612.5

Covfefe Down!

SANS | GIAC CERTIFICATIONS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

All reference links are operational in the browser-based delivery of the electronic workbook.

SANS

Covfefe Down!

This page intentionally left blank.

Covfefe Down!

The plant is currently shutdown. Do not touch anything until after the morning meeting!

This page intentionally left blank.

Background

- During a scheduled maintenance and upgrade of some equipment at the Houston plant, there was a major storm that came in. Many workers were trapped and had to remain in the plant for about a week.
- Food was scarce and alcohol was in abundant supply.
- Floods damaged some equipment.
- Power outages occurred on and off throughout two evenings.
- There has been an ongoing labor dispute at the site as well. In preparation for a potential strike, there has been contractor and staff augmentation cross training.

This page intentionally left blank.

Current Status

Prior to plant start up –

- Operators are reporting inconsistencies across many elements of the environment.
- The vendors and integrators involved in the upgrades and maintenance have left to return to their homes.
- Plant managers have requested individual pod status updates in 30 minutes

This page intentionally left blank.

Prep for the Meeting

- Take the next 30 minutes to troubleshoot issues
- When all local issues are resolved, validate your local operation
- Identify any odd behaviors within your environment and report them in the meeting

This page intentionally left blank.

Status Meeting

- Field personnel Pod updates
- Operator Status
- Next Steps

This page intentionally left blank.

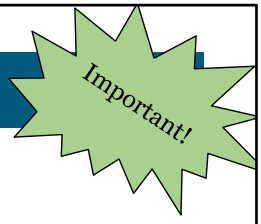
Post Meeting

- Continue to plug away
- Grab available personnel resources to resolve remaining issues
- Return the plant to acceptable pre startup condition

- Covefe CEO statement: “We did not come all this way and do all of this work to NOT grind beans!!!!”

This page intentionally left blank.

Quick Start Guide



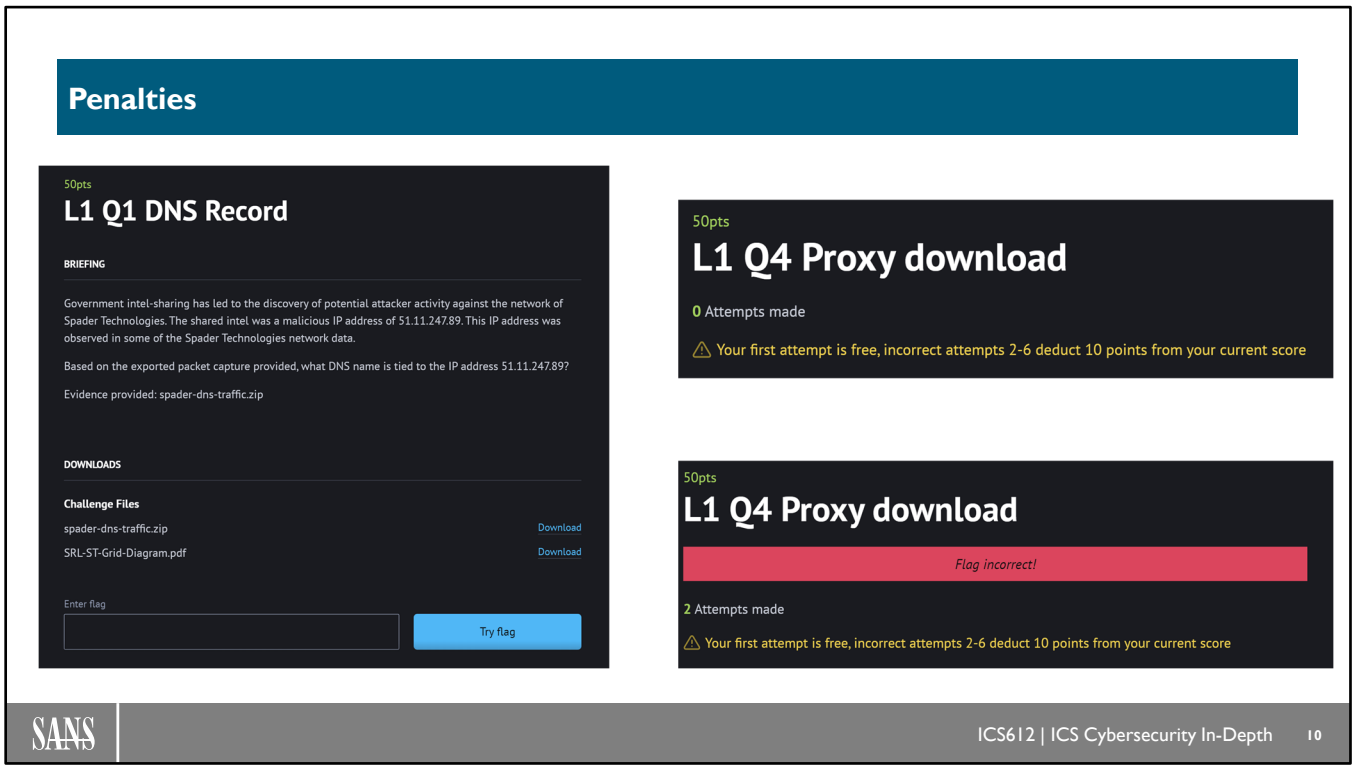
- Log in to the ranges.io portal at
- https://www.ranges.io
- Select “Sign up”
- Provide your name, email, and create a password
- Verify your email and then create your display name for the scoreboard
- Navigate to your “Events page” and wait for your instructor to give you an Event code for this class run
- When this opening presentation is complete, and everyone is ready your instructor will launch the event and you will have access to the challenges.

