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 hands-on experience and a robust professional network, you'll be poised for a fulfilling career.

At Refonte Learning, we are committed to transforming the education-to-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

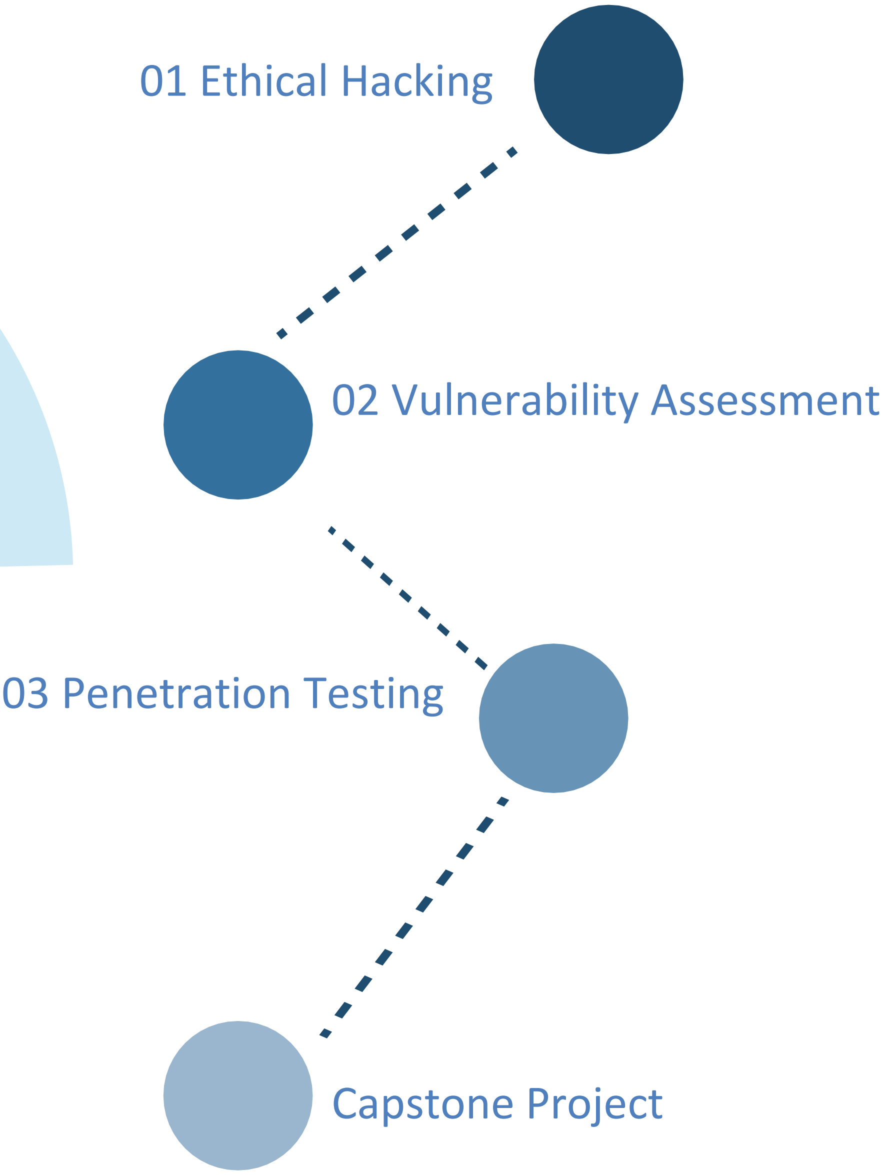
Accessing integrated labs through Refonte's LMS.

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.

Visualization of Learning Paths



01 Ethical Hacking

02 Vulnerability Assessment

03 Penetration Testing

Capstone Project

https://refontelearning.com

Who Would Benefit from Enrolling in this Program?

This program is tailored for individuals aspiring to enter the cybersecurity field or seeking to enhance their skills. It is designed to accommodate diverse professional backgrounds. 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

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

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

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

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

Testing

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

Reconnaissance

Introduction to Reconnaissance
Passive Reconnaissance
Active Reconnaissance

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

CONTACT US

official@refontelearning.com

Enroll Now