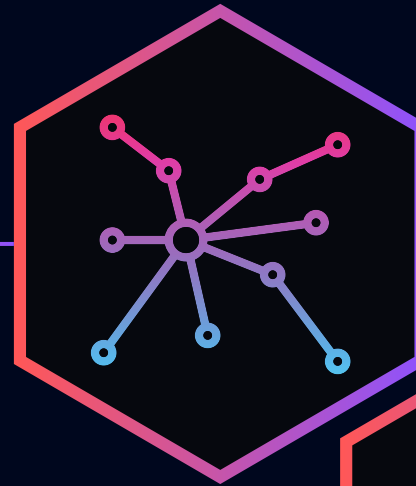


Courses & Certifications

CompTIA Network+



Linux +

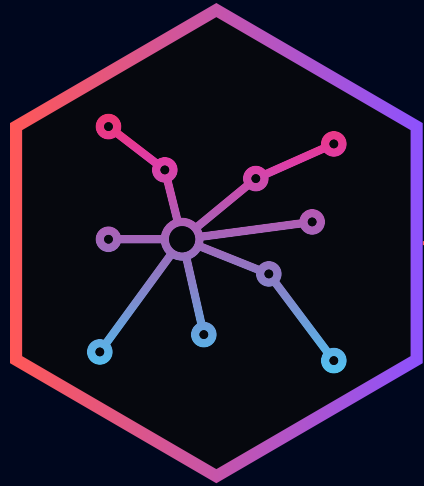


Certified Ethical Hacker V12



Certified SOC Analyst





CompTIA Network+

Overview of CompTIA Network+

CompTIA Network+ helps take your IT infrastructure to the next level, covering troubleshooting, configuring and managing networks.

Who is the course for?

CompTIA Network+ is for professionals with the recommended prerequisite of CompTIA Network+ certification and nine months of networking experience looking develop their networking careers.

Take a look at our Comprehensive Curriculum

01. Module

Networking Fundamentals

02. Module

Network Implementations

03. Module

Network Operations

04. Module

Network Security

05. Module

Network Troubleshooting

Cybersecurity Careers

- ➡ Network Security Operations
- ➡ Tier II IT Support Technician
- ➡ Network Security Specialist
- ➡ Solution Architect
- ➡ Network Administrator
- ➡ IT Support Manager
- ➡ Server Administrator
- ➡ Systems Administrator



Linux +

Overview of linux+

Linux+ certification in April of 2019 and we'll help you prepare to succeed in taking it. This course is intended for the IT Professional who uses Linux every day in their personal and professional lives. You only have to pass a single exam now, but keep in mind you will no longer get the LPI 2-for-1 certification as a result. This certification preparation course is designed to cover job-focused Linux foundational skills. The exam covers tasks that are associated with all major distributions of Linux and lays the foundation for more advanced vendor or distribution specific knowledge.

Who is the course for?

Linux+ measures the necessary skills of an IT professional with hands-on experience configuring, monitoring, and supporting servers running the Linux operating system.

Take a look at our Comprehensive Curriculum

01. Module

Command line basics

02. Module

Files and the filesystem

03. Module

Users and groups

04. Module

Installing software

05. Module

Shell basics

06. Module

Redirecting I/O

07. Module

Searching text

08. Module

Common utilities

09. Module

File editors

10. Module

Process management

11. Module

Regular Expressions

12. Module

Shell scripting



Certified Ethical Hacker V12

Overview of World's Leading Ethical Hacking Certification Course – CEH v12

A Certified Ethical Hacker(CEH) professional is a specialist typically working in a red team environment, focused on attacking computer systems and gaining access to networks, applications, databases, and other critical data on secured systems. A CEH recognizes attack strategies, the use of creative attack vectors, and mimics the skills and creativity of malicious hackers. Unlike black hat hackers, Certified Ethical Hackers operate with permission from the system owners and take all precautions to ensure the outcomes remain confidential. Bug bounty analysts are expert ethical hackers who use their attack skills to reveal vulnerabilities in the systems.

The Certified Ethical Hacker- CEH v12 Training Program certification is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired and demanding information security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is considered as a standard within the information security community.

CEH v12 continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used by malicious hackers and information security professionals today. The Five Phases of Ethical Hacking and the original goal of Certified Ethical Hacker- CEH v12 Training remain valid and relevant today: “To beat a hacker, you need to think like a hacker.”

Who is the course for?

This Certified Ethical Hacker- CEH v12 Training Program is meant for Graduates, Under Graduates, Network and Systems Administrators, IT staffs or anyone interested in learning information security

Take a look at our Comprehensive Curriculum

01. Module

Introduction to Ethical Hacking

02. Module

Footprinting And Reconnaissance

03. Module

Scanning Networks

04. Module

Enumeration

05. Module

Vulnerability Analysis

06. Module

System Hacking

07. Module

Malware Threats

08. Module

Sniffing

09. Module

Social Engineering

10. Module
Denial-Of-Service

11. Module
Session Hijacking

12. Module
Evading IDS, Firewalls, And Honeypots

19. Module
Cloud Computing

13. Module
Hacking Web Servers

14. Module
Hacking Web Applications

15. Module
SQL Injection

20. Module
Cryptography

16. Module
Hacking Wireless
Networks

17. Module
Hacking Mobile
Platforms

18. Module
IoT And OT Hacking

Cybersecurity Careers

- ➡ Cybersecurity Auditor
- ➡ Vulnerability Assessment Analyst
- ➡ Security Administrator
- ➡ Network Security Engineer
- ➡ Senior Security Consultant
- ➡ Information Security Manager



Certified SOC Analyst

Overview of Certified SOC Analyst

SOC Analyst (CSA) course is the first step to joining a security operations centre (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

Certified SOC Analyst (CSA) is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team.

Who is the course for?

This certification is meant for SOC Analysts (Tier I and Tier II), Network and Security Administrators, Network and Security Engineers, Cybersecurity Analysts, Entry-level cybersecurity professionals, or Anyone who wants to become a SOC Analyst.

Take a look at our Comprehensive Curriculum

01. Module

Security Operations and Management

02. Module

Understanding Cyber Threats, IoCs, and Attack Methodology

03. Module

Incidents, Events, and Logging

04. Module

Incident Detection with Security Information and Event Management (SIEM)

05. Module

Enhanced Incident Detection with Threat Intelligence

06. Module

Incident Response