

ROCHESTON® CERTIFIED
CYBERSECURITY ENGINEER

RC
CE

Cybersecurity Engineer

Level
2



Silotech
Academy

RCCE® Certification Program Guide
<https://www.silotech-academy.com/rocheston>

Why You Need to **Attend RCCE Training?**

The **Rocheston Certified Cybersecurity Engineer (RCCE)** training is a prestigious and advanced certification program designed for professionals seeking to excel in the cybersecurity industry.

This comprehensive training program equips participants with the necessary skills, knowledge, and hands-on experience to tackle complex cybersecurity challenges and vulnerabilities.



**Stand out from the crowd
Be different**



As an **RCCE**, individuals set themselves apart from their peers within the cybersecurity community due to the highly respected nature of the certification.

The ANSI accredited **RCCE certification** is globally recognized, opening up career opportunities across the world and within multinational organizations.



Not only does the **RCCE training program** enhance career prospects, but it also leads to **high earning potential**, with cybersecurity engineers being among the highest-paid professionals in the sector.

By becoming an RCCE, individuals invest in their future career success and long-term growth within the cybersecurity field.

DoD 8140 **Approved**

The **U.S. Government officially recognizes and approves Rochester Certified Cybersecurity Engineer (RCCE)** certification under Department of Defense DoD 8140 directive.

RCCE is approved under the Job roles:

- All-Source Analyst
- Warning Analyst
- Forensics Analyst
- Cyber Defense Forensics Analyst
- Cyber Operations Planner
- Systems Security Analyst,
- Cyber Defense Analyst
- Cyber Defense Incident Responder
- Vulnerability Assessment Analyst
- Secure Software Assessor
- Research & Development Specialist
- Program Manager
- IT Project Manager
- Product Support Manager
- IT Program Auditor



RCCE Level 2 Penetration Testing

The **RCCE Level 2 Rocheston Certified Cybersecurity Engineer (Penetration Testing) course** is an advanced, comprehensive, and highly specialized program that equips cybersecurity professionals with the knowledge and skills required to excel in penetration testing.

This course stands out for its extensive coverage of advanced penetrating testing techniques.



The Course is Divided into 4 Parts

The course is meticulously designed and divided into 4 parts to ensure maximum learning and practical exposure:

- 
1. Cyber Range Sphere
 2. ZombieCop.Run
 3. Vulnerability Vines
 4. JuggyBank Project
- 

Part 1: Cyber Range Exercises



Cyber Range Sphere

In this part, students engage in capture-the-flag-style exercises where they attack machines with varying vulnerabilities. **The cyber range comprises more than 100 machines with diverse vulnerability configurations.** This hands-on approach enables students to:

- Gain real-world experience in identifying and exploiting vulnerabilities
- Understand how attackers think and strategize
- Develop the ability to prioritize and remediate vulnerabilities effectively
- Enhance their problem-solving and critical thinking skills

Cyber Range Sphere



Part 2: **ZombieCop.Run**



ZombieCop.Run Red Team / Blue Team Exercises

This part involves students dividing into **red and blue teams and attacking more than 100 targets**. The benefits of conducting these exercises include:

Learning to collaborate and communicate effectively within a team. Understanding the defense strategies employed by the blue team. Gaining insights into the offensive tactics used by the red team. Developing a well-rounded understanding of both attack and defense methodologies.

Part 3: Vulnerability Vines



Rocheston's Vines is a full-scale vulnerability assessment and penetration testing tool that students will learn to implement within their organizations to secure their networks.

Vines covers a wide range of security aspects, such as DevSecOps, IAM, vulnerability scanning, cloud firewall, zero-trust, VPN, and more.

Students will receive in-depth training on how to use Vines effectively.

