VAHAP EREN • AHMET KOMUT • YUSUF CAN ÇAKIR

UYGULAMALI SİBER GÜVENLİK VE SIZMA TESTİ EĞİTİMLERİ

CAPTURE THE FLAG ÇÖZÜMLERİ

hayykitap

YAYINA HAZIRLAYANLAR
OĞULCAN ÖZDEMİR • OZAN ÜNAL • İSMAİL BÜLBÜL • SUAT SEZGİN

Hayykitap - 760
Bize Söylenmeyenler - 60

Uygulamalı Siber Güvenlik ve Sızma Testi Eğitimleri
Vahap Eren - Ahmet Komut - Yusuf Can Çakır

Yayına Hazırlayanlar:
Oğulcan Özdemir, Ozan Ünal, İsmail Bülbül, Suat Sezgin

Editörler:
Kürşat Tatlıcan, Eren Yılmaz, Hulusi Bindebir, Ahmet Ufuk Yavuzer, Eren Öztürk, Furkan Öztürk

Kapak ve Sayfa Tasarımı: Turgut Kasay

ISBN: 978-625-7909-64-8
1. Baskı: İstanbul, Temmuz 2020

Baskı: Yıkılmazlar Basım Yay.
Prom. ve Kağıt San. Tic. Ltd. Şti.
15 Temmuz Mah. Gülbahar Cad. No: 62/B
Güneşli - İstanbul
Sertifika No: 45464
Tel: 0212 630 64 73

Hayykitap
Zeytinoğlu Cad. Şehit Erdoğan İban Sk.
No: 36 Akatlar, Beşiktaş 34335 İstanbul
Tel: 0212 352 00 50 Faks: 0212 352 00 51
info@hayykitap.com
www.hayykitap.com
facebook.com/hayykitap
twitter.com/hayykitap
instagram.com/hayykitap
Sertifika No: 12408

Vahap Eren - Ahmet Komut - Yusuf Can Çakır

UYGULAMALI SİBER GÜVENLİK VE SIZMA TESTİ EĞİTİMLERİ

Capture The Flag Çözümleri

Vahap Eren

Siber güvenlik uzmanı, yazar. 1987 doğumlu. Ağ ve bilgisayar sistemleri, bilgisayar programcılığı, yazılım geliştirme ve veri tabanı yönetimi konularında birçok kurum ve özel kuruluşa destek verdi. 2006 yılından beri aktif olarak çeşitli siber güvenlik pozisyonlarında yer aldı.

2015 yılında Siber Güvenlik Teknolojileri Derneği'nin kurucuları arasında yer aldı ve Türkiye'de siber güvenlik alanında dernek kuran ilk birkaç kişiden biri oldu. 2017 yılında Türkiye'deki ilk Siber Güvenlik Federasyonu'nun kurucular listesinde yer alarak 2 yıl kadar Kurucu Genel Sekreter görevini yürüttü. Ulusal ve uluslararası birçok kuruluşa ait sitelerde güvenlik açığı bularak bunları bildirdi. Birçok haber yayın organında haber oldu. Siber güvenlik alanlarında uluslararası alanda geçerli olan CISA ve CEH sertifikalarına sahiptir.

Halen birçok teknoloji, siber güvenlik etkinliğine ve konferanslarına konuşmacı olarak katılmaktadır.

Ahmet Komut

1983 Kocaeli doğumlu olan yazar ilk, ortaokul ve liseyi Kocaeli'nde okuduktan sonra çeşitli siber güvenlik firmalarında çalışmaya başladı. Daha çok Linux ve Siber Güvenlik alanında çalışmalar yaptı. Çeşitli platformlarda online olarak eğitimler, konferanslar, seminerler verdi. Şu anda siber güvenlik araştırmacısı olarak çalışmalarına devam ediyor.

Yusuf Can Çakır

2001 Balıkesir doğumlu. İlk ve ortaöğretimini Balıkesir Merkez'de tamamladı. Babasının mesleğinden dolayı bilgisayarla küçük yaşta tanıştı ve küçüklüğünden beri bilgisayar ile içli dışlı oldu. Bilgisayarın çalışma mantığı ve mimari yapısını merak etmesi, bu alanda ilerlemesine yardımcı oldu. Lise sona doğru siber güvenliğe ilgisinin olduğunu fark etti ve bu alanda çalışmalar yapmaya başladı. Özellikle Windows mimarisi ve adli bilişim alanları ilgisini çekiyor.

