# Siber Durum Farkındalığını Artırmada Etkili Bir Yöntem: Bayrağı Yakala

Osman Akın, Işıl Çınar, Muhammer Karaman, Fatih Bilekyiğit

**Özet— Bilgi teknolojilerinin her geçen gün yaygınlaşması ve sayısal ortamda hem kişisel hemde kamusal verinin günden güne katlanarak artması beraberinde siber tehditlerin getirdiği riskleri artırmaktadır. Siber güvenlik alanında önemli adımlardan birisi durumsal farkındalık oluşturmaktır. Bu çalışmada siber durum farkındalığını artırmaya yönelik bayrağı yakala (BY) yarışmaları ayrıntılı olarak incelenmiş ve bu kapsamda kurum içi farkındalık çalışması olarak uygulanan bir yarışma sonrasında elde edilen sonuçlar ve alınan dersler paylaşılmıştır. Sonuçlar göstermiştir ki siber güvenlik alanında çalışan ve gerçek sistemlere saldırı yapma imkanı olmayan personel için düzenlenecek bayrağı yakalama yarışmaları ile bilgi düzeyi ve farkındalık artırılabilir. Yine bu çalışma göstermiştir ki siber güvenlik alanında çalışsa dahi bir personel için bizzat yaşanacak tecrübeler teorik olarak öğrenilen bilgiden çok daha etkili bir şekilde farkındalık oluşturmaktadır.**

***Anahtar Kelimeler*— Siber güvenlik, bayrağı yakala, siber güvenlik farkındalığı, siber oyun.**

**An Effective Method of Increasing the Situational Awareness of Cybersecurity: Capture the Flag**

***Abstract*— The spread of information technologies and the exponential growth of both personal and public data in digital media increase the cyber threats risks. One of the main important issue in the field of cyber security is to create situational awareness. In this study, capture the flag contests that help improve situational awareness are studied in detail. As a part of in-house awareness study, a capture the flag contest is implemented, the results and lessons learned have been shared. The results have shown that the level of knowledge and awareness can be advanced among cyber security personnel who do not have an opportunity to attack real systems. This study has also demonstrated that the real experiences, which are gained by attending capture the flag contest, can increase the level of awareness a lot more than theoretical knowledge for cyber security personnel.**

***Index Terms*— Cyber security, capture the flag, cyber security awareness, cyber game.**

## I. GİRİŞ

BİLGİ teknolojilerinin kullanımının yaygınlaşması ve günümüzde kurumların bilgi ve verilerinin büyük bir bölümünün sayısal ortamda bulundurulması ile siber tehditlerin oluşturduğu risk her geçen gün bir kat daha artmaktadır. Özellikle sosyal ağların sayısının ve kullanıcısının artması, birçok devlet uygulamasının internet ortamından sunulması, sanal ortamdaki verinin artmasını beraberinde getirmiştir. Bu durum birçok kötü niyetli kişilerin ve çoğu devletin iştahını kabartmaktadır. Tıpkı gerçek savaşlarda olduğu gibi siber güvenlik konusunda önceden almış olduğunuz güvenlik tedbirleri, yapmış olduğunuz testler, yaşadığınız tecrübeler, kurumlar arası işbirliği ve en önemlisi oluşturmuş olduğunuz durumsal farkındalık sistemlerinizi korumaya yardımcı olacaktır. Siber güvenlik farklı adımları barındıran bütünleşik bir olgu olmasına rağmen, en temel adımlardan bir tanesi bu alanda çalışan personelin farkındalığıdır. Siber güvenlik alanında farkındalığı artırmak için farklı yöntemler ve çalışmalar önerilmiştir. Barındırdığı sistemler ve kritik veriler açısından farkındalığın en yüksek olması gereken alanların (organizasyonların) başında kamu kurumları gelmektedir. Bu alanda kamu algısı 2010 yılında yapılan bir çalışmada [1] ele alınmış ve birçok kamu kurumunda siber güvenlik farkındalığının çok zayıf olduğu, sadece güvenlik duvarı kurulmasıyla sistemlerin güvenli kabul edildiği ortaya konmuştur. Türkiye'de kamu kurumlarında siber güvenliğin sağlanması noktasında ortaya çıkan ve çıkacak olan teknik, idari, hukuki, yönetimsel vb. alanlarda zayıflıkları öngörmek, tespit etmek ve gidermek maksadıyla ulusal çapta politika, strateji ve eylem planlarından oluşan ve Haziran 2013'de yayımlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda "Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirme Faaliyetleri" başlığı altında siber güvenlik farkındalığı ele alınmış ve artırılmasına yönelik vurgular yapılmıştır [2]. Siber güvenlik alanında farkındalıkları artırmak için yapılan çalışmalardan bir tanesi de BY yarışmaları düzenlemektir. BY, beyaz şapkalı hackerlar arasında oynanan öğretici bir oyundur. BY'de yarışmacılar dijital labirentler içinde bir hedefin başarılı bir şekilde tamamlandığını gösteren bir bayrağı yakalamaya çalışırlar. Bir başka ifadeyle hacker timlerinin belirli yazılımlar ve ağ yapılarını kullanarak bilgisayarlar ve ağlara saldırmaya veya savunmaya çalıştığı bir yarışmadır [5]. Belirlenen hedefe ulaşmak ve bayrağı(hedef sistemlerde gizli metin dosyası) önce kapmak için sistemlerdeki güvenlik açıklıkları değerlendirilerek bayrağa ulaşılır [3]. Bu bayraklar; gizli bir parola, bir veriye ulaşma, veya bir resim bile olabilir. Bayraklar her yarışmacı için ayrı veya farklı da olabilir.

BY yarışmasının temel amacı proaktif güvenliğin faydalarının gösterilmesidir. Diğer bir ifadeyle önlem alınmayan basit güvenlik hatalarının sonuçlarının nelere mal olacağını uygulamalı olarak göstermektir. Burada dikkat edilmesi gereken husus bu oyunun yıkıcı bir hacking anlayışından ziyade katılımcının teorik bilgilerini uygulamaya koymasını sağlamak ve çeşitli sistemler arasındaki güvenlik sorunlarını hızlıca bulup değerlendirmesini yapmaktır [4].

