

- **ICS OVERVIEW**
  - Terms & Definitions
  - Generic architectures
  - History of ICS
- **Hands on: Basic PLC Programming**
  - Creating a first Flowchart-based program
  - Creating visualisation
- **Commonly used ICS protocols**
  - Overview of ICS protocols
  - Security considerations for commonly used protocols
  - Hands-on: Wireshark captures
- **Introduction to ICS Security**
  - Basics of an ICS security penetration test
  - Red team Exercise & Demo's



# Misconceptions

- **SAFETY != SECURITY**
- I have an Antivirus, I am secure
- Proprietary protocols are more secure
- BIG VENDOR products are certainly secure

# Network segmentation



- Mostly a fail
- ACLs on routers are very important, but difficult to get perfect (and to **keep** perfect)
- Air-gapping is not the holy grail ([Stuxnet](#))
- Network segmentation is not working correctly if you can copy files directly from the office network to the ICS network...

Shodan Scanhub Developers View All...

SHODAN


Explore Contact Us Blog Enterprise Access

New to Shodan? [Login or Register](#)

# The search engine for Power Plants


Shodan is the world's first search engine for Internet-connected devices.

[Create a Free Account](#) [Getting Started](#)




### Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.




### See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



### Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



### Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

# The biggest threat: the internet

- There is a special ***search engine*** that scans the entire internet for ***devices: Shodan***
- Shodan is free-to-use, gives you information about the types of technologies that are used and clients often do not know these are online...
- What can you find?
  - PLCs, Webcams, Smart Devices (TV, HVAC ...), IoT ...
- What does it provide?
  - Extensive reports: <https://www.shodan.io/report/zsNizYWj>

# ICS Security, the definition of hard

- “uptime” is everything with ICS, every *second* of downtime is a loss of money.
- That means applying security patches is difficult
  - Sometimes “not allowed” by vendors
- ICS vendors also not advise to install Antivirus software to prevent false positives

# Pentesting ICS

- **Not** as easy as it sounds
  - ICS hardware (HMI, PLC, OPC ...) has **very, very** limited hardware
  - These devices cannot handle an excessive amount of traffic
- For example (<http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>):
  - In a factory for integrated circuits, a **ping sweep** caused a 3M robotic arm to swing out of control
  - Natural gas distribution utility, a pentester went **a little bit** out of scope and caused a gas blockage to the customers for four (4!) hours



# Can I still scan?

Yes, even Nmap can still be used and here is why:

- Reduce the scanning speed! Use “*--scan-delay=1*” to scan only one port at a time
- Perform no ping, SYN or UDP scans, but stick to TCP scans
  - *nmap -sn -PR -n*
- No fingerprinting options, these will send a lot of extra packets to **force** the listener to respond with certain crafted packets. These often contain “fingerprints” that nmap compares with a built-in database to determine services and operating systems.



# However, there is another way

## ***SNMP!***

- Simple Network Management Protocol is a technology designed to gather information on “your” network. (SNMP GET)
- It can sometimes even be used to configure certain devices (SNMP SET)
- Since devices that allow this traffic are supposed to be able to handle the load it is a more or less “safe” way of scanning a network
  - Sometimes with surprising results 😊

# SNMP howto

- There are 3 versions of which SNMPv1 is too old and SNMPv3 is too new to be seen regularly.
  - SNMPv3 supports credentials, but is hardly used nor supported in older hardware
- So SNMP version 2c is the main focus.
  - Good and Free Windows Tool to get and set data for a given device:
    - MIB Browser (<http://ireasoning.com/mibbrowser.shtml>)
  - But off course extensive scanners are out there as well:
    - snmpwalk, for [Windows](#) or Linux (*apt-get install snmp*)
    - And Home Made Scripts ☺

# And ICS itself?

- As seen earlier today: **No Focus On Security**
- Most common ICS protocols like ProfiNet, Modbus and S7Comm do not even support encryption and sometimes not even authentication.
- Easily confirmed: for any PLC or HMI, just download the **official** programming software (e.g. *trial*). Install it and start connecting to and controlling the PLC!



# ICS security tools?

Yes, a lot of specialized tools:

- PLCScan: <http://www.digitalbond.com/tools/plcscan/>  
by <http://scadastrangelove.org/>
  - Only scans ports 102 (Siemens S7Comm) & 502 (Modbus)
- Mbtget for ModbusTCP: <https://github.com/sourceperl/mbtget>
  - Stop/Run PLC's can be done with [modicon command](#)
  - Logic down- and upload can be done with [modicon stux transfer](#)
- Profinet, IEC, S7-1200 scripts:  
<https://github.com/atimorin/scada-tools>
- Some are built into [metasploit](#) ...
- And we have some of our own as well 😊

```
msf auxiliary(modbusdetect) > show info
```

```
Name: Modbus Version Scanner  
Module: auxiliary/scanner/scada/modbusdetect  
License: Metasploit Framework License (BSD)
```

```
msf auxiliary(modbusdetect) > use auxiliary/scanner/scada/  
use auxiliary/scanner/scada/digi_addp_reboot  
Pr use auxiliary/scanner/scada/digi_addp_version  
use auxiliary/scanner/scada/digi_realport_serialport_scan  
Ba use auxiliary/scanner/scada/digi_realport_version  
use auxiliary/scanner/scada/indusoft_ntwebserver_fileaccess  
use auxiliary/scanner/scada/koyo_login  
use auxiliary/scanner/scada/modbus_findunitid  
use auxiliary/scanner/scada/modbusclient  
use auxiliary/scanner/scada/modbusdetect  
De use auxiliary/scanner/scada/sielco_winlog_fileaccess
```

