1.BÖLÜM SİBER GÜVENLİK İHTİYACI

Siber güvenlik nedir?

Siber güvenlik, bu ağa bağlı sistemleri ve tüm verileri yetkisiz kullanıma veya zararlara karşı korumak için devam eden çabadır.

Çevrim içi ve çevrim-dışı kimlik nedir?

Çevrimdışı kımlik:Çevrimdışı kimliğiniz, arkadaşlarınızın ve ailenizin günlük olarak evde, okulda veya işte etkileşime girdiği kişidir. Adınızı, yaşınızı veya yaşadığınız yer gibi kişisel bilgilerinizi bilirler.

Çevrimiçi kimlik:Çevrimiçi kimliğiniz ise, siber alanda olduğunuz kişidir. Çevrimiçi kimliğiniz, kendinizi çevrimiçi olarak başkalarına sunma şeklinizdir. Bu çevrimiçi kimlik, sizin hakkınızdaki yalnızca sınırlı miktarda bilgiyi ortaya çıkarmalıdır.

Verileriniz

Finansal Veriler

Bilgi işlem cihazlarındaki veriler

Tıbbi Veriler

İstihdam

Online Bilgi

Kimliğiniz

Eğitim Verileri

Gizlilik, Bütünlük ve Uygunluk

CIA üçlüsü olarak bilinen gizlilik, bütünlük ve uygunluk(Şekil 1), bir kuruluşun bilgi güvenliği için bir kılavuzdur.

Gizlilik, kimlik doğrulama şifrelemesi yoluyla erişimi kısıtlayarak verilerin gizliliğini sağlar.

Bütünlük, bilgilerin doğru ve güvenilir olmasını sağlar.

Uygunluk (kullanılabilirlik), bilgilerin yetkili kişiler tarafından erişilebilir olmasını sağlar.

**Gizlilik**

Gizlilik için diğer bir terim de "mahremiyet" olacaktır. Şirket politikaları, bilgilere yetkili personelin erişimini kısıtlamalı ve bu verileri yalnızca yetkili kişilerin görüntülemesini sağlamalıdır. Veriler, bilginin güvenlik veya hassasiyet düzeyine göre bölümlere ayrılabilir.

Gizliliği sağlamak için kullanılan yöntemler arasında veri şifreleme, kullanıcı adı ve parola, iki faktörlü kimlik doğrulama ve hassas bilgilerin maruz kalmasını en aza indirgeme sayılabilir.

**Bütünlük**

Bütünlük, tüm yaşam döngüsü boyunca verilerin doğruluğu, tutarlılığı ve güvenilirliğidir. Veriler transfer sırasında değiştirilmemeli ve yetkisiz kuruluşlar tarafından değiştirilmemelidir. Dosya izinleri ve kullanıcı erişim denetimi, yetkisiz erişimi engelleyebilir. Sürüm kontrolü yetkili kullanıcılar tarafından yanlışlıkla yapılan değişiklikleri önlemek için kullanılabilir. Bozuk verileri geri yüklemek için yedeklemeler kullanılabilir olmalıdır ve aktarım sırasında verilerin bütünlüğünü doğrulamak için sağlama toplamı karması (checksum hashing) kullanılabilir.

Yaygın kullanılan sağlama toplamlarından bazıları MD5, SHA-1, SHA-256 ve SHA-512'dir.

**Uygunluk**

Ekipman bakımı, donanım onarımlarını yapma, işletim sistemlerini ve yazılımları güncel tutma ve yedeklemeler oluşturma, ağın ve verilerin yetkili kullanıcılara ulaşılabilir ve kullanılabilir olmasını sağlar. Doğal veya insan kaynaklı felaketlerden hızlı bir şekilde kurtulma planları yapılmalıdır. Güvenlik duvarları (firewall) gibi güvenlik ekipmanları veya yazılımları, hizmet reddi (DoS) gibi saldırılardan kaynaklanan arıza sürelerine karşı koruma sağlar. Hizmet reddi, bir saldırgan, hizmetlerin kullanıcılar tarafından kullanılamaması için kaynakları bunaltmaya çalıştığında gerçekleşir.

# Güvenlik İhlalinin Sonuçları

# Yıkılmış İtibar

# Vandalizim

# Hırsızlık

# Gelir Kaybı

# Zarar Görmüş Fikri Mülkiyet

# Saldırgan Türleri

# Amatörler

# — Bu insanlara bazen Script Kiddies denir. Genellikle saldırıları başlatmak için internette bulunan mevcut araçları veya talimatları kullanarak, az ya da hiç beceriye sahip olmayan saldırganlardır.

# Beyaz şapkalı saldırganlar, sistemlerin güvenliğinin geliştirilebilmesi ve zayıf yönleri keşfetmek için ağlara veya bilgisayar sistemlerine girerler. Bu girişler önceden izin alınarak yapılır ve her sonuç sahibine bildirilir.

# siyah şapkalı saldırganlar yasadışı kişisel, mali veya siyasi kazanç için herhangi bir güvenlik açığından yararlanırlar.

# Gri şapkalı saldırganlar, beyaz ve siyah şapkalı saldırganların arasında bir yerdedirler. Gri şapkalı saldırganlar bir sistemde bir güvenlik açığı bulabilirler. Gri şapkalı hackerlar, bu eylem amaçlarına uyuyırsa güvenlik açığını sistem sahiplerine bildirebilir.

# Organize Hackerlar

# — Bu hackerlar siber suçlular, hacktivistler, teröristler ve devlet destekli bilgisayar korsanlarıdır.

# Siber suçlular genellikle kontrol, güç ve zenginlik odaklı profesyonel suç gruplarıdır.

# Hacktivistler, kendileri için önemli olan konularda farkındalık yaratmak için siyasi açıklamalar yaparlar.

# Devlet destekli saldırganlar hükümetleri adına istihbarat toplar ya da sabotaj yaparlar. Bu saldırganlar genellikle yüksek eğitimli ve iyi finanse edilirler ve saldırıları hükümetleri için yararlı olan belirli hedeflere odaklanır.

