AYI NEDJIMI Consultants

Cloud Pentest : Méthodologie Complète Audit AWS et Azure

Catégorie : Cloud Security Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Méthodologie pentest cloud complète : reconnaissance, escalade privilèges IAM AWS Azure, outils Pacu ScoutSuite PMapper et rapport audit sécurité.

Le test d'intrusion cloud est une discipline distincte du pentest traditionnel, nécessitant des compétences spécifiques sur les services, les APIs et les mécanismes de sécurité de chaque cloud provider. Les vulnérabilités les plus critiques dans le cloud ne sont pas des failles logicielles classiques mais des **misconfigurations de services**, des **permissions IAM excessives** et des **chemins d'escalade de privilèges** propres à l'écosystème cloud. En 2026, la demande de pentests cloud a explosé sous l'impulsion des réglementations (NIS 2, DORA) et de la multiplication des incidents impliquant des environnements cloud mal configurés. Ce guide présente une méthodologie structurée d'audit de sécurité cloud couvrant les phases de reconnaissance, d'évaluation, d'exploitation et de reporting, avec des outils et techniques spécifiques pour AWS et Azure. Notre approche combine l'évaluation automatisée des configurations avec les tests manuels d'exploitation pour identifier les risques réels et exploitables, au-delà des simples non-conformités aux benchmarks qui constituent le périmètre habituel des audits de configuration automatisés.

Résumé exécutif

Méthodologie complète de pentest cloud : reconnaissance, évaluation des configurations, escalade de privilèges IAM, tests de segmentation réseau, contournement des contrôles de détection et rapport structuré pour AWS et Azure. La migration vers le cloud transforme radicalement les paradigmes de sécurité : responsabilité partagée, identités éphémères, surfaces d'attaque distribuées et configurations complexes multiplient les vecteurs de compromission. Les équipes sécurité doivent adapter leurs compétences et leurs outils à ces nouveaux environnements tout en maintenant une visibilité complète sur les ressources déployées. Ce guide technique détaille les approches éprouvées en production, les pièges courants à éviter et les stratégies de durcissement prioritaires pour sécuriser efficacement vos workloads cloud en 2026. Chaque recommandation est issue de retours d'expérience concrets en environnement entreprise.

Retour d'expérience : lors d'un pentest cloud pour une fintech européenne, nous avons obtenu un accès administrateur complet au compte AWS de production en partant d'un rôle Lambda avec des permissions légèrement excessives. Le chemin d'attaque exploitait la capacité de la Lambda à lister les secrets Secrets Manager, combinée avec un secret contenant des credentials d'un utilisateur IAM disposant de la permission `iam:CreatePolicy`. En quatre étapes, nous avons escaladé les privilèges jusqu'au rôle OrganizationAccountAccessRole. Ce scénario, invisible à un scan de configuration automatisé, illustre la valeur des tests d'exploitation manuels.

Cadre juridique et règles d'engagement

Le pentest cloud s'exerce dans un **cadre juridique spécifique** défini par les conditions d'utilisation de chaque provider et le contrat entre le pentester et le client. **AWS** autorise les tests d'intrusion sur la plupart des services (EC2, RDS, Lambda, API Gateway, CloudFront, etc.) sans notification préalable, mais interdit explicitement les tests DDoS, le DNS zone walking et le flooding de ports. **Azure** autorise les tests sur les ressources du client en respectant les Microsoft Cloud Penetration Testing Rules of Engagement, qui interdisent les tests sur l'infrastructure partagée et les attaques par déni de service. **GCP** autorise les tests sur les ressources appartenant au client sans processus d'approbation, en respectant les Terms of Service et l'Acceptable Use Policy.

Le **contrat de pentest cloud** doit définir précisément le périmètre (comptes, régions, services inclus et exclus), les *règles d'engagement* (actions autorisées et interdites, procédure d'escalade en cas de découverte critique), les fenêtres de test et les contacts d'urgence. La question de la **responsabilité** en cas d'impact involontaire sur les services de production doit être adressée contractuellement. L'utilisation d'un compte AWS/Azure dédié au pentest est recommandée pour les phases de test destructif. Consultez AWS Security pour les politiques de test d'intrusion AWS et CIS Benchmarks pour Azure. Notre article sur Cloud Encryption Chiffrement Donnees Cles fournit un cadre complémentaire pour les pentests cloud.

Phase de reconnaissance cloud

La reconnaissance cloud identifie les assets exposés et les informations exploitables. La **reconnaissance passive** utilise les moteurs de recherche (Google dorks pour les buckets S3, Shodan pour les services exposés), les bases de données de certificats (crt.sh pour la découverte de sous-domaines), les DNS records et les informations publiques (registres WHOIS, offres d'emploi mentionnant les technologies cloud). La **reconnaissance active** énumère les services cloud exposés : scan des endpoints API Gateway, découverte des buckets S3 par brute-force de noms, identification des domaines CloudFront/Azure CDN et test des services exposés sur des ports non standard.

