‹ Dashboard

AWS CLOUD SECURITY BOOTCAMP

These video recordings are from our live online bootcamp

Session I

The following topics are covered

- Introduction to IAM
    - IAM users, roles and groups
    - Temporary security credentials
    - IAM Policies and permissions
    - Permission Boundary, Session Policy and SCPs
    - AWS Organization
    - Policy evaluation logic
- Enumerating IAM users, groups, roles and policies
    - AWS Console
    - AWS CLI
- Enumeration with open-source tools
    - PACU
    - ScouteSuite
    - PMapper
    - Enumerate IAM

3:47:20

List of labs covered during the session (and homework):

- IAM Enumeration (https://attackdefense.com/challengedetails?cid=2245)

Session II

The following topics are covered

- Cross account enumeration
- Leveraging misconfigured role trust policy
- Overview of EC2, VPC, and Lambda service

- Introduction to API Gateway
  - Enumerating API Gateway and API keys
  - Understanding stage variables and usage plans
  - Policy Authorization Workflow
- Bypassing authentication by verb tampering
- Abusing overly permissive resource policies
- Attacking misconfigured private API endpoints
- Performing denial of service attack on API Gateway

4:02:36

List of labs covered during the session (and homework):

- IAM Cross Account Enumeration (https://attackdefense.com/challengedetails?cid=2246)
- Misconfigured Trust Policy (https://attackdefense.com/challengedetails?cid=2247)
- Overly Permissive Permission I (https://attackdefense.com/challengedetails?cid=2248)
- Dangerous Policy Combination I (https://attackdefense.com/challengedetails?cid=2249)
- Dangerous Policy Combination II (https://attackdefense.com/challengedetails?cid=2250)
- Overly Permissive Permission II (https://attackdefense.com/challengedetails?cid=2251)
- Pass Role : EC2 (https://attackdefense.com/challengedetails?cid=2253)
- Pass Role : Lambda (https://attackdefense.com/challengedetails?cid=2252)
- Pass Role : CloudFormation (https://attackdefense.com/challengedetails?cid=2254)
- API Gateway Enumeration (https://attackdefense.com/challengedetails?cid=2275)
- Verb Tampering (https://attackdefense.com/challengedetails?cid=2276)
- Misconfigured Private API (https://attackdefense.com/challengedetails?cid=2277)
- IAM based Authentication (https://attackdefense.com/challengedetails?cid=2278)
- Denial of Service (https://attackdefense.com/challengedetails?cid=2279)
- Poor Lambda Authorizer (https://attackdefense.com/challengedetails?cid=2280)

Session III

The following topics are covered

- Introduction to AWS Lambda
  - Lambda functions
  - Lambda applications
  - Lambda layers
  - Lambda alias routing
  - Custom runtimes
- Enumerating Lambda functions and layers.
- Application Vulnerabilities
  - Command injection
  - Insecure Deserialization
  - Server-side request forgery (SSRF)
  - XML external entity (XXE)
- Abusing AWS Lambda permissions
- Lambda Alias Routing
- AWS Lambda Execution Environment
- Lambda Runtime API

3:50:32

List of labs covered during the session (and homework):

- Lambda Enumeration (https://attackdefense.com/challengedetails?cid=2281)
- Command Injection (https://attackdefense.com/challengedetails?cid=2282)
- Insecure Deserialization (https://attackdefense.com/challengedetails?cid=2283)
- Server Side Request Forgery (https://attackdefense.com/challengedetails?cid=2286)
- XML External Entity : Python Runtime (https://attackdefense.com/challengedetails?cid=2284)
- XML External Entity : PHP Runtime (https://attackdefense.com/challengedetails?cid=2285)
- Retrieving Invocation Event (https://attackdefense.com/challengedetails?cid=2287)
- Lambda Alias Routing (https://attackdefense.com/challengedetails?cid=2288)

Session IV

The following topics are covered

- Lambda Authorizers
- Leverage Lambda functions for performing attacks
- Abusing temporary file systems of Lambda Environment
- Maintaining access on an AWS account (Lambda backdoor)
- Retrieving application secrets, keys, and credentials
- Manipulating function execution flows
- Injecting Malicious runtime and taking control of Lambda environment.
- Exfilterating Lambda event data

3:25:35

List of labs covered during the session (and homework):

- Poor Lambda Authorizer (https://attackdefense.com/challengedetails?cid=2280)
- Dictionary Attack via Lambda (https://attackdefense.com/challengedetails?cid=2291)
- Lambda Backdoor (https://attackdefense.com/challengedetails?cid=2289)
- Persistent Access on Lambda (https://attackdefense.com/challengedetails?cid=2290)

Session V

The following topics are covered

- Introduction to DynamoDB

    - CRUD operations
    - PartiQL support
- Overview of RDS and DocumentDB
- 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 with SQLMap
- Bypassing poorly implemented WAF
- 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
- Understanding S3 Storage Classes
- Access Control Policy Evaluation
- 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
- Chaining web application attacks through S3 resources

4:31:52

List of labs covered during the session (and homework):

- Database Enumeration (https://attackdefense.com/challengedetails?cid=2297)
- DynamoDB : SQL Injection (https://attackdefense.com/challengedetails?cid=2292)
- DynamoDB : NoSQL Injection (https://attackdefense.com/challengedetails?cid=2293)
- RDS : SQL Injection (https://attackdefense.com/challengedetails?cid=2294)
- DocumentDB : NoSQL Injection (https://attackdefense.com/challengedetails?cid=2295)
- WAF Bypass : SQL Injection (https://attackdefense.com/challengedetails?cid=2296)
- S3 Enumeration (https://attackdefense.com/challengedetails?cid=2298)
- Sensitive Data Exposure (https://attackdefense.com/challengedetails?cid=2299)
- Hardcoded Credentials (https://attackdefense.com/challengedetails?cid=2300)
- Readable Bucket Policy (https://attackdefense.com/challengedetails?cid=2301)
- Special Request (https://attackdefense.com/challengedetails?cid=2302)
- Writable Bucket Policy (https://attackdefense.com/challengedetails?cid=2303)
- Writable Bucket ACL (https://attackdefense.com/challengedetails?cid=2304)
- Writable Object ACL (https://attackdefense.com/challengedetails?cid=2305)
- Chaining Attacks (https://attackdefense.com/challengedetails?cid=2306)