#MİLLİ TEKNOLOJİ HAMLESİ

DENEYAP TÜRKİYE

SİBER GÜVENLİK

LİSE

TÜBİTAK

TÜRKİYE TEKNOLOJİ TAKIMI

TÜBİTAK Deneyap Kitapları 10

Siber Güvenlik
LİSE

Doç. Dr. Çelebi ULUYOL
Doç. Dr. Mehmet DEMİRCİ

TÜBİTAK Deneyap Kitapları *DENEYAP TÜRKİYE*
Projesi kapsamında hazırlanmıştır.

ISBN: 978-605-312-480-1
Yayıncı Sertifika No: 47703

TÜBİTAK Başkanı: Prof. Dr. Hasan MANDAL
Bilim ve Toplum Başkanı: Doç. Dr. Rukiye DİLLİ
Genel Yayın Yönetmeni: Fatma BAŞAR
Editör: Dr. Eda AŞILI
Düzelti: Mustafa ORHAN
Telif İşleri Sorumlusu: Öznur KILIÇKAYA

TÜBİTAK Bilim ve Toplum Başkanlığı
Tunus Caddesi No: 80 Kavaklıdere 06680 Ankara
Tel: (312) 298 96 50
e-posta: deneyap@tubitak.gov.tr
https://yayinlar.tubitak.gov.tr/deneyap-atolyesi

DENEYAP

Teknoloji Atölyeleri

SİBER GÜVENLİK

LİSE

Doç. Dr. Çelebi ULUYOL

Doç. Dr. Mehmet DEMİRCİ

TÜBİTAK

İçindekiler

Sunuş

Ülkemiz çeşitli kademelerde öğrenimlerine devam eden öğrencileri geleceğe hazırlamak için birçok girişimi eş zamanlı olarak hayata geçirmektedir. Gelecekte ülkenin refah ve mutluluğuna katkıda bulunacak, yeni ürünler geliştirecek, geliştirdiği ürünleri ticarileştirerek yurt içi ve yurtdışı satışa sunacak olan öğrencilerin, ürünlerini sergilemeleri için çeşitli eğitim programları, yarışmalar, turnuvalar ve festivaller düzenlenmektedir. Bu bağlamda gençlerimizi geleceğe emin adımlarla taşıyacak önemli girişimlerden birisi de Deneyap Teknoloji Atölyeleri'dir.

Deneyap Teknoloji Atölyeleri'nin genel amacı, gençlere özellikle teknolojik alanda üretme becerisi kazandırmaktır. Bu amaçla ilgisi, becerisi ve yeteneği olan gençlere sistematik ve planlı biçimde hem donanım hem de eğitim desteği verilmektedir. Bu hedeflere ulaşabilmek için 81 ilde Deneyap Teknoloji Atölyeleri kurulmuştur. Bu atölyeler tasarlanırken öğrencilerin girişimcilik, yaratıcı düşünme, eleştirel düşünme, karmaşık problemleri çözme, etkili iletişim ve takım çalışması gibi becerileri kazanmalarına yönelik bir anlayış benimsenmiştir. Ortaokul ve liseye başlangıç seviyesinde olan öğrenciler çeşitli sınavlarla seçilerek 36 ay boyunca ücretsiz eğitimlere katılmaktadır. Seçilen öğrenciler *Tasarım ve Üretim*, *Robotik ve Kodlama*, *Elektronik Programlama ve Nesnelerin İnterneti*, *Nanoteknoloji ve Malzeme Bilimi*, *Havacılık ve Uzay Teknolojileri*, *Siber Güvenlik ve Yapay Zekâ* gibi birçok eğitimden uzman eğiticiler eşliğinde derinlemesine bilgi ve eğitim almaktadır. Toplam 11 farklı teknolojik disiplinde eğitim alan öğrenciler ilk 24 ay sonunda iş birliği içerisinde çalıştıkları gruplarla birlikte bir proje hazırlığı yapıp projelerini sunmaktadır. 24 ay bitiminde ise uzmanlaşmak istedikleri konularla ilgili oluşturdukları takımlarına mentorluk desteği verilerek ulusal ve uluslararası yarışmalara katılmaları için destekler sağlanmaktadır.

Bu kitap, Deneyap Teknoloji Atölyeleri kapsamındaki Siber Güvenlik dersinde öğrencilerimize eğitim verecek eğitmenlerin kullanacağı bir kaynak olarak geliştirilmiştir. İnternetin hayatımızın vazgeçilmez bir parçasına dönüştüğü, çok çeşitli cihazların birbirleriyle haberleştiği nesnelerin interneti teknolojisinin giderek yaygınlaştığı, akıllı telefonlar ve sosyal medya ile birlikte kişisel verilerin daha önce hiç olmadığı kadar kolay erişilebilir hale geldiği bu dönemde siber güvenlik, üzerinde düşünülmesi gereken en önemli konulardan birisidir. Siber güvenlik; bilgisayarlar, akıllı telefonlar, sunucular gibi elektronik sistemlerde tutulan veri ve bilginin, tipi ve biçimi her geçen gün değişen çeşitli saldırılara karşı korunması olarak tanımlanabilir. Bu kapsamda, ağ, uç nokta, veri, kimlik yönetimi, veritabanı, bulut sistemleri ve mobil sistemlerin güvenliği gibi birçok konu üzerinde çalışmalar yapılmakta ve çözümler geliştirilmektedir. Bunun yanı sıra, kullanıcıların siber güvenlik bilincini ve farkındalığını artıran eğitimlerinin sürekli olarak planlanıp hayata geçirilmesi gerekmektedir.

Siber Güvenlik eğitiminde yararlanılmak üzere geliştirilen bu kitapta her ünite için öğretim tasarımı modeli olarak *Gözle, Uygula, Tasarla, Üret ve Değerlendir* adıyla bir öğrenme döngüsü benimsenmiştir (Çetin, Üçgül, Top & Yükseltürk, 2021; Üçgül, Çetin, Yükseltürk & Top, 2021). *Gözle* kısmında öğrencilerin ön bilgileri harekete geçirilmekte, dikkat ve motivasyonları sağlanmakta ve eğitmen tarafından ilgili konu başlıkları detaylı olarak anlatılmaktadır. *Uygula* basamağında gözle kısmında anlatılan konularla ilgili çeşitli örneklerin öğrenciler tarafından yapılması istenmektedir. *Tasarla* kısmında eğitmen rehber pozisyonuna

geçmekte ve öğrenciler daha etkin rol üstlenerek çeşitli uygulamalar yapmaktadırlar. *Üret* kısmında eğitmen planlanan etkinliklerde öğrencilerin aktif rol alarak uygulama yapmalarına rehberlik etmektedir. Son bölüm olan *Değerlendir* kısmında ise öğrenme sürecinde ilgili ünite ile ilgili öğrencilerin çeşitli biçimlerde değerlendirilmesi amaçlanmaktadır.

Kitapta toplam yedi farklı konu başlığı bulunmaktadır. Bu konu başlıkları Siber güvenliğin temelleri, Kali Linux, Parolalar, Kriptografi, Kötü amaçlı yazılımlar, Siber saldırı analizi ve Web saldırıları ve savunma olarak sıralanmıştır. Her ünite içinde yer alan etkinliklere ilaveten, ünitenin sonunda "Ek etkinlik" başlığı altında çeşitli etkinlikler yer almaktadır. Eğitmenlerin kendi sınıfındaki öğrencilerin durumunu, dersin işlenişini veya zaman planlaması gibi çeşitli hususları göz önüne alarak bu etkinlikleri ders içi veya ders dışında uygulamalarında yarar vardır. Eğitmenler tüm etkinliklerin tamamlanması durumunda ise, kendileri de konuyla ilgili olarak öğrencilere daha detaylı uygulamalar yaptırabilirler.

Günümüzün ve geleceğin en önemli konularından birisi olan siber güvenlik alanı ile ilgili olarak, geleceğin siber güvenlik uzmanı olacak öğrencilerimize ve öğrencilerin eğitiminde önemli görevler üstlenen rehber öğretmenlerimize bu kitabın faydalı olmasını dileriz.

Siber Güvenlik Dersi Öğretim Planı Uygulama Kılavuzu

Siber Güvenlik Dersi Bilgi Paketi

Dersin Amacı

Bu dersin amacı, öğrencilere temel siber güvenlik farkındalığını, saldırı ve savunma yöntemlerini açıklama ve sınıflandırma becerilerini, çeşitli uygulamalar vasıtasıyla güvenlik analizi yapma, risklerin ve güvenlik önlemlerinin etkilerini değerlendirme kabiliyetlerini kazandırmaktır. Bu amaç doğrultusunda belirlenen hedefler;

- Siber güvenlik temellerinin öğretilmesi,
- Kali Linux işletim sisteminin tanıtılması,
- Parolalar ve kötü amaçlı yazılımlar gibi kritik siber güvenlik kavramlarının incelenmesi,
- Kriptografiye giriş yapılarak farklı şifreleme, şifre çözme ve şifre kırma yaklaşımlarının uygulamalı olarak tanıtılması,
- Çeşitli siber saldırıların analiz edilmesi ve bunlara karşı kullanılan çözümlerin uygulanmasıdır.

Dersin Çıktıları

Bu dersi alan bir öğrenci;

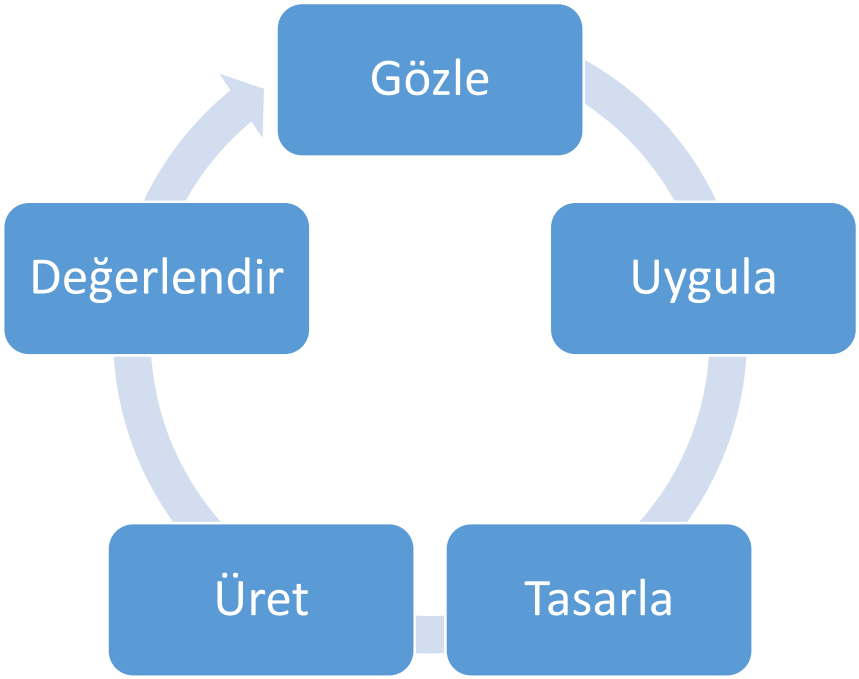
- Bilgi güvenliğinin bileşenlerini, siber tehdit ve siber saldırı kavramlarını örneklerle açıklar.
- Siber saldırıların hedeflerini ve etkilerini analiz eder.
- Linux'taki dizin yapısıyla ilintili temel komutları, dosya içeriği görüntüleme ve dosya kopyalama komutlarını çeşitli şekillerde çalıştırır.
- Linux'taki dosya erişim izinlerini görüntüler, açıklar ve değiştirir.
- Parolaların gücünü analiz eder, güçlü parola seçme yöntemlerini uygular.
- Parola kırma saldırılarının nasıl yapılabileceğini açıklar ve bu saldırıların bazı örneklerini uygular.
- Şifrelemenin genel mantığını açıklar ve basit şifreleme algoritmalarını uygular.
- Şifre kırma yaklaşımlarını tanımlar ve sınıflandırır.
- Frekans analizi ve şifre kırma yöntemlerini tasarlar ve gerçekleştirir.
- Kötü amaçlı yazılımların türlerini ve zararlarını, kötü amaçlı yazılımlardan korunmak için kullanılan teknikleri açıklar.
- Kötü amaçlı yazılımları temel statik analiz yöntemleriyle analiz eder.
- Sosyal mühendislik ve oltalama kavramlarını tanımlar, yöntemlerini açıklar ve uygular.
- Ağ trafiğini izler, bazı ağ saldırısı türlerini açıklar ve uygular.
- Bir web sitesindeki açıklıkları tespit edecek işlemleri yaparak güvenlik analizi yapar.
- SQL enjeksiyonu saldırısı işlem basamaklarını açıklar ve uygular.
- Güvenlik açıklarını tespit ederek gerekli savunma mekanizmalarını tasarlar.

Ders Haftalık Planlaması

- Hafta 1: Bilgi güvenliğinin önemi, temel kavramları ve tanımları, güncel olaylar
- Hafta 2: Kali Linux tanıtımı, temel komutlar ve araçlar
- Hafta 3: Parola kavramı, güçlü parola seçimi, parola tahmin saldırıları, hash algoritmaları
- Hafta 4: Kriptografinin temelleri, basit şifreleme algoritmaları, modern şifreleme algoritmaları, temel kriptanaliz, açık anahtarlı şifreleme, sayısal imza
- Hafta 5: Kötü amaçlı yazılım (malware) kavramı ve çeşitleri, antivirus yazılımları, malware tespit yöntemleri, oltalama (phishing), sosyal medyanın güvenli kullanımı
- Hafta 6: Siber saldırıların sınıflandırılması ve analizi, sızma yöntemleri, ağ trafiği izleme, DoS/DDoS
- Hafta 7: Web güvenliği, web uygulama saldırıları ve savunma yöntemleri, SQL enjeksiyonu, XSS saldırıları
- Hafta 8: Yarışma

Derste Kullanılacak Öğretim Tasarım Modeli

Bu derste ayrıntıları aşağıda verilecek olan gözle, uygula, tasarla, üret ve değerlendir öğrenme döngüsü kullanılmıştır (Çetin, Üçgül, Top & Yükseltürk, 2021; Üçgül, Çetin, Yükseltürk & Top, 2021).



Şekil 1. Öğrenme Döngüsü

Gözle: Bu bölüm iki kısımdan oluşur. Birinci kısımda eğitmenden öğrencilerin geçmiş bilgilerini aktive etmesi ve onların dikkat ve motivasyonlarını sağlaması beklenmektedir. . Eğitmen öğrencilerin geçmiş bilgilerini aktive etmek ve onların dikkatini çekmek için bir önceki derste yapılan etkinlikleri / çalışmaları kısaca özetleyebileceği gibi günlük yaşamdan ilgi çekici örnekler de kullanabilir. Bu bölümün ikinci kısmında eğitmen bir konuyu uygulamalı olarak (göstererek) anlatır. Bu kısımda eğitmen daha aktiftir. Uygulamayı yaparken öğrencilere sorular sorabilir ve öğrencilerin sorularını yanıtlayabilir.

Uygula: Bu bölümde eğitmen öğrencilerden bir önceki bölümde gösterilen uygulamaların aynısını veya bir benzerini ister / birlikte yapar. Örneğin, öğrenilen bir komutun örneklerini gözle kısmında gösteren eğitmen, öğrencilerden komutu yeni örneklerde daha farklı şekillerde kullanmalarını isteyebilir.

Tasarla: Bu bölümde öğrenciler daha aktif rol üstlenir. Eğitmen rehber pozisyonundadır. Eğitmen, öğrencilere takıldıkları noktalarda destek olacaktır. Öğrencilerin etkinlikten kopup motivasyonlarının düşmesine izin vermemeye çalışacaktır. Fakat eğitmenin sağladığı destek gereğinden fazla da olmamalıdır. Bu bölümde eğitmen tarafından öğrencilere bir problem verilir. Öğrencilerden öncelikle bu problemin çözümünü tasarlamaları istenir. Tasarlama aşamasında öğrenciler temel itibariyle bilinenler ile istenenler arasındaki bağı kurarak bir plan üreteceklerdir. Bu amaçla öğrenciler (Bilgi işlemsel düşünme becerisi bileşenlerini kullanırlar):

- Bilinenleri ve istenilenleri ayrı ayrı belirler,
- İstenilenleri alt bileşenlere ayrılabiliyorsa ayırır,
- Bu problem veya alt problemlerin aynılarına veya benzerlerine daha önceden çözüm ürettiyse bunları tanımlar,
- Bu problemler veya alt problemlerin çözümü için bilgisayar biliminde daha önceden belirlenmiş çözümlerin (sıralama ve arama algoritmaları gibi) olup olmadığını belirler,
- Daha önceki adımlarda ortaya koyduklarını kullanarak bir çözüm planı üretir.

Bu aşamadaki önemli nokta, öğrencilerin çözüme doğrudan başlaması yerine önce çözüm hakkında düşünmesi ve bir çözüm planı üretmesidir. Öğrenciler her defasında yukarıda bahsi geçen beş adımı yapmak istemeyebilir veya bu adımları yaparken sıkılabilir. Bu durumlarda, öğrencilerin adımları bire bir uygulaması yönünde zorlamak yerine onlardan problemi doğrudan çözmeye başlamadan önce problem hakkında düşünmesi ve planlama yapması istenebilir.

Üret: Bu bölümde öğrenciler aktif rol üstlenir. Eğitmen rehber pozisyonundadır. Eğitmen öğrencilere takıldıkları noktalarda destek olacaktır. Destek, bireyin yardım ile gerçekleştirebileceği, ancak henüz bağımsız olarak yapamayacağı bir durum oluştuğunda sağlanmalıdır. Eğitmen, bu durumda öğrencilerin sordukları sorulara geri bildirim vererek onları yönlendirebilir. Gerektiğinde İnternet üzerinden çeşitli örnekleri görmeleri için yönlendirme yapabilir. Eğitmen, öğrencinin aktif katılımı ve problemi grup içerisinde birlikte çözmelerine ve algoritmik düşünme biçimlerine izin veren bir yapıda rehberlik etmek durumundadır. Üret aşamasında, öğrencilerden bir önceki adımda tasarladığı planı kullanarak probleme algoritmik bir çözüm üretmesi istenebilir. Öğrenciler bilgisayar başında çalışarak gerekli yazılım çözümlerini geliştirirler.

Değerlendir: Buradaki değerlendirme ile anlatılmak istenen doğrudan öğrencinin başarısının notlandırılması değildir. Temel hedef, öğrencinin öğrenme sürecinde yaşadıkları ve öğrendikleri üzerine düşünmesini sağlamaktır. Bu sayede öğrenci; problem çözme, dersin konusu ve kendisi ile ilgili gözlemler yaparak yeni öğrenmeler, kendisini değerlendirme ve planlama açısından fırsatlar elde edecektir. Öğrencilerden şu soruları yanıtlamaları istenebilir:

- Verilen problemi tanımlayınız (problemi kendi cümleleri ile ifade etme).
- Problemin çözümü için hangi stratejileri kullandınız ve neden bu stratejileri seçtiniz?
- Problemi çözerken ne gibi sıkıntılar yaşadınız ve bunların üstesinden gelmek için neler yaptınız?
- Kullandığınız yöntemler, bu sıkıntıları gidermekte başarılı oldu mu?
- Grup arkadaşınızla ihtilafa düştüğünüz durumlar oldu mu ve bunların üstesinden gelmek için neler yaptınız?
- Grup arkadaşınızdan ne öğrendiniz?

Öğrencilerden buradaki soruların tamamına cevap vermesi beklenmemektedir. Bu sorulardan, verilen etkinlikten elde ettikleri deneyimlere bağlı olarak, kendilerine uyanları cevaplayabilirler. Cevaplar, öğrencilerden yazılı olarak da istenebilir. Fakat öğrenciler, belirli bir süre sonra sürekli aynı sorulara cevap vermekten sıkılabilir/sıkılacaktır. Bu durumda, belirli derslerin sonunda öğrencilerden genel olarak dersteki deneyimlerini değerlendirmeleri istenebilir.

Derste Kullanılacak Programların Tanıtımı

- Dersin belli haftalarında kullanılacak olan Kali Linux, siber güvenlik odaklı geliştirilmiş olan ve içinde güvenlikle ilgili birçok yazılımı bulunduran bir dağıtımdır. Web sayfası: https://www.kali.org/

- Kali Linux kurulumu için bir sanallaştırma yazılımı olan VirtualBox kullanılacaktır. Web sayfası: https://www.virtualbox.org/

- 3. haftada Kali Linux üzerinde yer alan John the Ripper adlı parola kırma aracıyla deneyler yapılacaktır.

- 5. haftada Microsoft Defender Antivirus ve Microsoft Word kullanılacaktır.

- 6. Haftada Wireshark adlı paket izleme yazılımı kullanılacaktır. Web sayfası: https://www.wireshark.org/

- 7. haftada Microsoft Access kullanılacaktır.

Eğitmenin Kullanacağı Diğer Teknolojik Araçların Tanıtımı

Öğrenme Yönetim Sistemi (ÖYS): Derste aktif şekilde kullanılacak olan temel ortamlardan biri öğrencilerin ilgili derse kullanıcı kaydı yapacakları bir Öğrenme Yönetim Sistemidir. Deneyap Teknoloji Atölyeleri tarafından Moodle açık kaynaklı popüler bir öğrenim yönetim sistemi kullanılacaktır.

Siber Güvenlik dersi için Moodle aşağıdaki amaçlara hizmet etmektedir:

- Dersle ilgili genel duyuruların iletilmesi
- Öğrencilere sunulacak öğrenme materyallerinin paylaşılması
- Grup olarak oluşturulacak ürün ya da tamamlanan görevlerin teslimi
- Eğitmenin öğrenci ürünlerini takip etmesi ve geri bildirim sağlaması
- Öğrenci-eğitmen, öğrenci-öğrenci ve eğitmen-eğitmen etkileşiminin atölye dışında da sürdürülmesi
- Gerektiğinde BigBlueButton aracılığıyla senkron (canlı) ders ortamının oluşturulması (Oluşturulan canlı ders çalışma odaları destekli olup grup çalışmalarına imkân vermektedir.)
- Eğitmen eğitimleri sürecinde gerekli kaynakların, sunumların ve dokümanların eğitimcilerle paylaşılabilmesi
- Eğitimcilerin fikir alışverişi yapabilmesi için tartışma ortamlarının kurulabilmesi

Siber Güvenlik Dersi için Etik Kılavuzu

Bilişim teknolojilerinin doğru bir şekilde kullanımı için Uluslararası Bilgisayar Etik Enstitüsü tarafından uyulması gereken kurallar sıralanmıştır. Eğitmen öğrencilerine siber güvenlik ile ilgili uygulamalar geliştirirken aşağıda sıralanan etik unsurları unutmamaları gerektiğini mutlaka hatırlatmalıdır. Bu kurallar şu şekilde özetlenebilir:

- Bilişim teknolojileri başkalarına zarar vermek için kullanılmaz.
- Başka bir kişiye ait veriler izinsiz incelenmez.
- Başkalarının oluşturduğu çalışmalar izinsiz karıştırılmaz.
- Bilişim teknolojileri hırsızlık için kullanılmaz.
- Bilişim teknolojileri yalancı şahitlik için kullanılmaz.
- Lisanssız, kopya ya da kırılmış yazılımlar kullanılmaz.
- Başka birisi tarafından bilişim teknolojileri ile oluşturulmuş çalışmaları kendinize mal edemezsiniz.
- Yazdığınız kod, program ya da yazılımların/sistemlerin sonuçlarını göz önüne almak zorundasınız.
- Bilişim teknolojilerini diğer insanlara saygı duyarak kullanmalısınız.

Kaynaklar

Çetin, İ., Üçgül, M., Top, E. & Yükseltürk, E. (2021). Robotik Kodlama: Lise. İ. Pirpiroğlu Gencer., K. Bal Çetinkaya, (Ed.), *Robotik kodlama: lise* (ss. 1-5). Ankara: TÜBİTAK Popüler Bilim Kitapları.

Üçgül, M, Çetin, İ.,Yükseltürk, E. & Top, E. (2021). Robotik Kodlama: Ortaokul. İ. Pirpiroğlu Gencer., K. Bal Çetinkaya, (Ed.) *Robotik kodlama: ortaokul* (ss. 1-5). Ankara: TÜBİTAK Popüler Bilim Kitapları.

HAFTA 1. SİBER GÜVENLİĞİN TEMELLERİ

AMAÇ

Bu bölümün amacı, öğrencilere siber güvenliğin temel kavramlarını tanıtmaktır. Bu kapsamda, bilgi güvenliğinin bileşenleri ile siber tehdit, siber saldırı gibi terimler örneklerle açıklanacaktır. Öğrencilerin uygulama ve vaka çalışmalarıyla bilginin temel özellikleri, siber saldırılar ve olası etkileri hakkında öğrendiklerini göstermeleri ve pekiştirmeleri hedeflenmiştir.

BÖLÜM KAZANIMLARI

Bu bölümü tamamlayan bir öğrenci,

- Bilgiyi ve bilgi güvenliğini tanımlar.
- Bilgi güvenliğinin bileşenlerini örneklerle açıklar.
- Siber tehdit ve siber saldırı kavramlarını açıklar.
- Siber saldırıların hedeflerini ve etkilerini analiz eder.

KULLANILACAK MATERYAL VE ARAÇLAR

Bilgisayar, kâğıt, kalem

HAFTANIN İŞLENİŞİ

Gözle	Bilgi güvenliğinin temel bileşenleri Siber tehditler ve siber saldırılar Siber saldırıların hedefleri ve alınabilecek önlemler

Uygula	Bilgi güvenliğinin temel bileşenlerini örnek olaylarla eşleştirme
Tasarla ve Üret	Siber saldırı vaka çalışması ve savunma stratejisi tasarımı
Değerlendir	Haftanın içeriğinin değerlendirilmesi ve çalışmanın devam ettirilmesine yönelik öneriler

1. GÖZLE: TEMEL KAVRAMLAR

Bu bölümde bilgi güvenliği ve siber güvenlik ile ilgili temel kavramlar tanıtılarak tartışılacaktır.

1.1. GİRİŞ

Eğitmen öğrencilere siber güvenliğin ne olduğunu ve önemini örneklerle açıklar. Bu kısımda aşağıdaki açıklamalar ve örnekler ile birlikte eğitmenin ekleyeceği örnekler kullanılabilir. Bu bölüm için 15 dakika yeterlidir.

Siber güvenlik, bilgisayar sistemlerinin ve bilgisayarlarda saklanan bilginin güvenliğidir. Günümüzde bilginin büyük çoğunluğu bilgisayar ortamında üretilmekte ve saklanmaktadır. Bu nedenle kişisel bilgisayarların, mobil telefon ve tabletlerin, sunucuların, diğer elektronik cihazların ve bunlardan oluşan ağların korunması çok önemlidir.

Yarın sabah bilgisayarınızı açtığınızda siyah bir ekran üzerinde şu mesajı gördüğünüzü düşünün: “Bütün dosyalarınız ve programlarınız erişime kapatılmıştır. Eğer 48 saat içinde hesabımıza 10 bin TL değerinde Bitcoin göndermezseniz bütün dosyalarınız yok edilecektir.” Sonra telefonunuzdan e-postanıza giriş yapmaya çalışıyorsunuz ama yapamıyorsunuz çünkü birisi hesabınızı ele geçirerek parolanızı değiştirmiş. Mesajlarınıza baktığınızda fark ediyorsunuz ki telefonunuzda kayıtlı bütün yazışmalar rehberinizdeki herkes ile paylaşılmış, bütün arkadaşlarınız sizinle alay ediyor.

Bu kâbus gibi senaryo gerçekleşirse neler yapabiliriz? Daha önemlisi, böyle bir senaryoyla karşılaşmamak için nasıl davranmalı, ne gibi önlemler almalıyız? Siber güvenlik dersinde, kişileri yukarıda verilen örneklerdeki gibi zor durumlara sokabilen, hatta bazen ülkelerin güvenliğini tehdit edebilen siber saldırılardan korunma yöntemlerini inceleyeceğiz.

Eğitmen öğrencilere siber güvenliğin önemine ilişkin bildikleri başka örnek olaylar olup olmadığını sorarak tartışma yürütür.

1.2. BİLGİ GÜVENLİĞİNDEKİ TEMEL KAVRAMLAR

Eğitmen öğrencilere "Bilgi nedir" sorusunu sorarak kısa bir tartışma yürütür. Öğrenciler 3-4 kişilik gruplar halinde tartışarak tanımlarını yazabilirler. Sonrasında eğitmen grupların tanımlarını aşağıdaki bilgiler çerçevesinde yorumlar ve geri bildirim yapar. Bölüm 1.2 için toplam 45 dk süre yeterlidir.

Bilgi farklı şekillerde tanımlanabilir. Türk Dil Kurumu sözlüğündeki tanımlardan birinde bilgi için "*öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek*" ifadesi kullanılmıştır.

Cambridge sözlüğünde ise bilgi (information), "*bir durum, kişi, olay vb. hakkındaki gerçekler*" olarak tanımlanmıştır.

Örneğin; bir kişiye ait isim, T.C. kimlik no, adres, fotoğraf, okuduğu okul/çalıştığı işyeri vb. bilgiler onun kişisel bilgileridir. Bir kurumun işleyişiyle ilgili olarak belli kişi veya grupların sahip olduğu bilgi ise kurumsal bilgidir. Belli kişi veya kurumların parayla ilgili işlemleri hakkındaki bilgiye finansal bilgi denir. Bilginin bu gibi farklı türlerinin hepsi için güvenlik önemli bir hedeftir.

Bu noktada öğrencilere "Bilgi güvenliğinden ne anlıyorsunuz" sorusu sorularak 3-4 kişilik gruplar halinde tartışmaları istenir.

Gruplar fikirlerini belirttikten sonra eğitmen aşağıdaki tanımlar çerçevesinde geri bildirim yaparak her grubun fikirlerini yorumlar ve sonrasında aşağıda açıklanan her temel kavram hakkında ayrıntılı anlatıma geçer.

Bilgi güvenliği, bilginin birtakım temel özelliklerinin korunması anlamına gelir. Bu özelliklerden başlıcaları aşağıda verilmektedir. Aşağıdaki Şekil 1 benzeri bir şekil tahtaya çizilebilir veya sanal ortamda gösterilebilir.