Bu alanda bir çok çalışma önerilmesine rağmen genellikle yapılan yarışmalar belli platformları gerektirmekte ve katılımcıların belli bir ön bilgi seviyesine sahip olması gerektiği ön koşul olarak sunulmaktadır. Bu çalışmanın temel amacı bu tür yarışmaların küçük ölçekli işletmelerde ve kamu kurumlarında öğretici ve siber güvenlik farkındalığını artırıcı olarak uygulanabilirliğini göstermektir. Bu çalışmada BY yarışması bir kurum içi eğitim kapsamında ele alınmış, yarışmacılar siber güvenlik alanında çalışanlardan herhangi bir ön kriter uygulanmadan seçilmiş, elde edilen sonuçlar anket

O.Akın Hacettepe Üniv.Bilg.Müh., e-mail: (oakin@hacettepe.edu.tr).
I.Çınar Gazi Üniv.Bilg.Müh., e-mail: (isil.cinar@gazi.edu.tr).
M.Karaman, Siber Güv.Uzmanı, e-mail: (muammerkaraman29@gmail.com).
F.Bilekyiğit, Siber Güv.Uzmanı, e-mail: (fatihbilekyigit@gmail.tr).

yöntemiyle değerlendirilmiş ve bu alanda yapılacak çalışmalara bir fikir oluşturması için alınan dersler özetlenmiştir. Bu çalışma göstermiştir ki gelişmiş sistemlere sahip olmadan yaklaşık 20 günlük bir sürede basit bir ağ ortamında bu şekilde bir yarışma hazırlanabilmektedir. Yine bu yarışmanın sonuçları ve elde edilen tecrübeler göstermiştir ki siber güvenlik çok geniş bir olgudur ve her bir alanda mutlaka çok tecrübeli olunması gerekmektedir. Yarışma sonucunda elde edilen bilgilerle katılımcıların kendilerine olan güvenlerinin ve tecrübelerinin arttığı gözlemlenmiştir.

Bu makalenin bundan sonraki kısımları şu şekilde ele alınmıştır:Bir sonraki bölümde bu alanda yapılan çalışmalar özetlenmiş ve çalışmaların artıları eksileri tartışılmıştır. Üçüncü bölümde soruların nasıl ve ne amaçla oluşturulduğu, yarışmanın nasıl dizayn edildiği, nasıl gerçeklendiği konuları detaylı olarak ele alınmıştır. Bir sonraki bölümde ise yarışma sonucunda değerlendirmenin nasıl yapıldığı ve sonuçları özetlenmiştir. Beşinci bölümde yarışma ile kazanılan deneyimler ve alınan dersler paylaşılmıştır. Son olarak bu şekilde bir yarışmayı gerçekleştirmenin artı ve eksileri değerlendirilerek sonuçlar ortaya konmuştur.

## II. İLGİLİ ÇALIŞMALAR

Akademik ve farkındalık artırma amaçlı yapılan birçok siber güvenlik çalışması BY'yi oluşturmaktadır. Bu alanda şimdiye kadar birçok çalışma yapılmıştır ancak önerilen her farklı yöntem yeni bir farkındalık oluşmasına olanak sağlamaktadır. BY çalışmaları, güvenlik alanında söz sahibi bir eğitim kurumu olan SANS'ın yayınladığı dokümana [3] göre temel olarak 3 farklı grupta toplanmıştır. Bunlar sadece saldırı(only offensive) olanlar, saldırı veya savunma olanlar(ofensive/defensive) bir de saldırı ve savunmanın bir arada olduğu karışık saldırı/savunma (mixed offensive/defensive) olanlar şeklinde belirtilmiştir. BY ilk olarak 1996 yılında, 4'üncü DefCon Konferansında yapılmıştır. Söz konusu yarışmanın katılımcılarını, bilgisayar güvenlik uzmanları, köşe yazarları, hukukçular, hükümet çalışanları, güvenlik araştırmacıları ile; yazılım, bilgisayar mimarisi, telefon sistemlerine yasadışı girme, donanım değişikliği ve hacklenebilecek herhangi bir konuda ilgisi olan hackerlar oluşturmuştur [5].

Müteakiben DefCon yarışmaları her yıl düzenlenmeye devam edilmiştir. Bu yarışma dünya çapında herkese açık olmasına rağmen öncesinde belirli eleme aşamalarından geçildiği için bir bakıma profesyonellerin katıldığı bir yarışmadır. Elemelerde başarılı olan sekiz takım DefCon konferansında daha önce oluşturulmuş olan tecrübeli bir takıma karşı yarışmaktadır [6].

Düzenlenen yarışmaların uygulama şekli de farklılık gösterebilmektedir. Örneğin yine DefCon'un düzenlediği ve amacı DARPA'nın 5 yıllık birikmiş Ar-Ge dayanıklılığının etkisini test etmek olduğu yarışmada [6] her takımın hem saldırı hem de savunma yeteneği bulunmakta ve her takım kendi bayrağını savunurken diğer takımların bayrağına ulaşmaya çalışmaktadır. DARPA'nın "kırmızı takım" ismi verilen ve gelenekselleşen yarışmalarında ise takımların sadece saldırı yetenekleri ölçülmektedir.

Bu alanda yapılan başka bir çalışmada [7], BY farklı altyapılara sahip öğrenciler için siber güvenlik farkındalığı ve tecrübesi oluşturulması amacıyla uygulanmıştır. Yarışmanın farklı bilgi birikimine sahip öğrenciler için ele alınmasının temel nedeninin çok daha fazla öğrencinin bu deneyimi yaşamasını sağlamak olduğu ifade edilmiştir. Bu yarışmada öğrencilerden farklı takımlar oluşturulmuş ve her bir takım, oluşturulan sanal sunucularda kendi web sitesini korurken başka takımın web sitesinde yer alan bayrağı ele geçirmeye çalışmıştır.

Benzer yapılan bir diğer çalışmada [8], BY için farklı okullardan öğrencilerle farklı takımlar oluşturulmuştur. Bu çalışmada yine her bir takım kendi web sitesini korurken diğer takımların web sitesinde yer alan bayrağı ele geçirmeye çalışmaktadır. Bu çalışma siber güvenlik alanında her bir açıklık için çok iyi derecede spesifik bilgiye sahip olunması gerektiğini ortaya koymuştur.

