Siber Güvenlik Bayrağı Yakala (CTF - Capture The Flag) Yarışması Şartnamesi

Kocaeli Büyükşehir Belediyesi ve Kocaeli İl Milli Eğitim Müdürlüğü tarafından bu yıl ilki düzenlenecek Siber Güvenlik Bayrağı Yakala (Capture The Flag) yarışması Tübitak Bilgem Siber Güvenlik Enstitüsü tarafından geliştirilen Sanal Siber Güvenlik Laboratuvarı (Siberlab) katkılarıyla liseler arasında yapılacaktır.

Siber Güvenlik Bayrağı Yakala (CTF - Capture The Flag) yarışması, bilgisayar güvenliği ile ilgili zorluklar ve görevler içeren bir yarışmadır. Katılımcılar, belirli hedefleri tamamlamak için çeşitli yöntemler kullanarak mücadele ederler.

Siber güvenlik; bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü amaçlı saldırılardan koruma uygulamasıdır. Bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinir. Bu terim, işletmelerden mobil bilgi işleme kadar çeşitli bağlamlarda geçerlidir ve birkaç ortak kategoriye ayrılabilir.

- **Ağ güvenliği**, hedefli saldırganlar veya fırsatçı kötü amaçlı yazılımlar olması fark etmeksizin bir bilgisayar ağını davetsiz misafirlerden koruma uygulamasıdır.
- **Uygulama güvenliği**, yazılım ve cihazların tehditlerden etkilenmemesine odaklanır. Ele geçirilmiş bir uygulama, korumak için tasarlanan verilere erişim sağlayabilir. Başarılı güvenlik, daha tasarım aşamasındayken bir program veya cihaz dağıtılmadan önce başlar.
- **Bilgi güvenliği**, hem depolama hem de aktarma sırasında verilerin bütünlüğünü ve gizliliğini korur.
- **Operasyonel güvenlik**, veri varlıklarının işlenmesi ve korunmasına ilişkin süreçleri ve kararları içerir. Kullanıcıların bir ağa erişirken sahip oldukları izinler ve verilerin nasıl ve nerede depolanabileceğini veya paylaşılabileceğini belirleyen prosedürler bu kapsama girer.

Son dönemde tüm dünyada olduğu gibi, ülkemize karşı yapılan siber saldırılarda da artışlar yaşanmaktadır. Bu saldırılara karşı koyabilmek, saldırganların saldırı metodolojilerini anlamak, bu konuda uygulamalar yapmak ve saldırılara karşı koyabilecek yetenek ve kabiliyetlerin sayısını artırmak ile mümkün olabilecektir.

- Genel olarak yarışma içeriği şu başlıkları içermektedir;

Kriptoloji: Çeşitli kriptoloji yöntemlerini kullanarak hazırlanmış soruların kripto analiz ve kaba kuvvet saldırıları gibi yöntemlerle kırılması sonrasında bayrağın elde edildiği yarışma kategorisidir.

Forensics: Dosya formatı analizi, stenografi, hafıza dökümü analizi gibi uygulamalardan sonra bayrağın elde edildiği yarışma kategorisidir.

Reverse: Yarışmacılara verilen uygulamaların tersine mühendislik yöntemleri ile kaynak kodlarına ulaşmaları ve kodun analizi ile bayrağın bulunması beklenen yarışma kategorisidir.

Web: Web yazılımlarında bulunan güvenlik zafiyetlerinin bulunması, bulunan zafiyetler üzerinden bayrağın elde edildiği yarışma kategorisidir.

Network: Network hareketlerinin incelenmesi sonucunda elde edilen bilgiler ile bayrağa ulaşılması beklenen yarışma kategorisidir.

Gençlerimizin ilgisini bu alana çekmek ve siber saldırılarla mücadele edebilecek insan kaynağı geliştirmek amacıyla Siber Güvenlik Bayrağı Yakala (Capture The Flag) Yarışması düzenlenecektir. Kriptoloji, forensics, reverse ve web gibi konular üzerinden hazırlanan soruların yarışmacılar tarafından çözülmesi beklenmektedir.