İçindekiler

Önsöz

Siber güvenlik, son yıllarda adından sıkça söz ettirir oldu. Bu alanda ülkeler önlemler alıyor, hacker orduları kuruluyor, zararı milyonlarca dolara ulaşabilen siber saldırılar gerçekleşiyor...

İnternet ve ağlar hayatımızın bir parçası olduğu sürece bu saldırılar gerçekleşecek ve karşılıklı savaş devam edecek. Bu savaşta önlemlerimizi alıp siber güvenliğimizi sağlamak zorundayız. Peki önemi her geçen gün daha iyi anlaşılan bu alanda neredeyiz diye hiç düşündünüz mü?

Siber güvenlik bilincinin artmasıyla birlikte eğitimler ve yatırımlar da hayli arttı. Eğitici dersler, konferanslar ve birçok etkinlik yapılıyor. Peki teorik olarak öğrendiğimiz, nasıl kullanacağımızı bilmediğimiz bu bilgiler bize ne katıyor? Çoğu zaman hiçbir şey... Bu durumda öğrendiklerimizi uygulamak mecburiyetinde kalıyoruz ve yardımımıza CTF'ler yetişiyor.

CTF (Capture The Flag), Türkçeye "Bayrağı Ele Geçirme, Bayrağı Yakalama" olarak geçen, katılanlara öğrendikleri teorik bilgileri uygulama fırsatı sunan ve farklı bakış açıları kazandırmayı amaçlayan öğretici siber güvenlik yarışmalarıdır. "Uygulamalı Siber Güvenlik ve Sızma Testi Eğitimleri" kitabı sayesinde siber güvenlikte vazgeçilmez olan CTF'lere adım atacak, kitapta yer alan örneklerle öğrendiklerinizi uygulama imkanı bulabileceksiniz.

Hulusi BİNDEBİR

Birinci Bölüm

CTF'E GENEL BAKIŞ

1.1. CTF Nedir, Ne Değildir?

"Capture the Flag" teriminin her kelimesinin baş harflerini yan yana getirdiğiniz vakit elde edeceğiniz kısaltmadır CTF. Dilimize "bayrak kapmaca" olarak çevrilebilecek olan bu kelime dizisi, karşı takımın bayrağını elde etme çabasına dayanan takımlar arası bir mücadeleyi simgeler. Her kelimenin bağlamına göre büründüğü anlamlar olduğu gibi CTF de kullanıldığı yere göre bambaşka kılıflara girer. Bu kitabın konusunu meydana getirecek olan anlamı ise bir tip bilgisayar güvenliği yarışmasıdır.

Katılımcılara farklı bakış açıları kazandırmayı prensip edinmiş olan ve kendilerini sınama olanağı sunan bu siber güvenlik yarışmaları, genel olarak içerisinde teorik birikimin uygulanmasını talep eden sorular barındırır. Değişkenlik gösteren formatlarda yayımlanıp literatürün çeşitli başlıklarına hitap eden bu sorulara verilen yanıtlarla "bayraklar toplanır", bunların bildirimi neticesinde de katılımcılar bir sıralamaya yansıtılırlar. Sonuç olarak bir sürenin ardından şekillenen tablo referans alınarak sıralamanın belli bir kesiminde yer eden katılımcılara, organizasyon sorumlularınca vadedilen ödüllendirmeler yapılır.

CTF'in kelimeler ile olası bir tarifi budur, ne olmadığına dair soruşturma girişimi ise elbet havada kalacaktır. Retorik yapmak gerekirse, örneğin "CTF metafizik bir anlama sahip değildir" demek görece hatalı bir yargı olacaktır. Katılım bir ekip ile sağlanmış ise ekip bünyesindeki bireyler arasındaki sembolik bağı kuvvetlendirir. Yazılı, sabit bir öğretisi olmasa da kişilere araştırmayı, sabretmeyi öğütler; bazenleri bildiklerimizin, geri kalanı ile kıyasla bir hiç olduğunu tekrar tekrar anımsatır. Bazıları için yaşantının baskısından anlık bir sıyrılıştır. Kim bilir, belki birileri için "bir bütün, bütün ise birdir" söyleminin somut bir karşılığıdır. Bu biçim keyfi sürdürülebilecek olan bir dizi argümanla CTF'in çeşitli kesimlerce anlamı, ne olup ne olmadığı dilenen yere çekilebilir. Okuyucudan tarafımızca sezdirilecek olan CTF sürecinin ardından, bu soruya bizzat yanıt bulması beklenmektedir.

