ROCHESTON CERTIFIED

# CYBERSECURITY ENGINEER

Level 1

RCCE® Certification Program Guide

ROCHESTON®
RCCE HACKER
Signed by Haja
I'am a stealth Lady Hacker
I'am badass, seriously
I'm an RCCE® Cybersecurity Engineer

# About Rocheston

Rocheston, a young New York based internet technology start-up, despite being in its nascent stage, is a company that is raring to go. Rocheston has a worldwide presence, with its headquarters in New York. The company's technology development center is based out of Chennai, with reach offices in Singapore and Dubai.

The team at Rocheston consists of young, liberal, innovative and forward-thinking individuals **who want to make a difference and change the world. At its core, Rocheston is a next-generation innovation company**, with cutting-edge research and development in emerging technologies such as Cybersecurity, Internet of Things, Big Data and automation.

# Rocheston Certified Cybersecurity Engineer

## RCCE Level 1 Extreme Hacking

Dive into the world of cybersecurity with the comprehensive and in-depth **RCCE® Level 1 certification program.** This course offers a solid foundation in hacking concepts and provides extensive hands-on labs for mastering various hacking technologies and tools. Designed for those looking to excel in the field of cybersecurity, the **RCCE® Level 1 is a prerequisite for progressing to the advanced Level 2 program.**

## Pre-requisite

Participants should possess knowledge of server administration, HTML, web technologies, and TCP/IP. Familiarity with network management skills is also necessary.

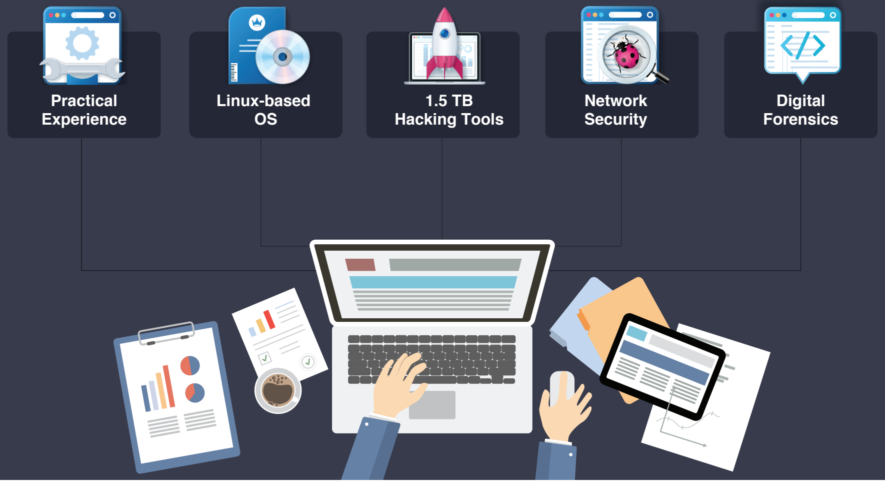
While Linux and programming skills are not required, basic exposure to Linux commands will be provided during the course.

CRITICAL ERROR
ALL PROCESS TERMINATED

# Hands-On Labs

The **Rocheston Certified Cybersecurity Engineer (RCCE) course is an intensive hands-on program designed to equip aspiring cybersecurity professionals with the skills and knowledge required to defend against a wide range of cyber threats.** A key component of the RCCE course is the hands-on labs, which provide students with practical experience in using cutting-edge cybersecurity tools and techniques.

These labs are powered by **Rocheston's proprietary Linux-based operating system, Rocheston Rose Cybersecurity OS.** This specialized OS has been developed specifically for use in the RCCE course and contains an extensive collection of hacking and cybersecurity tools, amounting to over 1.5 TB of resources.



Practical Experience

Linux-based OS

1.5 TB Hacking Tools

Network Security

Digital Forensics

**The hands-on labs in the RCCE course are hosted on the cloud,** which means students can access and complete them using a web browser. There is no need to install any additional software or hardware, making it incredibly convenient and easy for students to practice their skills from anywhere, at any time.

**The labs cover a wide range of topics and techniques, from penetration testing and vulnerability assessment to network security and digital forensics.** Students will work through real-world scenarios and challenges designed to test their knowledge and hone their skills in a safe, controlled environment.

**Penetration Testing:** Students will learn how to identify and exploit vulnerabilities in a target system, using a range of tools and techniques to gain unauthorized access and maintain control.

