Cloud Security: AWS Edition Bootcamp

Objective

Enterprises are increasingly running their IT and application infrastructure natively in the cloud. This fundamentally changes the security models and enterprise threatscape. It's important that as a security professional you are able to pentest these cloud native deployments and help secure organizations.

This hands-on labs based bootcamp teaches you the security basics of the five most popular cloud-native components on AWS. You will learn how to discover vulnerabilities and propose security fixes in applications and infrastructure leveraging AWS IAM, API Gateway, Lambda, DynamoDB and S3. Completing the bootcamp and passing the certification exam will prepare you for pentesting production cloud deployments in AWS.

Prerequisites

- A basic knowledge of computers and networking
- Familiarity with the Linux operating system
- An AWS Account

Course Content

Module I: Identity and Access Management (IAM)

- Introduction to IAM
    - IAM users, roles and groups
    - Temporary security credentials
    - Policies and permissions
    - Policy evaluation logic
    - IAM access analyzer
- Enumerating IAM users and roles
- Cross-account AWS roles and user enumeration
- Abusing overly permissive IAM trust policies
- Escalating privileges by abusing IAM policies and permissions

Module II: API Gateway Attack-Defense

- Introduction to API Gateway
  - Enumerating API Gateway and API keys
  - Understanding stage variables and usage plans
  - Authorization with lambda authorizers
- Bypassing authentication by verb tampering
- Abusing overly permissive resource policies
- Attacking misconfigured private API endpoints
- Performing Denial of Service attack on API Gateway

Module III: Serverless Functions: Lambda

- Introduction to AWS Lambda
  - Lambda functions
  - Lambda applications
  - Lambda layers
  - Lambda alias routing
  - Custom runtimes
- Enumerating Lambda functions and layers.
- Event data injection
  - Command injection
  - Function runtime code injection
  - XML external entity (XXE)
  - Server-side request forgery (SSRF)
  - Object deserialization attacks
  - SQL injection
  - NoSQL injection
- Abusing overly permissive resource policies
- Abusing AWS Lambda permissions
- Manipulating function execution flows
- Retrieving application secrets, keys, and credentials
- Retrieving sensitive information from Lambda Runtime API
- Exploiting vulnerable component and custom runtimes
- Abusing temporary and shared file systems
- Maintaining access on an AWS account (backdoor)

Module IV: DynamoDB and other Cloud Databases

- Introduction to DynamoDB
    - Tables, indexes, and streams
    - Partition key and sort key
    - CRUD operations
    - PartiQL support
- NoSQL injection attack on a DynamoDB-based application.
- SQL injection attack through PartiQL support on a DynamoDB-based application
- NoSQL injection attack on a MongoDB-based application.
- SQL injection attack on an RDS-based application.

Module V: Cloud Storage: S3 Misconfigurations

- Introduction to S3
    - Bucket and objects
    - Object metadata and versioning
    - IAM policies, bucket policies, and access control lists
    - Server-side encryption and client-side encryption
    - Object locking
    - Pre-signed URLs
    - Access analyzer for S3
- Enumerating public S3 buckets
- Identifying bucket policy/ACL constraints on an S3 bucket
- Identifying anonymous write operations on an S3 bucket
- Leveraging misconfigured bucket policies and ACPs
    - Anonymous/Authorized public read
    - Reading policies and identifying object names
    - Writing objects to buckets
    - Overwriting bucket ACL and object ACL
    - Overwriting bucket policies
    - Performing denial of service
- Identifying writable buckets without performing a write operations
- Chaining web application attacks through S3 resources