Bu alanda en çok bilinen diğer iki yarışma da Amerikan Ulusal Kolejler Arası Siber Savunma Yarışması (National Collegiate Cyber Defense Competition-NCCDC) [9] ve Kaliforniya Üniversitesinin Uluslararası Bayrağı Yakala Yarışmasıdır(International Capture the Flag Competition - iCTF) [10]. Her iki yarışma da hem ulusal hem uluslararası olarak yüzlerce öğrencinin katılımıyla ve ön elemeleri ile birlikte çok büyük organizasyonlar şeklinde icra edilmektedir.

Bu alanda daha spesifik ve farklı formata sahip askeri okullar için kullanılan çalışmalardan bir tanesi de Military Academies Cyber Defense Exercise (CDX) [11,12,13] yarışmalarıdır. Bu yarışma, öğrencilerin kendi ağlarını(network) kırmızı bir takıma karşı savunmaları bakımından NCCDC yarışmasına benzemektedir. Bu yarışmadaki farklılık kırmızı takımın National Security Agency (NSA) ve bu alanda uzman askeri personelden oluşturulması ve öğrencilerin var olan bir ağı kullanmak yerine verilen bir bütçe kapsamında kendi ağlarını kurmaları ve savunmalarıdır.

Büyük ölçekli yarışmaların yanında bu konuyu bizim yaptığımız çalışmaya benzer olarak küçük boyutta ele alan çalışmalar da mevcuttur [14]. Bu yarışmada öğrencilerden altışarlı gruplar şeklinde dört masa oluşturulmuş ve her bir masa kendi ağını(web sitesi, veritabanı, firewall, DNS vb. içermekte) kurarak ve savunarak diğer ağlara saldırı düzenlemiştir. Bu çalışmada BY yarışmalarının küçük boyutlu olarak etkin bir şekilde yapılabileceği gösterilmeye çalışılmıştır.

BY yarışmaları öğrenme amaçlı hazırlandığı için daha sonrasında yıkıcı amaçlı kullanılmaması önemlidir. Bununla ilgili bir çalışmada [15] bir BY yarışmasının amacının öğrencilerin eğitimine katkı sağlamak olduğu ve yarışma sorularının etik olarak hazırlanması gerektiği vurgulanmıştır. Bazı yarışmacıların konuyla ilgili yetenek ve bilgilerini zararlı faaliyetlerde kullanabileceği; bu sorunu aşmak için yarışma soruları içeriği ve genel müfredatın etik olması gerektiği belirtilmiştir. Yarışma sorularının kapsam ve içeriği belirlenirken bu durum kurum içi hazırlanan yarışmalarda da göz önüne alınmalı ve konunun hassasiyeti ve yarışmanın amacı katılımcılara çok iyi bir şekilde aktarılmalıdır.

İncelenen çalışmalarda önemle üzerinde durulan bir diğer husus ise yarışma icrası için kaynak kullanımı ve maliyet konusudur. Hoffman, L. ve ark. yaptıkları çalışmada [16] tedarik/temin (özellikle sadece yarışma için gerekli ise uygun donanım/yazılım tedariki zor ve maliyetli olabilmektedir), bakım (yarışmaların bütçeleme ve planlaması uzun süreye yayıldığında ve düzenli olarak her yıl uygulandığında teknik güncellemeler gibi bakım ihtiyacı doğmaktadır), personel ihtiyacı (bu tarz yarışmalarda yönetimsel ve teknik personel desteğine her zaman ihtiyaç duyulmaktadır), dış destek (iç destek seviyesine göre saldırgan, hakem veya denetçi gibi davranabilmek için dış bilgi hizmetinin alınması da önemlidir), yönetim (çeşitli sponsorlardan destek almak yarışma geliri

açısından önemlidir) ve imkanlar konularına dikkat çekmişlerdir.

Türkiye'de de son yıllarda artmakla birlikte farklı zaman ve formatlarda çeşitli BY yarışmaları düzenlenmektedir. Bu oyunlara zaman zaman çevrimiçi katılım sağlanabildiği gibi farklı platformlar da kullanılabilmektedir. Son yıllarda yapılan yarışmalardan bir tanesi de Prodaft şirketi tarafından düzenlenen, siber güvenlikle ilgili analitik düşünme ve teknik bilgi gerektiren 25 adet görevin verildiği "Dünyayı Kurtaran Hacker" adlı siber savaş oyunudur. Oyunun amacı Türkiye'de siber güvenliğin önemini duyurmak ve bu konudaki yetenekli gençleri bir araya getirmek olarak açıklanmıştır. Soruların web sayfası üzerinden yayımlandığı yarışmaya toplam 1599 kişi katılım sağlamıştır [17].

Bilgi Güvenliği Akademisi, İstanbul Bilgi Üniversitesi ve ADEO Bilişim ve Danışmanlık şirketi işbirliğiyle İstanbul Bilgi Güvenliği Konferansı'nda 2009 ve 2011 yıllarında düzenlenen konferaslarda yine BY yarışması icra edilmiştir. İlkinde BY yarışması iki ana kategoriye ayrılmış ve yarışma 5 farklı adımdan oluşmuştur [18]. İkinci yarışmada ise 38 farklı konuda 35 farklı uzman yer almış ve hem internet üzerinden hem de etkinlik alanında "Capture The Flag Ethical Hacking" yarışması gerçekleştirilmiştir. Yarışmaya ait detaylı çözümleri içeren doküman web üzerinden yayımlanmıştır [19].

Düzenlenen başka bir etkinlik, Bilgi Güvenliği Akademisi tarafından Nisan 2012 tarihinde genele açık BY ve Beyaz Şapkalı Hacker (Ethical Hacking) yarışmasıdır. Yarışma toplam 6 adımdan oluşmuş ve her bir adımda bir sonraki adım ile bağlantı kurulmuştur [20]. Yarışmaya yaklaşık 500 kişi katılmıştır. Sorular web uygulaması ortamında sunulmuş veya e-posta ile gönderilmiştir. Soruların çözümlerine ait teknik doküman ise yarışma sonrasında yayımlanmıştır.

