BÖLÜM 6

GÜVENLİK STRATEJİLERİ VE KORUNMA

ANAHTAR KAVRAMLAR

Bilgi Toplama, Temel Güvenlik, Güvenlik Yazılımları

ÖĞRENME HEDEFLERİ

1. Bilgi toplama araçlarını açıklar.
2. Temel güvenlik önlemlerini açıklar.
3. Zaafiyet derecelendirme sistemini tanımlar.
4. Güvenlik yazılımlarını tanımlar.
5. Güvenlik yönetim merkezinin işlevini açıklar.

ALTINCI BÖLÜM

GİRİŞ

Siber saldırılara, tehditlere ve zararlı yazılımlara karşı savunma yapabilmek ya da koruma stratejileri geliştirebilmek için, tehdit aktörlerinin yöntemlerini, tekniklerini, ağın işleyişini ve yapısını bilmeyi gerektirir. Saldırının ilk aşaması keşif aşamasıdır. Saldırgan bu aşamada hedefe ilişkin bilgi toplamaktadır. Siber güvenlik uzmanının da bu bilgi toplama yöntemlerini bilmesi, güvenlik stratejileri oluşturmada ve korunma aşamaları tasarlamalarında yararlı olacaktır. Bu bölümde, bilgi toplama yöntemleri, bilgi toplama araçları, temel güvenlik önlemleri ve stratejileri ele alınmıştır.

1. SİBER GÜVENLİKTE BİLGİ TOPLAMA ARAÇLARI

Siber güvenlik dünyasında gerek saldırı için olsun gerek savunma için olsun bilgi toplama ihtiyacı vardır. Bilgi toplama yöntemleri, Pasif Bilgi Toplama ve Aktif Bilgi Toplama olarak iki başlık altında ele alınabilir.

1.1. Pasif Bilgi Toplama Araçları

Pasif bilgi toplama sürecinde, bilgi alınmak istenen ağ ya da sistem ile doğrudan bir etkileşim bulunmaz. Elde edilen bilgi, doğrudan sistemden değil internet kaynaklarından elde edilir. Bu bilgi toplama yöntemlerinde şunlar yapılabilir.

- IP Adresleri Hakkında Bilgi Toplama Araçları
- Domainler Hakkında Bilgi Toplama Araçları
- Web Sayfalarında Bilgi Toplama Araçları

IP Adresleri Hakkında Bilgi Toplama

IP adreslerinin dünyadaki dağıtım merkezi ICANN (Internet Corporation for Assigned Names and Numbers)'dır. Bu kâr amacı gütmeyen kurum, İnternet adresi alanı tahsisi, protokol ataması ve ülke kodu (.tr, .de, .se gibi) internet alan adı yönetiminden sorumludur. Bir IP adresi sorgusunu en kısa yoldan Whois Sorgusu ile yapılmaktadır.

Whois Sorgusu

Whois sorgusu, sorgu yapılan alan adı ile bazı bilgilere ulaşmayı hedefler. Alan adı sahibi kişiye ait iletişim bilgileri ve alan adı ile ilgili teknik bilgiler yasal çerçevede (ICANN) listelenir. Whois sorgusunu herkes yapabilir yani herkes ulaşabilir. Ancak alan adı sahibi kendisine ait bilgilerin Whois sorgusu sırasında listelenmesini istemeyebilir. Bunun için Whois Gizleme servisinin aktif edilmesi gerekmektedir. Bu sayede, ICANN verileri gizleyip başka kişiler ile paylaşmayacaktır.

Şekil 1 Whois web sitesi ve arama işlemi

http://www.whois.com/ internet adresine bilgi edinmek istenilen alan adı yazıldığında (örnek: ankara.edu.tr) Şekil 2'deki ekran görünmektedir.

ankara.edu.tr

```
** Domain Name: ankara.edu.tr
Frozen Status: -
Transfer Status: The domain is LOCKED to transfer.

** Registrant:
   Ankara Üniversitesi
   Hidden upon user request
   Hidden upon user request
   Hidden upon user request
   Hidden upon user request

** Registrar:
NIC Handle              : tk1036
Organization Name       : TRABİS KK
Address                 : ANKARA
                          ANKARA
                          00000 Ankara Türkiye
Phone                   : 90-312-2100060
Fax                     : 90-312-2100060

** Domain Servers:
ns1.ankara.edu.tr 80.251.40.10
ns2.ankara.edu.tr 80.251.40.11

** Additional Info:
Created on..............: 1999-Apr-30.
Expires on..............: 2025-Apr-29.

** Whois Server:
Last Update Time: 2023-12-07T02:17:49+03:00
```

Şekil 2 Örnek Whois sorgusu

RIPE Üzerinden IP Sorgulama

Şekil 3 RIPE NCC sayfası

RIPE NCC, IANA kuruluşuna bağlı olan, Avrupa ve Ortadoğu bölgesi gibi bir bölgeye IP adresi dağıtımından sorumlu olan bir kuruluştur. Bu kuruluşa https://www.ripe.net/ internet adresinden erişilebilir. Belirtilen bölgede yer alan IP adreslerine ilişkin pasif bilgi sorgulaması yapılabilir. İlgili web sayfasında sorgulanmak istenen IP adresi yazılarak sorgulama yapılabilir. Şekil 4'te yer alan ekran görüntüsünde örnek bir sorgulama yapılmıştır.

Responsible organisation: Ankara University
Abuse contact info: abuse@ankara.edu.tr

inetnum:	5.23.120.0 - 5.23.123.255
netname:	TR-AU-NAT
descr:	Ankara University
country:	TR
admin-c:	AUID1-RIPE
tech-c:	AUID1-RIPE
status:	ASSIGNED PA
mnt-by:	ANKARA-NET-MNT
mnt-domains:	ANKARA-NET-MNT
created:	2012-05-15T14:03:02Z
last-modified:	2017-11-08T09:36:02Z
source:	RIPE

route:	5.23.120.0/21
descr:	ANKARA-NET
origin:	AS8678
mnt-by:	ANKARA-NET-MNT
created:	2012-05-15T12:43:50Z
last-modified:	2012-05-15T12:43:50Z
source:	RIPE

Şekil 4 Örnek Ripe NCC sorgulama

Site Durumunu öğrenme

https://ns.tools/ web sitesi, bir web sayfanın aktif mi yoksa pasif mi olduğunu öğrenmek için ping işlemi uygular. Bu yöntemle web sitesinin işlevsel ve aktif olup olmadığı öğrenebilir. Ayrıca bu web sitesi ile ilgili daha farklı bilgiler de toplanabilir.

Şekil 5 ns.tools sitesi

Alan Adları Hakkında Bilgi Toplama Araçları

Etki alan adları olarak da adlandırılan domain adları, genellikle web sitelerine IP numaraları yerine, hatırlaması daha kolay olan isim yazarak erişmek için kullanılan bir sistemdir. İnternet ortamında cihazların iletişiminde nümerik IP adresleri kullanılır. Ancak kullanıcılar erişmek istedikleri web sayfaları ya da herhangi bir kaynağın IP adresini akılda tutması güç olabilir. Bu nedenle belirli kurallar dâhilinde, benzersiz alan isimleri kullanılır.

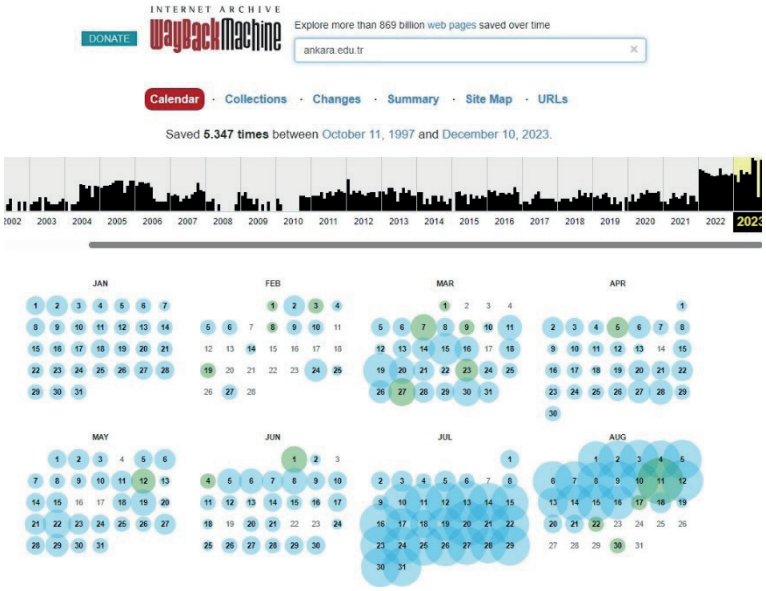
Alan adı isimlendirmesi, daha önce bahsedilen DNS sistemi ile ilişkilidir. Belirli bir web sitesine ilişkin bu benzersiz alan adları hakkında bilgi toplamak için isim sorgulaması yapılabilir. Alan adlarının kullanımda olup olmadığı ya da var olup olmadığına ilişkin bilgilere erişmek için domain sorgulama sistemleri kullanılabilir.

Web Sayfalarından Bilgi Toplama Araçları

- Archive.org
- Netcraft.com
- Pipl.com

Archive.org : İnternet ortamında yıllar boyunca devasa sayıda web sayfaları yayına girer ve bazen çeşitli nedenlerle kapanabilir. Archive.org sayfası, 1996 yılından itibaren web sitelerinin görüntülerini indeksleyen oldukça yararlı bir web sayfasıdır. Yayından kaldırılan ya da günümüzde var olmayanların yanı sıra, günümüzde var olan sitelerin de eski görüntülerine erişmek mümkündür.

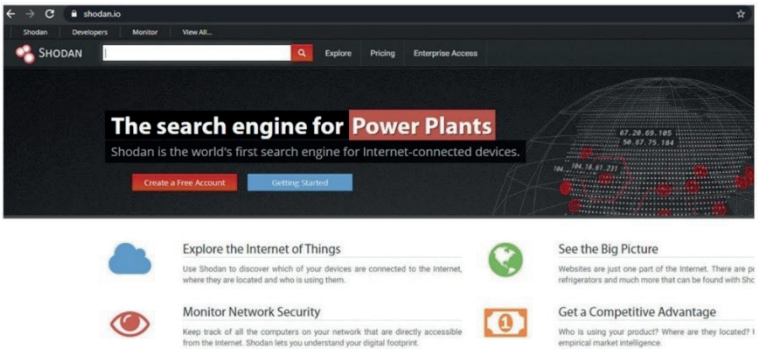
İlgili sayfada sorgulanmak istenen web sitenin adresi yazılır. Arama (“Search”) alanına sorgulanmak istenen site adresi yazılır ve “Go” tuşuna basılır.Şekil 6’da örnek bir ekran görüntüsü yer almaktadır.