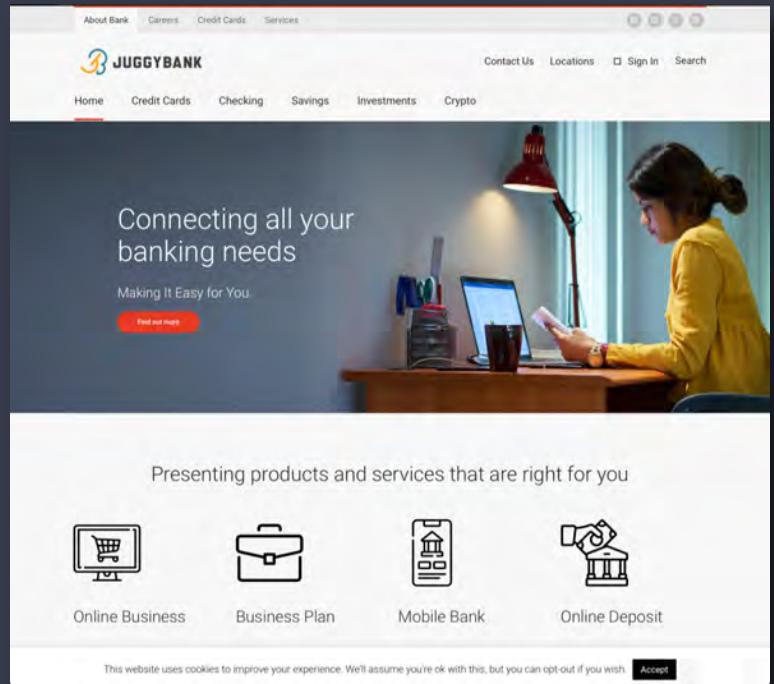
Part 4: JuggyBank Project

You will be intimately involved in a thorough penetration testing process for JuggyBank.

This real-world project is designed to deliver holistic understanding of **testing procedures, implementation of security measures, and subsequent defensive actions needed to secure JuggyBank.**

Each phase of this project, from execution to analysis, will enlighten you about the practical aspects of penetration testing in detail.

You will gain a realistic perspective of potential cybersecurity threats faced by banking institutions like JuggyBank.



What is **RCPT**?



The Rochester Certified Red/Blue Pentester (RCPT) certification is a significant part of the Rochester Certified Cybersecurity Engineer (RCCE) Level 2 program.

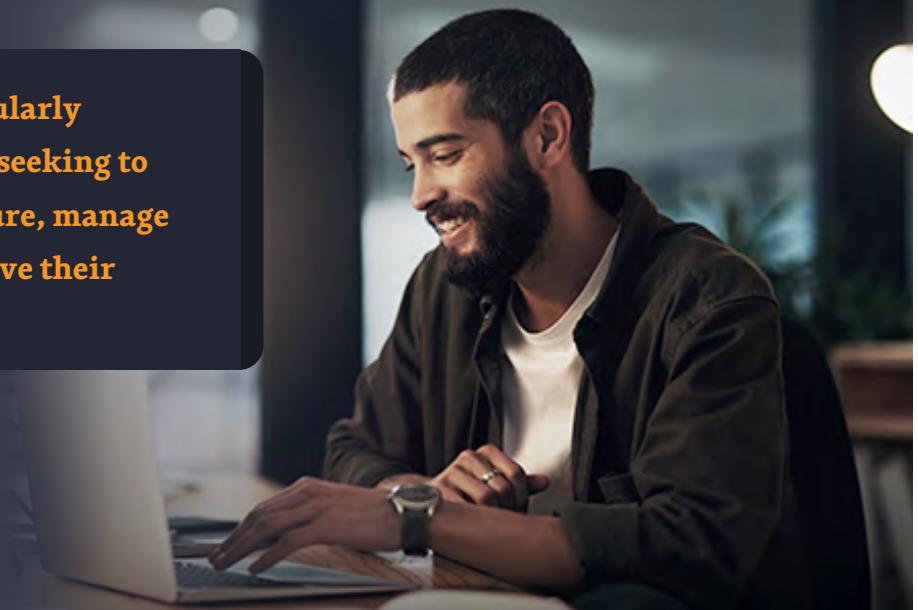
The **RCCE Level 2 program, incorporating RCPT**, aims to equip participants with an in-depth understanding of offensive and defensive cybersecurity strategies. The RCPT certification, in particular, has a strong emphasis on practical penetration testing techniques and methodologies.

RCPT Penetration Testing Framework

The **RCPT Framework touch on areas such as reconnaissance, scanning, gaining access, maintaining access, and covering tracks.** It also emphasizes on studying various penetration strategies, master hacking techniques, and become familiar with attack countermeasures in order to protect an organization's critical infrastructure.

Overall, the RCPT Framework strike a balance between aggressive red teaming and defensive blue teaming, making it an effective approach for comprehensive and robust penetration testing.

RCPT Framework are particularly beneficial for organizations seeking to evaluate their security posture, manage potential threats, and improve their overall defense strategies.



