

Rocheston Certified Cybersecurity Engineer Training and Certification

Course Description & Overview

SecureNinja's Rocheston Certified Cybersecurity Engineer (RCCE) certification training offers an immersive, hands-on experience designed to equip participants with the skills needed to defend modern networks, systems, and applications. This advanced program goes beyond traditional ethical hacking by teaching both offensive and defensive cybersecurity methodologies, with a strong emphasis on real-world application.

The RCCE course is built for professionals who want to master cybersecurity from the ground up using powerful tools, scripts, and techniques. From penetration testing and malware analysis to zero trust architecture and AI-driven attacks, learners gain the technical expertise to detect, mitigate, and prevent cyber threats. Training is delivered using Rocheston's customizable Cyberclass Lab platform, enabling secure, cloud-based practice environments with over 1,000 hacking tools at your fingertips.

Why Choose RCCE

- Complete Cybersecurity Toolkit: Gain mastery in Linux, Python, penetration testing, red teaming, cryptography, and more.
- Hands-On Cloud Labs: Train in a browser-based virtual lab preloaded with real-world tools and hacking environments.
- Cutting-Edge Curriculum: Learn AI hacking, IoT security, malware development, zero trust, and cybersecurity automation.
- Global Recognition: RCCE is respected worldwide and used in enterprise, government, and academic cybersecurity training.

Topics Covered

- Linux Security and Command-Line Tools: Master Bash scripting, kernel management, and permission models.
- Python Programming: Write offensive and defensive cybersecurity automation scripts.
- Penetration Testing and Red Teaming: Execute recon, exploit, and post-exploitation phases using tools like Metasploit.
- Malware Analysis and Reverse Engineering: Understand ransomware, Trojans, keyloggers, and obfuscation techniques.
- IoT and SCADA Security: Learn how to secure embedded devices and industrial control systems.
- AI and Machine Learning Hacking: Explore adversarial AI attacks and build AI-enhanced defense strategies.
- Cloud and Zero Trust Security: Secure AWS, Azure, and hybrid environments with microsegmentation and identity controls.

Who is it for

- Penetration Testers: Professionals seeking deep technical knowledge and modern

toolchains.

- Security Engineers: Those managing enterprise security infrastructure and incident response.
- Red Team/Blue Team Members: Offensive and defensive teams engaged in real-world cyber operations.
- IT Professionals: Those transitioning into cybersecurity-focused roles in infrastructure or cloud.

Who Would Benefit

- Cybersecurity Students: Learners building job-ready skills for a career in cyber defense and offense.
- Security Consultants: Experts seeking certification to demonstrate high-level technical ability.
- Government and Defense Technologists: Professionals supporting mission-critical cybersecurity programs.

Prerequisites

A solid understanding of networking fundamentals, operating systems, and basic scripting is recommended. Prior cybersecurity experience is helpful but not required.

Course Outline

1. Linux and Scripting for Cybersecurity

- Linux administration, command-line tools, kernel configuration, and Bash scripting.

2. Python for Security Engineers

- Writing automation tools, payloads, and log analysis scripts in Python.

3. Penetration Testing

- Footprinting, scanning, exploitation, and maintaining access with Metasploit and Nmap.

4. Malware and Exploit Development

- Analyzing malware samples, obfuscation techniques, and shellcode injection.

5. IoT, AI, and Cloud Security

- Securing IoT devices, machine learning models, AWS/Azure environments, and serverless apps.

Course Length

- 5 Days
- 40 Hours

Exam Details

- Number of Questions: 100
- Question Types: Multiple-choice and practical application
- Duration: 2 Hours
- Passing Score: 62%

The Rochester Certified Cybersecurity Engineer (RCCE) certification empowers professionals with advanced, hands-on skills to secure networks, applications, and cloud environments. It's ideal for those seeking a globally respected credential that reflects real-world expertise and modern cybersecurity proficiency.