Şekil 1. Bilgi Güvenliğinin Bileşenleri

Gizlilik: Sadece yetkisi olan kişilerin bilgiyi görebilmesidir. Bir başka deyişle, yetkisiz kişilerin bilgiye ulaşamaması, onu okuyamaması anlamına gelir.

Bilginin gizli olup olmadığını ve onu görmeye kimin yetkili olduğunu genellikle bilginin sahibi veya bilgiyi üreten belirler.

Öğrencilere "Sizce hangi bilgilerin gizli olması gerekir?" sorusu sorularak örnek vermeleri istenir. Aşağıdaki örnekler ve benzerleri ile tartışma zenginleştirilir.

Örnek olarak;

- Bir kurumun çalışanlarına ait ev adresi ve çocuklarının adları gibi kişisel bilgiler,
- Bir kuruluşa ait ticari sırlar,
- Kişinin cep telefonuna gelen mesajlar

gibi bilgilerin belli bir gizliliğe sahip olması gerekir.

Not: Aynı türdeki her bilginin aynı gizlilik düzeyine sahip olma zorunluluğu yoktur. Örneğin telefona gelen bayram tebrik mesajı gizli olmayabilir ama banka hesabına girebilmeniz için gelen tek kullanımlık şifreyi içeren mesaj gizli olmalıdır. Hangi bilginin kime açık kimden gizli olduğu da duruma bağlıdır mesela bir kuruluşun ticari sırlarını en üst düzeydeki bazı yöneticiler bilebilir ama bu bilgiler tanımlı birkaç kişi dışındaki herkesten gizli olmalıdır.

Bilgi güvenliğinde gizliliği korumakta kullanılan temel araç olan **şifreleme**, önümüzdeki derslerde incelenecektir.

Bütünlük: Bilginin gerçeğe aykırı biçimde değişmemesi anlamına gelir. Bazı bilgiler (örn. adres) zaman içinde değişebilir veya bilginin kaynağından güncellenebilir (örn. kişinin kendi siparişini iptal etmesi). Böyle değişimler bütünlüğü ihlal etmez. Ancak bilginin kaynağı veya onu değiştirmeye yetkili kişiler dışında birilerinin bilgide değişiklik yapması bütünlüğü bozar.

Örnek olarak aşağıdaki durumlar bütünlüğe aykırıdır:

- Kardeşinizin telefonunuzda kayıtlı isimleri değiştirmesi,
- İnternetten indirdiğiniz bir dosyanın siz açana kadar herhangi bir nedenle bozulması,
- Annenizin yemek tarifi defterinde bulunan kek tarifindeki "2 su bardağı şeker" yazısını "4 su bardağı şeker" diye değiştirmeniz.

Sonuçta, bilginin gerçeğe aykırı biçimde değişmediğinin garanti edilmesi, eğer değiştiyse bunun bilinmesi çok önemlidir. Bunu sağlamak için bazı matematiksel yöntemler kullanılır. Bu yöntemler önümüzdeki derslerde incelenecektir.

Not: Bütünlük ile gizlilik birbirinden farklıdır. Birinin varlığı diğerini garanti etmez. Her ikisini de sağlamak için farklı teknikler bir arada kullanılmalıdır.

Erişilebilirlik: Bilgiye ulaşılabilmesi anlamına gelir. Bilgiye erişim yetkisi olan kişilerin istedikleri zaman erişip erişemediğinin ve ne oranda erişebildiğinin ölçüsüdür.

Örneğin, sınav sonuçlarının açıklandığı web sitesinin çökmesi veya bazı kullanıcılara yanıt verememesi erişilebilirliği zedeler. Erişilebilirlik değerlendirilirken yüksek sayıda kullanıcının oluşturduğu yoğun yük altındaki duruma ağırlık verilmelidir. Örneğin bir web sitesinin normal durumda çalışması yetmez, asıl önemli olan binlerce kişi aynı anda girmeye çalıştığında sitenin düzgün çalışıp çalışmadığıdır.

Erişilebilirlik bilgi güvenliğinin en sık hedef alınan boyutlarından biridir. Erişilebilirliğe zarar vermeyi amaçlayan hizmet engelleme (denial of service, DoS) saldırıları önümüzdeki derslerde incelenecektir.

Gerçeklik: Bilginin uydurma olmaması, içeriğinin, kaynağının, üretilme zamanının vs. doğru olması anlamına gelir.

Örneğin bir arkadaşınıza şaka yapmak için pideciyi arayıp kendinizi arkadaşınızın adıyla tanıtıp onun adresine gönderilmek üzere vereceğiniz lahmacun siparişi, gerçek olmayan bir bilgidir. Bunun gibi gerçek olmayan bilgilerin fark edilmesi, gerçek bilgilerin ise gerçekliğinin ispat edilmesi bilgi güvenliğinin önemli bir parçasıdır.

İnkâr edilemezlik: Bilgiyi üretenin bilginin gerçekliğini inkâr edememesi anlamına gelir. Bütünlük ve gerçeklik özelliklerinin bir arada bulunması olarak düşünülebilir.

Örnek olarak, bir belgeye imza atan bir kişi sonradan "Bunu ben imzalamadım." diyememelidir. Yani imza, inkâr edilemezlik özelliğini sağlamalıdır.

Sorumluluk: Bilgiyle ilgili işlemleri (üretme, erişme, değiştirme vb.) kimin yaptığının belli olması ve bir sorun çıkması durumunda kimden hesap sorulacağının bilinmesi anlamına gelir.

2. UYGULA

Eğitmen öğrencilere "Aşağıdaki örnek olayların her biri bilginin hangi temel özelliklerine zarar verir?" sorusunu sorarak 3-4 kişilik gruplar halinde tartışmalarını ve yanıtlarını yazmalarını ister. Eğitmen her olayın bir veya birden fazla özelliğe zarar verebileceğini belirtir. Bu örnek olaylar eğitmen tarafından çoğaltılabilir. Bu uygulamada grup çalışması için 10 dk, sonrasındaki tartışma için 20 dk olmak üzere 30 dk yeterlidir.

1. Arkadaşın senin telefonundaki mesajların hepsini okumuş.
2. Uzaktan eğitim sistemi çöktüğü için ders kayıtlarına ulaşamıyorsun.
3. Ödevini öğretmenine teslim etmiştin ama kapak sayfası kopup düşmüş ve kaybolmuş.
4. Arkadaşın sana gelen bir mesajı okumuş sonra da silmiş.
5. Birileri okulun web sayfasındaki bazı duyuruları izinsiz olarak yok etmiş.

Doğru yanıtlar:

1. Gizlilik
2. Erişilebilirlik
3. Bütünlük
4. Gizlilik ve bütünlük (artı erişilebilirlik de olabilir)
5. Bütünlük ve erişilebilirlik

Gruplar fikirlerini açıklar. Eğitmen geri bildirim yaparak her grubun fikirlerini yorumlar ve tartışmayı yönetir.

3. GÖZLE: SİBER TEHDİTLER VE SALDIRILAR

Bu bölüm için toplam 50 dk süre yeterli olacaktır.

Bölümün başında öğrencilerin gruplara ayrılıp aşağıdaki sorular hakkında tartışma yürütmeleri sağlanır. Daha sonra eğitmen gruplardan yanıtlarını paylaşmalarını ister.

- Siber güvenliğin korunmadığı durumlarda ne gibi olumsuz sonuçlar ortaya çıkabilir?
- Siber saldırı yapan kişilerin hedefleri neler olabilir?

Eğitmen tartışmayı aşağıdaki açıklamalar ışığında devam ettirir.

Siber güvenlik gerektiği gibi korunmazsa,

- Maddi kayıp,
- İtibar kaybı,
- Psikolojik zarar,
- Fiziksel hasar

gibi sonuçlar ortaya çıkabilir.

Bir akıllı telefonu koruyucu kılıfla kullanıp yere düşürmemeye özen göstermek onu fiziksel hasardan korumak için gereklidir. Telefonu kaybetmemek ve çaldırmamak için dikkatli davranmak da önemlidir. Ancak bunun gibi önlemler siber güvenliği sağlamak için yeterli değildir. Çünkü günümüzde çok çeşitli siber tehditler ve saldırılar vardır.

Siber güvenlikte **tehdit (threat)**, "*sistemlere ve kuruma zarar verebilecek bir olayın nedeni*" olarak tanımlanır (International Organization for Standardization, 2018). Tehditler kasıtlı ve kasıtlı olmayan (kazara oluşan) olarak ikiye ayrılır. Kasıtlı tehditlere hackerlar, casuslar, suç örgütleri vb. örnek verilebilir.

Burada öğrencilere "Kasıtlı olmayan (kazara oluşan) tehditler neler olabilir?" sorusu sorularak örnek vermeleri istenir. Aşağıdaki örnekler ve benzerleri ile tartışma zenginleştirilir.

Kazara oluşan tehditler; doğal afetler (deprem, sel, yangın vb.), arıza kaynaklı elektrik veya internet kesintileri, bilgisayar arızaları gibi şeylerdir.

Siber saldırı (cyber attack), "*sistem güvenliğini hedef alan akıllı bir tehdit kaynaklı saldırı*" olarak tanımlanır (Shirey, 2000). Yani kasıtlı olmayan tehditler nedeniyle ortaya çıkan durumlara saldırı denmez. Siber tehdit (cyber threat) kavramı da siber saldırıların kaynağında olan kişilerin saldırıda kullandıkları yöntemleri ve hareketleri ifade eder.

Siber saldırı yapan kişiler, aşağıdakilerden birini veya birkaçını hedefleyebilirler:

- Maddi kazanç elde etme,
- Şöhret elde etme ve bununla övünme,
- Karşı tarafa maddi veya manevi zarar verme,
- Önemli bilgileri belli bir amaçla çalma, (örn. casusluk)

Siber saldırı yapan kişilere genel olarak **saldırgan (attacker)** denir. Saldırganlar için kullanılan bir diğer terim **siyah şapkalı (black hat) hacker** terimidir. Siyah şapkalı hacker, siber güvenliği ihlal ederek karşı tarafa zarar vermek veya maddi kazanç elde etmek isteyen kişi demektir. **Beyaz şapkalı (white hat) hacker veya etik hacker** kavramı ise, bir kurumun izniyle o kuruma ait bilgisayar sistemlerini saldırılara dayanıklılık ve güvenlik açısından test edip değerlendiren kişileri tanımlar.

Siber saldırılarla ilgili "Neden?" sorusunu tartıştık. Bir diğer önemli soru da "Nasıl?" sorusudur. Siber saldırıların nasıl yapıldığını önümüzdeki derslerde örnekler ve uygulamalarla birlikte ayrıntılı olarak göreceğiz.

Genel olarak siber tehditler, sistemlerde bulunabilecek **zayıflıkları (zafiyetleri)** kullanırlar. En basit ve yaygın zayıflık, insanlarda siber güvenlikle ilgili **farkındalık** eksikliğidir. Bu dersi alan öğrenciler toplumun büyük bir çoğunluğundan daha fazla bilgiye ve farkındalığa sahip olacaklardır.

Siber tehditler çok çeşitlidir:

- Kötü amaçlı yazılımlar (virüs, casus yazılım vb.),
- Oltalama (phishing),
- Hizmet engelleme (denial of service, DoS),
- Veri sızdırma,
- Yetki çalma,
- Aradaki adam (man in the middle) saldırıları

yaygın siber tehditlere örnek olarak verilebilir.

Tehditlerin zarar vermesini engellemek veya zararlarını azaltmak için bazı **önlemler** alınır. Bu noktada öğrencilerden bildikleri önlemleri söylemeleri istenebilir. En başta gelen önlem, farkındalığın artırılmasıdır. Sıkça kullanılan bazı diğer önlemler şunlardır:

- Kimlik doğrulama ve erişim denetimi araçları (parolalar, akıllı kartlar, biyometrik sistemler vb.): Sistemlere yetkili kişilerin erişebilmesini, diğer kişilerin erişiminin engellenmesini sağlayan araçlardır.

- Güvenlik yazılımları (antivirüs, bilgisayardaki güvenlik duvarı vb.): Sistemin zararlı yazılımlardan ve internet üzerinden gelebilecek olan zararlı trafikten korunmasına yardımcı olan yazılımlardır.
- Güvenlik cihazları (sızma tespit sistemi – IDS, donanım güvenlik modülü – HSM, derin paket inceleme cihazı – DPI vb.): Genellikle bilgisayarların bağlı olduğu ağların içinde konuşlanan, ağ trafiği üzerinde incelemeler yapan ve çeşitli güvenlik kurallarını uygulayan cihazlardır.
- Güvenli yazılım geliştirme teknikleri: Yazılımlarda saldırganların kullanabileceği zayıflıkların ortaya çıkmasını önleme amaçlı yöntemlerdir.
- Kriptografi ve güvenli iletişim teknikleri: Gönderici(ler) ile alıcı(lar) arasında iletilen verinin temel güvenlik özelliklerini (gizlilik, bütünlük, kimlik doğrulama vb.) korumakta kullanılan yöntemlerdir.

Siber güvenlik ancak bu gibi önlemlerin bir arada kullanılmasıyla sağlanabilir. Hiçbir önlem tek başına yeterli güvenlik sağlayamaz.

3. TASARLA VE ÜRET: VAKA ÇALIŞMASI

Bu bölüm için toplam 45 dk süre yeterli olacaktır.

Bu bölümde, son yıllarda dünyada gerçekleşen bazı siber saldırılar hakkında tartışma yürütülecek ve bu saldırılara karşı alınabilecek temel güvenlik önlemleri düşünülerek çözümler tasarlanacaktır. En az iki, süre yeterse üç farklı vaka incelenebilir. Aşağıda bazı örnek olaylar verilmiştir. Eğitmen güncel olayları araştırarak bunlara eklemeler yapabilir.

- **WannaCry fidye yazılımı saldırısı (2017):** Bu saldırı, Microsoft Windows işletim sistemine sahip bilgisayarları hedef alan bir kripto-solucan tarafından, verileri şifreleyerek ve Bitcoin kripto para biriminde fidye ödemeleri talep ederek gerçekleştirilen dünya çapında bir siber saldırıydı. Windows sistemlerinde bulunan bir açıklıktan faydalanıyordu. Her ne kadar Microsoft bu açıklığı kapatmak için daha önce yamalar yayınlamış olsa da, WannaCry genellikle bu yamaları uygulamayan veya kullanım ömrünü doldurmuş eski Windows sistemlerini kullanan kuruluşlarda hızla yayılmayı başardı. Bu yamalar bir kuruluşun siber güvenliği için zorunluydu, ancak çoğunlukla ihmal, cehalet, yanlış yönetim, personel veya zaman yetersizliği ve

durumun öneminin farkında olmama gibi nedenlerle uygulanmamıştı (Whittaker, 2019).

- **Air India veri sızıntısı (2021):** 21 Mayıs 2021'de Air India adlı havayolu şirketinin bir siber saldırıya maruz kaldığı ve dünya çapında yaklaşık 4,5 milyon müşterinin pasaport, kredi kartı bilgileri, doğum tarihleri, isim ve bilet bilgileri dâhil kişisel bilgilerinin ele geçirildiği bildirildi (Satija, 2021).
- **Microsoft Exchange Server veri sızıntısı (2021):** Şirket içi Microsoft Exchange Server'daki dört sıfırıncı gün açıklığı (henüz varlığı bilinmeyen veya bilindiği halde giderilmemiş açıklık) üzerinden Ocak 2021'de başlatılan küresel bir siber saldırı dalgası sonucunda saldırganlar, etkilenen sunuculardaki kullanıcı e-postalarına ve parolalarına tam erişim, sunucuda yönetici ayrıcalıkları ve ağa bağlı cihazlara erişim izni elde ettiler. Saldırganlar, sunuculara tam erişime izin veren bir arka kapı kurarak saldırıları gerçekleştirdiler. 9 Mart 2021 itibariyle, ABD'deki yaklaşık 30.000 kuruluş, Birleşik Krallık'taki 7.000 sunucu ve Avrupa Bankacılık Otoritesi, Norveç Parlamentosu ve Şili Mali Piyasa Komisyonu sunucuları da dâhil olmak üzere toplam 250.000 sunucunun saldırılara kurban gittiği tahmin edildi (Duffy, 2021; O'Donnell, 2021). Küçük ve orta ölçekli işletmeler, yerel kurumlar ve yerel yönetimler, siber güvenliği sağlama konusunda genellikle daha küçük bütçelere ve daha az deneyime sahip oldukları için saldırının ana kurbanları olarak öne çıktılar (Whittaker, 2021).

Önce eğitmen tarafından örnek olay birkaç cümleyle anlatılır. Daha sonra öğrenciler 3-4 kişilik gruplara bölünerek incelenen saldırı hakkında aşağıdaki soruları yanıtlamaya çalışmaları istenir. Daha sonra her gruba yanıtları sorularak bu yanıtlar tartışılır.

- Bu saldırıyı yapanlar ne elde etmeyi hedeflemiş olabilirler?
- Bu saldırının zararları neler olabilir?
- Bu saldırının zararlarını azaltmak için neler yapılabilir?
- Bu saldırıdan korunmak için alınabilecek güvenlik önlemleri nelerdir?
- Yukarıda bahsedilen önlem çeşitlerinden üçünü seçerek bu saldırıya karşı bir savunma yaklaşımı tasarlamak isteseniz neleri seçersiniz? Neden?

4. DEĞERLENDİR

Bu bölüm için 15 dk süre yeterli olacaktır.

Eğitmen öğrencilerine aşağıdaki soruları sorarak yanıtları üzerinden tartışmayı yönlendirir.

- Günlük hayatınızda siber güvenliğe ilişkin hangi önlemleri alıyorsunuz?
- Bu dersten sonra daha fazla dikkat edeceğiniz veya farklı yapacağınız bir şey var mı?
- Sizi en çok endişelendiren siber tehdit hangisidir?

5. EK ETKİNLİK: SİBER SALDIRI TASARLAMA

Eğitmen öğrencilerin gruplar halinde aşağıdaki etkinliği yapmalarını sağlar.

Bir siber savaş durumunda düşmanı zor durumda bırakacak bir saldırı yapmak istediğinizi düşünerek aşağıdaki soruları cevaplayınız ve sonrasında cevaplarınızı diğer gruplarla paylaşınız.

- Saldırıda neyi hedef alacaksınız?
- Saldırıdan elde etmek istediğiniz sonuçlar nelerdir?
- Bu saldırı için kaç kişilik bir ekibe ve ne kadar zamana ihtiyaç duyacağınızı tahmin ediyorsunuz?

KAYNAKLAR

Duffy, C. (2021). Here's what we know so far about the massive Microsoft Exchange hack. *CNN Business*. 24.10.2021 tarihinde https://edition.cnn.com/2021/03/10/tech/microsoft-exchange-hafnium-hack-explainer/index.html adresinden erişim sağlanmıştır.

International Organization for Standardization. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO Standard No. 27000:2018). https://www.iso.org/standard/73906.html

O'Donnell, J. (2021). European banking regulator EBA targeted in Microsoft hacking. *Reuters*. 24.10.2021 tarihinde https://www.reuters.com/article/us-microsoft-hack-eba-idUSKBN2B01RP adresinden erişim sağlanmıştır.

Satija, R. (2021). Cyber-attack on Air India led to data leak of 4.5 million fliers. *Bloomberg*. 24.10.2021 tarihinde https://www.bloomberg.com/news/articles/2021-05-22/cyber-attack-on-air-india-led-to-data-leak-of-4-5-million-fliers adresinden erişim sağlanmıştır.

Shirey, R. (2000). RFC2828: Internet security glossary. https://datatracker.ietf.org/doc/html/rfc2828

Whittaker, Z. (2019). Two years after WannaCry, a million computers remain at risk. *TechCrunch*. 24.10.2021 tarihinde https://techcrunch.com/2019/05/12/wannacry-two-years-on/ adresinden erişim sağlanmıştır.

Whittaker, Z. (2021). America's small businesses face the brunt of China's Exchange server hacks. *TechCrunch*. 24.10.2021 tarihinde https://techcrunch.com/2021/03/10/america-small-business-hafnium-exchange-hacks/ adresinden erişim sağlanmıştır.

HAFTA 2. KALI LINUX

AMAÇ

Bu bölümün amacı, öğrencilere Kali Linux işletim sistemini tanıtmaktır. Bu kapsamda, temel bazı Linux komutları ve araçları örneklerle açıklanacaktır. Öğrencilerin birtakım uygulamalar yaparak öğrendiklerini göstermeleri ve pekiştirmeleri hedeflenmiştir.

BÖLÜM KAZANIMLARI

Bu bölümü tamamlayan bir öğrenci,

- Kali Linux'taki Terminal uygulamasını kullanır.
- Linux'taki dizin yapısıyla ilintili temel komutları çeşitli şekillerde çalıştırır.
- Linux'taki dosya erişim izinlerini görüntüler, açıklar ve değiştirir.
- Linux'taki özel sembolleri farklı komutların içinde kullanır.
- Terminalden dosya içeriği görüntüleme ve çıktı yönlendirme işlemlerini yapar.
- Linux'ta dosyaları bir dizinden başka bir dizine kopyalar.

KULLANILACAK MATERYAL VE ARAÇLAR

Bilgisayar, VirtualBox, Kali Linux, kâğıt, kalem

HAFTANIN İŞLENİŞİ

Gözle	Linux'a giriş ve terminal ekranı Temel dizin manipülasyon komutları Dosya erişim izinleri Özel semboller (wildcards) Çıktı yönlendirme
Uygula	Dosya inceleme ve izin değiştirme Özel sembol kullanımı ve çıktı yönlendirme Ek etkinlik: Proses izleme
Tasarla ve Üret	Bu haftanın içeriğinde Tasarla ve Üret bileşeni bulunmamaktadır.
Değerlendir	Haftanın içeriğinin değerlendirilmesi ve çalışmanın devam ettirilmesine yönelik öneriler

1. GÖZLE: TEMEL KAVRAMLAR VE KOMUTLAR

Bu bölümde Kali Linux ile ilgili temel kavramlar ve komutlar tanıtılacaktır. Bölüm için 80 dakika süre yeterli olacaktır.

1.1. GİRİŞ

Linux işletim sisteminin çekirdeği 1991 yılında Finlandiyalı Linus Torvalds tarafından geliştirilmiştir. Yıllar içinde bu çekirdeğin etrafında çeşitli kişilerin katkılarıyla uygulamalar geliştirilmiş ve Linux giderek daha kullanışlı hale gelmiştir. Linux, Microsoft Windows kadar olmasa da yaygın kullanılan bir işletim sistemidir.

Linux'un, geçmişi 1970'lere dayanan Unix'e benzer bir işletim sistemi olduğu söylenebilir ancak Linux bir Unix çeşidi değildir. Linux'un Ubuntu, Fedora, Red Hat gibi kendi dağıtımları bulunmaktadır. Kali Linux siber güvenlik odaklı geliştirilmiş olan ve içinde güvenlikle ilgili birçok yazılımı bulunduran bir dağıtımdır.

Kali Linux ve içindeki araçlar yaygın olarak sızma testi (penetration testing) için kullanılır. Doğrudan bilgisayara yüklenebildiği gibi sanal makine (virtual machine) üzerinde, bulutta veya

mobil cihazlarda kullanılabilir. Kali Linux içinde yer alan çeşitli araçların kullanım amaçlarından bazıları şunlardır:

- Parola kırma
- Ağ tarama
- Ağ paket analizi
- Veritabanına saldırı
- Kablosuz ağa saldırı
- Web uygulama güvenlik taraması

Kali Linux hakkında ayrıntılı bilgiler ve dokümanlar resmi sitesinde bulunabilir: https://www.kali.org/

1.2. TERMİNAL EKRANI

Terminal ekranı, Linux sistemlerinde komutları ve programları çalıştırmak için yoğun kullanılan bir araçtır.

Eğitmen bir terminal ekranı açar ve öğrencilerden de kendi Kali Linux pencerelerinde terminal ekranı açmalarını ister. Terminal ekranı açmanın birkaç farklı yolu aşağıda verilmiştir:

- Ctrl+Alt+T tuşlarına birlikte basmak,
- Masaüstünde varsa Terminal simgesine tıklamak,
- Arama kutusunda "terminal" yazarak çıkan uygulamayı açmak

Burada incelenebilecek ilk komut, `ls` komutudur. `ls`, belli bir dizinin içeriğini (içindeki dosyaları ve diğer dizinleri) görüntülemeye yarar. Aşağıdaki adımlar izlenir.

Linux'ta küçük harf – büyük harf ayrımı vardır. Bu nedenle, `ls` komutu `Ls` veya `LS` şeklinde yazılırsa çalışmaz. Bu ayrım bütün komutlar ve dosya adları için geçerlidir.

1. Eğitmen ve öğrenciler terminal ekranına aşağıdaki komutu yazarak Enter'a basar.

```
ls
```

Bu komutun sonucunda mevcut dizinin içeriği görüntülenmiş olur.

2. Eğitmen ve öğrenciler terminal ekranına aşağıdaki komutu yazarak Enter'a basar.

```
ls -a
```

Komut bu şekilde kullanıldığında mevcut dizinin içindeki gizli dosyalar da görüntülenir. Bu komut sonucunda ilk komuttakinden daha fazla sayıda dosya (ilk komuttakilere ek olarak başka dosyalar) görülecektir.

3. Eğitmen ve öğrenciler terminal ekranına aşağıdaki komutu yazarak Enter'a basar.

```
ls -l
```

Komut bu şekilde kullanıldığında mevcut dizinin içindeki dosyalar uzun formatta, yani adlarının yanı sıra dosyalara ait başka ayrıntılar da görüntülenir. Bu komutun çıktısında yer alan bilgiler şu şekildedir:

- Birinci sütunda dosyanın erişim izinleri,
- İkinci sütunda dosyaya verilen bağlantı sayısı,
- Üçüncü ve dördüncü sütunlarda dosyanın sahibi ve grubu,
- Beşinci sütunda dosyanın boyutu (byte cinsinden),
- Altıncı sütunda dosyanın son değiştirilme zamanı,
- Yedinci sütunda dosyanın adı

4. Eğitmen ve öğrenciler terminal ekranına aşağıdaki komutu yazarak Enter'a basar.

```
ls -al
```

Komut bu şekilde kullanıldığında mevcut dizinin içindeki tüm dosyalar (gizli dosyalar dâhil) uzun formatta görüntülenir.

1.3. LINUX DİZİN YAPISI VE İLGİLİ KOMUTLAR

Birçok işletim sisteminde olduğu gibi Linux'ta da hiyerarşik dosya sistemi yapısı vardır. Dizinler ve dosyalar, en üstte yer alan kök (root) dizininden başlayarak aşağıya doğru bir ağaç yapısı içerisinde organize edilir. Her dizinin altında dosyalar ve başka dizinler yer alabilir.

Aşağıdaki komutların her biri öğrencilere uygulamalı olarak açıklanır.

1. `pwd`: Print working directory (çalışılan dizini yazdır) ifadesinin kısaltması olan `pwd` komutu, içinde bulunulan dizinin sistemdeki tam adresini gösterir.

Eğitmen ve öğrenciler terminal ekranına aşağıdaki komutu yazarak Enter'a basar.

```
pwd
```

Bu komutun sonucunda mevcut dizinin sistemdeki tam adresi görüntülenmiş olur.

2. `cd:` Change directory (dizin değiştir) ifadesinin kısaltması olan `cd` komutu, mevcut dizinden başka bir dizine geçmekte kullanılır. `cd` kelimesinden sonra gelen dizin, gidilecek hedef dizindir. Yan yana iki nokta (`..`) bir üst dizini temsil eder.

Eğitmen ve öğrenciler terminal ekranına aşağıdaki komutu yazarak Enter'a basar.

```
cd ..
```

Bu komutun sonucunda bir üst dizine geçilmiş olur. Bundan sonra, dizinin içindekileri ayrıntılı biçimde görüntülemek için aşağıdaki komut kullanılabilir.

```
ls -l
```

Görüntülenen dizinlerden herhangi birine geçmek için `cd` kelimesinden sonra dizin adı yazılıp Enter'a basılarak geçiş yapılabilir. `cd` komutu birkaç kere farklı şekillerde kullanılarak dizinler arasında gezinti yapılabilir. Home (ev) dizinine dönmek için komut aşağıdaki şekilde tek başına kullanılabilir.

```
cd
```

3. `mkdir:` Make directory (dizin yap) ifadesinin kısaltması olan `mkdir` komutu, yeni bir dizin oluşturmak için kullanılır. `mkdir` kelimesinden sonra gelen kelime, oluşturulacak yeni dizinin adıdır.

Eğitmen ve öğrenciler terminal ekranında Ev dizinine döndükten sonra aşağıdaki komutu yazarak Enter'a basar.

```
mkdir deneme
```

Mevcut dizinin altında deneme adlı yeni bir dizin oluşturulduğu, `ls` komutu kullanılarak görülebilir.

1.4. DOSYA ERİŞİM İZİNLERİ

Linux'ta dosya erişim izinleri, kimin hangi dosya ile ne yapabileceğini belirler. Linux'ta dizinler de aslında birer dosyadır ve dizinler için de erişim izinleri tanımlanır.

Linux'ta bir dosya için tanımlı üç kullanıcı sınıfı bulunmaktadır:

- **Sahip (owner, u):** Dosyayı oluşturan kullanıcı
- **Grup (g):** Sınırlı ve belli bir kullanıcı grubu
- **Diğerleri (others, o):** Diğer herkes

Erişim izinleri, yukarıdaki kullanıcı sınıflarının her birinin dosyaya hangi şekilde erişim sağlayabileceğini, yani dosyayla ne yapabileceğini belirler. Erişim izinleri üç çeşittir:

- **Oku (read, r):** Dosyanın okunabileceği anlamına gelir.
- **Yaz (write, w):** Dosyaya yazılabileceği yani dosya içeriğinin değiştirilebileceği anlamına gelir.
- **Çalıştır (execute, x):** Dosyanın bir program gibi çalıştırılabileceği anlamına gelir.

Terminal ekranında `ls -l` komutu çalıştırıldığında gelen ilk sütunda dosya izinleri gösterilmektedir. Her izin 10 sembol ile ifade edilir. İlk sembol '-' (tire) ise dosya, 'd' ise dizin olduğu anlamına gelir. Sonraki 3 sembol sahibin izinlerini, diğer 3 sembol grubun izinlerini, sondaki 3 sembol de diğer kullanıcıların izinlerini gösterir.