Şekil 6 Örnek archive.org sorgusu

Açılan takvimden, (indekslenmişse) istenilen bir tarihe ait sayfanın görüntüsüne ulaşılabilir.

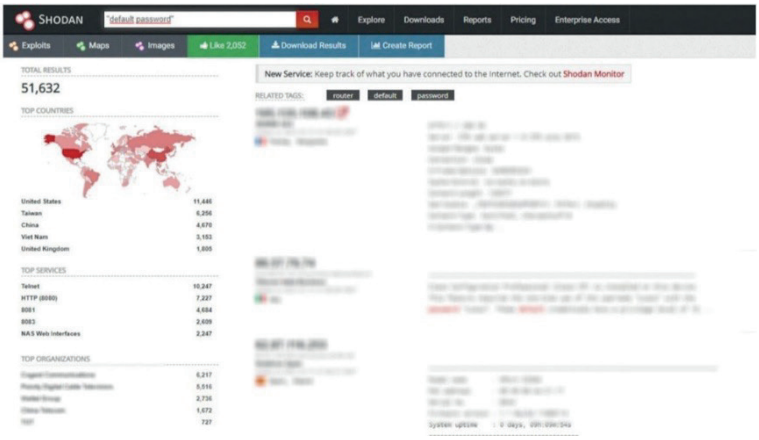
Shodan Kullanarak Bilgi Toplama: Shodan, çeşitli filtreler kullanarak internete bağlı bilgi işlem cihaz türlerini bulmayı sağlayan www.shodan.io sayfasından hizmet veren bir arama motorudur.



Şekil 7 shodan.io ana sayfası

Shodan, internete bağlı cihazları aramak için interneti sürekli olarak tarayan dünya çapına yayılmış sunuculara sahiptir. Web kameraları, varsayılan parola kullanan cihazlar, yönlendiriciler ve IoT cihazları gibi birçok cihazın bulunmasını sağlayabilir. Hangi cihazların bağlı olduğu, nereye bağlı oldukları ve hangi servislerin güvenlik açığı içerdiği ile ilgili olarak veri madenciliği yapmak amacıyla kullanılabilir.

Shodan ekranında görüntülenen tüm cihazlar, güvenlik açığı içeren sistemler değildir. Ancak bazı güvenlik açığı barındıran sistemlerin de tespit edilebilmesi mümkün olabilir. Örneğin, varsayılan parola kullanan sistemlerin tespit edilebilmesi için arama alanına "default password" yazınız.



Şekil 8 Örnek Shodan.io sorgusu

Şekil 8'deki Shodan ekran görüntüsünde varsayılan parolayı kullanan sistemlere ilişkin bilgiler gösterilmektedir. Shodan aramasında, filtreleme parametreleri de kullanılabilir. Shodan ile kullanılabilecek bazı filtreler şunlardır:

- city: Belirli bir şehirde arama yapar
- country: Belirli bir ülkede arama yapar
- os: işletim sistemine göre arama yapar
- port: Açık olan TCP/UDP portlarına göre arama yapar
- product: Belirli bir ürüne göre arama yapılır.

Örneğin, Amerika Birleşik Devletlerinde SNMP hizmeti açık olan Cisco 7200 yönlendiricileri görmek için arama kutusuna {country:US product:"Cisco 7200 Router" port:161} yazılabilir.

Siber güvenlik kapsamında yapılabilecek diğer bir Shodan araması da ileriki bölümlerde ele alınacak olan CVE güvenlik zafiyeti numarasına göre arama yapmaktır. Ancak bu tür bir arama sadece lisanslı ve akademik kullanıma açıktır.

DİKKAT EDELİM

Bu bölümde yapılan aramalar ve anlatılan konular eğitim amaçlıdır. Lütfen yasal olmayan durumlara karşı dikkatli olunuz.

1.2. Aktif Bilgi Toplama Araçları

Bu bilgi toplama yönteminde hedef sistem ile doğrudan iletişime geçirilir. Saldırgan açısından riskli bilgi toplama yöntemidir ve çok dikkatli olunması gerekmektedir. Yakalanma olasılığı her zaman mevcuttur. Bir siber güvenlik uzmanının da savunma amaçlı olarak bu aktif bilgi tekniklerini bilmesi gerekmektedir.

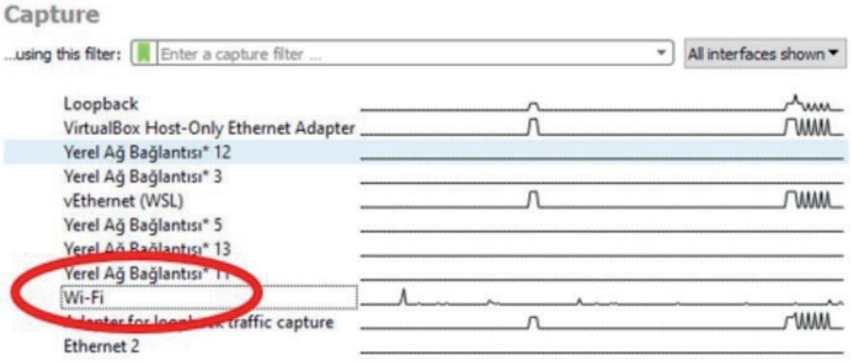
Network Maping

Network mapper, en yaygın bilinen şekliyle bilgisayarın açık olan bağlantı noktalarını, parmak izini, kullanılan servislerin isim ve versiyon numaralarını bulmaya yarayan bir araçtır. NMAP, daha önceki konularda ele alınan çeşitli ağ protokolleri aracılığıyla veri toplamayı sağlayan yararlı bir araçtır. Ağda yer alan konaklara ICMP gibi paketler gönderilerek sorgulamalar yapılır ve cihazlardan gelen cevaplar incelenir. Gelen cevaplardaki bilgilerdeki doğrudan bilgilere ya da ipuçlarına göre ağda keşif işlemleri yapılabilir, aktif olarak bilgi alınabilir.

Nmap, ağ haritalaması üzerine odaklanmış bir araçtır. Bu sayede incelenmek istenen bir ağda bulunan cihazların, kullanılan işletim sistemlerinin ve açık bulunan servis ve bağlantı noktası bilgileri tespit edilebilir. Bu bilgilerin elde edilebilmesi için sadece hedef bilgisayar sistemine ait web adresini veya IP adresini bilmek ve Nmap'i kullanmak yeterlidir. Örneğin bir IP'nin bulnduğu ağın haritasının çıkarılması için "nmap IP_adresi" yazmak yeterlidir. Bu komut ile o IP adresindeki bilgisayarın bilinen bağlantı noktalarına SYN taraması gerçekleştirir. Bağlantı noktaları, bir sistemde çalışan hizmetler ve uygulamalar ilişkili bir kavramdır. Hedefe ilişkin SYN taraması yapmak, TCP protokolünün SYN bayrağını kullanarak açık hizmetlerin bulunmasını sağlamaktadır.

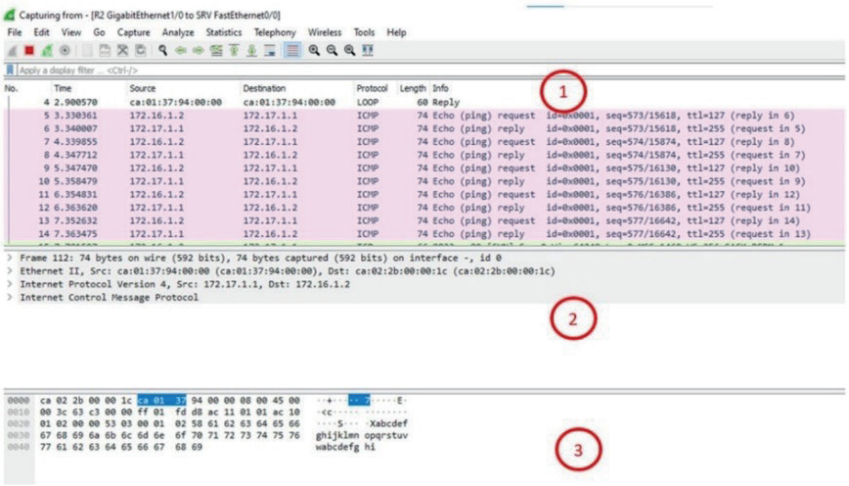
WireShark

WireShark, ağ ortamında paketlerin yakalanmasını ve analiz edimesini sağlayan ücretsiz ve en popüler protokol analiz ve paket yakalama aracıdır. Bu yararlı yazılım https://www.wireshark.org/ sayfasından indirilebilir.



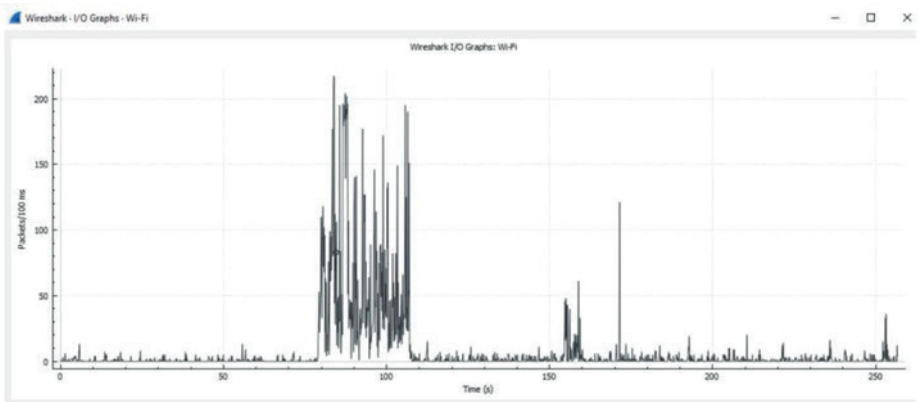
Şekil 9 Wireshark dinlenecek arayüz seçme

Yazılım çalıştırılırken ilk olarak paketin yakalanacağı arayüz (NIC) seçilir. Arayüz seçiminin ardından, Şekil 10'daki gibi bir ekran görüntüsü gelir.