Başka bir faaliyet olarak, TÜBİTAK ve Bilgi Güvenliği Akademisi, Türkiye'de siber güvenlik uzmanı eksikliğinin giderilmesine destek olmak ve kapasite geliştirilmesini sağlamak amacıyla üniversite öğrencilerine yönelik "Siber Güvenlik Yaz Kampı" düzenlemektedir. İlki 2012 yılında Gebze'de düzenlenen kampın ikincisi 2013 yılında düzenlenmiştir. Kamp süresince bilişim sistemleri güvenliği konusunda öğrencilere farklı konularda eğitimler verilmesinin yanısıra uygulamalı, eğitim amaçlı ve ödüllü BY yarışmaları düzenlenmektedir [21].

Katılımcıların çoğu kamu kurumu olmakla birlikte, içlerinde özel sektör ve sivil toplum kuruluşları da bulunan 2. Ulusal Siber Güvenlik Tatbikatı 2013 yılında düzenlenmiş; daha önceki yıllardan farklı olarak bu tatbikatta BY yarışması icra edilmiştir. Yarışmaya 5'er kişilik 4 farklı takım katılmıştır. Yarışmada önceden tasarlanmış, belirli açıklıkları olan sistemleri aşamalı olarak ele geçirmek üzere oyun senaryoları kurgulanmıştır [22].

Yine 2013 yılında İstanbul'da gerçekleştirilen ve amacı araştırmacılar, hackerlar ve geliştiriciler arasında fikir ve tecrübelerin öğrenilmesi ve paylaşılmasını sağlamak olan "NOPcon Güvenlik Konferansı"nda NOPcon BY yarışması düzenlenmiş ve çözümleri sunulmuştur [23].

Bir başka çalışma da, Web Güvenliği Topluluğu (Owasp Türkiye) tarafından geliştirilen "Davshan" isimli BY projesidir. Projede güvenlik konusunda kendini test etmek isteyen kişiler, sistem üzerinde bilerek bırakılmış olan açıklıkları tespit etmeye çalışmaktadırlar [24].

Bu noktadan hareketle; Türkiye'de icra edilen Siber Güvenlik Tatbikatları, Siber Güvenlik Yaz Kampları ve benzeri kapsamda yapılan diğer çalışmalar incelendiğinde son yıllarda düzenlenen bu gibi organizasyonlarda ciddi artış olduğu; ulusal, kurumsal ve doğal olarak bireysel farkındalığın arttığı ve buna paralel olarak BY yarışmalarının da bu farkındalığın artmasında, siber güvenlik alanında ihtiyaç duyulan motivasyonun sağlanmasında ve yeteneklerin keşfedilmesinde önemli bir etken olduğu görülmektedir.

Bu alanda özellikle Amerika kaynaklı çok fazla çalışma önerilmesine rağmen, bu yarışmaya hazırlanırken ve sonrasında bu çalışmayı oluştururken yapmış olduğumuz taramalarda BY'nin küçük ölçekli olarak kamu kurumlarında hizmet içi eğitim kapsamında uygulanmasına rastlanmamıştır. Amerika kaynaklı birçok yarışma özellikle öğrencilerin eğitimi için önerilmiştir. Bunun yanı sıra yaptığımız yarışma formatına benzer yarışmalar Türkiye'de yapılmışsa da bu yarışmalarla ilgili herhangi bir değerlendirme yapılarak paylaşılan herhangi bir çalışma bilgimiz dahilinde yoktur. Yaptığımız bu çalışma kamu kurumlarında BY'yi hizmet içi eğitim kapsamında ele alması anlamında bir ilki oluşturmaktadır. Bu çalışmada ayrıca farklı soru çeşitleri kullanılarak siber güvenliğin çok kapsamlı konuları barındırdığı ve farkındalık oluşturulurken bu durumun göz önünde bulundurulması gerektiği ortaya konmaya çalışılmıştır.

## III. YARIŞMANIN DİZAYN EDİLMESİ VE UYGULANMASI

Yarışma tasarlanırken siber güvenliğin önemi göz önüne alınarak, hem alanın ne kadar geniş olduğu hem de bu alanda yetişecek kişilerin temel konulara çok iyi hakim olması gerektiği hedeflenmiştir. Bu yarışmanın amacının savunmaya yönelik farkındalık oluşturmak olduğu katılımcılara özellikle vurgulanmıştır. Yarışmanın hazırlanması ve uygulanması prosedürel konular ve teknik konular olmak üzere iki farklı alt başlık altında toplanmıştır. Prosedürel konularda yarışmanın nasıl yapılması gerektiği, süresi, kullanılacak platform ve donanım gibi konular ele alınırken; teknik konular kısmında yarışmada kullanılan sorular ve çözümleri ayrıntılı olarak incelenmiştir.

### *A. Prosedurel Konular*

Sorular hazırlanırken, kurum içi alınan eğitimlerin katılımcılara faydası, katılımcıların çalışma alanları, yarışma sırasında kullanılacak donanım/yazılım yeterliliği, katılımcıların siber güvenlik konusundaki farkındalığının test edilmesi gibi hususlar göz önünde bulundurulmuştur.

Yarışmacılara donanım ve yazılım kullanımı kapsamında herhangi bir kısıtlama getirilmemiş, yarışmaya bireysel veya iki kişilik takımlar halinde katılabilecekleri belirtilmiş ve yarışmanın süresi 2 gün olarak kısıtlanmıştır. Süre yönünden kısıtlama getirilmesinin sebebi kullanıcıların daha iyi performans göstermelerini beklemektir. Yarışma için belirli sistemler oluşturarak katılımcıların bu sistemlere saldırmalarını beklemek yerine belirli formatta hazırlanan soruları içeren dosyalar gönderilerek yarışmanın yapılması kararlaştırılmıştır. Yarışmayı bu şekilde dizayn etmemizdeki temel amaç minumum donanım ve çaba ile yarışmanın yapılmasını sağlamaktır.

Yarışmanın içeriği, amacı, soru başlıkları, puanlaması gibi yarışmayla ilgili genel bilgiler Wordpress kullanılarak yarışma öncesinde katılımcılarla paylaşılmıştır. Katılımcılar siber güvenlik alanında çalışan personelden herhangi bir ön kriter uygulanmadan seçilmiştir.

