Refonte Learning

E-Learning Providers

WELCOME TO REFONTE LEARNING

We are a leading IT company specializing in data analytics. We're excited to unveil our newest data analytics cohort, representing our continuous efforts since 2016 to develop a cutting-edge scientific trading robot based on Artificial Intelligence for the crypto currency futures market.

Enroll Now

https://refontelearning.com

REFONTE INTERNATIONAL TRAINING AND INTERNSHIP PROGRAM (RITIP)

Our programs span across various sectors, affording you exposure to a wide array of opportunities within your chosen field. Armed with handson experience and a robust professional network, you'll be poised for a fulfilling career.

At Refonte Learning, we are committed to transforming the educationto-employment journey. Our virtual internship initiative serves as a conduit to practical experience, empowering you to acquire essential skills and industry insights in a remote environment.

ABOUT REFONTE INFINI

We are a leading IT company specializing in data analytics. We're excited to unveil our newest data analytics cohort, representing our continuous efforts since 2016 to develop a cutting-edge scientific trading robot based on Artificial Intelligence for the crypto currency futures market.

Refonte Learning

Program Eligibility Criteria and Application Process

Eligibility Criteria:

- Currently pursuing a Bachelor's degree or any higher qualification.
- Weekly Time Commitment: 12-14 hours per week.
- Duration: 3 months.

STEP 1
Register

Sign up and apply to the course/program you're interested In

STEP 2
Pay

Pay the course fees to enroll and secure your spot.

STEP 3
Start Learning

Your learning journey begins immediately with the next upcoming cohort!.

Refonte Learning

Key Distinctive Program Features

Program Certificate

Certificate of Program Completion issued by Refonte Learning

Top Instructors

Expert-led Cybersecurity Masterclasses

Career Service

Refonte Career Services aids in elevating your visibility to hiring firms.

Capstone Project

Acquire practical experience through a capstone project.

Sandboxed Labs

Accessing integrated labs through Refonte's LMS.

