Ofansif ve Defansif
Siber Güvenlik

İlker ERTUĞRUL

İçindekiler

1

Siber Güvenliğe Giriş

Bu Bölümde

Kitabımızın eğitim bölümlerine geçmeden önce bazı kavramları bilmenizin yararınıza olacağını düşünüyorum. Bu kavramları bilenler bu bölümü atlayabilirler.

Bu bölümde, sızma testi nedir? Hacker çeşitleri vb. kavramların açıklaması yapılacaktır.

Kavramlar için doğru bildiğiniz yanlışlar olabilir bu yüzden bu bölümü atlamadan birkaç dakikanızı ayırarak okumanızı tavsiye ederim.

SİBER GÜVENLİK NEDİR?

Siber güvenlik, günümüz bilişim çağında elektronik cihazların, dijital ortamdaki verilerin siber saldırılara karşı korunması ve gerekli güvenlik önlemlerinin alınmasıdır. Kısa bir tanım yapacaksak bu yorum yeterlidir. Siber güvenlik kavramı ayrıca çok geniş bir kavramdır.

HACKER NEDİR?

Hacker nedir? sorusunun cevabını vermeden önce **HACK** kavramını açıklamak daha doğru olacaktır. **Hack** kavramı, bir sistemin açıklarını yani zaaflarını bulmak, belirli kişilerin dosya ve sistemlerine izinsiz giriş yapmaktır. Hacker kavramı ise belirli teknik ve yöntemleri bilerek hack yapan kişidir. Hackerlar kendi prensiplerine göre çeşitli kategorilere ayrılırlar.

SİYAH ŞAPKALI HACKERLAR

Hackerların kendi prensiplerine göre çeşitli kategorilere ayrıldığını bir önceki paragrafımızda yazmıştım. Hackerlar kendi prensiplerine göre 3 kategoriye ayrılırlar. Bu kısımda siyah şapkalı hacker kavramı nedir onu açıklayacağım.

Siyah şapkalı hackerlar, kötü niyetli kişilerdir. Bildikleri yöntem ve teknikleri acımasızca kullanırlar. Genelde çıkarları doğrultusunda hareket ederler. Sistemlere ve kişilere izinsiz ve acımasızca saldırıp genelde ele geçirdikleri veriler için para talep ederler. Günümüzde sanal para teknoloji bitcoin çıktığından beri siyah şapkalı hackerların hareket alanı da artmıştır. Sanal para teknolojisinin devletler ve güvenlik ekipleri tarafından izlenememesi nedeniyle siyah şapkalı hackerlar genelde şifreledikleri veriler için bitcoin talep etmektedir. Sanal paranın iyi yanları olduğu gibi olumsuz yanı da para merkezli siyah şapkalı hackerların siber saldırılarını arttırmış olmasıdır.

Örnek bir saldırıdan bahsederek siyah şapkalı hackerların ne kadar tehlikeli olduklarını anlamanızı istiyorum.

Bir şirketin patronu bir gün çalışanlarının evde internet ortamından da işlerini yapabilmeleri fikrini düşünür ve hayata geçirir. Bu doğrultuda çalışanlara yazılım verilir. Şirkette çalışanlardan biri kendi şifresini basit bir şekilde koyar. Her ne olduysa bu basit şifreden sonra olur. Kötü niyetli bilgisayar korsanları yani siyah şapkalı hackerlar yazılımda yer alan verileri şifrelerler. Sonrasında ise bitcoin talep ederler ve bu bitcoinin ödenmesiyle yazılımdaki şifrelenmiş verileri sunarlar. Aynen okuduğunuz gibi basit bir şifre koymanın bile nelere mal olacağını kestiremezsiniz.

Her gün bu ve bu tarz siber saldırıları duyuyoruz bu yüzden gerekli güvenlik önlemlerini almalı sistemimizdeki güvenlik açıklarını minimuma indirmeliyiz. Siyah şapkalı hackerlar gerçekten tehlikelidirler.

