Cloud Penetration Testing: Exploitation Techniques

Simulate real-world attacks against cloud environments to identify security weaknesses before malicious actors can exploit them.

Request a Security Assessment

Download Methodology Guide

Understanding Cloud Penetration Testing

Cloud penetration testing simulates real-world attacks against IaaS, PaaS, and serverless deployments to uncover misconfigurations, logic flaws, and privilege escalation paths. As organizations adopt multi-cloud and hybrid architectures, continuous security validation becomes essential for maintaining a strong security posture and meeting compliance requirements.

Identify Vulnerabilities

Uncover security weaknesses before malicious actors can exploit them

Multi-Environment Testing

Test IaaS, PaaS, and serverless deployments across AWS, Azure, and Google Cloud

Compliance Validation

Meet regulatory requirements through structured security assessments

Cloud Threat Landscape & Attack

Cloud Misconfigurations

Public storage buckets, overly permissive security groups, exposed management consoles, and missing encryption create easy entry points for attackers.

IAM Privilege Escalation

Weak policies or unused permissions can be chained together, allowing attackers to gain full administrative access to cloud environments.

Stolen Credentials

Phishing attacks or leaked secrets in code repositories can lead to complete account takeover and compromise.

Lateral Movement

Pivoting from one compromised workload to others via metadata API abuse, open network ACLs, or overly permissive IAM roles.

By mapping these attack vectors—using techniques like metadata abuse, token hopping, and API throttling—testers can reveal the true blast radius of a potential breach.

Methodology & Planning Phase

Define Boundaries

Clearly identify target subscriptions, resource groups, and regions to establish the scope of testing.

Establish Permissions & Safeguards

Obtain explicit approval for live exploits and schedule testing windows to minimize business impact.

Set Success Criteria

Specify key objectives such as obtaining admin credentials or accessing critical data to measure effectiveness.

A well-defined methodology ensures comprehensive coverage while minimizing risks to production environments. Planning establishes the foundation for effective cloud penetration testing.

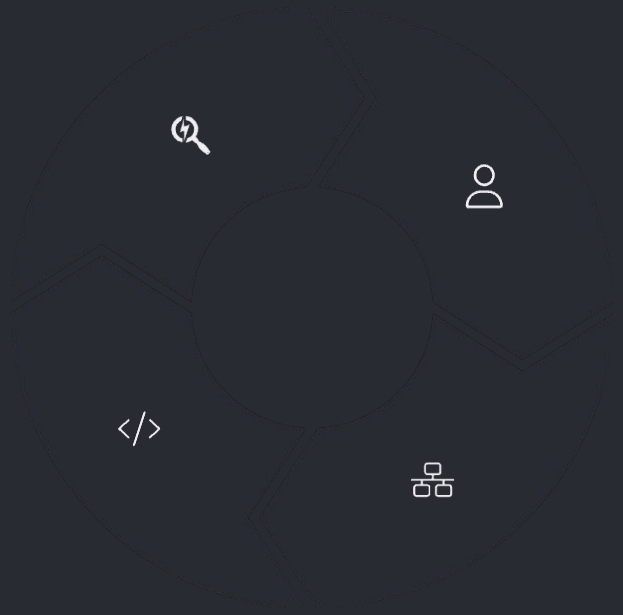
Reconnaissance & Enumeration Techniques

Resource Discovery

Use AWS CLI, Azure CLI, gcloud, and CloudMapper to list VMs, storage, functions, and roles

Permission Mapping

Enumerate IAM roles, policies, and trust relationships to identify potential privilege escalation paths



API Enumeration

Identify exposed APIs and services that could provide unauthorized access

Network Analysis

Review VPC/VNet configurations, NSGs/security groups, and peering rules for security gaps

Thorough reconnaissance reveals the attack surface and potential entry points. Effective enumeration techniques help penetration testers understand the cloud environment's structure before attempting exploitation.

