

Continuous Security with Jenkins, Docker Bench, and Amazon Inspector

Sandro Cirulli
Oxford University Press (OUP)

CD Summit and Jenkins Days
Amsterdam - Berlin, October 2016



Content

1. Introduction
2. DevSecOps
3. Docker Bench + Demo
4. Amazon Inspector + Demo
5. Summary

About Me

- ▶ I work as Platform Tech Lead at **Oxford University Press**
- ▶ I am responsible for **system administration and DevOps**
- ▶ I co-organize **DevOps Oxford Meetup** and we're **looking for speakers!**

Oxford University Press (OUP)

- ▶ OUP is the **largest university press in the world**
- ▶ OUP is a world-renowned **dictionary publisher** and the home of the **Oxford English Dictionary**
- ▶ We recently launched the **Oxford Dictionaries API**

OXFORD
UNIVERSITY PRESS

**In 2015 an average of 25
software vulnerabilities
were discovered every day**

National Vulnerability Database

<https://web.nvd.nist.gov/view/vuln/statistics>

- ▶ DevSecOps is a cultural mindset where **everyone is responsible for security**
- ▶ **Continuous Security, Security as Code, and Security by Design**
- ▶ DevSecOps is **NOT DevOps + Security**

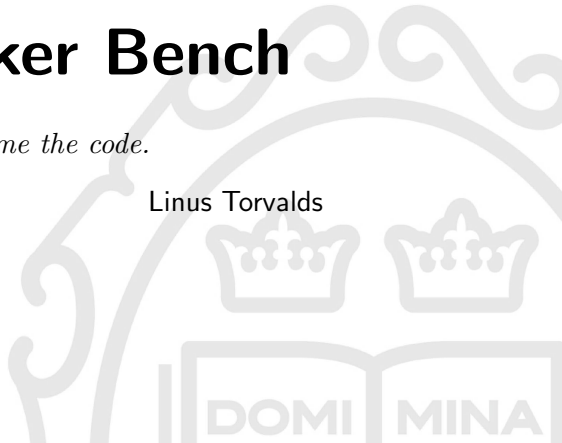
- ▶ Docker Bench is a script for checking **security best practices in Docker containers**
- ▶ Co-developed by **Diogo Mónica, security lead at Docker**
- ▶ Based on **CIS Docker 1.1.0 Benchmark**

Demo

Docker Bench

Talk is cheap. Show me the code.

Linus Torvalds



Amazon Inspector

- ▶ Amazon Inspector is an **automated security assessment service on AWS**
- ▶ Identifies **vulnerabilities at operating system and network levels**
- ▶ Scans against several **rules packages (CVE, CIS, etc.)**



Demo


Amazon Inspector

Talk is cheap. Show me the code.

Linus Torvalds



Integration with Jenkins Pipeline



Jenkins

Jenkins > CD Pipeline > Full Stage View

CD Pipeline - Stage View

	build	test	deploy
Average stage times:	11s	18s	76ms
#9 Sep 26 10:51 No Changes	10s	18s	84ms (paused for 19s)
#8 Sep 26 10:45 No Changes	12s	18s	68ms (paused for 18s)
#7 Sep 23 18:13	13s	18s	76ms (paused for 5s)

Summary

- ▶ DevSecOps is cultural mindset where **everyone is responsible for security**
- ▶ Docker Bench is a script for checking **security best practices in Docker containers**
- ▶ Amazon Inspector is an **automated security assessment service on AWS**
- ▶ Focus on **Continuous Security** rather than a specific tool

Thank you for your attention!

OXFORD
UNIVERSITY PRESS

Contact:

sandro.cirulli@oup.com

www.sandrocirulli.net/contact

Slides:

www.sandrocirulli.net/cd-summit-and-jenkins-days-2016

Blog Posts:

www.sandrocirulli.net/continuous-security-with-jenkins-and-docker-bench

www.sandrocirulli.net/continuous-security-with-jenkins-and-amazon-inspector

Links:

Oxford Dictionaries API: developer.oxforddictionaries.com

DevOps Meetup Oxford: www.meetup.com/doxford