Örnekler: Aşağıda birkaç örnek izin ve anlamları verilmektedir.

`-rwxr-xr-x` → Dosyanın sahibinin oku+yaz+çalıştır, grubunun oku+çalıştır, diğer kullanıcıların oku+çalıştır izinlerine sahip olduğunu gösterir.

`-rw-------` → Dosyanın sahibinin oku+yaz izinlerine sahip olduğunu, grubunun veya diğer kullanıcıların hiçbir izne sahip olmadığını gösterir.

`dr-xr--r--` → Dizinin sahibinin oku+çalıştır izinlerine, grubunun ve diğer kullanıcıların oku iznine sahip olduğunu gösterir.

Not: Bir dizin için;

okuma (r) izni, dizin içindeki dosyaların isimleri ve diğer bilgilerinin `ls` komutuyla görüntülenebilmesini,

yazma (w) izni, dizin içine dosya kopyalama, dizindeki dosyaları silme veya yeniden adlandırma gibi değişikliklerin yapılabilmesini,

çalıştır (x) izni, `cd` komutuyla dizin içine girilebilmesini sağlar.

Dosya izinlerini değiştirmek amacıyla `chmod` (change mode) komutu kullanılır. Komutun kullanımı şu şekildedir:

```
chmod [u|g|o|a] [+|-|=] [r|w|x] dosya(lar)
```

Görüldüğü gibi, `chmod` kelimesinden sonraki ilk kısım kimin izinlerinin değiştirileceğini (u: sahip, g: grup, o: diğerleri, a: hepsi), ikinci kısım işlem türünü (izin ekleme, izin çıkarma, izin

eşitleme), üçüncü kısım izin türünü, dördüncü kısım da işlem yapılacak dosya ad(lar)ını belirler.

Örnekler: Aşağıda bazı örnek izin değiştirme işlemleri verilmektedir. Bu örnekleri eğitmen ve öğrenciler birlikte uygulayarak incelemelidir.

1. Aşağıdaki komutları terminalde çalıştırınız.

```
touch dosya1

ls -l
```

`touch` komutu ile `-rw-r--r--` izinlerine sahip `dosya1` adlı boş bir dosya oluşturulmuş olduğu görülecektir.

2. Aşağıdaki komutları çalıştırınız.

```
chmod u+x dosya1

ls -l
```

dosya1 için dosya sahibine çalıştırma izni eklenmiştir.

3. Aşağıdaki komutları çalıştırınız.

```
chmod a-w deneme

ls -l
```

deneme dizini için herkesin yazma (değiştirme) izni kaldırılmıştır.

4. Aşağıdaki komutları çalıştırınız.

```
chmod ug=rw dosya1

ls -l
```

dosya1 için sahibinin ve grubunun izinleri okuma+yazma olarak belirlenmiştir.

1.5. ÖZEL SEMBOLLER (WILDCARDS)

Eğitmen öğrencilere şu soruyu sorar: Bir dizin içinde adı a harfi ile başlayan bütün dosyaları silmek istediğimizi düşünelim. Bunu nasıl yapabiliriz?

Bunun bir yolu, `ls` komutunu kullanarak dosyaları listeledikten sonra a ile başlayanları görüp tek tek silmektir. Ancak a ile başlayan dosya sayısı çoksa, bu zahmetli bir iş olabilir.

Linux'ta bu tür işlemleri kolaylaştıran bazı özel semboller bulunur. Bunlardan ikisini inceleyelim.

? sembolü: Soru işareti sembolü, herhangi bir tek karakter yerine geçer. Örneğin, a?c şeklindeki kelimenin karşılığı abc, azc, a1c, aBc vb. kelimelerdir, yani a?c bunların hepsinin yerine geçebilir.

*** sembolü:** Yıldız sembolü, sıfır veya daha fazla sayıda (üst sınır yok) karakter yerine geçer. Örneğin, d* kelimesinin karşılığı dosya1, dizin1, deneme, deneyap, dondurma vb. olabilir. Benzer şekilde, *.c şeklinde yazılan ifade, adı .c ile biten bütün dosyaları temsilen kullanılabilir.

Bu açıklamaların ardından aşağıdaki adımlar izlenir.

1. Eğitmen ve öğrenciler dizin1 adlı yeni bir dizin ve altında bazı dosyalar oluşturmak amacıyla terminal ekranında aşağıdaki komutları çalıştırırlar.

```
cd

mkdir dizin1

cd dizin1

touch a1 abc aaa a9 a11

ls -l
```

İçinde bulunduğumuz `dizin1` altında `a1, abc, aaa, a9, a11` adlı 5 tane boş dosya olduğunu göreceğiz.

2. Aşağıdaki komutlarla devam edelim.

```
rm a?

ls
```

Öğrencilere hangi dosyaları gördükleri, hangilerinin ise silinmiş olduğu sorulur.

`a1` ve `a9` adlı dosyaların silinmiş olduğu, diğer üç dosyanın ise yerinde durduğu görülecektir. Öğrencilerle bunun neden böyle olduğu tartışılır.

Yanıt: Yukarıdaki `rm` komutu, dosya silme komutudur. a? şeklindeki kelime, a ile başlayan iki harfli kelimelerin yerine geçtiği için, buna uyan `a1` ve `a9` adlı dosyalar silinmiştir.

3. Eğitmen ve öğrenciler aşağıdaki komutları çalıştırırlar.

```
rm *1

ls
```

Öğrencilere hangi dosyaları gördükleri, hangilerinin ise silinmiş olduğu sorulur.

`a11` adlı dosyanın silinmiş olduğu, diğer iki dosyanın ise yerinde durduğu görülecektir. Öğrencilerle bunun neden böyle olduğu tartışılır.

Yanıt: *1 şeklindeki kelime, 1 ile biten kelimelerin yerine geçtiği için, buna uyan `a11` adlı dosya silinmiştir.

4. Eğitmen ve öğrenciler aşağıdaki komutları çalıştırırlar.

```
rm a*

ls
```

Öğrencilere hangi dosyaları gördükleri, hangilerinin ise silinmiş olduğu sorulur.

`aaa` ve `abc` adlı dosyaların silinmiş olduğu, dizinde dosya kalmadığı görülecektir. Öğrencilerle bunun neden böyle olduğu tartışılır.

Yanıt: a* şeklindeki kelime, a ile başlayan kelimelerin yerine geçtiği için, buna uyan `aaa` ve `abc` adlı dosyalar silinmiştir.

1.6. ÇIKTI YÖNLENDİRME

Linux'ta programlar terminalden çalıştırıldıklarında çıktıları genellikle terminale yazılır. Ancak bazı durumlarda çıktıları bir dosyaya kaydetmek isteyebiliriz. Bunu yapmak için `>` sembolünü kullanabiliriz.

Eğitmen ve öğrenciler aşağıdaki komutu çalıştırırlar.

```
ls -l > dosya2
```

Bunun sonucunda, `ls -l` komutunun çıktısı, dosya2 adlı dosyanın içine kaydedilmiş olur. Linux'ta `cat` komutu, bir dosyayı açmadan içeriğini görüntülemek için kullanılır. Bu komutu aşağıdaki şekilde çalıştıralım.

```
cat dosya2
```

Ekranda görüldüğü gibi, az önceki `ls -l` komutunun çıktısı dosya2 içinde yer almaktadır.

Şimdi aşağıdaki komutları çalıştıralım.

```
cat dosya2 > dosya3

cat dosya3
```

Yukarıdaki iki `cat` komutundan ilkinin sonucunda ekrana bir şey yazılmamıştır. İkinciden sonra ise çıktı ekranda görülmüştür. Bunun neden böyle olduğu öğrencilerle tartışılır.

Yanıt: İlk `cat` komutu, çıktı yönlendirme ile birlikte kullanılmış ve çıktı dosya3 içine yazılmıştır. İkinci `cat` komutu ise dosya3'ün içeriğini ekrana yazdırmıştır.

2. UYGULA

2.1. DOSYA İNCELEME VE İZİN DEĞİŞTİRME

Bu bölümde öğrencilerin bölüm sonunda verilen Ek 2.1 içindeki problemleri 40 dk içinde çözmeleri istenir. Etkinliğin başlangıcında eğitmen Ek 2.1 dosyasını öğrencilerle paylaşır ve öğrencilerin her problem için verilen açıklamaları takip ederek dosyayı doldurmaları gerektiğini belirtir.

Eğitmen, öğrencilerin etkinlik boyunca ilerlemelerini sorularla takip ederek çoğu öğrencinin takıldığı bir adım varsa yardım edebilir. Daha sonra öğrenciler çözümlerini gösteren dosyayı eğitmene gönderir. Eğitmen, 10 dk süre içinde örnek çözümleri paylaşırken öğrencilerin kendi çözümlerinin doğru olup olmadığını görebilirler. Dersten sonra eğitmen öğrencilerin çözüm dosyalarını inceleyerek kaçıncı adıma kadar ilerleyebildiklerini değerlendirir.

Etkinliğin Yanıtları:

1. `mkdir ~/Uygulamalar`
2.
```
cd Uygulamalar
mkdir Hafta2
cd Hafta2
```
3.
```
pwd
/home/kali/Uygulamalar/Hafta2 (sisteme göre değişebilir)
```
4. `cd /usr/libexec`

5. ls -l veya ls -lS (boyuta göre sıralı gösterir)
   xdg-desktop-portal (sisteme göre değişebilir)
6. cp xdg-desktop-portal /home/kali/Uygulamalar/Hafta2 (sisteme göre değişebilir)
7. cd /home/kali/Uygulamalar/Hafta2
8. ls -l
   -rwxr-xr-x (sisteme göre değişebilir)
9. chmod o-x xdg-desktop-portal (dosya adı sisteme göre değişebilir)
10. ls –l
    -rwxr-xr-- (sisteme göre değişebilir)

2.2. ÖZEL SEMBOL KULLANIMI VE ÇIKTI YÖNLENDİRME

Bu bölümde öğrencilerin bölüm sonunda verilen Ek 2.2 içindeki problemleri 40 dk içinde çözmeleri istenir. Etkinliğin başlangıcında eğitmen Ek 2.2 dosyasını öğrencilerle paylaşır ve öğrencilerin her problem için verilen açıklamaları takip ederek dosyayı doldurmaları gerektiğini belirtir.

Eğitmen, öğrencilerin etkinlik boyunca ilerlemelerini sorularla takip ederek çoğu öğrencinin takıldığı bir adım varsa yardım edebilir. Daha sonra öğrenciler çözümlerini gösteren dosyayı eğitmene gönderir. Eğitmen, 10 dk süre içinde örnek çözümleri paylaşırken öğrencilerin kendi çözümlerinin doğru olup olmadığını görebilirler. Dersten sonra eğitmen öğrencilerin çözüm dosyalarını inceleyerek kaçıncı adıma kadar ilerleyebildiklerini değerlendirir.

Etkinliğin Yanıtları:

1. touch dosya1 dosya2 dosya3 dosya11 dosya21 dosya22
2. ls –l *1
3. chmod a=r *1 (farklı çözümler olabilir)
4. ls -al > dosya2
5. cat dosya2 > dosya1
   zsh: permission denied: dosya1 (mesaj sisteme göre değişebilir)
6. dosya1 salt okunur olduğundan içine yazma işlemi hata verdi. dosya1'e yazma izni eklemeliyiz.
   chmod u+w dosya1
   cat dosya2 > dosya1

3. TASARLA VE ÜRET

Bu haftanın içeriğinde Tasarla ve Üret bileşeni bulunmamaktadır.

4. DEĞERLENDİR

Bu bölüm için 20 dk süre yeterli olacaktır.

Eğitmen öğrencilerine aşağıdaki soruları sorarak yanıtları üzerinden tartışmayı yönlendirir.

- Bugün öğrendiğiniz komutların içinde en zoru hangisiydi? Neden?
- Sizce daha alışık olduğunuz pencereli arayüz yerine terminal ekranı arayüzünü kullanmanın avantajları ve zorlukları nelerdir?
- Linux yükleme sonrasında yaptığınız hazırlık ve inceleme sonucunda, Windows'ta kullandığınız ancak Linux'ta bulamadığınız özellikler ve programlar neler olmuştur? Bunların Linux'taki alternatifleri hakkında ders sonrasında araştırma yapınız.

5. EK ETKİNLİK: PROSES İZLEME

Bu bölümde öğrencilerin Ek 5 içindeki problemleri yine Ek 5 içinde verilen açıklamalar doğrultusunda çözerek ilerlemeleri istenir. Etkinliğin başlangıcında eğitmen Ek 5 dosyasını öğrencilerle paylaşır ve öğrencilerin her problem için verilen açıklamaları takip ederek dosyayı doldurmaları gerektiğini belirtir.

Daha sonra öğrenciler çözümlerini gösteren dosyayı eğitmene gönderir. Eğitmen, 10 dk süre içinde örnek çözümleri paylaşırken öğrencilerin kendi çözümlerinin doğru olup olmadığını görebilirler. Dersten sonra eğitmen öğrencilerin çözüm dosyalarını inceleyerek kaçıncı adıma kadar ilerleyebildiklerini değerlendirir.

Etkinliğin Yanıtları: Eğitmen etkinlik bitiminde aşağıdaki yanıtları öğrencilerle paylaşıp tartışma yürütür.

1. Her prosesi diğerlerinden ayıran tanımlayıcı numara **PID**'dir.

2. Prosesin adı, bir başka deyişle prosesi başlatmak için kullanılmış olan komut, **COMMAND** veya **CMD** sütununda gösterilmektedir.

3. **USER** başlıklı sütun altında kaç farklı kullanıcı hesabı gözüktüğü sayılacaktır. Kullanıcı adı sayısı sistemin durumuna göre farklılık gösterebileceği için kesin bir doğru yanıt yoktur. Burada her kullanıcı adının neye karşılık geldiği tartışılabilir. Görülen kullanıcı adları arasında, sistemdeki bütün dosyalara ve komutlara erişimi olan hesabı ifade eden **root** ve kurulum sırasında seçilen kullanıcı adı ile birlikte başka hesaplar da bulunabilir.

4. İşlemci (CPU) kullanımı en yoğun olan proses, **CPU** sütununda gösterilen yüzdeler arasında en yüksek değere bakılarak bulunur. Bu prosesin hangisi olduğu sistemin durumuna göre farklılık gösterebilir. Eğitmen kendi sistemi için elde ettiği yanıtı öğrencilerin yanıtlarıyla karşılaştırabilir ancak kesin bir doğru yanıt yoktur.

5. Verilen komut, “ps –aux” komutunun çıktısında “root” kelimesini içeren satırları gösterecektir.

6. grep, kendisine girdi olarak verilen metnin içinde, yine komutun girdisinde belirtilen örüntüye uyan satırları bulur ve gösterir. Komutun kullanımı hakkında ayrıntılı bilgi terminal ekranına “man grep” yazılarak veya internetten (örneğin https://linuxcommand.org/lc3_man_pages/grep1.html adresinden) elde edilebilir.

Ek 2.1. Dosya İnceleme ve İzin Değiştirme Uygulaması Adımları

1. Ev (home) dizininizin altında **Uygulamalar** adlı yeni bir dizin oluşturunuz.

Komut:

2. Uygulamalar dizinine giriniz. Bu dizinin altında **Hafta2** adlı yeni bir dizin oluşturunuz ve **Hafta2** dizinine giriniz.

Komut 1: Komut 2: Komut 3:

3. İçinde bulunulan dizinin sistemdeki tam adresini gösteren komutu çalıştırınız. Komutu ve çıktısını (sonucunu) aşağıdaki kutuya yazınız.

Komut: Çıktısı:

4. Tek adımda **/usr/libexec** dizinine gidiniz. (İpucu: Gerekli komutun yanına adres yazılarak gidilebilir.)

Komut:

5. Bu dizin içindeki dosyaları boyutlarıyla birlikte görüntüleyiniz. En büyük boyutlu dosyayı bulunuz.

Komut: Dosya adı:

6. Bulduğunuz dosyayı **Hafta2** adlı dizinin altına kopyalayacaksınız. Kopyalama işlemi için `cp` komutunu kullanacaksınız. `cp` kelimesinin yanına bir boşluk koyduktan sonra 5. adımda bulduğunuz dosyanın adını, sonra bir boşluk daha koyarak 3. adımda not aldığınız adresi yazarak Enter'a basınız.

Komut:

7. Kopyalama işleminden sonra tek adımda **Hafta2** dizinine dönünüz. (İpucu: 3. adımda not aldığınız adresi kullanabilirsiniz.)

Komut:

8. Hafta 2 dizini içindeki dosyaların ayrıntılarını (izin, boyut, tarih vb.) gösteren komutu çalıştırınız. Önce komutu, sonra da gördüğünüz tek dosyanın erişim izinlerini aşağıdaki kutuya yazınız.

Komut: Erişim izinleri:

9. Bu dosyanın "Diğerleri" için "Çalıştır" iznini kaldırınız.

Komut:

10. Dosyanın ayrıntılarını tekrar görüntüleyiniz. Kullandığınız komutu ve gördüğünüz erişim izinlerini aşağıdaki kutuya yazınız ve 8. Adımdaki izinlerle karşılaştırınız.

Komut: Erişim izinleri:

Ek 2.2. Özel Sembol Kullanımı ve Çıktı Yönlendirme Uygulaması Adımları

1. Önceki uygulamada oluşturduğunuz Hafta2 dizini altında dosya1, dosya2, dosya3, dosya11, dosya21, dosya22 adlı 6 tane boş dosya oluşturunuz (touch ile).

Komut:

2. Özel sembol kullanarak, adı 1 ile biten dosyaların ayrıntılarını görüntüleyiniz.

Komut:

3. Özel sembol kullanarak, adı 1 ile biten dosyaları salt okunur (read-only) yapınız. (İpucu: Erişim izni değiştiren komutu kullanarak dosyalarda sadece oku izni bulunmasını sağlayabilirsiniz.)

Komut:

4. `ls -al` komutunu uygun biçimde çalıştırarak çıktısını dosya2 içine yazınız. (İpucu: Çıktı yönlendirme)

Komut:

5. Bölüm 1.6'da tanıtılan cat komutunu ve çıktı yönlendirmeyi kullanarak, dosya2'nin içindekileri dosya1'e yazınız. (İpucu: Hata almanız beklenmektedir. Hata mesajını da kutuya yazınız.)

Komut: Hata mesajı:

6. Bir önceki adım sonucunda ne oldu? Neden? Bunu çözmek için ne yapmalıyız? Bu soruları yanıtlayarak çözüm bulunuz ve dosya2'nin içindekileri dosya1'e yazma işlemini tamamlayınız. (İpucu: Sorun ve çözümü yukarıdaki maddelerin birinde gizli.)

Yanıt: Sorunu çözen komutlar:

Ek 5. Proses İzleme Uygulaması Adımları

Bilgisayarda aynı anda birçok program çalışır. Bunların bazılarını aktif olarak kullanıyor olsak da, çoğunluğu arka planda bizden habersiz çalışan programlardır. Bilgisayarda çalışmakta olan programlara **proses** veya **süreç** adı verilir. Linux'ta prosesleri izlemek için `ps` komutu kullanılmaktadır.

Bu bölümde `ps` komutunu aşağıdaki sorular ve verilen ipuçları yardımıyla keşfederek ilerlemeniz beklenmektedir.

1. Komutu yalnızca `ps` şeklinde çalıştırarak çıktısını inceleyiniz. Bu çıktıda her prosesi diğerlerinden ayıran tanımlayıcı numara hangisidir?

Yanıt:

2. Prosesin adı, bir başka deyişle prosesi başlatmak için kullanılmış olan komut, hangi sütunda gösterilmektedir?

Yanıt:

3. Komutu `ps -aux` şeklinde çalıştırarak çıktısını inceleyiniz. Bu çıktıda USER başlıklı sütun altında kaç farklı kullanıcı hesabı gözüktüğünü inceleyerek adlarını aşağıdaki kutuya yazınız.

Yanıt:

4. İşlemci (CPU) kullanımı en yoğun olan proses hangisidir?

Yanıt:

5. Komutu aşağıdaki şekilde çalıştırınız.

```
ps –aux | grep root
```

Sizce bu komut ne yapmaktadır? (İpucu: root yerine 3. Adımda not aldığınız kullanıcı adlarını koyarak komutu tekrarlamayı deneyiniz.)

Yanıt:

6. `grep` komutu hakkında dersin geri kalanında ve ders sonrasında araştırma yapınız.

HAFTA 3. PAROLALAR

ÖN BİLGİ

- Bilgi güvenliğinin temel kavramları
- Kali Linux kullanımı, temel komutlar ve araçlar

AMAÇ

Bu bölümün amaçları arasında, öğrencileri parola kavramıyla tanıştırmak, parola gücünü değerlendirmeyi öğrenmelerini, doğru parola seçimi hakkında bilgi sahibi olmalarını sağlamak bulunmaktadır. Öğrenciler ayrıca basit parola kırma saldırıları gerçekleştirmeyi ve rastgele parola üretme programı geliştirmeyi uygulamalı olarak öğreneceklerdir.

BÖLÜM KAZANIMLARI

Bu bölümü tamamlayan bir öğrenci,

- Parola kavramını tanımlar,
- Parolaların gücünü analiz eder,
- Parola kırma saldırısı örneklerini açıklar,
- Parola seçimi kurallarını ve yöntemlerini açıklar,
- Parola kırma saldırısı uygular,
- Rastgele parola üretecek program tasarlar ve kodlar.

KULLANILACAK MATERYAL VE ARAÇLAR

Bilgisayar, Kali Linux, John the Ripper, Hydra, kod yazma için IDE, kâğıt, kalem

HAFTANIN İŞLENİŞİ

Gözle	Parola kavramı, parola kırma saldırıları, parola seçimi
Uygula	Parola sayısı hesaplama, parola kırma saldırısı uygulaması
Tasarla	Rastgele parola üretecek program tasarımı
Üret	Rastgele parola üretecek program yazma
Değerlendir	Haftanın içeriğinin değerlendirilmesi ve çalışmanın devam ettirilmesine yönelik öneriler

1. GÖZLE

Bu bölümde parola kavramı tanıtılarak parola gücü, parola kırma saldırıları ve parola seçim yöntemleri hakkında bilgi verilir. Bölüm 1 için toplam 60 dk süre yeterli olacaktır.

EĞİTMENE NOT

Parola (password) kelimesi yerine şifre kelimesinin kullanıldığını sıkça duyabiliriz (örn. e-posta şifresi, e-devlet şifresi, tek kullanımlık şifre vb.). Günlük hayatta bu kullanım ciddi bir sorun oluşturmasa da, parola demek daha doğrudur çünkü siber güvenlikte şifre (cipher) terimi şifreleme algoritmalarını ifade eder ve parola kavramının şifreleme ile doğrudan bir ilgisi yoktur.

1.1. GİRİŞ

Eğitmen öğrencilerinin parola konusunu tartışmalarını sağlar. Bunun için öğrencilerine çeşitli sorular sorarak onların cevabını alır ve ardından parola kavramı ile ilgili olarak detaylı açıklamalarını yapar. Bu bölüm için 15 dakikalık bir zaman ayırmak yeterlidir.

- Parolanız var mı?
- Parola ile nerelere giriş yapıyorsunuz?
- Parolalarınızı nasıl belirliyorsunuz?
- Belli zamanlarda parolanızı değiştiriyor musunuz?
- Parolaları kaç karakterden oluşturuyorsunuz?

- Parolalara doğum yeri ya da doğum tarihini vermek sizce doğru mudur?
- Parola oluştururken belli bir mantık, yapı ya da yol takip ediyor musunuz?

Eğitmen bu sorulara ek olarak başka sorular da sorabilir. Gelen cevaplarla birlikte öğrencilerden de yeni sorular ortaya çıkabilir. Bunlara benzer sorular çerçevesinde tartışma yönetilerek öğrencilerin fikirlerini beyan etmesi sağlanır.

Gerçek yaşam içinde parola kullanan öğrencilerden bazılarının şifreleri çok basit ya da kolay olabilir. Parolaların kolay ya da zor olmaları da tartışmanın konusu olabilir. Hangi parolaların kolay ya da zor ve neden kolay/zor olduklarına yönelik olarak öğrencilerin fikirleri alınabilir.

1.2. PAROLA KAVRAMI

Parola, bir kişinin erişim yetkisini doğrulamak için kullanılır. Örneğin, bir askeri alana veya kışlaya girmek isteyen birine kapıdaki nöbetçi asker parola sorabilir. Geleneksel parolalar bir kelime veya cümle olabilirken, günümüzde yaygın olarak bilgisayar sistemlerine giriş için kullanılan parolalar genellikle farklı bir yapıya sahiptir.

Tarihte parola kullanımı, genellikle gizli veya kısıtlı bir bölgeye erişim için sadece belli kişilerce bilinen bir kelime veya cümle (örn. “açıl susam açıl”) söyleme şeklindeyken, günümüz sistemlerinde her kullanıcının kendine özel kullanıcı adı ve parolası bulunmaktadır.

Bilgisayar sistemlerinde kullanılan parola bir dizi sembolden oluşur. Bu semboller küçük harf, büyük harf, rakam, noktalama işareti ve diğer özel semboller (tire, alt çizgi, yıldız vb.) olabilir. Bir paroladaki sembollerin sayısı ve çeşitliliği parolanın gücü açısından önemlidir. Bir saldırgan tarafından tahmin edilmesi zor olan parolalar daha güçlü kabul edilir.

1.3. PAROLALARIN SAKLANMASI

Parolalar erişim sağlanacak sistem üzerindeki özel bir dosya içerisinde, hash işleminden geçirilmiş halde saklanırlar. Parolaların orijinal hallerinin sistemde tutulmamasındaki amaç, sisteme sızmış olan bir saldırganın parolaları ele geçirmesini engellemektir. Hash fonksiyonları tek yönlü (geri döndürülemez) fonksiyonlar oldukları için, saklanan hash değerlerinden parolaya ulaşmak mümkün değildir.

1.4. PAROLA KIRMA SALDIRILARI

Bir parolanın kırılma zorluğunu belirleyen birçok etken vardır. Bunlardan bazıları aşağıda tartışılmaktadır.

Uzunluk: Kısa parolalar uzun parolalara göre genellikle daha kolay kırılır.

İçerdiği semboller: Sadece harf veya sadece rakam içeren, özel sembol içermeyen parolalar daha kolay kırılır.

Anlamlı olup olmaması: Belli bir anlama sahip olan parolalar (örn. kelime, cümle, tarih) daha kolay kırılır.

EĞİTMENE NOT

Uzun bir parola kısa bir parolaya göre daha zayıf olabilir. Örneğin, harf, rakam ve özel sembol içeren 6 karakterli bir parola, 123456789 gibi 9 karakterli bir parolaya göre çok daha güçlüdür. Öğrencilere bu konuda uyarı yapılmalıdır.

Parola Saldırısı Türleri

Aşağıda yaygın parola saldırılarından bazıları verilmiştir (Subangan & Senthooran, 2019).

- **Kaba kuvvet tahmin:** Belli bir sırayla bütün olası parolaların denenmesine dayalı saldırı türüdür. Bu saldırıda yapılacak tahmin sayısı, olası parola sayısıyla orantılıdır. En basit ama en yavaş parola saldırısı türüdür.
- **Sözlük saldırısı:** Önceden oluşturulmuş bir sözlükteki kelimeleri ve bunların kombinasyonlarını parola olarak denemeye dayalı saldırı türü. Birçok insanın parolalarının anlamlı kelimelere dayandığı gözleminden faydalanılır.
- **Popüler parola deneme:** İnsanların yaygın olarak kullandığı bilinen parolaları denemeye dayalı saldırı türüdür. Sözlük saldırısıyla veya kaba kuvvet tahminle birleştirilebilir, yani popüler parolalar başta denenerek başarısız olunması durumunda diğer saldırıya geçilebilir.
- **Kişiye özel saldırı:** Bir kişiyle ilgili bilgiler (doğum tarihi, memleketi, çocuklarının adları vb.) dikkate alınarak yapılan parola tahminlerine dayalı saldırı türüdür.

- **Sosyal mühendislik:** Kişileri kandırarak parolalarını söylemelerini veya saldırganın göreceği bir yere yazmalarını sağlamaya çalışan saldırı türüdür. Sosyal mühendislik, 5. haftada daha ayrıntılı olarak ele alınacaktır.

1.5. PAROLA SEÇİMİ

Güçlü parola seçmek için bazı hususlara dikkat etmek gerekmektedir.

- Parola olarak anlamlı bir kelime, isim, cümle, tarih vb. seçilmemelidir.
- Bir kelimenin veya ismin başına/sonuna bir veya birkaç rakam eklenerek parola oluşturulmamalıdır.
- Parola yeterince uzun olmalıdır. Birçok sistemde parola uzunluğu için bir alt sınır vardır (en az 8, en az 10 gibi). Genellikle parola uzadıkça kırılması zorlaşır.
- Parolada sembol çeşitliliği olmalıdır. Bir başka deyişle küçük harfler, büyük harfler, rakamlar, noktalama işaretleri ve diğer özel semboller birlikte bulunmalıdır.
- Parola tercihen kolay hatırlanır olmalıdır. Eğer parola akılda kalmıyorsa kişi parolayı bir yere yazmak isteyebilir, bu da güvenli değildir çünkü parolanın çalınma ihtimalini doğurur. Parola herhangi bir yere yazılmamalıdır.

Hem güçlü hem de kolay hatırlanır bir parola oluşturmak karmaşık ve özen gerektiren bir iştir. Güvenli parola oluşturmakta kullanılabilecek bir yöntem, sizin aklınızda kalacak ama kolay kolay tahmin edilemeyecek uzunca bir cümle seçip o cümleyi oluşturan kelimelerden bazı harfleri (örneğin her kelimenin ilk iki harfi veya ilk ve son harfleri) birleştirerek parola oluşturmaktır. Bunu yaparken bazı harfleri büyük harf yapmak, bazılarını da bir şekilde rakama veya özel karaktere çevirmek parolayı güçlendirir.

Örnek: Kafamızdan bir cümle uyduralım, sonra her kelimenin ilk ve son harflerini alalım.

Bayılırım biber dolmasına Perşembeleri kahvaltıda → BmbrdaPika

Bu cümlenin garipliği akılda kalıcılığını artıracaktır. Şimdi bazı harfleri kendilerine benzeyen rakam ve özel karakterlerle değiştirelim.