Refonte Learning

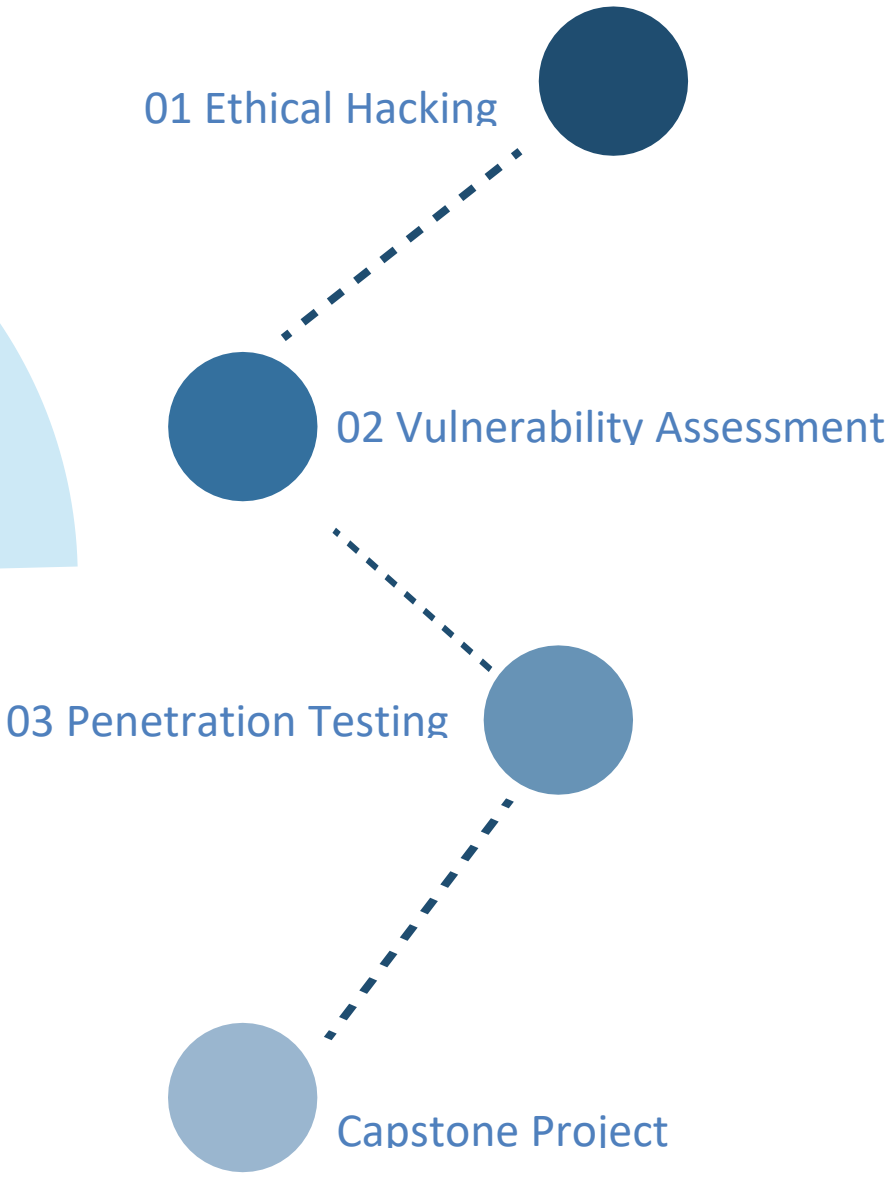
Connect with an Admission Counselor

We offer a team of committed admission counselors ready to assist you throughout the application process and address any related inquiries. They are available to:

- Respond to inquiries regarding the application.
- Aid in resolving your queries.
- Facilitate understanding of the program.

Refonte Learning

Visualization of Learning Paths



Refonte Learning

Who Would Benefit from Enrolling in this Program?

This program is tailored for individuals aspiring to enter the Cybersecurity and DevSecOps fields or seeking to enhance their skills.

While there are no specific prerequisites for enrollment, individuals in the following roles and disciplines would find this course particularly beneficial:

- Information Security Analyst
- Security Analyst
- Certified Ethical Hacker
- Security Consultant
- Information Security Manager
- Penetration Tester
- Vulnerability Tester
- Vulnerability Assessment Analyst
- Network Security Operations
- Application Security Vulnerability
- Cyber Penetration Testing Engineer
- Cybersecurity Application Engineer
- Security Architect
- Security Administrator
- Pentest Security Engineer

Refonte Learning

ETHICAL HACKING

In this course, you'll delve deeper into the concepts, implications, distinctions, and constraints of ethical hacking. You'll play a pivotal role in aiding organizations to implement novel hack-prevention strategies and technologies aimed at shielding systems from potential hacker intrusions.

Key Learning Objectives :

- Gain proficiency in utilizing online open-source intelligence tools for passive reconnaissance.
- Execute foot printing and reconnaissance, which are pivotal stages in the ethical hacking process, employing the latest methodologies and technologies.
- Master various scanning techniques utilizing NMAP and NPING, and perform scanning on the target network beyond the purview of Intrusion Detection Systems (IDS) and firewalls.
- Comprehend the functioning of web applications and web servers, identify their vulnerabilities, and learn preventive measures against potential attacks.

COURSE CURRICULUM

Introduction to Ethical Hacking

- Ethical Hacking
- Concepts & Outcome
- Differences & Limitations

Malware

- Malware Concepts
- Viruses and Worms
- Trojans
- Malware Analysis
- Anti-Malware Software

Scanning Networks

- Network Scanning Concepts
- Scanning Tools
- Port Scanning Techniques
- IDS/Firewall Evasion Techniques
- Banner Grabbing
- Draw Network Diagram

Footprinting & Reconnaissance

- Introduction to MReconnaissance
- Passive Reconnaissance
- Active Reconnaissance
- Counter Measures

Refonte Learning

Enumeration

What is Enumeration
LDAP Enumeration
NetBIOS Enumeration
DNS Enumeration
Enumeration Defence

Enumeration

Sniffing Concepts
Sniffing Techniques
- MAC Attack
- ARP Positioning
- Spoofing Attack
- DNS Poisoning

Sniffing Tools
Defending and Countermeasures
Techniques Against Sniffing

Vulnerability Identification & Exploit Selection

Vulnerability Assessment
Vulnerability Assessment Solutions
Vulnerability Scoring System
Exploit DB

Session Hijacking

Session Hijacking Concepts
Application-level Session

Social Engineering

Social Engineering Concepts
Social Engineering Attacks
Insider Threats
Social Networking Sites
Identity Theft
Assisted Demo:
- Getting Email IDs
- Available in the Public Domain using the Harvester

System Hacking

System Hacking Introduction
Password Cracking
Privileged Escalation
Executing Applications
Data Hiding
Covering Tracks

Denial of Service

DoS/DDoS Concepts
DoS/DDoS Attack Techniques

SQL Injection

SQL Injection Concepts
Types of SQL Injection

Refonte Learning

Hacking Wireless Networks

- Hacking Wireless Networks Concepts and Terminology
- Wireless Encryption
- Wireless Hacking
- Wireless Attacks
- Wireless Encryption Attacks

Cloud Computing

- Cloud Computing Concepts
- Cloud Computing Threats
- Cloud Computing Attacks
- Cloud Security Control Layers
- Cloud Security Tools