Yarışmaya katılacak kişilere birer adet bilgisayar tahsis edilmiş ve bu bilgisayarlar bir yerel ağ oluşturacak şekilde bir sunucu ile internete irtibatlandırılmıştır. Kullanıcılar kendi bilgisayarlarında yönetici yetkisine sahiptirler ve internet

ortamında gerekli yazılımları indirerek kullanabilmişlerdir. Yarışma puanlamasında cevap veren kişi sıralaması dikkate alınmış ve ilk üç kişiye cevap verme sırasına göre 10, 8 ve 6 puanları verilmiş, sonraki yarışmacılardan cevap veren her kişiye beşer puan verilmiştir. Puanlama Wordpress kullanılarak online olarak kullanıcılara iletilmiştir. Yarışmaya toplam 16 kişi katılım sağlamıştır.

Yarışma sorularının cevapları yarışma sonunda paylaşılmış; farklı teknik ve yöntemlerle sonuca giden yarışmacılar da soruların çözümüne katkı sağlamıştır. Böylece yarışmacıların sorularda hangi aşamaya kadar geldikleri, eksikliklerinin neler olduğu ve farklı çözüm yöntemleri öğrenilmiştir.

*B. Teknik Konular*

Yarışmada sorular; stegonagrafi, internet üzerinden bilgi toplama yöntemleri, sosyal mühendislik, şifre kırma bilgisi (Truecrypt, Winrar vb.), web uygulama güvenliği (SQL injection), parola kırma saldırıları (hash, md5 , rainbow table vb.), kriptolama bilgisi kullanma, ağ trafiği analizi , e-posta güvenliği gibi konuları içermektedir. Sorular hazırlanırken daha önce Türkiye'de ve dünyada gerçekleştirilmiş olan yarışmalardan faydalanılmıştır [3,17,20]. Sorularla ilgili ayrıntılı bilgiye ve değerlendirmeye aşağıda yer verilmiştir.

- E-posta Güvenliği

Yarışmacılardan yahoo, mynet ve gmail e-posta hesapları istenmiştir. Bu hesaplara kendilerine ait diğer e-posta adreslerinden gelmiş gibi görünen sahte e-posta gönderilmiştir. Metin içeriğinde şifreli bir şekilde flag bilgisi verilmiştir. Yarışmacının gelen e-postanın sahte olduğunu anladığı anda tespit etmek üzere gelen e-postanın başlık bilgisini kontrol etmesi gerekmektedir. Böylelikle yarışmacı sahte postanın hangi posta sunucusu kullanılarak gönderildiğini tespit etmektedir. Yarışmacıya bayrak olarak sahte posta göndermek için kullanılan sunucunun adı şifreli olarak verilmiştir.

- Web Uygulama Güvenliği

Bu senaryoda SQL Injection ile yerel olarak kurulmuş olan bir web tabanlı uygulamaya yetki olmadan ve herhangi bir parolaya sahip olmadan giriş yapılması istenmiştir. SQL Injection ile sisteme yönetici yetkisiyle giriş yapıldığında listedeki tüm personelin bilgilerine erişilebilecektir. Listedeki belirli bir kaydın bilgilerinin değiştirilmesi, silinmesi veya yeni kayıt girilmesi gibi SQL işlemlerinin gerçekleştirilmesi beklenmiştir. Bu işlemleri gerçekleştiren kullanıcı ekran görüntüsünü cevap olarak gönderecektir.

- Stegonagrafi

Stegonagrafi kullanılarak herhangi bir resim içerisine gizlenen metnin çözülmesi istenmiştir. Burada kullanılan orjinal resim ve içerisine metin gizlenmiş olan resim (Şekil 1) yarışmacıya e-posta ile gönderilmiştir.

Burada önemli olan nokta; herhangi bir resme bir stego aracı ile metin gizlendiğinde bu metni çözmek için yine aynı stego aracı kullanmak gerektiğidir. Sadece ticari birkaç ürünle herhangi bir araçla gizlenmiş olan metinlerin çözülebildiği iddia edilmektedir. Dolayısıyla katılımcıya kullanılan stegonagrafi aracı (Quick Stego) ipucu olarak verilmiştir. Yarışmacılar Şekil2'de yer alan sonuca ulaşmışlardır. Bu yarışma sorusu, siber güvenlik açısından bazı dosyaların göründüğünden farklı bilgiler içerebileceğini göstermiştir. Stegonografi teknikleri ile ilgili detaylı bilgi için Tatar ve ark.'nın çalışmasına [25] bakılabilir.

Şekil 1. İçerisine Metin Gizlenmiş Olan Resim


Şekil 2. Resim İçindeki Çözülmüş Gizli Metin

- Şifre Kırma

Bu soruda amaç TrueCrypt ile şifrelenmiş dosyanın parolasını bulup içerisindeki gizli mesajı ortaya çıkarmaktır. Yarışmacılardan öncelikle istenen özel bir wordlist oluşturarak şifrelenmiş olan dosyanın parolasını bulmalarıdır. TrueCrypt ile şifrelenmiş dosyanın parolasının ilk 5 karakterinin "siber" kelimesi olması, bu kelime hariç sadece rakamlardan oluşması ve toplam 10 karakter içermesi ipucu olarak verilmiştir. Bu senaryoda kullanıcılardan yukarıda yer alan ipuçlarını kullanarak oluşturdukları bir şifre listesi(wordlist -Bactrack ile birlikte gelen "Crunch" vb.) ile veya çoğu uygulamanın sağladığı "password pattern" seçeneğini kullanarak düzenli ifadeler (regex) ile TrueCrypt şifresini açık kaynak uygulamalardan birini (örneğin; OTFBrutus adlı araç hem "wordlist" hem de "password pattern" kullanımını sağlamaktadır) kullanarak kırmaları ve gizli mesajı ortaya çıkartmaları istenmiştir. Gizli mesaj içerisinde bayrak yer almaktadır. Bu soru ile basit parolaların kısa sürede kırılabilirliği ve kişisel hayatımızla ilgili bilgilerin parolalarda kullanılmasının tahmin edilebilirliği(word list oluştururken) kolaylaştırdığı katılımcılara gösterilmeye çalışılmıştır.

