



CTF (Capture The Flag) Nedir?

CTF (Capture The Flag) yani “**Bayrağı Yakala**”  , siber güvenlik alanında düzenlenen **uygulamalı ve öğretici yarışmalardır**.

Amaç:

Hack alanında öğrenilen teorik bilgilerin pratiğe dökülmesi ve katılımcıların kendilerini gerçek senaryolar üzerinden test etmesidir.

Kimler Katılır?

CTF yarışmalarına katılanlar geniş bir yelpazeye yayılır:

-  Güvenlik uzmanları
-  Etik hackerlar
-  Bilgi güvenliği araştırmacıları
-  Öğrenciler
-  Bireysel katılımcılar
-  Takımlar

 CTF’ler materyal olarak büyük organizasyonlar olmayabilir; ancak teknik yetkinliği ölçen **önemli bir performans göstergesidir**.

Neden Katılmalı?

CTF yarışmaları:

-  Bilgi güvenliği alanında çalışmaya başlamak için faydalıdır.

- 🧠 Teorik bilgiyi pratiğe dönüştürür.
 - 👥 Genellikle takım halinde yapılır.
-

🏆 CTF Türleri

CTF yarışmaları iki ana türe ayrılır:

- 🎯 Jeopardy
 - ⚔️ Attack – Defense
-

🎯 Jeopardy

Bu modelde:

- 📧 Katılımcılara güvenlik soruları gönderilir.
- 🏁 Doğru çözülen her soruda bir “flag” elde edilir.
- 📊 Soruların zorluk seviyeleri ve puanları farklıdır.
- ⛔ Genellikle bir soruyu çözmeden diğerine geçilemez.

💡 Odak: Problem çözme ve teknik bilgi.

⚔️ Attack – Defense

Bu modelde:

- 🛡️ Bir takım sistemi savunur.
- 🎯 Diğer takım saldırı yapar.
- 🔍 Açıkları bulan puan kazanır.
- 🗝️ Savunan ekip zafiyetleri kapatmaya çalışır.

💡 Gerçek dünya siber savaş simülasyonudur.

🔧 Tipik CTF Özellikleri

- 🎤 Genellikle hacking konferanslarında düzenlenir.

- 🧑 Takım olarak yarışılır (Lokal 🌍 veya Uzaktan 🌐).
 - 🧠 Farklı uzmanlık alanları avantaj sağlar.
 - 📌 Takım içi görev dağılımı kritiktir.
-

📁 CTF Kategorileri

- 🌐 Web
 - 📱 Mobile
 - 🗝️ Crypto (Kriptografi)
 - 🧬 Forensics
 - 🌐 Network
 - ⚡ Exploiting
 - 🔁 Reversing
 - 🗄️ Steganography (Bilgi Gizleme)
 - 🧬 Binary Analysis
-

🔧 Yarışmacılardan Beklenen Nitelikler

Başarılı bir CTF oyuncusu:

- 🔍 Açık bulma
- 🧪 Exploit geliştirme
- 🧰 Toolkit geliştirme
- 🧑 Takım çalışması

İdeal olarak ekip üyeleri bu alanların en az birinde uzman olmalıdır.

🔍 Teknik Yetkinlik Alanları

📡 Bilgi Toplama & Network

- 🔍 Port tarama & IPS atlatma

- 🌐 Network analizi ve saldırıları
- 📶 Kablosuz ağılara sızma (WPA/WPA2 kırma)
- 📦 Paket analizi
- 📡 TCP/IP seviyesinde saldırılar

🔑 Saldırı Teknikleri

- 🔑 Brute force & parola saldırıları
- 📁 Wordlist kullanımı
- 🌐 DNS saldırıları
- ⚡ Exploit geliştirme ve kullanma
- 🔍 Zafiyet tespiti (Vulnerability Discovery)

🛡️ Güvenlik Sistemlerini Aşma

- 🔥 Firewall
- 🚨 IDS
- 🚧 IPS
- 🧱 WAF

🧰 Geliştirme

- ⚙️ Süreç içinde ihtiyaç duyulan araçların (toolkit) geliştirilmesi

🎓 CTF'in Kazanımları

CTF katılımcıya şunları kazandırır:

- 🤝 Ekip ruhu & takım çalışması
- ⚡ Hızlı ve çözüm odaklı karar verme
- 🎯 Stratejik bakış açısı
- 💻 Gerçek hacking deneyimi
- 🛡️ Saldırı ve savunma bilgisi
- 🗣️ Yeni teknikler ve güvenlik açıkları hakkında bilgi

- 🕵️ Bir saldırgan gibi düşünebilme becerisi
 - 🏆 Yarışma deneyimi
-

📖 CTF Yarışmalarına Nasıl Hazırlanılır?

1️⃣ Geçmiş Soruları Çöz

- 📁 Önceki CTF sorularını çözerek deneyim kazan.

2️⃣ Uzmanlık Alanı Seç

- 🎯 En az bir kategoride ileri seviyeye gel.

3️⃣ Senaryo Analizi Yap

- 🧠 Önceki CTF metodlarını incele.
- 🧩 Soru hazırlama mantığını analiz et.

4️⃣ Çok Yönlü Ol

- 🌐 Diğer kategoriler hakkında temel bilgi sahibi ol.

5️⃣ Ekip Ruhu Geliştir

- 🤝 Takım içi iletişim kur.
- 📌 Görev paylaşımına adapte ol.