A Demonstration of Free Cybersecurity Training

Scenario Demonstration By:
Mike Kwiatkowski
And
Tony Hills

Why this project?

- The need for cyber security will only increase
- StuxNet and Ransomware
- OT is different than IT
  - OT makes money
  - IT costs money
- Manufacturing and Critical Infrastructure are excellent targets

Why is this free?

- Cybersecurity Education for Advanced Manufacturing (CAMO)
- Made possible by National Science Foundation (NSF) award number 1800929
- Underscores importance of cybersecurity training in advanced manufacturing and critical infrastructure
- The award provide funding to develop training scenarios focused on industrial control systems distinctive environment

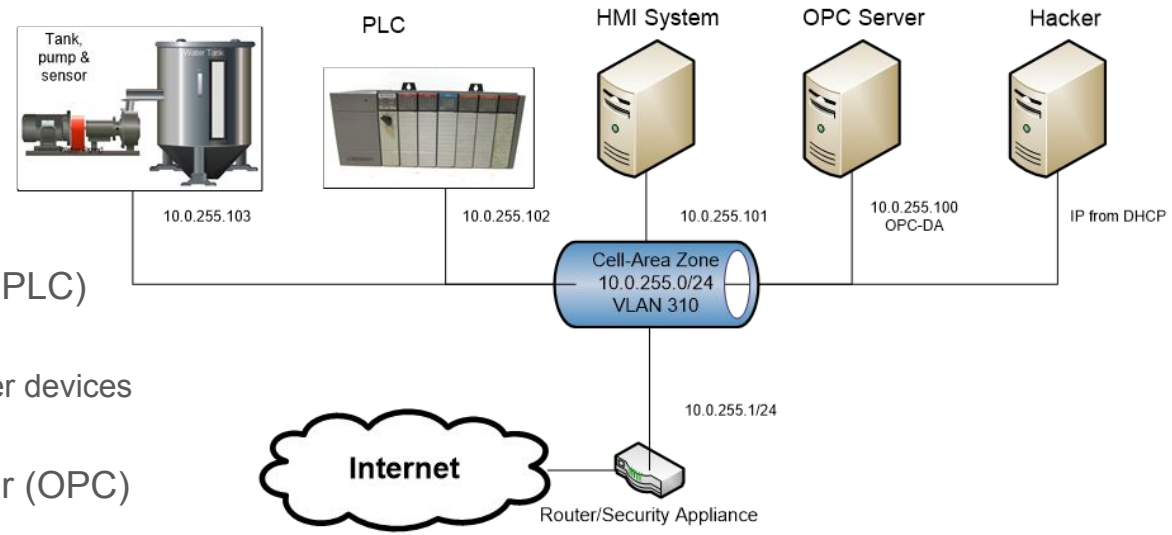
How is it kept free?

- NSF funding
- Use of “no cost” tools for the virtual lab environment
  - Open source software and operating systems
    - Free as Freedom! Free as in Beer!
  - Out of support software (XP anyone?)
    - It really does have a license!!
  - Demo versions of software
- Self hosting of virtual lab as needed

What is included?

- A Virtual Industrial Control Network (ICS)
- Videos
- Written material/presentations
- Labs
- Can be instructor led or self guided

Virtual Industrial Control (ICS) Lab



- Programmable Logic Controller (PLC)
- Sensor
  - And motors, actuators and other devices
- Human Machine Interface (HMI)
- Open Platform Computing Server (OPC)
- Security Appliance
  - pfSense firewall
- Hacker station
  - Kali workstation

PLC and Sensor systems

- Implemented using Arch Linux
- Simulated using Python program
- PyModbus - https://pymodbus.readthedocs.io/en/latest/
  - Modbus library for Python
- Python-snap7 - https://pypi.org/project/python-snap7/
  - Wrapper for Snap7. An open source Ethernet communication suite to interface with Siemen PLC systems

Other Open Source Systems

- Hacker workstation - Kali Linux
  - A toolbox build on top of Debian which focuses on network security applications
- Security Appliance - pfSense
  - A mature firewall/security appliance project with Community and Enterprise versions

Other “Free” Tools

- OPC Server
  - Runs on Windows XP
  - The OPC platform is PTC’s KepServerEX OPC server
  - https://www.ptc.com/en/products/kepware/kepserverex
- HMI Appliance
  - Runs Windows XP
  - The free Advanced HMI provides the HMI interface
  - https://www.advancedhmi.com/index.php?main_page=index&cPath=2

Available Training Scenarios

- Industrial Control System (ICS) Basics Scenario
- Wireshark Scenario
- Metasploit Scenario
- Zoning Scenario
- Virtual Private Network (VPN)/Firewall Scenario
- Intrusion Detection System/Intrusion Prevention System (IDS/IPS) Scenario

Why demo Wireshark?

