Faysal Aziz

Cloud Penetration Testing

Identify, Exploit, and Secure Modern Cloud Infrastructure - 2/3 days

FA-0132

DevOps, Cloud & Infrastructure · Cybersecurity · Automation, RPA & Power Platform

---

Introduction

Cloud computing has transformed how organizations build and deploy applications, but it has also introduced a new attack surface that traditional penetration testing methods cannot fully address. Cloud environments such as AWS, Azure, and Google Cloud rely on complex identity systems, APIs, dynamic infrastructure, and shared responsibility models that fundamentally change how security assessments are conducted. Unlike traditional networks, vulnerabilities in the cloud often arise from misconfigurations, overly permissive identity roles, exposed storage services, insecure APIs, and poorly designed infrastructure-as-code deployments.

As enterprises move toward multi-cloud architectures and containerized workloads, attackers increasingly target cloud services, identities, and automation pipelines rather than traditional servers. Research shows that a large portion of cloud security failures are caused by misconfigurations and identity access issues rather than software flaws, making cloud-focused penetration testing a critical skill for modern security professionals.

This intensive two/three-day course introduces the methodology, techniques, and tooling required to perform effective cloud penetration testing across modern cloud environments. Participants will learn how to identify attack surfaces, exploit common weaknesses, and simulate real-world attack paths in cloud infrastructures.

The course is delivered by an instructor with **over 30 years of industry experience**, ensuring that the material reflects **real-world industry demands and practical attack scenarios rather than purely academic theory**.

Learning outcomes

By the end of this course, participants will be able to:

- Understand the architectural differences between traditional and cloud penetration testing
- Interpret the cloud **shared responsibility model** and its impact on testing scope
- Identify common attack surfaces in AWS, Azure, and multi-cloud environments
- Perform reconnaissance and enumeration of cloud infrastructure
- Analyze identity and access management (IAM) misconfigurations
- Identify vulnerabilities in cloud storage, compute, and networking services
- Test APIs and serverless components deployed in cloud environments
- Evaluate container and Kubernetes security in cloud platforms
- Map cloud attack paths using identity chaining and privilege escalation techniques
- Utilize modern cloud pentesting tools and automation frameworks
- Produce structured cloud penetration testing reports with remediation guidance

---

Prerequisites

Participants should have:

- Basic understanding of networking concepts (TCP/IP, DNS, routing)
- Familiarity with Linux command-line usage
- Basic understanding of penetration testing concepts
- Introductory knowledge of cloud computing concepts (IaaS, PaaS, SaaS)
- Fundamental cybersecurity knowledge such as authentication, encryption, and access control
- Optional but helpful: experience with AWS, Azure, or other cloud platforms

---

Training outline

1. Cloud Security and Cloud Penetration Testing Foundations

1. Cloud computing architecture overview
2. Infrastructure as a Service (IaaS) architecture
3. Platform as a Service (PaaS) architecture
4. Software as a Service (SaaS) architecture
5. Differences between traditional infrastructure and cloud environments
6. Understanding cloud attack surfaces
7. Modern cloud threat landscape
8. Common causes of cloud breaches

9. Cloud misconfiguration risks
10. Identity-centric attack vectors in cloud platforms
11. Multi-cloud and hybrid cloud security challenges
12. The cloud shared responsibility model
13. Testing scope and rules of engagement for cloud pentests

2. Cloud Penetration Testing Methodology

1. Cloud penetration testing lifecycle
2. Scoping cloud penetration testing engagements
3. Legal considerations and provider testing policies
4. Rules of engagement for AWS, Azure, and GCP
5. Threat modeling for cloud environments
6. Asset discovery in cloud infrastructures
7. Identifying attack paths across cloud services
8. Risk classification for cloud vulnerabilities
9. Reporting methodology for cloud security assessments