Les outils spécialisés de reconnaissance cloud incluent **ScoutSuite** pour l'audit multi-cloud automatisé, **Prowler** pour l'évaluation de conformité AWS, **CloudMapper** pour la cartographie de l'infrastructure AWS et **AzureHound** pour le graphe de relations Azure AD. L'outil *Pacu*, framework de pentest AWS, automatise de nombreuses techniques de reconnaissance et d'exploitation. Sur Azure, **ROADtools** et **AADInternals** permettent l'énumération approfondie d'Azure AD. La phase de reconnaissance doit également identifier les **services cloud utilisés** (via les headers HTTP, les erreurs d'application, les fichiers de configuration exposés) et les **relations entre les comptes** (cross-account roles, organisations). Notre guide sur Azure Security Center Configuration Complete détaille les techniques d'exploitation RBAC Kubernetes applicables lors des pentests. Les benchmarks de ANSSI fournissent les référentiels de conformité utilisés comme base de l'évaluation.

Évaluation des configurations et escalade de privilèges

L'évaluation des configurations vérifie systématiquement les services cloud contre les benchmarks de sécurité. Les **CIS Benchmarks** pour AWS, Azure et GCP fournissent des check-lists détaillées couvrant la gestion des identités, la journalisation, le monitoring, la mise en réseau et le stockage. Les outils automatisés (Prowler, ScoutSuite, Checkov) exécutent ces vérifications en quelques minutes. Cependant, la **valeur ajoutée du pentest** réside dans l'exploitation manuelle des faiblesses identifiées pour démontrer l'impact réel.

L'**escalade de privilèges IAM** est la technique centrale du pentest cloud. Sur AWS, les chemins d'escalade exploitent des permissions comme `iam:CreatePolicy`, `iam:AttachUserPolicy`, `iam:PassRole`, `lambda:CreateFunction` combiné avec `iam:PassRole`, et `sts:AssumeRole` vers des rôles plus privilégiés. L'outil *PMapper* modélise les chemins d'escalade de privilèges dans un graphe explorable. Sur Azure, les escalades exploitent les **rôles custom** avec des permissions d'écriture sur les définitions de rôles, les **applications Azure AD** avec des permissions API excessives et les **managed identities** sur des ressources compromises. L'outil **Stormspotter** cartographie les relations d'accès Azure AD. La documentation complète de ces techniques est disponible dans notre article sur Zero Trust Microsoft 365 Implementation. Consultez AWS Security pour les bonnes pratiques IAM qui préviennent ces escalades.

Phase de pentest	Outils AWS	Outils Azure	Objectif
Reconnaissance	ScoutSuite, CloudMapper, Prowler	AzureHound, ROADtools, ScoutSuite	Cartographie assets et configurations
Évaluation	Prowler, Pacu, PMapper	ScoutSuite, Stormspotter, AzureADRecon	Identification misconfigurations
Exploitation	Pacu, aws-cli, custom scripts	ROADtools, AADInternals, az-cli	Démonstration d'impact réel
Escalade	PMapper, Pacu, CloudGoat	Stormspotter, PowerZure	Escalade de privilèges IAM
Persistance	Lambda, EventBridge, IAM users	App registrations, Runbooks	Test des contrôles de détection
Exfiltration	S3 copy, snapshot share	Blob download, disk export	Évaluation protection des données

Test des contrôles de détection et monitoring

Un pentest cloud complet évalue la capacité de l'organisation à **détecter et répondre** aux attaques. Cette phase teste les contrôles de monitoring en exécutant des actions connues pour déclencher des alertes : connexion depuis une géolocalisation inhabituelle, création de clés d'accès IAM, désactivation de CloudTrail/logging, accès volumétrique à S3, communication avec

des IP de threat intelligence connues. L'objectif est de mesurer le *temps de détection* (temps entre l'action malveillante et la génération de l'alerte) et le *temps de réponse* (temps entre l'alerte et l'action de containment).

Les techniques d'**évasion de détection** testent la robustesse des contrôles. L'utilisation de régions rarement surveillées, l'exploitation de services peu journalisés, la manipulation des logs via des actions en volume pour créer du bruit, et l'utilisation de canaux de communication légitime pour l'exfiltration (DNS, HTTPS vers des domaines de confiance) évaluent la maturité du SOC face aux techniques cloud-spécifiques. Le rapport doit documenter les gaps de détection identifiés avec des recommandations spécifiques pour chaque alerte manquante. Notre article sur Casb Cloud Access Security Broker Guide explore les techniques d'évasion et de détection complémentaires. Les recommandations du CIS Benchmarks fournissent les standards de monitoring attendus.

Mon avis : la majorité des pentests cloud se limitent encore à un scan de configuration automatisé (Prowler, ScoutSuite) avec un rapport de non-conformités CIS. Ce n'est pas un pentest, c'est un audit de configuration. La vraie valeur du pentest cloud réside dans l'exploitation manuelle des chemins d'escalade de privilèges, la démonstration d'impact métier (accès aux données sensibles) et l'évaluation des capacités de détection. Les organisations doivent exiger des tests d'exploitation réels, pas seulement des check-lists de conformité.

