CERTIFIED PENETRATION TESTING PROFESSIONAL (CPENT) EĞİTİMİ

5 GÜN

Digital Vizyon
Akademi

www.digitalvizyon.net

İçindekiler

Eğitim Hakkında

Certified Penetration Testing Professional (CPENT) Eğitimi, bilgi güvenliği profesyonelleri için özel olarak tasarlanmış kapsamlı bir programdır. Bu eğitim, katılımcılara etkili bir şekilde penetrasyon testi yapma becerilerini kazandırmayı hedefler. Aynı zamanda, siber güvenlik alanında derinlemesine bilgi ve uygulama deneyimi sağlar. CPENT eğitimi, gerçek dünya senaryolarında güvenlik açıklarını tespit etme, riskleri değerlendirme ve etkili önlemler alma konularında yetkinlik kazanmanızı sağlar.

CPENT eğitimi, ağ saldırıları, zafiyet analizi, saldırı tespiti, web uygulama güvenliği, veri güvenliği ve ağ güvenliği stratejileri gibi temel konulara odaklanır. Bu sayede, çeşitli saldırı vektörlerini anlama, zafiyetleri tespit etme ve güvenlik açıklarını giderme becerilerinizi geliştirirsiniz. Ayrıca, penetrasyon testlerinin planlanması, uygulanması ve raporlanması gibi süreçlere aşina olur ve bu alanda güvenilir bir uzman olarak kendinizi kanıtlarsınız.

CPENT eğitimi, teorik bilgiyi pratik çalışmalar ve canlı senaryolarla birleştirerek gerçek dünya deneyimi sunar. Gerçekçi senaryolar ve ağ ortamlarında yapacağınız penetrasyon testleri sayesinde bilgi ve becerilerinizi test ederken güvenlik stratejilerini de etkin bir şekilde uygulama fırsatı bulursunuz. Böylece, siber saldırıların önlenmesi ve güvenlik açıklarının kapatılması konusunda önemli bir rol oynayabilirsiniz.

CPENT eğitimini başarıyla tamamlayan katılımcılar, CPENT sertifikasını elde ederler. Bu sertifika, penetrasyon testi konusunda yetkinliğinizi belgeleyerek, işverenler ve sektördeki diğer profesyoneller tarafından güvenilirlik ve uzmanlık açısından takdir edilmenizi sağlar. CPENT sertifikası, kariyerinizde rekabet avantajı sağlayarak siber güvenlik alanında ilerlemenize yardımcı olur.

CPENT eğitimi, siber güvenlik profesyonelleri için önemli bir fırsat sunar. Bu program sayesinde güvenlik açıklarını tespit etme, riskleri değerlendirme ve güvenlik önlemleri alma konusundaki becerilerinizi geliştirerek organizasyonların güvenliğine katkıda bulunabilirsiniz. CPENT sertifikası, alanınızda uzmanlaşmanızı sağlayarak daha ileri düzey pozisyonlara yükselmenizi destekler. Certified Penetration Testing Professional (CPENT) Eğitimi daha fazla bilgi almak için ulaşabilirsiniz.

Neler Öğreneceksiniz?

Certified Penetration Testing Professional (C|PENT) eğitimi sırasında aşağıdaki konuları öğrenebilirsiniz:

Penetrasyon Testi Temelleri: Penetrasyon testinin temel kavramlarını ve süreçlerini öğrenirsiniz. Hedef belirleme, bilgi toplama, saldırı planlama, saldırı yürütme ve raporlama gibi adımları içeren bir penetrasyon testi sürecini anlarsınız.

Ağ Güvenlik Zafiyetleri: Ağ sistemlerinde yaygın olarak bulunan güvenlik zafiyetlerini ve saldırı vektörlerini öğrenirsiniz. Web uygulama güvenliği, ağ protokollerindeki zafiyetler, uygulama katmanı güvenlik açıkları gibi konular üzerinde çalışarak zafiyetleri tespit etme ve sömürme becerilerinizi geliştirirsiniz.

