Certified Cloud Pentesting Professional (CCPA)

US# +1(732)293-7829 | India# +91-9810803769

Module 1
- Cloud computing essentials
- Cloud computing service models
- Risk analysis
- Dividing operational responsibility and visibility
- Managing user authentication
- Managing user authorization

Module 2
- Identifying needed security measures
- Ensuring SLA meet security requirements
- Securing the cloud Infrastructure
- Restricting network access through security groups
- Integrating cloud authorization systems
- Configuring platform specific user access control

Module 3
- What is cloud pentesting
- Threats of cloud pentesting
- Pre-requisites of cloud pentesting
  LAB SETUP
- Setting up vulnerable instances
- Setting up ubuntu

Module 4
- Installation of vulnerable
- services in EC2 instances
- Installation of windows server instance
- Kali installation
- Installation of vulnerable services
- Testing AWS and configuration check
- Elastic block storage
- Snapshots
- Retrieving Deleted Data
- Configuration of firewall

Module 5
- Automatic Pentesting
- Performing an automated vulnerability assessment
- AWS IAM
- Secret and Access ID Persistence
- Privilege Escalation on AWS Accounts
- Docker Security-Securing the container Images

Module 6
- AWS Lambda Service : Writing scripts for lambda
- Pentesting Tools AWS Audit Scout suite
- Attacking AWS logging and Security Services- Pentesting Cloudtrail GuardDuty.

Tools

1. Nmap
2. Zenmap
3. Netdiscover
4. Wireshark
5. Burp Suite
6. Nikto
7. WhatWeb
8. Wappalyzer
9. Metasploit
10. CrackMapExec
11. NSE Scripts
12. ExploitDB
13. Impacket
14. Postman
15. Nuclei
16. Nessus
17. Fing
18. SSLScanner
19. Currports
20. Responder
21. Netcat
22. Hydra
23. Netsparker
24. Acunetix

Email: enquiries@predictiveintels.com | Website: www.predictiveintels.com