This page intentionally left blank.

Points

- Each question has a point value based on difficulty
- Answer correctly and you get points
- Wrong answers will cause you to lose points, and the penalties are unique to each question. In some cases, you may receive a free attempt and in other cases you will not (it will alert you with each challenge).
- How many points you are penalized for incorrect attempts varies by question, so pay attention to the information at the top of each challenge
- Do not brute force answers even if you lose no additional points; it is a violation of the Rules of Engagement

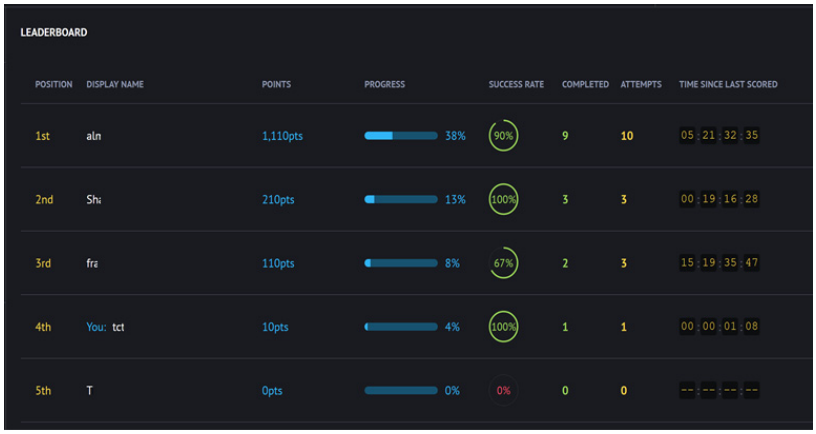
This page intentionally left blank.



This page intentionally left blank.

Scoreboard

- Top 10 individuals displayed on screen
- Stats
  - Score
  - Time since last score
  - Game Progress
  - Level Progress



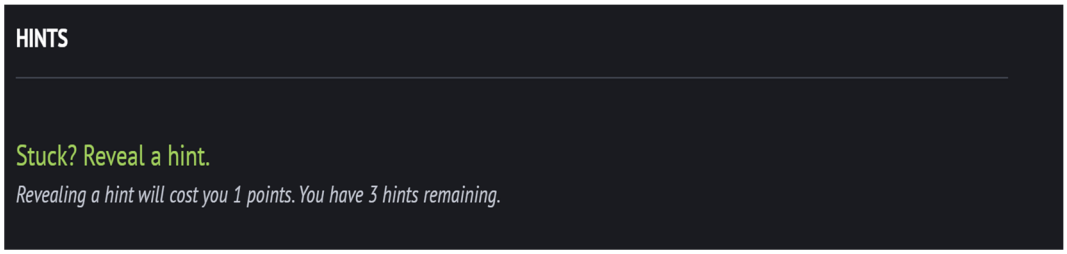
This page intentionally left blank.