Saldırı Araçları ve Teknikleri: Farklı saldırı araçlarını ve tekniklerini öğrenirsiniz. Port tarama, zayıf parola saldırıları, XSS (Cross-Site Scripting) saldırıları gibi saldırı türlerini gerçekleştirmek ve güvenlik zafiyetlerini tespit etmek için kullanılan araçları keşfedersiniz.

Zafiyet Analizi ve Raporlama: Zafiyet analizi sürecini ve raporlama yöntemlerini öğrenirsiniz. Zafiyetleri tespit etmek, riskleri değerlendirmek ve detaylı bir rapor hazırlamak için kullanılan teknikleri uygulayarak zafiyet analizi becerilerinizi geliştirirsiniz.

Etik Kurallar ve Yasa Uyumu: Penetrasyon testleri sırasında etik kuralları ve yasal uyumu öğrenirsiniz. Etik penetrasyon testi uygulamaları ve yasa ve düzenlemelere uyum konularında bilgi edinir ve testlerin doğru bir şekilde yapılmasını ve olumsuz sonuçlara yol açmamasını sağlamak için gerekli etik standartları ve yasal gereklilikleri öğrenirsiniz.

C|PENT eğitimi, gerçek dünya senaryolarında ağ sistemlerini test etme ve zayıflıkları tespit etme yeteneklerinizi geliştirmenizi sağlar. Bu eğitim, ağ güvenliği alanında derinlemesine bilgi ve beceriler kazanmanıza ve güvenlik testi konusunda yetkin hale gelmenize yardımcı olur.

Ön Koşullar

Certified Penetration Testing Professional (C|PENT) eğitimine katılmadan önce aşağıdaki ön koşulların karşılanması önerilir:

Temel Bilgisayar Bilgisi: Bilgisayar sistemleri, ağlar, işletim sistemleri ve temel ağ protokollerine ilişkin bir anlayışa sahip olmanız faydalı olacaktır.

Ağ ve Sistem Güvenliği Temelleri: Ağ güvenliği prensipleri, saldırı türleri, güvenlik önlemleri, temel ağ ve sistem güvenliği kontrolleri hakkında bir bilgiye sahip olmanız eğitimi daha iyi anlamanızı sağlar.

Ağ ve Sistem Yönetimi: Ağ ve sistem yönetimi konusunda deneyime sahip olmanız, ağ altyapısını ve sistem yapılandırmalarını anlamanızı ve penetrasyon testlerinde karşılaşacağınız ortamları değerlendirmenizi kolaylaştırır.

Temel Kriptografi Bilgisi: Temel kriptografi kavramları, şifreleme algoritmaları ve anahtar yönetimi hakkında bir anlayışa sahip olmanız, güvenli iletişim ve veri koruması konularında ön bilgi sahibi olmanızı sağlar.

Bu ön koşullar, C|PENT eğitimine katılmadan önce size avantaj sağlayabilir, ancak kesin bir zorunluluk değildir. Eğitimi sağlayan kuruluşun belirlediği spesifik ön koşulları kontrol etmek önemlidir, çünkü gereksinimler farklı kuruluşlar arasında değişebilir. Eğitim sağlayıcının belirlediği ön koşulları karşıladığınızdan emin olmanız önerilir.

Kimler Katılmalı

Certified Penetration Testing Professional (C|PENT) eğitimi, aşağıdaki profesyoneller için uygun olabilir:

Bilgi Güvenliği Uzmanları: Bilgi güvenliği alanında çalışan uzmanlar, ağ güvenliği testleri ve penetrasyon testleri konusunda bilgi ve becerilerini geliştirmek isteyebilirler. Bu uzmanlar genellikle şirketlerde veya danışmanlık firmalarında güvenlik testi konularında çalışmaktadır.

Ağ ve Sistem Yöneticileri: Ağ ve sistem yöneticileri, organizasyonların ağ altyapısının güvenliğini sağlamak ve zayıflıkları tespit etmekle sorumludur. C|PENT eğitimi, bu yöneticilere güvenlik testi teknikleri ve zayıflık analizi konularında bilgi ve beceri kazandırır.