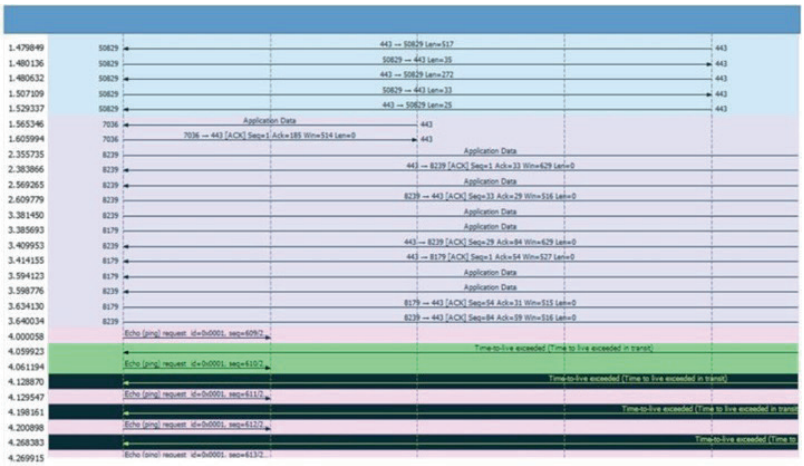
Şekil 10 Wireshark paket toplama ekranı

WireShark ekranı üç ana bölümden oluşur. İlk bölümde zamana göre yakalanan paketler yer almaktadır. İkinci bölümde yakalanan bu paketin katmanlı yapıdaki içerikleri, üçüncü bölümde ise paketin içerdiği veriler kodlanmış olarak görüntülenmektedir.



Şekil 11 Wireshark istatistiksel analiz ekranı

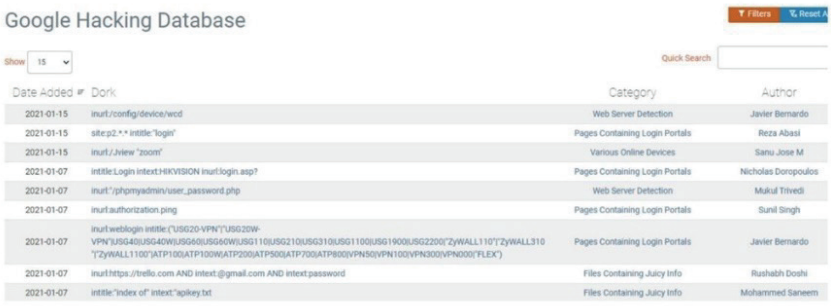
Yakalanan paketlerin tek tek incelenmesinin yanı sıra, ağ ortamı hakkında genel ağ kullanımı, en fazla iletişim kuran IP'ler, TCP veri akışı gibi istatistiksel ve görsel bilgiler de sunmaktadır.



Şekil 12 Wireshark iletişiminin görselleştirilmesi

Google Hack Veritabanı

Google internette en yaygın kullanılan arama motorudur. Siber güvenlik dünyasında bilgi toplamada, Google arama motorunun sağladığı anahtar kelimeler ile detaylı bilgi toplama yapılabilir. Arama motorunun indeksleme becerisi, zararlı olabilecek birçok kritik bilginin de indekslenmesine neden olmuştur. Google Hack Veritabanı, https://www.exploit-db.com/google-hacking-database bağlantısından erişilebilen Google sorgularının listesini içeren bir indeksleme veritabanıdır.



Şekil 13 Google Hack Veritabanı

Örneğin, bir web sunucusunun parmak izi, Google üzerinden Apache çevrimiçi dokümantasyonu veya IIS tarafından web kök dizinine eklenen özel bir klasör için sorgulama yapılaması mümkündür.

{intitle:"Apache HTTP Server" intitle:"documentation" site: hedefsite.abc}

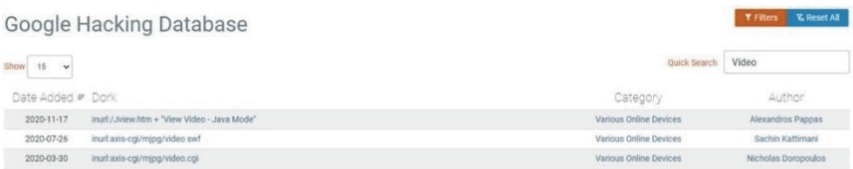
Bunun için belirli bir siteye yönelik (hedefsite.abc) yukarıdaki sorgulama cümlesi yazılarak, google'nin indekslediği verilerden özelleştirme yapılabilir.

Diğer bir örnek de dosya türüne göre belirli bir sitede arama yapmaktır. Buna göre hedefsite için bak dosyalarının tespitine yönelik olarak aşağıdaki gibi bir sorgulama yapılabilir.

{filetype:"bak" site:hedefsite.abc}

Görüleceği üzere, Google hack veritabanı kullanılarak, kullanıcı adı & parolalar, kritik bilgiler içeren hata mesajları ve güvenlik zafiyetleri bulunabilir. İlgili veritabanında yer alan güncel sorgular kullanılarak bilgiler toplanabilir.

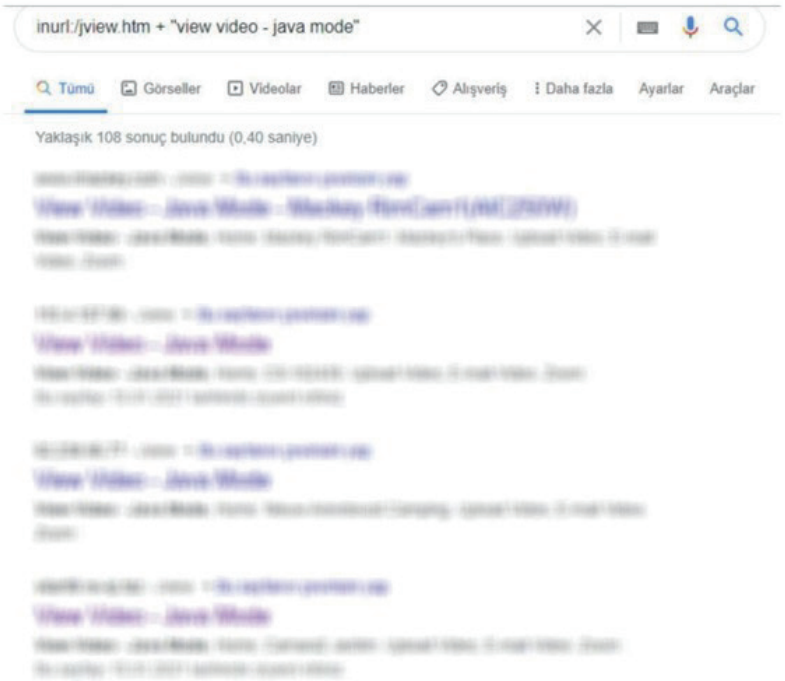
Örnek olarak, ilgili veritabanında yer alan arama kısmına "video" yazılarak, bununla ilgili sorgulara ulaşılabilir.



Şekil 14 Google Hack sorgulama sonucu

Gelen ilk ekrandaki ilk sorgu cümlesi Google arama motorunda yazılabilir. Bu durumda Şekil 15'teki gibi bir liste görüntülenecektir.

Bu sorguya cevap veren herhangi bir link açıldığında kamera video akışını gösteren cihaza erişim sağlanabilecektir.



Şekil 15 Örnek Google sorgusu

2. TEMEL GÜVENLİK ÖNLEMLERİ

Bir bilgisayarı güvenli hale getirmek, kişi veya kuruma göre farklı nedenlerden dolayı farklı türdeki eylemleri uygulamaya koymak amacıyla yapılması gereken işlemler ve kurallar bütünüdür. Bilgisayar güvenliği kuralları, bilgisayarı kullandığınız sürece devam eder. Bir bilgisayar sisteminin güvenliği ne kadar iyi tasarlanırsa tasarlansın, güvenlik ile ilgili işlemler kontrol edilmez ve zaman göre güncellenmezse, sisteminiz herhangi potansiyel bir bilgisayar korsanına karşı savunmasız bırakabilir.

Araştırmalara göre yeni bir bilgisayar kurulumu tamamlandıktan sonra ilk siber saldırı ortalama yedi dakika sonra gerçekleşmektedir. Bunun nedeni, bilgisayar saldırganlarının genellikle fırsat arayan ve sürekli araştıran otomatik tarama araçları kullanmasıdır. Bir istismar, genellikle bir kurulumu tamamladıktan sonra, güvenlik önlemleri alınmadan dakikalar içinde gerçekleşebilir. Bu araştırma bizlere, bilgisayar kurulumu yapıldıktan sonra internet bağlantısı kurulmadan tüm savunma ve koruma işlemlerini yerine getirmemiz gerektiği sonucunu ortaya çıkartmaktadır.

Bilgisayar kullanıcılarının sayısı arttıkça bilgisayar güvenliği konusuna yeterli önemi göstermeyen veya deneyimsiz bir kullanıcının kullandığı bilgisayar, belirlenmiş bir hedefe yönelik dağıtılmış bir hizmet reddi (DDoS) saldırısına dâhil edilebilir. Bu gibi sorunlara karşı üç konuda temel bilgisayar güvenliğini ele alabiliriz.

2.1. Fiziksel Güvenlik

Bilgisayar sisteminin fiziksel güvenliğidir. Bilgisayarın fiziksel olarak zarar görmemesi veya kötü niyetli kişilerce ele geçirilmemesi için gerekli önlemlerin alınmasıdır. Bununla beraber aşırı elektrik akımından korumak için kesintisiz güç kaynağı kullanmak bilgisayarın ve bilgisayar içinde saklanan verilerin güvenliği için oldukça önemlidir. Günümüzde kişisel bilgisayarlarda elektrik hatlarındaki problemler dolayısı ile veri kaybı oldukça sık görülmektedir. Modem, sabit sürücü veya ana kart arızaları nedenleri ile bilgisayarların bir süre kullanılamaması gibi problemlere karşı fiziksel güvenlik tedbirleri alınmalıdır.

