





# Configuring an Intrusion Detection System for an Industrial Control System

Robert Hamilton
Information Security Specialist
Oklahoma CareerTech



**ATE**CENTERS



## Introduction

- Introduction
  - What is an ICS?
  - Currently working with ICS?
  - Used VMware?





### IDS Lab

- · Configure an IDS for a Control System
  - Part One Create a Security Onion
     Xubuntu VM COMPLETED! (pages 1-7)
  - Part Two Configure a Security Onion
     IDS for Control System protocols
     (pages 8-16) START on page 8
  - Part Three Use custom Pcap files to generate attack traffic on a Control System Network (pages 17-19)





### IDS Lab

- Part Two on page 8
  - Login: scada
  - Password: pipelineandsafety
- Page 11 step 20
  - After step 20 through step 36 on page 14, some new options not shown in lab. Use default settings.
- · Page 15 step 39 Make note of the rules file locations
- Page 16 steps 41 & 42 SKIP these steps
- Page 17 step 3 Takes up to 10 minutes to complete
- Page 17 step 5a Add "sudo" to the command
- Page 18 step 9 Use a capital "I" before security





## **Additional Tasks**

- · Open Modbus Pcap files in Wireshark
- Open DNP3 Pcap files in Wireshark
- Open snort.conf file
- Open pulledpork.conf file
- · Open downloaded.rules file





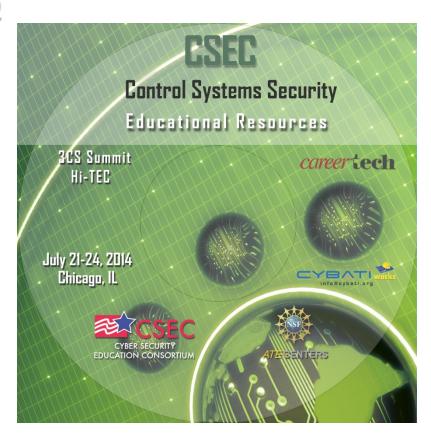
## Discussion

- Advantages of using IDS
- Limitations of an IDS
- Other options for ICS network monitoring
- Questions?



## Contents

- Instructor Training 3 Day Workshop
- Pipeline SCADA Security
- Cybati Resources
- DHS Documents
- DOE Cyber Security CD
- Reference Documents
- Vulnerabilities
- Significant Cyber Incidents
- Modbus PLC Trainer Information
- GE University Program





## **Contact Information**

# Robert Hamilton Oklahoma Department of CareerTech 405-743-5552

rhami@okcareertech.org

career tech





## **Contact Information**

#### Matthew Luallen

https://cybati.org/



