



CompTIA Security & Penetration Testing Program

Launch Your Career in CompTIA Security

CompTIA Security & Penetration Testing Program

The CompTIA Security & Penetration Testing Program is a comprehensive course designed to teach cybersecurity fundamentals and advanced ethical hacking techniques. It begins with CompTIA Security+, which focuses on building a strong foundation in cybersecurity, covering topics like threat management, risk mitigation, and system protection. This ensures learners are equipped with the essential skills to identify and prevent security breaches.

The program then delves into advanced penetration testing, helping learners explore how to find vulnerabilities in systems and networks. It offers practical knowledge of tools and methods used by ethical hackers to simulate real-world attacks and strengthen security measures. Ideal for IT professionals, this course is a stepping stone to careers in cybersecurity and ethical hacking. Digitalearn provides expert training and resources to ensure success in this program.

Key Features

- Live Projects
- Exam Simulation
- Access to Recorded Sessions
- 45-Hour LIVE Instructor-led Training
- Updated Content (Market Trends)
- Class Feedback with Assigned Advisor
- Micro Batches (10 Students per Class)
- Individual Doubt Sessions
- Career Guidance and Mentorship
- Practical Sessions (Online)



How this program works differently with highlighted **Key Solutions** ?



Career Preparation

- Mock Interview Prep (Technical + Behavioral)
- Resume Building (Ready-to-use Templates)
- Job Application Guide (Tips for Finding the Right Job)
- Internship Benefits (Hands-on Experience with Tools)



Practical Learning

- Live Projects (5+ Real-World Projects)
- Practical Sessions (Interactive Online Learning)
- Updated Tools and Techniques (Stay Ahead with the Latest in Cybersecurity)



Learning Support

- Personality Development Classes (Enhance Soft Skills)
- Class Recordings (Access Anytime for Review)
- E-books (Comprehensive Learning Materials)



Certification and Exams

- Exam Simulation (Prepare Effectively)
- Exam vouchers (Subject to Availability)



Ongoing Mentorship

- Lifetime Career Mentorship (Guidance Throughout Your Career)



Continuous Learning

- Updated Content (Stay Current with Market Trends)
- Demos (Optional Hands-on Demonstrations)

Benefits of Completing the **SPTP**

Professional Benefits:

- **Secure Job Roles:** Qualify for jobs like Security Analyst, Penetration Tester, or SOC Specialist.
- **Global Recognition:** A respected certification that's valued worldwide.
- **Career Growth:** Open doors to higher salaries and top cybersecurity positions.

Technical Benefits:

- **Find Vulnerabilities:** Learn to think like a hacker to identify risks.
- **Defend Systems:** Gain skills to stop attacks before they happen.
- **Hands-On Skills:** Work on real systems and scenarios for better learning.
- **Stay Updated:** Learn modern tools and techniques used by hackers and defenders.

Organizational Benefits:

- **Strong Security:** Help companies protect their networks and reduce risks.
- **Save Money:** Stop costly breaches by finding problems early.
- **Compliance Ready:** Assist businesses in meeting security regulations and standards.

Career Opportunities with SPTP

- **Ethical Hacker:** Test systems and help make them safer.
- **Cybersecurity Analyst:** Monitor threats and secure company data.
- **Penetration Tester:** Check the strength of security systems through testing.
- **Threat Analyst:** Study cyber risks and find ways to prevent them.

The **CompTIA Security & Penetration Testing Program** is a great choice if you want to grow your career in cybersecurity. The simple course design makes it easy for everyone, even beginners, to learn and succeed.

Who Should Pursue the **CompTIA Security & Penetration Testing Program**?