Şekil 16 Fiziksel güvenlik

2.2. Veri Bütünlüğü

Verilerin yedeklenmesi ve bu şekilde veri kaybının önlenmesidir. Kurumlar veya kişisel kullanıcılar kendileri için değerli gördükleri verileri korumalıdır. Her yıl, bir şekilde kaybedilen değerli bilgileri yeniden üretmek için büyük bir miktarda iş gücü kaybı oluşmaktadır. Yedeklemeler flaş diskler, sürücüler, kâğıt çıktılar veya diğer bilgisayar sistemlerinde olabilir. Orijinal verinin kaybolmasını önlemek ve verileri yangın, su baskını gibi nedenlerle yedeklemek için bu yedeklemelerin kopyalarını düzenli olarak orijinal verinin tutulduğu yerden daha uzak fiziksel konumlara koymak önemlidir. Ayrıca önemli veriler için RAID sistemleri kullanılabilir çözümlerdir. RAID sistemleri bir verinin kopyasını aynı zamanda başka sürücülere de yazması anlamına gelir. Bir sürücünün arızalanması durumunda, içeriği diğer sürücülerdeki verilerden elde edilebilir.

2.3. Veri Güvenliği

Veri güvenliğine yönelik en önemli tehdit, yasa dışı bilgisayar korsanlarıdır. İçten veya dıştan gelebilecek her türlü güvenlik ihlaline karşı alınması gereken bazı önemli tedbirler bulunmaktadır. Bilgisayarlara parola koymak, önemli doya ve dizinlere erişim izinleri koymak, güvenlik duvarı gibi çözümleri kullanmak, kullanılan yazılımların güvenliğini yamalar ve güncelleştirmeler ile sağlamak, veri tabanlarını güvende tutmak, e-posta gibi güvensiz uygulamalar için gerekli önlemleri almak veri güvenliği için oldukça önemlidir.

Bilgisayarları daha güvenli hale getirmek için yapılması gereken temel işlemlerin listesi aşağıdaki gibidir.

• Bilgisayarın fiziksel güvenliği sağlanmalı

• Yedekleme alınmalı ve sisteminizin olduğundan uzak bir yerde saklanmalı

• Elektrik sorunların karşın kesintisiz güç kaynağı kullanılmalı

• Periyodik olarak virüs kontrolü yapılmalı

• Güvenlik duvarı gibi çözümler kullanılmalı

• İyi ve güvenli parola kullanılmalı

• Düzenli aralıklarla parolaların güncellenmesi

• Kullanılmayan hesapların kaldırılması

• Dosya ve dizin erişimlerinin yapılması

• Önemli dosyaların şifrelenmesi

• Şifrelenmiş e-posta yazılımları kullanılmalı

• İşletim sistemi ve yazılımlara ait yamaların ve güncelleştirmelerin yapılması

• Bilinmeyen yazılımların yüklenmemesi ve izinlerin verilmemesi

• Bilgisayarın kullanılmadığı zamanlarda kapatılması

• Bilgisayarı mümkün olduğunca yönetici (administrator) hesabı ile kullanılmaması

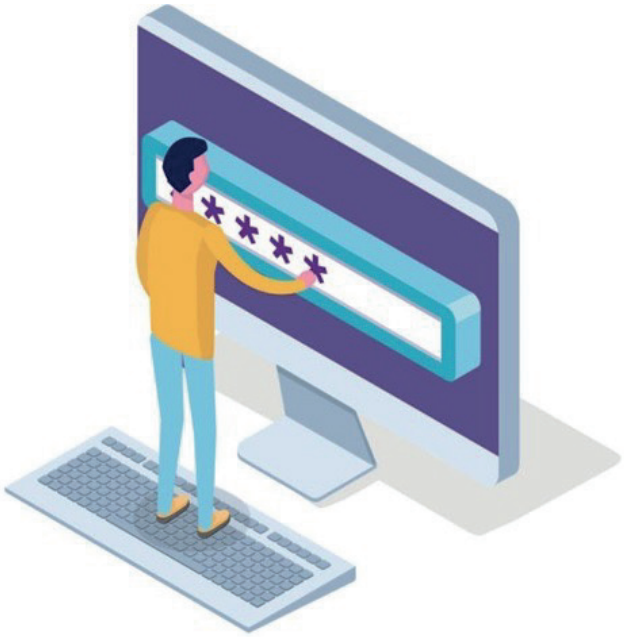
• E-posta adresinizi her web sitesine vermemelidir.

2.4. Parola Güvenliği

Parolalar günümüzde hayatımızda oldukça önemli yer tutmaktadır. Parolalar kimlik doğrulaması için kullanılan en etkili yöntemlerden birisidir. Bilişim teknolojilerinin gelişmesi ile hayatımıza gelen yeniliklerinin tamamına yakınında parolalar kullanılmaktadır. Banka kartlarımızda, internet hesaplarımızda, telefonlarımızda, ev güvenlik sistemlerinde vb. parolaları kullanmaktayız.

DİKKAT EDELİM

Parola ve şifre farklı kavramlar olsa da çoğu zaman birbirinin yerine kullanılır.



Şekil 17 Parola güvenliği

Parolaların kimlik doğrulamasında kullanılması beraberinde önemli bir sorunu meydana getirdiler. Bunların içinde en önemli olarak görünler sorunlar ise; kullanıcıların zayıf veya tahmin edilmesi kolay parolaları seçmeye ve aynı parolaları farklı yerlerde yeniden kullanmaya devam etmeleridir. Dünya üzerinde son on yılda yapılan araştırmalar kullanıcıların en sık tercih ettiği parolaları şu şekilde listelemektedir:

- 123456
- password
- qwerty
- 111111
- 123123
- 987654321
- 123456789
- asdfgh

Her yıl yapılan uyarılara rağmen bu liste pek değişmemiştir. Bunun için kullanıcılara bir takım parola belirleme kuralları tavsiye edilmektedir. Bu kurallar aşağıdaki listede belirtilmiştir.

- Minimum karakterin karşılanması gibi karmaşıklık gereksinimlerin belirlenmesi,
- Daha önceden kullanılan şifrelerin seçilmemesi,
- Parolaların periyodik olarak ve belki de sık sık değiştirilmesi,
- Kullanılan parolaların yukarıdaki listedeki gibi yaygın ve zayıf olarak kullanılan parolalardan seçilmemesi.

Parolaların belirlenmesi ve belirli standartların yakalanması için Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) parola ilkeleri sorununa çözüm getirmeyi amaçlamıştır. NIST parolalar ve bunların nasıl yönetilip saklanması gerektiği hakkında detayları ortaya koymaktadır. Buna göre, olası parolaların yaygın olarak kullanıldığı ve bilinen değerleri içeren bir listeye karşı kontrol edilmesi gerektiği belirtmiştir. Parolaların belirlenmesinde dikkat edilmesi gereken hususlar şunlardır:

- Kullanıcı tarafından sağlanan parolalar en az sekiz alfa numerik karakterden oluşmalıdır.
- Önceki ihlallerden elde edilen parolalar olmamalıdır.
- Sözlük kelimeleri olmamalıdır.
- Doğrum tarihleri gibi 1900-2020 arasındaki tarihler olmamalıdır.
- Tekrarlayan veya sıralı karakterler (örneğin aaaaaa veya 1234abcd) olmamalıdır.
- Hizmetin adı, kullanıcı adı ve bunların türevleri gibi kullanım amacına özgü kelimeler olmamalıdır.

Parolalar belirlenirken yukarıdaki kriterler dikkate alınmalı ve karmaşık yapıdaki parolaların oluşturulması sağlanmalıdır.

Parola Karmaşıklığı

Parola karmaşıklığı, parola belirleme ilklerine bağlı olarak, güçlü bir parola için biz dizi kuralı karşılaması anlamına gelmektedir. Parola karmaşıklığındaki temel kurallar şunlardır.

- Parola, hesap adını veya hesap adındaki varyasyonları içeremez.
- Parola hem büyük harf (A-Z) hem de küçük harf (a-z) içermelidir.
- Parola içinde özel karakterler (~! @ # $% ^ & * _- + = `| \ () {} [] :;” ‘<>,.?/) olmalıdır. (Genellikle ALT tuşu ile çıkan karakterlerdir. Ancak Euro gibi para birimi simgeleri, özel karakter olarak sayılmaz.).
- En az karakter sayısına uyulmalıdır. Bu değer sistemden sisteme, kullanıcıdan kullanıcıya değişebilir. En az parola uzunluğu 8 karakter olması gerekirken tavsiye edilen karakter sayısı 12’dir.

Parolalar yukarıda sıralanan kurallara göre en az 8 karakter ile oluşturulduğunda, tek bir parola için en az 218.340.105.584.896 farklı olasılık anlamına gelir. Oluşturulan parolanın olasılığı kaba kuvvet saldırısını oldukça zorlaştırır, ancak parolanın kırılması yine de imkânsız değildir. Kırılması neredeyse imkânsıza yakın bir parola için, parola karakter sayısını artırmak gereklidir. Minimum karakter sayısı artarsa, parolanın kırılma süresi de artar.

Parola karmaşıklığının sağladığı yararların yanı sıra bazı zorlukları da beraberinde getirmektedir. Bunların başında parolanın unutulması gelir. Daha uzun ve içinde özel karakterlerin bulunduğu bir parolayı hatırlamak zordur. Hele bir de tüm parolalar farklı farklı olduğunda hatırlamak ve diğerleri ile karıştırmamak oldukça zor bir olaydır. Bu nedenle parolalar oluşturulurken belirli bir mantık takip edilmelidir.

Örneğin;

Ben Dört Çocuklu Bir Ailenin 3. Bireyiyim!

gibi bir cümleyi kendi gerçek yaşamınızdan yazabilirsiniz. Cümlenin ilk karakterleri ve özel karakterleri alındığında Bdcba3.B! gibi bir parola elde etmiş olunur.

Bu Web Sitesine (eğitim ile ilgili) 20 Aralık günü üye oldum.

gibi bir cümleyi üye olduğunuz bir web sitesinin ilgi alanına ve üyelik tarihine göre özelleştirebilir ve unutmamanızı sağlayabilirsiniz. İlk karakterleri ile özel karakterleri alındığında BWS(eii)20Aguo. gibi bir parola elde etmiş olunur.

Güçlü parola oluşturmak için farklı teknikleri de kullanabilirsiniz. Bunlardan birkaçına dair örnekler aşağıda verilmiştir.

