ROCHESTON® CERTIFIED CYBERSECURITY ENGINEER

Level 1

RCCE® Certification Program Guide

INTRODUCTION (RCCE®) - Foundation Program

Cybersecurity holds out a safe haven for all the vulnerabilities and cyber threats that keep challenging our safe presence in the digital world. **With possibilities galore, the high-tech world of computers invites us, but at the same time it can intimidate us if we are caught unaware.** Today, we face the challenge of building a formidable citadel against the emerging threats in the cyberworld - we must prepare ourselves with adequate knowledge and expertise. Rocheston Cybersecurity Certification equips you to become certified specialists for safeguarding corporate and trade secrets, digital and intellectual properties, sensitive personal information and of course, for keeping computing devices safe against spying apps and malware.

With emergence of smart technologies, the future looks exciting, but are we adequately equipped to handle those technologies? **Rocheston offers you the training and awareness to deal with vices of the cyber world: prevent phishing, fraudulent activities, data theft and so on.**

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.

BENEFITS

Is our society well-equipped to fight the globally organized crime syndicates? Can we prevent the Dark Web from becoming the hideout for terrorists and criminals? Are we appropriately equipped to monitor and reverse engineer cyberattacks on company trade secrets and information databases? If the answer is not an emphatic "Yes", we must prepare ourselves!
A Rocheston Certified Cybersecurity Engineer is nurtured to be the savior!

Companies, governments and individuals must level up their defense and security controls against increasing exploits of hackers. **Therefore, we prepare our students with these benefits:**

Best business practices through real world case studies: Equip students with in-depth knowledge about instances of mobile 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.

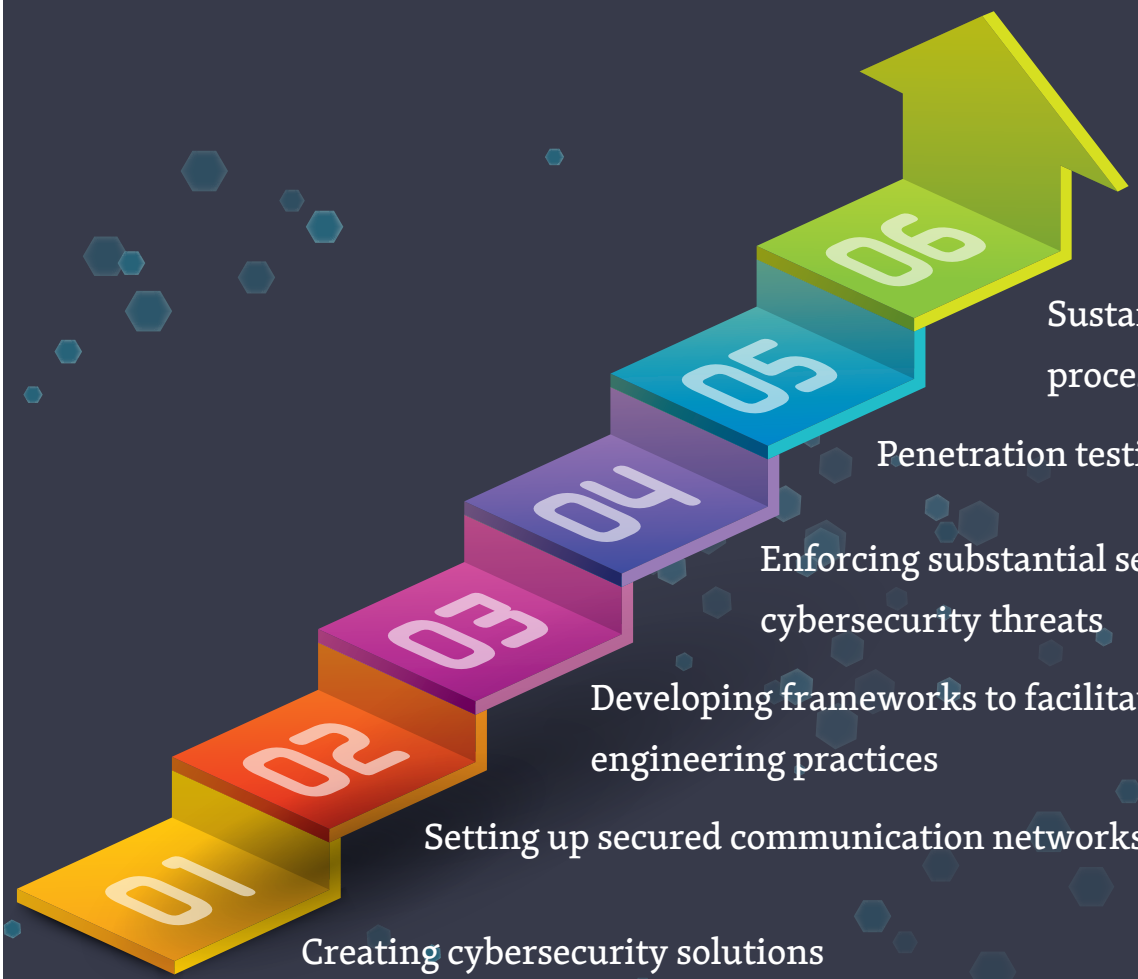
Ensure safe communication over networks: Students get to understand the network terminologies and communication protocols and learn how to identify and filter noise or anomalies in a network.