3. Cloud Reconnaissance and Enumeration

1. Cloud asset discovery techniques
2. Enumerating cloud services and resources
3. Identifying publicly exposed cloud assets
4. Enumerating cloud accounts and tenants
5. Identifying exposed storage services
6. Enumerating cloud networking configurations
7. Discovering exposed APIs and endpoints
8. Cloud metadata services discovery
9. Identifying container registries and images
10. Enumeration of serverless functions

4. Identity and Access Management (IAM) Security Testing

1. IAM architecture in cloud environments
2. Authentication mechanisms in cloud platforms
3. Authorization models and policy structures
4. Over-privileged identity roles

5. Privilege escalation techniques in IAM
6. Role chaining and attack path discovery
7. Abuse of temporary credentials
8. Token and session hijacking scenarios
9. Testing access policies and permission boundaries
10. Cross-account access vulnerabilities

5. Cloud Storage and Data Exposure Testing

1. Storage service architecture in cloud platforms
2. Public storage bucket misconfigurations
3. Access control misconfigurations in storage services
4. Data exposure through misconfigured permissions
5. Encryption configuration testing
6. Access key exposure in repositories and logs
7. Data leakage through backups and snapshots
8. Data access logging and monitoring weaknesses

6. Cloud Network and Infrastructure Security Testing

1. Virtual network architecture
2. Security groups and firewall rules
3. Network segmentation weaknesses
4. Misconfigured load balancers
5. Public exposure of internal services
6. Virtual machine security testing
7. Remote access misconfigurations
8. Bastion host misconfigurations
9. Testing internal network connectivity paths

7. API and Application Layer Security in Cloud Environments

1. Cloud API architecture
2. API authentication and authorization mechanisms
3. Testing REST APIs in cloud applications
4. Injection vulnerabilities in APIs
5. Broken authentication vulnerabilities

6. Data exposure through API responses
7. GraphQL API security testing
8. Abuse of cloud service APIs

8. Serverless and Container Security Testing

1. Serverless computing architecture
2. Security risks in serverless functions
3. Privilege escalation through serverless execution roles
4. Event-trigger exploitation scenarios
5. Container architecture in cloud environments
6. Container image vulnerability analysis
7. Kubernetes cluster security testing
8. Pod security policies and container runtime security
9. Container escape scenarios

9. Cloud Attack Path Analysis

1. Multi-stage cloud attack chains
2. Identity-based lateral movement
3. Privilege escalation across services
4. Exploiting misconfigured automation pipelines
5. Infrastructure-as-Code security weaknesses
6. Attack path visualization techniques
7. Mapping attacks using threat frameworks

10. Cloud Pentesting Tools and Automation

1. Cloud reconnaissance tools
2. Cloud configuration assessment tools
3. IAM enumeration tools
4. Container and Kubernetes scanning tools
5. Infrastructure-as-Code security scanning tools
6. Automation frameworks for cloud security testing
7. Integration with CI/CD pipelines
8. Continuous cloud security testing

11. Reporting and Remediation

1. Structuring cloud pentest reports
2. Mapping findings to risk severity
3. Remediation recommendations for cloud vulnerabilities
4. Communicating risks to DevOps teams
5. Secure cloud architecture recommendations
6. Continuous cloud security validation strategies

Disclaimer

This course outline is intended to serve as a general guideline for the topics and areas that may be covered during the training. While the outline provides a structured view of the material, the actual delivery of the course may vary based on the instructor's professional judgment, the experience level of the participants, time constraints, and the specific interests or requirements of the class.

The instructor, who brings over 30 years of industry experience, may adjust the sequence of topics, expand on certain areas, introduce additional relevant subjects, or modify the depth of coverage to ensure the training remains practical, current, and aligned with real-world industry practices. In some cases, topics may be condensed or replaced with more relevant material to better address the needs of the participants.

As a result, the final course content and flow may differ from this outline in order to provide the most effective and valuable learning experience.

© 2026 Faysal Aziz · Kuala Lumpur