Cümleler olduğu gibi yazılarak güçlü parola oluşturulabilir. Örneğin;

Bu Web Sitesine 4.Nisanda Python Ogrenmek icin uye oldum.

Siber Guvenlik dersini 13:30'a koymuşlar.

Benzer rakam ve harfleri birbirinin yerine kullanarak güçlü parolalar oluşturulabilir. Örneğin;

O yerine 0, L yerine 1, Z yerine 2, E yerine 3, S yerine 5, G yerine 6, B yerine 8 yazılarak;

Leylek = 13y13k

MorMenekşe = M0rM3n3k53

Zonguldak = 20n6u1dak

Bazı kelime veya karakterlerin yerine özel karakter kullanarak güçlü parolalar oluşturulabilir. Örneğin;

Yağmur yerine "" işareti, yüz yerine %, ve yerine &, ş yerine $, ı-i yerine !, boşluk yerine * yazılarak;

Yarın Yağmur yağacakmış = Yar!n""ya6acakm!$

Yüzmeyi severim = %mey!*sever!m

Parola için oluşturduğunuz cümledeki sadece sesli veya sadece sessiz harfleri kullanarak güçlü parolalar oluşturabilirsiniz. Örneğin;

Bu vatan 1 bütündür. = Bvtn1btndr.

Atam 30 Agustos'da zaferi ilan etti. = Aa30auo'azeiiaei.

Parola Güvenliğini Sağlama

Günümüzün çevrimiçi ortamında, güvenliğe yönelik basit "kullanıcı adı ve parola" yaklaşımı, siber suçlular için kolay bir avdır. Birçok oturum açma işlemi dakikalar içinde tehlikeye atılabilir ve özel veriler kötü niyetli kişilerin ellerine geçebilir.

Parolaların tahmin edilerek veya daha farklı yöntemler kullanılarak başkaları tarafından ele geçirilmesini engellemek için parolaların güvenliğinin sağlanması gerekmektedir. Bunlar için yapılması gereken hususlar şunlardır.

1. Gizli sorular ile güvenceye alma

2. İki aşamalı doğrulama yöntemi kullanılması

3. Biometrik kimlik doğrulama kullanılması

Gizli Soru

Güvenlik soruları, bir kullanıcının parolasını unutması veya çok faktörlü kimlik doğrulama (MFA) gerektiğinde ikincil kimlik doğrulama faktörlerini kaybetmesi durumunda hesabına yeniden erişim sağlamasına olanak sağlamak için birçok web sitesi tarafından kullanılır. Bununla birlikte, genellikle parolalardan çok daha zayıf bir kimlik doğrulama biçimidir.

Yeni bir çevrimiçi hesap oluşturulduğunda, web siteleri genellikle kullanıcıdan güvenlik sorularını yanıtlamalarını ister, böylece bir kullanıcı kendi kimliğini doğrulaması istenirse parolayı girecek, hatırlamaması durumunda kendisini kanıtlaması için güvenlik sorularını soracaktır. Bu sorular arasında

"Annenizin kızlık soyadı nedir?" , "Hangi şehirde doğdunuz?" veya "Gittiğiniz ilkokulun adı nedir?" gibi sorular yer almaktadır.

Şekil 18 Güvenlik soru ve cevap arayüzü

Maalesef web sitelerine üyelik veya hizmet alımı sırasında buna benzer çevrimiçi güvenlik sorularını doğru olarak yanıtladığınızda bu işlemin yeterli bir güvenli durum olmadığını söylemek gerekir. Bunun nedeni, hesabınıza erişmek isteyen birinin yanıtları bulmak için kolayca İnternet araştırması yapabilmesidir. Sosyal medya hesaplarınızı inceleyen saldırgan bilgisayar korsanı dayınıza yazdığınız bir mesaja ulaşabilir ve dayınızın soy isminden annenizin kızlık soyadını bulabilir.

Bir kullanıcının kimliğini doğrulamak için tek bir mekanizma olarak güvenlik sorularına güvenilmemelidir. Bir öneri olarak, "hangi şehirde doğdunuz?" gibi bir parola hatırlatma sorusuna ilk kayıt esnasında şehir adı olmayan ancak hatırda kalınabilecek bir ifade yazılabilir.

İki Aşamalı (Faktörlü) Doğrulama

İki faktörlü kimlik doğrulama (2FA), bir sisteme erişmek için iki farklı tanımlama biçimi gerektiren bir güvenlik sistemidir. Çevrimiçi bir hesabın, akıllı telefonun veya bir kapının güvenliğini güçlendirmek için iki faktörlü kimlik doğrulama kullanılabilir. Bu doğrula sistemi güvenli olan veriye veya sisteme erişilmeden önce kullanıcıdan iki tür bilgi talep ederek yapar. Bu bilgiler bir parola veya kişisel kimlik numarası (PIN), kullanıcının akıllı telefonuna gönderilen bir kod (SMS gibi) olabilir.

Yeni bir cihazda ilk kez oturum açılmak istenildiğinde, şifre ile telefon numaranıza gönderilen 4-8 basamaklı doğrulama kodu olmak üzere iki bilgi sağlanması gerekir. Kodu girilerek yeni cihaza güvenildiği doğrulanmış olur.

İki faktörlü kimlik doğrulama, yetkisiz kullanıcıların çalıntı bir parola kullanarak bir hesaba erişim sağlamasını önlemek için tasarlanmıştır. Kullanıcılar, özellikle aynı parolayı birden fazla web sitesinde kullanırlarsa, parolaların ele geçirilmesi konusunda büyük bir risk altında olabilirler.

İki faktörlü kimlik doğrulama, aşağıda verilen iki tekniğin birleşimidir:

• Bildiğiniz parolanız

• Sahip olduğunuz bir bilgi veya akıllı telefonunuza veya başka bir cihaza gönderilen bir kod içeren bir metin (veya bir akıllı telefon kimlik doğrulama uygulaması gibi).

2FA güvenliği artırsa da parolanın güvenliği için kusursuz değildir. Bilgisayar korsanları yine de hesaplara yetkisiz erişim elde edebilir. Bunu yapmanın yaygın yolları arasında kimlik avı saldırıları, hesap kurtarma prosedürleri ve kötü amaçlı yazılımlardır.

Biometrik Kimlik Doğrulama

Biyometrik kimlik doğrulama, kişinin kendisini kanıtlaması ve doğru kişi olduğunu ispatlamak için bireyin eşsiz biyolojik özelliklerine dayanan bir güvenlik sürecidir. Biyometrik doğrulama sistemleri, elde edilen biyometrik veriyi veri tabanındaki kayıtlı, depolanmış ve daha önceden onaylanmış gerçek verilerle karşılaştırır. Elde edilen biyometrik veri örneği ile kayıtlı olan biyometrik veri eşleşirse, kimlik doğrulaması onaylanır. Kişiye özgü olan bu biyometrik veriler unutulamaz veya kaybedilemez, taklit edilemez olmaları, bu kimlik doğrulamayı diğer yöntemlerden ayırır. Ancak son derece özel olan biyometrik kişisel bilgilerin kullanılıyor olması, siber güvenlik açısından önem gösterilmesini gerektirir.

Biyometrik kimlik doğrulama yöntemleri, birden fazla biyometrik deseni birleştirerek veya biyometrik doğrulamayı tamamlayan geleneksel bir şifre veya ikincil cihazla birlikte iki faktörlü kimlik doğrulama (2FA) veya çok faktörlü kimlik doğrulama (MFA) biçimi olarak da kullanılabilir.

Günümüzde yaygın olarak kullanılan biyometrik kimlik doğrulama teknolojileri şunlardır:

Parmak izi tarama: Parmak ucunda yer alan izlerin modelinde belirli özellikleri arayarak kimlik doğrulama yapar. Harici bir özelliğe sahip bir görüntüyü yakalamanın dezavantajı, bu görüntünün kodlanmış biçimde saklansa bile kopyalanabilmesidir. Parmak izleri, taklit edilebilen bir kimlik doğrulama yöntemidir. Bazı parmak izi çizgi modelleri o kadar benzerdir ki pratikte bu yüksek bir yanlış kabul oranına neden olabilir.

Retina taramaları, bireyin iç gözünü kaplayan ışığa duyarlı yüzeyde kan damarı deseninin bir görüntüsünü üretir.

İris tanıma: İnsanın göz bebeğinin etrafında yer alan benzersiz halkadaki desene göre yapılan kimlik doğrulamadır. Bir iris taraması gerçekleştirildiğinde, tarayıcı bir irisin benzersiz özelliklerini okur ve bunlar daha sonra şifrelenmiş bir koda dönüştürülür. İris taraması, özellikle kızılötesi ışık kullanılarak yapıldığında çok iyi sonuçlar vermektedir.

Parmak damar kimliği ve avuç tanıma: Bir insanın parmağında yer alan ve benzersiz olan damar desenine göre yapılan bir kimlik doğrulamadır. Damar deseni tanıma durumunda, parmaktaki damarların bitiş noktaları ve çatallanmaları bir görüntü biçiminde yakalanır, sayısallaştırılır ve şifreli bir koda dönüştürülür.

Yüz tanıma sistemleri: Bu sistemler, bir eşleşme belirlemek için yüzün farklı bölümlerinin şeklini ve konumunu analiz ederler. Bununla

birlikte, yüz tanımanın bir takım önemli dezavantajları da vardır. Örneğin bir kişinin tanımasını mümkün kılmak için genellikle doğrudan kameraya bakması gerekir.

Ses tanıma sistemleri, daha değişken koşullardan ziyade konuşmacının ağzının ve boğazının şekli tarafından oluşturulan özelliklere dayanır.

Biyometrik sahtekârlık, başka bir kişi olarak tanımlanmak amacıyla sahte bir biyometrik özelliğin sunulmasıdır. Bu, kopyalanmış bir parmak izi veya tahrif edilmiş iris modeline sahip bir kontakt lens kullanmayı içerebilir.

