INGUARDIANS™

THE BUST-A-KUBE CTF: ATTACKING AND DEFENDING A MULTITENANT KUBERNETES CLUSTER

BLUEHAT UNDERGROUND SEATTLE 2018

Jay Beale, CTO and COO at InGuardians

@jaybeale and @inguardians

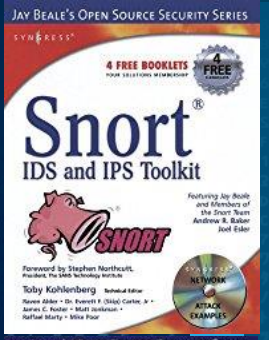
November 19, 2018

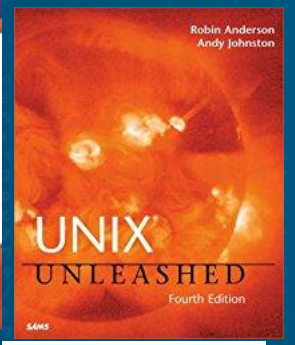
Jay Beale is a Linux security expert who has created several defensive security tools, including Bastille Linux/UNIX and the CIS Linux Scoring Tool, both of which were used widely throughout industry and government. He has served as an invited speaker at many industry and government conferences, a columnist for Information Security Magazine, SecurityPortal and SecurityFocus, and a contributor to nine books, including those in his Open Source Security Series and the “Stealing the Network” series. He has led training classes on Linux Hardening and other topics at Black Hat, CanSecWest, RSA, and IDG conferences, as well as in private corporate training, since 2000. Jay is a co-founder, Chief Operating Officer and CTO of the information security consulting company InGuardians.

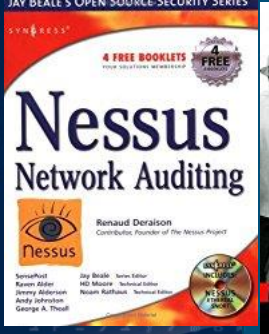
InGuardians is a leading information security consultancy with offices in Seattle, Boston, Chicago, Dallas, Atlanta and Washington, DC.

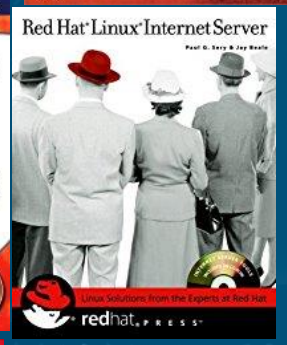
InGuardians™

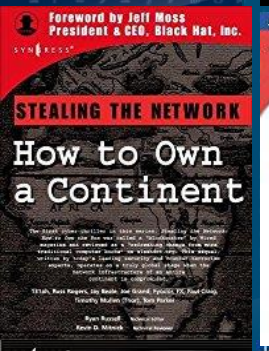
Graphical Bio

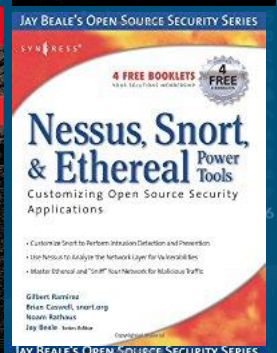


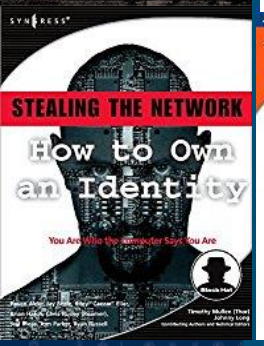


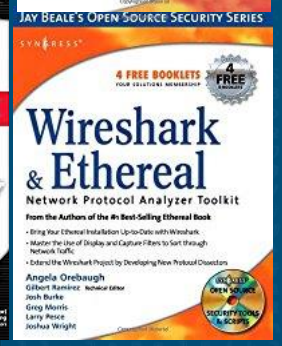


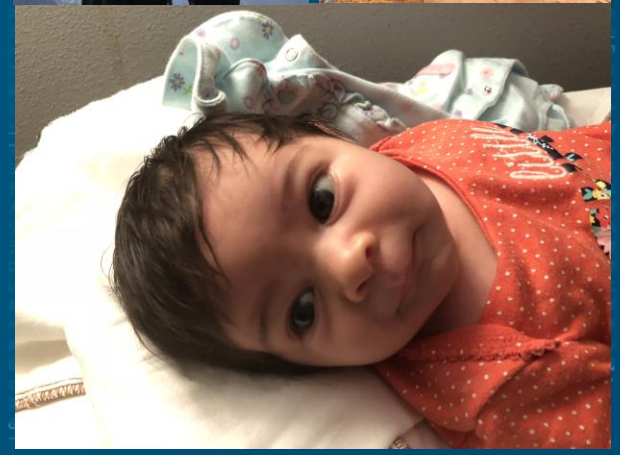












AIKIDO ON THE COMMAND LINE - LINUX LOCKDOWN AND PROACTIVE SECURITY

JAY BEALE, INGUARDIANS | AUGUST 4-5 & AUGUST 6-7

CIS Center for Internet Security®

OVAL®

SANS

DEFCON 11

toorcon

SecurityFocus™

CAN SEC WEST

INGUARDIANS™ RED TEAM

INGUARDIANS™

Talk Table of Contents

- What's a Kubernetes?
- Demo: Attack on a Multitenant Kubernetes Cluster
- Review of the Attack Path

Demo: Attacking a Multitenant Kubernetes Cluster

Take a look at a couple more involved Kubernetes attack and defense talks:

https://www.beyondtrust.com/resources/webinar/hacking-defending-kubernetes-based-application/

In this, we'll attack a Kubernetes cluster that has a soft multitenancy setup, with a Marketing department and a Development department.

What's Kubernetes?

Kubernetes orchestrates containers.

For our purposes:

Nodes run Docker, which run containers

Kubernetes coordinates multiple nodes, running Docker and a Kubelet

What Attack Steps Do I Have in Kubernetes?

Here are some of the attack steps we have available in Kubernetes:

- Exec a command / shell in a container via the API server
- Launch a container onto the cluster via the API server
- Abuse or set up a "volume mount" to steal/modify data or the host itself
- Ask a Kubelet to exec a command / shell in an existing container
- Interact with the Docker daemon on the host
- Interact with the internal or external networks

What You're About to See

In this video demo, we'll attack a Kubernetes cluster that has a soft multitenancy setup, with a Marketing department and a Development department.

Review of the Attack Path (1 of 2)

- Found a backdoor left by another attacker who had compromised Wordpress.
- Used the backdoor to enter Marketing's Wordpress container. (Flag 1)
- Moved into Marketing's MySQL container (Flag 2)
- Used the MySQL container's unfettered network access to reach a Kubelet on the master node.
- Used the Kubelet's lack of authentication to invade Development's dev-web container. (Flag 3)
- Reasoning that the dev-sync container in this same pod might be used to synchronize content, gained the pod's secrets (SSH key and account).

Review of the Attack Path (2 of 2)

- Authenticated to the high-value Developer machine. (Flag 4)
- Returned to the cluster, used the dev-web pod's placement on the master to gain control of the AWS account. (Bonus)

INGUARDIANS™

WEEKLY EXECUTIVE BRIEFING