BmbrdaPika → 8m6rdaP!ka

Yukarıdaki parola hem akılda kalıcıdır (parolayı hemen hatırlayamasak da kolayca türetebiliriz) hem de tamamen rastgele üretilen 10 karakterli bir parolaya yakın düzeyde güvenlik sağlar, yani kırılması oldukça zordur.

Eğitmen başka örneklerle parola türetebilir. Bu noktada öğrencilerden kendi seçecekleri bir yöntemle parola üretmeleri ve parolanın neden güçlü olduğunu açıklamaları istenebilir.

Ne kadar güçlü olduğunu düşünürseniz düşünün, parolaları sık sık değiştirmek önemlidir.

2. UYGULA

2.1. PAROLA SAYISI HESAPLAMA

Aşağıdaki sorulardan bir veya iki tanesi eğitmen tarafından çözülerek öğrencilere gösterildikten sonra diğer soruların her biri için 3'er dakikalık süre verilerek öğrencilerin çözmesi istenir. Toplam 20 dakikalık süre yeterli olacaktır.

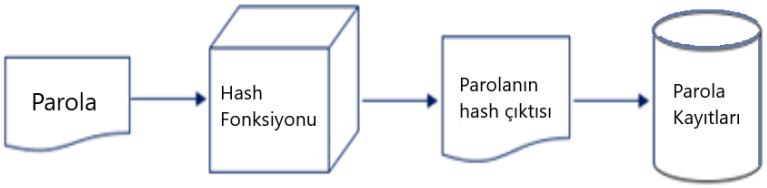
a. 4 karakterden oluşan ve sadece rakamlar içeren kaç tane farklı parola olabilir?
b. 6 karakterden oluşan ve sadece İngiliz alfabesinden küçük harfler içeren kaç tane farklı parola olabilir?
c. 8 karakterden oluşan ve İngiliz alfabesinden küçük veya büyük harfler içeren kaç tane farklı parola olabilir?
d. 10 karakterden oluşan ve sadece rakamlar içeren kaç tane farklı parola olabilir?
e. 10 karakterden oluşan ve rakamlar veya İngiliz alfabesinden küçük harfler içeren kaç tane farklı parola olabilir?
f. 12 karakterden oluşan ve sadece İngiliz alfabesinden küçük harfler içeren kaç tane farklı parola olabilir?

2.2. PAROLA KIRMA SALDIRISI UYGULAMASI

Bu etkinlik için 50 dakikalık zaman dilimi yeterli olacaktır.

Bu etkinlik için John the Ripper adlı uygulama kullanılacaktır. Öğrenciler bu uygulama yardımıyla parola tahmin saldırıları yaparak çeşitli parolaları ne kadar sürede kırabildiklerini göreceklerdir. Öncelikle bu uygulamanın eğitmen tarafından kısaca tanıtılması gerekecektir. Bu tanıtımda Kali'nin resmi sitesinde yer alan bilgilerden faydalanılabilir: https://tools.kali.org/password-attacks/john

Ön bilgi: Kullanıcı parolaları güvenlik nedeniyle sistemde düz metin olarak tutulmaz. Bunun yerine parola Şekil 1'dekine benzer bir şekilde hash işleminden geçirildikten sonra saklanır.



Şekil 1. Parolaların sistemde saklanması

Not: Gerçek sistemlerde parola hash fonksiyonuna girmeden önce tuz (salt) denen bir değer ile birleştirilerek hash eşleştirme tabanlı bazı parola saldırılarına karşı direnç sağlanır.

Bu uygulamada faydalanılacak aracın kullanım örneği aşağıda verilmiştir. Komutu çalıştırmadan önce öğrencilerin kelime listesi (password.lst) ve parola hash listesi (unshadowed.txt) dosyalarını incelemeleri istenerek bu dosyaların içerikleri hakkında tartışma yürütülür.

Bir kelime listesi yani wordlist kullanarak (–wordlist=/usr/share/john/password.lst) ve tanımlı karakter değiştirme kurallarını uygulayarak (–rules), verilen bir dosya (unshadowed.txt) içindeki parola hash değerlerini kırarak parolaları açığa çıkartmak için komut:

```
root@kali:~# john --wordlist=/usr/share/john/password.lst --rules unshadowed.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 1 password hash (sha512crypt [64/64])
toor             (root)
guesses: 1  time: 0:00:00:07 DONE (Mon May 19 08:13:05 2014)  c/s: 482  trying:
1701d - andrew
Use the "--show" option to display all of the cracked passwords reliably
```

Bu etkinlikte her öğrenci kendi kelime listesini, bir başka deyişle denenecek parola listesini, oluşturacak ve unshadowed.txt içindeki parola hash değerlerini kırmaya çalışacaktır. Yukarıda gösterilen john komutuna girdi olarak verilen unshadowed.txt dosyasını oluşturmak için aşağıdaki komut kullanılabilir:

sudo unshadow /etc/passwd /etc/shadow > unshadowed.txt

john komutunu çalıştırırken "No password hashed loaded" gibi bir hata alınıyorsa, komut aşağıdaki şekilde çalıştırılabilir:

john --format=crypt --wordlist=/usr/share/john/password.lst --rules unshadowed.txt

Kelime listesi oluştururken kullanılabilecek yöntemle ilgili eğitmen öğrencilere bazı tavsiyeler verebilir:

- Kullanıcılar tarafından yaygın kullanılan parolaların neler olduğu düşünülüp bunlar listeye eklenebilir.
- Bu parolaların başına veya sonuna rakam veya başka sembol ekleme, kelimeleri birleştirme gibi yöntemlerle başka parolalar üretilip liste genişletilebilir.
- Denenen bir liste başarıya ulaşamazsa liste daha da genişletilebilir.

Etkinlik süresinin sonuna kadar öğrenciler denemeler yapabilir. Etkinliğin sonunda, parola kırmada en kolay başarıya ulaştıran yöntemin ne olduğu üzerine tartışma yürütülebilir.

3. TASARLA VE ÜRET

Bu bölümde her öğrenci bağımsız olarak bir rastgele parola üretme programı tasarlayıp kodlayacaktır. Bu etkinlik için 60 dakikalık zaman dilimi yeterli olacaktır.

Tasarla ve üret bölümleri içerisinde öğrenci daha aktif olup eğitmen rehber konumundadır. Eğitmen öğrencilerin sordukları sorulara geri bildirim vererek onları yönlendirir. Gerektiğinde İnternet üzerinden çeşitli örnekleri görmeleri için yönlendirme yapabilir. Bu kısımlarda eğitmen kendisini biraz daha arka planda bırakmalıdır. Eğitmen, öğrencinin aktif katılımı ve problemi grup içerisinde birlikte çözmelerine ve algoritmik düşünme biçimlerine izin veren bir yapıda rehberlik etmek durumundadır.

3.1. RASTGELE PAROLA ÜRETME PROGRAMI

Girdi: Parola uzunluğu

Çıktı: Rastgele üretilmiş parola

Program, verilen bir uzunlukta rastgele parola üretecektir. Rastgele parola içinde en azından büyük-küçük harfler ve rakamlar bulunabilmelidir. Ek olarak her öğrenci kendi seçeceği bazı özel sembolleri de dâhil edebilir. Program her çalıştığında farklı bir rastgele parola üretmelidir. Programı tasarlamak, yazmak ve test etmek için 60 dakikalık süre ayrılabilir. Öğrencilerin önemli bir bölümü zorlanırsa süre 80 dakikaya çıkartılabilir.

Bu programı başarıyla tamamlayan öğrenciler, kodlarını güncelleyerek aşağıdaki özellikleri ekleyebilirler:

- Parola içinde en az 1 büyük harf olduğunu garanti etme,
- Parola içinde en az 1 özel sembol olduğunu garanti etme,
- Parola içinde en az 1 rakam olduğunu garanti etme,
- Girdi olarak verilen uzunluğu minimum olarak kabul edip daha uzun parola üretebilme

Etkinliğin sonunda süre uygunsa programı tamamlayan her öğrenci programının çalışmasını eğitmene yapacağı bir demo ile gösterebilir. Ayrıca, öğrencilerin kaynak kodlarını eğitmene göndermesi ve eğitmenin ders sonrasında çözümlerin uygunluğunu değerlendirmesi faydalı olacaktır.

4. DEĞERLENDİR

Tasarla ve üret bölümünün ardından aşağıdaki sorular eğitmen tarafından sorulabilir:

- Sizce yazdığınız rastgele parola üretme programı yeterince güçlü parolalar üretebilir mi? Daha güçlü parola üretmesi için neler yapılabilir?
- Verilen bir parolanın güçlü olup olmadığını değerlendiren bir program yazmak isteseniz nasıl bir yaklaşım izlersiniz?

Öğrencilerden süreç içinde kendileri için önemli veya ilginç buldukları hususları arkadaşlarına aktarmaları istenir.

Tüm tartışmaların ardından bu bölümde öğrenilenlerin gelecekte kullanımına yönelik öneriler üzerine beyin fırtınası yapılabilir. Örneğin eğitmen öğrencilere internetten alışveriş yapıp yapmadıklarını ya da ebeveynlerinin e-ticareti kullanıp kullanmadıklarını sorar. E-ticaret yaparken parolamızın başkası tarafından ele geçirilmesi durumunda neler olabileceğine yönelik sınıf içi tartışmalar yürütülerek detaylı biçimde konunun önemi vurgulanır. Bu durumda eğitmen tarafından, yaşanabilecek maddi kayıplarla ilgili olarak örnekler verilebilir. Böylelikle doğru parola seçiminin ne kadar önemli olduğunun öğrenciler tarafından daha net anlaşılması sağlanmış olur.

5. EK ETKİNLİK

Dersin sonunda zaman kalırsa parolalara alternatif kimlik doğrulama yöntemleri hakkında neler bildikleri veya parola kullanmadan kimliği nasıl doğrulanabileceğine ilişkin fikirleri sorulabilir. Eğitmen biyometrik kimlik doğrulama yöntemlerinden (Rui & Yan, 2018) kısaca

bahsedip bir örnek (örn. parmak izi, yüz, ses, retina, iris, el geometrisi tanıma) verdikten sonra öğrencilerden başka örnekler vermelerini isteyebilir. En sonda öğrencilerden parola kullanımı ile biyometrik kimlik doğrulama yaklaşımlarını karşılaştırmaları, avantaj ve dezavantajlarını tartışmaları beklenebilir.

KAYNAKLAR

Rui, Z., & Yan, Z. (2018). A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE access*, *7*, 5994-6009.

Subangan, S., & Senthooran, V. (2019). Secure authentication mechanism for resistance to password attacks. In *2019 19th International Conference on Advances in ICT for Emerging Regions (ICTer)* (Vol. 250, pp. 1-7). IEEE.

HAFTA 4. KRİPTOGRAFİ

ÖN BİLGİ

- Bilgi güvenliğinin temel kavramları
- Parolalar

AMAÇ

Bu bölümün amacı, öğrencileri kriptografinin temel kavramlarıyla tanıştırmaktır. Bölüm içerisinde şifrelemenin temel mantığı anlatılacak ve basit uygulamalarla öğrencilerin bu mantığı kavramaları sağlanacaktır. Ayrıca basit şifre kırma yaklaşımları ele alınarak modern şifreleme algoritmalarının giriş düzeyinde incelemesi gerçekleştirilecektir.

EĞİTMENE NOT

Kriptografi şifreleme bilimi olarak adlandırılabilir. Günümüzde bir üniversite, fakülte, enstitü, meslek kuruluşu ya da kişiye bırakılamayacak kadar önemli bir konudur. Bu nedenle kriptoloji ile ilgili olarak tüm toplumu işin içerisine katan bir yapılanmaya ve farkındalık çalışmalarına ihtiyaç vardır.

BÖLÜM KAZANIMLARI

Bu bölümü tamamlayan bir öğrenci,

- Kriptografinin temel kavramlarını tanımlar.
- Şifrelemenin genel mantığını kavrar.
- Basit bir şifreleme algoritmasını uygular.
- Sezar ve Vigenere algoritmalarını kullanarak şifreleme ve şifre çözme yapar.

- Şifre kırma yaklaşımlarını tanır.
- Şifre kırma uygulaması gerçekleştirir.
- Frekans analizi yöntemini açıklar.
- Modern şifreleme algoritmalarına örnek verir.
- Simetrik anahtarlı şifrelemeyi açıklar.
- Asimetrik anahtarlı şifrelemeyi açıklar.
- Sayısal imza kavramını açıklar.

KULLANILACAK MATERYAL VE ARAÇLAR

Bilgisayar, kâğıt, kalem

HAFTANIN İŞLENİŞİ

Gözle	Kriptografinin temel kavramları, Sezar algoritması, frekans analizi yoluyla şifre kırma, modern şifreleme algoritmalarına giriş ve sayısal imzanın çalışma prensipleri
Uygula	Sezar algoritması ile şifreleme Frekans analizi
Tasarla ve Üret	Şifre kırma yarışması Frekans analizi yapan program geliştirme
Değerlendir	Haftanın içeriğinin değerlendirilmesi ve çalışmanın devam ettirilmesine yönelik öneriler

1. GÖZLE

Bu bölümde kriptografi ile ilgili kavramlar tanıtılarak derinlemesine bir tartışma sağlanacaktır.

1.1. KRİPTOGRAFİNİN TEMEL KAVRAMLARI

Önerilen süre: 20 dakika

Eğitmen öğrencilerinin şifre ile ilgili tartışmalarını sağlar. Bunun için öğrencilerine çeşitli sorular sorarak onların cevabını alır ve ardından kriptografi ile ilgili olarak detaylı açıklamalarını yapar.

- Birine gizli bir mesaj göndermek isteseniz ne yaparsınız?
- Gönderdiğiniz mesajı herkes görebilsin ama sadece seçtiğiniz bir kişi anlayabilsin istiyorsanız bunu nasıl sağlarsınız?
- Kriptografi veya mesaj şifreleme terimlerini duydunuz mu? Bu terimler size ne ifade ediyor?

Eğitmen sadece bu soruları sorarak kendisini sınırlandırmak zorunda değildir. Gelen cevaplarla birlikte öğrencilerden de yeni sorular ortaya çıkabilir. Bunlara benzer sorular çerçevesinde tartışma yönetilerek öğrencilerin fikirlerini beyan etmesi sağlanır. Daha sonra aşağıdaki açıklamalarla devam edilir.

Kriptografi, kötü amaçlı kişilere karşı iletişim güvenliğini korumakta kullanılan yöntemleri inceleyen bilim dalıdır. Kriptografinin en temel tanımlarından bazıları şu şekildedir (Katz & Lindell, 2020):

Şifreleme: Mesajları yetkisiz kişilerce okunamaz hale getirme

Şifre çözme: Şifreli mesajı orijinaline dönüştürme

Şifreleme algoritması: Şifreleme ve/veya şifre çözme için kullanılan algoritma

Düz metin: Orijinal anlamlı mesaj

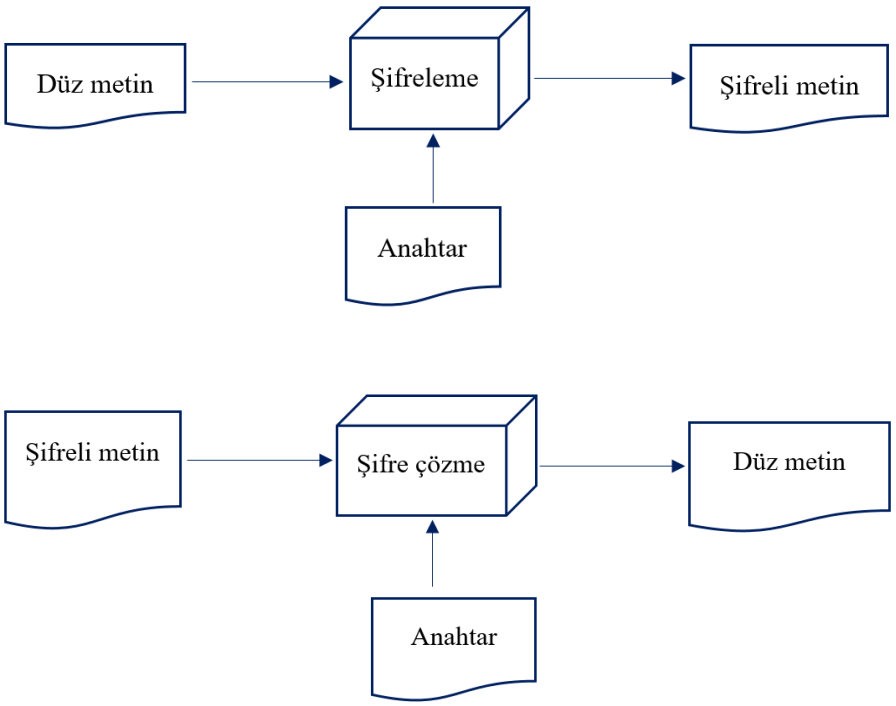
Şifreli metin: Okunamayan şifrelenmiş mesaj

Son yıllarda **"Kripto Para"** kavramı hepimiz tarafından sıkça duyulmaktadır.

Kripto paralar, sanal bir para birimi olup güvenlik amacıyla şifreleme bilimi (kriptografi) kullanmaktadır.

Anahtar: Şifreleme algoritmasının çıktısını belirleyen parametre

Şifreleme, güvenli iletişim için binlerce yıldır kullanılmaktadır. Birçok şifreleme algoritması mesajdaki karakterleri başka karakterlerle değiştirme veya karakterlerin yerlerini değiştirme işlemlerine dayalıdır. Şifrelemenin genel işleyişi Şekil 1'de gösterilmiştir.



Şekil 1. Şifrelemeye genel bakış

Şekil 1'de görüldüğü üzere düz bir metin ya da veri bir anahtar yardımıyla şifrelenerek şifreli hale getirilir. Şifreli hale getirilen metin ya da veri ise yine bir anahtar yardımıyla şifresi çözülerek aslına döndürülür.

1.2. BASİT ŞİFRELEME ALGORİTMALARI: SEZAR

Önerilen süre: 20 dakika

Sezar şifreleme ilk olarak Romalı lider Jül Sezar tarafından kullanılan bir şifreleme tekniği olup adını da buradan almaktadır. Askeri öneme sahip bilgileri ve mesajları korumak için kullanıldığı düşünülmektedir.

Tarihte bilinen ilk şifreleme algoritmalarından biri olan Sezar şifreleme algoritmasında her harf alfabede belirlenen bir k sayısı kadar sağındaki veya solundaki harf ile değiştirilir. Bu k sayısı Sezar algoritmasına verilen anahtar olarak düşünülebilir ve k pozitifse harfler k kadar sağa, negatifse k kadar sola kaydırılır. Örneğin her harfin 3 sağındaki ile değiştirildiği bir Sezar şifresinde, K harfi N ile, D harfi G ile, Z harfi ise (sondan başa dönerek) C ile değiştirilir. Şifreyi çözmek için de bu işlemin tersi yapılır.

Eğitmen aşağıdaki örnek üzerinden Sezar şifrelemenin nasıl yapıldığını öğrencilere açıklar.

Örnek: DENEYAP kelimesini Sezar yöntemi ile şifreleyelim. Anahtarı k = **7** olarak seçelim.

Alfabe: A B C Ç D E F G Ğ H I İ J K L M N O Ö P R S Ş T U Ü V Y Z

Düz metin: D E N E Y A P

Her harfi anahtar olarak belirlediğimiz k değeri olan 7 kadar sağa kaydıralım.

Şifreli metin: İ J T J E G V

Bu noktada şifreleme tamamlanmıştır ve metin okunamaz hale gelmiştir. Şifreli metni çözerek metnin aslına ulaşmak için her harfi 7 sola kaydırmak gerekir. Bu yapıldığında düz metin elde edilir. Yukarıdaki şifreli metin için şifre çözme işlemini eğitmen ve öğrenciler birlikte yaparlar. Eğitmen bu uygulama için öğrencilerin kâğıt ve kalem kullanarak işlemi takip etmelerini isteyebilir.

Şifreli metin yazılırken dikkat edilmesi gereken bir husus, kelimelerin bitiş ve başlangıç noktalarının belli olmamasıdır. Bunun için şifreli metin beşer karakterli kelimeler halinde yazılabilir. Yani şifreli metin DENEYAP TEKNOLOJİ ATÖLYELERİ ise, bunun DENEY APTEK NOLOJ İATÖL YELER İ şeklinde yazılması uygundur. Böylece kelime uzunluklarından şifreyi kırmaya yönelik bir çıkarım yapılamaz.

Sezar gibi karakter değiştirmeye dayalı basit şifreleme algoritmaları kullanıldığında, düz metinde birbirinin aynısı olan harfler şifreli metinde de birbirinin aynısı olur. Yukarıdaki örnekte düz metindeki E harfi şifreli metinde J olmuştur. Bu özellik şifrelemenin gücü açısından olumsuzdur, yani şifreyi kolayca kırılabilir hale getirir.

1.3. FREKANS ANALİZİ YOLUYLA ŞİFRE KIRMA (KRİPTANALİZ)

Önerilen süre: 10 dakika

Sezar gibi basit şifreleme algoritmaları kolayca kırılabilir. Aslında bu şifreleri kırarken şifreli metindeki harflerin asıllarını deneme-yanılma yoluyla bulmak iyi bir yöntem değildir. Çünkü her harf Sezar'da olduğu gibi belirli bir sayıda kaydırılmış olmayabilir. Örneğin, aşağıdaki gibi bir yönteme göre de şifreleme yapılabilir. Tabloda düz metin alfabesi ve harflerin şifreli metindeki karşılıkları gösterilmektedir.

Kriptanaliz, şifrelenmiş metinlerin kırılmasını ve bilinmeyen anahtarların bulunmasını konu alan bir bilim dalıdır.

Şifreyi kırarak şifreli metinden orijinal metni elde etmeye çalışan kişilere **kriptanalist** denmektedir.

Düz	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
Şifreli	V	F	S	Y	B	R	L	Z	D	T	P	Ö	M	I	K	C	Ç	U	İ	E	G	N	O	H	Ğ	Ş	J	Ü	A

Buradaki yöntem ilk bakışta daha karmaşık ve kırılması zor görünse de aslında Sezar'dan daha güçlü bir koruma sağlamaz. Bu tür bir şifreyi kırmak için **frekans analizi** yöntemi kullanılabilir. Frekans analizi, düz metinde birbirinin aynısı olan harflerin şifreli metinde de birbirinin aynısı olmasına dayanır. Şifreli metinde çok rastlanan bir harfin, muhtemelen düz metinde yaygın kullanılan bir harfe denk geldiği düşünülerek hareket edilir (Şenay, 2022).

Örneğin Türkçe bir metin için, şifreli metinde en çok geçen harf J ise, bunun düz metinde A harfine, A değilse E veya İ harflerine karşılık geliyor olması muhtemeldir, çünkü Türkçe'de en çok kullanılan harfler sırasıyla A, E ve İ harfleridir. Bu mantıkla harflerin karşılıkları teker teker tahmin edilip denenerek daha sistemli bir deneme-yanılma uygulanmış olur.

1.4. MODERN ŞİFRELEME ALGORİTMALARI

Önerilen süre: 20 dakika

Günümüzde yaygın bir şifreleme standardı olarak kullanılan algoritma, Advanced Encryption Standard (AES) algoritmasıdır. AES, karakter değiştirme ve yer değiştirme işlemlerinin karmaşık bir düzen içerisinde tekrarlanmasına dayalı bir algoritmadır. AES'te kullanılan anahtar çok büyük bir sayıdır (128, 192 veya 256 bit). Bu anahtarlar yaklaşık olarak 40 ile 80 arasında basamak kullanılarak yazılabilen sayılardır (United States National Institute of Standards and Technology (NIST), 2001).

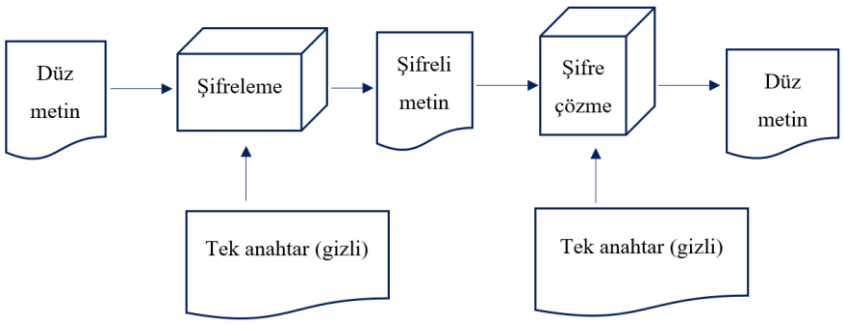
Şifrelemede hiçbir zaman şifreleme algoritmasının gizliliğine, yani nasıl çalıştığının bilinmemesine güvenilmez. Bir başka deyişle, gizli olması gereken şey asla şifreleme algoritması değildir. Tam tersine, şifreleme algoritmasının herkes tarafından bütün ayrıntılarıyla bilinmesi gerekir.

Şifrelemede gizli olması gereken şey **anahtar**dır. Daha önce tanımladığımız gibi anahtar, şifreleme algoritmasının çıktısını belirleyen bir parametredir. Şifreleme algoritmaları anahtar yapısına göre **simetrik** ve **asimetrik** olmak üzere ikiye ayrılırlar.

Simetrik anahtarlı şifreleme: Şifrelemede kullanılan anahtarla şifre çözmede kullanılan anahtarın **aynı** olduğu yaklaşımdır. Bu tek anahtar, sadece şifreli iletişim kuran taraflarca bilinir ve başkalarından gizli tutulur.

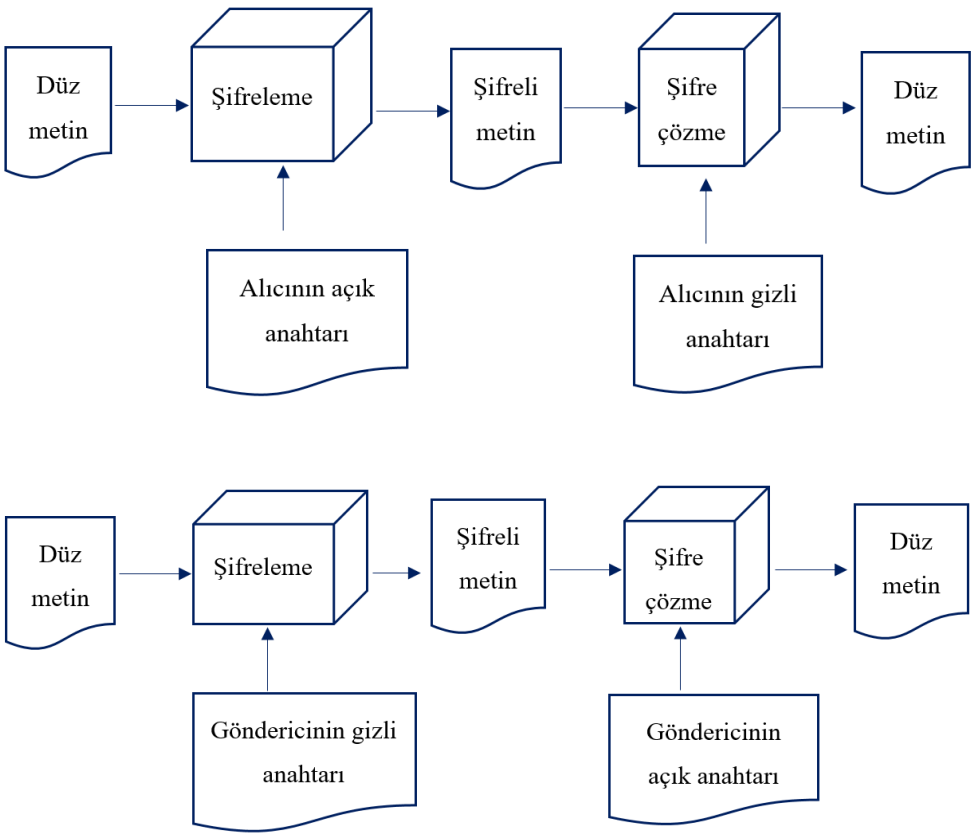
Asimetrik anahtarlı şifreleme: Şifrelemede kullanılan anahtarla şifre çözmede kullanılan anahtarın **farklı** olduğu yaklaşımdır. Bu sistemde herkesin biri gizli biri açık olmak üzere iki anahtarı vardır. Bu iki anahtardan biriyle şifreleme yapıldığından diğeri şifreyi çözmede kullanılır.

Simetrik ve asimetrik anahtarlı şifreleme arasındaki fark Şekil 2 ve Şekil 3'te gösterilmektedir.



Şekil 2. Simetrik anahtarlı şifreleme ve şifre çözme

Şekil 2'de görüldüğü üzere düz metni şifrelerken ve şifreli metni çözerken aynı gizli anahtar kullanılmaktadır.



Şekil 3. Asimetrik anahtarlı şifreleme ve şifre çözme için iki kullanım şekli

Şekil 3'te asimetrik anahtarlı şifrelemenin iki farklı biçimi görülmektedir. Üstteki kullanımda, düz metnin şifrelenmesinde alıcının açık anahtarı, şifrelenmiş metnin çözülmesinde ise alıcının gizli anahtarı kullanılmaktadır. Böylece şifreli metni yalnızca alıcı çözebilir çünkü alıcının gizli anahtarını bir tek alıcının kendisi bilmektedir. Alttaki kullanımda, şifreleme için göndericinin gizli anahtarı, şifre çözme için ise göndericinin açık anahtarı kullanılmaktadır. Bu kullanım ile gizlilik sağlanmaz ancak alıcı, şifreli mesajı göndericinin oluşturduğundan emin olabilir çünkü göndericinin gizli anahtarını bir tek gönderici bilmektedir.

Yaygın kullanılan bir açık anahtarlı (asimetrik) kriptografi algoritması RSA'dır. Bu algoritma adını Ron Rivest, Adi Shamir ve Leonard Adleman adlı geliştiricilerinin soyadlarının ilk harflerinden almıştır. Tamamen matematiğe (sayılar teorisine) dayalı olarak çalışır ve iki asal sayının çarpımından oluşan büyük bir sayıyı çarpanlarına ayırma probleminin zorluğuna dayalı olarak güvenlik sağlar (Beşkirli, Özdemir, & Beşkirli, 2019).

