

ANKARA UNIVERSITY CYBER CLUB

CAPTURE THE FLAG



CAPTURE THE FLAG

BAYRAĞI YAKALA





- → Geçmişi Roma dönemine kadar dayanır
- → Dönemin gençleri arasında CTF yarışmaları yapılarak savaşa hazırlık
- → Amaç teoriyi pratiğe dökmektir
- → Katılımcılar genellikle
 - ◆ Siber güvenlik uzmanları
 - Öğrenciler
 - hackerlar
- → Belirli bir süre vardır



~ baslik

Jeopardy

Farklı kategorilerde siber güvenlik ile ilgili teknik/teorik soruları çözerek bayrak elde edilmeye çalışılır. Genel işleyiş birbiri ile bağlantılı sorulardan oluşur. Adım adım devam edilir.

Attack - Defense

Ekipler rakiplerinin sistemlerini ele geçirip bayrağı yakalamaya çalışırken kendi sistemlerini de saldırılara karşı savunurlar.



Kategoriler:

- → Web
- → Kriptografi
- → Forensics
- → Network
- → Exploiting
- → Reversing
- → Steganography
- → Mobile

Ne gerekir?

- → Açıklık bulma yeteneği
- → Exploit geliştirme yeteneği
- → Custom tool geliştirme yet.
- → Grup çalışması becerisi
- → En az bir alanda uzmanlık
 - ideali her alan



CTF Yarışmalarının içerdiği aksiyonlar

- → Bilgi toplama (Aktif/Pasif)
- → IPS/IDS bypass
- → Network analizi/saldırısı
- → Kablosuz ağlara sızma WPA/WPA2
- → Paket analizi
- → Kaba kuvvet
- → Exploit geliştirme ve kullanma



Genel yapı

- → Genelde Hacking Konferanslarında düzenlenir
- → Takım olarak yarışılır
- → Minimum 1, max. 7 gün sürer
- → Saldırgan bakış açısı kazanılır
- → Hem saldırı hem savunma için bilginizi arttırırsınız
- → TAKIM ÇALIŞMASI ÖĞRENİLİR
- → Uluslarası yarışmalarda özgüven ve tecrübe kazanılır

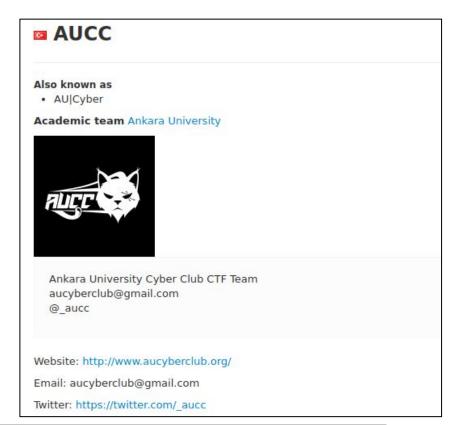


Nasıl hazırlanılır?

- → Kendi Lab ortamınızı hazırlayın
- → Daha önce sorulmuş soruların çözümlerini inceleyin
- → En azından bir alanda uzmanlık seviyesinde teorik bilgiye sahip olunmalı
- → CTF'ler takip edilmeli : https://ctftime.org/
- → Wargames soruları üzerine uğraşılmalı : http://overthewire.org/wargames/



AUCC CTF Ekibi





CTFTime

Position	Country position	Name	Points	Events
182	1	YubitSec	19.237	10
223	2	BreakPoint	15.895	2
426	3	lost+found	8.333	6
572	4	AUCC	5.394	7
643	5	67meem67	4.612	5
1002	6	Infected	2.086	3
1379	7	NavSec	1.051	1



Writeup / Walkthrough yazılarının bulunabileceği kaynaklar

- → https://ctftime.org/writeups
- → https://github.com/ctfs
- → https://www.reddit.com/r/securityCTF/
- → https://ctf.rip/
- → http://mslc.ctf.su/
- → http://tasteless.eu/
- → https://trailofbits.github.io/ctf/