Beyaz Şapkalı Hackerlar

Beyaz şapkalı hackerlar, siyah şapkalı hackerların tam tersidir. Beyaz şapkalı hackerlar genelde bu sektörde çalışan kişilerdir. Şirketleri, kurumları, devletleri siber saldırılara karşı korurlar. Tabii her beyaz şapkalı hacker bu sektörde çalışan değildir bu işi hobi olarak yapan beyaz şapkalı hackerlar da vardır.

Beyaz şapkalı hackerlar, siyah şapkalı hackerların sahip olduğu teknik ve yöntemleri bilen sistemleri ve kişileri siber saldırılara, kötü niyetli bilgisayar korsanlarına karşı koruyan kişilerdir. İzinsiz bir şekilde sistemlere ve kişilere kesinlikle saldırmazlar. Bilgi bakımından beyaz şapkalı hackerlar ve siyah şapkalı hackerlar arasında bir fark yoktur. Sadece amaç doğrultusunda ayrılırlar.

Gri Şapkalı Hackerlar

Gri şapkalı hackerlar için siyah ve beyaz şapkalı hacker karışımı hackerlar diyebiliriz. Bir sisteme izinsiz giriş yaparlar fakat zarar vermek yerine bunu sistem yöneticisine iletirler. Fakat günümüz bilişim yasalarında bir sisteme zarar vermeyecek olsanız da öncesinden gerekli izinleri almadan sisteme giriş yapmak suç teşkil etmektedir. Bu nedenden ötürü çoğu kişi gri şapkalı hacker kavramını kabul etmez. Bir sisteme izinsiz erişildiğinde hacker zarar vermeyecek olsa da bilişim yasalarına göre suç işlediğinden gri şapkalı hackerları, siyah şapkalı hackerlar olarak nitelendiren kişilerde vardır.

3

Temel Ağ Bilgisi

Bu Bölümde

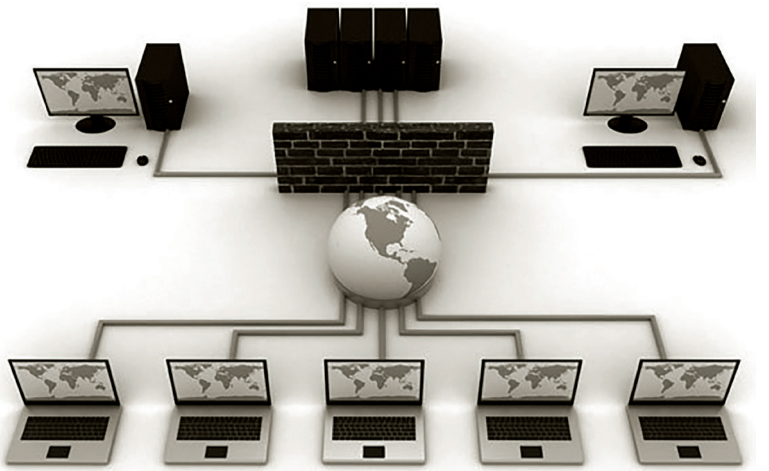
Network alanında bilgi sahibi olmak çok önemli. Gerek sızma testlerinde gerekse siber saldırılarda kullanılan yöntemlerde network bilginize ihtiyaç duyacaksınız.

Bu bölümde, temel seviyede ağ kavramlarını açıklayacağım. Kitap bir ağ kitabı olmadığı için ağ ile alakalı tüm kavramları açıklamam mümkün değil maalesef.

Kitabı bitirdikten sonra network bilginizi ileriye taşımanızı tavsiye ederim.

NETWOK (AĞ) NEDİR?

En az iki bilgisayarın birbirleriyle iletişim halinde olmasıdır. Bu iki bilgisayar birbirlerinden farklı uzaklıklarda olabilirler. Eğer bu iki bilgisayar aynı ortamdaysa yani aynı Ağ üzerindeyse **LAN** (Local Area Network) olarak adlandırılır. LAN dışında birçok Network daha vardır. Ancak ben kitapta LAN ağı dahil iki ağ çeşidine yer vereceğim. Bunlar **Wide Area Network** ve **Metropolitan Area Network**'dur.