# İç ve Dış Tehditler

# İç Güvenlik Tehditleri

Çalışan veya sözleşme ortağı gibi dahili bir kullanıcı kazara veya kasıtlı olarak şunları yapabilir:

* Gizli verileri yanlış kullanma
* İç sunucuların veya ağ altyapısı aygıtlarının işlemlerini tehdit etme
* Virüs bulaşmış USB ortamını kurumsal bilgisayar sistemine bağlayarak dış saldırıları kolaylaştırma
* Kötü amaçlı e-posta veya web siteleri aracılığıyla kötü amaçlı yazılımları (malware) ağa yanlışlıkla davet etme

# İç tehditler ayrıca dış tehditlere göre daha fazla zarar verme potansiyeline sahiptir, çünkü dahili kullanıcılar binaya ve altyapı cihazlarına doğrudan erişebilir. Çalışanlar ayrıca kurumsal ağın, kaynaklarının ve gizli verilerinin yanı sıra farklı kullanıcı veya idari ayrıcalıkların düzeyleri hakkında bilgi sahibidir.

**Dış Güvenlik Tehditleri**

Amatörlerden veya yetenekli saldırganlardan kaynaklanan dış tehditler, ağdaki veya bilgi işlem cihazlarındaki güvenlik açıklarından yararlanabilir veya erişim elde etmek için sosyal mühendisliği kullanabilir.

TERİM VE KAVRAMLAR UYGULAMA

* sensörler ve ekipman dahil olmak üzere fiziksel nesneler büyük bir ağ: Nesnelerin İnterneti (IoT)
* gizlilik, bütünlük ve kullanılabilirlik: CIA üçlü bileşenleri
* veri erişimi sadece yetkili personel sınırlı olduğu anlamına gelir gizlilik olarak da adlandırılan: Gizlilik
* veri şifreleme, kullanıcı adı kimliği ve şifre, iki faktörlü kimlik doğrulama, vb.: gizliliği sağlamak için yöntemler
* verilerin doğruluğunu, tutarlılığını ve güvenilirliğini gösteren terim: Bütünlük
* dosya izinleri, kullanıcı erişim denetimi, sürüm denetimi ve sağlama toplamları: bütünlüğü sağlamak için yöntemler
* Hizmetlerin ve verilerin bakımını açıklayan ve her zaman erişilebilen terim: uygunluk
* bir kuruluştan kaynaklanan saldırılar: güvenlik tehditleri
* bir kuruluşun dışından kaynaklanan saldırılar: Dış Güvenlik Tehditleri
* Bu sistemlerin güvenliğini artırmak amacıyla zayıflıkları keşfetmek için ağlara veya bilgisayar sistemlerine giren kişi veya kuruluşlar: Beyaz şapka saldırganları
* Yasadışı kişisel, finansal veya siyasi kazanç için herhangi bir güvenlik açığından yararlanan kişi veya kuruluşlar: Siyah şapka saldırganları
* siber suçlular, hacktivistler, teröristler ve devlet destekli hacker örgütleri: organize saldırganlar
* Bilgisayar sistemlerinin ve diğer ulusların ağlarının nüfuz etmesini içeren internet tabanlı bir çatışma: siber savaş
* İran'ın nükleer zenginleştirme tesisine zarar vermek için tasarlanmış bir kötü amaçlı yazılım programı, devlet destekli bir saldırı örneği olan bir program: Stuxnet
* siber tehditlerle uğraşırken küresel yetenekleri geliştirmeye adanmış dünya hükümetleri, endüstrileri ve akademi küresel bir ortaklık: Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklık (ETKİ)
* bazen davranış kodları, ama her zaman değil, yasalar tarafından uygulanan: Etik

# 2.BÖLÜM Saldırılar, Kavramlar ve Teknikler

# Güvenlik Açıklarını Bulma

# Güvenlik açıkları her türlü yazılım veya donanım kusurudur.

# Bir *exploit* , bilinen bir güvenlik açığından yararlanmak için yazılmış bir programı tanımlamak için kullanılan terimdir.

# Bir güvenlik açığına karşı bir istismar kullanma eylemine saldırı denir.

**Yazılım güvenlik açığı**

Yazılım güvenlik açıkları genellikle işletim sistemindeki veya uygulama kodundaki hatalardan kaynaklanır, ancak şirketlerin yazılım güvenlik açıklarını bulma ve düzeltme yamalarına rağmen, yeni güvenlik açıklarının ortaya çıkması yaygındır.

# Google'ın Proje Sıfır (Project Zero) isimli projesi, böyle bir uygulamanın harika bir örneğidir. Son kullanıcılar tarafından kullanılan çeşitli yazılımlarda bir takım güvenlik açıklarını keşfettikten sonra Google, yazılım güvenlik açıklarını bulmaya adanmış kalıcı bir ekip oluşturdu.

**Donanım güvenlik açığı**

Donanım güvenlik açıkları genellikle donanım tasarım kusurları nedeniyle ortaya çıkar.

# Donanım güvenlik açıkları cihaz modellerine özgüdür ve genellikle rasgele risk girişimleriyle kullanılmazlar. Donanım istismarları yüksek hedefli saldırılarda daha yaygın olmakla birlikte, geleneksel kötü amaçlı yazılım koruması ve fiziksel güvenlik günlük kullanıcılar için yeterli korumadır.

# 2.1.2.1 Güvenlik Açıklarını Kategorize Etme

# Arabellek taşması

# — Bu güvenlik açığı, veriler arabellek sınırlarının ötesinde yazıldığında oluşur. Arabellekler, bir uygulamaya ayrılan bellek alanlarıdır. Verileri bir arabellek sınırlarının ötesinde değiştirerek, uygulama diğer işlemlere ayrılan belleğe erişir. Bu, sistem çökmesine, verinin riske girmesine veya ayrıcalıkların artmasına neden olabilir.

# Doğrulanmamış girdi

# — Programlar genellikle veri girişi ile çalışır. Programa giren bu veriler, programı istenmeyen bir şekilde davranmaya zorlamak için tasarlanmış kötü amaçlı içeriğe sahip olabilir. İşlemek amacıyla resim alan bir program düşünün. Kötü amaçlı bir kullanıcı geçersiz boyutlara sahip bir görüntü dosyası oluşturabilir. Kötü amaçlarla oluşturulmuş boyutlar, programı yanlış ve beklenmeyen boyutlardaki arabellekleri ayırmaya zorlayabilir.

# Yarış koşulları

# — Bu güvenlik açığı, bir olayın çıktısının sıralı veya zamanlı çıktılara bağlı olmasıdır. Bir yarış koşulu, gerekli sıralı veya zamanlanmış olaylar doğru sırada veya uygun zamanlama gerçekleşmediğinde bir güvenlik açığı kaynağı haline gelir.

