Offensive Security AWS Guide

https://www.linkedin.com/in/joas-antonio-dos-santos

Joas A Santos

Concepts

Focus area

- External Infrastructure of your AWS cloud
- Application(s) you are hosting/building on your platform
- Internal Infrastructure of your AWS cloud
- AWS configuration review

Governance

- Understand AWS usage/implementation
- Identify assets & define AWS boundaries
- Access policies
- Identify, review & evaluate risks
- Documentation and Inventory
- Add AWS to risk assessment
- IT security & program policy

Network Management

- Network Security Controls
- Physical links
- Granting & revoking accesses
- Environment Isolation
- Documentation and Inventory
- DDoS layered defence
- Malicious code controls

S3 Buckets

- · Check for misconfigured buckets (unauthenticated)
- · Once authenticated, check access to S3 buckets for sensitive files and data
- · Leverage existing S3 buckets to exfil data or stage further attacks

Encryption Control

- AWS Console access
- AWS API access
- IPSec Tunnels
- SSL Key Mangement
- Protect PINs at rest

Logging and Monitoring

- Centralized log storage
- Review policies for 'adequacy'
- Review Identity and Access Management (IAM) credentials report
- Aggregate from multiple sources
- Intrusion detection & response

Lambda

- · Analyze code and configuration for sensitive information disclosure
- · Privilege Escalation through Lambda IAM Roles and SDK's
- · Data exfiltration through modification of data-processing functions

CloudTrail

- Various methods of trying to evade detection, cover tracks, and generally stay under the radar
- · Downloading logs to get a better idea of common activity in the environment and creating a lay of the land

EC2/VPC

- · Enumerating Instances, Security Groups and AMIs to stage EC2 attacks
- · Abusing Simple Systems Manager for remote access to instances
- · Analyzing EC2 User Data for secrets or system credentials
- · Identifying routes between VPCs for lateral movement and escalation

IAM

- Analyze permissions for privilege escalation paths (through services like Lambda, EC2, etc.)
- · Checking for misconfigured roles, attempting to access them
- · Establish persistence through backdoor users/roles

SNS/SQS

- Misconfigured topics or queues can allow unauthorized users to subscribe to topics or push messages to queues. Testing of this can be done with the AWS CLI.

Cognito Authentication

- An AWS pentest should determine if the Cognito configuration is appropriate for intended application behavior. This includes checking for self-signups, and enabling advanced security.

Tools

WeirdAAL	AWS Attack Library
Pacu	AWS penetration testing toolkit
Cred Scanner	A simple file-based scanner to look for potential AWS access and secret keys in files
AWS PWN	A collection of AWS penetration testing junk
Cloudfrunt	A tool for identifying misconfigured CloudFront domains
Cloudjack	Route53/CloudFront Vulnerability Assessment Utility
Nimbostratus	Tools for fingerprinting and exploiting Amazon cloud infrastructures
GitLeaks	Audit git repos for secrets
TruffleHog	Searches through git repositories for high entropy strings and secrets digging deep into commit history
DumpsterDiver	"Tool to search secrets in various filetypes like keys (e.g. AWS Access Key Azure Share Key or SSH keys) or passwords."
Mad-King	Proof of Concept Zappa Based AWS Persistence and Attack Platform
Cloud-Nuke	A tool for cleaning up your cloud accounts by nuking (deleting) all resources within it
MozDef - The Mozilla Defense Platform	The Mozilla Defense Platform (MozDef) seeks to automate the security incident handling process and facilitate the real-time activities of incident handlers.
Lambda-Proxy	A bridge between SQLMap and AWS Lambda which lets you use SQLMap to natively test AWS Lambda functions for SQL Injection vulnerabilities.
CloudCopy	Cloud version of the Shadow Copy attack against domain controllers running in AWS using only the EC2:CreateSnapshot permission
enumerate-iam	Enumerate the permissions associated with AWS credential set
Barq	A post-exploitation framework that allows you to easily perform attacks on a running AWS infrastructure
CCAT	Cloud Container Attack Tool (CCAT) is a tool for testing security of container environments
Dufflebag	Search exposed EBS volumes for secrets
attack_range	A tool that allows you to create vulnerable instrumented local or cloud environments to simulate attacks against and collect the data into Splunk
whispers	Identify hardcoded secrets and dangerous behaviours
Redboto	Red Team AWS Scripts
CloudBrute	A tool to find a company (target) infrastructure, files, and apps on the top cloud providers
Stratus Red Team	Granular, Actionable Adversary Emulation for the Cloud
Leonidas	Automated Attack Simulation in the Cloud complete with detection use cases.
Amazon Guardduty Tester	This script is used to generate some basic detections of the GuardDuty service