Leverage current trends to develop better business strategies: Students are taught about the current trends with the most recent statistical analysis to lay the groundwork for developing best business strategies.

Immediate distinction in your profile: The certification would enrich your profile to obtain the best possible, and highly paid positions in cybersecurity, across industries.

SKILLS YOU WILL LEARN

The following are the skills that the student 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.

JOB OPPORTUNITIES

- Intrusion Detection Specialist
- Computer Security Incident Responder
- Source Code Auditor
- Virus Technician
- Cyber Security Analyst
- Cyber Security Engineer
- Cyber Security Architect
- Cyber Security Administrator
- Security Software Developer
- Cryptographer
- Crypto Analyst
- Cyber Security Consultant
- Penetration Tester
- Information Security Manager

WHO CAN TAKE UP THE PROGRAM

Individuals who wish to build a career across the following industries:

- Healthcare
- Smart Cities
- Industry 4.0
- Transportation
- Electronics
- Governance
- Automation
- Robotics
- Telecom
- Smart Appliances
- Department of Defense
- Finance

Engineers

Cybersecurity Specialists

Data & IT Professionals

Software Professionals

ELIGIBILITY

Bachelor's degree with 1 year of work experience or degree in computer science, engineering, mathematics, and other computer-related fields.

Potential candidates should also have some basic knowledge in **web development, HTML, HTTP, and application security.**

WHY RCCE IS DIFFERENT FROM OTHER CYBERSECURITY COURSES?

A cybersecurity engineer is the knight in a shining armor, well-endowed to fight the vices of the fast-expanding cyber world today. **An RCC engineer can be called forth to fight Government espionage, hacktivists, organized crime groups, external and internal data theft and so on.**

As a Cybersecurity Engineer:

You will be equipped to pr event instances of cyber threats such as **hacking, detecting phishing attacks, malware, identifying internal and external security** threats and so on.

You will understand **distributed-denial-of-service attacks and implement strategies** to mitigate them.

You will be the architect for **secured modern web applications, understand use of right widgets and programming languages** that would prevent hackers from scraping websites, use Address Resolution Protocol, use botnets and so on.

You will develop understanding of **file systems and frameworks used for hacking.**

You will learn about **encryption algorithms and ways to generate encryption keys.**

SYLLABUS

Module 1: Cybersecurity threats, attacks and defenses

- Shape your fundamentals in Cybersecurity
- Types of Security Controls
- Discern the Vulnerabilities in this field
- Different Categories of Cybercriminals
- Kinds of Cyberthreats
- Understand cyber security breaches
- Learn to protect Data breaches
- Prevention from Distributed Denial of Service (DDoS) attack
- Anticipate Phishing Attacks
- Get acquainted with the Greynoise Visualizer
- Discover the intricacies of Internet of Things (IoT) in the Digital Age
- Venture into cloud computing
- Dangers of Social networks

- Get accustomed to two-factor Authentication that provides secure solution
- Kick-start your venture into the Dark Web
- Learn more about Ransom ware
- Methods of targeting or acquiring trade secrets
- The impact of Artificial Intelligence (AI)
- Analysing the defensive mechanisms
- Study the complexities of GDPR compliance