- Yarışma, ülke genelinde lise öğrencilerinin katılımlarıyla gerçekleşecektir. Öğrencilerin danışman öğretmenleri ile birlikte 1 kişi, 1 danışman şeklinde başvuru yapmaları gerekmektedir.
- Yarışma 30 takım ile sınırlıdır.
- Yarışmada ilk 3 dereceye giren öğrencilere hediyeler verilecektir. Hediyeler Kocaeli Büyükşehir Belediyesi tarafından temin edilecek olup, Kocaeli İl Milli Eğitim Müdürlüğü marifetiyle dağıtımı sağlanacaktır.
- **Yarışma Organizasyon Komitesi**
  - Kocaeli Büyükşehir Belediyesi
  - Kocaeli İl Milli Eğitim Müdürlüğü personellerinden oluşmaktadır. Bu yarışmada Tübitak Bilgem Siber Güvenlik Enstitüsü yarışma yürütücüsü ve paydaşıdır.

- **Yarışma Takvimi:**
  - Online Sınav Tarihi: 2 Ekim 2023 (Pazartesi) Saat:10:00-11:00 (Bu saat aralığı haricinde sınava katılım yapılamayacaktır.)
  - Yarışma Günü: 23 Ekim 2023 (08:30-9:20 Kayıt, 9:30-10:00 Kontrol ve Bilgisayarların sisteme bağlanması, 10:00 Yarışma Başlangıç, 13:00-13:30 Yemek İkramı, 18:00 Yarışma Bitiş ve Sonuçların İlanı)
  - Yarışma sonucuna itiraz halinde komisyon tarafından değerlendirilecektir.
  - Yarışma başvuruları https://ebelediye.kocaeli.bel.tr/KulturSosyal/CTFBasvuru adresinden yapılacaktır.
- **Yarışma Yeri:** Kocaeli Kongre Merkezi
- **ÖDÜLLER;**
- **Derece alan öğrenciler;**
- Birinci olan öğrenciye Bilgisayar
- İkinci olan öğrenciye Tablet
- Üçüncü olan öğrenciye Rasperry Pi Seti
- **Derece alan Danışman öğretmenler;**
- Birinci olan öğretmene Tablet
- İkinci olan öğretmene e-kitap okuyucu
- Üçüncü olan danışmana Akıllı Saat hediyeleri verilecektir.
- **ÖDÜL TÖRENİ**

  23 Ekim 2023 tarihinde gerçekleştirilecektir.

Siber Güvenlik Bayrağı Yakala Yarışması Yönergesi

- Bu yarışmaya katılım ücretsizdir. Katılım gönüllülük esası ile yapılır. Yarışmaların planlanması, tanıtılması ve uygulanması eğitim ve öğretim aksatılmadan yapılacaktır.
- Engelli bireylerin etkinliğe katılımını teşvik edilecek, kolaylaştırıcı ve etkinlikten azami şekilde faydalanmalarını sağlayıcı tedbirleri alınacaktır.
- Yarışmaya, yarışma günü itibariye Milli Eğitim Bakanlığı'na bağlı okullarda kayıtlı lise öğrencileri başvurabilir. Katılımcıların çalışmalarının dereceye girmesi

durumunda katılımcılardan ayrıca öğrenim belgelerini ibraz etmeleri istenecektir. Ödülleri kanuni temsilcileri (veli/danışman öğretmen) ile birlikte verilecektir. Yarışmada dereceye giren takımlara belirtilen ödüller verilir. Ödülün dağıtımından danışman öğretmen ve okul idaresi sorumludur.