LAN (LOCAL AREA NETWORK) NEDİR?

LAN ağlarına örnek vermek gerekirse internet kafeler gösterilebilir. İnternet kafelerde yer alan bilgisayarlar çoğunlukla aynı ağda bulunurlar. İnternet kafede arkadaşlarınız ile oynadığınız multiplayer oyunları LAN ağı sayesinde oynamaktasınız. İnternet kafelerde bulunan bilgisayarlar aynı ağda yer aldıkları için arkadaşınız ve siz multiplayer oyunlarda iki bilgisayarın birbirleriyle iletişim kurmasıyla oyunu oynamaktasınız. Lan (Local Area Network) kavramını Türkçeye çevirecek olursak **Yerel Alan Ağı** diyebiliriz. Lan ağlarında bilgisayarlar ethernet kartları ve kablolar ile aynı ağa bağlanırlar.

WAN (WIDE AREA NETWORK) NEDİR?

WAN ağları, LAN ağlarından farklı olarak coğrafi uzaklıktaki iki veya ikiden fazla bilgisayarın birbirine bağlanmasıdır. Şehirler arası, kıtalar arası bilgisayarların ve Networklerin birbiri ile bağlanması ve iletişim kurması diyebiliriz. Türkçeye çevirdiğimizde **Geniş Alan Ağı** olarak geçer.

11

Yerel Ağ Saldırılarından Korunma Yöntemleri

Bu Bölümde

Bu bölümde yerel ağ saldırılarından korunma yöntemlerini işleyeceğiz.

Yerel ağ saldırılarına karşı gerekli güvenlik önlemlerini almak ve saldırılara karşı dikkatli olmak çok önemlidir.

Ortadaki Adam Saldırısı Korunma ve Tespiti

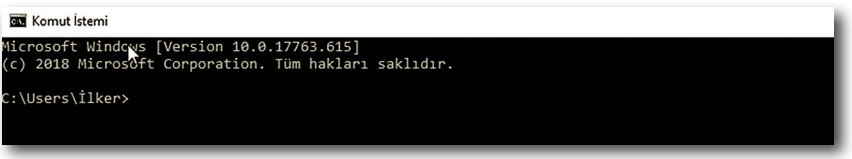
Ortadaki adam saldırısını zaten işlemiştik. Yerel ağlara yönelik en çok yapılan saldırılardan biri olan ortadaki adam saldırısına karşı nasıl korunuz bunu öğreneceğiz. Aynı zamanda olası bir ortadaki adam saldırısını nasıl tespit edebiliriz öğrenmiş olacağız. Ortadaki adam ve benzeri yerel ağ saldırılarından korunmanın en iyi yolu bağlı bulunduğunuz ağı korumaktan geçer. Bulunduğunuz ağda gerekli önlemleri almalı ve yabancı cihazların ağınıza bağlanmasını engellemelisiniz. Olurda bir yabancı cihaz ağınıza bağlanır ve bu saldırıyı yaparsa dikkatli olmalı ve saldırıyı tespit etmelisiniz.

İlk olarak ortadaki adam saldırısından korunmak için yapmanız gereken kesinlikle gitmek istediğiniz sitelerin adres satırını incelemeniz gerekmekte. Facebook, twitter gibi sosyal medya adreslerine giriş yaparken veya internet bankacılığı kullanırken gideceğiniz sitenin adres satırına bakarak https kullandığından emin olun. Http kullanan SSL sertifikası kullanmayan sitelerde bilgileriniz saldırganların eline geçeceği için bu tarz **http** kullanan sitelere oturum açmayın, giriş yapmayın.

En azından bu şekilde hesap bilgileriniz saldırganların eline geçmemiş olacaktır, fakat http kullanan sitelere giriş yaptığınızda saldırganlar gezindiğiniz siteleri görecektir. Ortadaki adam saldırısını tespit edip gerekli önlemleri alarak gezindiğiniz sitelerin saldırganlar tarafından görülmesini engelleyebilirsiniz.

