

RCCE® Certification Program Guide


ROCHESTON®
Signed by Haja
RCCE HACKER
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.

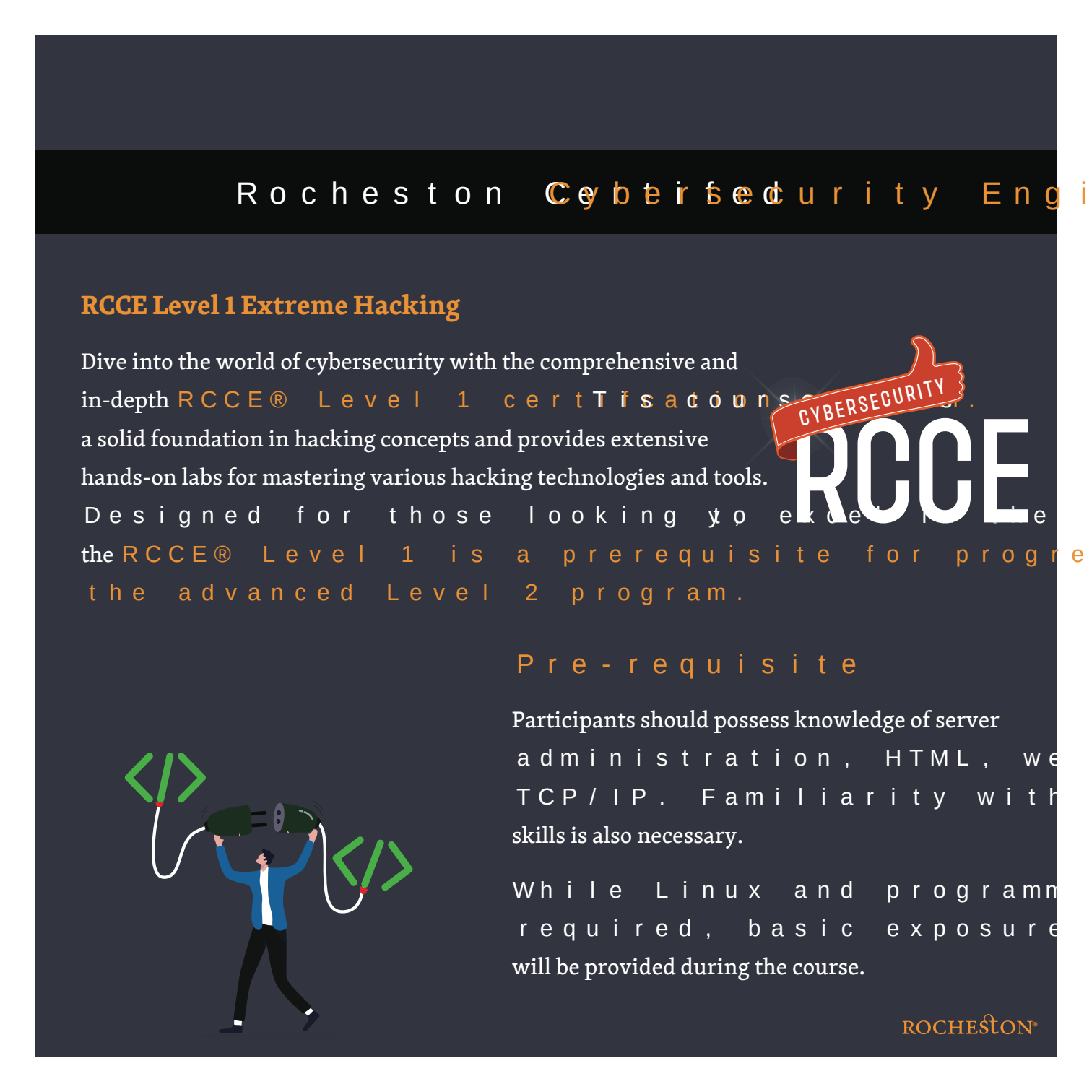
The team at Rocheston consists of young, liberal, innovative and forward-thinking individuals **who want to make a difference and change the world. At its core, Rocheston is a next-generation innovation company**, with cutting-edge research and development in emerging technologies such as Cybersecurity,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



Rocheston Cybersecurity Engi

RCCE Level 1 Extreme Hacking

Dive into the world of cybersecurity with the comprehensive and in-depth RCCE® Level 1 certification course. 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 elevate their cybersecurity skills, 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 programming skills is also necessary.