- Yarışmaya 1 kişilik takımlar halinde katılım yapılması gerekmektedir. Ekip danışman öğretmen ve 1 öğrenciden oluşacaktır. Yarışma alanında öğrenciler bulunacaktır.
- Yarışmacıya masa, elektrik ve internet bağlantısı sağlanır.
- Katılan her yarışmacı kayıt yaptırmak zorundadır. Kayıt yaptıran kişiler bilgilerin doğruluğunu önceden kabul eder. Yanlış bilgi verildiği tespit edildiği takdirde yarışmacı ve takımı yarışmadan elenir. Takım dereceye girmiş olsa dahi derece ödülleri geri alınır.
- Yarışma lise öğrencilerine yöneliktir.
- Yarışma ilk 30 takım arasında yapılacaktır. İlk 30'a giren kişiler kodeli.kocaeli.bel.tr sitesi üzerinden ilan edilecektir. Puanlarda eşitlik olması durumunda yaş olarak küçük yaşa öncelik sağlanır ve sıralamada önce geçer.
- Yarışmaya belirlenen yarışmacı sayısından fazla başvuru yapılırsa, müracaat eden takımlar arasında ön eleme yapılacaktır. Ön eleme sınavı ilan edilen tarihte online platform üzerinden yapılacaktır. Örnek sorular aşağıda verilmiştir.
- Yarışmacılar yarışmada kendi bilgisayarlarını getirecektir. Makinelerde Windows işletim sistemi kurulu olması tavsiye edilir.
- Yarışma belirlenen saatler arasında, belirlenen kurallar ile yapılır.
- Yarışmaya katılacak takımların belirtilen saatte ve yerde hazır olmaları gerekmektedir.
- Geciken takımlar yarışmaya alınmaz. Gecikmelerden takımlar kendileri sorumludur.
- Yarışmacılara ulaşım ve konaklama desteği verilmez. Yarışmacılar kendi masraflarını kendileri karşılar.
- Yarışmacı yarışma süresince, verilen yaka kartını kullanmak zorundadır.
- Yeterli başvuru olmaması ve benzeri durumlarda Yarışma Organizasyon Komitesi, Milli Eğitim Bakanlığı bilgisi dahilinde yarışmayı iptal etme yetkisi vardır.
- Yarışma Organizasyon Komitesi, Milli Eğitim Bakanlığı bilgisi dahilinde bu yönerge maddelerinde yarışma gününe kadar değişiklik yapma hakkını saklı tutar.
- Yarışma kapsamında Siber Güvenlik Enstitüsü tarafından geliştirilen Sanal Siber Güvenlik Laboratuvarı (Siberlab) ürünü kullanılacaktır.
- Her yarışmacı için birbirinden izole; sanal makine ve ağ cihazlarından oluşan birer sanal ortam oluşturulacaktır.
- Yarışmacıların sorulara girdiği cevaplar Siberlab arayüzü üzerinde takip edilecek, değerlendirilecek ve bir skor tablosu oluşturulacaktır.
- Yarışma sonrasında oluşan skor tablosu yarışmacılar ile paylaşılacaktır.
- Siberlab ortamına yalnızca yarışma zaman dilimi içerisinde erişim sağlanacaktır.
- Yarışmadan sonraki 1 gün süre ile sistem açık kalacaktır.
- İş bu yönerge, Yarışma Organizasyon Komitesi ve Tübitak Bilgem Siber Güvenlik Enstitüsü tarafından yürütülür.

Değerlendirme Kriterleri

1. Adım (20 puan) :

İlk olarak nmap taraması yapılır. Ardından açık olan portlar bulunur. Örneğin 80,21,443,9099 numaralı portlar açık durumdadır. Sonrasında her bir porta ayrı ayrı tarama yapılıp portlarda çalışan uygulamalar bulunur. Bizim bölümdeki bayrağımız SSH servisimizin default 22 portunda değil onun yerine açık olan 9099 portumuzda servis sağladığıdır. SSH bağlantımız 9099 numaralı porttan yapılacaktır.

2. Adım (20 puan) :

Bu adımda ise tüm portlara dizin taraması yapılır. Yapılan dizin taraması (gobuster) sonucunda 80 numaralı portumuzda robots.txt diye bir dizin karşımıza çıkıyor.

3. Adım (30 puan):

Bulduğumuz bu robots.txt okunduğunda ise içerisinde bizim DES ile şifrelenmiş ssh şifemiz ve kullanıcı ismimiz oluyor. Bulunan bu SSH şifremizin DES şifrelemesindeki secret bölümü ise makinamızdaki kullanıcılardan birinin ismi olur. Örneğin “user”. Bu DES ile şifrelenmiş anahtarı çözmek için online web sitelerinden yardım alınabilir, secret kısmına kullanıcımız olan user yazılır. Ardından şifre çözülür ve SSH şifresi ele geçirilmiş olur.

4. Adım(30 puan):

SSH şifresini ele geçirdikten sonra SSH servisinin çalıştığı 9099 portu üzerinden “user” kullanıcımız ve şifremiz ile SSH bağlantısı gerçekleştirilir. SSH bağlantısını başarılı bir şekilde gerçekleştirdik fakat bizim bağlandığımız kullanıcı olan “user” yetkisiz bir kullanıcıdır. Bundan dolayı kullanıcı listesine bakılır. Listeye baktıktan sonra “toor” adına root yetkili bir kullanıcı bulunur fakat şifresi bilinmiyordur. Ardından bu kullanıcıya geçiş yapabilmek için rockyou.txt kullanılarak hydra ya da başka bir araç ile brute force saldırısı gerçekleştirilir. Tebrikler artık root yetkisine sahip bir kullanıcı oldunuz. Son olarak toor kullanıcısının masaüstünde olan son.txt okunur “Tebrikler! Yarışmayı başarıyla tamamladınız.”