Hints

- Take good notes!
- We have provided you with all the tools you need to solve the challenges
  - Pay attention to the answer format requirements for some questions!!!
  - Feel free to use your own tools
- Use the internet for research
- **Questions have hints available!**
  - Small penalties for hints vary by Level and impact how many points can be earned for a challenge
  - Tie-breaker at the end

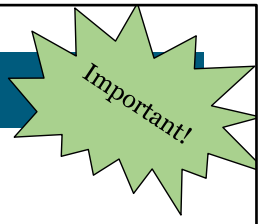
This page intentionally left blank.

Hints - Examples



This page intentionally left blank.

Quick Start Guide



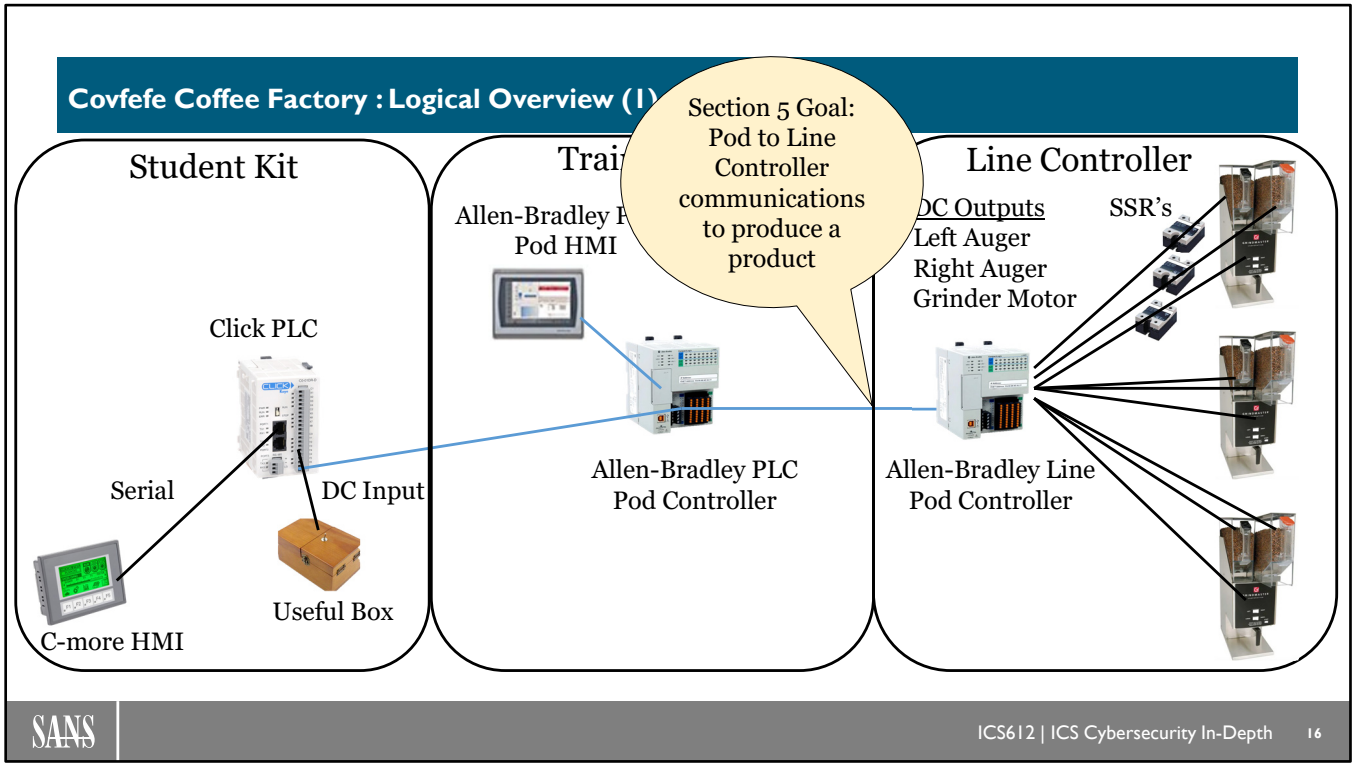
- Log in to the ranges.io portal at
- https://www.ranges.io
- Select “Sign up”
- Provide your name, email, and create a password
- Verify your email and then create your display name for the scoreboard
- Navigate to your “Events page” and wait for your instructor to give you an Event code for this class run
- When this opening presentation is complete, and everyone is ready your instructor will launch the event and you will have access to the challenges.