# Güvenlik uygulamalarındaki zayıflıklar

# — Sistemler ve hassas veriler kimlik doğrulama, yetkilendirme ve şifreleme gibi tekniklerle korunabilir. Geliştiriciler, büyük olasılıkla güvenlik açıklarını oluşturacaklarından, kendi güvenlik algoritmalarını oluşturmaya çalışmamalıdır. Geliştiricilerin önceden oluşturulmuş, test edilmiş ve doğrulanmış güvenlik kütüphanelerini (libraries) kullanmaları şiddetle tavsiye edilir.

# Erişim-denetim sorunları

# — Erişim denetimi, kimlerin ne yaptığını kontrol etme sürecidir ve donanıma fiziksel erişimi yönetmekten dosya gibi bir kaynağa kimin erişimi olduğunu ve dosyayı okumak veya değiştirmek gibi onunla neler yapabileceklerini kontrol etme sürecidir. Birçok güvenlik açığı, erişim denetimlerinin yanlış kullanımı nedeniyle oluşur.

# Saldırganın hedef ekipmana fiziksel erişimi varsa hemen hemen tüm erişim kontrolleri ve güvenlik uygulamaları aşılabilir. Makineyi ve içerdiği verileri korumak için fiziksel erişim kısıtlanmalı ve verilerin çalınmasını veya bozulmasını önlemek için şifreleme teknikleri kullanılmalıdır.

# Kötü Amaçlı Yazılım Türleri

# Casus yazılım

# — Bu kötü amaçlı yazılım kullanıcıyı izlemek ve casusluk yapmak için tasarlanmıştır. Casus yazılımlar genellikle etkinlik izleyicileri, tuş vuruşu toplama ve veri yakalama içerir. Casus yazılımlar, sistemdeki güvenlik önlemlerini atlatmak amacıyla genellikle güvenlik ayarlarını değiştirirler. Casus yazılımlar genellikle meşru yazılımlarla veya Truva atlarıyla birlikte paketlenir.

# Adware

# — Reklam destekli yazılım otomatik olarak reklam sunmak için tasarlanmıştır. Adware (reklam yazılımı) genellikle bazı yazılım sürümleriyle yüklenir. Bazı reklam yazılımları sadece reklam sunmak için tasarlanmıştır, ancak reklam yazılımlarının casus yazılımlarla birlikte gelmesi de yaygındır.

# Bot

# — Robot kelimesinden gelen bot kötü amaçlı yazılımı, genellikle çevimiçi olarak gelen otomatik bir eylem gerçekleştirmek için tasarlanmıştır. Çoğu botlar zararsız olmakla birlikte, kötü amaçlı botların giderek artan kullanımı botnetlerdir. Birkaç bilgisayara saldırgan tarafından sağlanan komutları sessizce beklemek için programlanmış botlar bulaşmıştır.

# Fidye Yazılımı (Ransomware)

# — Bu kötü amaçlı yazılım, bir bilgisayar sistemini veya içerdiği verileri bir ödeme yapılıncaya kadar tutsak tutmak için tasarlanmıştır. Fidye yazılımı genellikle bilgisayardaki verileri kullanıcı tarafından bilinmeyen bir anahtarla şifreleyerek çalışır. Fidye yazılımının diğer bazı sürümleri, sistemi kilitlemek için belirli sistem açıklarından yararlanabilir. Fidye yazılımı, indirilen bir dosya veya bazı yazılım güvenlik açığı tarafından yayılır.

# Korku Yazılımı (Scareware)

# — Bu, kullanıcıyı korkuya dayalı belirli bir eylem yapmaya ikna etmek için tasarlanmış bir kötü amaçlı yazılım türüdür. Korkutma, işletim sistemi diyalog pencerelerine benzeyen açılır pencereleri oluşturur. Bu pencereler, sistemin risk altında olduğunu veya normal çalışmaya dönmek için belirli bir programın yürütülmesi gerektiğini belirten sahte iletileri iletir. Gerçekte, herhangi bir sorun değerlendirilmedi veya tespit edilmedi ve kullanıcı söz konusu programı yürütmek üzere kabul eder ve temizlerse, sistemine kötü amaçlı yazılım bulaşacaktır.

# Rootkit

# — Bu kötü amaçlı yazılım bir arka kapı oluşturmak amacıyla işletim sistemini değiştirmek üzere tasarlanmıştır. Saldırganlar daha sonra bilgisayara uzaktan erişmek için bu arka kapıyı kullanırlar. Çoğu rootkit, ayrıcalık yükseltme gerçekleştirmek ve sistem dosyalarını değiştirmek için yazılım güvenlik açıklarından yararlanır. Ayrıca rootkitlerin sistem adli tıp (forensic) ve izleme araçlarını değiştirmesi de yaygındır, bu da tespit edilmesini çok zorlaştırır. Çoğu zaman, bir rootkit tarafından enfekte olan bir bilgisayar silinmeli ve yeniden kurulmalıdır.

# Virüs

# - Virüs, genellikle meşru program olan diğer yürütülebilir dosyalara eklenen kötü amaçlı yürütülebilir koddur. Çoğu virüs son kullanıcı aktivasyonu gerektirir ve belirli bir zamanda veya tarihte etkinleştirilebilir. Vieüsler, sadece bir resim göstermek gibi zararsız olabildiği gibi, veriyi değiştirmek ya da silmek gibi zararlı da olabilir. Virüsler ayrıca tespit edilmesini önlemek için mutasyona geçecek şekilde programlanabilir. Çoğu virüs artık USB sürücüler, optik diskler, ağ paylaşımları veya e-posta tarafından yayılır.

# Truva atı

# - Bir Truva atı, istenen bir işlem kisvesi altında kötü amaçlı işlemler yapan kötü amaçlı yazılımlardır. Bu kötü amaçlı kod, onu çalıştıran kullanıcının ayrıcalıklarından yararlanır. Çoğu zaman, Truva atları görüntü dosyalarında, ses dosyalarında veya oyunlarda bulunur. Bir Truva atı, kendisini yürütülebilir olmayan dosyalara bağladığından bir virüsten farklıdır.