1.5. SAYISAL İMZA

Önerilen süre: 10 dakika

Modern şifreleme algoritmaları başlığı altında Şekil 3'te gösterilen asimetrik şifrelemede şifreleme anahtarı olarak göndericinin gizli anahtarı kullanıldığında ne olduğunu daha ayrıntılı inceleyelim.

Soru: Ayça bir mesajı kendi gizli anahtarı ile şifreleyip Burak'a gönderirse, Burak bu şifreli mesajı nasıl çözebilir?

Cevap: Burak aldığı şifreli mesajı Ayça'nın açık anahtarını kullanarak çözebilir.

Ayça'nın anahtarı açık olduğuna göre aslında herkes bu mesajı çözebilir. Demek ki, bu şekilde yapılan şifreleme gizlilik sağlamaz. Gizlilik yerine bir başka önemli özellik sağlanmış olur: Ayça'nın kimliği bu yolla doğrulanabilir.

Hatırlayalım, asimetrik anahtarlı şifrelemede mesaj bir kişiye ait anahtarlardan biriyle şifrelendiyse diğeriyle çözülmelidir. Bu örnekte mesaj Ayça'nın açık anahtarıyla çözülebildiğine göre, şifreleme Ayça'nın gizli anahtarıyla yapılmış olmalıdır. Burak şifreyi çözdüğünde bunu anlar ve mesajın sadece Ayça'nın gizli anahtarını bilen kişi (yani Ayça) tarafından şifrelenmiş olabileceği sonucunu çıkarır. Bu sonuç, mesajı gönderenin Ayça olduğundan emin olunması anlamına gelir.

Elektronik ya da **sayısal imza**, dijital veriye eklenen ve kimlik doğrulamak amacıyla kullanılan elektronik bir veridir.

Elektronik imzanın atılabilmesi için kişiye ait bir Nitelikli Elektronik Sertifika'nın **(NES)** olması gerekir.

İşte günümüzde birçok sistemde kullanılan sayısal imza, yukarıda açıklanan mantığa dayalıdır. Sayısal imza, bir mesajın "Hash" adı verilen özetinin göndericinin gizli anahtarıyla şifrelenmesi yoluyla oluşturulur ve alıcı tarafından göndericinin açık anahtarı kullanılarak doğrulanabilir.

2. UYGULA

Uygula bölümünde eğitmen için farklı uygulama örnekleri sunulmuştur. Eğitmen zaman durumuna göre uygun sayıda etkinliği öğrencilerine uygulatabilir. Hatta bu etkinliklerin içeriğinde belirtilen mantıksal yoldan ve şifreleme metodolojisinden hareket ederek değişkenleri değiştirip örnekleri kendisi çoğaltarak öğrencilerine yaptırabilir.

2.1. SEZAR ŞİFRELEME UYGULAMASI

Önerilen süre: 15 dakika

Bu etkinlikte her öğrenci bireysel olarak Sezar algoritmasıyla şifreleme yapacaktır.

1. Aşama: Her öğrenci, eğitmenin adını ve soyadını k = 5 değerini kullanarak şifreler ve daha sonra şifreyi çözer.

2. Aşama: Eğitmen, her öğrencinin kendi adını ve soyadını kendi seçeceği bir k değerini kullanarak şifrelemesini ister.

3. Aşama: Her öğrencinin oluşturduğu şifreli metin sırayla incelenerek kullanılan k değeri diğer öğrenciler tarafından tahmin edilmeye çalışılır.

2.2. FREKANS ANALİZİ UYGULAMASI

Önerilen süre: 15 dakika

Eğitmen bir frekans analizi örneği olarak öğrencilerden İstiklal Marşı'nın birinci kıtasında her harften kaçar tane geçtiğini sayarak belirlemelerini ister. Bu etkinlik için öğrencilerin kâğıt kalem kullanması gereklidir.

Bu uygulama eğitmenin seçeceği başka cümleler üzerinden tekrar edilebilir. Bu sayede öğrenciler frekans analizi yöntemini farklı uzunluk ve yapıdaki cümleler üzerinde uygulama şansına sahip olurlar.

3. TASARLA VE ÜRET

Eğitmen bu bölümde iki farklı etkinlik planlayabilir. Önerilen birinci etkinlik Sezar şifreleme ve şifre kırma yarışması, ikinci etkinlik ise frekans analizi yapan program geliştirmedir.

3.1. SEZAR ŞİFRELEME VE ŞİFRE KIRMA YARIŞMASI

Önerilen süre: 40 dakika

Eğitmen sınıftaki öğrenci sayısını dikkate alarak öğrencileri 2 veya 3 kişilik gruplara ayırır.

1. Aşama (10 dk): Her grup en fazla 6 kelimeden oluşan bir Türkçe cümle seçer ve bu cümleyi kâğıt üzerinde veya Not Defteri, Word gibi bir uygulama içinde Sezar şifresi kullanarak elle şifreler. Şifrelemede harf değişimi yapılırken sağa mı sola mı kaydırma yapılacağını ve kaç harf kaydırılacağını gruptaki öğrenciler kendileri ortaklaşa karar alarak belirler.

2. Aşama (20 dk): 1. aşamanın sonunda her grup hem düz cümlesini hem şifreli cümlesini diğer grupların göremeyeceği şekilde eğitmene iletir. Eğitmen bütün şifreli cümleleri herkesin görebileceği şekilde paylaşır. Her grup 20 dakika süre boyunca diğer grupların şifreli cümlelerini çözmeye çalışır. Şifre çözmek için farklı k değerleri denenerek anlamlı sonuç elde edilip edilemediğine bakılabilir.

3. Aşama (10 dk): 2. aşamanın sonunda her grubun çözebildiği cümle sayısı eğitmen tarafından tespit edilir. En çok cümleyi çözmüş olan grup yarışmayı kazanır. Eğer bütün cümleleri çözen birden fazla grup olursa, ilk bitiren grup kazanır.

3.2. FREKANS ANALİZİ YAPAN PROGRAM GELİŞTİRME

Önerilen süre: 60 dakika

Bu etkinlikte her öğrenci verilen bir metin içinde her harften kaç tane olduğunu sayan bir program yazacaktır. Program herhangi bir programlama dilinde yazılabilir.

Girdi: Düz metin (uzunluğu için bir üst sınır koyulabilir, örneğin 1000 karakter)

Çıktı: Alfabedeki harflerden her birinin girdi metninde kaç kez geçtiğini gösteren sayılar

Programın daha kolay yazılabilmesi için, girdi metninin sadece büyük harfler kullanılarak yazıldığı ve harfler dışındaki bütün sembollerin (boşluk, noktalama vb.) girdiden çıkarıldığı varsayılabilir (1. durum). Ancak bu durumda, programı test etme aşamasında girdi verilirken metnin büyük harf dışında bir şey içermemesine dikkat edilmesi gerekmektedir. Programlama düzeyi daha yüksek olan öğrenciler, girdinin küçük harfler ve başka semboller de içerebileceğini (2. durum) düşünerek programı yazmayı deneyebilirler. Bir diğer seçenek, öğrencilerin önce 1. durum için çözüm üretmesi, bunu tamamlayan öğrencilerin 2. durumu çözmeye geçmesi olabilir.

EĞİTMENE NOT

Bu uygulamada girdi metni İngilizce ise ASCII kodlarına dayanan bir çözüm geliştirmek daha kolay olabilir çünkü ASCII tablosunda İngilizcedeki harfler A'dan Z'ye ardışıktır. Ama Türkçe metin için de farklı bir yaklaşımla çözüm geliştirilebilir.

4. DEĞERLENDİR

Önerilen süre: 20 dk

Sezar şifreleme ve şifre kırma yarışmasının ardından her bir gruba aşağıdaki sorular eğitmen tarafından sorulabilir:

- Grup çalışması sırasında sizi en çok zorlayan durum ne oldu? Bu durumu çözebildiniz mi? Nasıl çözdünüz?
- Şifrelemenin önemine ilişkin neler söyleyebilirsiniz?
- Hayatımızda şifrelemenin önemli olduğunu düşündüğünüz kritik alanlar ve uygulamalar aklınıza geliyor mu?

Her gruptan olmasa bile öğrencilerden süreç içinde kendileri için önemli veya ilginç buldukları hususları arkadaşlarına aktarmaları istenir.

Tüm tartışmaların ardından bu bölümde öğrenilenlerin gelecekte kullanımına yönelik öneriler üzerine beyin fırtınası yapılabilir.

5. EK ETKİNLİK: VIGENERE ALGORİTMASI İLE ŞİFRELEME

Eğitmen ek etkinlik olarak Vigenere algoritması ile simetrik anahtarlı şifreleme etkinliğini öğrencilerine yaptırabilir. Bu etkinlik iki kişinin kendi arasında haberleşirken aynı gizli anahtarı kullanması esasına dayanmaktadır. Yani hem verileri şifrelerken hem de şifreyi çözerken yalnızca haberleşen iki kişinin bildiği paylaşılan aynı anahtar kullanılmaktadır.

Vigenere algoritması: 16. yüzyılda icat edilmiş, 19. yüzyılda ise şifre kırma yöntemi bulunmuş bir şifreleme algoritmasıdır. Birden çok Sezar şifresinin iç içe geçmiş hali olarak tarif edilebilir.

Örnek olarak, KRİPTOGRAFİ kelimesini OKUL anahtar kelimesini kullanarak şifreleyelim. KRİPTOGRAFİ 11 harften oluştuğu için, OKUL kelimesini 11 harfe ulaşana kadar tekrar ederek OKULOKULOKU anahtarını elde ederiz. Şifreleme için izleyeceğimiz sonraki basamaklar aşağıdaki gibi olacaktır.

1. Her harfin yerine alfabedeki sırasını belirten sayısal değeri (0 ile başlayarak) yazarız. Bu değerleri belirlemek için aşağıdaki gibi bir tablo kullanabiliriz.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
0	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

KRİPTOGRAFİ = 13 20 11 19 23 17 7 20 0 6 11

OKULOKULOKU = 17 13 24 14 17 13 24 14 17 13 24

2. Şifrelenecek düz metni ve anahtarı alt alta yazarak birbirine denk gelen karakterleri mod 29'da toplarız (Türk alfabesinde 29 harf olduğu için).

Düz metin:	13	20	11	19	23	17	7	20	0	6	11
Anahtar:	17	13	24	14	17	13	24	14	17	13	24
Şifreli metin:	1	4	6	4	11	1	2	5	17	19	6

3. Şifreli metindeki sayıları yukarıdaki tabloya harflere çevirdiğimizde şifreleme işlemi tamamlanmış olur.

Şifreli metin:	B	D	F	D	İ	B	C	E	O	P	F

4. Şifreli metni çözmek için işlemin tersi, yani şifreli metindeki karakterlerden anahtardaki karakterleri mod 29'da çıkarma işlemi yapılır.

Uygulama:

- Öğrencileri ikişer kişilik gruplara ayırın.
- Öğrencilerden birisini mesaj gönderen, diğerini ise mesajı alan biçiminde iki farklı rol ile görevlendirin.
- Mesajı gönderen rolü üstlenen öğrencinin kısa bir anahtar kelime (4-6 harf arası uzunlukta) belirlemesini isteyin.
- Anahtar kelime belirlendikten sonra mesaj gönderen kişi belirlediği bu anahtarı mesajı alan rolündeki kişiye söyler ya da yazar.
- Mesaj gönderen kişi "**Milli Teknoloji Hamlesi DENEYAP**" cümlesini belirlenen anahtara göre şifreleyip yazarak mesajı alıcısına yollar. Bu etkinlik için büyük-küçük harf ayrımına dikkat etmeye gerek yoktur.
- Mesaj alıcısı şifreyi çözer ve mesajın çözülmüş halini kâğıda yazar.
- Gönderici ve alıcı mesajın çözüldüğünü doğrular. Eğer hata varsa hangi aşamada hata yapıldığını birlikte bulurlar.

EĞİTMENE NOT

Aynı etkinlik öğrencilerin belirleyeceği başka cümleler üzerinden tekrar edilerek uygulanabilir. Etkinlikleri uygulatırken öğrencilerin rol değişimlerini (mesaj gönderen, mesajı alan) yapmalarını sağlayınız. Bir uygulamada mesaj gönderen ikincisinde mesajı alan rolü üstlenmelidir.

KAYNAKLAR

Beşkirli, A., Özdemir, D., & Beşkirli, M. (2019). Şifreleme yöntemleri ve RSA algoritması üzerine bir inceleme. *Avrupa Bilim ve Teknoloji Dergisi*, 284-291.

Katz, J., & Lindell, Y. (2020). *Introduction to modern cryptography*. CRC press.

Şenay, Ş. C. (2022). *Basit şifreleme teknikleri*. Efe Akademi Yayınları.

United States National Institute of Standards and Technology (NIST). (2001). Federal Information Processing Standards Publication 197 - Announcing the Advanced Encryption Standard (AES). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

HAFTA 5. KÖTÜ AMAÇLI YAZILIMLAR

ÖN BİLGİ

- Bilgi güvenliğinin temel kavramları
- Kali Linux kullanımı, temel komutlar ve araçlar
- Parolalar
- Kriptografinin temelleri

AMAÇ

Bu bölümün amaçları arasında, öğrencilerin kötü amaçlı yazılım (malware) kavramı, bu yazılımların türleri ve zararları hakkında bilgi edinmelerini sağlamak, öğrencilere kötü amaçlı yazılımlardan korunma farkındalığı kazandırmak ve bu doğrultuda uygulamalar yaptırmak bulunmaktadır. Öğrenciler ayrıca oltalama (phishing) saldırılarını ve sosyal medyanın güvenli kullanımı konusunu öğreneceklerdir.

BÖLÜM KAZANIMLARI

Bu bölümü tamamlayan bir öğrenci,

- Kötü amaçlı yazılımların tarihini özetler ve örnekler verir,
- Kötü amaçlı yazılımların türlerini ve zararlarını açıklar,
- Kötü amaçlı yazılımlardan korunmak için kullanılan teknikleri açıklar,
- Antivirüs yazılımı kullanır,
- Kötü amaçlı yazılımları temel statik analiz yöntemleriyle analiz eder,
- Oltalama mesajı tasarlar ve üretir.

KULLANILACAK MATERYAL VE ARAÇLAR

Bilgisayar, Kali Linux, Windows 8.1 veya 10, Microsoft Defender Antivirus, Microsoft Word, internet bağlantısı, kâğıt, kalem

HAFTANIN İŞLENİŞİ

Gözle	Kötü amaçlı yazılımların tarihi, örnekler, türleri, zararları Antivirüs programı kullanımı Oltalama kavramı ve örnekleri
Uygula	Kötü amaçlı yazılım tespiti için temel statik analiz
Tasarla ve Üret	Oltalama mesajı tasarımı ve üretimi
Değerlendir	Haftanın içeriğinin değerlendirilmesi ve çalışmanın devam ettirilmesine yönelik öneriler

1. GÖZLE: KÖTÜ AMAÇLI YAZILIMLAR

Bu bölümde kötü amaçlı yazılım (malware) kavramı tanıtılarak kötü amaçlı yazılımların tarihi, çarpıcı örnekleri, türleri ve zararları hakkında bilgi verilir.

EĞİTMENE NOT

Kötü amaçlı yazılım için alternatif bir diğer terim zararlı yazılımdır. Kötü amaçlı yazılım, terimin aslının uzun hali olan “malicious software” için daha yakın bir çeviri olduğundan tercih edilmiştir.

Virüs kavramının kötü amaçlı yazılım anlamında kullanımı teknik olmayan dilde yaygındır, ancak virüs bir kötü amaçlı yazılım türüdür ve tüm kötü amaçlı yazılım türleri için bir çatı terim olarak kullanılması doğru değildir. Bununla birlikte, öğrenciler bu farkı anlayana kadar (özellikle Giriş kısmındaki soru-cevap etkinliğinde) bilgisayar virüsü terimi daha genel anlamda kötü amaçlı yazılım için kullanılabilir ve soru-cevabın hemen ardından kötü amaçlı yazılımların farklı türleri tanıtılabilir.

1.1. GİRİŞ

Önerilen süre: 15 dakika

Eğitmen öğrencilerinin kötü amaçlı yazılım ile ilgili tartışmalarını sağlar. Bunun için öğrencilerine çeşitli sorular sorarak onların cevabını alır ve ardından diğer bölümlerde kötü amaçlı yazılım kavramı ve türleri ile ilgili olarak detaylı açıklamalarını yapar.

- Kötü amaçlı yazılım sizin için ne ifade ediyor?
- Bilgisayarınıza, tabletinize veya telefonunuza hiç virüs bulaştı mı? Bulaştıysa neler oldu? Sorunu gidermek için ne yaptınız?
- Antivirüs yazılımı kullanıyor musunuz? Sizce kullanılmalı mı? Neden?
- Cihazlarınızı virüs gibi kötü amaçlı yazılımlardan korumak için nelere dikkat ediyorsunuz?

Eğitmen bu sorulara ek olarak başka sorular da sorabilir. Gelen cevaplarla birlikte öğrencilerden de yeni sorular ortaya çıkabilir. Bunlara benzer sorular çerçevesinde tartışma yönetilerek öğrencilerin fikirlerini beyan etmesi sağlanır.

1.2. KÖTÜ AMAÇLI YAZILIMLARIN TARİHİ VE ÇARPICI ÖRNEKLERİ

Önerilen süre: 15 dakika

Kötü amaçlı yazılımlar (1970'lerdeki birkaç deneysel çalışma dışında) 1980'lerde ortaya çıkmaya başlamıştır. Yaygın etki yapan ilk örneklerinden biri 1988 yılında üretilen ve kendini ağ üzerinden yayarak sistemleri çökerten Morris adlı solucandır (Spafford, 1989). Bu solucanı üreten Robert Morris, kötü amaçlı yazılım geliştirdiği için cezayla karşılaşan ilk kişidir. Morris solucanı, Unix sistemlerindeki bazı programların zafiyetlerinden ve kullanıcıların zayıf parolalarından faydalanmıştır (Furnell & Spafford, 2019).

1990'lar ve 2000'ler boyunca İnternet'in giderek yaygınlaşmasıyla kötü amaçlı yazılımlar da yaygınlaşmış ve etkilerini artırmışlardır. 2010'lara gelindiğinde artık bu yazılımlar çoğunlukla ülkeler arası siber savaşta kullanılmak üzere veya büyük suç örgütleri tarafından maddi kazanç elde etmek amacıyla geliştirilir hale gelmiştir.

2017'de ortaya çıkan WannaCry adlı fidye yazılımı (ransomware) yoluyla, Windows sistemlerindeki bir zafiyeti kullanarak bilgisayardaki bütün dosyaları kilitleyen ve erişilmez hale getiren bir saldırı gerçekleştirilmiştir. Saldırganlar dosyaları tekrar erişilebilir hale getirmek için fidye talep etmiştir. Oltalama (phishing) e-postalarıyla yayılan WannaCry, yüz

binlerce kullanıcıyı etkilemiş ve ciddi maddi kayba yol açmıştır (Chen & Bridges, 2017; Ghafur ve diğerleri, 2019). (Not: Oltalama dersin devamında detaylı olarak anlatılacaktır.)

EĞİTMENE NOT

Kötü amaçlı yazılım olayları çok fazla sayıda ve çeşitli olduğundan bu dokümandaki örneklerin kapsayıcı olması mümkün değildir. Yukarıdaki örneklere ek olarak eğitmen kendi bilgi dağarcığına ve deneyimine dayanan başka örnekler de vererek dersi zenginleştirebilir.

Bu noktada eğitmen öğrencilere duydukları veya karşılaştıkları kötü amaçlı yazılımların neler olduğu, bunların ne amaçla kullanıldığı, geliştirenlerin neleri amaçladığı gibi sorular sorarak 10 dakikalık bir tartışma yönetebilir.

1.3. KÖTÜ AMAÇLI YAZILIM TÜRLERİ

Önerilen süre: 20 dakika

Eğitmen öğrencilere aşağıdaki soruları sorar ve sözlü olarak cevaplarını alır.

- Bildiğiniz bir kötü amaçlı yazılım adı veya türü var mıdır?
- Kötü amaçlı yazılımlar bulaştıkları sistemde neler yapabilir?
- Kötü amaçlı yazılımların kişilere, kuruluşlara, topluma ve ülkeye zararları nelerdir?

Bu tartışmanın ardından eğitmen aşağıdaki açıklamaları yapar.

Kötü amaçlı yazılımlar çok çeşitlidir. Yaygın rastlanan kötü amaçlı yazılımlar ve bunların zararları aşağıda açıklanmaktadır.

Virüs: Kendisini başka bir programa ekleyerek parazit gibi yaşayan kötü amaçlı yazılımlara virüs denir. Virüsün amacı hem kendisini başka programlara yaymak hem de bilgi çalma, cihaza veya dosyalara zarar verme gibi hedefleri gerçekleştirmektir. Virüslerin bazı genel özellikleri aşağıda verilmektedir:

- Virüs kendi başına çalışamaz, başka bir programa tutunarak çalışması gerekir.
- Virüs bağlandığı programın yetkilerine sahip olur.
- Virüsler kendilerini çoğaltırlar ve yeni programları enfekte ederler.

Solucan (worm): Solucanlar kendi başlarına çalışma ve hem sistem içinde hem de ağ üzerinden kendilerini yayma özelliğine sahip programlardır. Solucanlar kendilerini kopyalayarak çoğaltırlar ve gizlenmek için masum görünümlü bir isimle sistemde çalışırlar.

Truva atı (Trojan horse): Kullanıcının kandırılması sonucunda sisteme kullanıcı izniyle yüklenen ve faydalı bir iş yapıyormuş gibi görünüp gizlice zararlı işler yapan program. Truva atı en yaygın kötü amaçlı yazılım türlerinden biridir ve yeterince dikkatli olmayan kullanıcılar çeşitli vaatlere (virüs temizleme, bilgisayarı hızlandırma vb.) aldanarak bu zararlı yazılımları kendileri indirip yükleyebilmektedir.

Casus yazılım (spyware): Bilgileri çalarak başka bir yere gönderme amaçlı program. Yaygın bir casus yazılım türü, kullanıcının bastığı tuşları kaydederek bütün yazdıklarını ele geçirebilen **keylogger** adlı yazılımlardır.

Reklam yazılımı (adware): Kullanıcıya reklam göstererek programı geliştiren kişiye maddi kazanç sağlamayı amaçlayan program. Bu programlar bilgisayarı boş yere meşgul ederek yavaşlatır, bazen de pop-up pencere açarak kullanıcıya rahatsızlık verirler.

Fidye yazılımı (ransomware): Kullanıcının dosyalarını şifreleyip kilitleyen ve açmak için fidye isteyen program. İstenen fidye ödenmezse program dosyaları yok edebilir.

En yaygın kötü amaçlı yazılım türleri yıldan yıla değişim göstermektedir. Truva atları ve reklam yazılımları çok yaygın olmakla birlikte, fidye yazılımları son yıllarda giderek daha sık rastlanır hale gelmektedir.

Özet olarak, kötü amaçlı yazılımlar aşağıdaki hedeflerden birini veya birkaçını gerçekleştirmeye çalışan zararlı programlardır:

- Veriyi yok etme
- Sisteme zarar verme
- Bilgi çalma ve başka yere gönderme
- Kullanıcı dosyalarını şifreleyip fidye isteme
- Sistemi bot (zombi) haline getirme (Not: Bot ya da zombi sistemler, uzaktan ele geçirilip kontrol edilebilen sistemlerdir.)
- Sisteme uzaktan erişim için arka kapı açma

Kötü amaçlı yazılımlar türlerine ve hedeflerine göre farklı kaynaklardan çıkabilmektedir. Maddi kazanç hedefleyen fidye yazılımı gibi yazılımların kaynağı çoğunlukla suç örgütleri iken, solucan ve casus yazılım gibi kendilerini gizleyerek yayılmaya çalışan ve sonrasında bilgi

toplama veya uzaktaki saldırganlara arka kapı açma gibi eylemleri kovalayan yazılımlar, ağırlıklı olarak siber ordular ve istihbarat kuruluşları tarafından kullanılmaktadır.

1.4. KÖTÜ AMAÇLI YAZILIMLARDAN KORUNMA

Önerilen süre: 20 dakika

Eğitmen öğrencilere "Bilgisayarınıza kötü amaçlı yazılım bulaşmaması için nelere dikkat etmelisiniz" sorusunu yönelterek yanıtlarını alır ve ardından açıklamalarını yapar.

Kötü amaçlı yazılımlardan korunmanın en etkili yolu, bilgisayarı ve interneti kullanırken tehlikelerden uzak durmaktır. Bunun için dikkat edilmesi gereken birkaç kural aşağıda verilmiştir.

- İnternete bağlanmadan önce güvenlik duvarı (firewall) etkinleştirilmelidir.
- Şüpheli web sayfaları ziyaret edilmemelidir.
- Truva atı olabilecek şüpheli yazılımlar (örneğin bilgisayarınızda virüs bulunduğu ve izninizle temizleneceği iddiasıyla yükletilmeye çalışılan yazılımlar) bilgisayara indirilmemeli ve yüklenmemelidir.
- Web sayfalarından otomatik olarak inen dosyalar açılmamalıdır.
- E-posta ekinde gelen dosyalar açılırken dikkatli olunmalıdır. Çalıştırılabilir (örneğin .exe uzantılı) dosyalar açılmamalı, diğer dosyalar ise ancak mesajın güvenilirliği doğrulandıktan sonra açılmalıdır.
- USB flash bellekler başkasına ait bilgisayarlara mümkün olduğunca takılmamalı, başkasına ait veya sahibi belirsiz flash bellekler kendi bilgisayarımıza takılmamalıdır.
- İşletim sistemi ve diğer yazılımlar güncel tutulmalı, gerekli yamalar yüklenmelidir.
- İnternetten indirilen veya flash bellekten alınan dosyalar antivirüs yazılımıyla taranmalıdır.

Kötü amaçlı yazılımlarla mücadelede önleme, tespit ve temizleme gibi çeşitli eylemlerin birlikte kullanılması gerekmektedir. Önleme için yukarıda sayılan temel kurallar önemli ölçüde fayda sağlayacaktır. Sistemlere kötü amaçlı yazılımların genellikle internet üzerinden gelen zararlı ağ trafiği yoluyla bulaşması nedeniyle, zararlı trafiği filtreleyen **güvenlik duvarı (firewall)** araçları büyük öneme sahiptir.

Güvenlik duvarı, internetten gelen paketleri belirli kurallara göre filtreleyen yazılımlar veya cihazlardır. Filtreleme, belirlenen kurallara göre zararsız kabul edilen paketlerin geçişine izin verme, zararlı veya şüpheli görülen paketlerin geçişini engelleme şeklinde yapılır. Güvenlik

duvarı, ağa bağlanan özel bir cihaz olabildiği gibi, bilgisayara yüklenen bir yazılım da olabilir. Üst düzey güvenlik sağlamak için ağ güvenlik duvarı, işletim sistemi güvenlik duvarı, web uygulama güvenlik duvarı gibi farklı cihaz ve yazılımların birlikte kullanılması önerilmektedir.

Kötü amaçlı yazılımları önlemekte yetersiz kalındığında bu yazılımlar sistemlere bulaşmaktadır. Bu noktadan sonra, sisteme bulaşan kötü amaçlı yazılımın bulunması ve tanımlanması, bir başka deyişle tespit edilmesi gerekecektir. Kötü amaçlı yazılımları tespit eden programların genel adı **antivirüs** yazılımıdır. Antivirüs yazılımları, kötü amaçlı yazılımlara özgü bazı kod parçaları ve/veya davranış örüntüleri üzerinden tespit yaparlar. Örneğin, bir virüse veya virüs ailesine özgü kod parçasına **virüs imzası** denir. Antivirüs yazılımları, bilinen virüs imzalarını veritabanlarında bulundururlar ve taradıkları programın bu imzalardan herhangi birini barındırıp barındırmadığını kontrol ederler. Eğer taranan programda bu imzalardan biri bulunursa o programın enfekte olduğu sonucuna varılır.

Görüldüğü gibi, bir antivirüs programının virüsü tespit edebilmesi için o virüsün imzasını bilmesi gerekir. Dolayısıyla, her antivirüs programı sık sık güncelleme yaparak yeni imzaları veritabanına katmalıdır. Güncelleme yapılmazsa antivirüs programı yeni virüsleri tanıyamaz hale gelecektir.

Kötü amaçlı yazılım tespiti için imza eşleştirmenin ötesinde daha karmaşık yöntemler de kullanılmaktadır. Kötü amaçlı yazılım analiz teknikleri temelde ikiye ayrılır.

Statik analiz: Program çalıştırılmadan, kod incelenerek yapılan analizdir. Genellikle kaynak kod, bazı durumlarda derlenmiş kod (nesne kodu – object code) üzerinden yapılır. Program kodunda belli örüntüler ve zararlı kod parçaları aranır.

Dinamik analiz: Program çalıştırılıp davranışı incelenerek yapılan analizdir. Programın neler yaptığı, hangi dosyalara eriştiği, sistemde ne gibi değişiklikler yaptığı vb. analiz edilerek zararlı yazılım olup olmadığı anlaşılmaya çalışılır.

Statik ve dinamik analiz çok karmaşık süreçler olduğundan çoğunlukla gelişmiş profesyonel araçlar kullanılarak gerçekleştirilir (Aboaoja ve diğerleri, 2022).

Kötü amaçlı yazılım tespit edildikten sonra gereken temizleme ve sistemi tekrar güvenli hale getirme işlemleri yapılmalıdır.

1.5. ANTİVİRÜS YAZILIMI KULLANIM ÖRNEĞİ

Önerilen süre: 15 dakika

Bu bölümde eğitmen tarafından öğrencilere bir antivirüs yazılımı (örn. Microsoft Defender Antivirus) tanıtılarak bazı temel işlemler gösterilecektir.

Eğitmenin ekran paylaşımı yoluyla öğrencilere aşağıdaki işlemlerin yapılışını gösterebilir:

- Sistem tarama
    - Hızlı tarama
    - Özel tarama (dosya veya konum seçerek)
- Korumayı güncelleme
- Virüs ve tehdit koruması ayarlarını değiştirme
- Denetimli klasör erişimini yönetme
- Karantina yönetimi

EĞİTMENE NOT

Linux için antivirüs yazılımları mevcut olsa da kullanımı pek yaygın değildir. Bu nedenle bu bölümde gösterimin Windows üzerinden yapılması önerilmektedir. Windows sistemlerinde yer alan Microsoft Defender Antivirus bu etkinlik için kullanılabilir.