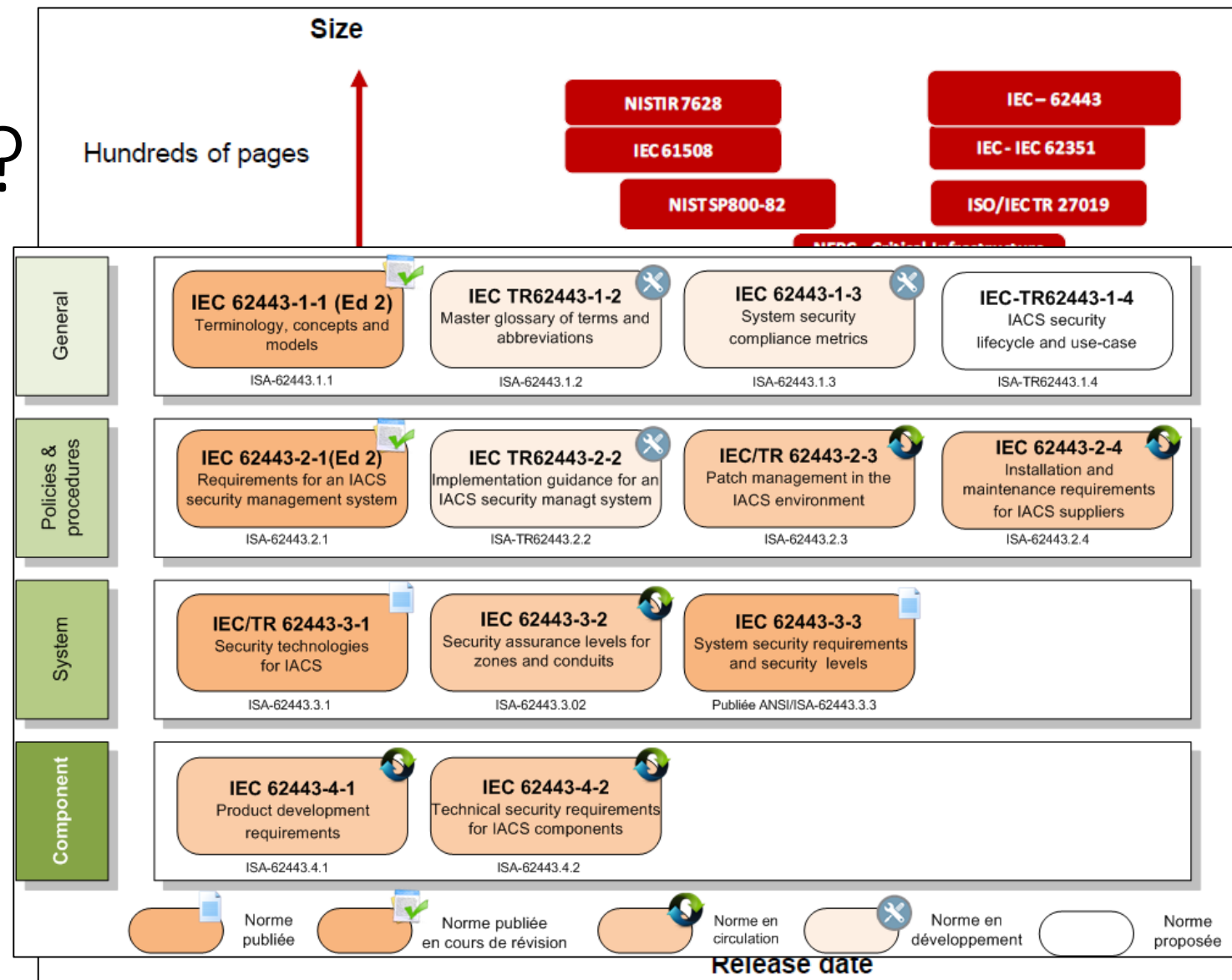
system. Modbus is a clear text protocol used in common SCADA systems, developed originally as a serial-line (RS232) async protocol, and later transformed to IP, which is called ModbusTCP.

