CTF HAKKINDA GENEL BİLGİLENDİRME

İçerikler

1. CTF Nedir?

CTF (Bayrağı Yakala), bir yarışmadır. Bizlere siber güvenlik alanında gizli bir şekilde, birkaç daldan (web zafiyetleri, küresel mühendislik, kriptografi vb. birazdan dalları ince hazırlanır) hazırlanmış olan açık yarışmaya uygun bir şekilde hazırlanır. Bu şekilde tespit edilebilir bayraklar yakalanır ve bir sonraki bayrağa doğru ilerlenir. Amaç, kayıtlı tüm bayrakları yakalayarak yarışmayı tamamlamaktır.

2. CTF'e Kimler Katılabilir?

- Bilgisayar mühendisliği
- Etik hacker adayları
- Siber güvenlik meraklıları
- Kariyerini bu alanda planlayan herkes

CTF yarışmalarına katılanlar, korsanlardan, güvenlik uzmanlarından, bilgi güvenliği araştırma gruplarından, kişilerden, kişilerden kolektif olarak geniş bir yelpazeye yayılıyor.

3. CTF Yarışmalarına Nasıl Hazırlanır?

- Daha önce yapılan açıklamada, CTF yarışlarının ortaya çıkan sorularını çözmeye başlama CTF'te nasıl ve Nereden başlamanın gerekli olduğu hakkında kalıcı olarak oluşturulacaktır.
- Yarışmada ortaya çıkabilen en az birinde uzman gelişmeler ortaya çıkabilir şekilde bilgi sahibi olunmalı.
- CTF yarışmalarında uygulanmış yol, yöntemler ve hangi mantıkla hazırlanmış bilginin incelenip, yarışmada yapılabilecek senoryolara usta olunmalı.
- Sadece bir alanda salgınlar değil diğer alanlarda da bilgi sahibi olunmaktadır.

4. CTF Türleri Nelerdir?

- Jeopardy Tarzı CTF: Farklı kategorilerdeki partiler sunulur. Daha çok bilgi amaçlıdır ve bir nehir bulamadığınızda bir sonraki bayrağa ulaşmak amaç puan toplamak. (Attack-Defense CTF ve Karma CTF için aynısı söylenemez). Görevi bir bayrak içerir ve çözülmüş puan kazanılır.
- Saldırı-Savunma CTF: Takımlar hem kendi sistemini savunur hem de rakip sistemlere saldırır. Bu CTF'te takım, daha çok gerçek zamanlı bir siber savaş deneyimi sunuyor.
- Karma (Karma) CTF: Saldırı-Savunma tehlikeleri barındırır.

a)Tehlike CTF'si

Siber güvenlik alanında bilgi yarışmasıdır ve sunulanların dağılımına göre elektronik puantajlanır. Bu tür, iletilen güvenlik sorularına doğru yanıt vererek adım adım bayrakları yakalamaya çalışır.

Görevi çözüldüğünde, genellikle belirli bir formatta (FLAG{bu_bir_bayraktir}) bulunan bir "bayrak" elde edilir. Yarışmacılar bu bayrak sistemleriyle puan kazanıyor. Yarışmanın sonunda en çok puanı toplayan takım veya kişi kazanan ilan edilir.

- Web, Stego, Misc, OSINT, Forensics, Crypto, Reverse Engineering, Malware ve Pwn dallarından zaafiyet bayraklarını bulmak için Jeopardy CTF'te yarışılır.

b) Saldırı-Savunma CTF

Bu türde, bir takım savunma yaparken diğer takım saldırıları gerçekleştirmektedir. Gruplara ait sistemleri zafiyetleri kapatmaya çalışmak için rakipler açıkları bulmak için uğraşırlar.

Saldırı-Savunma yarışması, takımların yarıştığı bir tür siber güvenlik mücadelesidir.

c) Karma (Karma/Hibrit) CTF

Jeopardy ve Attack-Defense ile karışık bir şekilde yarışmaların hazırlanması ve mevcut bu zorlu karma yarışının devamı için bayrak kovaları.