- İnternet Üzerinden Bilgi Toplama

Bu soruda yarışmacılara jpeg formatında bir fotoğraf ve bir senaryo verilmiştir. Yarışmacılar öncelikle bu fotoğrafı kullanarak internet üzerinde görsel arama yapacaklar ve fotoğrafın ait olduğu web sitesini keşfedeceklerdir. Bu web

sitesinde uygun kelimelerle arama yapacak ve kullanıcı bilgilerinin(kullanıcı adı, şifre vb.) yer aldığı bir excel dosyasına erişeceklerdir. Sonrasında ise yarışmacıların toplamış oldukları bilgileri kullanarak web sitesinin veritabanına sızmaları ve bu veritabanında yer alan bir makaleye erişmeleri istenmiştir. Buradaki bayrak veritabanına sızıldığını kanıtlayan, veritabanındaki makalelerden bir tanesinin kimlik bilgisidir. Sisteme giriş yapıldıktan sonra araştırma yöntemiyle web tabanlı uygulamada gerekli bilgiler elde edilebilecektir. Bu soruda katılımcıların "google hacking" ve arama motorunda görsel arama sayfasından resim arama özelliğini kullanmaları beklenmiştir. Bunun yanısıra katılımcılar, kullanıcı bilgilerini ve şifrelerini içeren herhangi bir dosyanın web sunucuda saklanmaması ya da unutulmaması gerektiğinin farkına varmışlardır.

- Farkındalık ve Biliçlendirme

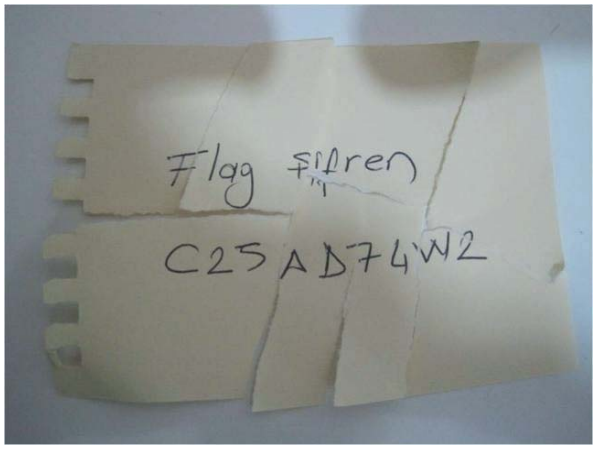
Bu alanda iki adet soru kullanılmıştır. İlk olarak katılımcılara sadece bir fotoğraf gönderilerek bayrağa erişmeleri istenmiştir (Şekil 3). Fotoğrafın parlaklık ve karşıtlık ayarlarıyla oynandığında içine yerleştirilmiş bir metin ortaya çıkmaktadır (Şekil 4). Bu soru katılımcılara bir dosyanın göründüğünden farklı bilgileri de barındırabileceği gerçeğini göstermiştir.

İkinci soru notlarımızı çöpe atarken ne kadar çok dikkat etmemiz gerektiğini hatırlatmak maksatlı hazırlanmıştır (Şekil 5). Soruda kağıt parçaları uygun şekilde birleştirildiğinde bayrağa erişilmektedir (Şekil 6) Birleştirme işlemi çeşitli yazılımlarla (photoshop vb.) kısa sürede yapılabilmektedir veya fotoğrafın çıktısının alınıp uygun şekilde birleştirilmesi de bayrağa ulaşmayı sağlayacaktır.

Şekil 3. İçerisine bayrak gizlenmiş resim

Şekil 4. Ayarları ile oynanarak bayrağın elde edilmesi

Şekil 5. Yarışmacılara gönderilen parçalı fotoğraf




Şekil 6. Parçaların uygun şekilde birleştirilmiş hali

- Parola Kırma Saldırıları (hash, md5 , rainbow table vb)

Bu soruda katılımcılara Winrar kullanılarak şifrelenmiş bir dosya içerisinde kullanıcı adlarının ve şifrelerinin hash kayıtları verilmiştir. Katılımcıların öncelikli olarak kaba kuvvet (Brute force) atak ile Winrar şifresini kırmaları istenmiştir (ör: Winrar Password Cracker, Rar Pasword Recovery). Yarışmacılar şifreyi kırdıktan sonra eriştikleri dosyada kullanıcı adları ve hash kayıtları bilgilerine erişeceklerdir. Sonrasında ise "Flag" adlı kullanıcının hash kaydını, online md5 kaydı kıran web sitelerinde [26] deneyerek şifreye ulaşmaları hedeflenmiştir. Bu senaryo ile katılımcılara şifrelerin zorlaştıkça kırılmasının daha zor olduğu ve uygulamalarda şifrelerin açık olarak (clear text) tutulmaması gerektiği anlatılmaya çalışılmıştır.

- Kriptolama

Katılımcılara Sezar Şifreleme yöntemi kullanılarak hazırlanmış bir metin gönderilerek kriptolama alanındaki bilgileri ölçülmüştür. En eski şifreleme yöntemlerinden biri olan Sezar algoritmasını yarışmacılara bir kez daha hatırlatmak için hazırlanan bu soruda amaç katılımcıların online şifre çözen web sitelerinin [27] ve araçların (crank v0.1.3 vb.) farkında olup olmadıklarını ölçmektir.

- Ağ Trafiği Analizi

Katılımcılara bir pcap (ağ sniff edilerek elde edilmiş dosya) dosyası gönderilerek; trafik analizinin yapılması istenmiştir. Katılımcılar analiz sonucunda flag olarak analiz

dosyası içinde yer alan şifre bilgisine ulaşmışlardır. Bu senaryoda amaç katılımcıların Wireshark, Networkminer, Tcpdump vb. trafik analiz araçlarını kullanmalarını sağlamaktır. Bu soru ayrıca yarışmacılara ağ üzerinden açık olarak gönderilen bilgilerin başkalarının eline geçme ihtimalinin çok yüksek olduğunu göstermiştir.