2.5. Parola Kırma Teknikleri

Parola kullanımı, kimlik doğrulama sistemlerinde en sık kullanılan yöntemdir. Kullanıcı ya da bir ağ cihazı, doğru parolayı kimlik doğrulayıcıya sunabilirse, iddia ettiği kullanıcı ya da cihaz olduğunu ispat etmiş olur. Parola, kimliğin ispatı olduğundan güvenliği ve gizliliği son derece önemlidir. Ancak tehdit aktörleri, parolayı elde etmeye yönelik oltalama saldırılarından, tersine mühendislik yöntemlerine kadar çok çeşitli yöntemler kullanırlar. Temel olarak parolayı elde etme yöntemleri "parola kırma (password cracking)" olarak adlandırılır.

Parola tahmin etme

Saldırgan açısından, uygulaması en kolay olan parola kırma tekniğidir. Hedef kullanıcı hakkında bilgi toplandıktan sonra, doğum tarihi, memleketi, tuttuğu futbol takımı gibi kişisel bilgilerden yola çıkarak parola tahmini yapılır. Bu kategorideki diğer bir yöntem de, en sık kullanılan "qwerty" veya "123qwe" parolaların denenmesidir. Yine bu kısımda ele alınabilecek diğer bir husus olarak, aynı parolanın farklı yerler için de kullanılması ile ilgilidir. Eğer kullanıcı her yerde aynı parolayı kullanıyorsa ve bu kullanım alanlarından birinde parola kırılmışsa, saldırganın ilk yapacağı aynı parolayı farklı noktalar için denemek olacaktır.

Sözlük saldırıları

Brute force (kaba kuvvet ya da deneme yanılma) saldırılarında kullanılan yöntemdir. Bir yazılım tarafından belirli bir kelime listesinde (sözlük) yer alan parolaların sıralı olarak denenmesi mantığına dayanır. Bu sözlük, en sık kullanılan gerçek kelimeleri içerdiği gibi, "Ankara06" ve "Passw0rd1" gibi yine sık kullanılan parolalardan da oluşabilir. Tehdit aktörleri, bu listelere internet ortamından rahatlıkla ulaşabilmektedir. Sözlük saldırısı kategorisinde yer alabilecek diğer bir yöntem de, karakter üreteçleri kullanarak kendi özelleştirilmiş listelerini oluşturmak ve bu oluşturulan liste üzerinden deneme yanılma saldırısı yapmaktır. Bu yöntem hem parola üretmek hem de denemek olarak iki kısımdan oluştuğu için uzun zaman alabilir. Kullanıcılar unutmamak için genellikle kısa parolalar kullandıklarından, bu saldırılar oldukça başarılı saldırılardır.

Önceden hesaplanmış parola listeleri

Daha önce ifade edildiği gibi, parolalar veritabanlarında genellikle özetlenerek (hash) saklanır. Bir şekilde bu veritabanı eğer saldırgan tarafından eşe geçirilmişse, parola açık olarak veri tabanında yer almayacaktır. MD5 ve SHA gibi özetleme fonksiyonları tek yönlü matematiksel fonksiyon olduklarından, hash değerinden parolanın ham haline ulaşmak tersine mühendislik yöntemi ile mümkün değildir. Ancak, bu durumda saldırgan önceden hesaplanan hash değerlerinin yer aldığı listelerden yola çıkarak parolanın ham haline ulaşabilir (rainbow table attacks). Ancak bu yöntemin başarılı olabilmesi için, parolanın bu listede önceden yer alıp özetlenmiş olması gerekir. Sık kullanılan kelimeler (ya da parolalar)

bu listede çok büyük ihtimalle yer aldığından, kırılması muhtemeldir. Bu nedenle, parolanın tek başına özetlenmiş olarak veritabanında kaydedilmesi yeterli bir güvenlik önlemi değildir, parolanın seçimi de son derece önemlidir.

Parolaların şifrelenmesi, özetlenmesi ya da veritabanına çeşitli tekniklerle kaydedilerek güvenliğinin sağlanması önemli bir konudur. Ancak tüm bu parola güvenlik çabalarını riske atabilecek bir durum vardır, kullanıcının hafızasında yer alan bu parola bilgisini bilinçli ya da bilinçsiz olarak saldırgana vermesidir. Saldırganlar son derece etkili sosyal mühendislik teknikleri (senaryoları) ile bu parolaları elde etmek için uğraşabilirler. Oltalama saldırıları ile bu işlem yapılabildiği gibi, yetkili bir otorite gibi görünerek parolayı kullanıcıdan isteyebilirler. Kullanıcı, parola girdiği her yere dikkat etmeli ve parolayı kesinlikle hiç kimseye vermemelidir.

3. GÜVENLİK ZAAFİYETİ DERECELENDİRME

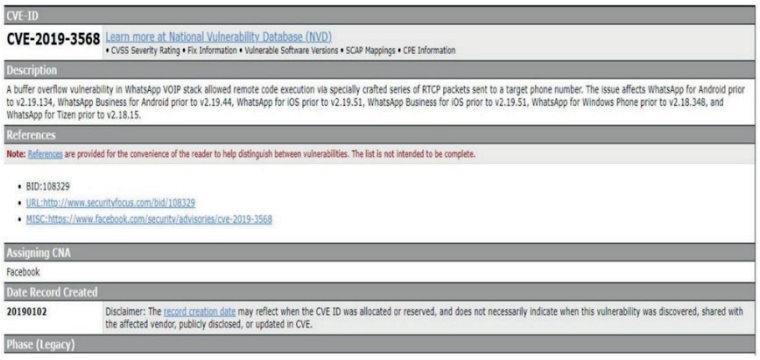
Siber güvenlikte amaç, sistemleri ve kullanıcıları tehdit aktörlerinin kötü amaçlı saldırılarına karşı korumaktır. Saldırılar, teknik, mantıksal veya fiziksel olabilen güvenlik açıklarını hedefler. Risk yönetimi gereği tüm potansiyel tehditler ele alınmalı ve güvenlik açısından riskleri tehdidin önemine göre ele alınmalıdır. Zararlı yazılımların resmi bir isimlendirme kural yapısı yoktur. Zararlı yazılımların bilinen isimleri, genellikle tehdidi tanımlayan araştırmacılar tarafından verilmiş isimlerdir. Bu başlıkta güvenlik tehditleri ve zafiyetlerin tanımlanmasında kullanılan isimlendirme ve zaafiyet derecelendirmesi ele alınacaktır.

3.1. CVE İsimlendirmesi

Siber güvenlik dünyasında bir güvenlik açığıyla ilişkili riski derecelendirmek ve bu güvenlik açığı hakkında iletişim kurmak için bir isimlendirme ve puanlama sistemi kullanılır. Bu sayede, siber güvenlik tarafları aynı güvenlik açığı hakkında herhangi bir kafa karışıklığı olmadan iletişim kurabileceklerdir.

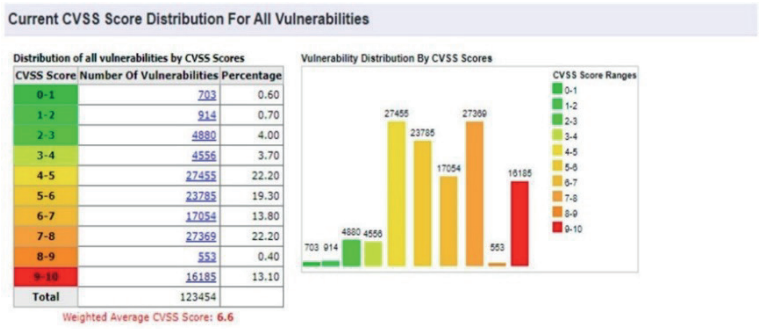
CVE (Common Vulnerabilities and Exposures), Ortak Güvenlik Açıkları ve Etkilenmeler sistemi, genel olarak bilinen bilgi güvenliği açıkları ve riskleri için bir referans yöntemi sağlar. Belirli tanımlamalara göre güvenlik zafiyetlerinin tutulmasını sağlayan bir isimlendirme veri tabanıdır. Bu veri tabanına https://cve.mitre.org/ sitesinden ulaşılabilir.

CVE yapısında, 1999 yılından itibaren tespit edilen güvenlik açıklarını listelemek için bir isimlendirme kuralı geliştirmiştir. Buna göre tespit edilen açık, CVE-YYYY-NNNN olarak isimlendiriliyordu. YYYY tespit edilen yılı, NNNN ise güvenlik açığına verilen numarayı gösterir. Ancak daha sonra bu isimlendirme geliştirildi. Aynı web sayfasından yeni isimlendirme kuralına bakılabilir. Örneğin Şekil 19'daki ekran görüntüsünde, CVE-2019-3568 numaralı WhatsApp uygulamasına yönelik bir güvenlik açığı listelenmektedir.



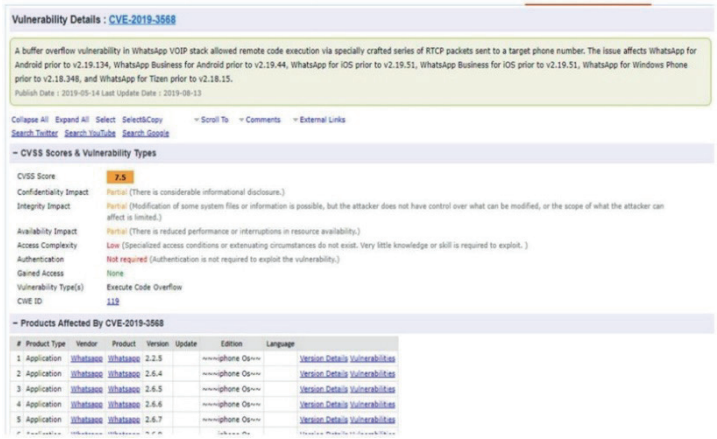
Şekil 19 Örnek CVE ekranı

Belirli bir CVE ile ilişkili daha fazla ayrıntılı bilgi için https://www.cvedetails.com/ sayfası ziyaret edilebilir.



Şekil 20 Zafiyete ilişkin CVE skor belgesi

CVE-2019-3568 numaralı güvenlik açığına ilişkin detaylı incelemenin ekran görüntüsü Şekil 3.21'de gösterildiği gibidir.



Şekil 21 CVE detay ekranı

Güvenlik açığına ilişkin detaylı bilgilerin sunulduğu bu sayfada, güvenlik açığının açıklaması, güvenlik açığı türü, etkilenen ürünler, zaafiyetin karmaşıklığı gibi bilgilerin yanı sıra, güvenlik açığının derecesini belirten CVSS skoru da yer almaktadır (Örnekte 7.5).