# Solucanlar (Worm)

# — Solucanlar, ağlardaki güvenlik açıklarından yararlanarak kendilerini çoğaltan kötü amaçlı kodlardır. Solucanlar genellikle ağları yavaşlatır. Bir virüs çalıştırmak için bir ana bilgisayar programı gerektirse de, solucanlar kendiliğinden çalışabilir. İlk enfeksiyon dışında artık kullanıcı katılımına ihtiyaç duymazlar. Bir host enfekte olduktan sonra, solucan ağ üzerinden çok hızlı bir şekilde yayılabilir. Solucanlar benzer desenleri paylaşır. Hepsinin etkin bir güvenlik açığı, kendilerini yaymanın bir yolu var ve hepsinde bir yük var.

**Man-In-The-Middle (MitM)**

**—**MitM, saldırganın kullanıcının bilgisi olmadan bir cihaz üzerinde kontrolü ele geçirmesini sağlar. Bu erişim düzeyi ile saldırgan, kullanıcı bilgileri istenen hedefe gönderilmeden önce, araya girebilir ve bu bilgileri yakalayabilir. MitM saldırıları finansal bilgileri çalmak için yaygın olarak kullanılmaktadır. Saldırganlara MitM yetenekleri sağlamak için birçok kötü amaçlı yazılım ve teknik mevcuttur.

**Man-In-The-Mobile (MitMo)**

**—**Ortadaki adamın bir varyasyonu olan MitMo, bir mobil cihaz üzerinde kontrolü ele geçirmek için kullanılan bir saldırı türüdür. Enfekte olduğunda, mobil cihaza kullanıcı duyarlı bilgileri dışa aktarması ve saldırganlara göndermesi talimatı verilebilir. MitMo yeteneklerine sahip bir istismar örneği olan ZeuS, saldırganların sessizce kullanıcılara gönderilen 2 adımlı doğrulama SMS mesajlarını yakalamasına izin verir.

# Kötü Amaçlı Yazılımların Belirtileri

kötü amaçlı yazılım belirtileridir:

* CPU kullanımında bir artış var.
* Bilgisayar hızında bir azalma var.
* Bilgisayar sık sık donuyor veya çöküyor.
* Web tarama hızında bir azalma var.
* Ağ bağlantılarıyla açıklanamayan sorunlar var.
* Dosyalar değiştirilmiştir.
* Dosyalar silinmiştir.
* Bilinmeyen dosyalar, programlar veya masaüstü simgeleri vardır.
* Çalışan bilinmeyen süreçler vardır.
* Programlar kendilerini kapatıyor veya yeniden yapılandırıyor.
* Kullanıcının bilgisi veya rızası olmadan e-posta gönderiliyor.

# Sosyal Mühendislik

# Sosyal mühendislik, bireyleri eylemleri gerçekleştirmeye veya gizli bilgileri ifşa etmeye yönlendirmeye çalışan bir erişim saldırısıdır.

* **Pretexting** - Bu, bir saldırganın bir kişiyi araması ve ayrıcalıklı verilere erişim elde etmek amacıyla onlara yalan söylemesidir. Örnek olarak, alıcının kimliğini doğrulamak için kişisel veya finansal verilere ihtiyaç duyuyormuş gibi görünen bir saldırgan verilebilir.
* **Tailgating** - Bu, bir saldırganın yetkili bir kişiyi hızlı bir şekilde güvenli bir yere takip etmesidir.
* **Bir şey için bir şey (Quid pro quo)** - Bu, bir saldırganın bir partiden kişisel bilgiler, ücretsiz bir hediye gibi bir şey istediği zamandır.

# Wi-Fi Parolası Kırma

Wi-Fi parolası kırma, bir kablosuz ağı korumak için kullanılan parolayı bulma işlemidir.

**Sosyal mühendislik** — Saldırgan, parolayı bilen bir kişiyi parolayı girmeye yönlendirir.

**Kaba kuvvet saldırıları** — Saldırgan parolayı tahmin etmek için birkaç olası parola dener. Kaba kuvvet saldırıları genellikle bir sözcük listesi dosyası içerir. Bu, bir sözlükten alınan kelimelerin listesini içeren bir metin dosyasıdır. Bir program daha sonra her kelimeyi ve ortak kombinasyonları dener. Parola kaba kuvvet araçlarının bazıları şunlardır: Ophcrack, L0phtCrack, THC Hydra, RainbowCrack ve Medusa .

**Ağ koklama —**Bir saldırgan, parola ağda şifrelenmemiş (düz metin olarak) olarak gönderiliyorsa, gönderilen paketleri dinleyerek ve yakalayarak bu parolayı bulabilir. Parola şifrelenmişse, saldırgan yine de parola kırma aracı kullanarak bunu ortaya çıkarabilir.

# Kimlik avı

Kimlik avı (Phishing veya Oltalama), kötü niyetli bir tarafın meşru ve güvenilir bir kaynaktan gizlenmiş sahte bir e-posta göndermesi demektir.

Spear phishing (yemleme kancası) kimlik avı, yüksek hedefli bir kimlik avı saldırısıdır. Kimlik avı ve yemleme kancası kimlik avı kurbanlara ulaşmak için e-posta kullanırken yemleme kancası kimlik avı e-postaları belirli bir kişiye özelleştirilir. Saldırgan, e-posta göndermeden önce hedefin ilgi alanlarını araştırır.

# Güvenlik Açığının Sömürülmesi

# Güvenlik açıklarından yararlanmak (sömürmek), yaygın bir başka sızma yöntemidir.

# 1.Adım . Hedef sistem hakkında bilgi toplayın. Bu, bir bağlantı noktası tarayıcı veya sosyal mühendislik gibi birçok farklı şekilde yapılabilir.

# 2.Adım. 1. adımda öğrenilen ilgili bilgilerin parçalarından biri işletim sistemi, sürümü ve üzerinde çalışan hizmetlerin bir listesi olabilir

# 3.Adım. Hedefin işletim sistemi ve sürümü bilindiğinde, saldırgan işletim sistemi veya diğer işletim sistemi hizmetlerine özgü bilinen güvenlik açıklarını arar.

# 4.Adım . Bir güvenlik açığı bulunduğunda, saldırgan kullanmak için önceden yazılmış bir istismar (exploit) arar. Eğer herhangi bir istismar yazılmadıysa, saldırgan bir istismar yazmayı düşünebilir.

# etki alanı adları ve tescil ettirenleri hakkında bilgi içeren genel bir İnternet veritabanı olan whoiskullanan bir saldırganı tasvir eder.

# Şekil 2, popüler bir bağlantı noktası (port) tarayıcısı olan nmap aracını kullanan bir saldırganı tasvir eder.

# Bir bağlantı noktası tarayıcısı ile saldırgan, hedef bilgisayarın bağlantı noktalarını araştırabilir ve bu bilgisayarda hangi hizmetlerin çalıştığını öğrenebilir.

