Hacking Cloud Infrastructure 2 Days

This 2-day course cuts through the mystery of Cloud Services (including AWS, Google Cloud Platform (GCP) and Azure) 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 class covers both the theory a well as a number of modern techniques that may be used to compromise various Cloud services and infrastructure.

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 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.

Delegate Requirements

Delegates must bring their own laptop 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, scripts and VPN 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 dedicated for the VM.

Course Takeaway

Our own customized version of kali linux with inhouse developed scripts and tools to help with hacking auditing and securing Cloud.

NotSoSecure part of claranet cyber security

Course Outline

DAY 1

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

DAY 2

IAM MISCONFIGURATION ATTACKS

- Attacking AWS cognito misconfigurations
- Exploiting Shadow Admins in AWS

POST - EXPLOITATION

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

EXPLOITING KUBERNETES CLUSTERS & CONTAINER AS A SERVICE

- Understanding how container technology works
- Exploiting docker environments and breaking out of containers
- K8s exploitation and breakouts

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

For more information:

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