3.2. Zafiyet Derecelendirmesi (CVSS)

CVSS, Ortak Güvenlik Açığı Puanlama Sistemi (Common Vulnerability Scoring System) olarak adlandırılan ve bir güvenlik açığının (güvenlik zafiyetinin) derecelendirilmesi için kullanılan bir sistemdir. Sistemde güvenlik açığının önem düzeyine göre, kompozit metrikler kullanılarak 0 (en az tehlikeli) ile 10 (en çok tehlikeli) arasında puanlama yapılır.

Puanlama birden fazla parametreye bakılarak hesaplanır. CVSS puanlama yapısı birkaç kez değişmiştir. Günümüzde kullanılan en güncel puanlama sürümü, 2019 yılı haziran ayından beri kullanılan CVSSv3.1 sürümüdür.

CVSSv2 puanının hesaplanmasında temel puanlama (base), zamansal puanlama (temporal) ve çevresel (environmental) puanlama olmak üzere üç ölçüt (metric) kullanılmaktadır.

Şekil 22 CVSS Base Score Metrikleri

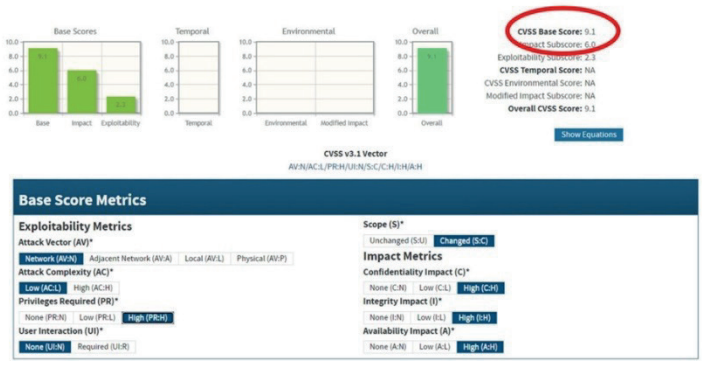
Temel puanlamada, siber güvenliğin temel bileşenleri (C-I-A) bir alt grupta, saldırı vektörü, erişim karmaşıklığı ve kimlik doğrulama da diğer bir alt grupta hesaplamaya katılır.

Erişim vektöründe yer alan "Lokal Erişim (Local)" istismarın ağ üzerinden yapılamayacağını, sadece yerel cihazdan yapılabildiğini belirtir. "Bitişik Ağ (Adjacent Network)" ifadesi saldırının aynı ortamda bulunan, aynı mantıksal ağdan yapılabildiğini belirtir. "Ağ (Network)" ifadesi ise, internet gibi farklı ağ üzerinden (ya da farklı VLAN üzerinden) yapılabildiğini belirtir. Bu durum, güvenlik açığı puanının daha yüksek olduğu anlamına gelir.

Zafiyetin erişim karmaşıklığı (access complexity) için düşük, orta ve yüksek ölçekler kullanılmaktadır. Karmaşıklık düzeyinin artması, zafiyetin puanını arttır.

Kimlik doğrulamada (Authentication) ise çoklu doğrulama (Multiple), tek doğrulama (Single) ve doğrulama yok (None) olmak üzere yine üç farklı ölçüt kullanılmaktadır. Çoklu kimlik doğrulamada, zafiyetin birden fazla kez kimlik denetiminden geçildikten sonra gerçekleşebileceği belirtilir. Her kimlik doğrulama bir güvenlik olduğundan, çoklu kimlik doğrulamaya sahip bir zafiyet düşük puanlı olmasını sağlar. Tek kimlik doğrulama ise, zafiyetin gerçekleşmesi için sadece bir kez kimlik doğrulamadan geçilmesinin yeterli olduğu anlamına gelir. Kimlik doğrulamanın olmaması, bu alt metrik için en tehlikeli olanıdır.

Aynı şekilde derecelendirmede gizlilik (confidentiality), bütünlük (integrity) ve kullanılabilirlik (availability) parametrelerinin her biri için üç düzey belirlenmiştir. CVSSv3.1 için güncellenmiş puanlama ölçütleri https://nvd.nist.gov/vuln-metrics/cvss/v3- calculator adresinde yer almaktadır.



Şekil 23 CVSS skor hesaplama

CVSSv3.1 için yukarıdaki bağlantıda yer alan hesaplama aracı kullanılarak, parametrelerin değişiminin CVSS skoruna etkisi görülebilir. Şekil 23'deki ekran görüntüsünde, CVSS temel metrik skoru 9,1 olarak belirlenen bir güvenlik zafiyetinin özellikleri görüntülenmektedir. Aynı araç kullanılarak, zamansal puanlama (temporal) ve çevresel (environmental) puanlama hesaplanabilir.

4. GÜVENLİK YAZILIMLARI

Önceki bölümlerde ele alındığı gibi ağlar siber saldırıların hedefidir. Ağları korumak için ağ düzeyinde koruma sağlayan IPS, IDS, güvenlik duvarları gibi sistemler kullanılır. Aynı şekilde son kullanıcı cihazlarında da kullanılabilecek güvenlik yazılımları vardır. Bazı güvenlik çözümleri birden fazla bileşen de içerebilir. Örneğin hem antivirüs hem de anti-malware aynı yazılımda sunulabilir.

4.1. Antivirüs

Virüsleri tespit etmek ve sistemden kaldırmak için bir hoşta yüklenen programlardır. Windows Defender, Norton Security, McAfee, Trend Micro gibi birçok antivirüs yazılımı bulunmaktadır. Antivirüsler genellikle daha önceden antivirüs üreticileri tarafından tespit edilen ve zararlı yazılımın karakteristik özelliklerini (imzaları) kaydeden veri tabanı yapısını kullanırlar. İmza veri tabanının sürekli olarak güncel tutulması bu nedenle önemlidir. Birçok antivirüs programı, verileri analiz ederek gerçek zamanlı koruma da sağlayabilir. Bu programlar aynı zamanda sisteme gerçek zamanlı olarak tanınmadan önce girmiş olabilecek mevcut zararlı yazılımları da tarar.

Yazılım olarak kullanılan konak tabanlı antivirüs koruması, ajan tabanlı antivirüs olarak da bilinir. Ajan tabanlı antivirüs, korunan her makinede çalışır ve merkezi bir sistemden tarama gerçekleştirir. Aracısız sistemler, aynı anda bir bilgisayarda birden çok işletim sistemi örneğinin çalıştığı sanallaştırılmış ortamlar için popüler hale gelmiştir. Sanallaştırılmış her sistemde çalışan ajan tabanlı antivirüs, sistem kaynakları üzerinde ciddi bir yük oluşturabilir.

4.2. AntiMalware

Günümüzde anti-virüs yazılımları ile birlikte entegre olarak çalışan yazılımlardır. Bu programlar, üç farklı yaklaşım kullanarak virüsleri algılayabilir. İmza tabanlı yaklaşımda, bilinen zararlı yazılım dosyalarının çeşitli özelliklerini (imzalarını) tanır. Sezgisel tabanlı yaklaşımda, çeşitli zararlı yazılım türleri tarafından paylaşılan genel özellikleri tanır. Davranış temelli yaklaşımda ise şüpheli davranışların analizini kullanır.

4.3. Konak Tabanlı Güvenlik Duvarı

Yazılımsal güvenlik duvarı, sistemi kötü amaçlı yazılımlardan, solucanlardan, virüslerden ve e-posta eklerinden korumayı amaçlayan konak tabanlı güvenlik duvarı programlardır. Genellikle konak bilgisayardan çıkan ve konak bilgisayara giren belirli protokollerin filtrelenmesini sağlamak üzere geliştirilmişlerdir.

4.4. Diğer Yazılımlar

Gelişmiş Kötü Amaçlı Yazılım Koruması (AMP)- Virüslere ve kötü amaçlı yazılımlara karşı uç nokta koruması sağlar.

E-posta Güvenlik Aracı (ESA)- SPAM ve potansiyel olarak kötü niyetli e-postaların uç noktaya ulaşmadan önce filtrelenmesini sağlar.

Web Güvenlik Aracı (WSA)- Konakların web üzerindeki tehlikeli konumlara ulaşmasını önlemek için web sitelerinin filtrelenmesini ve kara listeye alınmasını sağlar. Kullanıcıların internete nasıl eriştiğini kontrol eder ve kabul edilebilir kullanım politikalarını uygulayabilir, belirli sitelere ve hizmetlere erişimi kontrol edebilir ve zararlı yazılım taraması yapabilir.

Ağ Kabul Kontrolü (NAC)- Yalnızca yetkili ve belirli kriterlerin sağlandığı (örneği işletim sisteminin güncel olması) sistemlerin ağa bağlanmasına izin verir.

5. GÜVENLİK OPERASYONLARI MERKEZİ

Güvenlik operasyonları merkezi (Security Operations Center – SOC), kurumsal ve teknik düzeyde güvenlik sorunlarıyla ilgilenen merkezi bir birimdir (digitalguardian.com, 2023). Güvenlik Operasyon Merkezi, siber tehditleri önlerken, saldırıları tespit eder, ağı analiz eder ve olası tehditlere yanıt verir. Daha genel bir ifade ile bir kuruluşun güvenlik duruşunu sürekli olarak izlemek ve iyileştirmek için insanları, süreçleri ve teknolojiyi kullanan kuruluş içindeki merkezi bir işlevdir.

SOC, birbiri ile uyum içinde çalışan birimlerden ve teknolojilerden oluşan bir merkezi nokta olarak ele alınabilir. Bir kurumda SOC yapısının bulunması, ağın daha geniş bir ifade ile kurumdaki varlıkların sürekli izlenmesini sağlayarak, saldırı öncesi, saldırı anı ve saldırı sonrası eylemlerin gerçekleştirilerek potansiyel (veya devam eden) tehditlerin ortadan kaldırılmasını sağlar. SOC yapısının varlığı sadece kurumun fiziksel varlıklarını değil, iş döngüsünü, süreci ve yapıyı da korur.

Şekil 24 SOC bileşenleri

5.1. SOC Fonksiyonları

Güvenlik Operasyonları Merkezi, her biri son derece önemli olan ile ilişkili birçok fonksiyonlardan oluşur. Bu fonksiyonların yürütülmesi, ağın daha fazla güvenli olmasını sağlayacaktır. Aşağıda bu fonksiyonlardan bazıları ele alınmıştır (mcafee.com, 2023).