Hacking Web Servers

- Webserver Concepts
- Web Server Attack Methodologies
- Web Server Attacks
- Patch Management
- Web Server Security

Hacking Web Allocations

- Web Allocation Concepts
- Web A Threats
- Hacking Methodologies
- Hacking Tools
- Countermeasures

Hacking Mobile Platforms & IoT

- Mobile Platform Hacking
- Countermeasures
- Mobile Attacks
- Improving Mobile Security
- IoT Concepts
- IoT Technology Protocols
- IoT Operating Systems
- Countermeasures

Evading IDS, Firewalls, and Honeypots

- IDS/IPS - Basic Concepts
- Firewalls - Basic Concepts
- Honeypots
- How to Detect a Honeypot

Hacking Web Servers

- Cryptography Concepts
- Encryption Algorithms
- Hashes
- Public Key Infrastructure
- Disk Encryption
- Email Encryption
- Cryptonalysis
- Countermeasures

Refonte Learning

Vulnerability Assessment

Throughout this course, you'll develop the skills to systematically analyze security weaknesses within information systems. You'll assess whether the system is vulnerable to any known vulnerabilities, evaluate the severity of these vulnerabilities, and provide recommendations for mitigation or risk management as needed.

Key Learning Objectives:

- Develop a secure system and acquire expertise in vulnerability assessment and reconnaissance principles to safeguard both your infrastructure and online presence.
- Employ practical exploits to evaluate their impact on your systems effectively.
- Conduct a risk assessment and engage in threat modeling for web application architecture.
- Formulate an effective strategy for managing vulnerabilities to ensure success.

COURSE CURRICULUM

Lesson 1: Fundamentals of Vulnerability Assessment

- Introduction
- Scanning and Exploits
- Assisted Demo

Lesson 2: Analyzing Vulnerabilities and Exploits

- Uncovering Infrastructure Vulnerabilities
- Attacks Against Analyzers and IDS
- Exposing Server Vulnerabilities
- Assisted Demo
- Revealing Desktop Vulnerabilities

Lesson 3: Configuring Scanners and Generating Reports

- Implementing Scanner Operations and Configurations
- Creating and Interpreting Reports
- Assisted Demo

Lesson 4: Assessing Risks in a Changing Environment

- Researching Alert Information
- Identifying Factors that Affect Risk

Refonte Learning

Lesson 5: Risk Calculation

Risk Standard

Lesson 6: Managing Vulnerabilities

The Vulnerability Management Cycle
Vulnerability Controversies

Penetration Testing

Throughout this course, you'll conduct an assessment of a computer system's security by performing an attack. You'll analyze the system's resilience against both authenticated and unauthenticated attacks, considering various system roles and risk management factors.

Key Learning Objectives:

- Analyze the risk exposure of the organization across local and wide area networks.
- Perform penetration testing on web applications to enhance system security and stability.
- Simulate diverse attacks posing potential threats to business operations.
- Generate customized packets utilizing Netcat.

COURSE CURRICULUM

Introduction to Penetration Testing

Penetration Testing
Setting up a Hacking Lab
Phases of Penetration Testing

Reconnaissance

Introduction to Reconnaissance
Passive Reconnaissance
Active Reconnaissance

Testing

Exploit Identification
Web Application Concepts
Web App Threats
Web Application PT
Assisted Demo

Scanning Networks

Network Scanning Concepts
Scanning Tools
Port Scanning Techniques

Refonte Learning

System Penetration Testing

Exploiting and Gaining Access_x001D_
Setting up Metasploitable Exploitation_x001D_
Assisted Demo_x001D_

Web Application Penetration

Post Exploitation

Gaining Access

Refonte Learning

Secure Coding Practices

This part focuses on instilling secure coding principles and practices to minimize vulnerabilities in software development. By following industry standards and frameworks like OWASP and CWE, you'll learn how to proactively identify, address, and prevent common security flaws in your code. Through practical exercises and real-world examples, you'll gain the skills to build resilient, secure applications that stand up to modern cyber threats.

Key Learning Objectives :

- Understand the foundational principles of secure coding and why they are critical in the SDLC.
- Learn to identify and mitigate common vulnerabilities such as SQL injection, XSS, and CSRF.
- Develop secure authentication and authorization mechanisms to protect user data.
- Implement secure error handling, logging, and data validation techniques.
- Gain expertise in using tools for static code analysis (SAST) to identify vulnerabilities.