2. UYGULA

2.1. KÖTÜ AMAÇLI YAZILIM TESPİTİ İÇİN TEMEL STATİK ANALİZ

Önerilen süre: 40 dakika

Bu etkinlikte öğrenciler hash değeri karşılaştırması ve metin içinde arama yoluyla temel statik analiz yapmayı öğreneceklerdir.

Etkinlikte izlenecek adımlar için Ek 1'de sunulan doküman takip edilebilir.

3. GÖZLE: OLTALAMA VE SOSYAL MÜHENDİSLİK

Önerilen süre: 20 dakika

Eğitmen öğrencilerinin oltalama (phishing) hakkında tartışmalarını sağlar. Bunun için öğrencilerine çeşitli sorular sorarak onların cevabını alır ve ardından oltalama ile ilgili detaylı açıklamalarını örnekler kullanarak yapar.

- Size güvenilir gelmeyen e-postalar veya mesajlar alıyor musunuz?
- Sizce bir e-postanın veya mesajın şüpheli olması ne demektir? Nasıl mesajlardan şüphelenirsiniz?
- Oltalama saldırısı diye bir şey duydunuz mu? Örnek verebilir misiniz?
- Sosyal mühendislik kavramı size ne ifade ediyor?

Eğitmen bu sorulara ek olarak başka sorular da sorabilir. Gelen cevaplarla birlikte öğrencilerden de yeni sorular ortaya çıkabilir. Bunlara benzer sorular çerçevesinde tartışma yönetilerek öğrencilerin fikirlerini beyan etmesi sağlanır.

Tartışmadan sonra aşağıdaki temel bilgiler ve örnekler öğrencilere açıklanır.

Sosyal mühendislik, insanları kandırarak saldırganın istediği yönde hareket etmelerini sağlamayı amaçlayan yöntemlere denir. En yaygın amaçlardan biri hedefteki kişinin parola gibi gizli bilgilerini elde etmektir. Bir başka yaygın hedef, insanları yanlış bilgilerle korkutarak veya boş vaatlerle kandırarak saldırganlara para vermelerini sağlamak, yani dolandırıcılık yapmaktır. Günümüzde sosyal mühendislik elektronik posta, SMS, sosyal medya mesajları, hatta telefon aramaları kullanılarak yapılabilmektedir.

Oltalama, sahte mesajlar yoluyla gerçekleştirilen yaygın bir sosyal mühendislik saldırısı türüdür. Oltalamada e-posta, SMS veya sosyal medya mesajları kullanılabilir. Oltalama mesajının içine yerleştirilen linke tıklayan bir kullanıcı, genellikle kullanıcı adı ve parola gibi gizli bilgilerini girmesi istenen bir sayfaya yönlendirilir. Kullanıcının bu sayfada girdiği bilgiler saldırganın eline geçmiş olur.

Oltalama saldırılarının bazı örneklerini incelemek için University of California, Berkeley tarafından aşağıdaki adreste paylaşılan bağlantılar incelenebilir.

https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive

Günümüzde bu tür saldırılar için sosyal medya yaygın biçimde kullanılmaktadır. Sosyal medyayı güvenli kullanabilmek için dikkat edilmesi gereken bazı önemli hususlar vardır:

- Her zaman güçlü parolalar kullanılmalıdır.
- Bilgilerinizi ve yaptıklarınızı kimlerin görebileceğini belirleyen mahremiyet (privacy) ayarları öğrenilmeli ve dikkatlice kullanılmalıdır.
- Suç oluşturan, kırıcı söz içeren veya sizi yanlış tanıtan paylaşımlar yapılmamalıdır.
- Sahte hesaplara karşı dikkatli olunmalıdır.
- Mesajdaki linke tıklamak veya sosyal mühendislik girişimi olabilecek mesajları yaymak gibi hareketlerden kaçınılmalıdır.

Eğitmen bunları öğrencilere aktardıktan sonra sosyal medyanın güvenli kullanımında işe yarayabilecek başka kuralların ve tavsiyelerin neler olabileceğiyle ilgili tartışma yürütülür.

4. TASARLA VE ÜRET

Önerilen süre: 40 dakika

Bu bölümde öğrenciler iki kişilik gruplar halinde bir oltalama mesajı tasarlayacaklardır. Bu etkinliğin başında, Ders Uygulama Kılavuzu içinde yer alan etik ile ilgili hususların hatırlatılması önemlidir.

1. Aşama (20 dk): Her grup kullanacağı mesaj türünü kendisi seçer. Mesaj türü e-posta, SMS veya herhangi bir sosyal medya paylaşımı olabilir. Grup bu seçimden sonra mesajın içeriğini ve görünümünü bir Word dosyası içinde oluşturacaktır. Öğrenciler çalışmaya başlamadan önce eğitmen, oltalama saldırılarının hedefinin mesajı alan kişiyi kandırarak linke tıklamasını ve başka bir sayfada bilgilerini girmesini sağlamak olduğunu hatırlatır. Öğrencilerin mesajlarını bu hedefi gözeterek tasarlaması önerilir.

2. Aşama (20 dk): Gruplar 1. aşamanın sonunda mesajlarını paylaşacaklardır. Bu aşamada bir değerlendirme yapılarak en başarılı mesajlar belirlenecektir. Mesajın başarısı, kurbanın mesajdaki linke gitme ihtimali ile ölçülebilir. Öznel bir ölçüt olan bu ihtimali değerlendirme yöntemi olarak, her grubun kendi mesajı dışındaki bütün mesajları incelemesi ve en inandırıcı bulduğu üç mesajı seçerek 1-2-3 şeklinde oy vermesi istenebilir. Bütün gruplar bu değerlendirmeyi tamamladıklarında oylama sonuçlarına göre en başarılı bulunan mesajlar incelenerek neden başarılı oldukları tartışılır.

5. DEĞERLENDİR

Önerilen süre: 15 dakika

Tasarla ve üret bölümünün ardından aşağıdaki sorular eğitmen tarafından sorulabilir:

- Ürettiğiniz oltalama mesajını daha inandırıcı hale getirmek için neler yapabilirsiniz?
- En başarılı oltalama mesajı, alıcılarının ne kadarlık bir oranını (yüzde kaçını) kandırabilir?

Öğrencilerden süreç içinde kendileri için önemli veya ilginç buldukları hususları arkadaşlarına aktarmaları istenir.

Tüm tartışmaların ardından bu bölümde öğrenilenlerin gelecekte kullanımına yönelik öneriler üzerine beyin fırtınası yapılabilir. Eğitmen aşağıdaki örnek soru ve benzeri sorular üzerinden tartışmayı yönlendirip genişletebilir:

- Bir mesajın sosyal mühendislik veya oltalama olup olmadığını anlayan bir program yazmak isteseniz nasıl bir yaklaşım izlersiniz?

6. EK ETKİNLİK

6.1. SOSYAL MÜHENDİSLİK TESPİTİ İÇİN UYGULAMA TASARIMI

Önerilen süre: 45 dakika

Bu bölümde öğrenciler ikili gruplar halinde, incelenen bir e-postanın oltalama mesajı olup olmadığını anlayan bir program tasarlayacaklardır. Yöntemlerini koda dökmeden, algoritma adımları veya akış şeması şeklinde ifade edebilirler. Bu etkinlikte öğrenciler internetten araştırma yapabilir ve aşağıdaki soruları cevaplamaya çalışarak tasarımları için kılavuz olarak kullanabilirler.

- Oltalama e-postalarını diğer e-postalardan ayıran özellikler neler olabilir? Uzunluk, içerik, gönderen adres vb. yönlerden normal e-postalarla ne gibi farklar gösterebilir?
- Oltalama e-postalarının diğer e-postalardan bazı farklarını belirlersek bunları program içinde nasıl kullanabiliriz?
    - Örneğin, oltalama mesajlarında sık geçen bazı kelimeleri belirlediğimizi varsayalım. Bunları programımızda nasıl kullanabiliriz?

- Oltalama e-postası gönderdiği bilinen bazı e-posta edreslerini elde ettiğimizi varsayalım. Bunları programımızda nasıl kullanabiliriz?

Etkinliğin son 15 dakikasında gruplar tasarladıkları algoritmanın adımlarını veya akış şemasını eğitmene sunarlar. Sunumlar esnasında veya sonrasında eğitmen veya diğer gruplar geri bildirim yaparak tartışmaya katkı sağlayabilirler.

KAYNAKLAR

Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-rimy, B. A. S., Eisa, T. A. E., & Elnour, A. A. H. (2022). Malware detection issues, challenges, and future directions: A survey. *Applied Sciences*, *12*(17), 8482.

Chen, Q., & Bridges, R. A. (2017). Automated behavioral analysis of malware: A case study of wannacry ransomware. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 454-460). IEEE.

Furnell, S., & Spafford, E. H. (2019). The Morris worm at 30. *ITNow*, *61*(1), 32-33.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ digital medicine*, *2*(1), 1-7.

Spafford, E. H. (1989). The Internet worm program: An analysis. *ACM SIGCOMM Computer Communication Review*, *19*(1), 17-57.

Ek 1. Kötü Amaçlı Yazılım Tespiti için Temel Statik Analiz

Bu bölümde temel statik analiz için aşağıdaki adımlar takip edilecektir.

1. Kötü amaçlı yazılım örnekleri elde etmek için theZoo adlı github projesinden faydalanılacaktır. theZoo'nun web sayfasındaki (https://github.com/ytisf/theZoo) uyarı Türkçe'ye çevrilerek aşağıda paylaşılmıştır. Öğrencilerin bu uyarıyı dikkate alarak hareket etmeleri çok önemlidir.

   UYARI: "theZoo'nun amacı, kötü amaçlı yazılımların incelenmesine izin vermek ve kötü amaçlı yazılım analiziyle ilgilenen kişilerin canlı kötü amaçlı yazılımlara erişmelerine, bunların çalışma biçimlerini analiz etmelerine ve hatta belki de bilgili insanların belirli kötü amaçlı yazılımları kendi ortamlarında engellemelerine olanak tanımaktır.

   Lütfen bunların canlı ve tehlikeli kötü amaçlı yazılımlar olduğunu unutmayın! Şifreli ve kilitli olarak gelmelerinin bir sebebi var! Ne yaptığınızdan tam olarak emin değilseniz onları çalıştırmayın! Sadece eğitim amaçlı kullanılacaklardır!

   Bunları internet bağlantısı olmayan ve konuk eklemeleri veya eşdeğerleri olmayan bir VM'de çalıştırmanızı öneririz. Bunların bazıları solucandır ve otomatik olarak yayılmaya çalışırlar. Bunları kısıtlama olmadan çalıştırmak, **kendinize veya başkalarına acımasız ve tehlikeli kötü amaçlı yazılım bulaştıracağınız anlamına gelir!"**

   Öğrencilerin kötü amaçlı yazılımları kesinlikle çalıştırmamaları gerekmektedir.

2. Kali Linux terminal ekranında aşağıdaki komutu çalıştırınız:

```
sudo git clone https://www.github.com/ytisf/theZoo
```

3. Ev (Home) dizininizin altındaki theZoo/malwares/Binaries dizini içinde kötü amaçlı yazılım örnekleri bulunmaktadır. Bu dizine geçiş yapınız.

4. Binaries dizini altındaki dizinlerden herhangi birine geçiş yapılarak file komutu yardımıyla kötü amaçlı dosyanın türü ve hedef aldığı işletim sistemi tespit edilecektir. Bu alt dizinlerin altında .zip uzantılı bir dosya içinde yer alan malware örnekleri, unzip komutunun root olarak çalıştırılmasıyla çıkartılabilir. Örneğin, CryptoLocker_22Jan2014 dizini altında "sudo unzip CryptoLocker_22Jan2014.zip" komutu çalıştırılıp parola sorulduğunda CryptoLocker_22Jan2014.pass dosyası içindeki parola kullanılır. Daha sonra "file 1002.exe" komutu çalıştırılınca, dosyanın PE32, yani

32-bit Windows sistemlerini hedef alan bir çalıştırılabilir dosya olduğu görülür. Bu komutları birkaç farklı dizin ve dosya için tekrarlayarak incelemeyi sürdürünüz.

5. Bu adımda dosyaların içindeki karakter dizileri (stringler) incelenecektir. Seçtiğiniz bir `dosya_adı` için `strings` komutunu aşağıdaki şekilde çalıştırınız.

```
strings dosya_adı
```

İncelediğiniz çıktıda faydalı bir bilgi görüyor musunuz?

6. Seçtiğiniz bir `dosya_adı` için hash çıktılarını incelemek amacıyla aşağıda verilen komutları çalıştırınız ve çıktılarını ayrı bir yere kopyalayınız.

```
md5sum dosya_adı

sha1sum dosya_adı

sha256sum dosya_adı
```

7. Bu adımda VirusTotal uygulamasının web arayüzü yardımıyla kötü amaçlı yazılım örnekleri hakkında bilgi alacağız. Web tarayıcınızda aşağıdaki adrese gidiniz:

   https://www.virustotal.com/gui/home/upload

   6. adımda kopyaladığınız hash çıktılarından birini Search tabı altındaki alana yapıştırınız ve arama yapınız. VirusTotal, kötü amaçlı yazılım hakkında ayrıntılı bir rapor oluşturacaktır. Bu raporun farklı alanlarını inceleyiniz. Nasıl bilgiler görüyorsunuz?

8. 4-7 arasındaki adımları süre yettiğince istediğiniz kadar tekrarlayarak incelemenizi sürdürünüz.

Kaynak: https://www.theta432.com/post/malware-analysis-part-1-static-analysis

HAFTA 6. SİBER SALDIRI ANALİZİ

ÖN BİLGİ

- Temel güvenlik kavramları
- Yazılım güvenlik açığı bulma
- Donanım güvenlik açığı bulma

AMAÇ

Bu bölümün amacı, öğrencileri bir siber saldırının analizi ile ilgili temel kavramlar hakkında bilgi sahibi yapmaktır. Bu analizin amacı siber saldırılara karşı önlem alma mekanizmalarını öğrenmelerini sağlamaktır. Bölüm içerisinde güvenlik açığı türleri anlatılacak, kötü amaçlı yazılım türlerine değinilecek, sızma yöntemleri ve hizmet engelleme detaylı olarak anlatılacaktır. Ayrıca farklı konularla ilgili olarak öğrencilerin çeşitli uygulamaları yapmaları sağlanacaktır.

BÖLÜM KAZANIMLARI

Bu bölümü tamamlayan bir öğrenci,

- Güvenlik açıklarının sebeplerini açıklar.
- Yazılım güvenlik açıklarının sebeplerini sıralar.
- Donanım güvenlik açıklarının sebeplerini sıralar.
- Son yıllarda yaşanan güvenlik ihlallerine örnekler verir.
- Güvenlik açıklarını kategorize eder.
- Sızma yöntemlerini açıklar.
- WHOIS aracını uygular.
- ZENMAP port taramasını uygular.
- DoS saldırı türlerini açıklar.
- DDoS saldırı türlerini sayar.

- Wireshark ile ağ trafiğini izler.

KULLANILACAK MATERYAL VE ARAÇLAR

Bilgisayar, İnternet, Wireshark yazılımı, kâğıt, kalem

HAFTANIN İŞLENİŞİ

Gözle ve Uygula	Güvenlik açığı çeşitlerini kavrama, istismar (exploit) kavramını açıklayarak bir istismar çalıştırma, Meltdown ve Spectre güvenlik açıklarını tanımlama, saldırı türlerini sınıflandırma, güvenlik ihlali yöntemlerini sayma, DoS ve DDoS saldırılarını açıklama
Uygula	Wireshark ile ağ izleme uygulaması, Whois sorgulama etkinliği
Tasarla ve Üret	DDoS saldırı yarışması
Değerlendir	Haftanın içeriğinin değerlendirilmesi ve çalışmanın devam ettirilmesine yönelik öneriler

1. GÖZLE VE UYGULA

Bu bölümde siber saldırılar ile ilgili çeşitli kavramlar tanıtılarak derinlemesine bir tartışma sağlanacaktır.

1.1. GÜVENLİK AÇIĞI

Eğitmen öğrencilerinin güvenlik ile ilgili tartışmalarını sağlar. Bunun için öğrencilerine çeşitli sorular sorarak onların cevabını alır ve ardından güvenlik ve güvenlik açıklıkları ile ilgili olarak detaylı açıklamalarını yapar. Bütün bu işlemler için 15-20 dakikalık bir zaman ayırmak yeterlidir.

- Parola ile hangi mekânlara giriş yapıyorsunuz? (Buradaki parola herhangi bir fiziki anahtar ya da manyetik kart da olabilir)
- Okul ya da oturduğunuz apartmana girerken anahtar ya da parola kullanıyor musunuz? Eğer kullanıyorsanız neden böyle bir yol tercih etmekteyiz? Sebebi nedir?

- Oturduğunuz apartmanın ya da sitenin güvenlik personeli var mı? Varsa güvenlik bulundurmanın sebebi nedir?
- Okulunuzun güvenlik personeli var mı? Varsa güvenlik bulundurmanın sebebi nedir?
- Oturduğunuz apartman ya da sitede kameralar var mı? Varsa kamera bulundurmanın sebebi nedir? Bu kameralar nerede/nasıl işimize yarar?

"Tübitak BİLGEM Parola Güvenliği Ölçer" (https://sge.bilgem.tubitak.gov.tr/tr/bilgimi-koruyorum) ya da (https://bilgimikoruyorum.org.tr/ilkders/index.php?b223_yaparak_ogrenelim) ile parolaların testini çevrimiçi gerçekleştirebilirsiniz.

Parolanızı Ölçün!

Parola: Parolayı Göster

Puan (%): 0% Çok Zayıf

Toplam puan: -100 (Fazla tekrar yokken toplam puan : -100)

Tipi	Açıklama	Min. Sayı	Toplam sayı	Puan	Ceza	Toplam Puan
3	Kritik özellikler	3	0	10	-10	-10
3	Karakter sayısı *	5	0	10	-20	-20
3	Önerilen karakter sayısı	8	0	10	-10	-10
3	Küçük harf kullanımı *	1	0	10	-10	-10
3	Büyük harf kullanımı *	1	0	10	-10	-10
3	Rakam kullanımı *	1	0	10	-10	-10
3	Sembol kullanımı *	1	0	10	-10	-10
3	Rakamların aralarda kullanımı	1	0	10	-10	-10
3	Sembollerin aralarda kullanımı	1	0	10	-10	-10
2	Ardışık harf kullanımı		0	0	-10	0
2	Ardışık rakam kullanımı		0	0	-10	0
2	Klavye kalıpları kullanımı		0	0	-10	0
2	Tekrarlanan kısımlar var		0	0	-10	0
2	Tersten yazılan kısımlar var		0	0	-10	0

Eğitmen sadece bu soruları sorarak kendisini sınırlandırmak zorunda değildir. Gelen cevaplarla birlikte öğrencilerden de yeni sorular ortaya çıkabilir. Bunlara benzer sorular çerçevesinde tartışma yönetilerek öğrencilerin fikirlerini beyan etmesi sağlanır. Gerçek yaşam içinde öğrencilerin fikirleri ile birlikte güvenliğin ne kadar önemli olduğu sonucuna hep birlikte varılır. Günlük yaşamdaki güvenlik ve güvenlik açığı neticesinde ortaya çıkacak durumlardan yola çıkarak dijital ortamda güvenliğe geçiş yapılır. Dijital güvenliğe geçiş yaparken de eğitmen aşağıda yer alan sorularla tartışmayı yönetebilir:

- Bilgisayarınızın güvenliğini nasıl sağlıyorsunuz?
- Bilgisayara parola koymamızın amacı nedir?

- Bir web sitesine üye olurken kullanıcı adı ve parola seçiminde hangi kriterleri dikkate alıyorsunuz?
- Parolamız bir başka kişinin eline geçerse neler olabilir?
- Siber savaş kavramını duydunuz mu? Duyan varsa ne demek olduğunu açıklayabilir mi?

Öncelikle yaşam içindeki güvenlik ardından dijital hayattaki güvenlik konularına öğrenciler motive edilmek zorundadır. Devamında güvenlikle ilgili temel kavramlar eğitmen tarafından açıklanır.

EĞİTMENE NOT

Bilgi güvenliği ve önemi, parola güvenliği, zararlı programlar, sosyal mühendislik, e-posta güvenliği ve ADSL modem güvenliği konuları ile ilgili olarak öğrencilerin https://bilgimikoruyorum.org.tr/ilkders/index.php?b100_bilgi-guvenligi linkinde yer alan içeriklerden yararlanabilir ya da incelemeleri için öğrencilerinizle paylaşabilirsiniz.

İstismar (Exploit):

Bir bilişim sistemine saldırmak isteyen kötü niyetli kişiler öncelikle güvenlik açığı tespit eder. Bu açıklıklar donanım ya da yazılım kaynaklı olabilir. Herhangi bir güvenlik açığından, kod hatasından ya da sistemden kaynaklı hatalardan yararlanarak güvenlik ihlallerine sebep olan programlara istismar (exploit) adı verilmektedir (Çakır & Yaşar, 2015).

EĞİTMENE NOT

İstismar (exploit) kavramı ile ilgili olarak öğrencilerin https://www.youtube.com/watch?v=9ArppIx1lAg linkinde yer alan videoyu izlemesini sağlayınız.

Yazılım güvenlik açığı: Yazılım güvenlik açıklığı bir yazılım ya da işletim sisteminin kullanılmaya başlanmasıyla birlikte ortaya çıkan hatalardan oluşmaktadır. Üretici firmalar bu hataları gidermek için yama ya da güncelleme adı verilen programları piyasaya sürerek kullanıcıların yükleme yapmalarını istemektedir. Güncellemenin belli bir periyodik dönemi bulunmamaktadır, yıl içerisinde üreticiler tarafından herhangi bir güncelleme çıkarıldığında

kullanıcıya bildirim verilerek o yazılımla ilgili bir güncellemenin mevcut olduğu haber verilmektedir (Kekül, Ergen, & Arslan, 2021).

Donanım güvenlik açığı: Donanım güvenlik açıklıkları genellikle tasarımdan kaynaklanan hatalardır. Örneğin bir güvenlik açığı mikroişlemci (CPU) üretiminde gözden kaçırılmış olabilir. Üretilmiş olan CPU'nun kendisine gelen emirleri herhangi bir sıra gözetmeksizin uygulamaya koyması donanımdan kaynaklanan güvenlik açığına örnek olarak gösterilebilir. Böyle bir durumda CPU çalıştırmaması gereken bir kodu çalıştırarak güvenlik zafiyetine sebep olabilir.

EĞİTMENE NOT

Son dönemde Google güvenlik uzmanları tarafından AMD, Intel ve ARM işlemcilerde "**Meltdown** ve **Spectre**" isimli açıklar tespit edilmiştir. Öğrencilerin bu açıklarla ilgili araştırma yapmalarını sağlayınız.

Aşağıda yer alan uygulama ile öğrenciler istismar içerisinde yer alan kod bloklarını, bir istismarın neye benzediğini ve dizin yapısını inceleme şansına sahip olacaklardır.

Uygulama:

1. Kali Linux işletim sisteminde en yetkili kullanıcı olan root ile sisteme giriş yapınız.
2. Terminal ya da konsol ekranına cd /usr/share/exploitdb/ komutunu yazıp enter tuşuna basınız.
3. ls komutunu yazarak enter tuşuna basınız.
4. Listeleme işlemi ekranda görünecektir. Girmek istenen dizine cd komutu ile giriş yapınız. Örneğin cd platforms/
5. ls komutunu yazarak enter tuşuna basınız.
6. Ekranda birçok platformu göreceksiniz. Listedeki herhangi bir platforma girmek için cd komutu ile giriş yapınız. Örneğin cd windows/
7. ls komutunu yazarak enter tuşuna basınız.
8. Ekranda istismar çeşitlerinden dos, local, remote, shellcode, webapps seçenekleri görünecektir. Hangi istismar yapılacaksa ona cd komutu ile giriş yapmak gerekmektedir. Örneğin cd remote/ yazarak enter tuşuna basınız.
9. ls komutunu yazarak enter tuşuna basınız.
10. Ekranda uzaktan istismar (remote exploit) ile ilgili onlarca seçenek görünecektir.

11. Bu seçeneklere göz attıktan sonra cd ../ ../ .. komutunu yazarak enter tuşuna basınız.
12. ls komutunu yazarak enter tuşuna basınız.
13. Ekranda files.csv, platforms, searchsploit seçenekleri görünecektir. Bunların dışında seçenekler de işletim sisteminin farklılığından dolayı görünebilir.
14. grep freeSSHd files.csv yazarak enter tuşuna basınız.
15. Ekranı inceledikten sonra grep freeSSHd files.csv | grep remote komutunu girerek enter tuşuna basınız. Ekranda .pl uzantılı dosyaları göreceksiniz. Örneğin 5751.pl gibi bir sploid listede görebilirsiniz.
16. Ekranı inceledikten sonra cd platforms/windows/remote/ yazarak enter tuşuna basınız.
17. cp 5751.pl /root/freeSSHdexploi.pl komutunu yazarak enter tuşuna basınız.
18. cd /root/ komutunu yazarak enter tuşuna basınız.
19. ls komutunu yazarak enter tuşuna basınız. Listede istismarlar görünecektir. Örneğin freeSSHdexploit.pl gibi
20. İstismara girmek için vim freeSSHdexploit.pl komutunu yazarak enter tuşuna basınız.
21. Ekrana gelen istismarın içeriğini kaydırma çubuğu ile aşağı ve yukarı kaydırarak inceleyebilirsiniz.

Bu uygulama adımlarının videolu anlatımı için Siber Güvenlik Akademisi isimli Youtube kanalındaki videoyu izleyebilirsiniz: https://www.youtube.com/watch?v=tOsCwMOSRAY Bu uygulama ile öğrenciler bir istismar içinde yer alan kod bloklarının yapısını inceleyerek neye benzediği konusunda fikir sahibi olurlar.

Uygulamanın ardından eğitmen bazı güvenlik açıklığı türleri ile ilgili olarak aşağıdaki açıklamaları yapabilir.

Arabellek taşması: Her uygulamanın kullandığı ya da ürettiği veriler için bellekte bir yer kullanılır. Bellekte kendisine ayrılan yerin dışında başka yerlere de erişmeye ve kullanmaya çalışmak güvenlik sıkıntılarına neden olabilir. Üstelik sistemin çökmesine ve çalışmamasına da yol açabilir.

Doğrulanmamış girdi: Programın işlemesi için girdi olan verinin kötü amaçlı olarak kullanılmasıdır. Kötü amaçlı bir girdi programın çalışmamasına ya da hizmetin aksamasına neden olabilir.

Güvenlik zayıflıkları: Her bir üretici kendi güvenlik mekanizmalarını ya da algoritmalarını geliştirmekle birlikte, daha önceden güvenilir firmalar tarafından geliştirilmiş ve test edilerek güvenliği kanıtlanmış olan kütüphanelerin kullanılması çok daha uygundur.

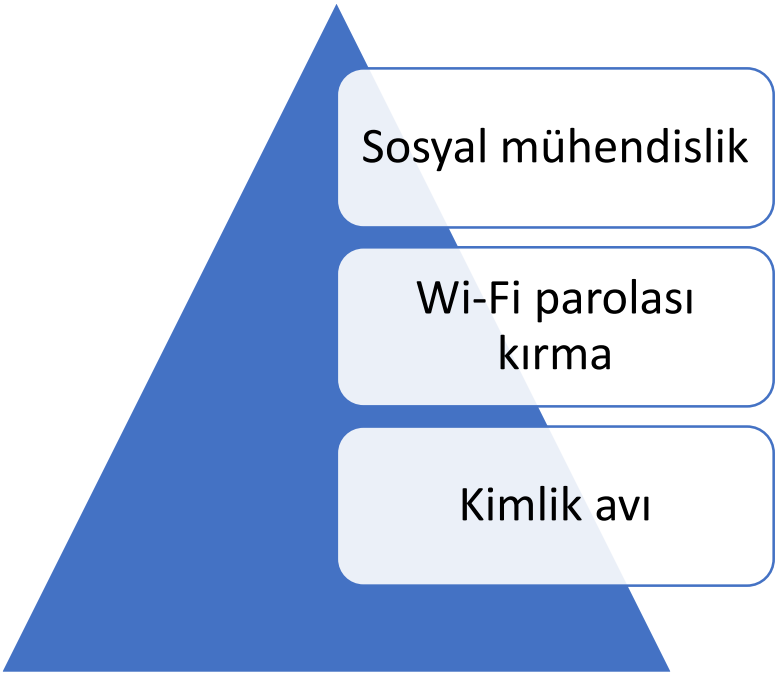
Erişim sorunları: Sistem kullanıcılarının izlenmesi oldukça önemlidir. Çünkü güvenlik sorunlarının büyük bir kısmına sistemin kullanıcılarının yol açtığı unutulmamalıdır.

EĞİTMENE NOT

Saldırı türlerinden **Morris Worm** ve **SQL Slammer Attack** saldırılarının öğrenciler tarafından araştırılmasını sağlayınız. Bu saldırıların hangi tür saldırı tipleri olduğuna yönelik öğrencilerin görüşlerini alabilirsiniz.

1.2. SIZMA YÖNTEMLERİ

Güvenlik açığı oluşturmada özellikle son dönemde kullanılan yöntemlerden bazıları Şekil 1'de gösterilmektedir (Doğan, 2021).



Şekil 1. Güvenlik ihlali yöntemleri

Sosyal mühendislik: Günümüzde özellikle karşılaşılan sızma yöntemidir. İnsanların zayıflıklarından, korkularından ya da dikkatsizliklerinden yararlanarak onları tuzağa düşürme işlemidir. Örneğin kişiye e-posta yollayarak mailbox şifrenizin süresi doldu, şifreyi yenilemek için linke tıklayınız; ya da bedava cep telefonu kazandınız, formu doldurunuz şeklinde gelen mesajlar sosyal mühendisliğe örnek olarak verilebilir.

Wi-Fi parolası kırma: Bir kablosuz ağa girebilmek için gerekli olan şifreyi elde edebilmek için sosyal mühendislik veya kaba kuvvet saldırıları yöntemleri kullanılabilir. Son dönemdeki önemli güvenlik problemlerinden birisidir.