Module 2: Information gathering and network scanning

- Understand information gathering
- Types of information gathering
- Understanding an attacker's perspective
- Understanding an investigator's perspective
- Seven layers of the OSI model
- Understanding an IP address
- Creating multiple logical networks using subnetting
- Working of ping and traceroute
- Port scanning types
- Working and types of DNS
- Concept of website monitoring

- Understanding tools like Maltego, theHarvester, Spiderfoot, Creepy, and Foca
- Understanding mirroring tools
- Dealing with fake news and fake people
- Accessing Blocked websites
- Understanding proxy servers
- Concept of Google's outline tool
- Different Tunnelling concepts
- Understanding e-mail tracking
- Protection of data
- Information gathering tools

Module 3: Cyber Vulnerabilities

- The effects of Vulnerability
- Categorization of vulnerabilities
- Vulnerable phase of common computer security
- Security of Internal Network
- Security auditing and vulnerability assessments according to Industry Compliance Standards
- Mechanism of a Network Vulnerability Scanner
- Methods of vulnerability management

- Overcoming Challenges in vulnerability management
- Learn more about MITRE ATT&CK and its observations
- Types of Vulnerability scanners
- Detect breaches with Threat Intelligence
- Delve into the heart of the problem using Darktrace-AI Scanner
- Analyse network traffic with Extrahop Reveal(X)
- Investigate anomalies in user behavior using Netwrix Auditor
- Accounting data breach with SolarWinds Risk Intelligence
- Check Cyber Exposure visibility through Nessus
- Study the Various bands under Qualys
- Get a clear picture of your IoT devices using Retina IoT Scanner (RIoT)
- Get acquainted with bbqsql SQL Injection Tool
- Test the compliance of systems with Lynis
- Sneak on stealth mode using Nikto

Module 4: Web Application Attacks

- Concept of web application and its complexity
- How do web application attack work
- Delve into web application analysis, information gathering and enumeration

- Understand web application attacks, land to network and Infrastructure penetration testing
- Different types of attacks
- Web application detection methods
- Understanding the software development lifecycle
- Steps involved in security assessment
- Handling error
- Concept of clickjacking
- Understanding SQL injection

Module 5: Web shells, Spywares and Backdoors

- Understand what a Docker is
- Understand what Containers are
- A comparison between Virtual machines and Containers
- Learn about container orchestration tool
- A list of Docker commands
- Go about the Attack Methodology
- Understand the Web Shell concept
- Understand Web Shell attacks
- The types of Web Shells

- Steps involved in Gmail Phishing Script
- Have a detailed understanding about the types of web shells
- Learn about Fat Rat Trojan
- Learn about Dr0o1t Framework Trojan
- Learn about EvilOSX Trojan for macOS X
- Understand the tools for setting up backdoors
- Steps in Backdoor Payloads transfer by DNS Traffic and its working
- Understand ICMP backdoor
- The working of DNS-Persist Trojan
- Learn about Keyloggers and types for different OSs
- Learn about various monitoring systems
- Understand the concept of Steganography
- Understand the working of Instegogram
- Go about Steganography tools
- A brief understanding of Ransomware

Module 6: Denial of Service Attacks

- Learn about what DoS attacks are
- How DDoS attacks works
- Detecting a DoS attack

- Understand DDoS attacks and how they work
- The types of DDoS attacks
- Learn about DDoS and DoS attacks in detail and their working
- Go through case studies for a better understanding
- Know about the tools that are used to launch DoS and DDoS attacks
- Difference between Dos and DDoS attacks
- Different types of DDoS attack tools
- The largest DDoS attacks of all time
- What is Blackhole Routing
- Understand DDoS mitigation strategies

Module 7: Packet Sniffers and Network Analyzers

- How computers are connected in a network
- Understanding the OSI model and addressing
- Address Resolution Protocol (ARP)
- Types of network analysers and packet sniffers
- Topology mapper
- Working of network monitor
- NetFlow traffic analyser and types
- Understand Scrutinizer

- Spoofing and its types
- Understanding Man-in-the-middle attack and its types
- Ways in which attackers work
- Understanding MITM tools and commands used
- Running spoofing and sniffing in Bettercap
- Network statistics tool
- Learn how hijacking is done and tools used
- Types of hacking tools

