Offensive Security: Hacking in the Clouds

Workshop & Hands-On Technical Lab Overview

Target Audience	Security Architects, Security Engineers, Software Engineers. No hacking experience required! A basic understanding of cloud and web applications is assumed.
Duration	4–6 Hours (Hands-On Technical Lab and Workshop)
Focus Area	Offensive Cyber Operations, Adversary Mindset, Attack Surface Exploitation
Format	On-site workshop for up to 15 attendees (English, Swedish, or Spanish)
Requirements	Internet access. Attendees bring their own laptops. No software installation required.

Objective

To defend our assets in the public and private clouds, we need to understand our adversary. We must understand the intruders' techniques and how they can attack our cloud assets and our applications in the cloud.

.

Practical Exercises

Attendees will operate within an isolated lab environment, systematically executing each phase. Each phase will reveal more details to the attacker, turning the exercises into a gamified treasure hunt!

- **Reconnaissance:** Learn about the target's cloud assets in AWS and Azure (and find out who works as developer in the targets Software Development department).
- **Stealing Keys:** Find and steal keys and secrets, from developer's laptop, from GitHub or from a vulnerable application.
- **Hacking the turned off computer:** With stolen keys we could do what seems impossible, completely compromise a computer that is turned off!
- **Exploring Kubernetes:** We will hack into a Kubernetes container and see if we can move laterally inside the cluster, across namespaces.

.