**Vulnerability Assessment:** Students will practice identifying and assessing potential security vulnerabilities in a system, using various scanning tools and methodologies to evaluate the risk and recommend appropriate remediation measures.

**Network Security:** Students will gain hands-on experience in securing networks from various threats, including configuring firewalls, intrusion detection systems, and VPNs, as well as monitoring network traffic for signs of malicious activity.

**Incident Response:** Students will learn how to conduct digital forensic investigations, including the collection and analysis of digital evidence and the proper handling and preservation of evidence to maintain its integrity.

**Risk Management:** Students will practice responding to cybersecurity incidents, including the identification, containment, and eradication of threats, as well as the recovery and restoration of affected systems.

# Course **Structure**

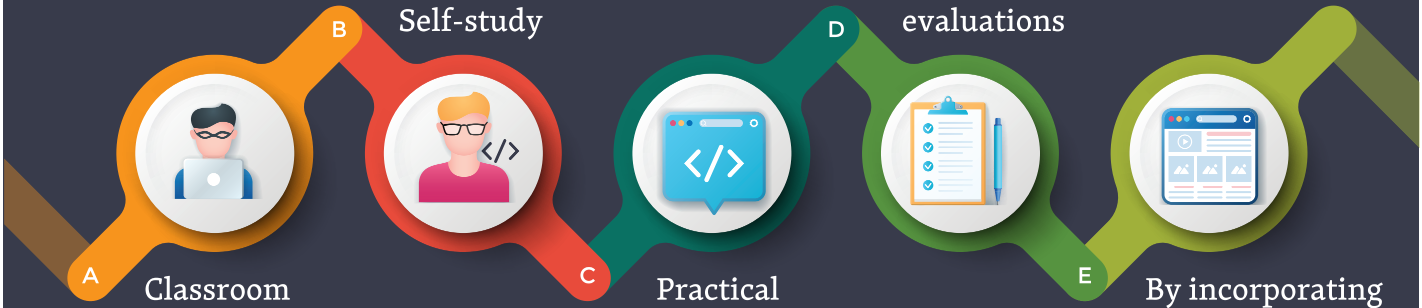
- The **RCCE® Level 1 is a 5-day intensive program**, running from 9:00 AM to 5:00 PM daily.
- The course is exclusively based on Linux. Despite being a foundation course, the **RCCE® Level 1 offers an unparalleled depth of knowledge and expertise in cybersecurity.**
- Blended learning is an educational approach that combines various teaching methods to create a comprehensive learning experience for participants.
- This approach merges traditional face-to-face instruction with technology-based learning, such as online resources, virtual classrooms, and digital tools.
- The primary goal of blended learning is to provide a more effective and engaging learning experience by catering to different learning styles, preferences, and schedules.

ROCHESTON®

# RCCE **Blended Learning**

In the context of the

**RCCE® Level 1 course, blended learning involves the following components:**



Classroom based learning

Self-study

Practical assignments and exercises

Assessments and evaluations

By incorporating these different components

**Classroom based learning:** This component involves direct interaction between the instructor and participants in a physical or virtual classroom setting. It allows for real-time feedback, group discussions, and hands-on activities. Participants can ask questions, clarify doubts, and engage in collaborative problem-solving. Classroom-based learning also fosters a sense of community among learners, which enhances motivation and commitment to the course.

ROCHESTON®

**Self-study:** This component enables participants to learn at their own pace using various online resources, such as videos, articles, and quizzes. Self-study allows learners to review course material as often as needed, practice skills, and explore additional resources to deepen their understanding of the subject matter. This approach is particularly beneficial for those who require more time to grasp complex concepts or prefer to study independently.

**Practical assignments and exercises:** These activities help participants apply the theoretical knowledge gained in the classroom to real-world scenarios. They often involve hands-on tasks or simulations that require learners to use specific tools, techniques, and procedures relevant to cybersecurity. Practical assignments not only reinforce learning but also help participants develop critical thinking and problem-solving skills.

**Assessments and evaluations:** Throughout the course, participants are assessed on their understanding of the material and their ability to apply it in practical situations. Assessments can take various forms, such as quizzes, tests, or project-based evaluations. Regular assessments help both the instructor and the learner gauge progress and identify areas that need improvement.

