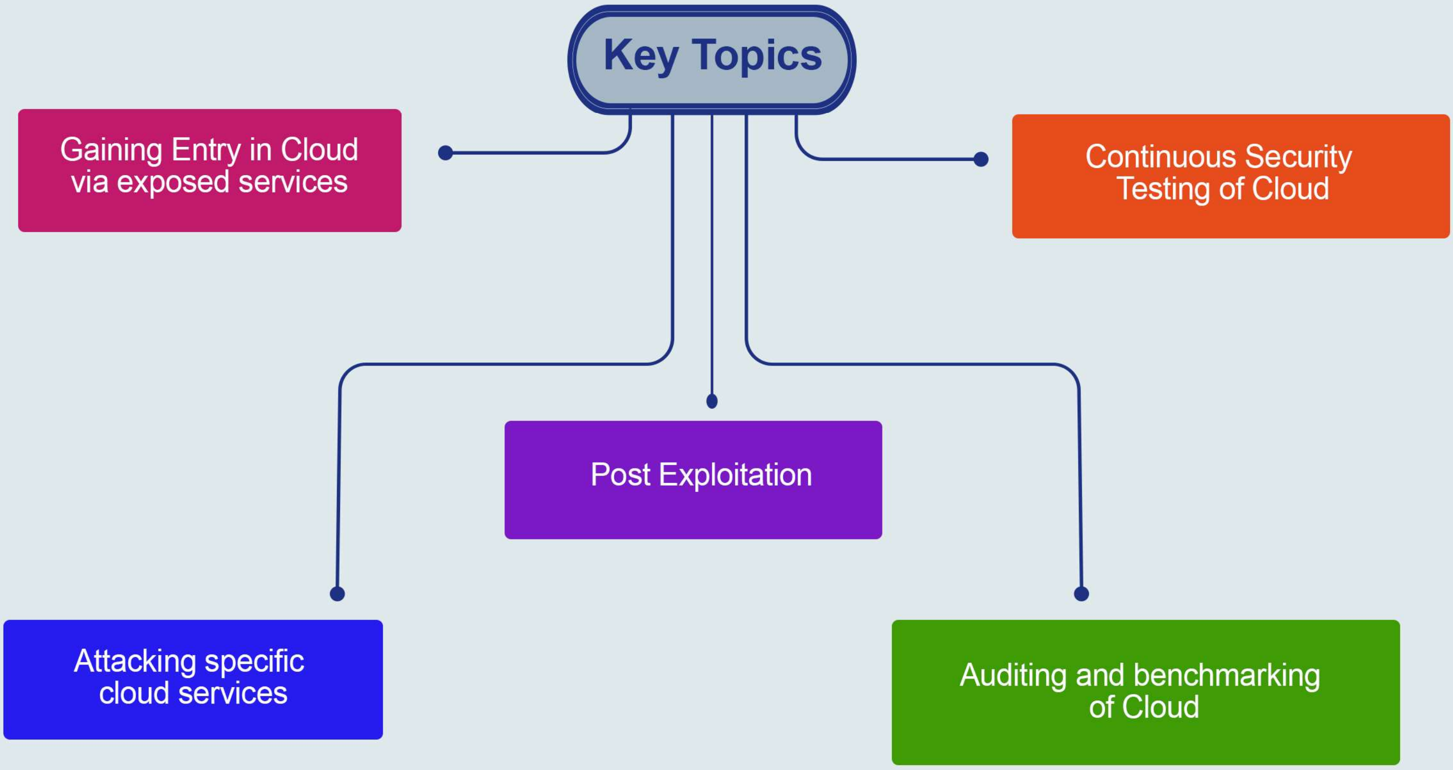
About the Course

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 and will equip you with the latest in cloud-focused penetration testing techniques and teach you how to assess cloud environments. You will learn specific tactics for penetration testing in Azure and Amazon Web Services, particularly important given that AWS and Microsoft account for more than half the market.

Learning Objectives

1. Gain knowledge of offensive cloud security hacking tools
2. Exploiting a variety of Cloud services and infrastructure
3. Compromising serverless apps, cloud machines, storage and database services
4. Pivoting techniques specific to cloud environments
5. Identify weaknesses in cloud deployment
6. Monitor your cloud environment for attacks

Key Topics


Key Topics
Gaining Entry in Cloud via exposed services
Continuous Security Testing of Cloud
Post Exploitation
Attacking specific cloud services
Auditing and benchmarking of Cloud

Pre Requisites

It is necessary to take the following courses:

- Ethical Hacking & Penetration Testing Concepts
- Ethical Hacking & Penetration Testing Tools
- Virtualization & Cloud Security

What You Will Receive

- Course Presentation File
- Complementary Files
- Cloud Ethical Hacking & Penetration Testing eBook

Who Should Attend

- CISOs
- Cloud Pentesters
- Threat & Vulnerability Analusts

Syllabus

Enumeration of Cloud environments

- Inventory Extraction for AWS, Azure and GCP
- Continuous inventory management
- DNS based enumeration
- OSINT techniques for cloud-based asset
- Serverless based attacks (AWS Lambda / Azure & Google functions)
- Web application Attacks

Vulnerabilities

- TravisCI and Git Actions
- Deployment Pipelines
- Web Application Injections
- Server Side Request Forgeries and Their Impacts
- Command Line Injections
- Serverless Functions in AWS
- Serverless Functions in Azure
- Exposed Databases and Ports
- SQL Injections in Cloud Applications

Gaining Entry in Cloud Environment

- Gaining entry via exposed services
- Serverless based attacks (AWS Lambda / Azure & Google functions)
- Web application attacks
- Exposed service ports

Syllabus

Attacking Cloud Services

- Storage Attacks
- Azure AD Attacks
- Containers and Kubernetes Clusters
- IAM Misconfiguration Attacks
- Roles and permissions-based attacks
- Attacking Incognito misconfigurations
- Mimikatz and PRT
- Microsoft Graph for Data Exfiltration
- AWS IAM Privilege Escalation Paths
- AWS Compute
- Amazon KMS and Keys
- PACU for AWS Attack Automation
- Azure Virtual Machines
- Code Execution on Azure VMs

Attacking Identity Systems

- The Mapping Process
- Authentications and Key Material
- AWS Command Line Interface (CLI) Introduction
- Azure CLI Introduction
- Username Harvesting
- Unauthenticated Fileshares
- Microsoft Identity Systems and Azure Active Directory
- Authentication Standards in the Web
- SAML and Golden SAML
- Introduction to Postman

Syllabus

Infrastructure Attacks

- Kubernetes and Kubernetes Clusters
- Leveraging Backdoors in Clusters
- Red Team and Methodologies
- Heavy and Lite Shells
- Data Smuggling
- Domain Fronting
- Avoiding Detections

Post – Exploitation

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

Hands-on Training

- Lab 1: Hunting for Key Material
- Lab 2: AWS User Enumerations
- Lab 3: Username Harvesting in Azure
- Lab 4: Discovery Open File Shares
- Lab 6: Microsoft Graph API and Exfiltration
- Lab 7: Kubernetes and Gaining Access to Clusters