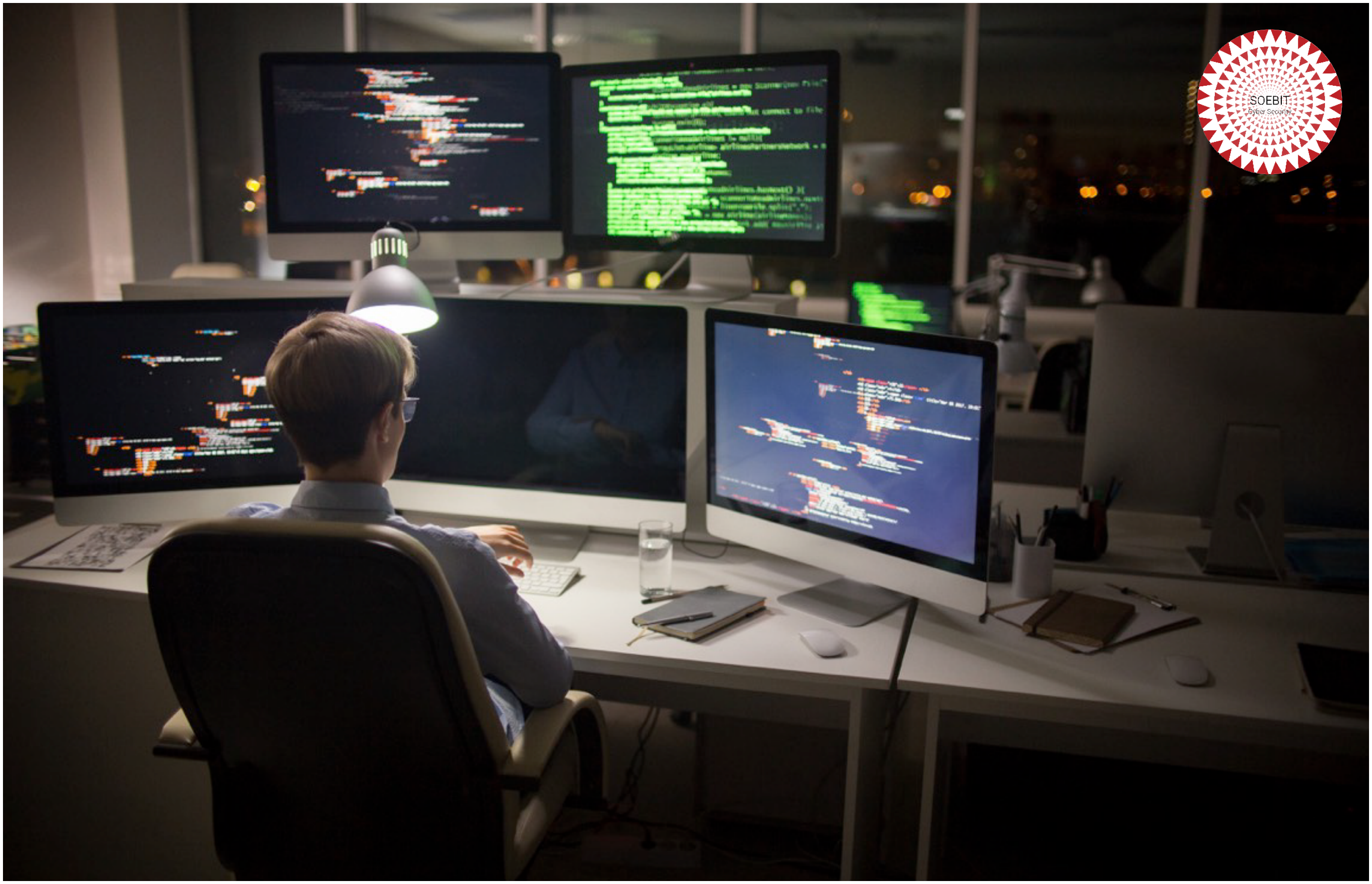

# ROCHESTON® CERTIFIED RED/BLUE PENTESTER

*Certified by Rocheston®*

## RCPT® Certification Program Guide

ROCHESTON

NEW YORK

DISTINGUISHED

# 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 Red/Blue Pentester (RCPT)

On successful completion of the **Rocheston Certified Cybersecurity Engineer (RCCE) level 2 course, you will be eligible to be certified as a Rocheston Certified Red/Blue RenTester (RCPT).** The RCPT program will teach you the methodologies, tools and exclusive techniques. The program will focus on hands-on attack-focussed education, which gives a keen insight into defensive, incident response processes, forensic and vulnerability assessment.