**By incorporating these different components:** The blended learning approach in the RCCE® Level 1 course ensures that participants receive a thorough and well-rounded education in cybersecurity. This approach caters to diverse learning preferences and enables learners to develop a strong foundation in the subject while acquiring practical skills relevant to the industry.

# RCCE Exam

The **ANSI accredited RCCE® Level 1 examination will be conducted on the final day of the course**. Successful completion of the exam will grant participants the prestigious Rochester Certified Cybersecurity Engineer Level 1 certification, setting them apart from their peers.

**Unlock your potential in cybersecurity engineering with the RCCE® Level 1 certification program and become a sought-after professional in this rapidly evolving field.** Rocheston has reinvented hacking, offering a unique and unparalleled learning experience.

RCCE
Cybersecurity Engineer

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17024
PERSONNEL CERTIFICATION BODY

# What You Will Learn?

The RCCE Cybersecurity training program encompasses sophisticated ideas, methodologies, and frameworks. This course is 95% focused on hands-on labs and practical exercises.

**The following subjects are addressed in the curriculum.**

- Vulnerability Management
- Penetration Testing
- Zero-Trust Model
- Quantum Computing
- Cyberthreat Intelligence
- Monitor Network Traffic
- Password and Credential Management
- Secure WiFi Deployments
- Encryption and Cryptography
- Scams and Phishing Attacks
- Malware Analysis and Research
- Hack Android and iOS Devices
- Patch Management
- Artificial Intelligence

ROCHESTON®

- Supply Chain Attacks
- Powershell Scripting
- Azure CLI Scripting
- SQL Injection Attacks
- Ransomware Attacks
- Generate Fake News and Images
- Penetration Testing Report Writing
- Cybersecurity Policies and  Governance
- Risk and Threat Assessments
- Incident Response and Mitigation
- Bullying Using Social Media
- Attacks On IOT Devices
- Dark Web and Cybercrime Market
- BGP, ASN and Internet Routing Protocols
- QUIC, Cloudfare and Caching Edge Servers
- IPFS Decentralized Filesystem
- DNS, Spoofing and Website Mirroring
- Faceswap and Deepfake Technologies
- Bots and DDOS Attacks

ROCHESTON®

- Intelligence Gathering With OSINT
- Face Detection and Machine Learning
- Video Tampering And Reputation Management
- VPN, Proxy Servers AND HTTP/ICMP Tunneling
- WebRTC, STUN TURN and Video Conferencing
- GDPR, CCPA and Regulatory Compliance
- Hacking Lifecycle O-Day Exploits, CVE and NVD
- Asset Discovery And Network Scanning
- Cyberthreat Intelligence
- Privacy Laws, Data Mining and Data Brokers
- Log Management Using Splunk Data Analysis
- Greynoise And Shadowserver
- SOC2 Dashboards Build Threat Intel Attack Maps
- Cybersecurity Policy Frameworks
- NIST Cybersecurity Standards
- CMCC Cybersecurity Framework
- Network Discovery And Network Monitoring
- Security Breaches And Test Cases
- Penetration Testing Cheat Sheets

ROCHESTON®

- Scan Networks Using Rocheston Vulnerability Vines
- Types of Vulnerability Scanners And Techniques
- Inspect Source Code Using Microsoft App Inspector
- Network Socket Programming Using NodeJS
- Modern Web Application Architectures
- Dfinity Distributed Internet Computer
- Program Microsoft SQL Server Database
- Manage LDAP Servers Using OpenLDAP
- Manage CMS Wordpress, Magento Drupal, Opencart
- Detect Vulnerable Web Applications
- Build Websites Using Jekyll
- Deploy Private Clouds
- Deploy Load Balancers Using HAPROXY
- Manage File Synchronization Across Servers
- Spoofing, Botnets, APT, Cache Poisoning And Encryption
- Role Based Access Controls
- Cross-Site Request Forgery And MiTM Attacks
- Cookies And Session Management
- DevSecOps Ci/cd Pipelines
- SDLC And Software Development Methodologies
- File Inclusion Attacks And Code Obfuscation

