

Acronym/Nickname ECSA		Certification Body EC-COUNCIL	
Description <p>The CNDA Program certifies individuals in the specific network security discipline of Network Defense from a vendor-neutral perspective. The Certified Network Defense Architect certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Network Defense Architect is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.</p>		Certification Level Professional Covered competencies <p>This class will immerse the student into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation</p>	
		Requirements <p>To achieve the Certified Network Defense Architect Certification, you must pass the CNDA exam 312-99</p>	
Target <p>This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.</p>		Career Path	
Authorized Testing Center: PEARSON VUE / PROMETRIC	Indicative Fee* 250 USD	Certification Schedule*	
<p>* Fees and schedules are subject to change without prior notice, please get in touch with certification body through contact details below</p>			
Recommended/Preparatory Training Module 1: Introduction to Ethical Hacking Module 2: Footprinting Module 3: Scanning Module 4: Enumeration Module 5: System Hacking Module 6: Trojans and Backdoors Module 7: Sniffers Module 8: Denial of Service Module 9: Social Engineering Module 10: Session Hijacking Module 11: Hacking Web Servers Module 12: Web Application Vulnerabilities Module 13: Web-based Password Cracking Techniques Module 14: SQL Injection Module 15: Hacking Wireless Networks Module 16: Virus and Worms Module 17: Physical Security Module 18: Linux Hacking Module 19: Evading IDS, Firewalls, and Honeypots Module 20: Buffer Overflows Module 21: Cryptography Module 22: Penetration Testing			
Where to get more information: http://www.eccouncil.org/cnda.htm			