Kimlik avı: Kimlik avı phishing, yemleme ya da oltalama olarak da adlandırılmaktadır. Günümüzde dolandırıcılıkta sıklıkla başvurulan bir yöntemdir. Örneğin, bildiğiniz bir telekom firması tarafından yollanıyormuş gibi gösterilen ve içinde bir linke tıklayarak görevinizi yapmanızı isteyen bir e-posta bu tür saldırıya örnektir.

1.3. SALDIRILAR

Güvenlik zafiyetine neden olan saldırılar ağ, sistem ve web saldırıları şeklinde sınıflandırılabilir. Bu kısımda günümüzde yaygın biçimde kullanılan ağ saldırılarından DoS ve DDoS açıklanmaktadır.

DoS (Denial of Service) saldırıları: Hizmeti yavaşlatan, aksatan ya da çalışamaz hale getiren ağ saldırı türüdür. Bir saldırgan bir sunucuya cevap veremeyeceği yoğunlukta ve miktarda veri yolladığında sunucu bunu kaldıramaz ve hizmet aksar. Bu durum DoS saldırısına örnek olarak verilebilir.

DDoS (Distributed DoS) saldırıları: DoS saldırısına benzer, ancak saldırı bir kaynak yerine çok sayıda dağıtılmış kaynaktan hedef sunucu üzerine gerçekleştirilir. Daha önceden başka bir saldırıyla ele geçirilmiş ve zombi olarak adlandırılabilen bilgisayarlar hedef sunucuya sürekli istek göndererek DDoS saldırılarının gerçekleşmesinde pay sahibi olurlar.

28 Şubat 2018 tarihinde **GitHub** şirketine yapılan **1.35 Tbps**'lik DDoS saldırısı o ana kadar gerçekleştirilen en büyük siber saldırı olarak tarihte yerini almıştır. Saldırı için yanlış yapılandırılmış **Memcache** sunucuları kullanılmıştır.

Aşağıda çeşitli saldırıların isimleri verilmiştir. İlgili kavramın İnternet üzerinden öğrenciler tarafından araştırılmasını sağlayınız. Her bir saldırı türünün sağ tarafına açıklaması öğrenci tarafından araştırılarak yazılacaktır.

Saldırı türü	Açıklama
Man-in-the-Middle (MitM) – Aradaki adam saldırısı	
ARP Poisoning (ARP Zehirlenmesi)	
DNS Spoofing (DNS Önbellek Zehirlenmesi, Aldatma)	
Port Çalma (Port Stealing)	
STP Mangling	

2. UYGULA

Eğitmen aşağıda yer alan farklı uygulamaları öğrencilerine yaptırır ve analiz etmelerine yardımcı olur.

2.1. AĞ TRAFİĞİ İZLEME UYGULAMASI

Beyaz şapkalı korsanların (etik hacker) en çok tercih ettikleri araçlar:

- Metasploit
- Nmap
- SQLMap
- Wireshark
- OpenVAS
- Nikto
- IronWASP
- SQLNinja
- Maltego

Ağ trafiğini izlemek için birçok program mevcuttur. Bu programlar arasında en çok kullanılan ve Kali Linux ile birlikte kurulu gelen Wireshark programını uygulama amaçlı kullanabilirsiniz. Bu yazılım ile ağ trafiği dinlenmekte ve dinlenen trafikle birlikte ağdaki bilgilere ulaşabilmek mümkün olmaktadır.

Bulunduğunuz yerde ağın trafiğini izlemek için eğitmenler tarafından öğrencilere aşağıdaki uygulama adımları sırasıyla uygulatılır:

1. Kali Linux üzerinde terminali (konsol) açın.

2. Terminal içinde wireshark yazarak enter tuşuna bastığınızda program çalışmaya başlayacaktır.
3. Ekrana bir uyarı penceresi gelebilir. Bu pencerenin herhangi bir önemi yoktur. Eğer böyle bir uyarı penceresi gelirse Ok butonuna basın.
4. Karşınıza gelen arabirimlerden Kali'nin kullandığı eth0 arabirimine çift tıklayarak seçin.
5. Bu aşamadan sonra eth0 dinlenmeye başlanmıştır.
6. Şimdi ağ üzerinde bazı işlemler gerçekleştiriniz. Konsol ekranına tekrar dönerek çeşitli adreslere ping atın. Örneğin ping 8.8.8.8 gibi.

EĞİTMENE NOT

Bir bilgisayarın başka bir bilgisayar ya da adresle arasındaki bağlantı durumunu kontrol etmek ping atmak olarak adlandırılır. Kendi bilgisayarınızın Ethernet kartının sorunsuz çalıştığını test etmek için cmd ekranında komut satırına **ping localhost** yazıp enter tuşuna basın. Eğer olumlu bir cevap dönerse Ethernet kartı sorunsuz çalışıyor anlamı taşımaktadır.

7. Konsol ile wireshark penceresini aynı anda ekranda görmeye çalışın. Ping atıldığı anda arka tarafta çalışan wireshark uygulamasında da yapılan işlemlerin takip edildiği görülecektir.
8. Terminal içinde firefox yazıp enter tuşuna basarak tarayıcıyı açın.
9. Tarayıcıda adres satırına http://www.gazi.edu.tr yazarak enter tuşuna basın, Gazi Üniversitesi web sayfası ekrana gelsin. Ardından tarayıcıyı tamamen kapatın.
10. Wireshark ekranına geri dönün. Programı tam ekran yaparak inceleyin. Şu ana kadar yaptığınız bütün işlemler, istekler ve komutlar izlenmeye başlanmıştır. Yakalanan paketlerle ilgili olarak attığınız ping işlemini gösteren ICMP paketlerini, web sayfasına bağlanırken kullanılan DNS, TCP ve HTTP protokollerini ekranda görebilirsiniz. Açıklama kısımlarını da detaylı inceleyebilirsiniz. Örneğin program içindeki en sağ kısım olan açıklamada görülecek olan "200 ok" web sayfasının ekrana sorunsuz bir biçimde geldiğini göstermektedir.
11. Her bir işlemi detaylı incelemek için program içindeki herhangi bir satıra tıklayın. Tıkladığınız işleme ilişkin bilgiler program penceresinin aşağı kısmında detaylı bilgileri içermektedir. Bu bilgileri de inceleyebilirsiniz.

12. Bu şekilde her yeni yaptığınız işleme ait ağın izleme durumunu wireshark programı üzerinden takip edebilirsiniz.

2.2. WHOIS İLE SORGU YAPMA UYGULAMASI

Whois satın alınan ya da kaydedilen alan adı bilgilerinin kime ait olduğu bilgisini sunan hizmettir. Bir alanın kime ait olduğunu kontrol etmek için whois hizmetini kullanabilirsiniz. Whois sorgulaması ile alan adının kime ait olduğunu, hangi firma tarafından kayıt altına alındığını, alanın ne zaman tescil edilip ne zaman sona ereceği vb. bilgileri sunmaktadır. Alan adı tescili yapan firmalar bütün bu teknik bilgileri alan adını satın alan kişiye düzenleme ve gizleme gibi haklar vermektedir. Yani kişiler bu bilgilerini alan adı hizmetinden yararlandıkları firmaların kendilerine sundukları araçları kullanarak güncelleme imkânına sahiptir.

Eğitmen aşağıdaki adımları öğrencilerine uygulatır:

1. Bilgisayarda kullandığınız web tarayıcıyı çalıştırın.
2. Google içerisinde Whois sorgulama yazabileceğiniz gibi herhangi bir hizmet sağlayıcının adresini de adres çubuğuna yazabilirsiniz. Örneğin www.turhost.com gibi.
3. İlgili firmanın ne olduğunun herhangi bir önemi yoktur. Karşınıza gelen sayfada domain seçeneğinin altında “whois sorgulama” seçeneğini seçin.
4. Karşınıza gelen ekranda sorgulamak istediğiniz alan adını yazın ve sorgula butonuna tıklayın. Örneğin celebiuluyol.com yazarak sorgula butonuna basın.
5. Karşınıza arama yaptığınız alan adı ile ilgili olarak çeşitli bilgiler gelmiştir. Bu bilgilerin tümünü ekrana getirerek detaylı olarak inceleyin.

3. TASARLA VE ÜRET

Bu kısımda öğrencilere tasarla ve üret etkinliği kapsamında aşağıda belirtilen DDoS saldırı yarışması açıklanmaktadır. Eğitmenin bu kısımda öğrencilere açıklaması gereken önemli bir husus etik kavramıdır. Aşağıda kısaca değinilen etik kavramını öğrencilerinize açıklayınız.

Etik kökeni Yunanca’ya dayanan bir kavram olup kişilik, karakter anlamına gelmektedir. Etik tüm toplumlar tarafından kabul edilmiş evrensel bir kavramdır. Dolayısıyla etik iyi, doğru, adalet, değer, erdem ve vicdan gibi kavramları temel alır.

Bilişim teknolojilerinin de doğru bir şekilde kullanımı için Uluslararası Bilgisayar Etik Enstitüsü tarafından uyulması gereken kurallar sıralanmıştır. Bu kurallar şu şekilde özetlenebilir. Eğitmen öğrencilerine siber güvenlik ile ilgili uygulamalar geliştirirken aşağıda sıralanan etik unsurları unutmamaları gerektiğini mutlaka hatırlatmalıdır.

- Bilişim teknolojileri başkalarına zarar vermek için kullanılmaz.
- Başka bir kişiye ait verileri incelememek gerekir.
- Başkalarının oluşturduğu çalışmaları karıştırmamak gerekmektedir.
- Bilişim teknolojileri hırsızlık yapmak için kullanılmaz.
- Bilişim teknolojileri yalancı şahitlik yapmak için kullanılmaz.
- Lisanssız, kopya ya da kırılmış yazılımları kullanmamak gerekir.
- Başka birisi tarafından bilişim teknolojileri ile oluşturulmuş çalışmaları kendinize mal edemezsiniz.
- Yazdığınız kod, program ya da yazılımların/sistemlerin sonuçlarını göz önüne almak zorundasınız.
- Bilişim teknolojilerini kullanırken diğer insanlara saygı duyarak kullanmak gerekir.

3.1. DDOS SALDIRISI YARIŞMASI

Bu etkinlik için 60 dakikalık bir zaman dilimi yeterli olacaktır. Eğitmen etkinliği öğrencilerin bireysel olarak ya da 2-3 kişilik gruplar halinde işbirliği içerisinde çalışmalarını sağlayabilir.

Eğitmen öğrencilerine aşağıdaki Youtube kanallarından ilgili videoları bireysel olarak izlemelerini ister. Bu videoları izlemek için 15 dakika yeterlidir. Öğrenciler tekrar tekrar videoları izleyebilirler.

- https://www.youtube.com/watch?v=3uZABZnc2IU
- https://www.youtube.com/watch?v=p-VnVAZkLvs&t=31s
- https://www.youtube.com/watch?v=J2rS6gKo95M

Bu web adreslerinde bir DDoS saldırısının nasıl gerçekleştirilebileceği ile ilgili detaylı anlatımlar mevcuttur. Bu anlatımların dışında da onlarca farklı araç ya da anlatım videosu mevcuttur. Ancak öğrencilerin basit bir DDoS işlemi yapım aşamalarını bu videolardan öğrenmeleri oldukça kolaydır.

Eğitmen videoların izlenmesinin ardından şu kılavuzu öğrencilerle paylaşır:

- 30 dakikalık süre içerisinde her bir öğrenci kendi bilgisayarında DDoS saldırısı gerçekleştirecektir. Bu işlemi doğru ve hızlı yapan kişiye ise 30 dakika sonunda anlatım ve sunum için 5 dakika bir süre verilecektir.

Eğitmen DDoS saldırısını başarıyla gerçekleştiren öğrencileri izler ve yönlendirmelerini yapar. Başarıyla tamamlayan öğrencilerin isimlerini ajandasına not eder. Daha sonra bu öğrencilerden doğru ve hızlı yapan bir kişi ya da grubu anlatım için sahneye davet ederek sunumu diğer arkadaşlarına yaptırır. Anlatımla birlikte 10 dakika soru-cevap ve tartışma ortamı sağlanmış olur.

Eğitmen tarafından öğrencilere sorulması gereken sorulardan birisi şudur: Peki bu saldırılara karşı firmalar, şirketler, kurum ya da kuruluşlar hangi önlemleri alıyorlar ki DoS ya da DDoS saldırılarına kalkan olunmaktadır? Öğrencilere beyin fırtınası yaptırılarak onların fikirleri alınır. Neticede cevap olarak eğitmenin vurgulaması gereken husus firewall adı verilen güvenlik duvarı yazılım ve donanımlarının saldırıları engellemede önemli olduğu, ancak güvenlik duvarlarının DDoS saldırılarına karşı yetersiz kalabildiğidir.

4. DEĞERLENDİR

Bu bölümdeki yarışma ve uygulamalarda her bir gruba ya da kişiye aşağıdaki sorular eğitmen tarafından sorulabilir:

- Bir kurumda bilgi işlem birimlerinin görevlerinin neler olduğunu biliyor musunuz?
- Bir kurumda bilgi işlem birimindeki yetkili kişiler kendi kurumlarının ağını her zaman izlemek zorunda mıdır? Neden izlemek gerekmektedir?
- Bir kurum kendi ağının analizini yapmalı mıdır? Neden ağ analizini yapmak zorundadır?
- Son dönemde hangi siber saldırıları duydunuz? Bu saldırılar hangi tip saldırılara örnek olarak verilebilir?
- 2021 yılı Mart ayında Yemeksepeti isimli firmaya yapılan siber saldırıyı duydunuz mu? (Eğitmen bu saldırıyı öğrencilerin detaylı arayarak saldırı hakkında bilgi sahibi olmalarını sağlayabilir).

Her gruptan ya da kişiden olmasa bile öğrencilerden süreç içinde kendileri için önemli veya ilginç buldukları hususları arkadaşlarına aktarmaları istenir.

Tüm tartışmaların ardından bu bölümde öğrenilenlerin gelecekte kullanımına yönelik öneriler üzerine beyin fırtınası yapılabilir. Örneğin eğitmen DoS ve DDoS saldırıları ile ilgili olarak meydana gelebilecek zararlar ile ilgili öğrencilerin görüşlerini alabilir. Böylelikle saldırılara karşı yetişmiş personelin alması gereken önlemlerin önemi anlaşılmış olur.

5. EK ETKİNLİK

Kali Linux üzerinde port taraması yapmak için çeşitli programlar hazır olarak gelmektedir: zenmap ve nmap programları gibi. Eğitmen bu programları kullanarak öğrencilerine port taraması uygulamalarını yaptırabilir. Aşağıda zenmap etkinliği anlatılmaktadır.

Zenmap etkinliği:

1. Kali Linux terminal içinde *zenmap* yazıp enter tuşuna basarak programı çalıştır.
2. Program ekranında *target (hedef)* kısmına IP adresi yazmak gereklidir. Hangi IP adresinin çalışıp çalışmadığını terminal ekranından *ping* atarak öğrenebilirsiniz. Örneğin *ping celebiuluyol.com* yazdığınızda cevap geliyorsa o web sitesi çalışır durumda ve size yanıt veriyordur.
3. Ping attığınızda ilgili sitenin IP adresi terminal ekranında çıkacaktır. Oradan kopyala yaparak program içerisinde target kısmına yapıştırın.
4. IP adresini yapıştırdıktan sonra hemen sağ tarafta “profile” aşağı açılır kutusu görünecektir. Bu kısım taramanın nasıl olacağı ile ilgilidir. Tüm TCP portlarını tara, akıllı tarama, hızlı tarama vb. seçenekler burada mevcuttur. *Quick scan* hızlı tarama seçeneğini seçin.
5. *Scan* düğmesine tıklayın.
6. Tarama işlemi için kısa bir süre bekleyin.
7. Ekranda arama sonucunda taranan portlara ilişkin çeşitli bilgiler yer almaktadır. Ekranda gördüğünüz yeşil portlar o portun aktif, sarılar ise aktif olmadığını göstermektedir.
8. İlgili ekranda port sütununda port numaraları, state sütununda açık veya filtreli kapalı olma durumları, service sütununda ise ftp, domain, http, pop3 vb. gibi hizmetin adı görünmektedir.
9. *Ports/hosts* düğmesine tıklayın. Ekranda açık ve kapalı portlar listelenecektir. Herhangi bir sızma girişiminde bulunmak istenen bilgisayara ait bu bilgilerin önceden bilinmesinde veya kontrol edilmesinde yarar vardır.

10. *Host details* düğmesine tıklandığında ise bu sunucuya ait portlarla ilgili istatistiksel bilgiler görülebilir, örneğin toplam kaç portun açık veya kaç tanesinin kapalı olduğu gibi.
11. Detaylı incelemelerin ardından programı kapatabilirsiniz.

KAYNAKLAR

Çakır, H., & Yaşar, H. (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3*(2), 488-507.

Doğan, D. (2021). *Siber güvenlik açısından siber saldırı senaryolarının incelenmesi* (Master's thesis, Maltepe Üniversitesi, Lisansüstü Eğitim Enstitüsü).

Kekül, H., Ergen, B., & Arslan, H. (2021). Yazılım Güvenlik Açığı Veri Tabanları. *Avrupa Bilim ve Teknoloji Dergisi*, (28), 1008-1012.

HAFTA 7. WEB SALDIRILARI VE SAVUNMA

ÖN BİLGİ

- Temel güvenlik kavramları
- Veritabanı yönetim sistemleri temel kavramlar
- SQL Sorgulama dili komut yapısı
- Ağ saldırı çeşitleri

AMAÇ

Bu bölümün amacı, öğrencileri bir web saldırısı hakkında bilgi sahibi yapmaktır. Özellikle SQL enjeksiyonu (SQL injection) olarak bilinen ve günümüzde sıklıkla kullanılan web saldırısı ile ilgili mekanizma ve işlem basamaklarını öğrenmelerini sağlamaktır. Bölüm içerisinde web saldırıları ile genel açıklamalar yapılmakta, web saldırı türlerine çeşitli örnekler verilmekte ve SQL enjeksiyon saldırıları detaylı anlatılmaktadır. Ayrıca çeşitli web saldırıları ile ilgili olarak öğrencilerin farklı uygulamaları yapmaları sağlanmaktadır.

BÖLÜM KAZANIMLARI

Bu bölümü tamamlayan bir öğrenci,

- Web saldırıları çeşitlerini açıklar.
- Bir web sitesindeki açıklıkları tespit edecek işlem adımlarını uygular.
- SQL enjeksiyonu saldırısı işlem basamaklarını analiz eder.
- SQL enjeksiyonu saldırısı uygular.
- SQL enjeksiyonu saldırısı korunma yollarını sayar.
- Güvenlik açıklarını tespit ederek savunma mekanizmalarını uygular.

KULLANILACAK MATERYAL VE ARAÇLAR

Bilgisayar, İnternet, İnternet tarayıcı programı, MS Access, kâğıt, kalem

HAFTANIN İŞLENİŞİ

Gözle ve Uygula	Siber saldırı haritalarını gözlemleme, Türkiye'ye yapılan saldırı girişimlerini görme, MS Access tablo oluşturma, SQL sorgularını uygulama, sorgu çalıştırarak sonucu görme, örnek bir siteden saldırı analizi
Uygula	Çeşitli tablolar oluşturma be bu tablolar üzerinde farklı SQL sorgularını çalıştırma
Tasarla ve Üret	Adım adım SQL enjeksiyon saldırı girişimi
Değerlendir	Haftanın içeriğinin değerlendirilmesi ve çalışmanın devam ettirilmesine yönelik öneriler

1. GÖZLE VE UYGULA

Bu bölümde web saldırıları ile ilgili çeşitli kavramlar tanıtılarak derinlemesine bir tartışma sağlanacaktır.

1.1. SALDIRILAR VE WEB SALDIRILARI

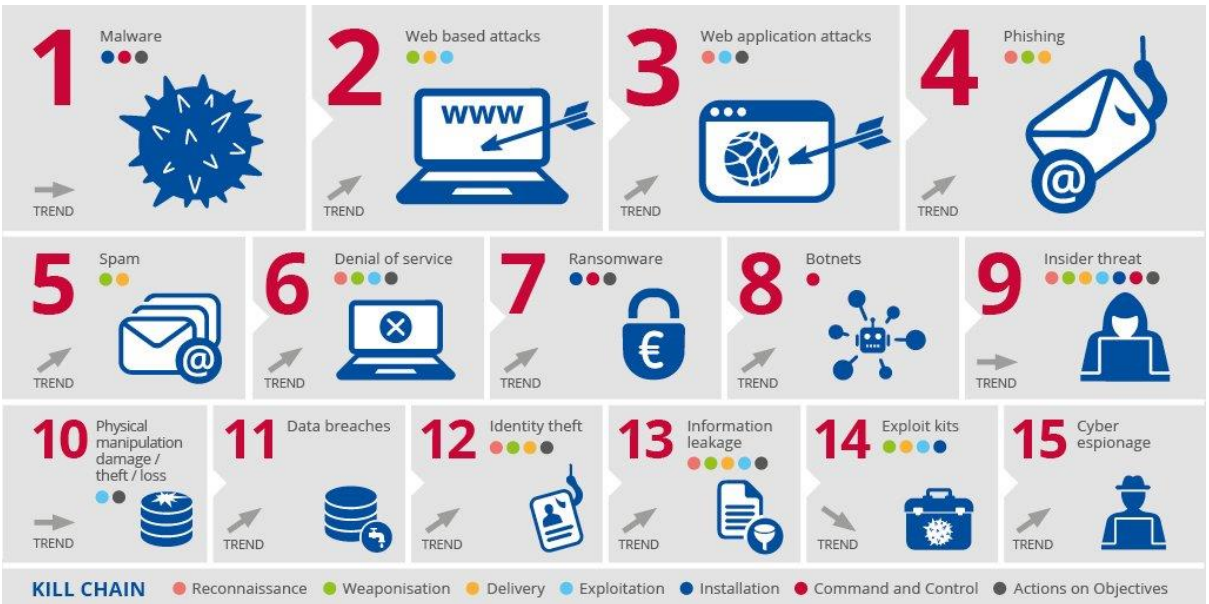
Eğitmen öğrencilerinin web saldırıları ile ilgili tartışmalarını sağlar. Bunun için öğrencilerine çeşitli sorular sorarak onların cevabını alır ve ardından web saldırıları ve saldırı çeşitleri ile ilgili olarak detaylı açıklamalarını yapar. Bütün bu işlemler için 35-40 dakikalık bir zaman ayırmak yeterlidir.

- Hacker ne iş yapar?
- Beyaz şapkalı hacker ne demektir?
- Çalışan bir web sitesinde hangi bilgilere ulaşabiliriz?
- Bir web sitesinin yönetici paneli (admin) paneli ne işimize yarar? Bu panel ile yetkili kullanıcı hangi işlemleri gerçekleştirebilir?
- Bir web sitesinin veritabanına ulaşırsak hangi bilgileri elde edebiliriz?

- Bugüne kadar bir web sitesinin arka planında ne olduğu hakkında bilgi sahibi olmak isteyen var mı?
- Bugüne kadar bir web sitesine ya da ağa sızma girişiminde bulunan oldu mu?
- Bir web sitesine ya da bir ağa sızmada başarılı olursak neler yapabiliriz?

Eğitmen sadece bu soruları sorarak kendisini sınırlandırmak zorunda değildir. Gelen cevaplarla birlikte öğrencilerden de yeni sorular ortaya çıkabilir. Bunlara benzer sorular çerçevesinde tartışma yönetilerek öğrencilerin fikirlerini beyan etmesi sağlanır. Gerçek yaşam içinde öğrencilerin fikirleri ile birlikte web saldırılarının ne kadar önemli olduğu sonucuna hep birlikte varılır. Günlük yaşamdaki web saldırıları neticesinde ortaya çıkacak durumlardan yola çıkarak web saldırılarına karşı savunma mekanizmalarının önemine de vurgu yapılır.

Avrupa Birliği Siber Güvenlik Ajansı'nın (ENISA) 2018 yılı itibariyle ortaya koyduğu "Threat Landscape report 2017" sonuçlarına göre web saldırıları, en üst sıralarda yer almaktadır.



(Resim kaynak: https://twitter.com/enisa_eu/status/1044952815515435011, Erişim tarihi: 14.11.2021)

EĞİTMENE NOT

Siber saldırı haritalarını öğrencilere canlı olarak tarayıcı programda açıp gösteriniz. Siber saldırı haritaları için kullanılacak web sitesi adresleri:

1. https://www.imperva.com/cyber-threat-attack-map/
2. https://threatmap.checkpoint.com/
3. https://www.fireeye.com/cyber-map/threat-map.html
4. https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18763&view=map

Eğitmen ekrana getirdiği canlı siber saldırı haritaları üzerinden öğrencilere açıklamalarını yapar. Ekranda ülkeler arası yaşanan siber saldırı durumları canlı olarak takip edilebilir. Eğitmen saldırının kaynağı olan ülkeler, saldırının hedefi olan ülkeler, en çok kullanılan saldırı tipleri ve saldırıdan en çok etkilenen sektörler ile ilgili öğrencilere bilgi verir.

Uygulama 1:

Eğitmen aşağıdaki işlem basamaklarını öğrencilerin uygulamasına imkân verir. Her bir öğrenci oturduğu bilgisayardan aşağıdaki işlemleri yerine getirir:

1. *https://cybermap.kaspersky.com/tr* adresini açar.
2. Siber tehdit haritasından Türkiye seçili gelmektedir. Eğer değilse *TR butonuna* tıklayarak ülkemizin maruz kaldığı tehdit haritasını açar.
3. Eğitmen öğrencilerin sayfanın üst kısmından "Veri Kaynakları" bölümüne giderek şu kötü amaçlı yazılım ya da saldırı girişimlerinin anlamını okumaları için öğrencilere 10 dakika süre verir: OAS - On-Access Scan, ODS - On Demand Scanner, MAV - Mail Anti-Virus, IDS - Intrusion Detection Scan, WAV - Web Anti-Virus, VUL - Vulnerability Scan
4. Eğitmen Türkiye'nin en çok saldırılan kaçıncı ülke olduğunu öğrencilere sorar (Öğrencilere Harita bölümüne dönerek dünya haritasında ilgili ülkenin üzerine gelip fare ile tıklamasını söyleyebilirsiniz).
5. Eğitmen Rusya'nın en çok saldırılan kaçıncı ülke olduğunu öğrencilere sorar.
6. Eğitmen Kanada'nın en çok saldırılan kaçıncı ülke olduğunu öğrencilere sorar.
7. Eğitmen Amerika Birleşik Devletleri'nin en çok saldırılan kaçıncı ülke olduğunu öğrencilere sorar.

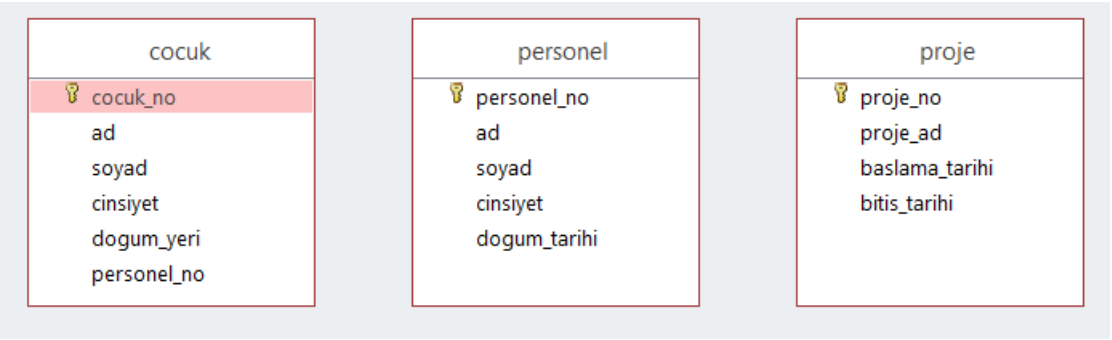
8. Eğitmen Çin'in en çok saldırılan kaçıncı ülke olduğunu öğrencilere sorar.
9. Eğitmen, dersi anlattığı gün en büyük enfeksiyon etkisi altında olan ilk beş ülkeyi öğrencilerine sorar (Ekranda sol üstte İstatistik linkinde tüm detaylara ulaşmak mümkündür).
10. Eğitmen geçen hafta itibariyle dünya çapında OAS - On-Access Scan, ODS - On Demand Scanner, MAV - Mail Anti-Virus, IDS - Intrusion Detection Scan, WAV - Web Anti-Virus, VUL - Vulnerability Scan saldırılarından etkilenen ilk 20 ülkeyi öğrencilerinin incelemesini ister. Genel durumla ilgili öğrencilerden birkaçına söz hakkı vererek öğrencilerin saldırı girişimleri ile ilgili olarak yorum yapıp analiz etmelerini sağlar.
11. Eğitmen Türkiye'ye yapılan OAS - On-Access Scan, ODS - On Demand Scanner, MAV - Mail Anti-Virus, IDS - Intrusion Detection Scan, WAV - Web Anti-Virus, VUL - Vulnerability Scan saldırıların istatistiklerini öğrencilerin detaylı olarak incelemelerini ister. Öğrencilere ülkemize en çok hangi saldırıların yapıldığı ve bu saldırıların toplam sayısının ne olduğu sorularını yöneltir.

Yukarıda yer alan uygulamanın ardından eğitmen genel bir değerlendirme yaparak, saldırı çeşitlerinden, saldırıların anlık olduğundan, saldırılara karşı savunma mekanizmalarının önemi vb. bahsedebilir.

Görüldüğü üzere birçok saldırı çeşidinden söz etmek mümkündür. Bu saldırıları daraltarak öğrencilere bir uzmanlık kazandırma ihtiyacı vardır. Dolayısıyla bu bölümde web saldırılarından SQL enjeksiyonu ve XSS saldırıları açıklanacak, ardından ise SQL enjeksiyonu saldırıları ile ilgili çeşitli uygulamalar gerçekleştirilecektir.

