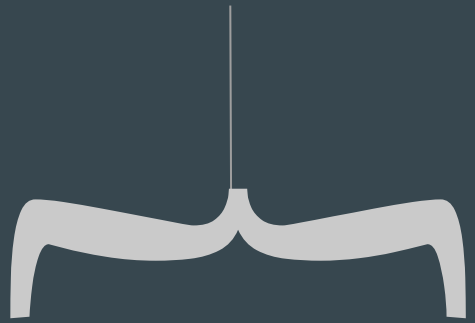
Hacking Powerplants

What is OT?

Operation Technology



Industrial Control Systems

Why do you care?

IT

- Data
- Personal Info
- Medical
- Intellectual Property

OT

- Controlling physical systems
- Physical effects

Ukraine 2015 Attack

- First cyber attack on a power plant
- BlackEnergy malware
- Prykarpattyaoblenergo (say that 3 times fast)
- 3.5 hour outage
- 200+ million affected

https://www.wired.com/story/video-hackers-take-over-power-grid-computer-mouse

ICS Components

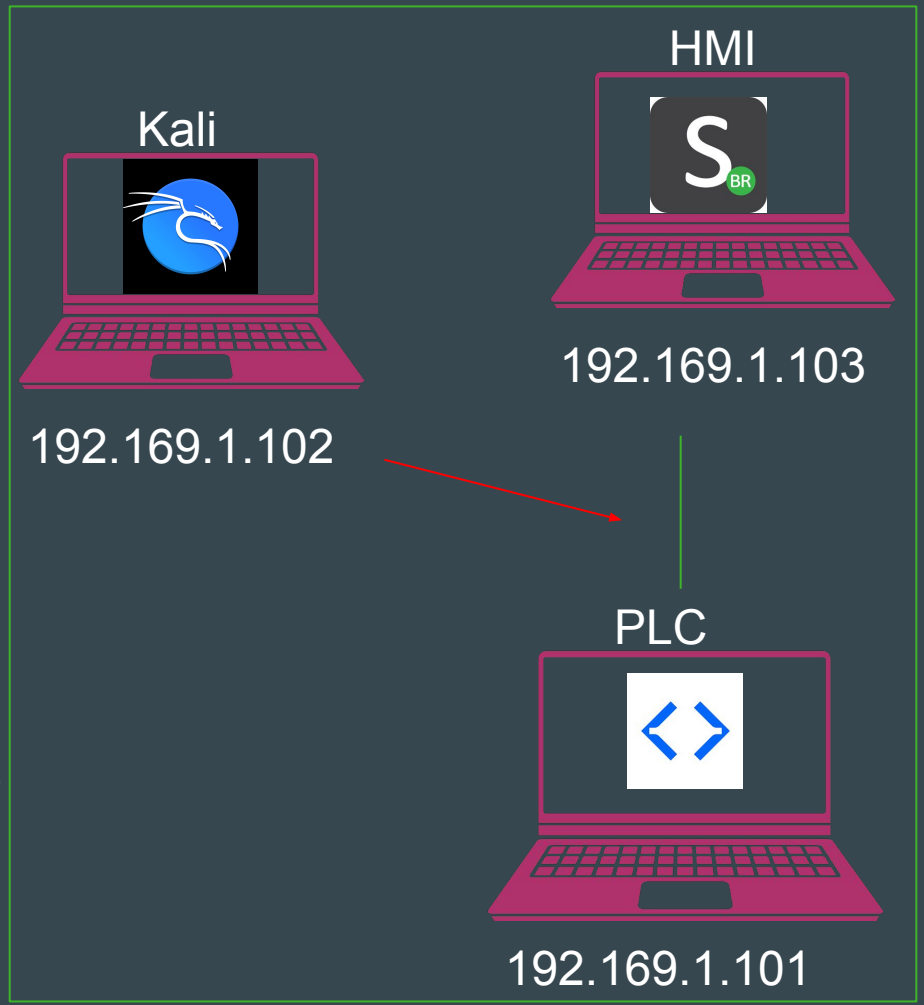
General

- PLC
  - Control machinery
  - Rugged, really low level
- HMI
  - Operator control of machine
  - GUI

Lab

- PLC
  - Ladder Logic made with OpenPLC editor
  - Hosted by OpenPLC runtime
- HMI
  - Hosted and made within ScadaBR

Topology



VirtualBox
Host-only network

Demo

Prevention

- Protect the IT layer
- Don’t get spear phished
- Secure segmentation

Questions?