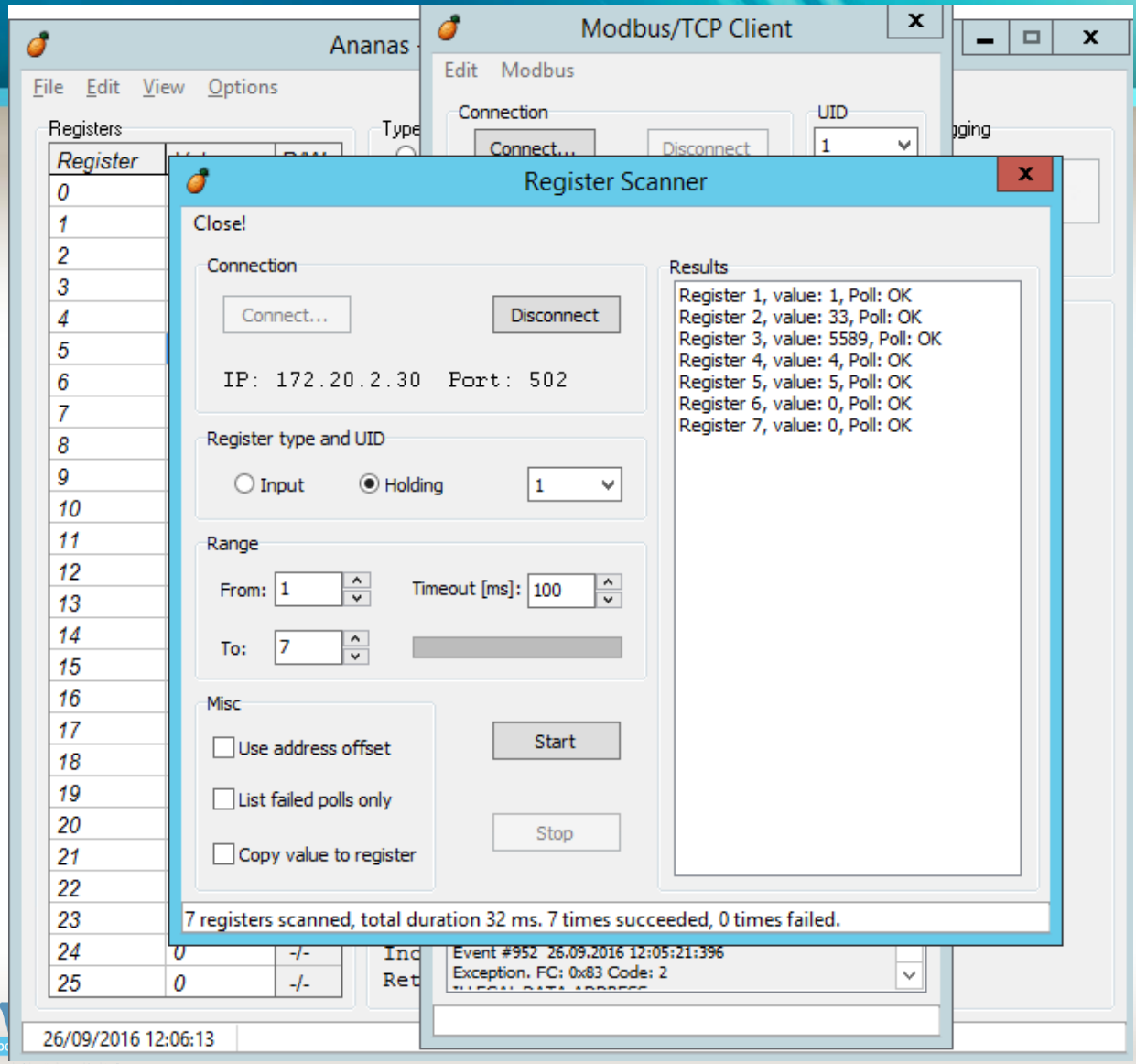
```
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.12.6-dev                          ]
+ -- --=[ 1549 exploits - 896 auxiliary - 267 post        ]
+ -- --=[ 438 payloads - 38 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search modbus

Matching Modules
================

   Name                                          Disclosure Date  Rank    Description
   ----                                          ---------------  ----    -----------
   auxiliary/admin/scada/modicon_command         2012-04-05       normal  Schneider Modicon Remote START/STOP Command
   auxiliary/admin/scada/modicon_stux_transfer   2012-04-05       normal  Schneider Modicon Ladder Logic Upload/Download
   auxiliary/scanner/scada/modbus_findunitid     2012-10-28       normal  Modbus Unit ID and Station ID Enumerator
   auxiliary/scanner/scada/modbusclient                           normal  Modbus Client Utility
   auxiliary/scanner/scada/modbusdetect          2011-11-01       normal  Modbus Version Scanner
```