**Gelişmiş Kalıcı Tehditler**

Sızıntıya ulaşmanın bir yolu, gelişmiş kalıcı tehditlerdir (APT). Belirli bir hedefe karşı çok fazlı, uzun vadeli, gizli ve ileri bir operasyondan oluşur. Karmaşıklığı ve gerekli beceri seviyesi nedeniyle, bir APT genellikle iyi finanse edilir. APT, kurumları veya ülkeleri ticari veya politik nedenlerle hedef alır.

# Genellikle ağ tabanlı casuslukla ilgili olan APT'nin amacı, hedeflenen sistemlerin biri veya birden fazlasına özelleştirilmiş kötü amaçlı yazılım dağıtmak ve tespit edilmeden kalmaktır. Birden fazla çalışma aşaması ve farklı aygıtları etkileyen ve belirli işlevleri gerçekleştiren çeşitli özelleştirilmiş kötü amaçlı yazılım türleriyle, tek bir saldırgan APT'leri yürütmek için genellikle beceri, kaynak veya kalıcılıktan yoksundur.

# ⁪

# DoS

# Hizmet Reddi (DoS) saldırıları bir tür ağ saldırısıdır. Bir DoS saldırısı, kullanıcılara, cihazlara veya uygulamalara yönelik bir çeşit ağ hizmetinin kesilmesine neden olur.

**Ezici Trafik Miktarı -** Bu saldırı, bir ağa, ana bilgisayara veya uygulamaya işleyemeyeceği bir hızda muazzam miktarda veri gönderilmesidir. Bu durum, iletimin veya yanıtın yavaşlamaya veya bir cihazın ya da hizmetin kilitlenmesine neden olur.

**Kötü Amaçlı Biçimlendirilmiş Paketler -** Bu, kötü amaçlı olarak biçimlendirilmiş bir paketin bir ana bilgisayara veya uygulamaya gönderildiği ve alıcı bunu işleyemediği durumdur. Örneğin, bir saldırgan, uygulama tarafından tanımlanamayan hatalar içeren paketleri iletir veya hatalı biçimlendirilmiş paketleri iletir. Bu durum, alıcı aygıtın çok yavaş çalışmasına veya çökmesine neden olur.

# DdoS

# Dağıtılmış DoS Saldırısı (DDoS) bir DoS saldırısına benzer ancak birden çok koordineli kaynaktan kaynaklanır.

Bir saldırgan, botnet adı verilen virüslü ana bilgisayarlardan (host) oluşan bir ağ oluşturur. Enfekte olmuş hostlara zombi denir. Zombiler işleyici sistemleri tarafından kontrol edilir.

Zombi bilgisayarlar sürekli olarak daha fazla ana bilgisayarı tarar ve enfekte ederek daha fazla zombi yaratır. Hazır olduğunda, hacker, işleyici sistemlerine zombilerin botnet'ini bir DDoS saldırısı gerçekleştirmesini söyler.

# SEO Zehirlenmesi

# SEO, Arama Motoru Optimizasyonu'nun İngilizce kısaltmasıdır ve bir web sitesinin bir arama motoru tarafından sıralamasını iyileştirmek için kullanılan bir dizi tekniktir.

# kötü niyetli bir kullanıcı, arama sonuçlarında kötü amaçlı bir web sitesinin daha yüksek görünmesini sağlamak için SEO'yu kullanabilir. Bu tekniğe SEO zehirlenmesi denir.

# SEO zehirlenmesinin en yaygın amacı, kötü amaçlı yazılım barındırabilecek veya sosyal mühendislik gerçekleştirebilecek kötü amaçlı sitelere yönelik trafiği arttırmaktır. Kötü amaçlı bir siteyi arama sonuçlarında daha yüksek sıralamaya zorlamak için saldırganlar popüler arama terimlerinden yararlanırlar.

# Harmanlanmış Saldırı Nedir?

# Harmanlanmış (veya karma da denir) saldırılar, bir hedefi tehlikeye atmak için birden fazla teknik kullanan saldırılardır. Aynı anda birkaç farklı saldırı tekniği kullanarak, saldırganlar solucanlar, Truva atları, casus yazılımlar, keylogger, spam'lar ve kimlik avı şemaları melezi olan kötü amaçlı yazılımlara sahiptir.

Nimbda, CodeRed, BugBear, Klez ve Slammer gibi en zararlı bilgisayar solucanlarının çoğu, aşağıda gösterildiği gibi karışık saldırılar olarak daha iyi kategorize edilir:

* Bazı Nimbda varyantları e-posta eklerini, güvensiz bir web sunucusundan dosya indirmelerini ve Microsoft dosya paylaşımını (örn. anonim paylaşımlar) çoğaltma yöntemleri olarak kullandı.
* Diğer Nimbda varyantları, saldırganın veya kötü amaçlı kodu yönetimsel ayrıcalıklarla sağlayacak şekilde sistemin konuk hesaplarını değiştirebildi.

Son zamanlarda Conficker ve ZeuS/LICAT solucanları da harmanlanmış saldırılardı.

