Hacking and Securing Cloud Infrastructure 4 Days

2021 EDITION

This 4-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 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 knowing how to protect yourself from them is critical. This course covers both the theory as 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 familiarity with common Unix command-line syntax will be beneficial.

This 4 Day class is the perfect class for cloud practitioners (defenders and attackers alike) who would like to have a deeper understanding of cloud environments and various attack surfaces. The training also extensively deals with defensive scenarios and various labs around defending cloud environments providing a 360 degree coverage on cloud security.

Note: Students will have access to a state-of-the-art Hacklab with a wide variety of vulnerabilities to practice exploitation and will receive a FREE 1 month subscription after the class to allow more practice time along with the support portal to clear doubts.

Delegates Requirements

Students must bring their own laptops and have admin/root access on it. The laptop must have a virtualization software (virtualbox / VMWare) pre-installed. A customized version of Kali Linux (ova format) containing custom tools and the scripts for the class will be provided to the students. The laptop should have at least 4 GB RAM and 20 GB of free disk space dedicatedly for the VM.

Delegates Receive

Numerous scripts and tools (some public and some NotSoPublic) will also be provided during the training, along with the student handouts.

Our courses also come with detailed answer sheets. That is a step by step walkthrough of how every exercise within the class needs to be solved. These answer sheets are also provided to students at the end of the class.

KEY TAKEAWAYS

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. Second, they will play the defender where they will learn about 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

The free 30 day lab access provides attendee surplus time to learn advanced topics in their own time and at their own pace.

Who Should Attend

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

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

NotSoSecure part of claranet cyber security®

For more information:

UK: +44 (0)1223 653 193
US: +1 (628)200-3053/3052
Email: contact@notsosecure.com
Visit: notsosecure.com

Hacking and Securing Cloud Infrastructure 4 Days

Continued

2021 EDITION

Course Outline

- Gaining Entry in cloud 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

INTRODUCTION TO CLOUD COMPUTING

- Introduction to cloud and why cloud security matters
- Comparison with conventional security models
- Shared responsibility model
- Legalities around Cloud Pentesting
- Attacking Cloud Services

ENUMERATION OF CLOUD ENVIRONMENTS

- DNS based enumeration
- OSINT techniques for cloud based asset identification

GAINING ENTRY VIA EXPOSED SERVICES

- Serverless based attacks (AWS Lambda / Azure & Google functions)
- Web application Attacks
  - SSRF Exploitation over AWS ElasticBeanStalk
  - Exploiting vulnerable applications over GCP and Azure

ATTACKING STORAGE SERVICES (AWS, AZURE, GCP)

- Exploring files in storage
- Exploring SAS URL's in Azure
- Achieving privilege elevation via secrets in Storage
- Remote code Execution via storage in PaaS, FaaS environment

ATTACKING AZURE AD ENVIRONMENT

- Enumeration in Azure AD
- Various Azure Services
- Azure Service exploitation
- Stealing secrets from Azure services

IAM MISCONFIGURATION ATTACKS

- Exploiting Shadow admins in AWS and Azure
- Attacking AWS Incognito misconfigurations

EXPLOITING PLATFORM AS A SERVICE ENVIRONMENTS (AWS BEANSTALK AND OTHERS) POST – EXPLOITATION

- Persistence in Cloud
- Post exploit enumeration
- Snapshot access
- Backdooring the account

CONTAINERS AS A SERVICE AND K8S EXPLOITATION

- Understanding how container technology work (namespaces, cgroup, chroot)
- From docker to kubernetes
- Identifying vulnerabilities in docker images
- Exploiting misconfigured containers
- Exploiting docker environments and breaking out of containers
- Exploring kubernetes (k8s) environments
- K8s exploitation and breakouts
- Pivoting to host OS

DEFENDING CONTAINERS

- Container Image security basics
- Container Host security

DEFENDING K8S

- Authentication Methods and Configuration
- Native Authorization and Third Party Solutions
- Cluster Network Protections
- Monitoring K8s Environments

DEFENDING THE CLOUD ENVIRONMENT

- Identification of cloud assets
  - Inventory Extraction for AWS , Azure and GCP
  - Continuous inventory management
- Protection of Cloud Assets
  - Principle of least privilege
  - Control Plane and Data Plane Protection
  - Financial Protections
  - Cloud specific Protections
  - Metadata API Protection
- Detection of Security issues
  - Setting up Monitoring and logging of the environment
  - Identifying attack patterns from logs
  - Revisiting day 1 attacks via logs
  - Real time monitoring of logs
  - Monitoring in multi-cloud environment
- Response to Attacks
  - Automated Defense techniques
  - Cloud Defense Utilities
  - Validation of Setup

AUDITING AND BENCHMARKING OF CLOUD

- Preparing for the audit
- Automated auditing via tools
- Golden Image / Docker image audits
- Auditing Kubernetes Environments using Opensource tools
- Windows IaaS auditing
- Linux IaaS Auditing
- Relevant Benchmarks for cloud

CTF TO REINFORCE LEARNING

NotSoSecure part of claranet cyber security®

For more information:

UK: +44 (0)1223 653 193
Email: contact@notsosecure.com
US: +1 (628)200-3053/3052
Visit: notsosecure.com