



CERTIFIED PENTESTING PROFESSIONAL PROGRAM

RC™ Ramaq
Chools
Consulting & Training

CONTENTS

1. Introduction to Pentesting Professional

2. Why Choose Chools?

3. Who Can Apply?

4. Program Overview

5. Objectives and Outcomes

6. Skills Learned

7. Job Positions and Opportunities

8. Key Industry Verticals

9. Program Outline

- Stage 1: Fundamentals of Penetration Testing
- Stage 2: Advanced Pentesting Techniques
- Stage 3: Practical Applications
- Stage 4: Capstone Project
- Elective Modules

10. Enrollment Information



INTRODUCTION TO PENTESTING PROFESSIONAL

Welcome, future penetration testing expert! This course teaches you how to perform penetration testing, which involves simulating cyberattacks on a system or network to identify and exploit security vulnerabilities. This course will teach you how to perform effective penetration testing in an enterprise network environment that must be attacked, exploited, evaded, and defended. You will also learn how to pen test IoT systems, OT systems, write your own exploits, build your own tools, conduct advanced binary exploitation, and more.





Why Choose Chools?

Numbers That Speak for Themselves:

- 10,000+ Successful Alumni: Join a network of impactful professionals.
- 95% Job Placement Rate: Secure your future with Chools' proven track record.
- 20+ Years of Excellence: Trust in a legacy of education and industry expertise.
- 200+ Industry Partnerships: Leverage our connections for real-world insights and opportunities.

What Sets Us Apart?

- **Expert Instructors:** Learn from industry veterans with hands-on experience.
- **Hybrid Learning Model:** Balance online flexibility with in-person engagement.
- **Comprehensive Curriculum:** Stay ahead with courses designed to meet market demands.
- **Community and Networking:** Be part of an active community of learners and professionals.

Who Can Apply?

Eligibility Criteria:

- A bachelor's degree in STEM.
- Prior knowledge of programming languages and computer networks may be helpful.





Ideal Candidates

- Professionals aiming to advance their careers in penetration testing and earn a globally recognized credential.

Program Overview

The Certified Pentesting Professional Program provides extensive education in penetration testing. Our curriculum ensures a comprehensive understanding through four progressive stages, combining theoretical knowledge with practical, hands-on experience.

Learning Mode:

- **Hybrid Learning Model:** Combines online learning with in-person sessions for flexibility and interactive engagement.
- **Interactive Sessions:** Includes live webinars, workshops, and Q&A forums with expert instructors and peers.
- **Self-paced Learning:** Access course materials anytime, allowing you to learn at your own pace.



Skills Learned

- **Penetration Testing Techniques:** Identifying and exploiting vulnerabilities.
- **Exploit Development:** Writing and using custom exploits.
- **Tool Building:** Creating your own security tools.
- **Advanced Binary Exploitation:** Conducting sophisticated exploits.
- **IoT and OT Penetration Testing:** Testing IoT and OT systems.
- **Network Security:** Understanding and securing network environments.
- **Incident Response:** Responding to security incidents.
- **Security Policies:** Developing and implementing security policies.

Job Positions and Opportunities

- **Career Paths:** Penetration Tester, Security Consultant, Security Analyst, IT Auditor, Systems Engineer, Security Architect.
- **Industry Demand:** High demand across various sectors, competitive salaries, and strong growth potential.

Key Industry Verticals

- **Skill Application Areas:** Finance, Healthcare, Technology, Government, Retail, Energy, Telecommunications, Manufacturing.

Curriculum Highlights

- **Fundamental Knowledge:** Core principles of penetration testing.
- **Advanced Techniques:** In-depth understanding of advanced pentesting tools.
- **Real-World Applications:** Practical projects and case studies to apply your learning.
- **Capstone Project:** A final project that integrates all your skills and knowledge, showcasing your proficiency in penetration testing.



Professional Development

- **Continuous Learning:** Stay updated with the latest trends and advancements in penetration testing.
- **Networking Opportunities:** Connect with industry experts, peers, and alumni to advance your career.
- **Ethical Considerations:** Learn about data ethics, privacy, and compliance to maintain the integrity of your practices.

Program Objectives

- Master technical skills in penetration testing.
- Implement advanced pentesting techniques and tools.
- Explore pentesting frameworks and best practices.
- Address real-world challenges in penetration testing.
- Understand ethical considerations in data governance.
- Foster continuous learning.
- Encourage teamwork and collaboration.
- Prepare for advanced roles in penetration testing.

Expected Outcomes

- Proficiency in penetration testing tools and techniques.
 - Practical experience through hands-on projects.
 - Strong analytical and problem-solving skills.
 - Application of ethical practices.
 - Innovation in penetration testing solutions.
- 



PROGRAM OUTLINE

Stage 1: Fundamentals of Penetration Testing

1. Introduction to Penetration Testing

- o Core principles, tools, and industry applications.

2. Network Security Basics

- o Understanding network environments and vulnerabilities.

3. Vulnerability Assessment

- o Identifying and assessing vulnerabilities.

4. Basic Exploits

- o Using pre-built exploits effectively.

Stage 2: Advanced Pentesting Techniques

5. Advanced Exploit Development

- o Writing and using custom exploits.

6. Tool Building for Pentesting

- o Creating your own security tools.

7. Binary Exploitation

- o Conducting advanced binary exploits.

8. IoT and OT System Testing

- o Testing IoT and OT systems for vulnerabilities.

Stage 3: Practical Applications

9. Practical Pentesting Projects

- o Developing and implementing penetration testing projects.

10. Security Operations Management

- o Managing security operations.

11. Data Analysis and Visualization

- o Analyzing security data and visualizing results.

12. Business Intelligence Applications

- o Using data for security decision making.

Stage 4: Capstone Project

13. Integration of Learned Skills

- o Apply tools and techniques to real-world security problems.

14. Advanced Pentesting Systems

- o Developing complex penetration testing systems.

15. Cloud Security Management

- o Securing cloud-based platforms.

16. AI for Security

- o Implementing AI solutions in security.



PROGRAM OUTLINE

Elective Modules

17. Data Ethics and Privacy

- o Ethical considerations, privacy laws, compliance strategies.

18. Predictive Analytics with Security Management

- o Building and validating predictive models.

19. AI for Security Management

- o Implementing AI solutions in security.

20. Advanced Data Warehousing Techniques

- o Optimizing data warehousing solutions.

21. Data-Driven Security Decision Making

- o Using data to inform and drive security strategies.

22. Cloud Security Solutions

- o Deploying security management systems on cloud platforms.

23. Security Project Management

- o Leading security projects, ensuring successful delivery.

24. Big Data Security

- o Securing data in big data environments.

25. IoT Security

- o Securing IoT devices and systems.

Enrollment Now Open!

Take the first step towards becoming a certified Penetration Testing Professional. Enroll in our program and enhance your career.