CYBERIUM

AWS PENETRATION TESTING & SECURITY

INTRODUCTION

In today's cloud-driven world, AWS powers thousands of businesses—but it also attracts attackers. This course is designed to equip you with real-world skills in identifying, exploiting, and securing vulnerabilities within AWS environments.

Whether you're a cybersecurity student, ethical hacker, cloud engineer, or IT professional, this course will take you through hands-on labs, practical tools, and real attack scenarios that mimic how adversaries breach cloud systems—and how to stop them.

You'll learn:

- AWS architecture from a hacker's point of view
- Cloud misconfigurations & privilege escalation
- IAM exploitation & defense
- S3 bucket attacks, Lambda abuse, and more
- Tools like Pacu, ScoutSuite, and CloudSploit
- Pro tips for securing your AWS infrastructure

By the end, you'll not only understand how to penetrate AWS environments, but also how to build a solid defense strategy to protect your cloud assets.
Let's dive into the cloud—and take full control of its security.

Course duration- 50 Hours

AWS PENETRATION TESTING & SECURITY SYLLABUS

Module 01- Introduction to AWS and Security

1. Basics of AWS and cloud computing
2. Shared Responsibility Model
3. Cloud service models (IaaS, PaaS, SaaS)
4. NIST Cloud Architecture
5. Key AWS services overview (EC2, S3, IAM, RDS, Lambda, etc.)
6. Introduction to AWS global infrastructure
7. Key terminology: Regions, Availability Zones, Budget
8. AWS penetration testing policy and scope
9. Permissible vs prohibited activities
10. Methodology and ethics of cloud penetration testing

Module 02- Configuring the Lab Environment

1. Creating a Free Tier AWS Account
2. Setting up Budget Alerts
3. Installing and Configuring the AWS CLI
4. Enabling Autocomplete for the AWS CLI
5. Installing CloudGoat
6. Installing Pacu
7. Creating Free Accounts on Cybr and Pwned Labs

Module 03- Understanding IAM in AWS

1. IAM Users, Groups, and Roles
2. IAM Policies (JSON structure and permission boundaries)
3. AWS STS and temporary credentials
4. MFA and IAM best practices
5. Principle of least privilege
6. 3.4 User and Policy Enumeration
7. 3.5 Group and Role Enumeration
8. Using Pacu to Automate Enumeration
9. Challenge Labs
10. IAM Security Guidelines

Module 04- S3 Buckets

1. Introduction to S3
2. Creation and Management of S3 Buckets
3. Utilizing S3 for Object Storage and Ensuring Data Consistency
4. S3 Security Measures and Bucket Policies
5. Implementing S3 Versioning
6. Identifying, Listing, and Downloading from Buckets
7. Challenge Labs
8. S3 Security Guidelines

Module 05- Network Security in AWS

1. Virtual Private Cloud (VPC) fundamentals
2. Security Groups vs Network ACLs
3. Subnetting and route tables
4. NAT Gateways, Internet Gateways, and Bastion Hosts
5. VPN and Direct Connect security
6. VPC peering and PrivateLink

Module 06- AWS Lambda

1. Introduction to Serverless Architecture
2. Creation and Deployment of Lambda Functions
3. Integration of Lambda with Other AWS Services
4. Utilizing Event Triggers
5. Lambda Enumeration (Console)
6. Lambda Enumeration (CLI / Pacu)
7. Challenge Labs
8. Lambda Security Guidelines

Module 07- AWS EC2

1. Initiating and Setting Up EC2 Instances
2. Understanding EC2 Instance Types and their Use Cases
3. Management of EC2 Instances and Security Groups
4. Launching Windows and Linux Instances
5. Configuration of Web Servers
6. Implementing Elastic IP
7. Load Balancing Varieties with EC2
8. Auto Scaling Applications with EC2
9. Snapshots of Volumes and Instances
10. EC2 Enumeration (Console)
11. EC2 Enumeration (CLI / Pacu)
12. Challenge Labs
13. EC2 Security Guidelines

Module 08- Data Security and Encryption

1. Data classification and handling
2. Encryption at rest and in transit
3. AWS S3 bucket policies and public access settings
4. Using AWS KMS and customer-managed keys
5. Secrets Manager

Module 09- AWS Privilege Escalation

1. **Overview of Privilege Escalation in AWS**
2. **Challenge Labs**
3. **Security Guidelines**

Module 10- AWS Security Tools and Services

1. **AWS Security Hub**
2. **AWS CloudTrail**
3. **AWS CloudWatch**
4. **AWS Inspector**
5. **AWS GuardDuty**
6. **AWS KMS (Key Management Service)**
7. **AWS WAF and AWS Shield**

Module 11- Capstone Challenges

1. **Real world Lab Introduction**
2. **Setting up a real world lab**
3. **Identifying vulnerabilities**
4. **Exploiting vulnerabilities**

Module 12- AWS Security Best Practices and Hardening

1. **Securing root account and credentials**
2. **Logging and monitoring best practices**
3. **Hardening EC2, S3, IAM, and Lambda**
4. **Real-world misconfigurations and lessons learned**