Cloud security, in concrete terms.

Cloud security is the practice of keeping cloud resources, identities, and data from being abused by attackers who reach your environment. Most cloud compromises today follow a small set of repeating patterns: an exposed credential or token, a permission that was broader than it needed to be, a storage bucket that was readable when it should not have been, or a metadata endpoint that handed out temporary access keys to anyone who asked.

HOW IT WORKS

01 Topics

- AWS Penetration Testing: Scope and Methodology: what a cloud pentest covers, where the AWS Acceptable Use Policy starts and ends, and what changes when the target is fully on AWS.
- What is the IMDSv1 Attack?: the EC2 instance metadata service, why version 1 was the trigger for the largest cloud breach on record, and what IMDSv2 fixes.
- S3 Bucket Misconfigurations: What Goes Wrong and How to Find It: public buckets, world-writable ACLs, signed-URL leaks, replication misconfigurations.
- AWS IAM Privilege Escalation: Common Attack Paths: the moves that turn a low-privilege role into administrator. PassRole, iam:CreatePolicy, lambda:UpdateFunctionCode, and friends.
- What is Kubernetes Penetration Testing?: what changes when the target is a Kubernetes cluster instead of a fleet of VMs.
- What is Kubernetes TokenRequest Abuse?-: The TokenRequest API issues short-lived service-account tokens on demand. An attacker with
- What is Kubernetes Node Impersonation?: On EKS, AWS identity maps to Kubernetes identity. An attacker who steals EC2 role credenti
- What is Kubernetes Secrets Enumeration?-: Kubernetes keeps credentials in Secret objects that are base64-encoded, not encrypted. An
- What is SelfSubjectRulesReview Abuse?: This Kubernetes API tells you exactly what your identity is allowed to do in a namespace.

SOURCES

[1] AWS Penetration Testing Policy

[2] CIS AWS Foundations Benchmark

[3] MITRE ATT&CK for Cloud

Scope a cloud penetration test.

securelayer7.net/learn/cloud-security

Open online