#### References:

<http://www.saia-pcd.com/en/products/plc/pcd-overview/Pages/pcdl-m2.aspx>  
<http://en.wikipedia.org/wiki/Modbus:TCP>

# So, any guidelines?

- Yes, dozens ...
- A lot of text has been written around the topic
- But it all boils down to



Source: <https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2014-Cyber-Security-of-Industrial-Control-Systems.pdf>

Cyber

The screenshot displays the CSET (Cyber Security Evaluation Tool) interface. The top navigation bar includes icons for Home, Information, Standards, SAL, Diagram, Questions (highlighted), Analysis, and Reports. The main content area is titled "Account Management" and shows a list of questions related to account management. The left sidebar contains a "Categories" section with a tree view showing "All" and "Component Defaults" under "Account Management". The right sidebar shows details for question #1, including a "Details" tab, a "Comments" section, and a "Documents" section. The bottom navigation bar includes icons for Diagram, Help, Documents, and a "Boundary Protection" button.

**CSET**

Home Information Standards SAL Diagram **Questions** Analysis Reports

Categories

Selected Standards:

Security Assurance Level: Moderate

Sort Questions By: Default

Filters:

Category Tree:

- All
- Component Defaults
  - Account Management**
  - Boundary Protection
  - Communication Protection
  - Encryption
  - Firewall
  - Logging
  - Management
  - Management Practices
  - Password
  - Physical Access
  - Policies & Procedures General
  - Remote Access Control
  - Securing Content
  - Securing the Component
  - Securing the Router
  - Securing the System
  - System Protection
  - User Authentication

Account Management

Account Management

1 Are accounts locked after a defined number of failed login attempts? Yes No N/A ALT

Active Directory: Do you use active directory for authentication services?

2 Do you use Active Directory to enforce authentication policies? (e.g. password complexity, lockout on failed attempts, password expiration) Yes No N/A ALT

3 Are the DNS administrators groups and users placed into a designated Organizational Unit (OU) with appropriate Group Policy applied? Yes No N/A ALT

# 1-Account Management

Details Components

Question: Are accounts locked after a defined number of failed login attempts? ID:1586

☐ Mark for review

Comments

Documents

Document Title

Title	File Name			
-------	-----------	--	--	--

Diagram Help Documents Boundary Protection



# System hardening (1)

- Patching process
  - How long since your routers, switches or printers have been updated?
- Services
  - Is it really necessary that SNMP on that XP is enabled (on by default)?
- Attack surface
  - Is it really necessary that the SQL server is available for everyone (0.0.0.0) and not only available for local websites (127.0.0.1)?
- User accounts & permissions
  - Is it really necessary that the receptionist has AD rights to every domain member?

# System hardening (2)

- Service permissions
  - Is it really necessary that apache is running as root?
- Network configuration
  - Is it really necessary that someone in the office can surf to an HMI on the factory floor?
- Remote administration
  - Do you know how many people (suppliers) have the PIN code to that TeamViewer machine in your network?
- And of course: perform your own scanning/pentesting!

# Importing data from corporate to ICS

- Use different USB keys for corporate and ICS networks (color codes?)
  - Enforce using GPO's for manufacturer / serial numbers
- Use several AV solutions
- Use a dedicated PC, not managed by Active Directory, to download updates. Use whitelists, binary signatures (SHA1 / MD5 checksums) and only one USB key.

# Think out of the box 😊

- Why not write a script that sends you an email every time an Active Directory domain admin is created?
- Why not configure the VPN (remote management) solution that it raises an alert when the same account is used by two different IP addresses half-way around the world?
  - No one will login from Belgium and then be in Russia 15min. later 😊
- Why not write a program that restarts TeamViewer every week and texts (SMS) the new PIN to the System Admin?

Actually, we already created this: <http://www.xiak.be/teamviewersender>

# All right, time to hack ...euh... pentest ...euh... audit!

## Methodology

- Scan
  - find all IP addresses and open ports on a network
- Enumerate
  - find OS and Service versions, create connections
- Vulnerability assessment
  - use specific vulnerability scanners
- Exploit
  - gain unauthorized access to a system
- Gather
  - reuse found data/credentials on earlier services (and repeat)

# Find all IP addresses and ports



As mentioned: nmap (Linux/Windows) is our preferred tool here

→ Zenmap is the GUI, but you lose control on what **exactly** is happening

- E.g. *nmap -n -sP 10.0.0.0/24*
  - Use the resulting MAC addresses (if possible) to determine the device types
- E.g. *nmap -n -sT 10.0.0.4,6,10-20*
  - The port number gives you an idea what service it is
- Important: use your head
  - what would be your reaction if you see an open port **80** ?
  - what would you try if you see an open port **21** ?

# Thinking out of the box (scanning)

Devices such as Routers, Switches, Printers, Access Points, Card Readers, Airconditioners, PDU's ... might **also** have an IP address!

