CERTIFIED NETWORK SECURITY PROFESSIONAL (CNSP) PROGRAM

Simple | Smart | Speed
CHOOLS

Email: info@choolsgroup.com **Phone:** +91 74067 33363 **Website:** chools.in

CONTENTS

INTRODUCTION TO CNSP

Welcome, future network security expert! The Certified Network Security Professional (CNSP) course teaches you the skills and knowledge required to secure networks and applications by deploying, managing, and monitoring network security products. A certified network security professional is someone who has successfully proven competence and credibility in network security. Topics covered include core security technologies, firewalls, email security, web security, VPNs, and more. To achieve this certification, you need to pass one core exam and one elective exam within two years. You also need to hold a current and valid CWNA credential

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 meet market demands.
- **Community and Networking:** Be part of an active community of learners and professionals.

Who Can Apply?

Eligibility Criteria:

- At least five years of paid, full-time experience in at least two of the eight ISC2 domains or four years of experience and a college degree.
- Good command of English.

Ideal Candidates:

- Professionals aiming ta advance their careers in network security and earn a globally recognized credential.

Program Overview

The Certified Network Security Professional (CNSP) Program provides an extensive education in network security. 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

- **Core Security Technologies:** Understanding fundamental security concepts.
- **Firewall Management:** Configuring and managing firewalls.
- **Email Security:** Securing email communications.
- **Web Security:** Protecting web applications.
- **VPN Management:** Setting up and managing VPNs.
- **Network Monitoring:** Monitoring and analyzing network traffic.
- **Incident Response:** Responding to security incidents.
- **Security Policies:** Developing and implementing security policies.

Job Positions and Opportunities

- **Career Paths:** Network Security Engineer, 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 network security.
- Advanced Techniques: In-depth understanding of advanced security 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 network security.

Professional Development:

- Continuous Learning: Stay updated with the latest trends and advancements in network security.
- 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 network security.
- Implement advanced security techniques and tools.
- Explore security frameworks and best practices.
- Address real-world challenges in network security.
- Understand ethical considerations in data governance.
- Foster continuous learning.
- Encourage teamwork and collaboration.
- Prepare for advanced roles in network security.

Expected Outcomes

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

PROGRAM OUTLINE

Stage 1: Core Security Technologies

1. Introduction Network Security
- Core principles, tools, and industry applications.

2. Firewall Management
- Configuring and managing firewalls.

3. Email and Web Security
- Securing email and web applications.

4. VPN Management
- Setting up and managing VPNs.

Stage 2: Advanced Security Tools

5. Advanced Network Monitoring
- Monitoring and analyzing network traffic.

6. Incident Response
- Responding security incidents.

7. Security Assessment and Testing
- Evaluating security measures.

8. Security Policies and Governance
- Developing and implementing security policies.

Stage 3: Practical Applications

9. Practical Security Projects
- Developing and implementing security projects.

10. Security Operations Management
- Managing security operations.

11. Data Analysis and Visualization
- Analyzing security data and visualizing results.

12. Business Intelligence Applications
- Using data for security decision making.

Stage 4: Capstone Project

13. Integration of Learned Skills
- Apply tools and techniques real-world security problems.

14. Advanced Security Systems
- Developing complex security systems.

15. Cloud Security Management
- Securing cloud-based platforms.

16. AI for Security
- Implementing AI solutions in security.

Elective Modules

17. Data Ethics and Privacy
- Ethical considerations, privacy laws, compliance strategies.

18. Predictive Analytics with Security Management
- Building and validating predictive models.

PROGRAM OUTLINE

19. AI for Security Management
- Implementing AI solutions in security.

20. Advanced Data Warehousing Techniques
- Optimizing data warehousing solutions.

21. Data-Driven Security Decision Making
- Using data inform and drive security strategies.

22. Cloud Security Solutions
- Deploying security management systems on cloud platforms.

23. Security Project Management
- Leading security projects, ensuring successful delivery.

24. Big Data Security
- Securing data in big data environments.

25. IoT Security
- Securing IoT devices and systems.

Enrollment Now Open!

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

Email: info@choolsgroup.com **Phone:** +91 74067 33363 **Website:** chools.in