Module 8: Password Cracking

- Understand the vulnerable types of passwords
- Methods in which passwords are attacked
- How password lengths help in increasing security
- Why attackers can't use Brute-force in web services
- Learn about the types of password alternatives
- What are Electronic tattoos
- Know about encryption key and its types
- Understand Hashing and CRCs

- Learn about the types of Hash functions
- Familiarise with Rainbow table
- Know about Password managers
- What happens when passwords are stored in one place
- The available software for storing and generating passwords and saving important credentials
- Learn about the cracking tools and types
- The types of applications that can be used by password crackers
- Password recovery tools available
- Steps to crack passwords in Windows OS
- Password reset utility tools for Windows
- Understand Quantum Computing

Module 9: Wireless Hacking

- Concept of Wi-Fi
- Types of attacks
- Understanding MiTM attacks
- Creation of rogue access points
- Concept of brute-force attacks
- Cracking Wi-Fi passwords

- Concept of Air crack
- How to monitor tools
- Understanding Pineapple wifi
- Usage of Commercial tools

Module 10: Firewalls and IDS

- The infrastructure components in organizations
- What are firewalls and its requirements
- Learn about Stateful Inspection
- Types of firewalls and their functioning
- Know about Nextgen Firewall
- The threat scanning techniques
- How the Nextgen Firewall functions
- The Threat scanning methods
- Learn about URL filtering
- Under the Unified Threat Management (UTM)
- What are firewalls for Virtual Infrastructure
- The limitations in Firewall Inspection
- Firewall recommendations based on requirement
- Policies considered in Firewall

- The list of open-source firewalls
- An elaborate understanding on the open-source firewalls
- Know about Firewall Analyser
- The list of cloud-managed firewalls
- A thorough understanding on cloud-managed firewalls
- Understand Microsoft Azure Security Centre
- How to hack firewalls
- Techniques for hacking firewalls
- Methods for bypassing firewalls
- HTTP tunnelling and steps involved in it
- Understand SSH tunnelling
- Understand Reverse SSH tunnelling
- Understand ICMP tunnelling and the steps involved
- How DNS tunnelling works
- Learn about Intrusion Detection System (IDS)
- The methodologies in IDS
- The types of IDS
- Working of the different types of IDS on LINUX OS
- Types of HIDS in Linux
- Types of NIDS in Linux

- A deeper understanding on the types of HIDS & NIDS
- Look through script examples
- What is policy-neutral logging
- Look through log examples
- Learn about Advanced Intrusion Detection System (AIDS)
- Go about the configuration steps
- Learn about Elastic Stack and its need
- Understand Logstash and its working
- Learn about Beats
- Learn about Journalbeat, Packetbeat, Heartbeat and Filebeat
- Know about Commercial IDS Products
- Learn about testing firewall configurations

Module 11: Hacking Frameworks

- Learn about Metasploit Framework
- Commands used in Metasploit Framework
- Learn how to import Nessus Scan into Metasploit
- Learn about Reverse Shell

- Understand Metasploit Payloads- Binaries, Web, Scripting, Shellcode
- Learn about Handlers
- Learn the steps involved in building Linux Trojan
- Understand Payloads Using VBScript and steps involved
- What is Privilege Escalation and the commands
- Steps for creating Trojan backdoors using EXE files
- Steps involved in Tomcat and Java Payload
- Learn about File Inclusion Attack, types and its working on different OSs
- Understand the steps in PHP Meterpreter
- Learn about Vulnerable Command Execution
- Rapid7 Metasploit Community Edition
- Social Engineering Toolkit
- How to launch credential harvesting attack

Module 12: Cryptography

- Understanding encryption
- Usage of PKI Keys
- Generation of private and public keys

- Concept of factorization
- File encryption using SSL Security
- How to go about encryption
- GPG and securing files
- Understanding digital signatures
- Cracking RSA encryption
- Generation of private keys
- Understanding Factordb

Module 13: Phishing attacks

- What is a Phishing attack?
- Types of Phishing attacks.
- Phishing scams
- How does a Phishing attack work
- Methods of attack
- The phishing attack structure
- Destination links and Tracking images in emails
- Challenges in securing online accounts.
- Bypassing two factor authentication
- How to be invisible online.