KAVRAMLAR

* kötü niyetli kullanıcıların yararlanmaya çalışacağı her türlü donanım veya yazılım hatası: güvenlik açıkları
* bilinen bir güvenlik açığından yararlanmak için yazılmış bir program: bir istismar
* hedef sisteme girme amacı ile bir güvenlik açığına karşı bir istismar kullanma eylemi: bir siber saldırı
* genellikle işletim sistemi veya uygulama kodundaki hatalardan kaynaklanır: Açıklar
* güvenlik açıklarının kullanılmasını önlemek için işletim sistemi ve uygulama üreticileri tarafından yayınlandı: Güvenlik Yamaları ve Güncellemeler
* Google tarafından oluşturulan bu, yazılım güvenlik açıklarını bulmaya adanmış üçüncü taraf bir daimi araştırmacı ekibinin bir örneğidir.: Proje Sıfır (Project Zero)
* bilgisayar aygıtlarında ve bileşenlerinde tasarım kusurlarının neden olduğugüvenlik zayıflıkları. Genellikle belirli cihaz modelleriyle sınırlıdır ve hedeflenen saldırılarla yaygın olarak kullanılırlar.: donanım zaafiyetleri
* veribir uygulamaya ayrılan bellek alanlarının sınırlarının ötesinde yazıldığında oluşan bir yazılım güvenlik açığı. Bu güvenlik açığı, bir uygulamanın diğer işlemlere ayrılan belleğe erişmesine neden olabilir: arabellek taşması
* Bir kullanıcı tarafından bir programa sağlanan verilerin veya istismar edilmesinin, uygulamanın istenmeyen bir şekilde davranmasına neden olduğu bir güvenlik açığı: doğrulanmamış girdi
* Sıralı veya zamanlanmış bir süreç kümesi bir istismar tarafından bozulduğunda veya değiştirildiğinde oluşan bir güvenlik açığı: yarış koşulları
* ekipmanın, verilerin veya uygulamaların fiziksel kontrolünü yöneten uygulamaların yanlış kullanımı: erişim-kontrol sorunları
* veri çalmak, erişim denetimlerini atlamak veya bir sisteme zarar vermek veya tehlikeye girmek için kullanılabilecek herhangi bir bilgisayar kodu: Kötü Amaçlı Yazılımlar
* kullanıcıların eylemlerini izlemek ve veri yakalamak için tasarlanmış kötü amaçlı yazılım: casus yazılım
* otomatik olarak reklamlar sunanyazılım. Bazı türler casus yazılım içerir.: adware
* Internet üzerinden otomatik olarak eylemleri gerçekleştirmek için tasarlanmış kötü amaçlı yazılım: bot
* Saldırganın ödeme yapılıncaya kadar, genellikle temel verileri şifreleyerek bilgisayar sistemini esir alan bir kötü amaçlı yazılım türü: Fidye yazılımları
* bir arka kapı üzerinden yetkisiz uzaktan erişime izin vermek için işletim sistemlerini değiştirmek için tasarlanmışkötü amaçlı yazılım. Rootkit, kullanıcı ayrıcalıklarını, sistem dosyalarını ve sistem adli tıp bilgilerini ve izleme araçlarını değiştirebilir, bu da onları algılamayı ve kaldırmayı son derece zorlaştırır.: rootkit
* meşru programlara eklenebilecekkötü amaçlı yürütülebilir kod. Virüsler genellikle son kullanıcı aktivasyonunu gerektirir ve nispeten zararsız veya çok yıkıcı olabilir. Bunlar genellikle USB sürücüler, optik medya, ağ paylaşımları veya e-posta tarafından yayılır.: virüs
* İstenilen bir işleve sahip görünürken kötü amaçlı işlemler gerçekleştiren kötü amaçlı yazılımlar. Yürütülebilir olan virüslerin aksine, yürütülebilir olmayan dosyalara dahil edilirler.: Truva Atı
* kötü amaçlı yazılım, ağlardaki güvenlik açıklarından yararlanarak kendini bağımsız olarak çoğaltan kötü amaçlı kod şeklinde. Bir ağ üzerinden çok hızlı yayıldılar çünkü kendi başlarına koşuyorlar. Etkinleştirilebilen bir güvenlik açığı, kendilerini yaymanın bir yolu ve bir yük de dahil olmak üzere tüm benzer kalıpları paylaşır.: solucanlar
* Bir saldırganın sahibinin bilgisi olmadan bir cihazın kontrolünü ele geçirebileceği bir teknik. Saldırgan, cihazdan başka bir hedefe giden yolda geçen bilgileri kesebilir ve yakalayabilir.: Ortadaki Adam
* bir varyasyonu olan bir saldırı (MitM). Bir mobil aygıta, cihazın kontrolünü ele alan ve hassas bilgileri saldırganlara iletmesine neden olan kötü amaçlı yazılım bulaşmıştır.: mobil adam (MitMO)
* bireyleri eylemleri gerçekleştirmek veya gizli bilgileriifşa etmek için manipüle eden kaynaklara erişim kazanmanın bir yolu. Saldırganlar zayıflıklarımıza yardım etme veya istismar etme isteğimizi istismar etmeye çalışıyorlar.: Sosyal Mühendislik
* bireyin ayrıcalıklı bilgilere erişmek için yattığı bir tür sosyal mühendislik saldırısı: pretexting
* Bir saldırganın yetkili bir kişiyi güvenli bir yere takip ettiği bir tür sosyal mühendislik saldırısı: bagaj kapısı
* Bir saldırganın ücretsiz hediye gibi bir şey karşılığında kişisel bilgi talep ettiği bir tür sosyal mühendislik saldırısı: bir şey için bir şey
* kablosuz ağı korumak için kullanılan bir şifre bulma eylemi: Wi-Fi parola kırma
* parola için kullanılabilecek tüm olası değerlerle veya parolalarda yaygın olarak kullanılan sözcüklerin bir listesiyle tekrar tekrar bir parola meydan okumak için bir yazılım programının kullanılması. Karmaşık parolaları tahmin etmek çok daha zordur.: Deneme yanılma saldırıları
* kablosuz ağdaki paketleri yakalamak için yazılım kullanımı. Şifrelenmemiş parolalar yakalanabilir ve bir saldırıda kullanılabilir ve şifrelenmiş parolalar bir yazılım aracıyla kırılabilir.: ağ koklama
* meşru bir kaynak tarafından gönderilmiş gibi görünen genel bir hileli e-postanınkullanılması. E-posta, insanları kötü amaçlı yazılım yüklemeye veya gizli bilgileri paylaşmaya yönlendirir.: Kimlik avı (oltalama)
* meşrubir kaynaktan gönderilen e-postaların belirli kişiler için özelleştirildiği yüksek hedefli bir saldırı. Saldırgan, belirli bir kişiyi kandıran bir e-posta oluşturmak için hedefin ilgi alanlarını araştırır.: yemleme kancası
* Yazılım araçları veya sosyal mühendislik dahil olmak üzere çeşitli yöntemlerin kullanımı, bir sistem hakkında bilgi kazandırmak. Bu saldırgan, belirli bir sistemde var olan zayıflıkları bulmak için bu bilgileri kullanır.: güvenlik açığı sömürü
* Belirlibir hedefe karşı çok fazlı, uzun vadeli, sinsi ve gelişmiş bir saldırı. APT'ler karmaşıktır ve yüksek düzeyde beceri gerektirir, bu nedenle saldırılar genellikle iyi finanse edilir ve iş veya siyasi nedenlerle örgütleri veya ülkeleri hedef alır. Genellikle hedef sistemlerde algılanmayan kötü amaçlı yazılım kullanan ağ tabanlı casusluk içerir.: İleri Düzey Kalıcı Tehditler
* Internet etki alanı adları ve etki alanlarını kaydeden kişiler veya kuruluşlar hakkında bilgi içeren genel bir İnternet veritabanı. Sistem açıklarından yararlanmak için kullanılabilecek bir bilgi kaynağıdır.: **whois**
* ağa bağlı sistemlerdeki güvenlik açıklarını keşfetmek için kullanılabilen popüler bir bağlantı noktası tarama aracı: **nmap**
* kullanıcılara, cihazlara veya uygulamalara ağ hizmetlerini kesintiye uğratan bir saldırı: hizmet reddi (DoS)
* çok sayıda paket bir ağa ağ sistemlerinin işleyemeyeceği bir oranda gönderilen bir DoS saldırısı. Bu, ağ iletimi veya yanıtının yavaşlamasına veya bir cihazın veya hizmetin çökmesine neden olur.: trafik ezici miktarı
* ağ aygıtlarının çalışmasını bozmak için oluşturulan ağ veri yapılarının kullanımı: kötü amaçlı biçimlendirilmiş paketler
* ağlar ve ağ aygıtları tarafından sağlanan hizmetleri bozan veri göndermek için birden fazla dağıtılmış sistem kullanımı: dağıtılmış hizmet reddi (DDoS)
* DDoS saldırısı başlatmak için kullanılan dağıtılmış virüslü ana bilgisayarlardan oluşan bir ağ: Botnet
* kötü amaçlı kod dağıtılacak veya sosyal mühendislik gizli bilgi toplamak için kullanılabilir siteye kullanıcıları çekmek için kötü niyetli bir web sitesinin sıralamasında manipülasyon: arama motoru optimizasyonu (SEO) zehirlenmesi
* Hedefi tehlikeye atabilmek için çoklu tekniklerin kullanılması: harmanlanmış saldırı
* başarılı bir saldırının neden olduğu hasarı sınırlamak için tekniklerin kullanılması. Bu teknikler, çalışanlara ve müşterilere saldırı hakkında iletişim kurma yolları, saldırının araştırılması ve gelecekteki saldırıları önleme tedbirleri içerir.: darbe azaltma