- So don't limit your scan to a single network...
- Which networks?
  - Use **tracert -d** (Windows) or **traceroute -n** (Linux)
- Make sure to also including scanning the **default** network range for most of the above devices:
  - 192.168.1.0/24 and 192.168.0.0/24
  - They may be forgotten about upon installation ☺  
→ E.g. Managed Switch still has IP 192.168.1.1 and default credentials, but has a lot of VLAN information





# Enumerate

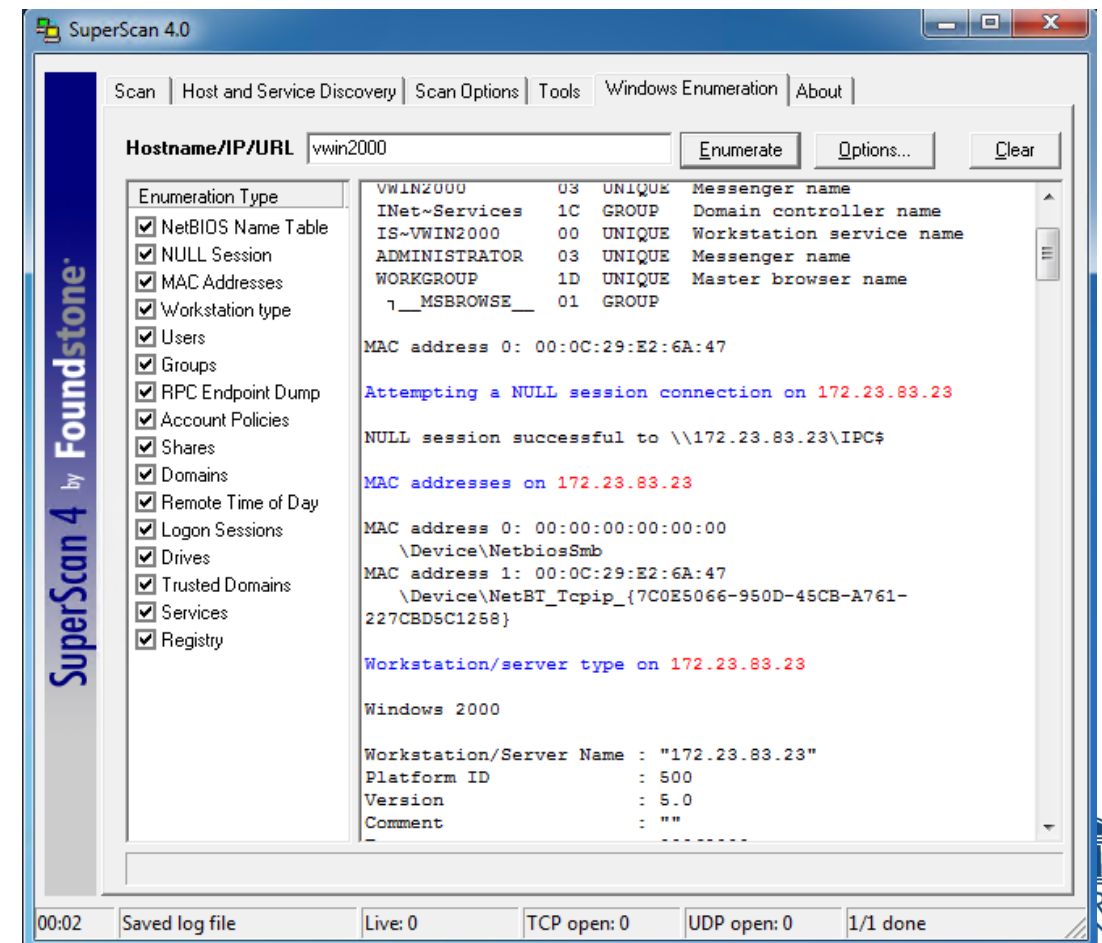
Again, nmap can make connections and perform basic version detection

- E.g. *nmap -n -sV -p102,3389,443,445 10.0.0.4,6,10-20*
  - This may even already disclose vulnerabilities, e.g. if you find SMB version 5.1.2600 (WinXPSP2)
- Can even run scripts (C:\Program Files (x86)\Nmap\scripts)  
E.g. *nmap --script=tftp-enum,vnc-info 10.0.0.1-20*
  - There are more scripts online
  - Siemens Scada: <https://github.com/drainware/nmap-scada>
  - ICS: <https://github.com/digitalbond/Redpoint>