Rocheston Certified Red/Blue Pentester (RCPT) Framework

Module 1

Introduction to Penetration Testing

Module 2

Penetration Testing Methodologies

Module 3

Legal and Ethical Issues in Penetration Testing

Module 4

Rules of Engagement

Module 5

Network Penetration Testing

Module 6

Vulnerability Assessment and Exploitation

Module 7

Web Application Penetration Testing

Module 8

Wireless Network Penetration Testing

Module 9

Physical Penetration Testing

Module 10

Database Penetration Testing

Module 11

Source Code Penetration Testing

Module 12

Social Engineering in Penetration Testing

Module 13

Cyber Threat Intelligence in Penetration Testing

Module 14

Mobile and IoT Penetration Testing

Module 15

Cloud Penetration Testing

Module 16

Firewalls & IDS in Penetration Testing

Module 17

Report Writing in
Penetration Testing

Module 18

Active Directory (AD)
Penetration Testing

Module 19

Administrative
Interface Penetration
Testing

Module 20

Anti-Malware Efficacy
Penetration Testing

Module 21

Apache2 and nginx
Penetration Testing

Module 22

Multi-factor
authentication (MFA)
Penetration Testing

Module 23

Network Mapping
Penetration Testing

Module 24

Ongoing Tests
Penetration Testing

Module 25

OWASP Top 10
Penetration Testing

Module 26

Best Practices
Penetration Testing

Module 27

Password Strength
Penetration Testing

Module 28

Patch Management
Penetration Testing

Module 29

Penetration Testing
from Various Locations

Module 30

Phishing Attack
Simulation
Penetration Testing

Module 31

Post-Exploitation
Techniques

Module 32

Privilege Escalation
Penetration Testing

Module 33

Race Condition Bugs
Penetration Testing

Module 34

Ransomware Attacks
Penetration Testing

Module 35

Real-time Alerting
Penetration Testing

Module 36

Reconnaissance
Penetration Testing

Module 37

Red Teaming
Penetration Testing

Module 38

Regulatory
Compliance
Penetration Testing

Module 39

Remote Access
Penetration Testing

Module 40

Rogue Device
Detection
Penetration Testing

Module 41

Scan Open Ports
Penetration Testing

Module 42

Secure Token
Penetration Testing

Module 43

Security Policy
Compliance
Penetration Testing

Module 44

Security Tool
Efficacy
Penetration Testing

Module 45

Security Training
Efficacy
Penetration Testing

Module 46

Server
Misconfigurations
Penetration Testing

Module 47

Server Security
Headers Penetration
Testing

Module 48

Server-side Request
Forgery
Penetration Testing

Module 49

Session Hijacking
Penetration Testing

Module 50

Session Management
Penetration Testing

Module 51

Shadow IT Detection
Penetration Testing

Module 52

Social Media
Footprinting
Penetration Testing

Module 53

Spear Phishing
Penetration Testing

Module 54

SSL-TLS
Penetration Testing

Module 55

Wordpress
Penetration Testing

Module 56

Third Party and
Supplier
Penetration Testing

Module 57

Third-party Software
Penetration Testing

Module 58

Threat Hunting
Penetration Testing

Module 59

Token Permissions
Penetration Testing

Module 60

Unauthorized
Data Access
Penetration Testing

Module 61

URL Manipulation
Penetration Testing

Module 62

Use of Known
Vulnerabilities
Penetration Testing

Module 63

Version Detection
Penetration Testing

Module 64

Virtual
Machine Security
Penetration Testing

Module 65

VoIP
Penetration Testing

Module 66

VPN Security
Penetration Testing

Module 67

Vulnerabilities and
Exposures (CVE)
database
Penetration Testing

Module 68

Vulnerability
Analysis
Penetration Testing

Module 69

Web Services-
API Penetration Testing

Module 70

Work from home
Penetration Testing

Module 71

Zero Trust
Architecture
Penetration Testing

Module 72

Zero-day Exploit
Penetration Testing

Module 73

Mobile Application
Penetration Testing

Module 74

Man-in-the-Middle
(MITM) Attacks
Penetration Testing