1.2. SQL ENJEKSİYON SALDIRILARI

SQL enjeksiyon saldırılarının amacı bir web uygulamasının veritabanına ulaşarak veritabanındaki her türlü bilgiyi görüntülemek, kopyalamak, değiştirmek ve güncellemeye izin vermektir (Çınar & Bilge, 2016). Bir web sitesinin veritabanı yetkili kişi tarafından yönetilmektedir. Bu kişi kurum içerisinde kendisine hak ve rol tanımlanan bir bilgi işlem çalışanı olabilir. SQL enjeksiyon saldırı yapan kişi bu yetkili dışında hakkı olmadığı halde veritabanına girme teşebbüsünde bulunarak tüm kayıtları ele geçirebilir. Şekil 1'de bir örnek bir veritabanı ve veritabanındaki tablolar gösterilmektedir.



Şekil 1. Veritabanı örneği

Şekil 1'de bir veritabanı örneği görülmektedir. Bu veritabanında üç adet tablo bulunmaktadır. Tablo isimleri ise cocuk, personel, proje şeklindedir.

EĞİTMENE NOT

Şekil 1'de yer alan tablolardan cocuk isimli tabloyu tahtaya çiziniz ve gerekli açıklamaları tahtada çizerek anlatınız.

cocuk tablosunun altında çocuk_no, ad, soyad, cinsiyet, dogum_yeri, personel_no o tabloda yer alan alanları göstermektedir. Bu alanlar veri girilecek olan sütunların başlıkları olarak düşünülebilir.

Verilerin tablolarda nasıl tutulduğuna yönelik örnek bir ekran görüntüsü Şekil 2'de görülmektedir.

cocuk_no	ad	soyad	cinsiyet	dogum_yeri	personel_no	*Eklemek İçin Tıklatın*
1	Tuna	Uluyol	Erkek	Çankaya	3	
2	Zeynep	Demirci	Kadın	İstanbul	105	
Yeni						

Şekil 2. Veritabanındaki bir tabloda saklanan verilerin görünümü

EĞİTMENE NOT

Şekil 2'de yer alan örnek verilerin olduğu tabloyu tahtaya çiziniz ve gerekli açıklamaları tahtada çizerek anlatınız.

Eğitmen tahtaya çizdiği bu tabloda iki adet kayıt bulunduğunu öğrencilerine açıklar. Ardından Türkiye'de faaliyet gösteren bir bankayı örnek vererek bu bankanın 5 milyon müşterisi bulunduğunu söyler. Müşterilere ait hangi verilerin veritabanında tutulabileceği ile ilgili olarak

öğrencilere söz hakkı vererek onların cevaplarını alır. Eğitmen, bu şekilde veritabanında birçok tablo ve bu tablolarda birçok kaydın bulunabileceği ile ilgili bir beyin fırtınası gerçekleştirebilir.

Uygulama 2:

1. Eğitmen 10 dakika süre vererek öğrencilerin https://support.microsoft.com/tr-tr/office/tablolara-giri%C5%9F-78ff21ea-2f76-4fb0-8af6-c318d1ee0ea7 adresindeki (Microsoft resmi web sitesi) açıklamaları okumalarını sağlar. Bu bağlantıda Tablolara Giriş konusu basit biçimde anlatılmış ve önemli terimler özetlenmiştir.
2. Eğitmen her bir öğrenciden kâğıt ve kalem ile en az 5 alandan oluşan, bir alanın birincil anahtar olarak belirlendiği bir tabloyu tasarlamalarını ister. Bunun için öğrencilere 5 dakikalık bir süre verilebilir.
3. Eğitmen istekli öğrencilerden seçim yapmak koşuluyla, örnek tabloları tahtaya yazdırarak bu tabloların açıklamalarını sınıfa öğrenciyle birlikte yapabilir.

Uygulama 3:

1. Uygulama 2'de kâğıt üzerinde tasarlanan tablo ya da tabloların bilgisayar ortamında yapılmasını sağlayınız.
2. Eğitmen bu işlem için öğrencilerin bilgisayarda yüklü olan MS Access programını çalıştırarak bu işlemi yapmalarını sağlar.
3. Eğitmen tablo tasarımını doğru bir şekilde yapan öğrencilerden tabloya 2 kayıt girmelerini ister.
4. MS Access ekran görüntüsü yansıtılarak öğrencilerle birlikte tartışmalar gerçekleştirilir.

EĞİTMENE NOT

Öğrenciler "Tablo oluşturma ve Alan ekleme" ile ilgili olarak https://support.microsoft.com/tr-tr/office/tablo-olu%C5%9Fturma-ve-alan-ekleme-8fdc65f9-8d40-4ff5-9212-80e6545e8d87#bmaddfield adresini detaylı inceleyebilirler.

Buraya kadar öğrenciler veritabanı ve tablo yapısının mantığını kavramış ve uygulamış oldular. Bu aşamadan sonra binlerce kayıt içerisinden sorgulama yaparak bir bilgiyi filtrelemenin önemini anlatmak gerekmektedir. Bunun için de kullanılan temel dil SQL olarak adlandırılır. Bu kısımda SQL dilinin tüm komutlarını değil sadece belli temel komutları anlatarak, öğrencilerin SQL dilinin yapısını anlamasını sağlayınız.

SQL Temel Kullanım

Bir SQL sorgusunun genel olarak doğru yazımı şu şekildedir:

Select *ad* FROM *personel* WHERE *id*=1;

Bu sorgu, personel isimli tablodan id değeri 1 olan üyenin ad bilgisini çekecektir. Dolayısıyla komutun genel kullanım şekli şu şekilde olacaktır:

Select sütun_adı1, sütun_adı2, ... FROM tablo_adı

INSERT INTO komutu tablo içerisine yeni bir kayıt eklemek için kullanılır. Kullanımı şu şekildedir:

INSERT INTO tablo_adı (sütun_adı1, sütun_adı2, ...) VALUES (deger1, deger2, ...)

Aşağıda yer alan komut personel tablosunun adi alanına Çelebi, Soyadi alanına ise Uluyol isimli yeni bir kayıt ekler.

INSERT INTO personel (Adi, Soyadi) VALUES ('Çelebi', 'Uluyol’)

UPDATE komutu bir tablonun bir kaydını değiştirmek ya da güncellemek için kullanılır.

UPDATE tablo_adı SET sütun_adı1=deger1, sütun_adı2=deger2, ... WHERE sütun_adı=deger

Aşağıda yer alan komut Adi Mehmet, Soyadi Demirci olan kaydın Adi Çelebi, Soyadi Uluyol olarak günceller. Komutta WHERE parametresinin kullanımını farklı örneklerle açıklayabilirsiniz. Ayrıca AND parametresi de her iki koşulun birlikte sağlanması anlamına gelmektedir. AND kullanımını da farklı örneklerle açıklayabilirsiniz.

UPDATE personel SET Adi='Çelebi', Soyadi='Uluyol' WHERE Adi='Mehmet' AND Soyadi='Demirci'

DELETE komutu bir tablodaki bir kaydı ya da kayıtları silmek için kullanılır.

DELETE FROM tablo_adı WHERE sütun_adı=değer

Aşağıda yer alan komut Adi Çelebi Soyadi Uluyol olan kaydı personel tablosundan silme işlemini yerine getirir.

DELETE FROM personel WHERE Adi='Çelebi' AND Soyadi='Uluyol'

Uygulama 4:

1. Eğitmen olarak MS Access yazılımında öğrencilerin her birinin bir önceki aşamada bir tablo oluşturup oluşturmadıklarını tekrar kontrol ediniz. Tablo oluşturmayan öğrencilerin yeni bir tablo oluşturmalarını sağlayınız ve tablo ismini *uretici* olarak belirlemelerini isteyiniz.
2. Tabloda şu alanların olmasını isteyiniz: no, ad, soyad, dogum_tarihi, ilce, il
3. Tablolara en az 10 adet kayıt girmelerini sağlayınız. Bazı kayıtların adı ve il bilgisi aynı olabilir.
4. MS Access içinde *Oluştur* sekmesinden *sorgu sihirbazı* ya da *sorgu tasarımı* seçeneklerini kullanarak sorgu yapılabilir.
5. *SELECT* komutu ile il alanına göre sorgulama yaptırınız.
6. *UPDATE* komutu ile ad alanına göre güncelleme yaptırınız.
7. *DELETE* komutu ile soyad alanına göre güncelleme yaptırınız.

EĞİTMENE NOT

Temel SQL komutları söz dizimi kullanımı öğrenciler tarafından anlaşılıp uygulandıktan sonra artık eğitmen olarak SQL enjeksiyon saldırıları anlatımına geçiş yapabilirsiniz.

SQL Enjeksiyon Saldırısı:

SQL enjeksiyon saldırıları veritabanına dayalı uygulamalara saldırı girişimi için kullanılan bir tekniktir. Bu saldırı girişimi için web sitesi ve arka planında çalışan veritabanına sızmak için SQL komutları saldırı için kullanılır. Veritabanına saldıran ya da veritabanına erişen bir kişi tabloları görebilme, tablolarda bulunan alanları okuyabilme, kayıtlara ulaşabilme vb. birçok işlemi yapabilir. Sonuç olarak yetkisi olmadığı halde tüm veritabanındaki bilgileri kendi bilgisayarına indirebilir.

Örnek bir web adresini düşünecek olursak: personel.com

Bu web adresi veritabanında her bir personele tanımlanmış bir kimlik numarası (ID) vardır. Bu bilgiler Şekil 3'tekine benzer bir tabloda tutulduğu gibidir.

Personel Adı	Kimlik numarası (ID)
Çelebi	1
Mehmet	2
Tuna	3
Hatice	4

Şekil 3. Örnek personel tablosu

ID'si 3 olan kişinin web tarayıcıdaki adresi şu şekilde olur:

personel.com/personel.php?id=3

Tarayıcı programın adres çubuğuna dikkatlice bakıldığında, böyle bir ifade eğer adres çubuğunda görüntüleniyorsa, arka planda bir SQL sorgulamasının mevcut olduğu anlaşılabilir. Böyle bir ifadenin SQL sorgulama kodu ise şu şekildedir:

Select * from personel where id=3

Bu SQL sorgusunun anlamı, id'si 3 olan kaydın personel isimli tablodan çekilerek bilgilerinin görüntülenmesidir. Böyle bir sorguda cevabın hep doğru olarak geri döndürülmesi için kod üzerinde oynama yapabiliriz. Yaptığımız manipülasyon neticesinde kod her zaman doğru sonucu verecektir. Çünkü sıfır her zaman sıfıra eşit olacaktır:

SELECT ad FROM personel WHERE id=3'%' or '0'='0'

Her zaman doğru döndürecek yukarıdaki ifadenin yanına ekleyeceğimiz yeni kod blokları ile artık saldırı girişimlerinde bulunmak mümkün olmaktadır.

Genellikle herhangi bir yorum, forum vb. sayfa içerisinde kullanıcılardan gelen komutlar POST metodu denilen yöntemle gönderilmektedir. Bu metotla birlikte tarayıcı içerisinde sayfa adresinde parametreler gizlenerek kullanıcıya gösterilmemektedir. Böyle durumlarda ise sayfanın kaynak koduna bakarak gerekli inceleme ve analizler yapılabilir. Yapılacak olan kod incelemesinde form ile başlayan kodları incelemek gerekmektedir. Form komutları arasındaki parametrelere özellikle odaklanmak gereklidir. Örneğin;

< form method="post" action="ana/deneme.asp">
< input type="hidden" name="X" value="Z" />
< form>

Uygulama 5:

1. Eğitmen olarak öğrencilerin her birinin İnternet tarayıcısı ile *http://testphp.vulnweb.com/index.php* adresine girmelerini sağlayınız.
2. Öğrencilerin *home, categories, artists, …* gibi linklere tıklayarak sayfada dolaşmalarını sağlayınız.
3. Linklere tıklayarak dolaşan öğrencilerin *"http://testphp.vulnweb.com/listproducts.php?cat=1"* benzeri bir yapıyı görmelerini sağlayınız. Burada öğrencilerin görmesi gereken üst kısımlarda anlatıldığı üzere *"listproducts.php?cat=1"* benzeri bir yapı yakalamalarıdır.
4. *Categories* linki altında, *posters, paintings, stickers, graffity* linklerine tıklayan öğrencilerin İnternet tarayıcısının adres çubuğunda gördükleri adresleri analiz etmelerini isteyiniz.
5. Farklı linklere tıklayan öğrencilerin İnternet tarayıcısı adres çubuğunda gördükleri adres yapısını açıklamalarını isteyiniz.

1.3. XSS SALDIRILARI

XSS (Cross Site Scripting) bir web sayfasına script kodları ile saldırı yapılması anlamına gelmektedir. Saldırı için web uygulamaları içerisinde yer alan güvenlik açıklıkları tespit edilip kullanılmaktadır. Günümüzde web sitelerine bağlanan bireyler olarak bu saldırılar hakkında fikir sahibi olmak oldukça önemlidir. XSS saldırılarında çoğunlukla Javascript ve HTML dilleri kullanılmaktadır.

XSS saldırılarına maruz kalma durumu farklı biçimlerde ortaya çıkabilir. Reklam pencereleri açan web siteleri, toplu biçimde gönderilen e-postalar, e-posta içerisine gömülmüş olan linkler, kişiler bilgiler isteyen formlar ve kötü amaçlı komut dosyaları gibi yöntemler XSS saldırı amacıyla kullanılabilir.

XSS saldırıları, Reflected, Stored/Persistent ve DOM olmak üzere üç farklı biçimde sınıflandırılabilir. XSS saldırılarından en basiti Reflected olarak adlandırılan saldırı türüdür. HTTP veri isteğinde bulunulduğunda güvenli olmayan biçimde cevabın içerisine veriler yerleştirilir. Stored XSS, güvenilmeyen bir kaynaktan veri alındığında ortaya çıkmaktadır. DOM tabanlı XSS ise güvenilmeyen bir kaynaktan güvenilmeyen bir biçimde işleyen ve genellikle Javascript içeren uygulamalarda ortaya çıkmaktadır.

XSS saldırılarına karşı filtreleme, kara liste veya beyaz liste oluşturma gibi çeşitli yöntemlerle önlem alınabilemektedir. Filtreleme yöntemi ile sahte olarak gönderilen ya da bir form içerisinden yollanan karakterler tanınarak önlem alınabilemektedir. Beyaz liste ile izin verilen girişler sisteme girmekte, kara liste yöntemi ile de izin verilmeyen unsurların sisteme girişi engellenmektedir. Çerezleri daha güvenli hale getirme ve kullanıcının kendisine gönderilen her bağlantıya tıklamaması için farkındalığının artırılması da bu saldırılara karşı alınabilecek önlemlerden birkaçıdır.

Bu bölümün sonunda "Ek Etkinlik 2" olarak örnek bir XSS saldırısının incelemesine yer verilmiştir.

2. UYGULA

Eğitmen aşağıda yer alan uygulamayı öğrencilerine yaptırır ve analiz etmelerine yardımcı olur. Bu uygulama ile öğrenciler tablo oluşturma ve tablolar üzerinde sorgulama işlemlerini uygulamış olurlar.

2.1. TABLO OLUŞTURMA VE SORGULAMA UYGULAMASI

Eğitmen öğrencilerine veritabanında tablo oluşturma ve tablo üzerinde sorgulama işlemleri ile ilgili uygulama yaptırmak için bilgisayarda yüklü olan MS Access programını kullanır. Öğrenciler istenen tüm işlemleri MS Access programı üzerinde gerçekleştirir.

1. *MS Access* programını çalıştır.
2. Yeni bir veritabanı oluşturulur ve isim vererek kaydetmeleri istenir.
3. Öğrenciler 3 adet tablo oluşturur. Tablo isimleri *cocuk, personel, proje*
4. *cocuk* tablosundaki alanlar: *cocuk_no, ad, soyad, cinsiyet, dogum_yeri, personel_no*
5. *personel* tablosundaki alanlar: *personel_no, ad, soyad, cinsiyet, doğum_tarihi*
6. *proje* tablosundaki alanlar: *proje_no, proje_ad, baslama_tarihi, bitis_tarihi*
7. Her bir tabloya öğrencilerin 5 adet kayıt girmesini sağlayınız.
8. MS Access içinde *Oluştur* sekmesinde *Sorgu Sihirbazı* ya da *Sorgu Tasarımı* seçenekleri ile öğrencilerin sorgular oluşturmalarını sağlayınız.
9. Öğrenciler sorgular içerisinde SQL kodlarından *SELECT, UPDATE ve DELETE* komutlarını kullanarak çeşitli işlemler gerçekleştirsin.
10. Bu sorgulama komutlarını her bir öğrencinin farklı örneklerle tekrar ederek uygulamasını sağlayınız.

3. TASARLA VE ÜRET

Tasarla ve üret bölümünde SQL enjeksiyon saldırı girişimi etkinliği yer almaktadır. Grubun özelliğine göre problem çözülürken öğrencilerin işbirliği içerisinde çalışmalarını teşvik etmek gerekmektedir. Ancak etkinlik bireysel olarak da yapılabilir. Eğitmen bu etkinliği yaptırırken, kitabın başındaki Etik Kılavuzunda ve Hafta 6 Tasarla ve Üret kısmında detaylı olarak açıklanmış olan Uluslararası Bilgisayar Etik Enstitüsü tarafından ortaya konulan etik kuralları öğrencilerine bir kez daha açıklayabilir.

3.1. SQL ENJEKSİYON SALDIRI GİRİŞİMİ

Bu etkinlik için 60 dakikalık bir zaman dilimi yeterli olacaktır. Eğitmen etkinliği öğrencilerin bireysel olarak ya da 2-3 kişilik gruplar halinde işbirliği içerisinde çalışmalarını sağlayabilir. Tasarla ve üret etkinliği Ek 1'de sunulmuştur. Etkinliğin çevrimiçi hali ise https://forms.gle/DPDM11KCmB9RFeuz9 adresinde mevcuttur. Eğitmen etkinliği koşulların durumuna göre ister yüz yüze ister çevrimiçi olarak öğrencileri ile paylaşır. Öğrenciler bu etkinlikte kendilerinden istenen kısımları doldurmakla görevlidir.

http://testphp.vulnweb.com/index.php web sitesi SQL enjeksiyon saldırıları ve eğitimi için kullanılan örnek bir sitedir. Bu sitede herhangi bir güvenlik sorunu bulunmamaktadır, yalnızca eğitim amaçlı oluşturulmuştur. Bütün tasarım ve üretim etkinliği bu web sitesi (URL) üzerinden gerçekleştirilecektir.

Eğitmen SQL enjeksiyon saldırısını başarıyla gerçekleştiren öğrencileri izler ve yönlendirmelerini yapar. Başarıyla tamamlayan öğrencilerin isimlerini ajandasına not eder. Daha sonra bu öğrencilerden doğru ve hızlı yapan bir kişi ya da grubu anlatım için sahneye davet ederek sunumu diğer arkadaşlarına yaptırır. Anlatımla birlikte 10 dakika soru-cevap ve tartışma ortamı sağlanmış olur.

Eğitmen tarafından öğrencilere sorulması gereken sorulardan birisi şudur: Peki bu saldırılara karşı firmalar, şirketler, kurum ya da kuruluşlar hangi önlemleri alıyorlar ki SQL enjeksiyon saldırılarına engel olmaktadır? Öğrencilere beyin fırtınası yaptırılarak onların fikirleri alınır.

4. DEĞERLENDİR

Eğitmen için aşağıda bir uygulama değerlendirme formu tasarlanmıştır. Eğitmen çalışmaları grup olarak ya da öğrencileri bire bir olacak şekilde aşağıdaki formu kullanarak kendi gözlemlerine göre doldurur.

Uygulama değerlendirme formu

Kriterler	**Çok iyi**	**İyi**	**Orta**	**Yetersiz**
Yeni konuları öğrenme çabası				
Gayretli olma becerisi				
Verilen işi tam ve doğru yapma becerisi				
Ayrıntılarda dikkatli ve özenli olması				
Yapamadığında tekrar edebilme				
Verilen talimatları doğru anlama becerisi				
İş birliği içinde çalışma becerisi				
Kendini ifade etme yeteneği				
İşini sevmesi ve isteyerek yapması				
Çalışmaya gönüllü katılımı				
Bildiklerini grup içinde paylaşımı				
Arkadaşlarıyla yardımlaşması				
Görevi zamanında yerine getirmesi				
Diğer görüşlere saygılı olması				
Tartışmalara katılımı				
Grup çalışmasında iş bölümüne katılımı				

Eğitmen öğrencilerine şu soruları sorabilir:

- Günümüzde hangi e-posta hesabını kullanıyorsunuz?
- E-postalara giriş yaparken ilgili web sitesi arka planda bir veritabanı kullanıyor mu?
- Bu veritabanına SQL enjeksiyon saldırısı yapılması mümkünse, ilgili şirketler bunun için nasıl bir savunma mekanizması kullanıyorlar?

Tüm tartışmaların ardından bu bölümde öğrenilenlerin gelecekte kullanımına yönelik öneriler üzerine beyin fırtınası yapılabilir. Örneğin E-ticaret yapılan şirketlere karşı web saldırılarının neden olabileceği hususların önemi vurgulanır. Bu durumda eğitmen tarafından yaşanabilecek maddi kayıplarla ilgili olarak çok uç örnekler verilebilir. Böylelikle saldırılara karşı firmaların ya da kurumların kendi güvenlik mekanizmalarını/önlemlerini almalarının önemi vurgulanmış olur.

Eğitmen değerlendirme formunu kullanarak süreci değerlendirebileceği gibi aşağıdaki formu kullanarak öğrencilerin SQL enjeksiyon saldırılarına karşı bir savunma mekanizması geliştirmelerini isteyebilir.

SQL Enjeksiyon Saldırılarına karşı korunmak için savunma mekanizmalarını İnternet üzerinden araştırınız. En az 5 farklı savunma mekanizmasını maddeler halinde yazınız. Bunun için öğrencilere 15 dakika verilmesi yeterlidir.

1. …….
2. …….
3. …….
4. …….
5. …….

15 dakikalık süre tamamlandıktan sonra beyin fırtınası tekniği ile tüm öğrencilerin fikirleri tartışılır.

5. EK ETKİNLİK

Eğer kullanıcı adı ve şifre ile girilen bir siteye siteyi oluşturan yazılımcılar tarafından zararlı karakterlerin algılanarak filtreleme yapılmaması söz konusu ise bu açıklığa login bypass adı verilmektedir. Tıpkı SQL enjeksiyon saldırısında olduğu gibi veritabanına sızma işlemi gerçekleştirilebilir. Bu tür girişimde temel amaç kullanıcı adı ve şifre yazan metin kutusuna çeşitli komut ya da kodlar yazarak sisteme giriş yapmaktır.

Ek Etkinlik 1:

Eğitmen aşağıdaki uygulamayı öğrencilerin yapmasını sağlar:

1. İnternet tarayıcı programın adres çubuğuna *http://testphp.vulnweb.com/index.php* yazıp Enter tuşuna basın.
2. Sol menüde *signup* linkine tıklayın. Karşınıza kullanıcı adı ve şifre isteyen ekran gelecektir.
3. Kullanıcı adı ve şifre yazan yere şu kodları yazınız (Tek tırnak işareti kullanın): *'OR'1'='1*
4. Sisteme başarılı bir şekilde giriş yaptığınıza dair form ekranı karşınıza gelecektir.
5. Bu şekilde login bypass yöntemi ile sisteme yetkisiz bir biçimde giriş yapılmıştır.

Ek Etkinlik 2:

XSS (Cross Site Scripting), genellikle Javascript gibi script kodları üzerinden bir web sayfasına yapılan saldırıdır. Bu saldırılar tarayıcıda saklanan ve cookie olarak adlandırılan yapılara saldırı amacı taşımaktadırlar. Bu saldırılar ile oturum açma bilgileri ele geçirilebilir ya da cihazlara zararlı yazılımlar gönderilebilir.

1. İnternet tarayıcı programın adres çubuğuna *http://testphp.vulnweb.com/index.php* yazıp Enter tuşuna basın.
2. Açılan sayfada sol tarafta arama kısmı olan *Search* görünecektir. Bu kısma klavyeden deneme yazarak *go* butonuna basın.
3. Eğer ekranda searched for deneme yazıyorsa kullanıcının girdiği kelime sayfa tarafından yorumlanarak çıktı olarak yazılıyor demektir. Bu durum da aslında sayfada girilen kodların da yorumlandığı anlamına gelmektedir. Böyle bir durumda sayfanın XSS'e zaafının olduğu ortaya çıkmaktadır.

4. Sol tarafta arama kısmına şu kodları yazıp çalıştıralım: *<script>window.location='https://www.google.com'</script>*
   Kodların sonucunda ne olduğunu aşağıya yazınız.
   …….
5. Sol tarafta *our guestbook* kısmına şu kodları yazıp çalıştıralım: *<script>window.location='https://www.google.com'</script>*
6. Kodların sonucunda ne olduğunu aşağıya yazınız.
   …….

EK 1: Tasarla ve Üret Laboratuvar Etkinliği

(Çevrimiçi form https://forms.gle/viCFdwqnAccSdrqx9 adresinde mevcuttur. İlgili linki tarayıcı programın adres çubuğuna kopyala-yapıştır yaparak formu açabilirsiniz.)

1. *http://testphp.vulnweb.com/index.php* web adresine bağlanın.
2. Önce *categories* linkine, onun altında ise *posters* linkine tıklayın. İnternet tarayıcı programın adres çubuğunda gördüğünüz adresi tam olarak yazın:

   ……..
3. Adres çubuğunun devamına *OR 1=1* yazıp Enter tuşuna basın. Sayfada ne gibi bir değişiklik olduğunu ve ekranda ne gördüğünüzü aşağıya yazınız.

   ……..
4. Şimdi ise adres çubuğunda *OR 1=1* devamına *bir tek tırnak işareti* ekleyerek Enter tuşuna basın. Sayfada ne gibi bir değişiklik olduğunu yazınız. Bu değişikliği nasıl yorumlarsınız?

   ……..

   ……..

   ……..

   ……..

   ……..
5. 3.maddede belirtilen *OR 1=1* adres satırına *order by 12* ekleyerek Enter tuşuna basınız. Sayfada ne gibi bir değişiklik olduğunu yazınız. Bu değişikliği nasıl yorumlarsınız?

   ……..

   ……..

   ……..

   ……..
6. *Order by 12* yazıp Enter tuşuna basınız.
7. *Order by 11* yazıp Enter tuşuna basınız. Sayfada ne gibi bir değişiklik olduğunu yazınız. Bu değişikliği nasıl yorumlarsınız?

   ……..

   ……..

   ……..

   ……..
8. 3.maddede belirtilen *OR 1=1* adres satırına *union select 1,2,3,4,5,6,7,8,9,10,11* yazıp Enter tuşuna basınız. Bu şekilde 11 sütun olduğunu tekrar doğrulamış oldunuz.

9. Karşınıza gelen sayfada en alta geliniz. En alttaki satırda 7, 2 ve 9 gibi rakamlar göreceksiniz. Bunun anlamı adres çubuğundan yapılan sorguda 2, 7 ve 9 numaralı sütunları kullanabilirsiniz. Aşağıda 2 numaralı sütun kullanılarak devam edilecektir.
10. İnternet tarayıcı program adres satırında en sonda yer alan *union select 1,2,3,4,5,6,7,8,9,10,11* kısmı içerisinde *2* yazan yeri silip yerine *@@version* yazıp Enter tuşuna basınız. Sayfada en alta inerek bu sayfayı çalıştıran işletim sisteminin adını ve versiyon bilgilerinin ne olduğunu yazınız.

    ……..
11. İnternet tarayıcı adresinde *1, @@version,3,4,5,6,7,8,9,10,11* adresinde *@@version* yazan yeri değiştirerek uygulamaya devam edelim. Kodu şu şekilde manipüle ederek Enter tuşuna basınız:

    1,group_concat(table_name),3,4,5,6,7,8,9,10,11 from information_schema.tables where table_schema=database()

    Bu kodu yazdıktan sonra sayfanın en altına gidip kontrolleri yapınız. Gördüğünüz tablo isimleri nelerdir? Yazınız.

    ……..

    ……..
12. Users tablosu içerisinden kullanıcı bilgilerine ulaşmaya çalışalım, hatta admin şifresini elde etmeye çalışalım.
13. *1,group_concat(column_name),3,4,5,6,7,8,9,10,11 from information_schema.columns where table_name=0x7573657273* yazarak Enter tuşuna basınız.

> BİLGİ NOTU
>
> Bir metnin hexadecimal kodunu öğrenmek için Google arama motoruna “text to hext” yazınız. Açılan sitelerden herhangi birinde giriş metni olarak users yazıp çevir diyerek users metninin hexadecimal kodunun 7573657273 olduğunu görebilirsiniz.

14. Sayfanın en altına inerek users tablosundaki sütun isimlerinin neler olduğunu yazınız.

    ……..

    ……..
15. Şimdi ise tablodan kullanıcı adı ve şifrelerini elde edelim. İnternet tarayıcı adres satırından sorguyu değiştirmeye devam edelim.

1,group_concat(uname,0x3a,pass),3,4,5,6,7,8,9,10,11 from users yazarak Enter tuşuna basınız.

Sayfanın en altına inerek sayfadaki kullanıcı adı ve kullanıcı şifresinin ne olduğunu yazınız.

……..

16. Bu bilgileri denemek için İnternet tarayıcı programı adres satırına *http://testphp.vulnweb.com/login.php* yazıp Enter tuşuna basınız. Elde ettiğiniz kullanıcı adı ve şifresini yazarak sisteme giriş yapınız. Başarılı bir giriş yaptıysanız ekranda ne gördüğünüzü not ediniz.

……..

……..

……..

……..

17. 11 ile 16 numaralı işlem adımlarını users tablosu dışında başka bir tablo için deneyiniz. Sonuçları not ederek adım adım hangi bilgilere ulaştığınızı yazınız.

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

Not: Bu etkinlikle ilgili daha detaylı teorik açıklamalara bilgeis.net adresinden ulaşılabilir (Bilge İş, 2022).

KAYNAKLAR

Bilge İş (2022). Sızma testine giriş. 10.09.2022 tarihinde http://bilgeis.net adresinden erişim sağlanmıştır.

Çınar, I., & Bilge, H. Ş. (2016). Web Madenciliği Yöntemleri ile Web Loglarının İstatistiksel Analizi ve Saldırı Tespiti. *Bilişim Teknolojileri Dergisi*, *9*(2), 125.

SİBER GÜVENLİK

LİSE

DENEYAP TÜRKİYE