The CompTIA Security & Penetration Testing Program (SPTP) is perfect for anyone looking to start or grow their career in cybersecurity. It's designed to teach both security basics and advanced penetration testing techniques. Here's who can benefit most:

1. Beginners in Cybersecurity
2. IT Professionals Switching to Security
3. Network Administrators
4. Students and Fresh Graduates
5. Security Analysts
6. System Administrators
7. Freelancers and Consultants
8. Organizations Training IT Teams





Industries That Benefit from **SPTP** **Professionals**

- **IT and Technology:** To secure software, systems, and networks.
- **Healthcare:** To protect sensitive patient data.
- **Finance:** To safeguard transactions and customer information.
- **Retail:** To ensure secure online shopping systems.
- **Government:** To defend critical infrastructure from cyber threats.

The CompTIA Security & Penetration Testing Program is suitable for anyone passionate about learning security skills. It's simple, practical, and useful for building a strong career in cybersecurity.

CompTIA Security & Penetration Testing Program Curriculum

The CompTIA Security & Penetration Testing Program (SPTP) is a step-by-step course designed to teach both defense and attack techniques in cybersecurity. This program covers the basics of security and advanced penetration testing in a simple, easy-to-understand way.

Module 1: Introduction to Cybersecurity

- What is cybersecurity?
- Basics of security and ethical hacking.
- Understanding threats and vulnerabilities.

Module 2: Security Fundamentals

- Learn how security protects networks and systems.
- Introduction to encryption and access control.
- How firewalls and antivirus tools work.

Module 3: Network Basics

- Understand how networks connect devices.
- Learn IP addresses, protocols, and how data moves.
- Spot weak points in networks.

Module 4: Recognizing Cyber Threats

- Types of attacks like phishing, malware, and ransomware.
- Tools used by hackers to exploit systems.
- Methods to identify and avoid threats.

Module 5: Hands-On Penetration Testing

- Learn to test systems for security flaws.
- Use tools like Metasploit and Kali Linux.
- Practice exploiting vulnerabilities in a safe environment.

CompTIA Security & Penetration Testing Program Curriculum

Module 6: Securing Networks and Systems

- How to block attacks and protect systems.
- Secure routers, servers, and user data.
- Learn about VPNs and secure network design

Module 7: Incident Response

- Steps to take during and after a cyberattack.
- Learn to recover data and fix security gaps.
- Create a plan to prevent future attacks.

Module 8: Cloud and IoT Security

- Basics of cloud storage and its risks.
- How to secure Internet of Things (IoT) devices.
- Recognize vulnerabilities in smart devices.

Module 9: Threat Analysis and Reporting

- Learn to read system logs and find signs of attacks.
- Understand how to gather and use threat intelligence.
- Create clear, simple reports on security issues.

Module 10: Practical Labs and Projects

- Practice with over 50+ hands-on labs.
- Use real tools to learn practical skills.
- Work on projects to test what you've learned

The CompTIA Security & Penetration Testing Program is perfect for beginners and professionals wanting practical skills. It's easy to follow and teaches both securing systems and testing for risks



The CompTIA Security & Penetration Testing Program is designed for beginners and professionals who want to secure systems and learn ethical hacking. This program focuses on both defensive and offensive cybersecurity skills.

Learning Objectives of the **CompTIA Security & Penetration Testing Program**



Building Strong Security Foundations

- Understand the basics of cybersecurity and network security.
- Learn about firewalls, antivirus, and encryption.
- Identify risks and protect systems effectively.



Identifying Threats and Weaknesses

- Find vulnerabilities in networks, systems, and software.
- Learn to detect unusual activities in network traffic.
- Understand how attackers exploit weaknesses.



Mastering Ethical Hacking Techniques

- Learn how to perform ethical hacking in a safe way.
- Use tools like Metasploit and Nmap to test systems.
- Understand how hackers think to prevent attacks.



Why did Digitalearn Become the chosen for Corporate Training?

Digitalearn keeps its content fresh. We continuously update our courses to include the latest trends and technologies like cloud computing, AI, and cybersecurity, ensuring your team is always ready for the future.

Choose Digitalearn for your IT and cybersecurity training needs and watch your team thrive with the skills they need to excel in today's fast-paced tech environment!