Module 75

Malware Analysis and
Reverse Engineering

Module 76

Logs Auditing
Penetration Testing

Module 77

Logic
Penetration Testing

Module 78

Local Network
Access Control
Penetration Testing

Module 79

Load balancer
Penetration Testing

Module 80

Linux Servers
Penetration Testing

Module 81

IoT Device
Penetration Testing

Module 82

Intrusion Prevention
System (IPS)
Penetration Testing

Module 83

Insider Threat
Simulation
Penetration Testing

Module 84

Input Validation
Penetration Testing

Module 85

Infrastructure
Configuration Review
Penetration Testing

Module 86

Information
Disclosure
Penetration Testing

Module 87

Incident Response
Capability
Penetration Testing

Module 88

Human Interface
Device (HID) Attacks
Penetration Testing

Module 89

HTTP protocol verbs
Penetration Testing

Module 90

Firewall Configuration
Penetration Testing

Module 91

File Upload
Penetration Testing

Module 92

File system
permissions
Penetration Testing

Module 93

Encryption At
Rest & In Transit
Penetration Testing

Module 94

Embedded Device
Penetration Testing

Module 95

Email Phishing
Campaigns
Penetration Testing

Module 96

Email Configuration
Penetration Testing

Module 97

DNS Security
Penetration Testing

Module 98

DDoS Mitigation
Capability
Penetration Testing

Module 99

Database Security
Penetration Testing

Module 100

Cyberthreat
Intelligence
Penetration Testing

Module 101

Cryptography for
Penetration Testers

Module 102

Cross-Site Request
Forgery (CSRF) Attacks
Penetration Testing

Module 103

Cookie Security
Penetration Testing

Module 104

Content Management
System (CMS)
Penetration Testing

Module 105

Codebase Review
Penetration Testing

Module 106

Code Injection
Penetration Testing

Module 107

Cloud Storage
Penetration Testing

Module 108

Cloud Container
Penetration Testing

Module 109

Client-side Security
Controls
Penetration Testing

Module 110

Clickjacking
Penetration Testing

Module 111

Business Logic
Penetration Testing

Module 112

Brute Force Attacks
Penetration Testing

Module 113

Breach Readiness
Assessment
Penetration Testing

Module 114

Bot Detection
Penetration Testing

Module 115

Backup and Recovery
Penetration Testing

Module 116

Azure, AWS,
GC Penetration Testing

Module 117

Asset Discovery
Penetration Testing

Module 118

ARP Spoofing
Penetration Testing

Module 119

Application
Container
Penetration Testing

Module 120

Application
Behavior
Penetration Testing

Module 121

SSH
Penetration Testing

Module 122

WAF
Penetration Testing

Module 123

Blockchain
Penetration Testing

Module 124

DevSecOps in
Penetration Testing

Module 125

Identity and access
management (IAM)
Penetration Testing

Module 126

Ethics in
Penetration Testing

Module 127

Tools in
Penetration Testing

Module 128

POS Systems
Penetration Testing

Module 129

Advanced Persistent
Threat (APT)
Penetration Testing

Module 130

ATM
Penetration Testing

Module 131

RFID and Access
Control
Penetration Testing

Module 132

Endpoint
Penetration Testing

Module 133

Industrial Control
Systems (ICS) & SCADA
Penetration Testing

Module 134

Dark Web
Penetration Testing

Module 135

Quantum Computing
Penetration Testing

Module 136

AI and Machine
Learning Systems
Penetration Testing

Module 137

Big Data
Penetration Testing

Module 138

Biometric Systems
Penetration Testing

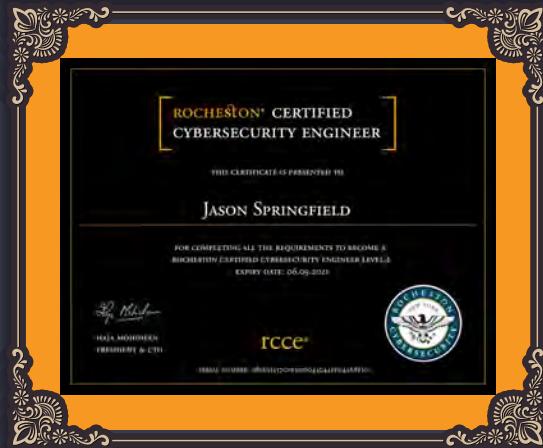
Module 139

Drone & Robotics
Penetration Testing

Module 140

Password Cracking
Penetration Testing

RCCE Level 2 Exam



The examination for the **RCCE Level 2** will be administered on the last day of the course.

Upon successful completion of this exam, participants will earn the highly regarded **RCCE and RCPT certifications**, distinguishing them from their colleagues.

You will
walk away



with
RCCE and RCPT
certifications.

