CREST Practitioner Security Analyst Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Bu {*eğitim}, siber güvenlikte kariyer yapmak isteyen profesyoneller için tasarlanmış, **uluslararası geçerliliğe sahip bir temel seviye sızma testi (penetration testing) ve güvenlik analizi sertifikasyon programıdır.**

Bu eğitim, **CREST onaylı bir sağlayıcı** olan QA tarafından sunulmakta olup, katılımcılara **ağ servisleri, işletim sistemleri, uygulama güvenliği ve temel web güvenlik testleri** konularında güçlü bir teknik altyapı kazandırır.

Eğitim sonunda katılımcılar, **Pearson VUE üzerinden CPSA sınavına** girer ve başarıyla tamamlayanlar **CREST Practitioner** unvanını kazanır.
Bu sertifika, **CREST Registered Penetration Tester (CRT)** sınavına girmek için ön koşuldur.

Bu eğitim, siber güvenlik dünyasına güçlü bir giriş yapmak isteyen profesyoneller için**CREST onaylı uluslararası bir başlangıç noktasıdır.**
CPSA sertifikası, katılımcılara hem **pen test ekiplerinde görev alma** hem de **bir üst seviye olan CRT veya OSCP** sınavlarına hazırlık avantajı sağlar.

Prerequisites

Bu eğitime katılmak için:

- **Temel BT bilgisi** (ağlar, işletim sistemleri, IP, port kavramları vb.) önerilir.
- **Security Fundamentals** veya eşdeğer bir ön eğitim tavsiye edilir.
- Daha önce siber güvenlik veya sistem yönetimi konularında deneyim sahibi olmak avantaj sağlar.

Who Should Attend

- Sızma testi alanında kariyer hedefleyen siber güvenlik uzmanları
- Ağ veya sistem yöneticileri
- Olay müdahale (incident response) ekipleri
- BT güvenlik analistleri ve yöneticileri
- Adli bilişim (digital forensics) profesyonelleri
- Kamu kurumları ve özel sektör güvenlik ekipleri
- Güvenlik denetçileri ve yeni başlayan etik hacker adayları

CREST Practitioner Security Analyst Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Bu {*eğitim} sonunda aşağıdaki konularda bilgi ve beceri kazanmış olacaksınız:

- Temel sızma testi süreçlerini ve güvenlik analizi yöntemlerini öğrenir.
- Ağ protokolleri, IP mimarisi ve güvenlik katmanlarını kavrar.
- İşletim sistemleri (özellikle Windows) üzerinde güvenlik açıklarını analiz eder.
- Web uygulamalarında yaygın güvenlik zafiyetlerini tespit eder.
- Güvenli yazılım geliştirme ve uygulama denetimi prensiplerini uygular.
- Kriptografi, kimlik yönetimi ve erişim kontrolü temellerini öğrenir.
- Siber tehdit modelleme ve risk değerlendirme süreçlerini uygular.

Outline

Siber Güvenliğe Giriş

- Siber güvenlik kavramları, tehdit modelleme, risk yönetimi
- Sızma testi ve yasal uyumluluk

Ağ Güvenliği Temelleri

- Ağ topolojileri, cihazlar, IP protokolleri, OSI modeli
- TCP/IP iletişimi ve ağ analizi

İşletim Sistemleri Güvenliği

- Windows güvenlik mimarisi
- Mantıksal port analizi ve güvenlik konfigürasyonları

Uygulama Güvenliği

- Web uygulama zafiyetleri, exploit teknikleri
- Güvenli kodlama ve uygulama denetimi

Kriptografi ve Kimlik Yönetimi

- Şifreleme algoritmaları, dijital kimlik doğrulama
- Kripto para ve güvenli işlem yönetimi