# Thinking out of the box (enumeration)

The most common services can be enumerated

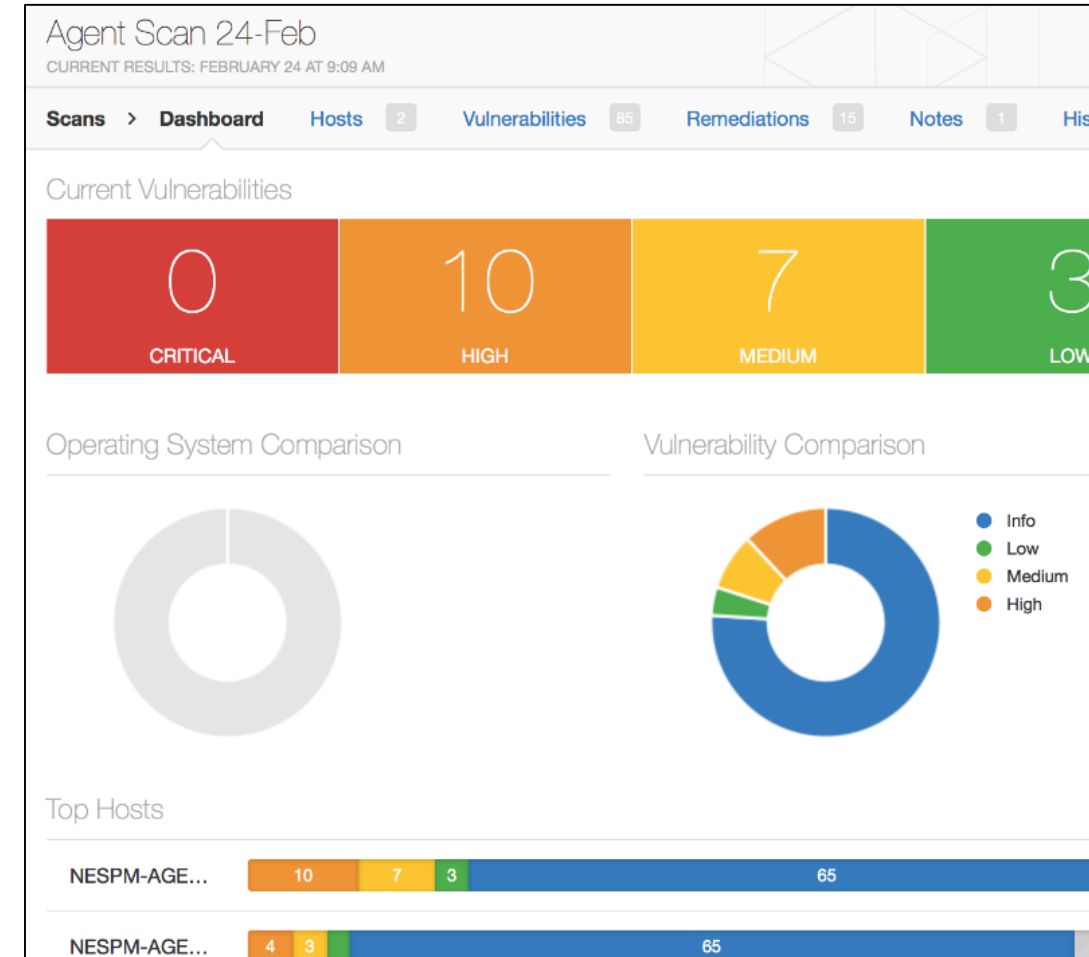
- SNMP (see earlier)
- DNS (zone transfer, anyone?)
- NetBIOS →
- Active Directory / LDAP  
(E.g. with [ridenum](#))
- SMTP (*nmap --script=smtp\**)



# Vulnerability Assessment

Finding vulnerabilities can be automated

- Tenable Nessus Vulnerability Scanner
- Has a free version (16IP limitation)
- Some (ICS) companies run Nessus on a weekly base
- Delivers beautiful reports
- Can be configured with scan delays
- Detailed information on vulnerabilities and potential exploitability



