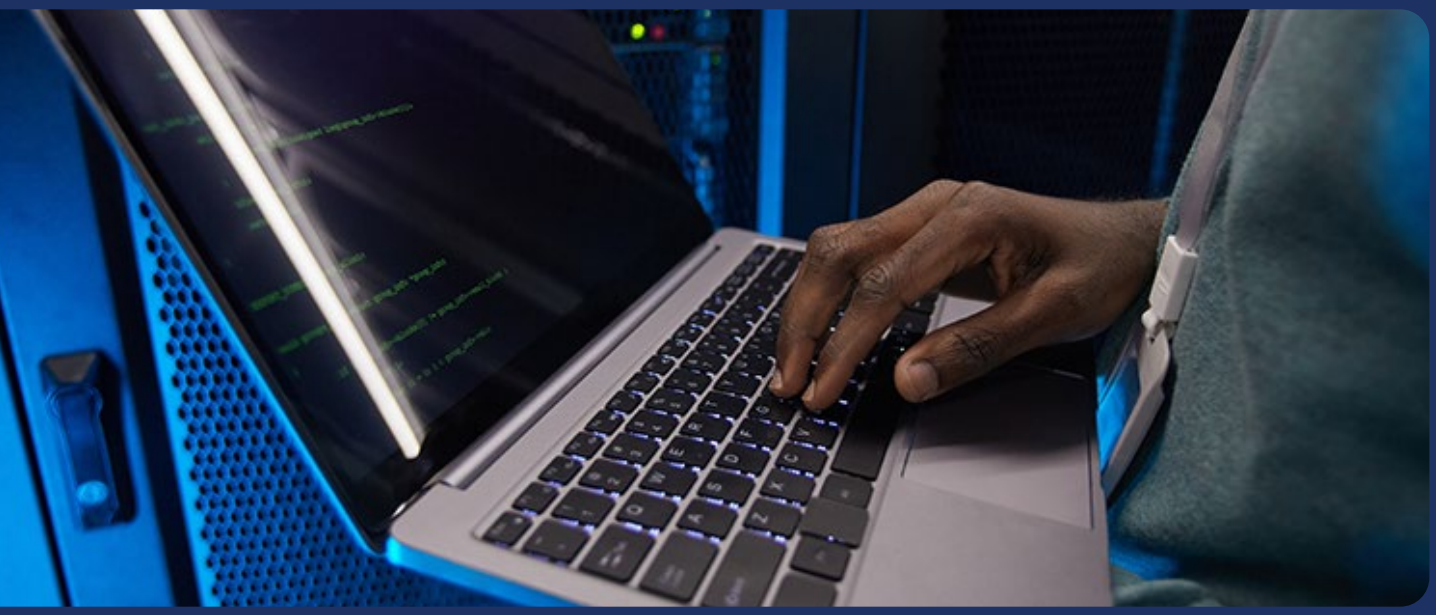
INFOSECTRAIN

AWS Cloud Penetration Testing

TRAINING COURSE



Course description

The AWS Cloud Penetration Testing course is designed to give a detailed understanding of the security challenges and threat landscape in AWS cloud platform and performing potential penetration testing activities. Being the most popular public cloud provider in the market, AWS offers nearly over 200+ services to their tenants and they've opened certain services to organizations for penetration testing activities as well. InfoSec Train's AWS Cloud Penetration Testing program walks you through how to set up a test environment in AWS and then use various techniques to identify the vulnerable points and reveal sensitive information.

Target Audience

AWS Penetration Testing course is designed for:

- AWS Architects and Security Specialists
- Cloud Architects who wish to learn offensive security in AWS Cloud
- Anyone who is interested in securing their cloud infrastructure
- Anyone who want to start with Cloud Pentesting