1. Mevcut Kaynakların Listesini Alma: SOC, farkında olmadığı ya da varlığından habersiz olduğu kaynakları koruyamaz. Bu nedenle kurumda korunması gereken kaynakları ve varlıkların belirlenmesi ile bu kaynakların nasıl korunacağının belirlenmesi gerekir. Bu aşama aynı zamanda saldırı yüzeyinin ve saldırı vektörlerinin de tanımlanmasını sağlar. Savunma esasında kullanılabilecek donanımların, yazılımların ve araçların varlığının tespiti bu fonksiyon içerisinde ele alınır.

2. Hazırlık ve Önleyici Bakım: Ağlar için en tehlikeleri saldırılardan birisi, sıfırıncı gün olarak bilinen saldırılardır. Bu tür saldırılardan korunmanın en önemli yöntemlerinden biri, hazırlık yapma ve önleyici bakım yapmaktır. SOC ekibinin, güncel saldırıları takip etmesi gerektiği gibi en güncel güvenlik gelişmelerini de takip etmesi gerekir. Ancak yine de saldırı gerçekleşebilir. Bu nedenle olası bir saldırı durumunda, felaket kurtarma planının bulunması gerekir. Önleyici bakım olarak, tüm sistemlerin güncel olduğu sağlanmalıdır. Yine sistemdeki beyaz liste (kabul edilebilir) ya da kara listenin de (kabul edilemez) bu doğrultuda güncellenmesi gerekebilir. Aynı şekilde personelin de periyodik olarak eğitimler ile bilgilendirilmesi gerekir.

3. Sürekli Proaktif İzleme: Saldırının ne zaman gerçekleşeceği bilinmez. Bu nedenle anormal bir durum oluşup oluşmadığının belirlenmesi için varlıkların sürekli olarak izlenmesi gerekir. Ağdaki günlük dosyalarının, mesajların ve olayların izlenmesini sağlayan SIEM yazılımları bu amaç doğrultusunda kullanılır.

4. Uyarı Sıralaması ve Yönetimi: Ağın izlenmesi sırasında çok farklı düzeyde ve önemde tehditler yakalanabilir. SOC analistinin görevi, uyarılara göre tehditleri önem sırasına dizmek ve acil eylem gerekenler ile diğerlerini birbirinden ayırt edebilmektir.

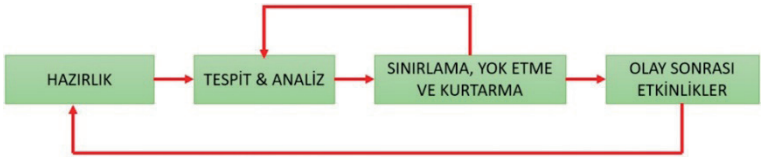
5. Olay Müdahale: Tehdit ya da saldırının gerçekleştiği anlaşıldığı anda yapılması gerekenleri ifade eder. Genellikle ilk verilen tepki, saldırının yayılmasını önlemek amacıyla izolasyon sağlamaktır. Zararlı yazılımın tespit edilip silinmesi, zararlı işlemin durdurulması ve zararlı dosyanın silinmesi bu aşamada gerçekleşir. Hedef izole edildikten sonra tüm ağ tekrar analiz edilir.

6. Kurtarma ve İyileştirme: Saldırı gerçekleştikten sonra mümkün olan en kısa sürede sistemin tekrar devreye alınması gerekir. Geciken her süre, itibar ve parasal kayıp olarak yorumlanabilir. Sistem yapılandırmalarının düzenlenmesi, yedeklerin yüklenmesi gibi işlemler bu fonksiyonun sorumluluğundadır.

7. Log Yönetimi: SOC için belki de en önemli işlemlerdendir. Sistemdeki tüm kaynaklardan gelen loğların ve olayların SIEM yazılımları ile yönetimini ifade eder. Hem saldırı öncesi hem de saldırı sonrası ayrı ayrı incelenmesi gereken bir durumdur. Saldırı öncesinde anomali tespiti yapılması bir örnek olarak verilebilir. Aynı şekilde saldırı sonrasında, saldırının nasıl gerçekleştiğinin ve etkisinin analizi de yine bu fonksiyonun sorumluluğundadır.

5.2. Olay Müdahale Yaşam Döngüsü

Bir saldırıya hazırlıklı ve planlı olmak önemlidir. Olay müdahalesi bir kez gerçekleşen bir durum değil, her zaman gelişen bir döngüdür. Bu yöntemlerden biri de Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından belirlenen, olay müdahale yaşam döngüsüdür.



Şekil 25 .Olay Müdahale Yaşam Döngüsü

Hazırlık, olay müdahale ekibinin bir olaya nasıl müdahale edecekleri konusunda eğitimi aşamasıdır.

Tespit ve Analiz- Sürekli izleme yaparak, bir olayı hızla tanımlar, analiz eder ve doğrular.

Sınırlama, Yok Etme ve Kurtarma- Tehdidi kontrol altına almak, kurumsal varlıklar üzerindeki etkiyi ortadan kaldırmak, verileri ve yazılımı geri yüklemek için yedekleri kullanmak gibi işlemleri uygular. Daha fazla bilgi toplamak veya araştırmanın kapsamını genişletmek için tespit ve analize geri dönebilir.

Olay Sonrası Aktiviteler- Daha sonra olayın nasıl ele alındığının belgelenmesidir. Gelecekteki müdahale için güncellemeler önerir ve bir tekrar oluşmasının nasıl önleneceğini belirtir.

BÖLÜM ÖZETİ

Saldırı ve savunma için bilgi toplama yöntemleri, pasif ve aktif olmak üzere iki kategoriye ayrılır. Pasif Bilgi Toplama, doğrudan etkileşim olmadan, internet kaynaklarından bilgi toplanmasıdır. Örnekler arasında IP adresleri, domainler ve web sayfaları hakkında bilgi toplama yer alır. Aktif Bilgi Toplamada ise hedef sistemle doğrudan iletişime geçilerek yapılan, riskli bilgi toplama yöntemidir. Network mapping ve WireShark gibi araçlarla ağ haritalaması ve paket analizi yapılabilir. Ayrıca fiziksel güvenlik, veri bütünlüğü ve veri güvenliği gibi temel güvenlik önlemleri ve parola güvenliği hakkında bilgiler sunulmuştur. Parola karmaşıklığı ve güvenliğini sağlama yöntemleri detaylandırılmıştır. Bunun yanında siber güvenlikte zafiyetlerin derecelendirilmesi açıklanmıştır. Bu derecelendirme tehditlerin ciddiyetini ve aciliyetini belirlemek için kullanılır. Zafiyetlerin etkisini değerlendirmek için kullanırlar. Kritik Zafiyet Skorlama Sistemi (CVSS) açıklanmıştır. Bu sistem, zafiyetlerin teknik özelliklerine ve potansiyel etkilerine göre puanlama yapar. Zafiyetlerin tespiti, değerlendirilmesi ve giderilmesi süreçlerini içeren Zafiyet Yönetimi süreci de açıklanmıştır. Bu süreç, organizasyonların güvenlik duruşunu güçlendirmek için kritik öneme sahiptir.

GÖZDEN GEÇİRELİM

1. **Siber güvenlikte pasif bilgi toplama sürecinde hangi bilgiler toplanabilir?**
   a) Yalnızca IP adresleri
   b) Domain bilgileri ve web sayfaları
   c) Yalnızca Whois sorgusu sonuçları
   d) IP adresleri, domain bilgileri ve web sayfaları

2. **Whois sorgusu ne amaçla kullanılır?**
   a) Web sayfasının aktif olup olmadığını öğrenmek
   b) Alan adı sahibinin iletişim bilgilerine ulaşmak
   c) IP adreslerinin dağıtımını yapmak
   d) Ağ güvenliği analizi yapmak

3. **RIPE NCC ne iş yapar?**
   a) Alan adı sorgulama
   b) Avrupa ve Ortadoğu bölgesine IP adresi dağıtımı
   c) Güvenlik duvarı hizmetleri
   d) Parola güvenliği sağlama

4. **Bir web sayfasının aktif olup olmadığını öğrenmek için hangi araç kullanılır?**
   a) Whois sorgusu
   b) RIPE NCC
   c) ns.tools
   d) Shodan

5. **Shodan arama motoru ne için kullanılır?**
   a) Domain bilgilerini sorgulamak
   b) İnternete bağlı cihazları bulmak
   c) Parola güvenliği test etmek
   d) Veri bütünlüğünü sağlamak

6. **Nmap aracı ne işe yarar?**
   a) Paket analizi yapmak
   b) Ağ haritalaması yapmak
   c) Güvenlik duvarı oluşturmak
   d) Veri yedeklemek

7. **WireShark ile ne tür bilgiler toplanabilir?**
   a) Parola güvenliği bilgileri
   b) Ağ paketlerinin analizi
   c) Güvenlik zafiyeti derecelendirmesi
   d) Domain sorgulama sonuçları

8. **Google Hack Veritabanı ne için kullanılır?**
   a) Güvenlik zafiyetleri bulmak
   b) Parola karmaşıklığını test etmek
   c) Ağ güvenliği analizi yapmak
   d) IP adresi sorgulama

9. **Bilgisayar sistemlerinin fiziksel güvenliği için hangi önlem alınmalıdır?**
   a) Parola güvenliği sağlamak
   b) Kesintisiz güç kaynağı kullanmak
   c) Virüs taraması yapmak
   d) Güvenlik duvarı kurmak

10. **Parola karmaşıklığı sağlamak için hangi kural uygulanmalıdır?**
    a) Parola içinde sadece rakamlar kullanılmalıdır
    b) Parola, hesap adını içermemelidir
    c) Parola, en az 4 karakter olmalıdır
    d) Parola, yalnızca özel karakterler içermelidir

Yanıt Anahtarı: 1-D, 2-B, 3-B, 4-C, 5-B, 6-B, 7-B, 8-A, 9-B, 10-B

Kaynakça

digitalguardian.com. (2023, 8 4). https://digitalguardian.com/blog/what-security-operations-center-soc adresinden alındı

mcafee.com. (2023, 8 10). mcafee.com: https://www.mcafee.com/enterprise/en-us/security-awareness/%20operations/%20what-is-soc.html adresinden alındı