## IV. DEĞERLENDİRME

BY yarışmasının etkinliği yapılan anket ile değerlendirilmiştir. Kullanıcılara yarışmadan önce ve sonra siber güvenlik alanında kendilerine güvenlerinin nasıl olduğu sorulduğunda, katılımcılar ortalama olarak %50 oranında güvenlerinin arttığını belirtmişlerdir. Buna ek olarak böyle bir yarışmaya tekrar katılmak ister misiniz ya da yarışmanın hazırlanması aşamalarında yer almak ister misiniz sorularına katılımcıların hepsi "Evet" cevabını vermişlerdir. Ayrıca katılımcılar yarışma için kullandıkları donanım ve yazılımların yeterli olduğunu, yarışmanın formatının ve yayımlanma şeklinin uygun olduğunu belirtmişlerdir. Katılımcılara yarışmanın siber güvenlik farkındalığına katkısı sorulduğunda tamamından "çok iyi" cevabı alınmış ve tekrarlanması istenmiştir. Başka bir soruya cevap olarak katılımcılar yarışmanın alınan eğitimlerin uygulanması için kendilerine bir fırsat sunduğunu dile getirmişlerdir.

Bunun yanı sıra katılımcılarla yüz yüze yapılan görüşmelerde yarışmanın güvenliğe bakış açısını nasıl değiştirdiği sorulmuştur. Yarışmacılardan bir tanesi kişisel bilgisayarında eksik olan yamaları yüklediğini, bir diğeri virüs programını güncellediğini ve bir başkası da şifresiz olarak açılan bilgisayarına şifre koyduğunu belirtmiştir. Bunun yanı sıra kullandığı şifrenin basit olduğunun farkına varan başka bir yarışmacı şifresini güçlendirdiğini dile getirmiştir. Bir başka etkinlik olarak yarışma sonrasında soruların cevapları yarışmacılarla paylaşılmış ve yarışmacıların kullandıkları farklı yöntemler öğrenilmiştir. Bu sayede çok farklı ve özgün çözümlerin de olabileceği diğer yarışmacılar tarafından tecrübe edilmiştir. Yarışma sorularından elde edilen tecrübenin yanında katılımcılar bu paylaşım sayesinde birbirlerinin tecrübelerinden de faydalanma imkanı bulmuşlardır.

## V. ALINAN DERSLER VE GELECEK ÇALIŞMALAR

Bu şekilde bir yarışma dizayn etmek ve uygulamak bizim açımızdan bir ilk olduğu gibi katılımcılar açısından da bir ilki oluşturmaktadır. Bu anlamda bu yarışmadan öğrenmiş olduğumuz ve paylaşılmaya değer bulduğumuz konuları paylaşmak istedik. Öncelikle böyle bir yarışmayı icra edebilmek için çok büyük miktarda bir veri kaynağını taradık ve böyle bir yarışmanın nasıl icra edilmesi gerektiği konusunda bilgi sahibi olduk. İlk adım olarak bu faaliyet siber güvenlik konusunda öncelikle bizim farkındalığımızın artmasını sağladı.

Özellikle kurumsal bir BY gerçekleştirilmesi sebebiyle, yarışmanın hem mesai saatlerini hem de sonrasını kapsıyor olması kurum işlerinden dolayı zaman zaman yarışmacıların ara vermelerine ve puanlamada geriye düşmelerine neden olmuştur. Yarışmanın gerçekleştirileceği tarihlerin, katılımcılara haftalar öncesinden bildirilmesi, iş yükünün daha az olduğu haftaların seçilmesi, yarışmaya katılacak personele mesai sırasında imtiyaz gösterilmesi gibi hususların sonraki yarışmalarda dikkate alınması gerektiği sonucuna varılmıştır.

Yarışmada kullanılan donanım/yazılım alt yapısı her ne kadar iyi seviyede olsa da daha karmaşık soruların hazırlanıp uygulanması ve yarışmanın kapsamının genişletilerek daha çok personelin katılımının sağlanması için her yıl düzenlemeyi planladığımız yarışmalara özel laboratuar çalışması yapılması gerektiği sonucuna ulaşılmıştır.

Yarışma öncesinde yarışmacıların kullanacakları araçlarla ilgili gerekli kontrolleri yapmaları konusunda bilgilendirme yapılması ve yarışma öncesi destek verilmesi gerektiği sonucuna varılmıştır. Örneğin sanal makine kullanan bazı yarışmacılar konfigürasyon konusunda sıkıntı yaşamış ve zaman kaybetmişlerdir.

Yarışma yapı itibari ile birbirinden bağımsız sorulardan ve bayraklardan oluşmaktadır. Soruların yarışmacılara başlangıçta bütün olarak verilmesi, zorluk derecesi bakımından aynı seviyede olmayan sorulara yarışmacıların farklı sırada cevap verebiliyor olması, puanlamadaki dengeleri değiştirmiştir. Bundan sonra gerçekleştirilecek olan yarışmalarda yapı değiştirilerek, bir önceki sorudan elde edilen bayrakla sonraki sorulara geçiş yapılmasının daha uygun olacağı düşünülmektedir. Bu şekilde basit sorudan zor soruya doğru bir hiyerarşik yapı oluşturulmuş olacak ve herkes aynı zamanda aynı soru için çaba harcayacaktır.

## VI. SONUÇ VE ÖNERİLER

Bu yarışma hem katılımcılar hem de yarışmayı hazırlayanlar için üst düzeyde bir öğrenme tecrübesi oluşturmuştur. Öncelikle bu yarışmaya katılanlar siber güvenlik alanında ne derecede bilgi birikimine sahip olduklarının farkına varmışlar ve bu alanda ne tür yeteneklerini geliştirmeleri gerektiğini daha iyi kavramışlardır. Bunun yanı sıra bu yarışma hem katılımcılara hem de hazırlayanlara siber güvenliğin ne kadar karmaşık bir yapıda olduğunu ve çok geniş bir bilgi alanını içine aldığını göstermiştir. Bu yarışma için oluşturulan altyapı, kurulması düşünülen siber güvenlik test laboratuarı için bir ön çalışma niteliği taşıyabilir. Yapılan yarışmanın daha da geliştirilerek bir sonraki adımda daha çok personel ile ve daha farklı konuları içerecek şekilde yapılması planlanmaktadır. Bu alanda ülke ve kurumlar çapında yapılacak bayrak yarışmalarının; ulusal ve kurumsal farkındalığın artırılmasına, bireysel yeteneklerin ortaya çıkarılmasına, siber güvenlik alanında dinamikliğin sağlanması açısından faydalı olacağı değerlendirilmektedir. Bunun yanı sıra üniversitelerin de bayrak yarışmaları adı altında yarışmalar düzenlemesinin büyük öneme sahip olduğunu düşünülmektedir. Bayrak yarışmalarının kapsamlarının genişletilerek bireysel ve kurumsal katılımın da artırılmasıyla siber güvenlik tatbikatlarından ayrı olarak "Ulusal Bayrak Yarışmaları" düzenlenmesinin, bu ve benzer faaliyetlerin icra edildiği haftanın da "Ulusal Siber Güvenlik Farkındalık Haftası" olarak ilan edilmesinin siber güvenlik farkındalığına ve eğitimine katkı sağlayacağı değerlendirilmektedir.