While Linux and programming skills are required, basic exposure to these areas will be provided during the course.


CRITICAL ERROR

Hands-On Labs

The Rocheston Certified Cybersecurity Engineer program designed to equip aspiring cybersecurity professionals with the knowledge required to defend against modern cyber threats. Central to the 6CCE course is the hands-on practical application in using cutting-edge cybersecurity tools.

These labs are powered by Rocheston Rose Cybersecurity OS. This specialized Linux-based OS has been meticulously curated to include over 1.5 terabytes of cybersecurity tools, amounting to over 1,500 hacking tools.



ROCHESTON®

Hue hands-on labs in the RCCE which means students can access and complete them using g ian swteabl lb raonwys so ìware or hardware, making iotr isntcurdeednitbslyt c their skills from anywhere, at any time.

Hue labs cover a Uide range of tapiics tanstitreg vulnerability assessment to neitUotruldesnetcsurwiit y through real_world scenariose iamdkncdwalledgneea hone their skills in a safe, controlled en

Penetration 7 tuedetnitsgdwill learn how tosidena target system, using a range of tools and unauthorized access and maintain control.

:ulnerability 7 tusdeentssmewitdl practice identriif Tulnerabilities in a system, using Tarious methodologies to eTaluate the risk and rec remediation measures.

2etUorl 7 tudentsd will gain hands_on exper Tarious threats, including cnfguring frew systems, and :P2s, as well ass monitoring n of malicious actiTity.

ROCHESTON®

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 identifcation, containment, as well as the eradication and restoration of afected systems.



ROCHESTON®



Course Structure

- The **RCCE® Level 1 is a 5-day intensive program**, running from 9 AM to 5 PM.
- The course is exclusively based on cybersecurity. With the **RCCE® Level 1 offers an unparalleled depth in cybersecurity.**
- Blended learning is an educational approach that combines traditional face-to-face classroom methods to create a comprehensive learning experience.
- This approach leverages digital tools such as online resources, virtual classrooms, and interactive modules.
- The primary goal of blended learning is to enhance learning outcomes by providing a flexible and engaging learning experience by catering to different learning styles and preferences.



ROCHESTON®



RCCE Blended Learning

In the context of the

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



Classroom based learning: Tis component inTolTes direct instructor and participantsseint ianphysticaallc feedback, group discussions,ntasndc ahnanadssk_oqnue doubts, and engage in collabdoraasteidTel eparrombilnegr sense of community among learnders, which e commitment to the course.

Self-study: This component enables participants to engage in additional online resources, such as study guides, practice exercises, and supplementary course material as often as needed. This allows participants to reinforce their understanding of the subject matter at their own pace, ensuring that those who require more time to grasp certain concepts can do so without feeling rushed.

Practical assignments and exercises: These activities help participants apply the knowledge gained in the classroom to real-world scenarios. Hands-on exercises or simulations that require learners to analyze data, identify patterns, and respond to cybersecurity incidents. Practical assignments encourage participants to develop critical thinking and problem-solving skills.

Assessments and evaluations: Throughout the course, participants' understanding of the material is regularly evaluated. Assessments can take various forms, such as quizzes, exams, or practical assessments. These assessments help both the instructor and participants identify areas that need improvement.

By incorporating these different components, the 6CC)z LeTel y course ensures a comprehensive approach to cybersecurity education. This approach enables learners to develop a well-rounded understanding of the subject matter relevant to the industry.



RCCE Exam

The ANAB-accredited RCCE® Level 1 exam is available on the last day of the course. Successful completion of the exam validates existing knowledge and skills, setting you apart from your peers.

Unlock your potential in cybersecurity engineering with the RCCE® Level 1 program and become a sought-after professional in the field. Rochester has reinvented hacker-themed learning to be engaging,







What You Will Learn?

