



ITSA SAFE

Cyber Security Trainings



7 שעות תוכן

36 שיעורים

110 שעות מעבדה

מעבדות תירגול

בדיקות חוסן בסביבות AWS

1. IAM

- Refresher of IAM
- IAM users, roles and groups
- IAM policy structure
- AWS Managed Policy
- Inline Policy
- Security Token Service (STS)
- Enumerating IAM users & roles
- Abusing overly permissive
- IAM trust policies
- Privilege escalation
- Gathering credentials with Pacu
- Persistence

2. S3

- Refresher of S3 buckets
- Bucket ACLs
- Bucket ACPs
- Bucket policie
- Identifying Vulnerable S3 Buckets
- Extracting sensitive data from S3
- Policy bypassing
- S3 malicious code Injection

3. Lambda

- Refresher of AWS Lambda
- Understanding & setup a Lambda service
- Understanding Lambda misconfigurations
- Setting up a vulnerable Lambda function
- Attacking Lambda functions with read access
- Installing and using Bandit
- Popping reverse shells with Lambda

4. API Gateway

- Refresher of API Gateway
- Enumerating API Gateway and API keys
- Exploring and configuring AWS APIs
- Creating API with AWS
- Manipulating API calls
- Authorization with lambda authorizers

5. RDS

- Understanding Vulnerable RDS Services
- Setting up RDS (MySQL)
- Understanding basic SQL syntax
- Database maneuvering and exploration
- Learning about injection points
- Setting up a lab for SQLi
- Exploitation and data extraction from a vulnerable RDS instance