# Thinking out of the box (vulnerabilities)

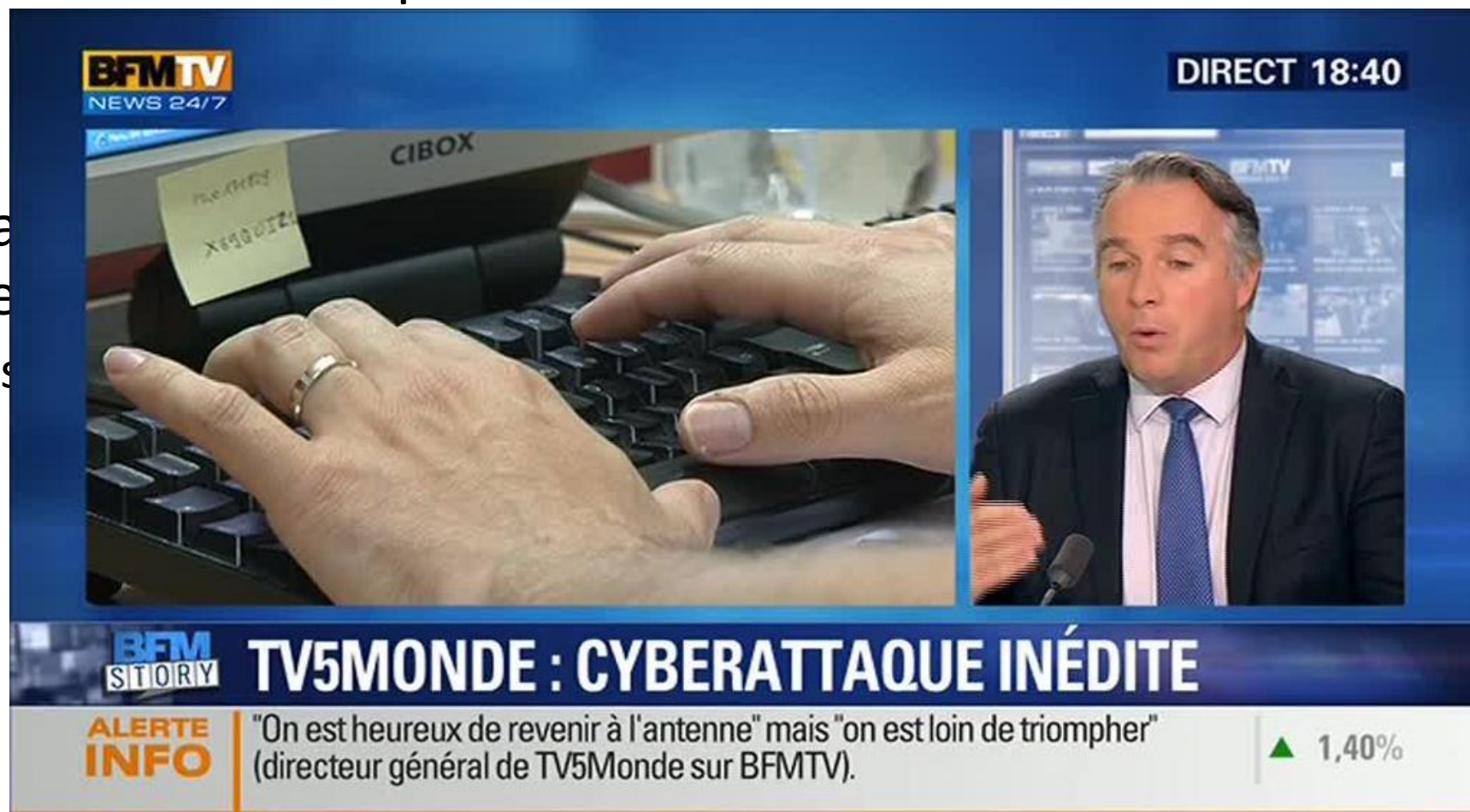
- There are also **protocol vulnerabilities**:
  - DNS
  - HTTP
  - TELNET
  - FTP
  - SMTP
  - ...
- ... all have one thing in common: they're **cleartext** protocols!
- Which means: they can be MiTM'ed and sniffed easily
  - Windows-tool: Cain & Abel, Linux-tool: ettercap

# Exploiting

- Now is the time to send special crafted packets to certain devices or portals
  - SQL Injection on websites?
  - Buffer Overflow on Windows SMB?
  - Profinet Set on PLC?
- There is a good tool for that: the ***Metasploit Framework***
  - Has a community edition (free), and exists for both Windows (buggy) and Linux (better)
  - Has a lot of built in exploits (currently around 1530), scanners and modules
- There are also online exploit databases like [www.exploit-db.com](http://www.exploit-db.com)

# Thinking out of the box (exploitation)

- Just logging into a device without permission is also considered exploitation
- Not only devices can be exploited (and they often are)
  - Dropping USB Keys
  - Phishing emails
  - Shoulder surfing
  - Or - - - - - >



```
root@kalitijl:~/Desktop# ls /usr/share/metasploit-framework/modules/post/windows
/gather/
arp_scanner.rb          enum_ms_product_keys.rb
bitcoin_jacker.rb       enum_muicache.rb
```

```
root@kalitijl:~/Desktop# ls /usr/share/metasploit-framework/modules/post/windows
/gather/credentials/
bulletproof_ftp.rb      gpp.rb                  skype.rb
coreftp.rb              idm.rb                  smartermail.rb
credential_collector.rb imail.rb                smartftp.rb
domain_hashdump.rb     imvu.rb                 spark_im.rb
dyndns.rb               mcafee_vse_hashdump.rb sso.rb
enum_cred_store.rb     meebo.rb                steam.rb
enum_laps.rb           mremote.rb              tortoisessvn.rb
enum_picasa_pwds.rb    mssql_local_hashdump.rb total_commander.rb
epo_sql.rb             nimbuzz.rb              trillian.rb
filezilla_server.rb    outlook.rb              vnc.rb
flashfxp.rb            razer_synapse.rb        windows_autologin.rb
ftpnavigator.rb        razorsql.rb             winscp.rb
ftpx.rb                rdc_manager_creds.rb    wsftp_client.rb
```

```
enum_domain_admin.rb   cephfs.rb
enum_files.rb           usb_history.rb
enum_hostfile.rb        win_privs.rb
enum_ie.rb              wmic_command.rb
enum_logged_on_users.rb word_unc_injector.rb
```

## Information



# Thinking out of the box (gather)

- Just looking through files, browser history and stored passwords is one thing the aforementioned modules can assist with
- However nothing beats a manual search through some text files (*password.txt* on the desktop?), installing keyloggers or going for software like KeePass.
- And then there is also the PC's **Memory**
  - Data stored inside PC memory is generally not encrypted
  - It is a default setting for Windows to store all Kerberos and Windows local passwords in memory for future authentication (and backwards compatibility)
  - [Mimikatz](#) is a software that can extract these secrets
- Don't underestimate the importance of password hashes

# The Workshop

Has two parts:

- Perform your own scanning on our *special* demo network.
  - Nothing is off limits, we have everything backed up
  - Learn to use Nmap, in Windows or Linux, maybe extended with extra (ICS) scripts
  - Feel free to try enumeration (recommended), vulnerability scanning and maybe even exploitation
- Inside this network we have also set up several Siemens S7-1200 PLC's connected to a functional setup, on every table.
  - You can read out the MAC address of the PLC closest to you, find the corresponding IP address and using S7Comm (script provided) you can then interact and override the functionality.
  - Target: make the treadmill run in a certain direction



ICS Workshop - 2016 – 04 – 14



# FicTile company

**KU LEUVEN**

  
UNIVERSITEIT  
GENT  
CAMPUS KORTRIJK

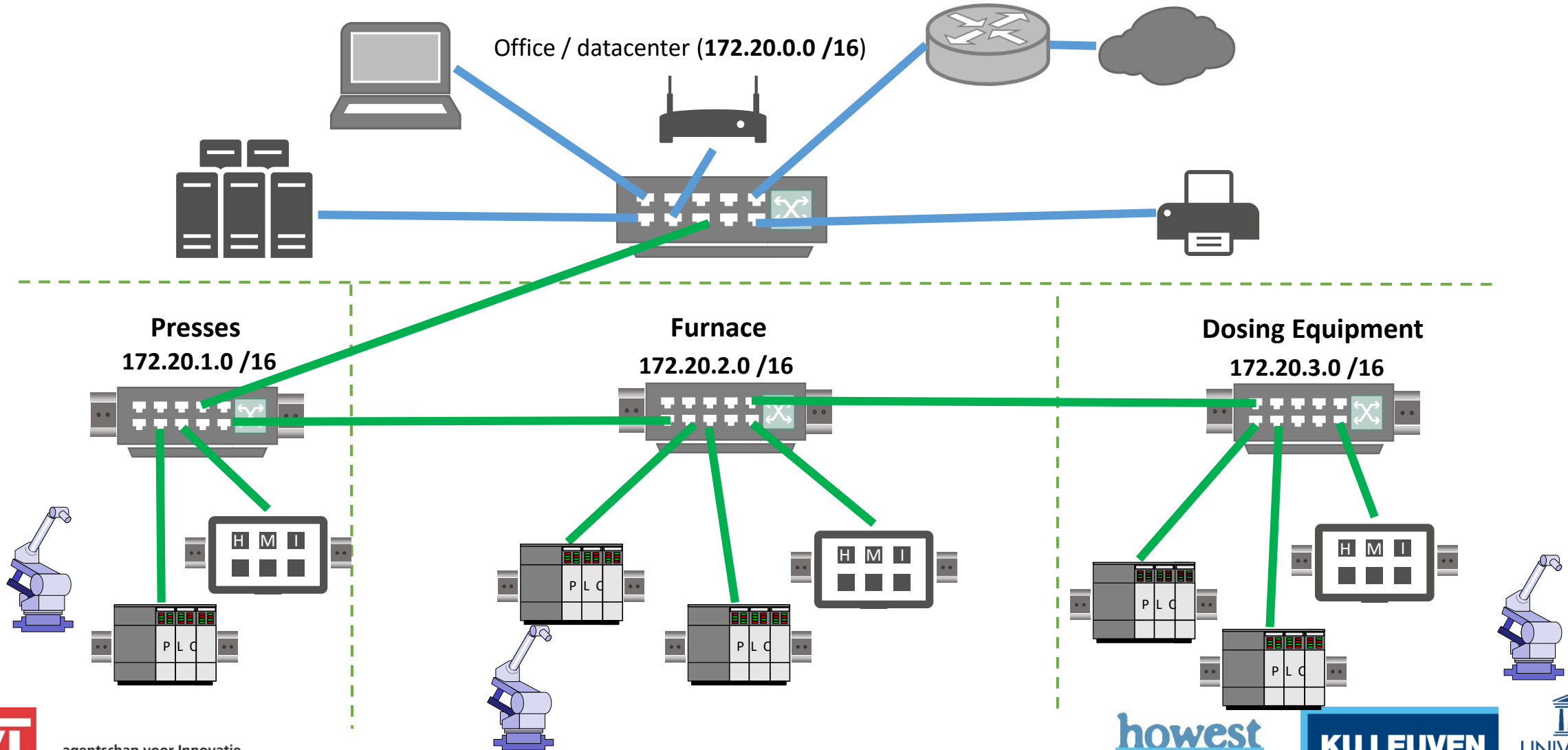
**howest**  
De Hogeschool West-Vlaanderen