Comment réaliser un pentest cloud sans enfreindre les conditions d'utilisation ?

La réalisation d'un pentest cloud conforme aux conditions d'utilisation des providers nécessite une préparation rigoureuse. **Premièrement**, lisez les politiques de test d'intrusion de chaque provider concerné et identifiez les actions explicitement interdites (DDoS, zone walking DNS, scan de ports sur l'infrastructure du provider). **Deuxièmement**, limitez le périmètre aux ressources appartenant au client, jamais à l'infrastructure partagée du provider. **Troisièmement**, documentez contractuellement les actions autorisées avec le client et obtenez les autorisations écrites couvrant les comptes et services testés. **Quatrièmement**, évitez les actions à fort impact opérationnel (suppression de ressources, modification de configurations critiques en production) sans accord explicite et fenêtre de maintenance définie. **Cinquièmement**, maintenez un journal détaillé de toutes les actions exécutées pendant le test pour la traçabilité et la résolution d'éventuels incidents. L'utilisation d'environnements de staging pour les tests destructifs et d'environnements de production uniquement pour les tests non destructifs (lecture, énumération) est la pratique recommandée.

Pourquoi un pentest cloud diffère-t-il d'un pentest traditionnel ?

Le pentest cloud se distingue fondamentalement du pentest traditionnel sur plusieurs dimensions. La **surface d'attaque** est constituée de services cloud et d'APIs plutôt que de serveurs et de ports réseau. Les **vulnérabilités prioritaires** sont des misconfigurations et des permissions excessives plutôt que des CVE sur des logiciels. L'**escalade de privilèges** exploite les mécanismes IAM du provider (assume role, pass role, permission policies) plutôt que les

vulnérabilités kernel ou les failles SUID. Le **mouvement latéral** traverse les comptes cloud et les services via les relations de confiance et les rôles cross-account plutôt que les segments réseau. L'**exfiltration** utilise les APIs cloud natives (copie S3, partage de snapshots) plutôt que les canaux réseau traditionnels. Les **outils** sont spécialisés (Pacu, PMapper, ScoutSuite) plutôt que génériques (Metasploit, Nmap). Les **compétences** requises incluent une connaissance approfondie des services et des APIs de chaque provider, en plus des compétences de sécurité offensive classiques. Notre article sur Kubernetes Security Durcissement Cluster fournit des perspectives complémentaires sur les techniques d'escalade cloud.

Quelles sont les phases d'un audit de sécurité cloud structuré ?

Un audit de sécurité cloud structuré se déroule en sept phases progressives. **Phase 1 : Cadrage.** Définition du périmètre, des objectifs, des règles d'engagement et des critères de succès. **Phase 2 : Reconnaissance.** Cartographie des assets cloud, découverte des services exposés et collecte d'informations. **Phase 3 : Évaluation de configuration.** Vérification systématique des configurations contre les benchmarks CIS et les bonnes pratiques du provider. **Phase 4 : Analyse IAM.** Cartographie des permissions, identification des chemins d'escalade et évaluation du moindre privilège. **Phase 5 : Tests d'exploitation.** Exploitation manuelle des faiblesses identifiées pour démontrer l'impact réel (accès aux données, escalade de privilèges, mouvement latéral). **Phase 6 : Évaluation de la détection.** Test des capacités de monitoring et de réponse aux incidents. **Phase 7 : Rapport et restitution.** Documentation des findings avec sévérité, impact, preuves, recommandations de remédiation et priorisation. Le rapport doit distinguer clairement les non-conformités (écarts aux benchmarks) des vulnérabilités exploitables (chemins d'attaque démontrés).

À retenir : le pentest cloud va au-delà de l'audit de configuration pour démontrer les impacts réels via l'exploitation des misconfigurations et des permissions IAM excessives. La méthodologie couvre la reconnaissance, l'évaluation, l'exploitation, les tests de détection et le reporting structuré. Le respect des conditions d'utilisation des providers et la documentation contractuelle du périmètre sont des prérequis indispensables.

Votre dernier pentest cloud incluait-il de véritables tests d'escalade de privilèges IAM, ou se limitait-il à un scan automatisé de conformité CIS ?

Sources et références : CISA · Cloud Security Alliance

Perspectives et prochaines étapes

L'évolution du pentest cloud intègre l'automatisation continue via les solutions BAS (Breach and Attack Simulation) qui exécutent des scénarios d'attaque cloud de manière régulière et mesurable. Les plateformes de purple teaming cloud permettent la collaboration entre les équipes offensives et défensives pour améliorer itérativement les contrôles de détection. L'intégration du pentest cloud dans les programmes de bug bounty étend la couverture au-delà des tests ponctuels. Les organisations matures adoptent un cycle de pentest cloud trimestriel, complété par du monitoring continu de la posture de sécurité via les outils CSPM et CNAPP.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr

© 2026 — Reproduction interdite sans autorisation.