KubeCon | CloudNativeCon

North America 2019

@tabbysable, @jimmesta, @petermbenjamin, @bradgeesaman

Attacking and Defending K8s Clusters

To be ready to go *before* we start, please:

1. Find a seat that you are comfortable with.
2. Connect your laptop to the wireless network.
3. Visit **https://securekubernetes.com** and complete the instructions in the **Getting Connected** section.

Don't fear! You only need a web browser and the ability to copy/paste commands to be able to fully participate!
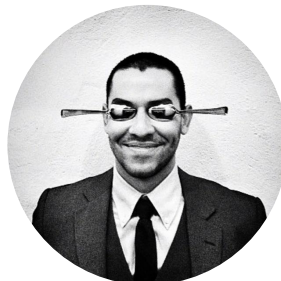
@tabbysable, @jimmesta, @petermbenjamin, @bradgeesaman

Meet Your Guides

Tabitha Sable
@tabbysable

Jimmy Mesta
@jimmesta

Peter Benjamin
@petermbenjamin

Brad Geesaman
@bradgeesaman

take a moment to meet your fine neighbors, too

Important Rules to Follow

1. Follow the provided instructions
2. ***Whisper*** while presenters are presenting
3. Ask your neighbor for help if you need it
   a. Confirm they want assistance ***before*** offering help
4. Raise your hand if you are completely stuck
5. Attack ***only*** your own cluster
6. Do not attack anything from your cluster
7. Remember to have fun

@tabbysable, @jimmesta, @petermbenjamin, @bradgeesaman

Plan of Attack (and Defense)

Activity	Time
Scenario 1: Guided Attack and Defense	25 mins
Scenario 2: Guided Attack and Defense	35 mins
Self-Guided Bonus Challenges	10 mins
Guided Bonus Challenges Walkthrough	10 mins

@tabbysable, @jimmesta, @petermbenjamin, @bradgeesaman

Getting Connected

Open the following URL in a Private/Incognito Window
https://securekubernetes.com

@tabbysable, @jimmesta, @petermbenjamin, @bradgeesaman

Free Compute

Scenario 1

@tabbysable, @jimmesta, @petermbenjamin, @bradgeesaman

Guided Attack and Defense

Proceed to **Scenario 1** *Attack* at
https://securekubernetes.com

@tabbysable, @jimmesta, @petermbenjamin, @bradgeesaman

Free Compute: Recap

- How did **Red** gain access?
- What was **Red** able to do?

- What did **Blue** discover?
- What did **Blue** do?
- What did **Blue** miss?

Persistence
Scenario 2

@tabbysable, @jimmesta, @petermbenjamin, @bradgeesaman

Guided Attack and Defense

Proceed to **Scenario 2** *Attack* at
https://securekubernetes.com

@tabbysable, @jimmesta, @petermbenjamin, @bradgeesaman

Persistence: Recap

- How did **DarkRed** gain access?
- What was **DarkRed** able to do?

- What did **Blue** discover?
- How did **Blue** remediate?

@tabbysable, @jimmesta, @petermbenjamin, @bradgeesaman

Bonus Challenges

- See if you can go even further and discover two more issues.
- If you complete both challenges, *whisper* the answers to us to get an **expert edition** sticker!

Proceed to **Bonus Challenges** at
https://securekubernetes.com

@tabbysable, @jimmesta, @petermbenjamin, @bradgeesaman

Bonus Challenges: Walkthrough

- Bonus Challenge 1: **Red**
  - Exploring the underlying host

- Bonus Challenge 2: **Blue**
  - Finding even more evidence of persistence
  - Tracing back to the attacker