Te 6CC) Cybersecurity trainingdpr ogram, ech
and frameworks. Tis course isp ct fo cused

Hue folloUing subHects are addressed in the

- :ulnerability Management
- Penetration Testing
- >ero_Trust Model
- 5uantum Computing
- Cyberthreat Intelligence
- Monitor 2etwork Tr
- Password and Creden ial Management
- 7ecure WiFi Deploym ts
-)ncryption and Cry ogr
- 7cams and Phishing %ttac
- Malware %nalysis a d 6esearch
- Hack %ndroid and i37 DeTices
- Patch Management
- %rtifcial 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
- 6isk and Treat %ssessm
- 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
- D27, 7poofng and Website M roring
- 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
- 73CŻ Dashboards &uild Treat I t tack
- 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 7ource Code 9sing Microsoì %pp In
- Network Socket Programming Using NodeJS
- Modern Web Application Architectures
- Dfnity Distributed Internet Computer
- Program Microsoì 75L 7erTer D abase
- Manage LD%P 7erTers 9sing %P
- Manage CM7 Wordpress, Mag p , 3pe
- Detect Vulnerable Web Applications
- Build Websites Using Jekyll
- Deploy PriTate Clouds
- Deploy Load &alancers 9s
- Manage File 7ynchroniXat o 7erTer
- 7poofng, &otnets, %PT, Cache Poisoning %n
- Role Based Access Controls
- Cross-Site Request Forgery And MiTM Attacks
- Cookies And Session Management
- DeT7ec3ps Ci/cd Pipelines
- 7DLC %nd Deïelopment Methodologies
- File Inclusion Attacks And Code 3bfuscation



- Trap Hackers Using Honeypots
- Sonarqube Source Code Analyzer
- Cybersecurity +amifcation
- 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 :irtual Machines in %Xure
- Face Detection 9sing Micr tiTe
- Face Detection Using Amazon Rekognition
- Mitre Attack Framework And Methodologies
- Deploy PHP Webshells And Backdoors
- Deploy Wordpress Fake Plugins
- %nalyXe Treat :ectors and % tors
- Deplay Phishing %ttacks %nd 2 7poofng
- Run Phishing Campaigns Using Frameworks
- Launch Secure Tunnels And Bypass Firewalls
- Deploy &ackdoor Payloads 9si g 27 Traæc
- F%T 6at,)Tilosx %nd DrooIT r Hans
- How To Hack Passwords With 2FA Authentication



ROCHESTON®

- 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
- DD37 %ttacks, IP 7poofng %nd &otnets
- Tor Circuits RedEye and UFONET
- HTTP Flooding, 7=2 Flooding %nd D27 %mplif
- Cloudêare +lobal 2etwork 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 7tuǽng
-)_mail HiHacking, Wi_Fi 7niǽng and 7teali
- Brute-Force Attacks and Cracking Online Passwords
- Cracking Encryption Keys, CRC and Checksum
- Distributed Password Cracking 9sing Hydra
- +oogle Captcha and 3%9TH 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 9nified Treat Management
- Deploy Web Application Firewalls
- Stateful Packet Inspection, IPFire, pfSense, Untangle
- Intrusion Detection Firewalls, 7moothwall Iptables and nìaI
- Cloudêare W% Encapsula 7ecuri and
- Manag)ngine Firewall %nalyXer
- AWS WAF Firewall, AWS Shield DDOS Protection
- Microsoì)nd_Pa d t)D6 6 es t
- Microsoì %Xure 7ecurity Ce e
- HTTP Tunneling, SSH Tunneling and ICMP Tunneling
- SNORT IDS, SAGAN, and BRO Intrusion Detection System
- 377)C ID7, &63 7cript
-)lastic 7eatch, Logs
- Treat Hunting With Microsoì %Xure 7entinel
- Cisco Firepower, Tripwire and Tipping Point
- 7ocial)ngineering Toolkit



