ÜNİVERSİTE ÖĞRENCİLERİNE YÖNELİK

# SİBER GÜVENLİK ATÖLYESİ

## ÇANAKKALE

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

BTK AKADEMİ

# ATÖLYENİN AMACI

Siber Güvenlik Atölyesi, 21.yüzyıl toplumunda siber güvenlik bilincine sahip bireylerin sayısını arttırmak, bu konuda farkındalığı arttırmak ve aynı zamanda siber güvenlik ve yazılım geliştirme alanında kariyer yapmayı hedefleyen bireyler için BTK Akademi ve USOM tarafından gerçekleştirilmektedir.

# HEDEF KİTLE

- 30 yaş altı yeni mezunlar ve üniversite öğrencileri
- Siber Güvenlik ve yazılım alanında kariyer yapmayı hedefleyen
- Mevcut deneyimlerini ileri seviyeye taşımak isteyen,

# ATÖLYEYE KATILIM İÇİN ÖN KOŞULLARI

01 12 Mayıs 2024 tarihine kadar sayfa sonunda yer alan link üzerinden "Siber Güvenlik Atölyesi" etkinliğine başvurmak

02 14 Mayıs 2024 tarihinde gerçekleştirilecek olan çevrim için sınav konuları kapsamında geç 12 Mayıs 2024 23:59'a kadar BTK Akademi çevrim içi eğitim portali üzerinden aşağıdaki eğitimi %100 oranda tamamlamanız tavsiye edilmektedir.

| Eğitim Adı | Saat | Link | Zorunluluk |
|---|---|---|---|
| Siber Tehdit İstihbaratı ve Tehdit Avcılığı | 03:03:31 | https://www.btkakademi.gov.tr/portal/course/siber-tehdit-istihbarati-ve-tehdit-avciligi-21060 | Tavsiye |
| Sosyal Mühendislik ve Oltalama | 00:51:27 | https://www.btkakademi.gov.tr/portal/course/sosyal-muehendislik-ve-oltalama-21012 | Tavsiye |
| Uygulamalı Sızma Testi Eğitimi | 14:52:48 | https://www.btkakademi.gov.tr/portal/course/uygulamali-sizma-testi-egitimi-16025 | Tavsiye |
| Siber Güvenlikte Linux İşletim Sistemleri | 01:32:15 | https://www.btkakademi.gov.tr/portal/course/siber-guevenlikte-linux-isletim-sistemleri-10869 | Tavsiye |
| Güvenli Yazılım Geliştirme | 00:44:41 | https://www.btkakademi.gov.tr/portal/course/guevenli-yazilim-gelistirme-9201 | Tavsiye |
| Veri tabanı Saldırıları ve Veri tabanı Güvenliği | 04:16:29 | https://www.btkakademi.gov.tr/portal/course/veri-tabani-saldirilari-ve-veri-tabani-guevenligi-6569 | Tavsiye |
| Web Uygulama Güvenliği ve Web Sızma Tekniklerine Giriş | 02:30:46 | https://www.btkakademi.gov.tr/portal/course/web-uygulama-guevenligi-ve-web-sizma-tekniklerine-giris-10587 | Tavsiye |

03 Ön eleme sınavında en yüksek puanı alan ilk 30 kişi arasına girmek. ****

04 14 Mayıs 2024 tarihinde BTK Akademi çevrim içi eğitim portali üzerinden düzenlenecek çevrim içi ön eleme sınavına katılmak. ***

*** Ön eleme amaçlı çevrim içi sınav www.btkakademi.gov.tr üzerinden yapılacaktır. Atölyeye başvuran ve ön koşulları sağlayan herkes çevrim içi sınava girmeye hak kazanacaktır. **Sınav soruları çoktan seçmeli olup, tavsiye olarak belirtilen eğitimlerin içeriğini kapsayacaktır.**

****Ön eleme sınavından en yüksek puanı alan ilk 30 kişi seçilecektir. Son sıradaki aday ile aynı puana sahip olan sonraki adayların sınav süreleri dikkate alınacaktır.

