AWS PT 7 hours of content | 110 hours of practice | Project

1.IAM

- Refresher
- 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 ACL's
- Bucket ACP's
- Bucket policie
- Identifying Vulnerable S3 Buckets
- Extracting Sensitive data from S3
- Policy Bypassing
- S3 malicious code injection

3.Lambda

- Refresher of AWS Lamda
- Understanding & setup a Lambda service
- Understanding Lambda misconfigurations
- Setting up a vulnerable lambda function
- Attacking Lambda read access
- Installing and using bandit
- Popping Reverse Shells with Lambda

4. API Gateway

- Refresher of API Gateway
- Enumeration API Gateway and API keys
- Exploring and configuring AWS API's
- 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
- Injection Points
- SQLi Lab
- Exploitation And Data Extraction