CREST Practitioner Security Analyst Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

The training provides an internationally recognized foundation for individuals beginning their career in **cybersecurity and penetration testing**.

Delivered by **CREST-approved training providers**, this course equips participants with the knowledge to assess network services, operating systems, and web applications for vulnerabilities.

The training concludes with the **CPSA exam**, a multiple-choice assessment conducted via **Pearson VUE**, which confers **CREST Practitioner status** upon successful completion.
CPSA is the **prerequisite for the CREST Registered Tester (CRT)** exam and aligns closely with **OffSec OSCP (PEN-200)** standards.

The **CPSA certification** validates your understanding of key penetration testing and security assessment concepts.
It's the ideal entry point for professionals aiming to advance toward **CREST Registered Tester (CRT)** or **OffSec OSCP (PEN-200)** certifications.

Completing this course positions you at the forefront of the cybersecurity industry — ready to join professional pen test and incident response teams.

Prerequisites

To get the most from this course, participants should have:

- A **basic understanding of IT systems** (networking, IP, ports, OS concepts).
- Prior completion of a **Security Fundamentals** course is recommended.
- Some hands-on experience with system or network administration is beneficial.

Who Should Attend

- Entry-level cybersecurity professionals
- Aspiring penetration testers and ethical hackers
- Network/system administrators
- Incident response and forensics specialists
- Security analysts and managers
- Law enforcement professionals expanding digital skills

CREST Practitioner Security Analyst Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this training, you will have gained knowledge and skills in the following areas:

- Understand cybersecurity fundamentals, threats, and risk management concepts.
- Perform basic infrastructure and web application testing.
- Identify and interpret common vulnerabilities and attack surfaces.
- Understand secure coding, cryptography, and identity management.
- Apply principles of incident handling and vulnerability assessment.
- Build a foundation for advanced penetration testing and ethical hacking roles.

Training Outline

Introduction to Cybersecurity

- Threat modeling, risk management, and legal compliance

Network Security Fundamentals

- Network types, topologies, devices, and protocols

Operating System Security

- Logical port assessments, Windows OS security principles

Application Security

- Web and browser exploits, secure coding, auditing techniques

Cryptography and IAM

- Encryption, identity and access management, cryptocurrency concepts