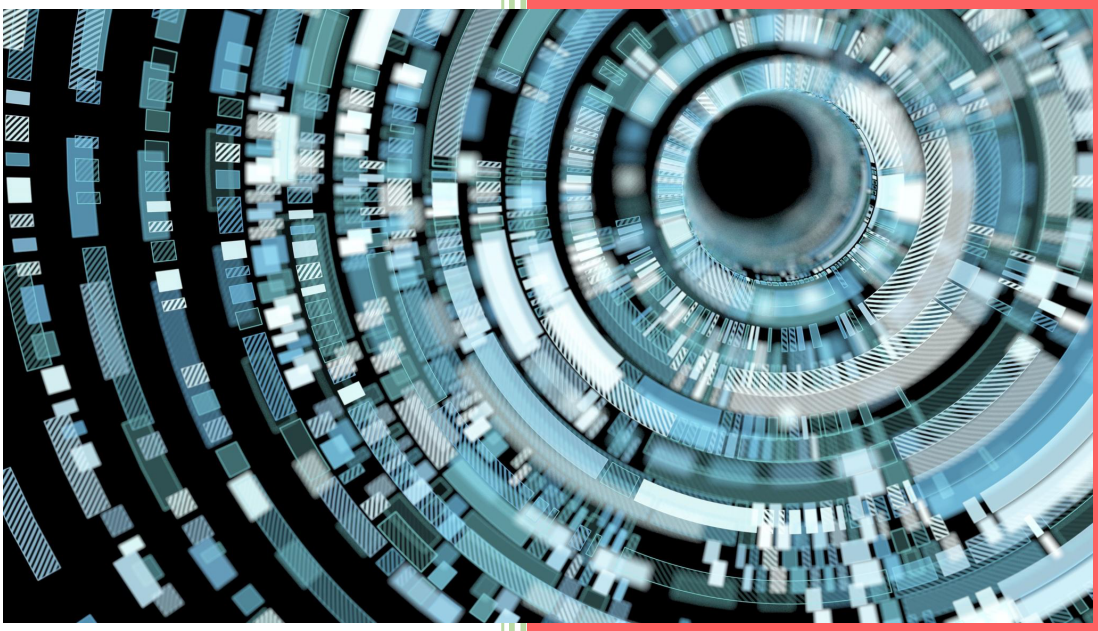
DARKRELAY

MASTERING CLOUD PENETRATION TESTING

CLOUD PENETRATION TESTER (CPT)



DarkRelay Security Labs

www.darkrelay.com

Mastering Cloud Penetration Testing

Mastering Cloud Penetration Testing

Table of Contents

Mastering Cloud Penetration Testing

About the Course

Cloud Penetration Tester(CPT) instructor-led course is designed for Security Professionals, Security Architects, Cloud Administrators, and Penetration Testers who want to master the art of cloud penetration testing. The student will thoroughly understand cloud computing architecture and security fundamentals, learn the various types of cloud penetration testing, and explore the latest cloud infrastructure and platform attacks.

The student will also delve into cloud application attacks and discover how to identify, report, and remediate vulnerabilities in your cloud environment. With hands-on exercises, real-world scenarios, and a focus on best practices, the student will leave this course equipped with the knowledge and skills they need to secure their cloud infrastructure and applications.

Whether you're just getting started with cloud security or looking to expand your existing knowledge, this course will help you become an expert in cloud penetration testing.

Course Dependencies

Signup for an AWS account: https://aws.amazon.com/resources/create-account/

Hardware Prerequisites

Laptop or PC with 8 GB RAM, 50 GB free space.

Mastering Cloud Penetration Testing

Module I: Introduction

Introduction to AWS

- Overview of AWS
- Understanding the AWS cloud computing platform
- Overview of AWS services and offerings
- AWS Security Best Practices
- Implementation of security controls in AWS environments

Penetration Testing

- Introduction to Penetration Testing
- Penetration Testing Methodology
- Types of Penetration Testing
- AWS Permissions

Module II: Penetration Testing Fundamentals

Networking Fundamentals

- Networking Fundamentals
- TCP/IP Model
- Understanding IP Addressing, Subnetting, and Routing
- Network Protocols

Kali Linux Introduction

- Kali Linux Introduction
- Installing and Configuring Kali Linux on AWS
- Overview of Kali Linux Tools

Mastering Cloud Penetration Testing

Module III: AWS Infrastructure

AWS Infrastructure Components

- Understanding AWS VPCs, Subnets, and Security Groups
- Overview of AWS EC2, RDS, and S3
- Overview of AWS IAM
- Understanding AWS Roles and Policies
- Overview of AWS Network Security
- Understanding AWS Security Groups and Network Access Control Lists

AWS Infrastructure Penetration Testing

- Enumerating the AWS environment
- Identifying AWS services and configurations
- Test AWS VPCs, Subnets, and Security Groups
- Test AWS EC2, RDS, and S3
- Test AWS IAM Roles and Policies
- Vulnerability Scanning in AWS

Module IV: AWS Web Application Security

AWS Web Application Components

- Overview of AWS Elastic Beanstalk, CloudFront, and Route 53
- Understanding AWS Load Balancers and Auto-Scaling

AWS Web Application Penetration Testing

- Overview of OWASP Top 10 Web Application Vulnerabilities
- Understanding AWS WAF and Shield
- Test AWS Web Applications API deployed on Elastic Beanstalk.
- Test AWS CloudFront and Route 53
- Test AWS Load Balancers and Auto-Scaling
- Automated Scanning Tools for AWS Web Applications
- Burp Suite Cloud Penetration Testing Plugins

Module V: AWS Web API Penetration Testing

AWS Web API Components

- Overview of AWS API Gateway and AWS Lambda
- Understanding AWS RESTful APIs and SOAP APIs

AWS Web API Security

- Overview of OWASP Top 10 Web API Vulnerabilities
- Understanding AWS API Gateway security features
- Overview of AWS Lambda security best practices
- Test AWS RESTful APIs and SOAP APIs
- Test AWS API Gateway
- Test AWS Lambda functions

Module VI: AWS Container Penetration Testing

AWS Container Components

- Overview of AWS ECS, ECR, and Fargate
- Understanding AWS container security and orchestration

AWS Container Security

- Security best practices for ECS, ECR, and Fargate
- Test AWS ECS containers and clusters
- Test AWS ECR container registries
- Test AWS Fargate-managed containers