ROCHESTON®

- Trap Hackers Using Honeypots
- Sonarqube Source Code Analyzer
- Cybersecurity Gamification
- Dockers, Containers And Virtualization
- Deploy Kubernetes on Google Cloud
- Run Linux Desktop inside Dockers
- Deploy Containers in Google Cloud
- Deploy EC2 Instances in Amazon AWS Cloud
- Deploy Virtual Machines in Microsoft Azure
- Face Detection Using  Microsoft Cognitive Services
- Face Detection Using Amazon Rekognition
- Mitre Attack Framework And Methodologies
- Deploy PHP Webshells And Backdoors
- Deploy Wordpress Fake Plugins
- Analyze Threat Vectors and APT Actors
- Deplay Phishing Attacks And DNS Spoofing
- Run Phishing Campaigns Using Frameworks
- Launch Secure Tunnels And Bypass Firewalls
- Deploy Backdoor Payloads Using DNS Traffic
- FAT Rat, Evilosx And DrooIT Trojans
- How To Hack Passwords With 2FA Authentication

- Create ICMP Backdoor Tunnels
- Infect Systems With Backdoors Using C&C Servers
- macOS Trojans, Windows Trojans, And Window Botnets
- Employee Monitoring Services
- Keyloggers and Spywares
- Phone Monitoring And Screen Recorders
- Hide Data Using Steganography
- Create And Launch  Ransomware Attacks
- DDOS Attacks,IP Spoofing And Botnets
- Tor Circuits RedEye and UFONET
- HTTP Flooding,SYN Flooding And DNS Amplification
- Cloudflare Global Network Data Centers
- OSI and TCP/IP Networking Model
- ARP, Data Frames, Mac Address and TCP/IP v6
- Network Topology Mapper and  Network Monitoring
- Password Cracking Credentials Stuffing
- E-mail Hijacking, Wi-Fi Sniffing and Stealing Cookies
- Brute-Force Attacks and  Cracking Online Passwords
- Cracking Encryption Keys, CRC and Checksum
- Distributed Password Cracking Using Hydra and Hashcat
- Google Captcha and OAUTH Protocol
- OpenID Decentralized Authentication

ROCHESTON®

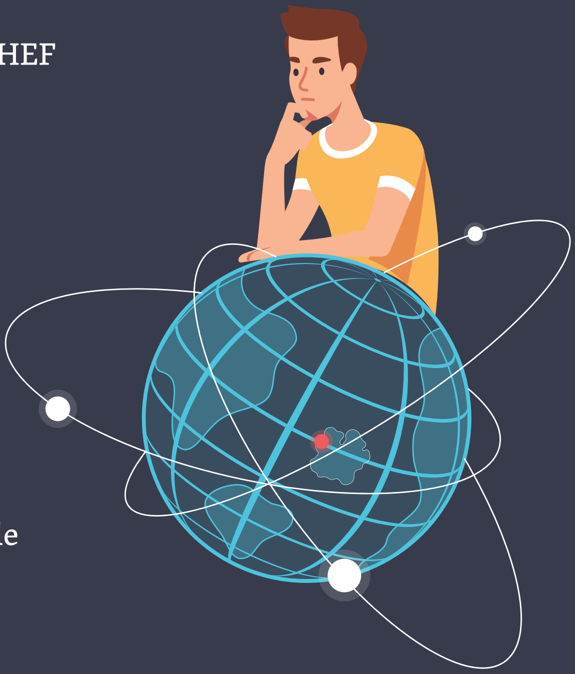
- Deploy LDAP Authentication
- WPA2, WPA3 and WiFI 6 Protocols
- Airmon, Aireplay, Aircrack; Airgraph and Airserve
- Cracking Wi-Fi Passwords Using Airerack-NG
- Firewalls, URL Filtering and Unified Threat Management
- Deploy Web Application Firewalls
- Stateful Packet Inspection, IPFire, pfSense, Untangle
- Intrusion Detection Firewalls, Smoothwall Iptables and nftables
- Cloudflare WAF, Securi and Incapsula
- ManagEngine Firewall Analyzer
- AWS WAF Firewall, AWS Shield DDOS Protection
- Microsoft End-Point Protection and EDR Response
- Microsoft Azure Security Center
- HTTP Tunneling, SSH Tunneling and ICMP Tunneling
- SNORT IDS, SAGAN, and BRO Intrusion Detection System
- OSSEC IDS, BRO Scripts and AIDE Tools
- Elastic Seatch, Logstash and Kibana
- Threat Hunting With Microsoft Azure Sentinel
- Cisco Firepower, Tripwire and Tipping Point
- Social Engineering Toolkit