Exploitation & Post-Exploitation Techniques

IAM Abuse

Exploit iam:CreatePolicyVersion or iam:SetDefaultPolicyVersion to escalate privileges within cloud environments

Storage Exploits

Leverage public S3 buckets or Blob containers to steal or tamper with sensitive data

Serverless & Container Attacks

Use SSRF in Lambda/Azure Functions, or break out from Kubernetes pods via known CVEs

Credential Harvesting

Abuse instance metadata endpoints to retrieve temporary tokens for further access

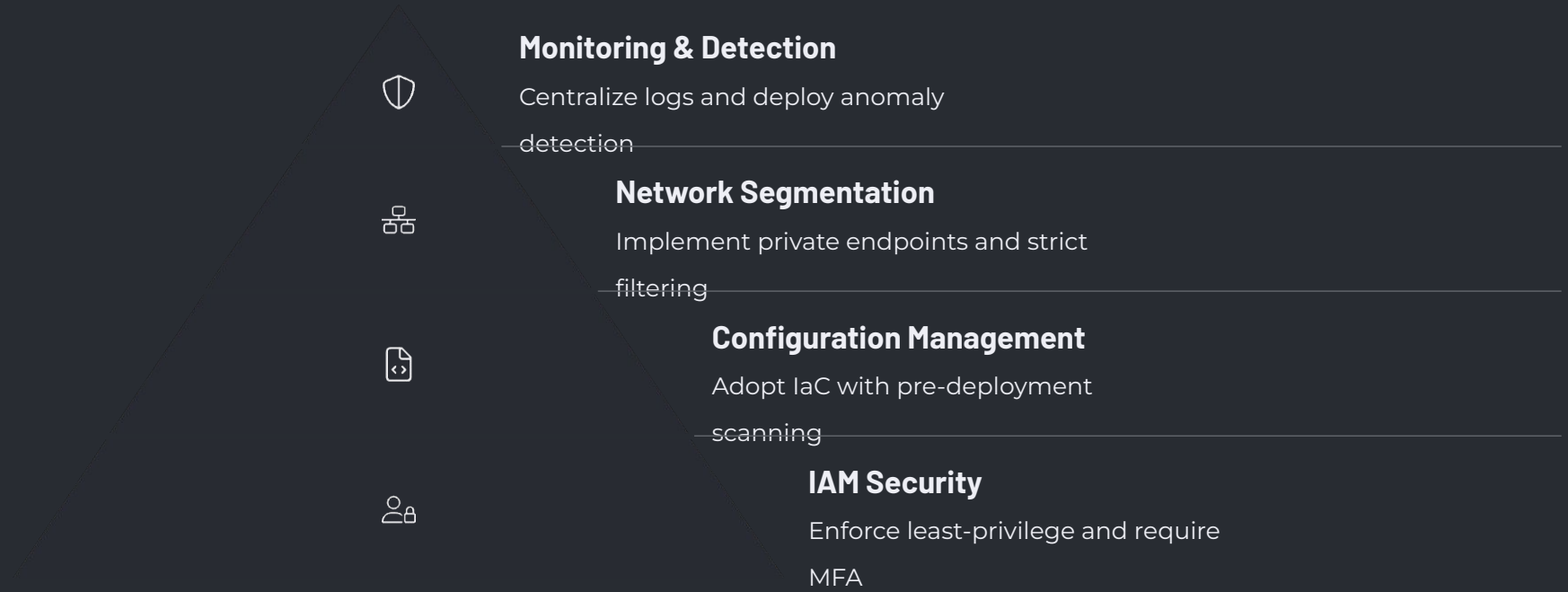
Exploitation techniques focus on bypassing defenses and demonstrating real-world impact. Post-exploitation activities reveal the potential damage attackers could cause after initial compromise.

Essential Tools & Frameworks

Category	Tools	Purpose
Scanning & Enumeration	Prowler, ScoutSuite, CloudMapper	Discover resources and identify misconfigurations
Exploitation	Pacu, Responder, kubectl-trivy	Execute attacks against AWS, Azure AD, and Kubernetes
Continuous Testing	Terrascan, Checkov, Trivy, Clair	Automate security scanning in CI/CD pipelines

Choose tools that integrate into CI/CD pipelines to automate recurring cloud penetration tests and vulnerability scans. The right toolset enhances testing efficiency and coverage across complex cloud environments.

Defensive Controls & Hardening Recommendations



Monitoring & Detection

Centralize logs and deploy anomaly detection

Network Segmentation

Implement private endpoints and strict filtering

Configuration Management

Adopt IaC with pre-deployment scanning

IAM Security

Enforce least-privilege and require MFA

By centering on exploitation and defense bypass techniques—paired with a structured methodology, the right toolset, and continuous hardening—organizations can transform cloud penetration testing from a compliance exercise into a proactive, risk-reduction engine that safeguards modern cloud environments.