

Hacking and Securing Cloud Infrastructure

2 day class

Get Certified



Brand new for 2019, this 2-day class cuts through the mystery of Cloud Services (including AWS, Azure and G-Cloud) to uncover the vulnerabilities that lie beneath. We will cover a number of popular services and delve into both what makes them different, and what makes them the same, as compared to hacking and securing a traditional network infrastructure.

Whether you are an Architect, Developer, Penetration Tester, Security or DevOps Engineer or anyone with a need to understand and manage vulnerabilities in a Cloud environment, understanding relevant hacking techniques and how to protect yourself from them is critical. This class covers both the theory as well as a number of modern techniques that may be used to compromise various Cloud services and infrastructure.

WHO SHOULD TAKE THIS CLASS

Cloud Administrators, Developers, Solutions Architects, DevOps Engineers, SOC Analysts, Penetration Testers, Network Engineers, security enthusiasts and anyone who wants to take their skills to next level.

Prior pen test experience is not a strict requirement, however, some knowledge of Cloud Services and a familiarity with common command line syntax will be greatly beneficial.



STUDENT PREREQUISITES

Students must bring their own laptop and must either be able to launch a Docker Container provided by us, which includes all tools required for the class, or have root/admin access and be comfortable installing command line tools and downloading and building tools from source on GitHub, such as AWS CLI and Nimbostratus and more tools.

CLASS CONTENT

Prior pen test / security experience is not a strict requirement, however, some knowledge of Cloud Services and a familiarity with common Unix command line syntax will be beneficial. The syllabus for the class is as follows:

- Introduction to Cloud Computing
- Why cloud matters
- How cloud security differs from conventional security
- Types of cloud services
- Legalities around attacking / pen testing cloud services.
- Understanding the Attack Surfaces of various Cloud offerings, such as IaaS, PaaS, SaaS, FaaS
- Exploiting serverless applications
- Owning cloud machines
- Attacking cloud services such as storage service or database services
- Examples and case studies of various cloud hacks
- Privilege escalation (horizontal and vertical) and pivoting techniques in cloud
- Obtaining persistence in cloud
- Exploiting dormant assets: Id's, services, resources groups, security groups and more
- Cloud Infrastructure Defence
- Monitoring and logging
- Benchmarks
- Auditing Cloud Infrastructure (Manual and automated approach)
- Base Images / Golden Image auditing for Virtual Machine / Container Infrastructure
- Preventive measures against cloud attacks
- Host-based Defence
- Using Cloud services to perform defence
- Ending CTF to reinforce the learning

CLASS TAKEAWAY

Our own pre-bundled Docker Image containing all the tools needed to begin hacking/auditing/securing the Cloud.