Siber Güvenlik Bayrağı Yakala Puan Tablosu									
S.N.	Kayıt Numarası	Takım Adı	1. Adım (20 Puan)	2. Adım (20 Puan)	3. Adım (30 Puan)	4. Adım (30 Puan)	Toplam Puan (100)	Toplam Süre	Sıralama Derecesi
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									
26									
27									
28									
29									
30									

Online Sınav Örnek Soruları:

1. Aşağıdakilerden hangisi tüm verileri şifreler ve dosyaların şifresini çözmek için kripto para biriminde ödeme talep eder?

A) Ransomware B) Rootkit C) Scareware D) Solucan E) Virüs

2. Aşağıdakilerden hangisi nmap komutu ile SYN taraması yapmak için kullanılan parametredir?

A) -sF B) -sN C) -sO D) -sS E) -sV

3. Aşağıdaki programlardan hangisi ağ haritalama için kullanılır?

A) ping B) ipconfig C) nmap D) hydra E) crunch

4. msfconsole içinde seçilen bir exploit'in uygulanacağı uzak bilgisayarı belirtmek için aşağıdakilerden hangi komut uygulanır.

A) SET LHOST 192.168.1.100 B) EXPLOIT 192.168.1.100 C) NMAP 192.168.1.100

C) PING 192.168.1.100 D) SET RHOST 192.168.1.100

5. Sızma testi işlemi için hiçbir bilgiye sahip olunmadan yapılan test türü aşağıdakilerden hangisidir?

A) Beyaz kutu B) Dış ağ sızma C) Gri kutu D) İç ağ sızmaE) Siyah kutu

6. Ağ aygıtlarındaki açık bağlantı noktalarının listesini sağlamak için aşağıdaki programlardan hangisi kullanılır?

A) Metasploit B) Meterpreter C) Nmap D) Ping E) Tracert

Not1: Yarışma Organizasyon Komitesi, işbu belge ve eklerde değişiklik yapma hakkına Milli Eğitim Bakanlığı bilgisi dahilinde sahiptir.
Not2: Yarışma Organizasyon Komitesinin yeterli katılımcı olmaması halinde yarışmayı iptal etme hakkı Milli Eğitim Bakanlığı bilgisi dahilinde saklıdır.
Not3: İlgili değişiklik ve duyurular www.kodeli.com.tr adresinden yapılacaktır.

Ek Bilgi:

Siberlab Ürün Açıklaması:
Gelişen siber güvenlik teknolojileri; uygulama odaklı eğitimler, tatbikatlar ve analiz laboratuvarları için kullanıcıları hızlı ve kolay tasarlanabilir sanal ortamlara yönlendirmektedir. Sanal Siber Güvenlik Laboratuvarı altyapısı ile ağ cihazları ve bilgisayarları içeren topolojiler tasarlanabilmekte ve kullanıcının tasarıma uygun ortamlara tarayıcı üzerinden ve herhangi bir kaynak gereksinimi olmadan hızlı bir şekilde erişebilmesi sağlanmaktadır. Sanal Siber Güvenlik Laboratuvarı ve Tatbikat Altyapısı siber güvenlik eğitim, test, tatbikat ve siber güvenlik analizi gibi faaliyetleri bulut üzerinde oluşturulmuş sanal ortamlar üzerinde hızlı, kolay ve düşük maliyetle oluşturabilmektedir.

Yetenekler:

- Sunucu sanallaştırma altyapısı
- Hızlı, güvenli ve izole laboratuvar erişimi
- Görsel laboratuvar tasarım arayüzü
- Kullanıma hazır laboratuvar ortamı şablonları
- Uzmanlar tarafından hazırlanan sanal makine imajları
- Yeni imaj oluşturma
- Kullanıcı gruplarına göre kota yönetimi
- Tatbikat arayüzü
- Ansible destekli skorlama arayüzü

Kullanım Alanları:

- Siber güvenlik analiz laboratuvarı
- Zararlı yazılım analiz laboratuvarı
- Adli analiz laboratuvarı
- Uygulamalı eğitim ortamı
- Siber güvenlik yarışmaları ve tatbikatlar