30 YAŞ ALTI ÜNİVERSİTE ÖĞRENCİLERİ ve 30 YAŞ ALTI YENİ MEZUNLARA YÖNELİK

SIZMA TESTİ VE OLAY MÜDAHALE EĞİTİMİ

ANKARA

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

BTK AKADEMİ

EĞİTİM AMACI

Bu eğitimin amacı, üniversiteli öğrencileri ve 30 yaş altı mezunlarımızın temel sızma testi yaparak web ve sunucular üzerinde hackleme yeteneklerine ve siber saldırı sonrasında hacklenmiş bir sunucunun incelenmesi ve olay müdahale bilgi ve becerisini kazanmalarını sağlamaktır.

HEDEF KİTLE

Siber Güvenlik alanında kendini geliştirmek isteyen **30 yaş altı** Üniversite Öğrencisi ya da **30 yaş altı** yeni üniversite mezunu gençler

SON BAŞVURU TARİHİ: 08 Eylül 2024

EĞİTİM HAKKINDA GENEL BİLGİLENDİRME VE ÖNEMLİ UYARILAR

- Eğitim 14 Eylül-06 Ekim 2024 tarihlerinde gerçekleştirilecektir.
- Eğitim çalışması toplam 48 saattir.
- Eğitim kontenjanı 25 kişidir.
- Katılımcılar başvuru sıralamasına göre alınacaktır.
- Eğitimde %80 devam koşulu bulunmaktadır. %20 üstü devamsızlığı olan öğrencilerin kaydı programdan otomatik olarak silinecektir.
- Devamsızlık nedeniyle kaydı silinen öğrenciler kara listeye alınacak ve 3 yıl içerisinde yapılacak olan hiçbir BTK Akademi eğitiminden faydalanamayacaktır.
- Eğitimi tamamlayan katılımcılar "Katılım Sertifikası" almaya hak kazanacaktır.
- Etkinliğe kayıt yaptıran tüm adaylarla e-posta yoluyla iletişim sağlanacaktır. E-posta adreslerinizin doğru olduğundan emin olunuz.
- Adaylar süreç içerisinde karşılaştıkları tüm problemleri destek@btkakademi.gov.tr adresine iletebilirler.
- www.btkakademi.gov.tr üzerinde yer alan eğitimler ve atölye çalışması ücretsizdir.
- Atölye **ANKARA İlinde yüz yüze gerçekleşecektir.**
- **Eğitime katılmaya hak kazananlar eğitim süresince kendi bilgisayarlarını kullanacaktır.**
- **Eğitim ücretsiz olup, konaklama, ulaşım ve yeme-içme katılımcılara aittir.**

EĞİTİM TARİH VE SAATLERİ

30 Yaş Altı Üniversite Öğrencileri ve 30 Yaş altı Üniversite Mezunlarına Yönelik Sızma Testi ve Olay Müdahale Eğitimi (14 Eylül 2024- 06 Ekim 2024)	
Haftalar	**Eğitim Gün ve Saatleri**
1.Hafta	14.09.2024 Cumartesi – 15.09.2024 Pazar 09:00-12:00 13:00-16:00
2. Hafta	21.09.2024 Cumartesi – 22.09.2024 Pazar 09:00-12:00 13:00-16:00
3.Hafta	28.09.2024 Cumartesi – 29.09.2024 Pazar 09:00-12:00 13:00-16:00
4.Hafta	05.10.2024 Cumartesi – 06.10.2024 Pazar 09:00-12:00 13:00-16:00

EĞİTİM İÇERİĞİ

Sızma Testi Eğitimi:

Giriş ve Temel Kavramlar:
Konu Açıklamaları:

- Siber güvenlik ekosistemi ve sızma testinin rolü.
- Etik hackerın tanımı ve sorumlulukları.
- Sızma testinin iş dünyasına katkıları.
- Canlı Senaryo:
- Bir etik hackerın gerçek dünya senaryosu üzerinden anlatımı.
- Interaktif Öğrenme Aktivitesi:
- Katılımcıların siber güvenlik senaryosunu çözmeleri.

Bilgi Toplama ve Keşif Aşaması:
Konu Açıklamaları:

- OSINT yöntemleri.