Comprehensive and Tailored Training Programs:

- Expert-Led Training with Hands-On Experience
- Flexible Delivery Options
- Enhancing Employee Skills for Business Success
- Corporate Certification and Assessments
- Tailored Corporate Solutions
- Cost-Effective Training for Large Teams
- Proven Success and Client Satisfaction
- Ongoing Support and Learning
- Up-to-Date Content on Emerging Technologies

How Schedule and Commitments will work?



Duration
2 months
(8 weeks)



Mode
Online Live
Classes + Hands-
on Training



Commitment
2 Months /
2 hours a Day /
Mon-Wed-Thur-Sat

What are **Practical Tasks** in the training Program?



Network Monitoring and Threat Detection

Use Wireshark to analyse network traffic and detect anomalies.



Vulnerability Assessment

Conduct vulnerability scans and assess risk impact on simulated environments.



Incident Response Simulation

Practice identifying, responding to, and documenting security incidents.



Risk Assessment Project

Develop a risk management plan aligned with industry standards

Upon Completing the **Program**,
You'll Receive:

- Digitalearn Certified CompTIA Security & Penetration Testing Program Certificate
- Portfolio-ready projects and access to career advancement resources



4.9 Average
Rating



3500+
Students
Got Job



4000+
Satisfied
Learners



100+ Highly
Qualified
Trainers

What Kind of Support Will You Receive?



Mentorship

A dedicated mentor to guide you through the learning journey



Alumni Network

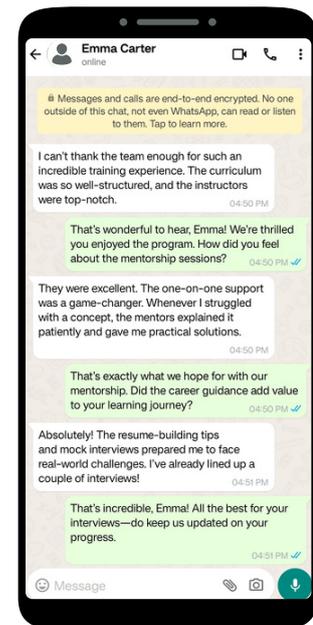
Access to a supportive community of cybersecurity professionals



Career Assistance

Networking tips, job search strategies, and interview prep

What our **students** say ?



CompTIA Security & Penetration Testing Program **FAQ**

? 1. What is the CompTIA Security & Penetration Testing Program?

- ✓ This program teaches you the skills to secure systems and perform ethical hacking. It covers both defensive (security) and offensive (penetration testing) techniques.

? 2. Who should take this program?

- ✓ This program is great for:
 - Beginners in cybersecurity.
 - IT professionals wanting to improve security skills.
 - Those interested in ethical hacking and penetration testing.

? 3. What skills will I learn?

- ✓
 - Protecting networks and systems from cyber threats.
 - Testing security by simulating real-world attacks.
 - Using tools like Wireshark, Nmap, and Kali Linux.

? 4. Are there any prerequisites?

- ✓ No formal prerequisites are needed. Basic knowledge of IT and networking is helpful but not required.

? 5. How long does the program take?

- ✓ The program usually takes 4 to 6 weeks, depending on how quickly you study.

? 6. What is the exam format?

- ✓
 - Type: Multiple-choice questions.
 - Duration: 90 minutes.
 - Passing Score: Around 70%.

? 7. How much does it cost?

- ✓ The cost of the exam is around \$350 to \$400. Training programs may cost extra, depending on the provider.

? 8. What job roles can I get after completing this program?

- ✓ You can work as:
 - Cybersecurity Analyst
 - Network Security Specialist
 - Ethical Hacker
 - Penetration Tester



Social Media Handles:

 @digitalearn_official

 Digitalearn

Ask your queries to our experts?

 +91 90124 95693
+91 9625585022

 www.digitalearn.info

 support@digitalearn.info

 Office Hours :
09:00 AM EST to 07:00 PM EST