Windows Client

Ananas Modbus/TCP Client

→ Freeware

http://www.tuomio.fi/ananas/



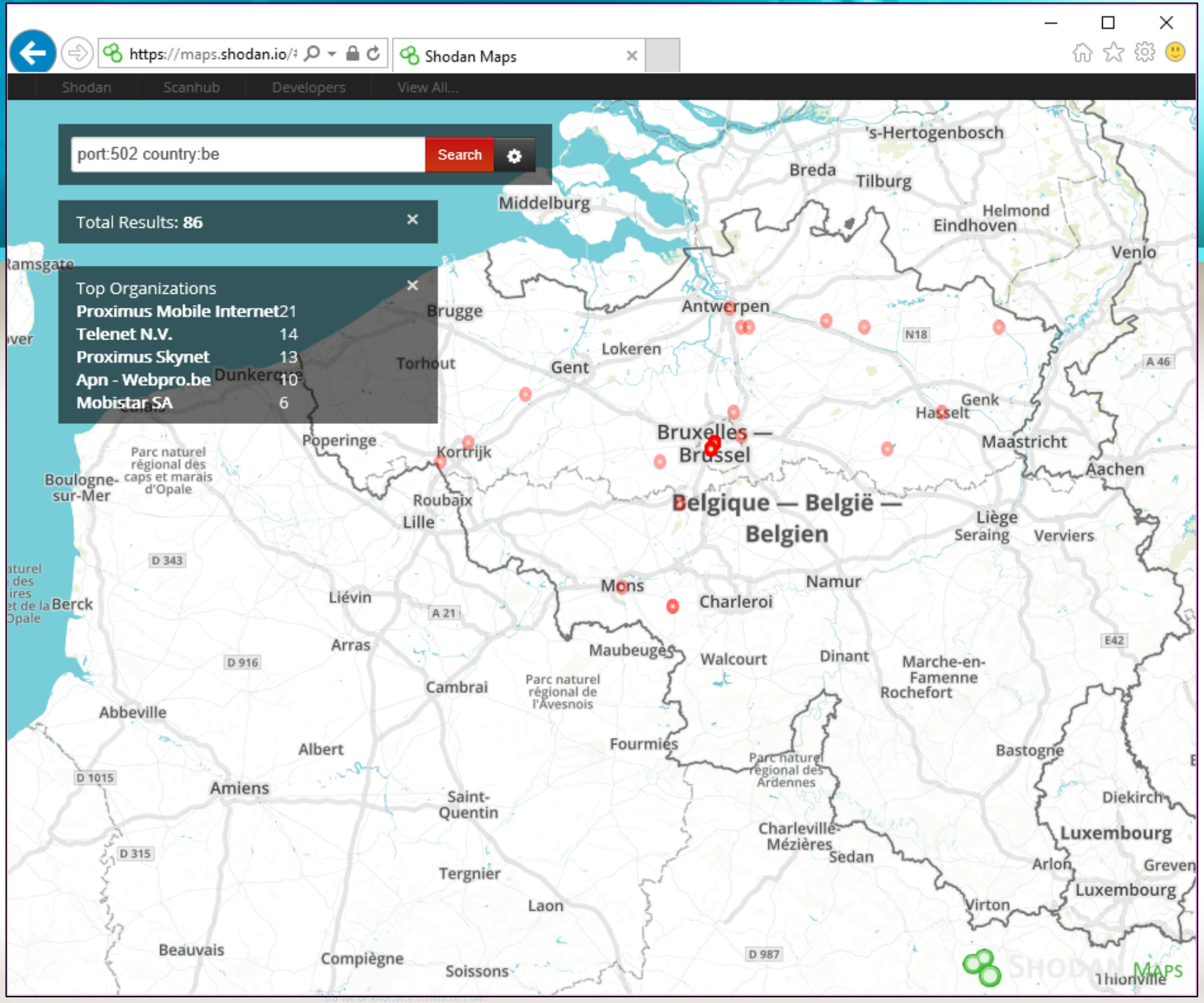
UNIVERSITEIT GENT
CAMPUS KORTRIJK

Modbus publiek?

Cijfers van Shodan.io

- **12851 resultaten** van publieke Modbus systemen

- **86 in België**


https://maps.shodan.io/#
Shodan Maps
Shodan
Scanhub
Developers
View All...
port:502 country:be
Search
Total Results: 86
Top Organizations
Proximus Mobile Internet 21
Telenet N.V. 14
Proximus Skynet 13
Apn - Webpro.be 10
Mobistar SA 6
's-Hertogenbosch
Breda
Tilburg
Middelburg
Helmond
Eindhoven
Venlo
Ramsgate
Brugge
Antwerpen
N18
Lokeren
Gent
Torhout
Dunkerque
A 46
Genk
Hasselt
Bruxelles — Brussel
Poperinge
Kortrijk
Maastricht
Aachen
Parc naturel régional des caps et marais d'Opale
Boulogne-sur-Mer
Roubaix
Lille
Belgique — België — Belgien
Liège
Seraing
Verviers
D 343
Namur
Mons
Charleroi
Liévin
Berck
A 21
Arras
E42
D 916
Maubeuge
Walcourt
Dinant
Marche-en-Famenne
Rochefort
Cambrai
Parc naturel régional de l'Avesnois
Abbeville
Fourmies
Albert
Bastogne
Parc naturel régional des Ardennes
D 1015
Amiens
Saint-Quentin
Diekirch
Luxembourg
Charleville-Mézières
Sedan
D 315
Arlon
Greven
Luxembourg
Tergnier
Virton
Laon
Beauvais
Compiègne
Soissons
D 987
Thionville
SHODAN MAPS

Time for defensive actions

… Volgende presentatie: Hendrik Derre