# ICS Workshop - 2016 – 04 – 14

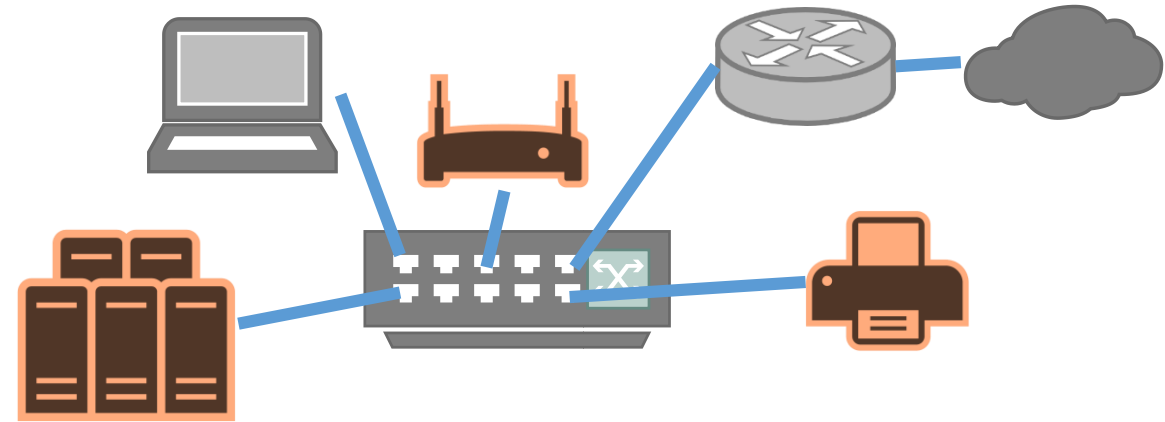


## Network Overview Layout



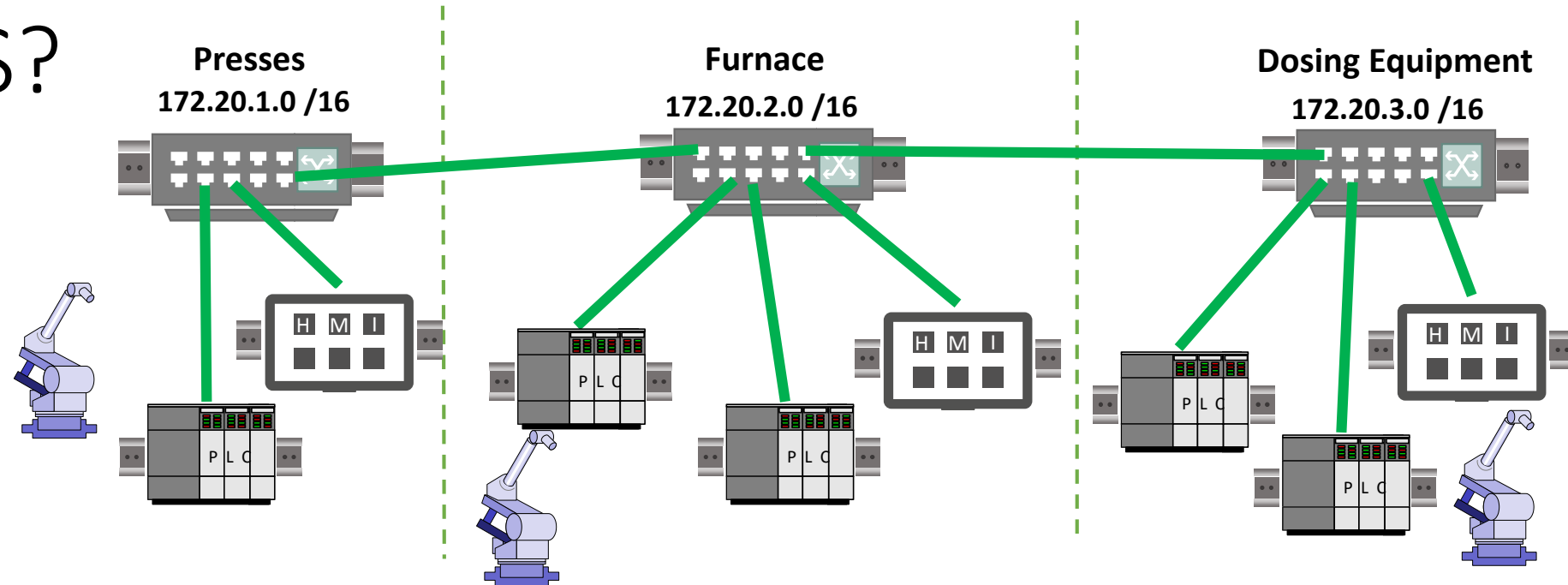
# What can be done?

- Everything off course 😊
- The AD Environment is completely vulnerable
  - Don't go directly for the Domain Controller, but it is the ultimate goal
  - Find the weak spot!
- Can you print any text on the network printer? (One command!)
- There is also a vulnerability on the WiFi AP (on the LAN side)



# And the ICS?

- Also everything



- For PhoenixContact; there are misconfigurations and vulnerabilities
  - No special scripts needed for some of these
- Beckhoff has several vulnerabilities in both the HMI as the PLC
  - Special scripts may be needed but are available
- Siemens has the most common configuration

# The final destination

- When ready (or fed up) with all general hacks, we have a mission
  - *RUN THE THREADMILL CLOSEST TO YOU*
  - Firstly: press the red banana plug next to it down
  - Scan for the IP of the **correct** PLC and then use our script to run it