You will learn to test and improve your security in a network with extreme hacking tools, gather intelligence using reconnaissance tools and protect against privilege escalation to prevent intrusions. Through Red and Blue team Pentesting, you will learn to test security of systems through manual and tool-based testing to detect and fix unknown vulnerabilities without exposing sensitive assets.

ROCHESTON® CERTIFIED
RED/BLUE PENTESTER

ROCHESTON®

```
        fetch(`${API_URL}
            .then(functio
                if (respo
                    throw
                }
                return re
            })
            .then(data =>
                this.setS
                    quest
                    isLo
                });
            });
    }

    componentWillReceive
        console.log(next
    }

    shouldComponentUpdat
        console.log('Sho
        if (
            (
                nextStat
                && nextS
                && nextS
            ) ||
            (
                nextSta
                && this
```

# Target **Audience**

There is a growing need for an equally sophisticated cybersecurity framework with the increased dependence on interconnected cloud technologies.

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

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

# Eligibility

A Bachelor’s degree with one year of professional experience or credential in computer science, engineering, mathematics, or other information technology related fields. You will need basic hacking, networking, system administration, and Linux skills.

### What the course will consist of:

- A 5-day Training Program
- Time: 9:30 AM – 6 PM
- The provision of an active web portal
- Seminars conducted by qualified engineers
- Best in-class environment

### Cost

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

**Note:** If you don’t have basic hacking skills you can attend Rocheston’s Extreme Hacking Level 1 Program (which is included in this course).

# RCPT **Exam**

- Exam can be taken on Rocheston Cyberclass or Pearson VUE testing platform.
- Multiple Choice Objective Questions
- Total count - approximately 90 questions for each exam
- Pass Percentage: 72%
- Retake Policy - You may retake the exam any time on an additional fee. For further details contact the exam coordinator.

# The Cyberclass Web Portal

The access to an online e-learning platform will be given to attendants on registration. It will contain a series of study videos, pre-recorded lectures, white papers, educational animations and power point presentations. The web portal can be used to catch up on a missed session or to view an attended session again.

**http://cyberclass.rocheston.com**

# Course Completion

- On completing the course and successfully passing the exam, the candidate will be provided with an RCPT certification.
- Candidates are free to use the logo as per the Terms & Conditions as a Rocheston Certified Professional.
- The candidate will also receive a Welcome Kit and login information to access the Members’ Portal.
- The Members’ Portal is an online forum for certified RCPTs to interact.
- The certification is valid for two years and it can be renewed online.
- Contact the course coordinator for any enquiries about the renewal fee or downloading of the updated course material.

## Course Objectives

### In the RCPT program you will learn to:

- RCCE Level 2 imparts specialist knowledge on persistent privacy problems, IoT vulnerabilities, open source intelligence, sophisticated stealth tools in the Dark web and other specialist concepts.
  The RCPT program will delve into the methods and standards of penetration testing in over 80 frameworks.
- Simulate software-defined network architecture that centrally map out and control network pathways and devices
- Red team strategies for response readiness, safeguard data, and blue team strategies for securing and providing internal protection against external attacks.
- Scan and test multiple networks on machines and to deploy specific operations on running programs
- Understand Powershell automated framework and different software methodologies for business environments.
- Analyze and select the best security controls and protection mechanisms in a database.

- Understanding and implementing various protocols such as Lightweight Directory Access protocol (LDAP) and authentication protocol Kerberos.
- Utilize directory service and active directory attack techniques with dumping memory.
- Create a Docker environment and test with virtualization method in pen testing lab.
- Protect yourself from remote exploits by testing for vulnerabilities within your existing devices and infrastructure.