1.2. CTF'e Katılmak İçin Sebepler

İnsan eylemleri pragmatiktir. Her türlü yönelimi, attığı her adım esasında benliğin tatminine hizmet eder. Katılımın ardındaki motivasyon da haliyle katılımcının beklentilerine göre değişkenlik gösterecektir. CTF ile türevi yarışmaların maneviyatta vadettikleri ve hatta sundukları bir

kesimi doyursa da daha geniş kitlelerin ilgisini çekmek, rekabeti artırmak maksadıyla ortaya bir ödül konmasına ihtiyaç vardır. Bu vaat ile ödüllendirmenin koşulları organizasyon sahibi oluşum tarafından yarışma öncesinde ilan edilir. Maddi ve manevi teşvik unsurlarıyla harmanlanmış bir reklamın ardından etkinlikten haberdar olan potansiyel katılımcının kendi sebebini bizzat kendisinin bulması gerekse de, elbette bizim de önerilerimiz olacak.

1. **Haz.** Kendinize uygun olan bir CTF etkinliğine katılmanız durumunda karşılaşacağınız sorular baş edebileceğiniz düzeyde olacaktır. Bir uğraşının ardından yer verilen problemlere çözüm getirebilmenin verdiği haz, bizden söylemesi, katılıma değecektir.
2. **Sürpriz.** Verinin anlamlandırılmasıyla elde edilen, kişinin ihtiyaç duyduğundan bir haber olduğu bilgi, ne var ki bazenleri verideki fazlalıktan ve gürültüden ötürü fark edilesi olmayan bir detay olduğuyla kalır. Genellikle uzun soluklu literatür karıştırmalarından meydana gelen CTF sorularında bu bilginin net bir biçimde sunulmuş olması mümkündür, beklenmedik arayışa oracıkta cevap verir.
3. **Dayanışma.** Etkinliğe katılım bir ekip gerektiriyorsa, halihazırda bir ekip bünyesinde de yer alıyorsanız, takım içerisindeki her bir kimsenin kendi odaklandığı kategoriyle cebelleşmesi ve bazı soruların ekip arasında tartışılması kaçınılmazdır. Her iki durumda da biçilen puan havuzuna katkıda bulunmanın, bir ekibe dahil, kısaca dayanışma içerisinde olmanın bilinci dikkate değer.
4. **Ölçüm.** Uygulamada olası senaryolara çözüm getirebilme kabiliyeti, pratikteki yetkinlik teorik birikimin kişi tarafından verimli kullanılabilirliğiyle alakalı bir durumdur. Ne var ki bahsedilen yeti yine pratikle geliştirilir. Kısıtlı zaman içerisinde, rekabetten ötürü baskı altında iken sunulan özgün bir probleme çözüm getirme çabası şahsın kendini sınayabilmesi için uygun ortamı sunmaktadır.
5. **Ödül.** Tüm manevi getirileri bir yana, CTF etkinliğinde başarı gösteren bireylere vadedilen ödül de katılım göstermeniz için bir sebep olabilir. Para ödülünden sertifikaya, donanımdan hizmete değişkenlik gösteren ödül yelpazesindeki seçim elbet organizasyonu düzenleyen oluşumun takdirindedir.

İtibar, referans ve bunların haricindeki sayısız kavram katılımınızın nedeni olabilir. Sebebinize dair seçim her ne olursa olsun, CTF'in geleneksel anlamına sadık kalıp eğlenmeyi ihmal etmemeniz önerilmektedir. Her şey bir yana, bir perspektiften de bu yalnızca bir oyundur.

