AYI NEDJIMI Consultants

Pentest Cloud AWS Avancé 2026 : IMDSv1 + IAM PrivEsc

16 mai 2026 • Mis à jour le 17 mai 2026 • 18 min de lecture • 3708 mots • 17 vues •

> À retenir — Pentest cloud AWS avancé Le pentest cloud AWS avancé exploite cinq surfaces : IMDSv1 sur EC2, IAM policies trop permissives, S3 misconfig, Lambda env vars en clair.

À RETENIR

À retenir — Pentest cloud AWS avancé

Le pentest cloud AWS avancé exploite cinq surfaces : IMDSv1 sur EC2, IAM policies trop permissives, S3 misconfig, Lambda env vars en clair, EKS pod identity abuse.

IMDSv1 reste actif sur 17 % des EC2 audités en 2026 — SSRF + IMDSv1 = vol des credentials role EC2 en une requête HTTP.

Top 5 chaînes IAM privilege escalation : `iam:PassRole + ec2:RunInstances`, `iam:AttachUserPolicy`, `iam:CreateAccessKey`, `iam:UpdateAssumeRolePolicy`, `lambda:InvokeFunction + iam:PassRole`.

Outils incontournables 2026 : Pacu (Rhino Security), CloudFox (Bishop Fox), ScoutSuite, Prowler v4, Cloudsplaining, Pmapper.

Coût marché : 14 000 à 38 000 € HT pour un compte AWS multi-services (50-200 ressources), 30 000 à 90 000 € HT pour multi-comptes Organisations.

Le **pentest cloud AWS** avancé en 2026 va bien au-delà du scan de buckets S3 publics ou de l'énumération de groupes IAM. Avec l'explosion des architectures serverless, multi-comptes Organisations, EKS workloads et IaC Terraform/CDK, la surface d'attaque s'est densifiée — et les techniques d'élévation de privilèges aussi. Cet article documente la méthodologie avancée d'un pentest AWS 2026 : exploitation IMDSv1 résiduel, chaînes IAM privilege escalation, abus Lambda et EKS, exfiltration via SSM et CloudWatch Logs, persistence via roles cross-account. Issu de 30+ missions sur infrastructures AWS de 50 à 1 200 comptes (Organizations) chez des clients FinTech, SaaS et industriels. Stack outils détaillée, scénarios concrets, et défenses CIS / AWS Well-Architected.

Réponse sous 24h

Devis gratuit →