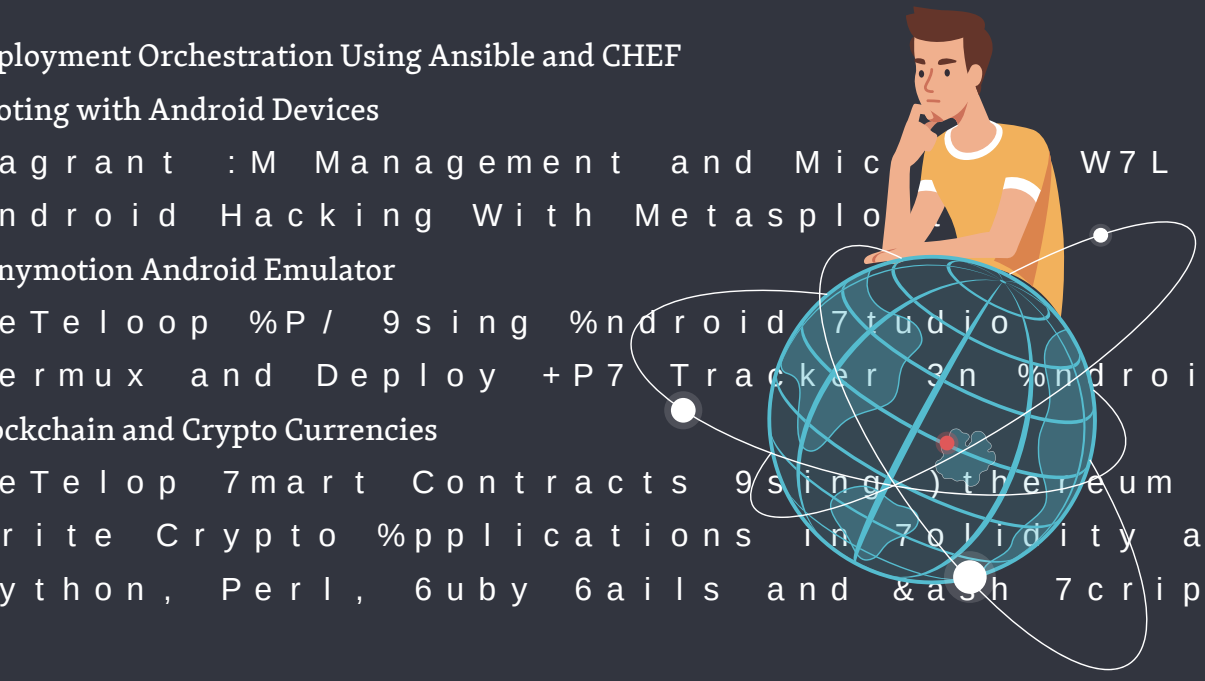
ROCHESTON®

- 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
  T r o u g h %n t i _ : i r u s
- W h a t %p p) n d _ ƶ _) n
- 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
- :agrant :M Management and Mic W7L
- %ndroid Hacking With Metasplo
- Genymotion Android Emulator
- DeTeloop %P/ 9sing %ndroid 7tudio
- Termux and Deploy +P7 Tracker 3n %ndroid
- Blockchain and Crypto Currencies
- DeTelop 7mart Contracts 9sing)thereum
- Write Crypto %pplications in 7olidity and
- Python, Perl, 6uby 6ails and &ash 7cripti





ROCHESTON®



RCCE Detailed Course Objectives

1. Cybersecurity Treats, %ttacks, and Defens
2. 6econnaissance, ML and % tifcial Intellig
3. Cyber :ulnerabilities
4. Web %pplication %ttacks C ctiTes
5. Web 7hells, 7pywares, an kdo
6. Denial of 7erTice %tta
7. Log Management and 2etwor al
8. Identity and %ccess Manage
9. Wireless Hacking
10. Firewalls and ID7
11. Hacking Frameworks
12. Cryptography
13. Malware %nalysis



ROCHESTON®

ƴƷ. Cybersecurity Certifcation Test Plan

ƴƐ. :irtualiXation with 5)M9 and PriTate

ƴƐ. %ndroid Hacking

ƴƷ. &lockchain and Cryptocu

ƴƲ. 5uantum Computing

ƴƵ. Cybersecurity Policie and +oTe nance

ƲƳ. 6isk %ssessment

Ʋƴ. 6isk Management

ƲƲ. 7ecurity Incidence 6es e and ecoTe

ƲƷ. Cloud 7ecurity

ƲƸ. DeTsecops

ƲƐ. >ero_Trust %rchitectur

ƲƐ. Patch management




RC
CE
Cybersecurity Engineer




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