COURSE CURRICULUM

Introduction to Secure Coding

- Secure coding
- Analyzing a vulnerable application
- Identifying security risks

Secure Authentication and Authorization

- Implementing secure user authentication
- Securing APIs with OAuth2 and JWT
- Role-Based Access Control (RBAC)

Refonte Learning

Error Handling, Logging, and Sensitive Data Protection

- Writing secure error messages
- Logging best practices
- Encryption and hashing

Secure Code Analysis and Testing

- Static Application Security Testing (SAST)
- Writing secure unit tests

Infrastructure as Code (IaC)

This part will empower you with the knowledge and skills to design, implement, and manage infrastructure as code (IaC) securely and efficiently. You'll gain hands-on experience using IaC tools and frameworks to automate infrastructure deployment, enforce compliance, and mitigate risks. By the end of this course, you'll be equipped to apply best practices for IaC in real-world environments, enhancing both productivity and security.

Key Learning Objectives :

- Understand the principles and importance of Infrastructure as Code (IaC) in modern DevSecOps practices.
- Learn to write secure and scalable IaC templates using tools like Terraform, Ansible, or CloudFormation.
- Implement automated testing and validation for IaC configurations to minimize misconfigurations.
- Develop skills to integrate IaC with CI/CD pipelines for streamlined infrastructure deployment.
- Gain insights into managing secrets, permissions, and compliance for infrastructure.

COURSE CURRICULUM

Introduction to Infrastructure as Code

- Popular IaC tools
- Shifting security left

Refonte Learning

Writing Secure and Scalable IaC

- Structuring IaC for scalability and maintainability
- Best practices for writing secure IaC templates
- Common vulnerabilities in IaC

Testing and Validating IaC Configurations

- Tools for validating IaC configurations
- Automated testing and policy enforcement
- Debugging and troubleshooting IaC deployment issues

Integrating IaC with CI/CD Pipelines

- Setting up CI/CD pipelines for IaC
- Automating infrastructure deployment and updates
- Managing secrets and credentials in IaC workflows

Auditing and Monitoring IaC

- Security auditing tools for IaC
- Monitoring infrastructure changes and drift detection

CI/CD Pipeline Security

This part is designed to help you secure your Continuous Integration and Continuous Deployment (CI/CD) pipelines. You will learn how to integrate security into the pipeline, enabling the detection and prevention of vulnerabilities at every stage of the software development lifecycle. By the end of this course, you'll be equipped to design and maintain CI/CD pipelines that are resilient to modern threats while ensuring compliance with industry standards.

Key Learning Objectives :

- Understand the importance of securing CI/CD pipelines and their role in DevSecOps.
- Learn to identify potential security risks in pipeline components and configurations.
- Integrate security scanning tools for code, dependencies, and container images.
- Implement access control, secrets management, and compliance checks in pipelines.

Refonte Learning

Fundamentals of CI/CD Pipeline Security

- Overview of CI/CD pipeline
- Analyzing a CI/CD pipeline for potential risks

Securing Source Code and Dependencies

- Implementing secure coding practices in CI/CD
- Static and dynamic application security testing

Secrets Management in CI/CD

- API keys, tokens, and credentials
- Tools for secure secrets management
- Avoiding hardcoded secrets in code

Container and Infrastructure Security

- Scanning container images for vulnerabilities
- Securing IaC templates in CI/CD pipelines

Access Control and Pipeline Hardening

- Implementing role-based access control (RBAC)
- Preventing unauthorized access and supply chain attacks
- Hardening CI/CD pipelines

Monitoring, Auditing, and Incident Response

- Monitoring pipeline activities for anomalies
- Setting up alerts for security incidents
- Auditing pipelines for compliance with security standards
- Developing an incident response plan

Refonte Learning

Observability and Incident Response

This course focuses on equipping participants with the knowledge and skills required to implement robust observability practices and an effective incident response strategy. By mastering tools and techniques for monitoring, logging, and tracing, you'll ensure real-time visibility into system performance and reliability. Additionally, you'll learn to handle incidents systematically, minimizing downtime and mitigating risks to ensure service continuity.

Key Learning Objectives :

- Understand the fundamentals of observability and its components: metrics, logs, and traces.
- Develop the skills to identify, triage, and resolve incidents effectively.
- Create incident response plans and conduct post-mortem analysis to prevent recurrence.

Fundamentals of Observability

- What is observability ?
- Key pillars of observability: Metrics, logs, and traces
- Differences between monitoring and observability

Logging and Log Management

- Effective logging strategies for troubleshooting and compliance
- Securing and anonymizing sensitive log data

Monitoring and Alerting

- Best practices for monitoring system
- Setting up alerting systems
- Designing dashboards

Incident Response Workflow

- Lifecycle of an incident
- Effective communication during incidents

Refonte Learning

CONTACT US

official@refontelearning.com

Enroll Now

https://refontelearning.com