Contribution ID: **17** Type: **not specified**

Attacking AWS - From initial access to hardcore persistance

Cloud platforms like Amazon Web Services (AWS) are foundational to many critical infrastructures and enterprise applications, making them prime targets for attackers. In this session, we will not only explore the most relevant attack vectors cybercriminals use to compromise AWS infrastructures but will also simulate these attacks using known threat actor techniques in an adversary emulation context. From initial access to hardcore persistence, this talk will provide a comprehensive look at how attackers operate in AWS environments.

We will take a technical journey through the tactics, techniques, and procedures (TTPs) employed by attackers at every stage of the threat lifecycle, aligned with the MITRE ATT&CK framework. We'll start by reviewing common methods of initial access, such as exploiting exposed credentials or vulnerabilities in services like IAM, Lambda, and EC2. From there, we'll detail how attackers escalate privileges, move laterally, and evade detection from tools like CloudTrail.

The session will conclude with an in-depth look at advanced persistence techniques in AWS, including the manipulation of IAM policies, backdooring Lambda functions or Docker containers, and tampering with logs. Along the way, we'll demonstrate how security teams can implement defensive and detection strategies to mitigate these risks. By leveraging AWS-native services and third-party tools, attendees will learn how to enhance their incident response capabilities.

This hands-on workshop will give attendees practical, technical insights into AWS security, adversary behavior, and how to better defend against sophisticated, persistent attacks. With only two slides and full hands-on experience, this talk ensures deep technical immersion.

Length

120 minutes

Optional: Speaker / convener biography

Former Police Officer from Argentina, now a Cloud Incident Responder and Security Engineer with over 10 years of IT experience. A Digital Nomad an international speaker, I've presented on Cloud Security and Incident Response at Ekoparty, FIRST, Virus Bulletin (three times), Hack.Lu, and various BSides events worldwide. I hold a Bachelor's degree in Information Security and an MBA (Master in Business Administration).

Primary author: ABASTANTE, Santiago (Solidarity Labs)

Track Classification: Workshops, training, tabletop games, hands-on exercises, birds of a feather sessions, etc.