# OTLab 07

## *Default Password Exposure*

Prof. Dr. Luiz Fernando Freitas-Gutierres (a.k.a. substationworm)

`linkedin.com/in/lffreitas-gutierres`

`github.com/substationworm/OTLab`

`luiz.gutierres@ufsm.br`

## Tasks

1. Verify the IP address of the `otlab-student` workstation.
2. Determine the subnet range of the network where the `otlab-student` workstation is deployed.
3. Discover the IP address, MAC address, and vendor information of other active hosts within the network.
4. Identify open ports and available services on the OT-ICS host over both TCP and UDP protocols.
5. Obtain the authentication credentials and log in to the user management and access control interface of the OT-ICS host. *Hint: Weak authentication mechanism.*

Note: The `plc`-hmi is based on Conpot, which remaps standard protocol and service ports to non-privileged ports. Refer to the link for a list of some default and remapped ports.

## Tools

These are the tools available on the `otlab-student` workstation for completing OTLab 07: `ifconfig`, `masscan`, `netdiscover`, and `nmap`.

## Nomenclature

- ICS: Industrial control system.
- IP: Internet protocol.
- MAC: Media access control.
- OT: Operational technology.
- TCP: Transmission control protocol.
- UDP: User datagram protocol.