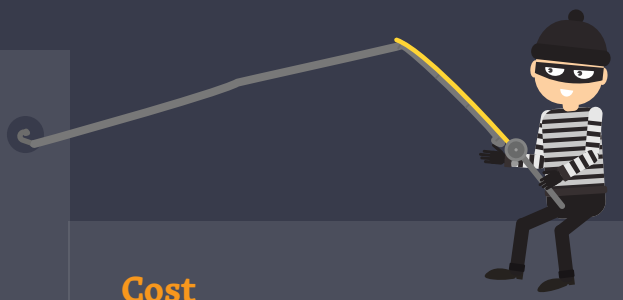
Module 14: Malware Attacks

- What is Malware Analysis?
- Fully automated analysis
- Static properties analysis
- Interactive behavior analysis
- Manual code reversing
- Dynamic malware analysis
- Binary Analysis tools
- Debuggers
- Sandboxes
- Disassemblers
- Malware analysis use cases
- Infection Vectors

Course Structure

What the course will consist of:

- Exam Code: RCT-79
- No. of Question: 90
- Passing score: 72%
- Exam is available at VUE and Cyberclass®
- The RCCE Level 1 exam will be conducted on the last day of the training
- The students will receive the RCCE Level 1 certification after passing this test
- The certification is valid for 2 years. You can renew at Accord portal

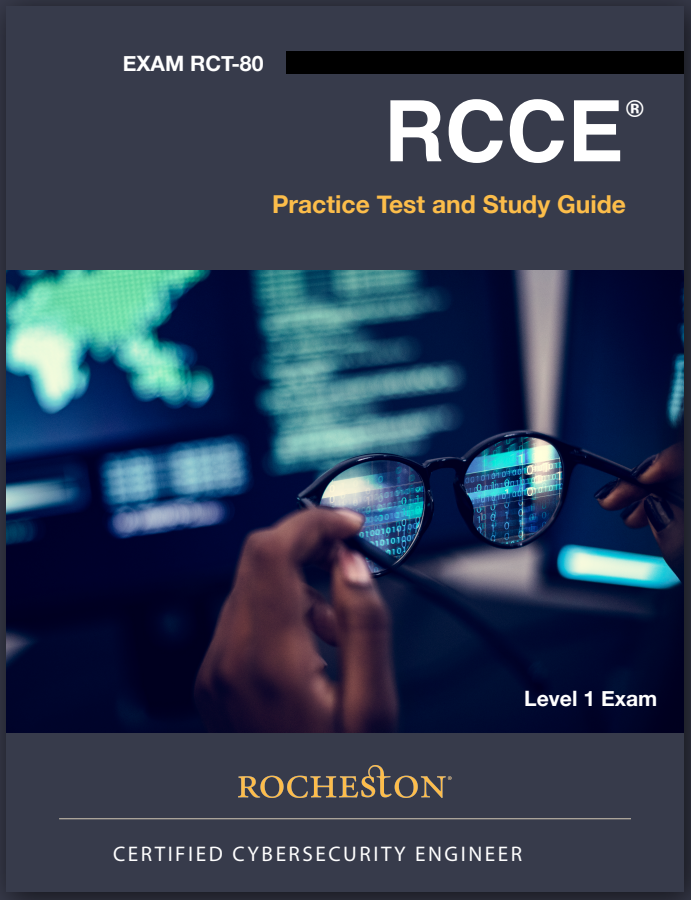


Cost

For pricing in your region, please contact the local distributor.

RCCE® Exam Preparation Study Guide

Students will receive **RCCE® Level 1** as part of the training kit. The study guide will prepare the students to pass the test. The guide comes with over **500 sample exam questions.**



RCCE Certificate

ROCHESTON® CERTIFIED
CYBERSECURITY ENGINEER

THIS CERTIFICATE IS PRESENTED TO

Jason Springfield

FOR COMPLETING ALL THE REQUIREMENTS TO BECOME A
ROCHESTON CERTIFIED CYBERSECURITY ENGINEER

HAJA MOHIDEEN
PRESIDENT & CEO

rcce

ROCHESTON® AUTHORIZED
TRAINING PARTNER

ROCHESTON® CERTIFIED CYBERSECURITY ENGINEER

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON® CERTIFIED CYBERSECURITY ENGINEER

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON®

BE EXCEPTIONAL