RCPT Course Outline

- **Reconnaissance:** Includes collecting initial information about the target, typically via search engines, WHOIS, and DNS records.
- **Scan Open Ports:** Analyze open ports on the network.
- **Version Detection:** Understand the versions of web servers, operating systems any outward-facing software by network footprinting.
- **Network Mapping:** Use tools like Nmap to create a map of the network.
- **Vulnerability Analysis:** Perform a vulnerability analysis to identify potential points of exploitation.
- **Firewall Configuration Testing:** Checking the robustness of firewall rules and identifying misconfigurations.
- **Intrusion Detection/Prevention System Testing:** Evaluate the effectiveness of IDS/IPS.
- **Password Strength Testing:** Test the complexity and strength of passwords.
- **Password Cracking:** Use password cracking tools to identify weak and easily crack-able passwords.

- **Brute Force Attacks:** Try brute force attacks on login fields and other entry points.
- **Application Behavior:** Understand the behavior of applications under varied user inputs.
- **Input Validation:** Testing for weaknesses in input validation, such as cross-site scripting (XSS) or SQL injection vulnerabilities.
- **HTTP protocol verbs Testing:** Test to see if unsupported or potentially risky HTTP protocol verbs are in use.
- **URL Manipulation:** Manipulate URLs to bypass access controls or gain unauthorized access.
- **Cookie Security:** Evaluate the security measures in place for cookies.
- **Session Management:** Examine whether sessions are managed securely, including session timeouts and handling of concurrent logins.
- **Secure Token Testing:** Confirm that secure tokens are used and are handled correctly.
- **Phishing Attack Simulation:** Simulate phishing attacks to test response mechanisms and educate users.
- **Social Engineering:** Use social engineering techniques to identify vulnerabilities in human factors.
- **Malware Testing:** Test the protections against malicious software like viruses, worms, and Trojans.

- **Active Directory (AD) Testing:** Evaluate the security of AD configurations.
- **Wi-fi Network Security:** Assess the security of wireless networks and their configurations.
- **DDoS Mitigation Capability:** Test the system's ability to sustain a Distributed Denial of Service (DDoS) attack.
- **DNS Security:** Test the Domain Name System for cache poisoning or spoofing vulnerabilities.
- **Email Configuration:** Check the email configurations to ensure security settings like SPF, DKIM, and DMARC are in place.
- **VoIP Testing:** Voice over IP also needs to be tested for potential vulnerabilities.
- **SSL/TLS Testing:** Check the implementation of cryptography, deprecated protocols, weak ciphers, and certificate validity.
- **Third-party Software:** Any software from third parties or open-source libraries should be tested.
- **Intrusion Detection System (IDS):** Test and evaluate its capacity to detect malicious traffic.
- **Intrusion Prevention System (IPS):** Test and evaluate its capacity to prevent malicious traffic.

- **Patch Management Process:** Evaluate how patches are managed and how quickly they're implemented.
- **Backup and Recovery Test:** Validate the backup and recovery process of a company's data.
- **Physical Security Testing:** Evaluate the effectiveness of physical security controls if relevant to the pen test.
- **Cloud Environment:** Test security in cloud environments like AWS, Azure, or Google Cloud.
- **Database Security:** Check for SQL injection, misconfigurations, and exposure of sensitive data in any database used.
- **Remote Access Testing:** Assess the security of the Remote Desktop Protocol (RDP) or other remote access used.
- **Multi-factor authentication (MFA) Testing:** Understand how MFA is implemented and identify any weaknesses.
- **File system permissions:** Review file and directory permissions for any insecure settings.
- **Token Permissions:** Review user and application tokens for unnecessary permissions.
- **Logs Auditing:** Audit system, security and application logs to check for security incidents and anomalies.
- **Virtual Machine Security:** Test the security of virtual machines if utilized.

- **Web Services/API Testing:** Evaluate the security of any APIs or web services in use.
- **Mobile Application Testing:** Testing mobile apps, if relevant, for any inherent vulnerabilities.
- **Unauthorized Data Access:** Attempt to access sensitive or confidential data without appropriate permissions.
- **Administrative Interface Testing:** Check for vulnerabilities in admin interfaces.
- **IoT Device Testing:** Internet of Things devices, often overlooked, need proper pen testing too.
- **ARP Spoofing:** Test for man-in-the-middle attack vulnerabilities.
- **VPN Security:** Evaluate the security of Virtual Private Networks deployed in the organization.
- **Load balancer testing:** Test to confirm it correctly handles network traffic and ensures data availability and redundancy.
- **Content Management System (CMS) Testing:** Test the security of the CMS, a common target for attackers.
- **File Upload Testing:** Check that file upload features sanitize input and reject potential malicious files.