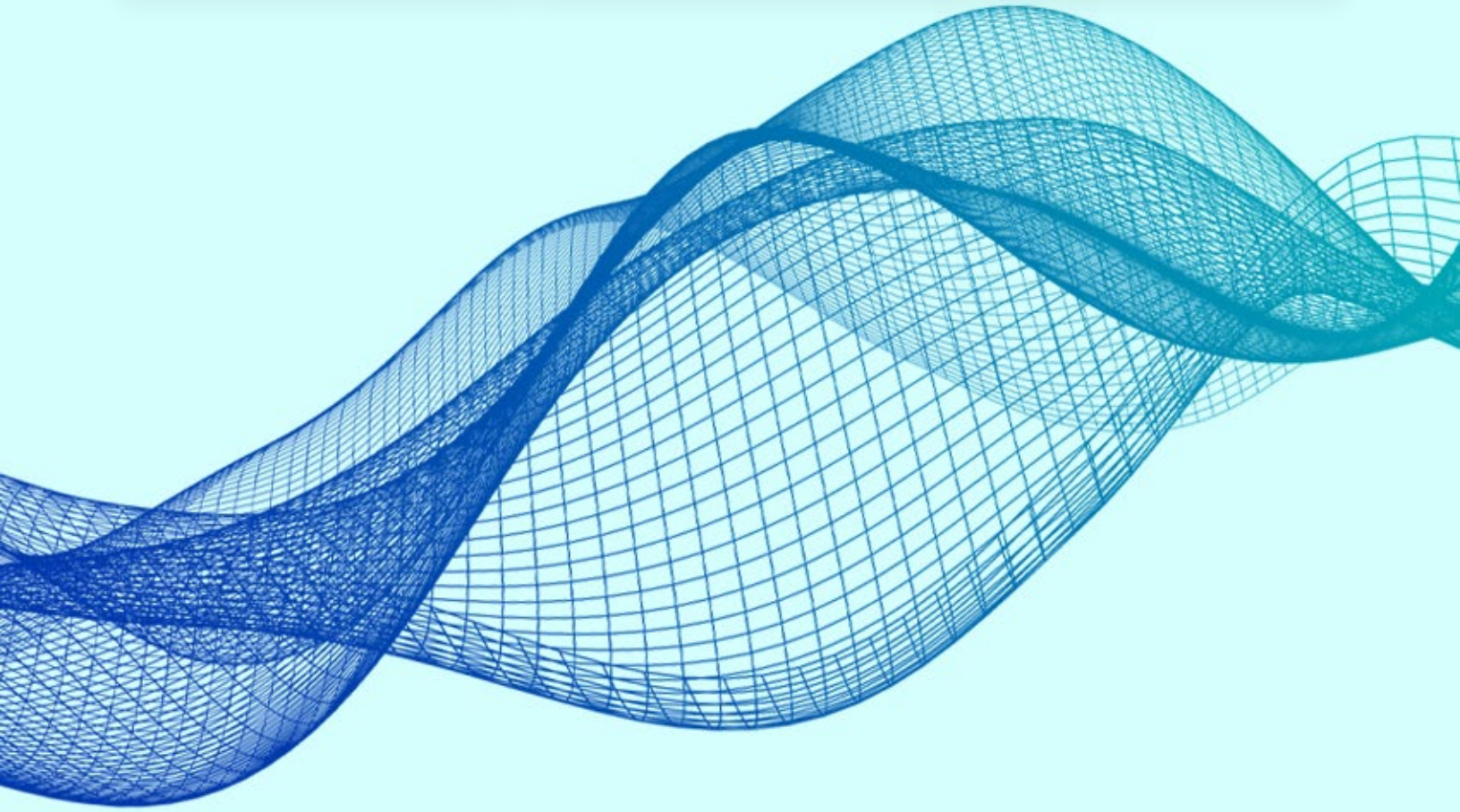
Prerequisites

- Good understanding of key AWS Services
- Familiar with Linux and AWS CLI
- Knowledge in security concepts and Controls

INFOSECTRAIN

Why Infosec Train?

- Certified & Experienced Instructor
- Flexible Schedule
- Access to the recorded sessions
- Post Training Support
- Tailor Made Training
- 4 hrs/day in Weekend/ Weekday



Course Content

INFOSECTRAIN

MODULE 1

Cloud Security & Penetration Testing fundamentals

- AWS Security Fundamentals
- Overview of AWS Security Services
- AWS CLI & Cloud Shell
- IAM Policy JSON walkthrough
- Penetration testing concepts and methodologies
- Penetration Testing in a public cloud platform.
- AWS Acceptable usage policy and penetration testing guidelines
- Deploying Kali Linux

MODULE 2

Linux Fundamentals

- Linux architecture
- File Permissions
- Package management
- User management & Sudo

MODULE 3

Vulnerability Assessment

- Vulnerability assessment concepts
- CVE & CVSS
- AWS Inspector

MODULE 4

Pen testing the Cloud

- Enumerating and Understanding AWS services
- Setting up a penetration testing environment in AWS
- Installing the prerequisites on your Kali Linux
- Vulnerable IAM accounts
- Misconfigured EC2 Instances
- Misconfigured Elastic Load Balancers
- Misconfigured S3 Buckets
- Privilege escalation
- Data and Information enumeration
- PACU Framework for AWS Exploitation

MODULE 5

Security Auditing in AWS

- Cloud Audit Concepts
- Common Cloud auditing tools (ScoutSuite, Prowler, etc.)
- AWS Trusted Advisor
- CloudSploit
- Creating a sample audit checklist for various services

www.infosectrain.com | sales@infosectrain.com