3.BÖLÜM VERİLERİNİZİ VE GİZLİLİĞİNİZİ KORUMAK

# Bilgi İşlem Cihazlarınızı Koruyun

# Güvenlik Duvarı'nı Açık Tutun

# Antivirüs ve Antispyware kullanın

# İşletim Sisteminizi ve Tarayıcınızı Yönetin

# Tüm Cihazlarınızı Koruyun

# İnternet'e erişim için çoğu IoT cihaz üreticisi müşterinin yerel ağına güvenir. Sonuç olarak, IoT cihazlarının oluşması muhtemeldir ve bunlar olduğunda müşterinin yerel ağına ve verilerine erişime izin verirler. Kendinizi bu senaryodan korumanın en iyi yolu, IoT aygıtlarının yalıtılmış bir ağ kullanarak yalnızca diğer IoT cihazlarıyla paylaşmasıdır.

# Kablosuz Ağları Güvenle Kullanma

**İyi bir parola seçmek için ipuçları**:

* Herhangi bir dildeki sözlük kelimelerini veya isimleri kullanmayın
* Sözlük kelimelerinin yaygın yazım yanlışlarını kullanmayın
* Bilgisayar adlarını veya hesap adlarını kullanmayın
* Mümkünse  "!" gibi özel karakterler kullanın @ # $% ^ & \* ()
* On veya daha fazla karakter içeren bir parola kullanın

# Parola Yerine Passphrase Kullanma

# Bilgisayar aygıtlarınıza yetkisiz fiziksel erişimi önlemek için parolalar yerine passphrase kullanın. Bir paroladan daha uzun bir passphrase oluşturmak daha kolaydır, çünkü genellikle bir kelime yerine bir cümle şeklindedir.

**İyi bir passphrase seçiminde ipuçları:**

* Sizin için anlamlı olan bir ifade seçin
* ! gibi özel karakterler ekleyin @ # $% ^ & \* ()
* Ne kadar uzun olursa o kadar iyi olur.
* Yaygın veya ünlü ifadelerden kaçının, örneğin, popüler bir şarkının sözleri gibi...

# NIST standartları Yeni yönergelerin özeti:

* En az 8 karakter uzunluğunda olmalı, ancak 64 karakterden fazla olmamalıdır
* Parola, abc123 gibi yaygın, kolay tahmin edilen parolalar olmamalıdır
* Küçük ve büyük harfler ile sayılar dahil etmek gibi kompozisyon kuralları olmamalıdır
* Yazarken kullanıcının parolayı görmesine izin vererek yazım doğruluğu arttırılmalıdır
* Tüm yazdırılabilir karakterlere ve boşluklara izin verilmelidir
* Parola hatırlatıcı ipucu (hint) olmamalıdır
* Periyodik veya isteğe bağlı parola süresinin dolması olmamalıdır
* Paylaşılan gizli sorulardan bilgi edinme, pazarlama verileri, işlem geçmişi gibi bilgiye dayalı kimlik doğrulama olmamalıdır

# İki Faktörlü Kimlik Doğrulaması

# Google, Facebook, Twitter, LinkedIn, Apple ve Microsoft gibi popüler çevrimiçi hizmetler, hesap oturumları için ekstra bir güvenlik katmanı eklemek için iki faktörlü kimlik doğrulaması kullanır. Kullanıcı adı ve parola veya kişisel kimlik numarası (PIN) veya deseninin yanı sıra, iki faktörlü kimlik doğrulaması ikinci bir belirteç gerektirir,

* **Fiziksel nesne** - kredi kartı, ATM kartı, telefon veya fob
* **Biyometrik tarama** - parmak izi, avuç içi izi, yüz veya ses tanıma

# OAuth 2.0

# Açık Yetkilendirme (OAuth), son kullanıcının kimlik bilgilerinin kullanıcının parolasını açığa çıkarmadan üçüncü taraf uygulamalara erişmesini sağlayan açık standart bir protokoldür. OAuth, son kullanıcıların üçüncü taraf uygulamalarına erişmesine izin verilip verilmeyeceğine karar vermek için aracı görevi görür.