This page intentionally left blank.

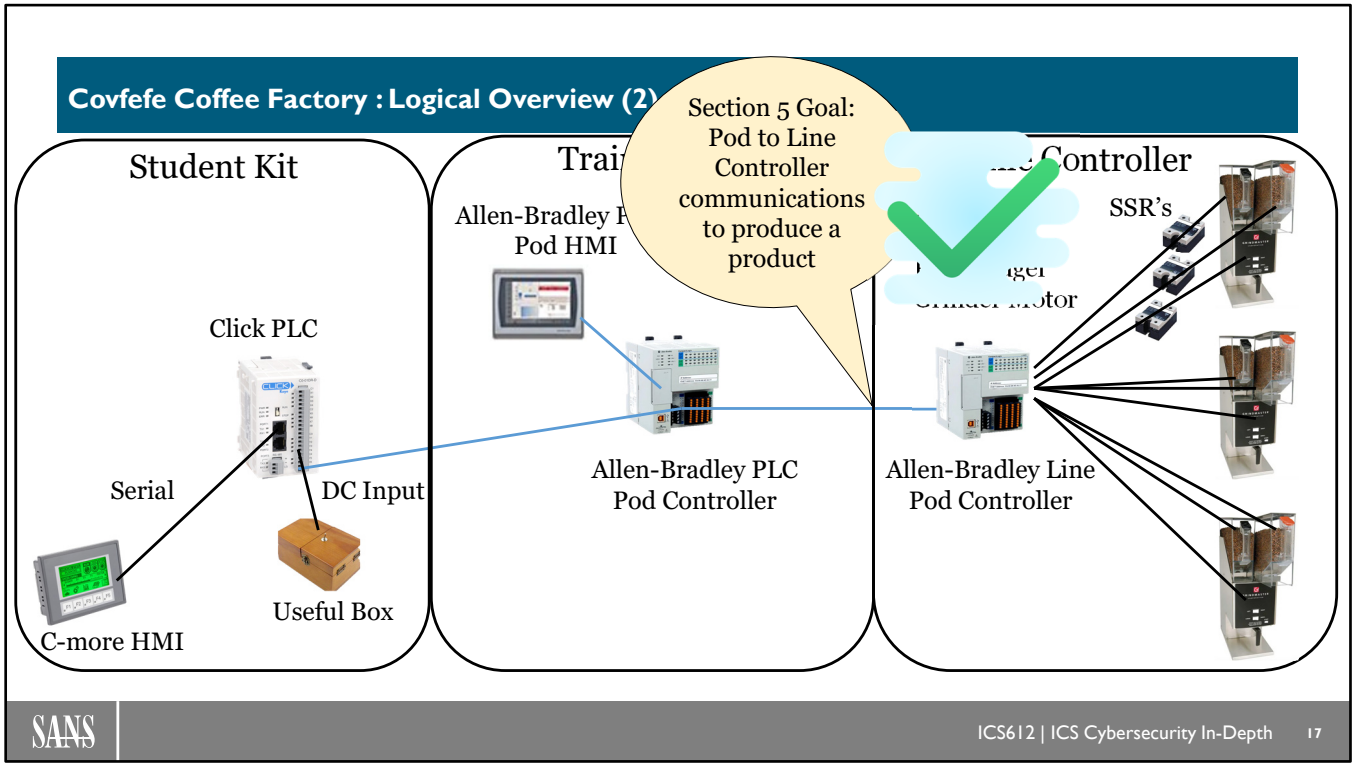
Join Key

Will be provided by instructor

This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

Section 5: Eval Link

This page intentionally left blank.

This page intentionally left blank.