Ortadaki adam saldırısını nasıl tespit edebileceğinizi öğrenelim. Sanal makineye kurduğumuz Windows makinemizi açalım.

Ortadaki adam saldırısının olup olmadığını görebilmek için ARP tablosuna bakmamız gerekiyor. Windows bir cihazda ARP tablosunu görebilmek için komut satırını açmamız gerekiyor. Komut satırını açabilmek için Windows cihazda arama kutusuna komut istemi yazınız. Bu şekilde komut satırını açın.



Görüldüğü üzere komut istemi açıldı. ARP Tablolarını görebilmek için `arp -a` komutunu komut satırına girelim.

```
C:\Users\İlker>arp -a

Interface: 192.168.1.110 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           30-b5-c2-8c-f3-fa     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\İlker>
```

Resimde olduğu gibi ARP tablolarını görebildik. Ortadaki adama saldırısı olup olmadığını görebilmek için ARP tablolarına göz atmamız yeterlidir. Görseli inceleycek olursak ARP tablosunda ortadaki adam saldırısı olmadığı görülüyor. Şimdiki aşamada ise Kali bilgisayarımızdan şu anki Windows makineye ortadaki adam saldırısını gerçekleştirelim. Bakalım ARP tablolarında ne gibi değişiklikler olacak.

```
Interface: 192.168.1.110 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           08-00-27-93-cc-e0     dynamic
  192.168.1.106         08-00-27-93-cc-e0     dynamic
  192.168.1.107         08-00-27-93-cc-e0     dynamic
  192.168.1.109         08-00-27-93-cc-e0     dynamic
  192.168.1.111         08-00-27-93-cc-e0     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\İlker>
```

Yukarıdaki resimde görüldüğü üzere ortadaki adam saldırısını gerçekleştirdikten sonra ARP tablolarında değişiklikler oldu. ARP tablolarına ilk baktığımızda **192.168.1.1** yani modemin MAC adresi gözükürken saldırıdan sonra modemin MAC adresi 08 ile başlayan MAC adresi ile değiştiğini görüyoruz. Sadece modemin MAC adresi değil birçok IP adresinin de MAC adresinin 08 ile başlayan MAC adresi ile değiştiğini görüyoruz. Şimdiki aşamada ise ortadaki adama saldırısını sonlandıralım ve ARP tablolarına tekrar göz atalım.

```
C:\Users\İlker>arp -a

Interface: 192.168.1.110 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           30-b5-c2-8c-f3-fa     dynamic
  192.168.1.106         5c-1d-d9-14-1a-21     dynamic
  192.168.1.107         00-26-18-b5-81-2c     dynamic
  192.168.1.109         68-07-15-83-77-1e     dynamic
  192.168.1.111         08-00-27-93-cc-e0     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\İlker>
```

13

Nessus ile Zafiyet Taramaları

Bu Bölümde

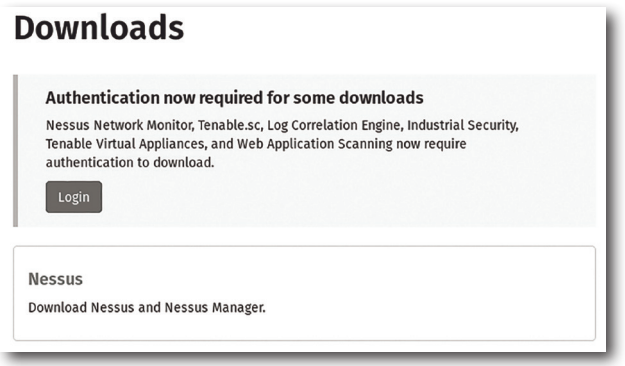
Bu bölümde Nessus ile zafiyet taramaları nasıl yapılır bunu öğreneceğiz.

Bir sistemde yer alan açıkları ve zaafları bulmak, tespit etmek gereklidir. Nessus kapsamlı bir güvenlik açığı tarama yazılımıdır.