**Daha öncesinde BTK Akademi tarafından düzenlenen Siber Güvenlik Kamp / Sınıf Eğitimi / Atölyesine katılmış olan katılımcılar katılamaz.**

## ÇEVRİM İÇİ SINAVA GİRİŞ İÇİN YAPILMASI GEREKENLER

14 Mayıs tarihinde gerçekleştirilecek olan çevrim içi sınava katılmaya hak kazanan adaylara e-posta ile bilgilendirme sağlanacaktır. E-postada iletilecek olan bağlantı üzerinden çevrim içi sınava katılım sağlanacaktır.

## SON BAŞVURU TARİHİ: 12 MAYIS 2024

## ATÖLYE HAKKINDA GENEL BİLGİLENDİRME VE ÖNEMLİ UYARILAR

- Atölye 21-24 Mayıs 2024 tarihlerinde gerçekleştirilecektir.
- Atölye çalışması toplam 32 saattir.
- Atölye kontenjanı 30 kişidir.
- Atölyede %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.
- Atölyeyi başarıyla tamamlayan katılımcılar "Başarı 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 **ÇANAKKALE İlinde yüz yüze gerçekleşecektir.**
- **Eğitime katılmaya hak kazananlar eğitim süresince kendi bilgisayarlarını kullanacaktır.**
- **Atölye ücretsiz olup, konaklama, ulaşım ve yeme-içme katılımcılara aittir.**
- **Atölye 30 yaş altı olup üniversite öğrencileri ve yeni mezunlar içindir.**

# ATÖLYE TARİH VE SAATLERİ

| **SİBER GÜVENLİK ATÖLYESİ**<br>**Ders Tarih ve Saatleri (21-24 Mayıs 2024)** | |
|---|---|
| **Haftalar** | **Eğitim Gün ve Saatleri** |
| **1. Hafta** | SALI-ÇARŞAMBA-PERŞEMBE-CUMA<br>**21-24 Mayıs 2024**<br>09.00 – 12.00<br>13.00 – 17.00 |

## SIKÇA SORULAN SORULAR

- **Atölyeye katılmak için ilgili eğitimleri tamamlamak zorunlu mudur?**

Hayır eğitimler tavsiyedir.

- **Atölye duyurusundan tavsiye eğitimi hali hazırda başarıyla tamamlamış ve sertifikalarını almıştım. Başvuru yapabilir miyim?**

Evet. Tavsiye eğitimi tamamlamışsanız yeniden bu eğitimi tamamlamak zorunda olmadan, direk başvuru yapabilirsiniz.

- **Atölyeye grup olarak katılabilir miyiz?**

Hayır. Atölyeye sadece bireysel katılım sağlanabilir.

- **Eğitimleri tamamlayan ve başvuru yapan tüm katılımcılar çevrim içi ön eleme sınavına girebilecek midir?**

Evet. Başvurular sonucunda koşulları sağlayan tüm adaylar Çevrim içi ön eleme aşamasına geçebilecektir.

- **Çevrim içi ön eleme sınavı nasıl gerçekleştirilecektir?**

Ön eleme sınavı www.btkakademi.gov.tr üzerinden Çevrim içi olarak yapılacaktır. Çevrim içi sınava katılmaya hak kazanan adaylara sınav katılım linki, saati ve süreci e-posta ile iletilecektir. Sınav esnasında aldatma ve kopyaya yönelik hareketler tespit edilirse adayın sınavı iptal edilecek ve diskalifiye edilecektir.