ROCHESTON®

- Create Trojan Backdoors with MSVENOM
- Privilege Escalation With Metasploit Framework
- Credential Harvesting Attack With Cobalt Strike
- Public Key and Hashing Algorithms
- PKI and Encryption Techniques
- RSA and Eliptic Curve Cryptography
- NIST Key Size Recommendations
- SSL and Let's Encrypt Services
- PEM Passphrase Cracker
- Analyze RunningMalware Through Anti-Virus Programs
- WhatApp End-2-End Encryption
- VirusTotal, Sandboxing Yara Tool
- Malware Analysis Using Cuckoo
- IDA Disassembler and Debugger
- IOT and CTIA Lab Tests
- IoT products on which the Code of Practice is applicable
- IoT Device Identity Security
- QEMU, KVM and ZEN Hypervisor
- GNOME Boxes, Multipass and LXD Hypervisor
- Data Centers Using OpenNebula

ROCHESTON®

- Deployment Orchestration Using Ansible and CHEF
- Rooting with Android Devices
- Vagrant VM Management and Microsoft WSL
- Android Hacking With Metasploit
- Genymotion Android Emulator
- Develoop APK Using Android Studio
- Termux and Deploy GPS Tracker On Android
- Blockchain and Crypto Currencies
- Develop Smart Contracts Using Ethereum
- Write Crypto Applications in Solidity and Truffle
- Python, Perl, Ruby Rails and Bash Scripting



# RCCE Detailed Course Objectives

**Module 1:** Cybersecurity Threats, Attacks and Defenses

**Module 2:** Information Gathering and Network Scanning

**Module 3:** Cyber Vulnerabilities

**Module 4:** Web Application Attacks

**Module 5:** Web shells, Spywares and Backdoors

**Module 6:** Denial of Service Attacks

**Module 7:** Packet Sniffers and Network Analyzers

**Module 8:** Password Cracking

**Module 9:** Wireless Hacking

**Module 10:** Firewalls and IDS

**Module 11:** Hacking Frameworks

**Module 12:** Cryptography

**Module 13:** Malware Analysis

ROCHESTON®

**Module 14:** Cybersecurity Certification Test Plan for IoT Devices

**Module 15:** Virtualization with QEMU and Private Cloud

**Module 16:** Android Hacking

**Module 17:** Blockchain and Cryptocurrency

**Module 18:** Quantum Computing

**Module 19:** Cybersecurity Policies and Governance

**Module 20:** Risk Assessment

**Module 21:** Risk Management

**Module 22:** Security Incidence Response and Recovery Plan

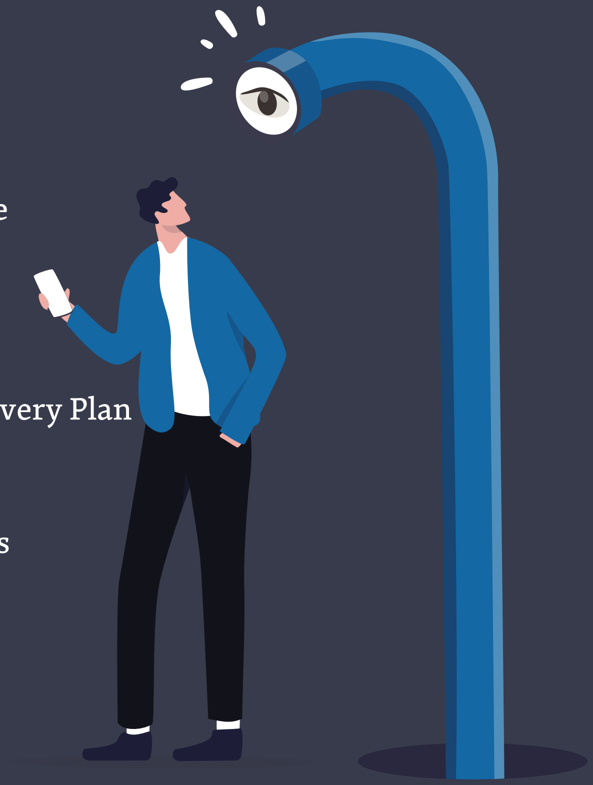
**Module 23:** DevSecOps

**Module 24:** Patch Management and Cloud Backups

**Module 25:** Securing Cloud Networks

**Module 26:** Rocheston Cybersecurity Framework

**Module 27:** Zero-Trust Architecture



ROCHESTON®

RC
CE

Cybersecurity Engineer

MODULES

https://www.rocheston.com/rcce/

ROCHESTON®