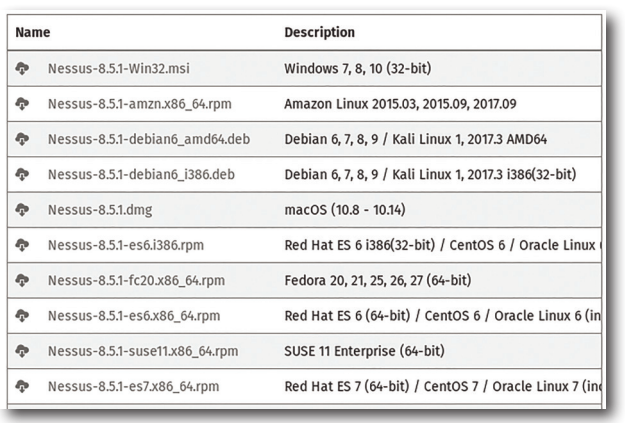
NESSUS KURULUMU

Nessus kurulu olarak gelmemektedir. Nesssus'u kullanabilmek için sistemimize kurmamız gereklidir. Nessus'un farklı sürümleri bulunmakta olup, ücretli sürümü daha çok ticari amaçlar için kullanılmaktadır.

Nessus Tenable firması tarafından geliştirilmektedir. Nessus kurulumu için Kali makinemizde arama motorunun URL kısmına ***httos://www.tenable.com/downloads*** adresini yazalım.



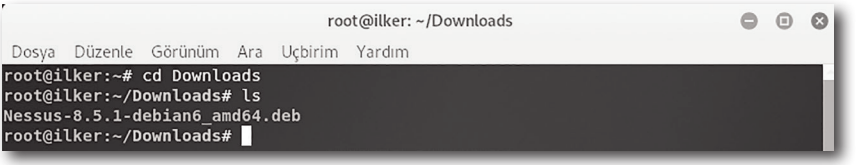
Siteye eriştikten sonra görselde görünen **Nessus download Nessus and Nessus Manager** kısmına tıklayalım.



Görüldüğü üzere belirttiğim kutucuğa tıkladıktan sonra indirme sayfası açılacak. İndirme sayfasında sistemimize uygun olan kurulum dosyasını seçmeliyiz. İndirme sayfasında da görüldüğü üzere Linux dışında Windows ve macOS cihazlarda da Nessus kullanabiliyoruz.

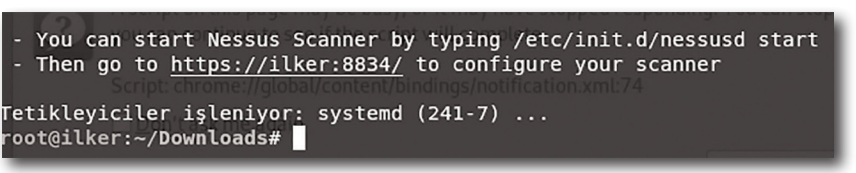
İndirme sayfasında indirmemiz gereken dosya eğer Kali sistemini 64 bit olarak kurduysanız **Nessus-8.5.1-debian6_amd64.deb** dosyası olacaktır. Kali sistemini 32 bit olarak kuranlar **Nessus-8.5.1-debian6_i386.deb** dosyasını indirecektir. Siz bu satırları okuduğunuz vakit Nessus'un yeni bir sürümü çıkmış olabilir. En yeni sürüm zaten indirme sayfasında yer alacaktır.

Kurulum dosyasını sisteminize göre uygun olanını seçerek indirelim. İndirme için Lisans sözleşmelerini kabul ediniz. İndirme tamamlandıktan sonra komut satırından İndirilenler dizinine geliyoruz.



Görüldüğü üzere kurulum dosyamız indirilenler dizininde bulunuyor. Kurulumu başlatmak için `dpkg -i Nessus-8.5.1-debian6_amd64.deb` komutunu giriyoruz. `dpkg -i` komutundan sonra kurulum dosyasının adını komut satırından kopyalayıp doğrudan yapıştırabilirsiniz.

Kurulumu başlattıktan sonra kurulumun tamamlanmasını bekleyelim. Bu süre zarfında komut satırını kapatmayın!