- Ağ haritalama ve keşif araçları.
- Keşfedilen bilgilerin etkin analizi.
- Canlı Senaryo:
- Kamu kaynaklarından elde edilen bilgilerle bir kurumun zayıflıklarının belirlenmesi.
- Interaktif Öğrenme Aktivitesi:
- OSINT araçlarıyla bilgi toplama pratikleri.

Zayıflıkların Keşfi ve Analizi:
Konu Açıklamaları:

- Zayıflıkların sınıflandırılması ve öncelendirilmesi.
- Zayıflık tarama araçları ve metodolojileri.
- Zayıflıkların sömürülmesi ve potansiyel tehlikeler.
- Canlı Senaryo:
- Sistemdeki bir zayıflığın tespit edilmesi ve bu zayıflığın nasıl sömürüldüğünün gösterimi.
- Interaktif Öğrenme Aktivitesi:
- Zayıflık tarama araçlarıyla çalışma ve raporlama.

Saldırı Aşaması:
Konu Açıklamaları:

- Exploitation teknikleri ve yöntemleri.
- Metasploit ve benzeri araçlarla saldırı senaryoları.
- Saldırı sonrası sistem kontrolü ve yönetimi.
- Canlı Senaryo:
- Bir saldırı gerçekleştirilerek hedef sistem üzerinde kontrol sağlanması.
- Interaktif Öğrenme Aktivitesi:
- Metasploit ile temel saldırı senaryolarının simülasyonu.

Zafiyetli Makine Çözümleri:

Konu Açıklamaları:

- Sanal makineler üzerinde zafiyetli sistemlerin oluşturulması.
- Zafiyetli sistemlerde güvenlik açıklarının tespiti.
- Pratik zafiyet çözüm senaryoları.
- Canlı Senaryo:
- Zafiyetli bir sistem üzerinde gerçekleştirilen saldırının ardından çözüm adımlarının gösterimi.
- Interaktif Öğrenme Aktivitesi:
- Katılımcılara sunulan zafiyetli sistemlerde uygulamalı çözüm alıştırmaları.

Web Uygulama Güvenliği:

Konu Açıklamaları:

- Web uygulama güvenliğinin temel prensipleri.
- OWASP standartları.
- En yaygın web uygulama saldırıları ve savunma stratejileri.
- Canlı Senaryo:
- Bir web uygulamasındaki zayıf noktaların tespiti ve güvenli hale getirilmesi.
- Interaktif Öğrenme Aktivitesi:
- Web uygulama güvenliği tarama araçlarıyla çalışma ve raporlama.

Sürdürülebilirlik ve Raporlama:

Konu Açıklamaları:

- Sızma testi raporunun oluşturulması.
- İyileştirme önerilerinin detaylandırılması.
- Müşteri veya organizasyonla etkileşim stratejileri.
- Canlı Senaryo:
- Bir sızma testi raporunun hazırlanması ve müşteri sunumu.
- Interaktif Öğrenme Aktivitesi:
- Katılımcıların kendi sızma testi raporlarını hazırlamaları ve sunmaları.

Olay Müdahale Eğitimi:

Incident Response Temelleri:

- IR süreçlerinin belirlenmesi ve belgelenmesi
- IR ekiplerinin oluşturulması ve rolleri
- Önceden belirlenmiş müdahale planlarının oluşturulması
- Olay Tespit ve Analiz:
- Güvenlik olaylarının tespit edilmesi ve teşhisi
- Log analizi
- Olayların hızlı bir şekilde analiz edilmesi

- Olay Müdahalesi:
- Hızlı yanıt stratejileri ve taktikleri
- Malware analizi ve temizleme süreçleri
- Hedef sistemlerin kurtarılması ve güvenli hale getirilmesi
- Olay Sonrası Değerlendirme ve Raporlama:
- Olayın etkilerinin değerlendirilmesi
- Saldırı vektörünün belirlenmesi ve saldırının kökeni
- Olay raporunun oluşturulması ve paylaşılması
- İyileştirme ve Önleme:
- IR süreçlerinin sürekli geliştirilmesi
- Güvenlik önlemlerinin güçlendirilmesi ve güncellenmesi
- Gelecekteki olaylara karşı hazırlıklı olmak için stratejiler