## KAYNAKLAR

[1] Adnan Yılmaz, M. Akif Bakır: *Kamu Kurumlarında Bilgi Güvenliğine Yönelik Bir Durum Tespiti,* ISCTurkey'10,. pp.97-101

[2] http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm (Karar Sayısı : 2013/4890 Ekli "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nın kabulü; Ulaştırma, Denizcilik ve Haberleşme Bakanlığının 18/2/2013 tarihli ve 412 sayılı yazısı üzerine, Bakanlar Kurulu'nca 25/3/2013 tarihinde kararlaştırılmıştır.)

[3] http://www.sans.org/reading_room/whitepapers/casestudies/capture-flag-education-mentoring_33018, Haziran 2013

[4] CTF, http://www.istsec.org/ctf/, Kasım 2009

[5] Gavas, Efstratios, Nasir Memon, and Douglas Britton. "Winning Cybersecurity One Challenge at a Time." Security & Privacy, IEEE 10.4 (2012): 75-79.

[6] Cowan, Crispin, et al. "Defcon capture the flag: Defending vulnerable code from intense attack." DARPA Information Survivability Conference and Exposition, 2003. Proceedings. Vol. 1. IEEE, 2003.

[7] Werther, Joseph, et al. "Experiences in cyber security education: The MIT lincoln laboratory capture-the-flag exercise." Cyber Security Experimentation And Test 8 (2011).
[8] Ho, Jun-Won, Nayantara Mallesh, and Matthew Wright. "The Design and Lessons of the ASCENT Security Teaching Lab." Proceedings of the 13th Colloquium for Information Systems Security Education. 2009.
[9] The National Collegiate Cyber Defense Competition. Web Site, Haziran 2013: http://www.nationalccdc.org/
[10] The UCSB iCTF. Web Site, February 2012: http://ictf.cs.ucsb.edu/
[11] Mullins, Barry E.; Lacey, Timothy H.; Mills, Robert F.; Trechter, Joseph E. and Bass, Samuel D. *How the Cyber Defense Exercise Shaped an Information- Assurance Curriculum*. IEEE Security and Privacy, 5(5) (September 2007), pp. 40-49
[12] DeLooze, Lori L. Counter Hack: *Creating a Context for a Cyber Forensics Course.* In Frontiers in Education Conference 2008 (FIE 2008), Saratoga Springs, NY, October 2008.
[13] Fanelli Robert L. and O'Connor, Terrence J. *Experiences with practice-focused undergraduate security education. In Proceedings of the 3rd international conference on Cyber security experimentation and test* (CSET'10). Washington, DC, August 2010.
[14] O'Leary, Mike. "*Small-Scale Cyber Security Competitions.*" (2012).
[15] Conti, Gregory, Thomas Babbitt, and John Nelson. "*Hacking competitions and their untapped potential for security education*." Security & Privacy, IEEE 9.3 (2011): 56-59.
[16] Hoffman, Lance J., Timothy Rosenberg, Ronald Dodge, and Daniel Ragsdale. "*Exploring a national cybersecurity exercise for universities*." Security & Privacy, IEEE 3, no. 5 (2005): 27-33.
[17] www.dunyayikurtaranhacker.com, 2012
[18] http://www.istsec.org/ctfdetay/, 2009
[19] http://blog.bga.com.tr/2011/05/istsec-istanbul-bilgi-guvenligi.html,2011
[20] http://www.bga.com.tr/calismalar/BGACTF2012_Cozumleri.pdf , 2012
[21] *Siber Güvenlik Yaz Kampı Duyurusu*, Http://www.uekae.tubitak.gov.tr/home.do?ot=5&rt=&sid=0&pid=0&cid=9365, 2013
[22] Ulusal Siber Güvenlik Tatbikatı 2013, http://www.tk.gov.tr/bilgi_teknolojileri /siber_guvenlik/usgt2013.php, Haziran, 2013
[23] http://www.signalsec.com/nopcon-ctf-cozumleri-ve-sunumlari ,6 Haziran 2013, nopCON Security Conference
[24] http://www.davshan.com/, Haziran 2013
[25] Ünal Tatar, Tolga Mataracıoğlu: *Analysis and Implementation of Distinct Steganography Methods*., ISCTurkey'12, pp.298-303
[26] www.md5decrypter.co.uk, Mayıs 2013
[27] http://rumkin.com/tools/cipher/caesar.php, Haziran 2013

**Osman Akın**, Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümünde doktora öğrencisidir. Şimdiye kadar web tabanlı uygulama geliştirme, web güvenliği konularında çalışmış olup şu anda siber güvenlik konusunda çalışmalarını devam ettirmektedir. Doktora programında tez aşamasında olup Bilgisayarlı Görme alanında nesne takibi(object tracking) konusunda çalışmaktadır.

**Işıl Çınar**, Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde yüksek lisans yapmaktadır. Bilgi Sistemleri Güvenliği, Veri Madenciliği, İnsan Bilgisayar Etkileşimi alanlarına ilgi duymaktadır.

**Muhammer Karaman**, Siber güvenlik üzerine 2 yıldır uzman olarak çalışmaktadır. Kurumsal ve ulusal Siber Güvenlik yol haritaları belirleme, siber savaş, siber-elektronik savaş, siber güvenliğin milli güvenliğe entagrasyonu ve siber savaş hukuku konularına ilgi duymaktadır.

**Fatih Bilekyiğit**, Bilgi Sistemlerinin İşletmesi ve Ağ topolojileri üzerine yaklaşık 10 yılı aşkın bir süre çalışmış olup şu an siber güvenlik üzerine çalışmaktadır.