- **Logic Testing:** Make sure the application logic cannot be manipulated to achieve unauthorized access.
- **Session Hijacking:** MethodInvocation and testing of session management to identify weaknesses.
- **DOS and DDOS:** Test resilience against Denial of Service (DoS) or Distributed DoS attacks.
- **Business Logic Testing:** Examine business processes to detect any logical or technical frailties.
- **Privilege Escalation:** Try to gain higher permissions to access more resources.
- **Man-in-the-Middle (MITM) Attacks:** Test vulnerabilities to MITM attacks.
- **Code Injection:** Try injecting malicious code to exploit system or create unfavorable outcomes.
- **Information Disclosure:** Test if internal system information disclosure happens through error messages.
- **Embedded Device Testing:** If embedded or IoT devices are deployed, these need to also be pen tested.
- **Application Container Testing:** Check the security of application container environments like Docker.
- **Infrastructure Configuration Review:** Review security configurations of routers, switches, firewalls, etc.

- **Server Misconfigurations:** Identify any server misconfigurations that could potentially expose the network.
- **Clickjacking:** Test for vulnerabilities to clickjacking attacks.
- **Server Security Headers:** Check for appropriate implementation of HTTP security headers.
- **Server-side Request Forgery (SSRF) Attacks:** Test for vulnerabilities to SSRF attacks.
- **Race Condition Bugs:** Test to detect potential race condition bugs in code execution.
- **Client-side Security Controls:** Test all client-side security measures.
- **Cross-Site Request Forgery (CSRF) Attacks:** Test for vulnerabilities to CSRF attacks.
- **OWASP Top 10 & other Standard Framework Testing:** Test for vulnerabilities listed in the OWASP . Top 10 and other recognized security frameworks.
- **Insider Threat Simulation:** Simulate actions of malicious insiders to identify vulnerabilities.
- **Human Interface Device (HID) Attacks:** Test for potential HID attacks, such as BadUSB.
- **Regulatory Compliance Pen Testing:** Specialized tests to ensure compliance with regulations such as PCI DSS, HIPAA, GDPR.
- **Spear Phishing:** Test employee susceptibility to targeted spear phishing attacks.

- **Third Party and Supplier Security:** Test security preparedness of third parties and supply chain elements.
- **Cloud Storage Security:** Test the security of storage buckets like Amazon S3 or Azure Blob Storage.
- **Red Teaming:** Conduct complete cyber-attack simulations to evaluate organization's defense capability.
- **Zero-day Exploit Testing:** If zero-day exploits are discovered, understand their impact and mitigation.
- **Cloud Container Testing:** Test the security of containers in cloud services.
- **Shadow IT Detection:** Detect unmanaged systems or services within the network.
- **Breach Readiness Assessment:** Understand the readiness of the organization to handle a breach.
- **Social Media Footprinting:** Check for unintentionally revealed information on social media that could help attackers.
- **Security Policy Compliance:** Test to ensure adherence to organization's security policy.
- **Incident Response Capability:** Test the organization's readiness to respond to security incidents.

- **Security Training Efficacy:** Evaluate how effective the security awareness and training programs are within the organization.
- **Codebase Review:** Manually review the codebase for any bugs or oversights that automated tools missed.
- **Security Tool Efficacy:** Assess whether the security tools deployed by the organization are performing as expected.
- **Zero Trust Architecture Testing:** Evaluate the effectiveness of zero trust models if implemented.
- **Local Network Access Control:** Evaluate the controls in place for local network access.
- **Encryption At Rest & In Transit:** Test for proper implementation of encryption both for data at rest and in transit.
- **Cyber Threat Intelligence Integration:** Utilize cyber threat intelligence to add context and better identify potential threats.
- **Bot Detection:** Test if the system has adequate protection against bots.
- **Email Phishing Campaigns:** Test employees ability to recognize and avoid phishing scams.
- **Anti-Malware Efficacy:** Test if the deployed antivirus or antimalware solution is effective.
- **Real-time Alerting:** Test the incident alert mechanisms to ensure they are working properly.

- **Use of Known Vulnerabilities:** Utilize known vulnerabilities from repositories like the Common Vulnerabilities and Exposures (CVE) database.
- **Rogue Device Detection:** Test the organization's ability to detect unauthorized devices on the network.
- **Pen Testing from Various Locations:** Test the security measures from diverse geographical locations and IP addresses.
- **Threat Hunting:** Proactively identify whether there are any unknown threats lurking in the infrastructure.
- **Ongoing Tests:** Regular and scheduled penetration tests to account for new vulnerabilities and system changes.





 Silotech
Academy

<https://www.silotech-academy.com/rocheston>

ROCHESTON®