# Course Outline

**Module 1:** Penetration Testing Methodologies

**Module 2:** Penetration Testing Rules of Engagement

**Module 3:** Penetration Testing Code of Conduct

**Module 4:** Penetration Testing Legal Agreements and Jail Free Card

**Module 5:** Penetration Testing Web Servers

**Module 6:** Penetration Testing Firewalls

**Module 7:** Penetration Testing Intrusion Detection Systems

**Module 8:** Penetration Testing Intrusion Prevention Systems

**Module 9:** Penetration Testing Logging Systems

**Module 10:** Penetration Testing Databases

**Module 11:** Penetration Testing Individual Servers

**Module 12:** Penetration Testing RDP

**Module 13:** Penetration Testing SSH

**Module 14:** Penetration Testing Apache2

**Module 15:** Penetration Testing Cloud Networks

**Module 16:** Penetration Testing Linux Kernel

**Module 17:** Penetration Testing Windows 2019 Servers

**Module 18:** Penetration Testing Windows 10 Machines

**Module 19:** Penetration Testing MacOS

**Module 20:** Penetration Testing iOS and Android Devices

**Module 21:** Penetration Testing Email Servers

**Module 22:** Penetration Testing Webshells and Backdoors

**Module 23:** Penetration Testing Social Engineering

**Module 24:** Penetration Testing Phishing Attacks

**Module 25:** Penetration Testing Ransomware Attacks

**Module 26:** Penetration Testing DNS Systems

**Module 27:** Penetration Testing Encryption

**Module 28:** Penetration Testing VPN’s

**Module 29:** Penetration Testing Windows Domain Controllers

**Module 30:** Penetration Testing Network Sharing

**Module 31:** Penetration Testing Internal Company Networks

**Module 32:** Penetration Testing Intranet

**Module 33:** Penetration Testing Node Points

**Module 34:** Penetration Testing Routers

**Module 35:**Penetration Testing Network Endpoints

**Module 36:** Penetration Testing Leased Lines

**Module 37:** Penetration Testing Ethernet and Data Cables

**Module 38:** Penetration Testing Photocopiers

**Module 39:** Penetration Testing Fax Machines

**Module 40:** Penetration Testing Video Conferencing Systems

**Module 41:** Penetration Testing Supply Chain Attacks

**Module 42:** Penetration Testing SIEM

**Module 43:** Penetration Testing User Account Management

**Module 44:** Penetration Testing Data Leakage Protection

**Module 45:** Penetration Testing Password Authentication Systems

**Module 46:** Penetration Testing Biometric Tokens

**Module 47:** Penetration Testing Access Cards

**Module 48:** Penetration Testing 2FA Systems

**Module 49:** Penetration Testing Mobile Phones

**Module 50:** Penetration Testing Mobile Apps

**Module 51:** Penetration Testing Laptops

**Module 52:** Penetration Testing Televisions

**Module 53:** Penetration Testing IoT Devices

**Module 54:** Penetration Testing Smart Watches

**Module 55:** Penetration Testing Biometric Devices

**Module 56:** Penetration Testing Health Wearables

**Module 57:** Penetration Testing Medical Equipment

**Module 58:** Penetration Testing Home Networks

**Module 59:** Penetration Testing Connected Cars

**Module 60:** Penetration Testing Third Party Contractors

**Module 61:** Penetration Testing Alexa, Google Home, Apple Homepod

**Module 62:** Penetration Testing Chromecast, Apple TV, Amazon Firestick

**Module 63:** Penetration Testing Wi-fi And Bluetooth Devices

**Module 64:** Penetration Testing Telecom Networks

**Module 65:**. Penetration Testing Physical Networks

**Module 66:** Penetration Testing Doors, Windows and Ventilation Ducts

**Module 67:** Penetration Testing Surveillance Systems

**Module 68:** Penetration Testing Backup Tapes

**Module 69:** Penetration Testing End Point Security

**Module 70:** Penetration Testing Fire Alarm Systems

**Module 71:** Penetration Testing VOIP Systems

**Module 72:** Penetration Testing Office Phone Systems

**Module 73:** Penetration Testing Power Backup Systems

**Module 74:** Penetration Testing Spy Systems

**Module 75:** Penetration Testing Anti-Virus Systems

**Module 76:** Penetration Testing Whatsapp, Slack, Skype and Messenger Services

**Module 77:** Penetration Testing Content Management Systems

**Module 78:** Penetration Testing Patch Management Systems

**Module 79:** Penetration Testing Vulnerability Management

**Module 80:** Penetration Testing Assessments

**Module 81:** Penetration Testing Report Writing and Submission

https://www.rocheston.com

ROCHESTON®

https://www.facebook.com/Rocheston/

https://www.linkedin.com/company/rocheston-accreditation-institute/

https://twitter.com/rocheston