COURSE RESOURCES AND CONTACT INFORMATION

AUTHOR CONTACT

Jason Dely
jdely@sans.org

Jeff Shearer
jshearer@sans.org

Tim Conway
tconway@sans.org

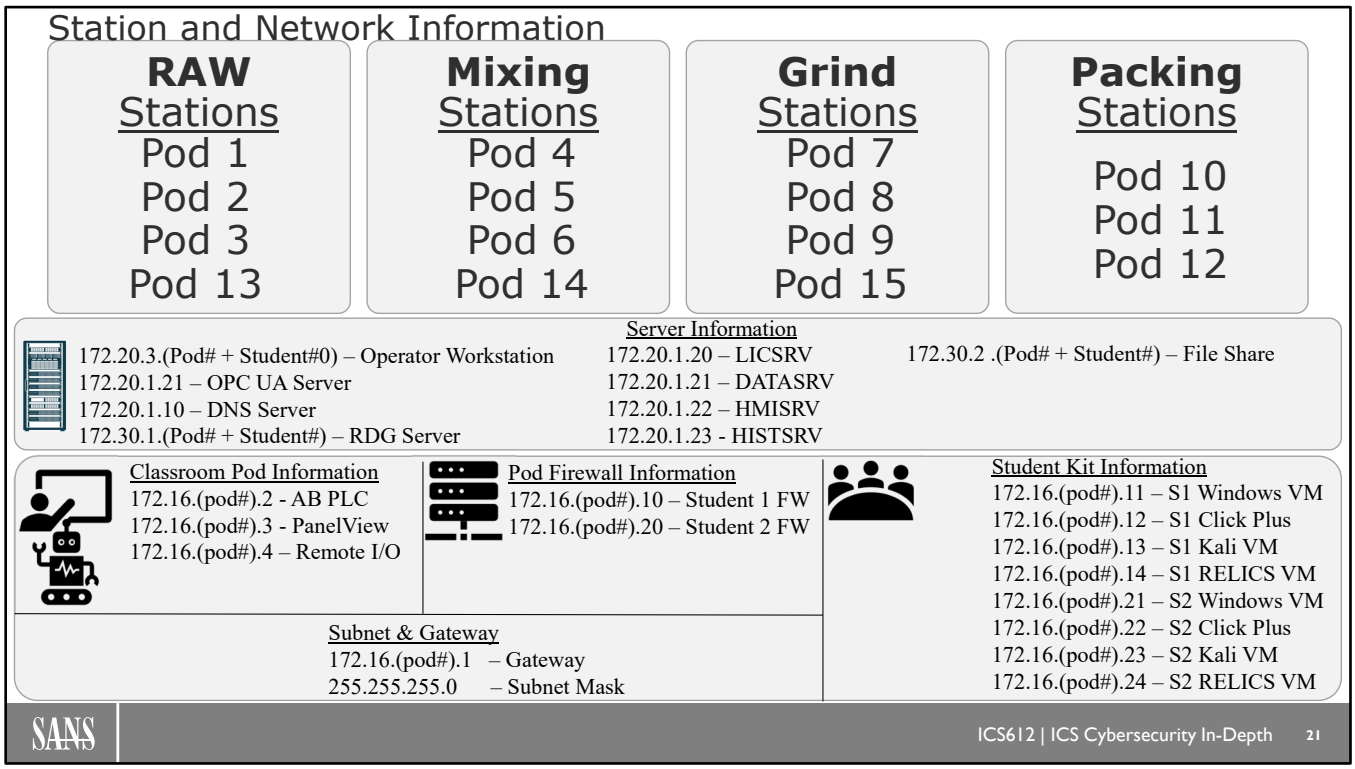
Chris Robinson
crobinson.sd@gmail.com

SANS INSTITUTE
11200 Rockville Pike
Suite 200
North Bethesda, MD 20852
301.654.SANS(7267)

ICS RESOURCES
https://ics.sans.org
https://ics-community.sans.org/
Twitter: @sansics

SANS EMAIL
GENERAL INQUIRIES: info@sans.org
REGISTRATION: registration@sans.org
TUITION: tuition@sans.org
PRESS/PR: press@sans.org

This page intentionally left blank.



This page intentionally left blank.

This page intentionally left blank.

Index

A

B

C

D

E

F

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W