# ATÖLYE İÇERİĞİ

| | |
|---|---|
| **1. Giriş ve Temel Kavramlar:**<br>• **Konu Açıklamaları:**<br>o Siber güvenlik ekosistemi ve sızma testinin rolü.<br>o Etik hackerın tanımı ve sorumlulukları.<br>o Sızma testinin iş dünyasına katkıları.<br>• **Canlı Senaryo:**<br>o Bir etik hackerın gerçek dünya senaryosu üzerinden anlatımı.<br>• **Interaktif Öğrenme Aktivitesi:**<br>o Katılımcıların siber güvenlik senaryosunu çözmeleri. | **Bilgi Toplama ve Keşif Aşaması:**<br>• **Konu Açıklamaları:**<br>o OSINT yöntemleri.<br>o Ağ haritalama ve keşif araçları.<br>o Keşfedilen bilgilerin etkin analizi.<br>• **Canlı Senaryo:**<br>o Kamu kaynaklarından elde edilen bilgilerle bir kurumun zayıflıklarının belirlenmesi.<br>• **Interaktif Öğrenme Aktivitesi:**<br>o OSINT araçlarıyla bilgi toplama pratikleri. |
| **3. Zayıflıkların Keşfi ve Analizi:**<br>• **Konu Açıklamaları:**<br>o Zayıflıkların sınıflandırılması ve öncelendirilmesi.<br>o Zayıflık tarama araçları ve metodolojileri.<br>o Zayıflıkların sömürülmesi ve potansiyel tehlikeler.<br>• **Canlı Senaryo:**<br>o Sistemdeki bir zayıflığın tespit edilmesi ve bu zayıflığın nasıl sömürüldüğünün gösterimi.<br>• **Interaktif Öğrenme Aktivitesi:**<br>o Zayıflık tarama araçlarıyla çalışma ve raporlama. | **4. Saldırı Aşaması:**<br>• **Konu Açıklamaları:**<br>o Exploitation teknikleri ve yöntemleri.<br>o Metasploit ve benzeri araçlarla saldırı senaryoları.<br>o Saldırı sonrası sistem kontrolü ve yönetimi.<br>• **Canlı Senaryo:**<br>o Bir saldırı gerçekleştirilerek hedef sistem üzerinde kontrol sağlanması.<br>• **Interaktif Öğrenme Aktivitesi:**<br>o Metasploit ile temel saldırı senaryolarının simülasyonu. |

| | |
|---|---|
| **5. Zafiyetli Makine Çözümleri:**<br>• **Konu Açıklamaları:**<br>o Sanal makineler üzerinde zafiyetli sistemlerin oluşturulması.<br>o Zafiyetli sistemlerde güvenlik açıklarının tespiti.<br>o Pratik zafiyet çözüm senaryoları.<br>• **Canlı Senaryo:**<br>o Zafiyetli bir sistem üzerinde gerçekleştirilen saldırının ardından çözüm adımlarının gösterimi.<br>• **Interaktif Öğrenme Aktivitesi:**<br>o Katılımcılara sunulan zafiyetli sistemlerde uygulamalı çözüm alıştırmaları. | **6. Web Uygulama Güvenliği:**<br>• **Konu Açıklamaları:**<br>o Web uygulama güvenliğinin temel prensipleri.<br>o OWASP standartları.<br>o En yaygın web uygulama saldırıları ve savunma stratejileri.<br>• **Canlı Senaryo:**<br>o Bir web uygulamasındaki zayıf noktaların tespiti ve güvenli hale getirilmesi.<br>• **Interaktif Öğrenme Aktivitesi:**<br>o Web uygulama güvenliği tarama araçlarıyla çalışma ve raporlama. |
| **7. Sürdürülebilirlik ve Raporlama:**<br>• **Konu Açıklamaları:**<br>o Sızma testi raporunun oluşturulması.<br>o İyileştirme önerilerinin detaylandırılması.<br>o Müşteri veya organizasyonla etkileşim stratejileri.<br>• **Canlı Senaryo:**<br>o Bir sızma testi raporunun hazırlanması ve müşteri sunumu.<br>• **Interaktif Öğrenme Aktivitesi:**<br>o Katılımcıların kendi sızma testi raporlarını hazırlamaları ve sunmaları. | |