Nessus kurulumu başarıyla tamamlandı. Nessus'u başlatmamız gerekli. Nessus'u başlatmak için komut satırına `/etc/init.d/nessusd start` komutunu girmeniz yeterlidir. Bu komutu girdikten sonra komut satırında `Starting Nessus` yazısını görürseniz Nessus başarıyla başlatılmış demektir.

Nessus'u tarayıcımızdan kullanıyoruz. Bir web paneli var. Bu panele ulaşmak için ***https://ilker:8834/*** URL adresine gitmem yeterli. Zaten yukarıdaki görselde görüldüğü üzere panele ulaşmak için yazmanınız gereken URL adresini söylüyor. Sizin gireceğiniz URL adresi Kali'yi kurduğunuz vakit belirlediğiniz isim. Ben kendi adımı vermiştim. Nessus kurulumu tamamlandıktan sonra URL adresini söyleyecektir. URL adresini tarayıcımıza girerek panele ulaşalım.

14

Metasploit ile Güvenlik Zafiyetlerini Sömürmek

Bu Bölümde

Metasploit güvenlik zafiyetlerini sömürmek için kullanılan en iyi araçlardan biridir. Sadece güvenlik zafiyetlerini sömürmek için kullanılmaz. Kitabın ilerleyen bölümlerinde Metasploit ile bilgi toplama işlemi bile gerçekleştireceğiz.

Metasploit bir siber saldırı ve analiz aracıdır. Ruby dili ile kodlanmıştır. İçerisinde exploit, auxiliary, payload, nop ve encoder modüllerini bulundurur.

İlk olarak bazı temel kavramları öğreneceğiz. Sonrasında Metasploit içerisinde kullanabileceğimiz önemli komutları tanıyacağız. Son olarak Metasploit ile hedef sistemde yer alan zaafları sömüreceğiz.

TEMEL KAVRAMLAR

Metasploit framework kullanırken bazı kavramlar ile oldukça haşır neşir olacağız. Bu kavramları bilmemiz anlam karmaşasının önüne geçecektir.

EXPLOIT NEDİR?

Exploit, sistemde yer alan güvenlik zaaflarını sömürmek için geliştirilmiş, bir bilgisayar programı veya scrip'tir. Perl, Ruby, C, Python gibi programlama dilleri ile yazılmaktadırlar. Exploit yazmak oldukça zordur. Exploit'ler iki türlü yayımlanır. **Ücretli** ve **ücretsiz** olarak yayımlanırlar.

Metasploit framework içerisinde exploit modülü mevcuttur. Biz uygulamamızı gerçekleştirirken ücretsiz yayımlanan hazır exploitleri kullanacağız. Başlangıç aşaması için hazır exploitleri kullanmak ve bu exploitler ile hedefi sömürmek iyi bir başlangıçtır. Kim bilebilir ilerde belki bir gün kendi exploitinizi yazacak seviyeye bile gelebilirsiniz.

Exploitlerin kendi aralarında farklı çeşitleri bulunmaktadır. Exploit çeşitlerini tanıyalım.

» **Remote Exploits;** Bu Exploit çeşidinde, uzak sistemlerde bulunan sistemleri sömürmek için kullanırız.

» **Local Exploits;** Bu Exploit çeşidi, genelde sistemde hak ve rütbe yükseltmek için kullanılır. Linux bir sistemde root kullanıcı olmak istiyorsak ve bir güvenlik zafiyeti keşfettiysek Local Exploit kullanırız.

» **Zero-Day Exploits;** Bu Exploit çeşidi, oldukça tehlikelidir. Sistemde yer alan güvenlik zafiyetlerini sömürmek için yazılırlar. Birçok teknoloji sitesinde bir makalede veya haberde bu tarz exploitler ile yapılan siber saldırıları duymuş olabilirsiniz. Çoğunlukla ücretli satılırlar.

» **Client Side Exploit;** Ağ üzerinden sistemle etkileşim kurulur. Tetiklenmesi gerekmektedir. Sosyal mühendislik atağıyla exploit tetiklenir.