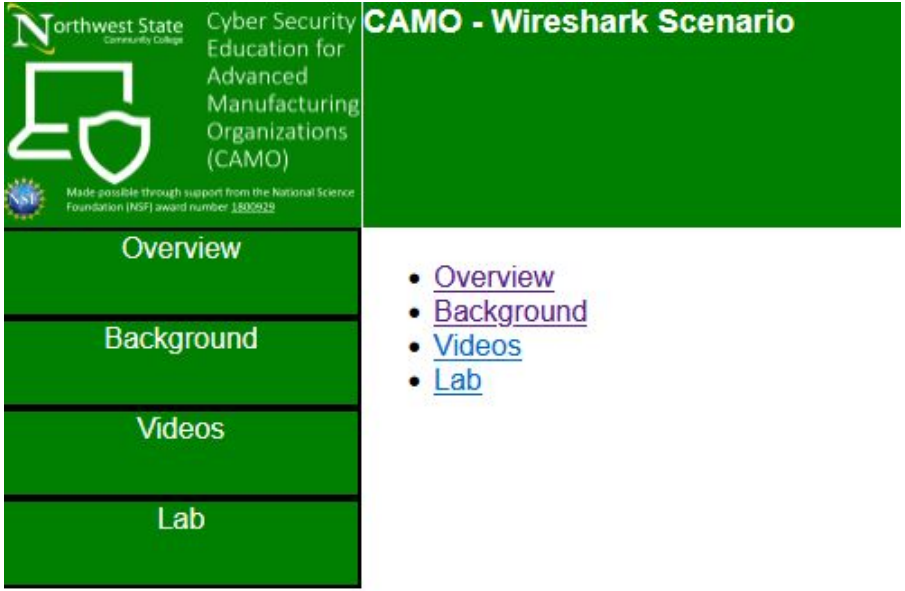
- Wireshark for the win!
- Important skill for data networking and security
- Common and mature open source tool
- Familiar to someone who may use this scenario for instructional purposes

Demonstration - How to use Wireshark

Access the scenario here:

https://www.nl.northweststate.edu/CAMO-Wireshark/

Scenario Layout



- Overview
  - List summary of lesson, learning outcomes and system configuration
- Background
  - A PDF and Powerpoint Point presentation over the material
- Video
  - Contains an original instructor led video lesson
- Lab
  - Actual virtual lab over material

Accessing the Virtual Labs

Where applicable there are separate instructions for performing the labs remotely or on local equipment.

- Local labs will be available using VMware and Virtualbox
  - With either hypervisor the entire VM must be downloaded
- Remote labs are currently hosted on our local infrastructure
  - We must set up accounts for access
  - Possible hosting site part our goal
- The VM’s are freely available for you to execute and maintain on your own virtualization solution as well

Accessing the Virtual Labs

To connect remotely to our infrastructure…

- Have us create accounts for your own use
- Use any modern browser and connect to
- https://guac.nl.northweststate.edu
- See the individual lab for further instructions!

DEMO Time!

Take a moment to connect remotely…

Let’s kick the tires!

Lab: https://www.nl.northweststate.edu/CAMO/scenarios/index.html

Remote Login: https://guac.nl.northweststate.edu

Send us a message if you wish to give it a try!!

Contact information

- Contact
  - Mike Kwiatkowski - mkwiatkowski@northweststate.edu
  - Tony Hills - thills@northweststate.edu
- References
  - CAMO Scenarios
    - https://www.nl.northweststate.edu/CAMO/scenarios/index.html
  - NSF Award
    - https://www.nsf.gov/awardsearch/showAward?AWD_ID=1800929
  - More Freely available resources and training from CISA
    - https://www.cisa.gov