Hacking and Securing Cloud Infrastructure

Training Course

28th & 29th of October

Table of Contents

All training courses are two full days of intensive, hands-on learning and include complimentary morning tea, lunch and afternoon tea. Tickets can be secured by going to the website https://appsecday.io/.

Course Abstract

Brand new for 2019, this 2-day course 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, Pentester, 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 course covers both the theory a well as a number of modern techniques that may be used to compromise various Cloud services and infrastructure. Prior pentest / 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.

Highlights of our Trainings:
• Attacking Cloud Services
• Gaining Entry via exposed services
• Attacking specific cloud services
• Post - Exploitation
• Defending the Cloud Environment
• Host base Defenses
• Auditing and benchmarking of Cloud
• Continuous Security Testing of Cloud

What attendees will learn?

Students will gain knowledge of attacking, exploiting and defending a variety of Cloud infrastructure. First, they will play the part of the hacker, compromising serverless apps, cloud machines, storage and database services, dormant assets and resources. Students will learn privilege escalation and pivoting techniques specific to cloud environments. This is followed by Infrastructure Defense, secure configuration, auditing, logging, benchmarks. Students will learn preventive measures against cloud attacks, host-based defense and a number of cloud tools that can help in securing their services and resources.

Apply the learning to
• Identify weaknesses in cloud deployment
• Fix the weaknesses in your cloud deployment
• Monitor your cloud environment for attacks

What attendees will be provided?

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

What attendees should bring?

A laptop administrative privileges will be useful. Some challenges might require creation of trial accounts towards cloud service providers, Azure, AWS, GCP.

Pre-requisites

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 course, 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..

Detailed Outline

Day 1

- Introduction to Cloud Computing
  - What is cloud
  - Why cloud security matters
  - Types of clouds and cloud services
  - What changes from conventional security models
  - Shared responsibility model
  - Legalities around Cloud Pentesting

- Attacking Cloud Services
  - How to approach pentesting cloud services
  - Understand the attack surface in each type of cloud
  - Enumerating for cloud assets
  - Roles and permissions based attacks

- Gaining Entry via exposed services
  - Lambda based attacks
  - Web application Attacks
  - Exposed Service ports
- Attacking specific cloud services
  - Storage Attacks
  - AD Attacks
  - DB and other services
  - Finops attacks
  - IAM Misconfiguration Attacks
  - Dormant assets
- Post – Exploitation
  - Maintain access after the initial attack
  - Post access enumeration
  - Snapshot access

Day 2

- Defending the Cloud Environment
  - Setting up Monitoring and logging of the environment
  - Catching various attacks (reference to previous attacks and how those can be caught)
  - Metadata API Protection
- Host base Defenses
  - Windows server auditing

    - Linux Server Auditing
- Auditing and benchmarking of Cloud
    - Prepare for the audit
    - Automated auditing via tools
    - Golden Image / Docker image audits
    - Relevant Benchmarks for cloud
- Continuous Security Testing of Cloud
    - Continuous inventory updating by extracting list of Assets from the Cloud Environment
    - Automated scans to pick changes in environment and setup
      Beer101

Trainer Biography

Anthony Webb

https://www.linkedin.com/in/antjwebb/

Anthony Webb works as a Principal Consultant with NotSoSecure. His expertise involves Cloud Security, Infrastructure Security, penetration testing and red teaming. he has delivered multiple advanced training at conferences such as Black Hat, CPX360, as well as smaller classroom groups and live web-based training delivery.