Training Course	**ROCHESTON Certified Cybersecurity Engineer (RCCE) Certification**
Course Language	**English**
Course Duration	**Total Number of hours: 40hours**
Course Objectives	**This cutting-edge innovation training is for corporate executives and students seeking to understand the key concepts involved in equipping you with the skillset needed to deal with the globalizing world, and to keep up with the changing times. The course offers you the training and awareness to deal with the vices of the digital world: prevent phishing, fraudulent activities, data theft and so on.** **The RCCE® Level 1 covers the foundational concepts of hacking. This course will give you a detailed, in-depth knowledge and hands-on labs. You will have mastery over hacking technologies and tools. For instance, it looks at Web application attacks, Trojans and Malware, Denial of Service attacks, metasploit, man-in-the middle attacks, android hacking, Wifi, Bluetooth, NFC, phishing attacks among others, firewalls, cryptography, cracking passwords, hacking the cloud and etc.**

Course Content	**Course Key Topic Area Includes:** **Module 01: Cybersecurity Threats, Attacks and Defenses** **Module 02: Information gathering and network scanning** **Module 03: Cyber Vulnerabilities** **Module 04: Web Application Attacks** **Module 05: Web shells, Spywares and Backdoors** **Module 06: Denial of Service Attacks** **Module 07: Packet Sniffers and Network Analyzers** **Module 08: Password Cracking** **Module 09: Wireless Hacking** **Module 10: Firewalls and IDS** **Module 11: Hacking Frameworks** **Module 12: Cryptography** **Module 13: Phishing attacks** **Module 14: Malware Attacks** **Module 15: Hacking Smart Objects** **Module 16: Hacking Power Grids** **Module 17: Hacking Connected Cars** **Module 18: Hacking Mobile Phones** **Module 19: Hacking the Cloud Networks** **Module 20: Patch Management** **Module 21: IoT Hacking** **Module 22: Penetration Testing** **Module 23: Cybersecurity Policies and Procedures** **Module 24: Incident Response** **Module 25: AI in Cybersecurity** **Module 26: Cyber threat Intelligence** **Module 27: Supply Chain Attacks** **Module 28: Python, PHP, Perl and Ruby Scripting Languages**
Learning Outcomes	**At the end of the program the trainees will be able to:** • **Form best business practices through real world case studies**

Learning Outcomes	• **Equip with in-depth knowledge about instances of mobile/Computer/Personal Network attacks, wireless attacks, application attacks, phishing, social network attack and so on, bringing them closer to the real-life experiences of cyber-attack and hacking.** • **Analysis of tools, techniques and models: Students gain insight into OSI and TCP/IP models, understand software flaws, network misconfigurations, ARP protocol, sniffing and hijacking tools to stay ahead of hackers and keep organizational systems secure.** • **Ensure safe communication over networks: Students get to understand the network terminologies and communication protocols and learn how to identify and filter noise or anomalies in a network.** • **Leverage current trends to develop better business strategies - equip with current trends with the most recent statistical analysis to lay the groundwork for developing best business strategies.** • **Equip with knowledge on encryption algorithms and ways to generate encryption keys, develop an understanding of file systems and frameworks used for hacking, understand the architecture for secured modern web applications, understand the use of right widgets and programming languages that would prevent hackers from scraping websites, use Address Resolution Protocol, use botnets and so on.**

- **Be equipped to prevent instances of cyber threats such as hacking, detecting phishing attacks, malware, identifying internal and external security threats as well as understand the distributed-denial-of-service attacks and implement strategies to mitigate them.**
- **A Rocheston Certified Cybersecurity Engineer (RCCE) is equipped with a strong foundation to handle cybersecurity for future technologies and use tools to keep hackers from exploiting the unseen breaches in the digital world.**

The following are the skills that the trainees will pick up upon enrolling for the course:

- **Creating cybersecurity solutions - Finding solutions for all cybersecurity problems and avoiding crisis.**
- **Setting up secured communication networks - Become aware of safer ways and means of communication.**
- **Developing frameworks to facilitate best engineering practices - Implement technologies for storing information in a safe and secure manner.**
- **Enforcing substantial security to avoid potential cybersecurity threats - Gaining the capacity to apply best security practices to avert potential cybersecurity incidents.**
- **Penetration testing - Learn how to test the existing security tools and document the periodical reviews.**
- **Sustaining risk management processes - Best practices to ensure proper risk management processes across domains.**

Target Audience	**The RCCE program is aimed at Software Professionals, Cybersecurity Personals, Data & IT Professionals and anyone that wants to broaden their horizon on their cybersecurity knowledge.** **Requirement :** **Bachelor's degree with 1 year of work experience or degree in computer science, engineering, mathematics, and other computer-related fields.** **Knowledge of Server administration, HTML, Web technologies, TCP/IP and network management skills. Linux and programming skills is not a requirement, we will expose you to basic Linux commands in the class.** **Computer with minimum 8GB Ram.**
Course Material /Technology used/ Details Relevant to the course.	**Electronic Kit via Cyberclass (ROCHESTON's E-Learning Platform) inclusive of online Course Materials for 1 year access.** **Exam Duration: 120 minutes** **No of Exam Question: 90** **Passing Mark: 72** • **Exam Retake Fee: USD400** • **The exam will be conducted on the last day of the training based on the trainer's discretion.** • **The students will receive the RCCE Level 1 certification after passing this test. The certification is valid for 2 years. You can renew the certification.**