Whitepaper

Offensive Security in the Cloud Era:

Training Teams to Outsmart Modern Infrastructure

OffSec
The Path to a Secure Future™

As cloud adoption accelerates, offensive security teams are tasked with navigating complex, hybrid infrastructures where traditional tactics fall short. This white paper explores how to rethink offensive operations in the cloud, where identity is the new perimeter, recon demands architectural awareness, and misconfigurations replace open ports as prime targets.

Leaders must equip their teams with modern capabilities to uncover real-world vulnerabilities before adversaries do. Inside, you'll discover a new mental model for cloud pentesting, practical approaches to hybrid environments, and how OffSec's hands-on learning path builds the skills needed to stay ahead in today's rapidly evolving threat landscape.

1 Cloud is Not Just Infrastructure. It's a Strategy

2 The Offensive Security Reality: New Environments, Old Constraints

3 How to Do a Good Cloud Pentest: A New Mental Model

4 Hybrid Cloud: The New Norm, Not the Edge Case

5 The OffSec Advantage: Hands-On Cloud Offense at Scale

6 Build Teams That Can Attack your Cloud Before Adversaries Do

Introduction

1 Cloud is Not Just Infrastructure. It's a Strategy.

Modern offensive security teams are expected to operate as innovation scouts for the enterprise. They are tasked not only with testing defenses but with challenging assumptions and revealing blind spots before adversaries do. Yet as infrastructure moves to the cloud, many offensive security leaders are finding themselves without the frameworks, tools, or talent readiness to conduct effective operations in this new environment.

The stakes are high. Cloud misconfigurations, overly permissive identities, and vulnerable CI/CD pipelines are not hypothetical threats—they are real-world attack vectors exploited daily by both threat actors and penetration testers. But doing cloud pentesting well requires more than just cloud knowledge. It demands a mindset shift, an identity-first approach, and an ability to think beyond siloed environments to hybrid ecosystems.

30%

of cloud environment attacks in early 2024 were due to misconfigurations, up from 17% in the previous half-year, indicating a growing trend.[1]

90%

of granted permissions in cloud environments are not utilized, unnecessarily expanding the attack surface and increasing risk.[2]

2 The Offensive Security Reality: New Environments, Old Constraints

Offensive security leaders face several challenges as they adapt to the cloud:

- Limited time and resources to retrain or upskill their team on cloud-native attack techniques
- Legacy playbooks that do not translate well to cloud environments, particularly around identity, privilege escalation, and lateral movement
- Difficulty demonstrating value to the organization when cloud operations are considered the domain of DevOps or platform teams

Despite the shift to cloud, most offensive security teams were built for traditional network environments. They excel at lateral movement through Windows environments or simulating ransomware scenarios on-prem. But when it comes to attacking IAM roles, exploiting metadata APIs, or chaining misconfigurations across cloud services, the knowledge gaps are substantial.

That's where cloud offensive training becomes mission-critical.

3 How to Do a Good Cloud Pentest: A New Mental Model

Cloud pentesting is fundamentally different from traditional network pentesting. It requires:

Step 1
Solutioning as Recon

Cloud environments are built from services. Offensive operators must understand not just what is exposed, but why it is exposed, the architectural decisions behind each resource.

- Can I identify and enumerate S3 buckets to learn more about the environment?
- What can I infer from DNS or certificate data?
- Are there common naming conventions that reveal environment segmentation (e.g., `prod`, `dev`, `qa`)?
- What infrastructure-as-code or CI/CD patterns can I guess from GitHub repos, Terraform files, or public documentation?

Effective recon in the cloud involves mapping not just assets, but intentions.

Step 2
Identity is Everything

In the cloud, identity is the perimeter. Once offensive teams have compromised a credential (whether through leaked keys, exposed IAM roles, or misconfigured policies), the next phase is:

- Enumerating attached policies and permissions
- Mapping out privilege escalation paths (can this role create a new role with broader access?)
- Understanding which APIs and services are now accessible

OffSec's learning path includes lab exercises on techniques like IAM enumeration, chained privilege escalation, and abusing overly broad trust policies. These are critical real-world skills that traditional pentests miss.

Step 3
Posture Over Ports

Traditional pentesting often revolves around scanning for open ports and known vulnerabilities. In the cloud, the goal is to evaluate security posture:

- Misconfigured storage (public buckets or blobs)
- Users and roles with excessive access or permissions
- Exposed CI/CD environments (e.g., Jenkins instances with weak controls)
- Overprivileged containers or insecure Kubernetes dashboards

These misconfigurations often live in metadata, not in exposed services, and they require offensive teams to think like cloud architects and attackers at once.

4 Hybrid Cloud: The New Norm, Not the Edge Case

Most enterprises are not fully cloud-native. They operate in hybrid environments that blend on-prem infrastructure with AWS, Azure, or GCP. This introduces complexity but also opportunity:

- Hybrid environments increase the attack surface by introducing multiple identity systems (AD + IAM + custom SSO)
- They often lack unified logging, making lateral movement detection more difficult
- Trust relationships between environments (e.g., domain-joined EC2 instances) can be abused for escalation

Offensive security teams must understand how to:

- Traverse trust boundaries (e.g., moving from an EC2 instance with domain access back into on-prem AD)
- Abuse hybrid misconfigurations like cloud-connected VPNs or unmonitored service accounts
- Chain identity exploits across environments

OffSec's learning path includes different cloud scenarios that simulate these real-world conditions, giving offensive teams a chance to test and develop multi-environment adversarial tactics.

5 The OffSec Advantage: Hands-On Cloud Offense at Scale

The Offensive Cloud Learning Path from OffSec is a comprehensive, 100+ hour immersive training environment built specifically for:

- Offensive security leaders seeking to upskill or reskill their teams for modern adversarial operations
- Security consultants who need to deliver high-value engagements in cloud environments
- Platform security teams that want to understand attacker mindset to better secure their infrastructure

What makes it different:

- Public cloud labs using AWS that simulate real-world architectures, not sandboxed VM networks
- Modules covering recon, IAM abuse, CI/CD exploitation, container escape, and more
- A continuous feedback loop where learners build, break, and rebuild offensive strategies

Conclusion

6 Build Teams That Can Attack your Cloud Before Adversaries Do

Security leaders know that tomorrow's attacks will not look like yesterday's. As cloud adoption accelerates, so too does the need for offensive security teams who understand the nuance of cloud architecture, identity missteps, and escalation paths.

With OffSec's Offensive Cloud Learning Path, you can equip your team with the skills to:

1. Recon cloud resources with attacker precision
2. Exploit IAM and privilege paths the way real adversaries do
3. Identify and exploit overlooked functionality, such as CI/CD pipelines

Gain access to training for your team and stay ahead of the next generation of threats.

Connect with OffSec

OffSec

[1]Kapko, Matt. "Weak Credentials Behind Nearly Half of All Cloud-based Attacks, Research Finds." Cybersecurity Dive, 17 July 2024, www.cybersecuritydive.com/news/cloud-attacks-weak-credentials/721573/.
[2]Venkat, Apurva. "Misconfiguration and Vulnerabilities Biggest Risks in Cloud Security: Report." CSO Online, 1 Feb. 2023, www.csoonline.com/article/574453/misconfiguration-and-vulnerabilities-biggest-risks-in-cloud-security-report.html.