Güvenlik Danışmanları ve Denetçiler: Güvenlik danışmanları ve denetçiler, müşterilere güvenlik testi hizmetleri sağlamak ve güvenlik açıklarını tespit etmek isteyebilirler. C|PENT eğitimi, danışmanlık ve denetim süreçlerinde etkili bir şekilde güvenlik testi yapma yeteneklerini geliştirir.

Uygulama Geliştiricileri: Uygulama geliştiricileri, güvenli yazılım ve uygulamalar oluşturma süreçlerinde zayıflık analizi ve güvenlik testi yapmak isteyebilirler. C|PENT eğitimi, uygulama düzeyinde güvenlik testi ve zayıflık analizi konularında bilgi ve beceri kazandırır.

Siber Güvenlik Araştırmacıları: Siber güvenlik alanında çalışan araştırmacılar, yeni güvenlik açıklarını tespit etmek ve saldırı tekniklerini incelemek için C|PENT eğitimine katılabilirler. Bu eğitim, araştırma becerilerini geliştirerek siber güvenlikte ileri düzeyde uzmanlık sağlar.

Yukarıda belirtilen gruplar, C|PENT eğitimine katılmak için uygun olabilecek örneklerdir. Ancak, herhangi biri, ağ güvenliği ve penetrasyon testi konularında ilgi ve motivasyona sahipse, bu eğitime katılarak bilgi ve becerilerini geliştirebilirler. Ağ güvenliği alanında çalışmak isteyen veya mevcut bilgi ve becerilerini güçlendirmek isteyen herkes, C|PENT eğitimine katılabilir.

Outline

Module 01: Module 01: Introduction to Penetration Testing and Methodologies

Cover the fundamentals of penetration testing, including penetration testing approaches, strategies, methodologies, techniques, and various guidelines and recommendations for penetration testing

Module 02: Penetration Testing Scoping and Engagement

Learn the different stages and elements of scoping and engagement in penetration testing.

Module 03: Open-Source Intelligence (OSINT)

Learn how to use techniques and tools to gather intelligence about the target from publicly available sources such as the World Wide Web (WWW), through website analysis, by using tools/frameworks/scripts, and so on.

Module 04: Social Engineering Penetration Testing

Learn different social engineering techniques and perform social-engineering penetration testing on a target organization.

Module 05: Network Penetration Testing – External

Learn how to implement a comprehensive penetration testing methodology for assessing networks from outsiders' perspectives. Learn the process attackers follow to exploit the assets using vulnerabilities from the outside of the network perimeter.

Module 06: Network Penetration Testing – Internal

Learn how to implement a comprehensive penetration testing methodology for assessing networks from insider's perspectives.

Module 07: Network Penetration Testing – Perimeter Devices

Learn how to implement a comprehensive penetration testing methodology for assessing the security of network perimeter devices, such as Firewalls, IDS, Routers, and Switches.

Module 08: Web Application Penetration Testing

Learn how to analyze web applications for various vulnerabilities, including the Open Web Application Security Project (OWASP) Top 10, and determine the risk of exploitation.

Module 09: Wireless Penetration Testing

Learn how to test various components of wireless networks, such as WLAN, RFID devices, and NFC technology devices.

Module 10: IoT Penetration Testing

Understand various threats to Internet of things (IoT) networks and learn how to audit security controls for various inherent IoT risks.

Module 11: OT and SCADA Penetration Testing

Understand OT and SCADA concepts and learn the process of testing various components of OT and SCADA networks.

Module 12: Cloud Penetration Testing

Understand various security threats and concerns in cloud computing and learn how to perform cloud penetration testing to determine the probability of exploitation.

Module 13: Binary Analysis and Exploitation

Understand the binary analysis methodology and reverse engineer applications to identify vulnerable applications that may lead to the exploitation of an information system.

Module 14: Report Writing and Post Testing Actions

Learn how to document and analyze the results of a penetration test and recommend post-penetration test actions.