5. CTF'in Avantajları

-Ekip ruhu
- Çözüm odaklı geçme
- Stratejik bakış açısı geliştirme
- Hacking deneyimi
- Saldırı ve Koruma için güvenlik bilgisi edinilmesi
- Teknik bilgiler bilgileri öğrenme

6. Tipik CTF Özellikleri

- Hacking konferansları bünyesinde bulunmaktadır.
- Takım olarak yarışılır. (Çevrimdışı ya da Çevrimiçi)
- Farklı özelliklerde uzman olan kişilerin takımınızda olması bir avantaj sağlar.
- Takım içi iş paylaşımı önemlidir.

7. CTF Katagorileri

- Web Güvenliği (Web Kullanımı/Web)
- Tersine Mühendislik (Tersine Mühendislik/Rev):
- Mobil
- Kriptografi (Kriptografi/Kripto)
- Adli Bilişim (Adli Bilişim)
- Açık Kaynak İstihbaratı (OSINT — Açık Kaynak İstihbaratı)
- Ağ (Ağ)
- Steganografi (Bilgi gizleme)
- İkili Sömürü (İkili Sömürü/Pwn)

8. CTF Yapabileceğimiz Araçlar Nelerdir?

Web Güvenliği için “Burp Suite Community Edition”

Tersine Mühendislik için“Ghidra”

Mobil için , Jadx / JAD

Kriptografi için, CyberChef

Adli Bilişim için, Wireshark

Açık Kaynak İstihbaratı için , Google Dorking

Network (Ağ) için, Nmap veya Wireshark

Steganografi için, steghide

Binary Exploitation/Pwn için , “GDB (GNU Debugger) + Pwndbg/Gef/Vim-Pwn”

Araçların kullanılabilirliği.

9. CTF'e Hızlandırmak İçin Antreman Yapabileceğimiz Web Siteleri?

- **OverTheWire: Seviye Hedefi**

Bu seviyenin amacı SSH kullanarak oyuna giriş yapmanızdır. Bağlanmanız gereken ana bilgisayar...

overthewire.org

- **picoCTF - CMU Siber Güvenlik Yarışması**

picoCTF, capture-the-flag çerçevesi üzerine kurulu, özgün içeriklere sahip, ücretsiz bir bilgisayar güvenliği eğitim programıdır...

picoctf.org

- **pwn.kolej**

Hacklemeyi Öğrenin!

pwn.kolej

- **Google CTF**

Açıklamayı düzenle

capturetheflag.withgoogle.com

- https://www.centralinfosec.com/

- **Ekose CTF 2025**

Açıklamayı düzenle

ekosectf.com

- **Bayrağı Yakala (CTF)**

CTF, BSidesSF 2025'te geri dönecek!Nasıl oynanır?2025 CTF'miz 25 Nisan Cuma günü, PDT ile 16:00'da başlayacak ve...

bsidessf.org

10. Ayrıca Bakmanızı Tavsiye Ettiğim

- https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/ (Ulusal Güvenlik Ajansı / ABD)
- https://www.enisa.europa.eu/ (Avrupa Birliği Siber Güvenlik Ajansı)
- https://muhammetadibas.com.tr/arsiv/ctf-yarismalari-nedir-nasil-hazirlanilir/

11. Son

Türkiye'de de STM CTF, TÜBİTAK BİLGEM CTF, İTÜ CTF gibi birçok popüler CTF yarışması düzenlenmektedir. Belki bir gün aynı takımda veya rakip takımda karşılaşırız :)

Amaçlar:

- Siber güvenlik uygulamaları konusunda bilmediklerinizi öğrenmeli, öğrendiklerinizi pekiştirmek ve gelişmenizi sağlamak için CTF çözmelidir.
- Baskı altında takımın çalışması ve problemin çözülmesini hızlandırır.

Kaynakça

- https://www.inetmar.com/blog/ctf-nedir-ne-ise-yarar/#ctf8217ye-kimler-katilmali
- https://www.beyaz.net/tr/guvenlik/makaleler/ctf_nedir.html
- https://en.wikipedia.org/wiki/Capture_the_flag_(siber_güvenlik)
- https://muhammetadibas.com.tr/arsiv/ctf-yarismalari-nedir-nasil-hazirlanilir/
- https://www.quora.com/Saldırı-Savunması-CTF-Nedir
- https://trailhead.salesforce.com/content/learn/modules/capture-the-flag-activities/get-started-with-capture-the-flag