1.3. CTF'in Özellikleri

Bilgisayar güvenliği kapsamında düzenlenen CTF etkinlikleri çevrimiçi yahut çevrimdışı olabilmektedir. Çevrimiçi olması durumunda problemler bir platform üstünden yayımlanır. Genellikle internet ağından erişilebilir bir sayfa üstünden çeşitli formatlarla sunulan problemler, o ağa bağlı herhangi bir hizmet alıcısı için belli bir süre boyunca erişilebilir durumda olur. Çevrimdışı tipinde ise katılımcıların belli bir yer ve zamanda fiziksel olarak bulunmaları, toplanmaları istenir. Her iki tip düzenlenen etkinlikte de katılımın sıklıkla belli kişi sayılı takımlar halinde sağlanması beklenmektedir. Tüm bu değişkenlik gösteren katılım şartlarından ötürü katılacağınız etkinliğin önceden yayımlanan yönergelerini gözden geçirmeniz önerilir.

En yaygın formuyla bir bayrak kapma mücadelesinde sorular çeşitli kategoriler altında derlenerek yayımlanırlar. Bu kategoriler "web uygulama güvenliği (web), ağ mimarileri (network), tersine mühendislik yahut veri analizi (reverse engineering, binary analysis), açık kaynak istihbaratı (OSINT), steganografi" veya "ortaya karışık (misc.)" olabilmektedir. Meselenin teorisi ve paradigması, tanımları üstüne dilediğimiz kadar konuşalım; öğrenimin en verimli biçimiyle pratiklerle, "CTF ruhunun" bizzat sahadan örneklerle sezdirilmesiyle gerçekleştiğine dair inancımızdan ötürü ilerleyen bölümlerde bu kategorileri, yine örnekler üstünden ele alacağız.

VAHAP EREN • AHMET KOMUT • YUSUF CAN ÇAKIR

UYGULAMALI SİBER GÜVENLİK VE SIZMA TESTİ EĞİTİMLERİ

CAPTURE THE FLAG ÇÖZÜMLERİ

"Her geçen gün daha fazla online cihazın hayatlarımıza girmesi siber riskleri de beraberinde getiriyor. İnternet kullanımı*; bilgisayar, laptop ve tabletlerden kapalı devre televizyon sistemlerine, kameralara, medikal ekipmanlara, ev ekosistemlerine ve otonom endüstrilere doğru bir gelişme göstermiştir. Bu durum, sistemlerin güvenliğini yeterince sağlayamazsak acemi kullanıcıların daha fazla zarar görmesine neden olmaktadır. Bizlerin bu konuda uzmanlığımızı geliştirerek, eksiklikleri telafi etmemiz gerekmektedir. Oluşabilecek zararları en aza indirmek ve hafifletebilmek için siber savaşçılara ihtiyacımız vardır.*

Böyle bir uzmanlık ve beceri yalnızca deneyim ve uygulama ile mümkün olabilir. CTF yani Capture The Flag (Bilgisayar Güvenliği Yarışmaları) siber güvenlik ile alakalı bir dizi beceriyi öğrenmek ve bunun yanı sıra bunları geliştirmek için fırsatlar sunmaktadır.

Capture The Flag, üç farklı formda gerçekleştirilen bir çeşit bilgisayar güvenliği yarışmasıdır. *Bunlar; saldırı/savunma, donanım mücadelesi ve risktir. Saldırı/savunma formunda bir takımın kendi sistemini, saldıran bir diğer sistemden koruması gerekmektedir. Donanım mücadelesi sisteminde, takıma güvenliği aşmaları/atlatmaları için bilinmeyen bir donanım verilmektedir. Risk mücadelesinde ise bir takımın belirli bir zaman diliminde bir dizi zorlukla yüzleşmeleri gerekmektedir."*

Raj Chandel

Siber güvenlik ve sızma testi alanında yeterli profesyonelliğin kazanılması için muhakkak uygulamalı eğitimler ve laboratuvar ortamının olması gerekiyor. Teknik bir alan olmasından dolayı teorik verilen eğitimler, yeterli kabiliyette insan kaynağının oluşmasında yetersiz kalıyor. Laboratuvar ortamında gerçekleştirilmiş ofansif atakları kitabımıza aktararak okurların maksimum seviyede bilgiye ulaşmasını sağlamayı amaçladık. Teknik kabiliyetinizi geliştireceğiniz ve çeşitli örneklerin nasıl çözüleceğini öğreneceğiniz bir kaynak oluşturduk.

hayykitap

ISBN: 978-625-7909-64-8

32 TL
KDV'DEN MUAFTIR