# KAVRAMLAR

# bilgisayar korsanlarının kişisel veya şirket verilerinize erişmesini engelleyen donanım veya yazılım: güvenlik duvarı

# bir bilgisayarı kötü amaçlı yazılımlar için tarayan ve silen bir program: Antivirüs

# çevrimiçi etkinlikleri izler ve izinsiz kişisel bilgileri toplar: casus yazılım

# verileri yok eder ve bir bilgisayarı yavaşlatabilir: virüs

# en son yazılım ve güvenlik yamaları/güncellemeleri kullanmak için: Tarayıcıyı ve işletim sistemini güvence altına alın

# web tabanlı bir cihaz tarayıcısı: Shodan

# ağ tanımlayıcısı aracılığıyla belirli bir kablosuz ağa bağlanın: Hizmet Kümesi Tanımlayıcısı (SSID)

# ağı keşfetmek için ek bir engel ekler ve en az güvenlik sağlar: SSID genel yayınını devre dışı bırakma

# kablosuz güvenliği etkinleştirin ve WPA2 şifreleme özelliğini kullanın: kablosuz iletişimi şifrele

# internette sörf için kamuya açık bir konum, ancak herhangi bir hassas kişisel bilgiye erişmek veya göndermek için en iyi nerede: halka açık Wi-Fi noktası

# veri kesilmesini önlemek için bilgisayar ve VPN sunucusu arasında şifreli bir bağlantı: şifreli VPN

# çevrimiçi hesaplarla kullanılmak üzere farklı ve karmaşık şifreleri depolayan ve şifreleyen bir yazılım veya hizmet: Parola yöneticisi

# Herhangi bir dilde sözlük sözcükleri veya isimleri kullanmayın. Sözlük kelimelerinin yaygın yazım yanlışlarını kullanmayın. Bilgisayar adlarını veya hesap adlarını kullanmayın. Mümkünse özel karakterler kullanın : ! @ # $% ^ & \* (). En az on karakterli bir parola kullanın.: Nasıl güvenli bir parola yapabilirsiniz?

# bilgileri yetkisiz bir tarafın okuyamayacağı bir forma dönüştürme süreci: şifreleme

# yerel veya bulut depolama çözümü aracılığıyla yeri doldurulamaz veri kaybını önler: Veri yedeklemeleri

# Sabit sürücüyü veya depolama aygıtını fiziksel olarak yok edin.: Bir dosyayı nasıl kurtarılamaz hale getirebilirsiniz?

# kullanıcı adı ve şifreye ek olarak, bir kullanıcının kimlik bilgilerini doğrulamak için kredi kartı veya telefon numarası gibi ikinci bir belirteç gereksinimi: İki Faktörlü Kimlik Doğrulaması

# Son kullanıcının kullanıcının kullanıcının şifresini açığa çıkarmadan üçüncü taraf uygulamalarına erişmesini sağlayan açık standart bir protokol: Açık Yetkilendirme (Oauth)

# Çerezleri otomatik olarak devre dışı bırakarak, geçici İnternet dosyalarını silerek ve pencereyi veya programı kapattıktan sonra tarama geçmişini kaldırarak İnternet tarama geçmişini gizli tutma yöntemleri: Microsoft Internet Explorer: InPrivate, Google Chrome: Gizli, Mozilla Firefox: Özel sekme/özel pencere, Safari: Özel: Özel tarama

# Bölüm 4: Kurumun Korunması

# Güvenlik Duvarı Türleri

# Güvenlik duvarı (Firewall), yangının bir binanın bir bölümünden diğerine yayılmasını önlemek için tasarlanmış bir duvar veya bölümdür. Bilgisayar ağlarında, bir güvenlik duvarı, şekilde gösterildiği gibi, hangi iletişimlere izin verildiğini ve aygıttan veya ağdan izin verildiğini denetlemek veya filtrelemek için tasarlanmıştır.

* **Ağ Katmanı Güvenlik Duvarı** — kaynak ve hedef IP adreslerine göre filtreleme
* **Aktarım Katmanı Güvenlik Duvarı** — kaynak ve hedef veri bağlantı noktalarına göre filtreleme ve bağlantı durumlarına göre filtreleme
* **Uygulama Katmanı Güvenlik Duvarı** — uygulama, program veya hizmete dayalı filtreleme
* **Bağlam Duyarlı Uygulama Güvenlik Duvarı** — kullanıcı, cihaz, rol, uygulama türü ve tehdit profiline göre filtreleme
* **Proxy Sunucusu** - URL, etki alanı, medya vb. Gibi web içerik isteklerinin filtrelenmesi.
* **Ters Proxy Sunucusu** - web sunucularının önüne yerleştirilir, ters proxy sunucuları web sunucularına erişimi korur, gizler, üzerindeki yükü boşaltır ve dağıtır
* **Ağ Adresi Çevirisi (NAT) Güvenlik Duvarı** — ağ ana bilgisayarlarının özel adreslerini gizler veya maskeler
* **Ana bilgisayar tabanlı Güvenlik Duvarı** — tek bir bilgisayar işletim sisteminde bağlantı noktalarının ve sistem servis çağrılarının filtrelenmesi

# Bağlantı Noktası Tarama

# Bağlantı noktası tarama, açık bağlantı noktaları için bir bilgisayar, sunucu veya başka bir ağ ana bilgisayarını sondaj işlemidir.

Bir bağlantı noktasının taranması genellikle üç yanıttan biriyle sonuçlanır:

* **Open veya Accepted** — Ana bilgisayar, bir servisin bağlantı noktasını dinlediğini belirterek cevap vermiştir.
* **Closed, Denied veya Not Listening** — Ana bilgisayar bağlantı noktasına yapılan bağlantıların reddedileceğini belirterek yanıt vermiştir.
* **Filtered, Dropped veya Blocked** — Ana bilgisayardan yanıt alınamamıştır.

# Güvenlik Uygulamaları

# Günümüzde, tüm ağ güvenliği ihtiyaçlarını çözecek tek bir güvenlik cihazı veya teknoloji bulunmamaktadır.

# Güvenlik cihazları, yönlendirici veya güvenlik duvarı, bir ağ aygıtına takılabilen bir kart veya kendi işlemcisine ve önbelleğe alınmış belleğe sahip bir modül gibi bağımsız cihazlar olabilir. Güvenlik cihazları, bir ağ aygıtında çalıştırılan yazılım araçları da olabilir.

**Yönlendiriciler**- Şekil 1'de gösterilen Cisco Entegre Servis Yönlendiricisi (ISR) yönlendiricileri, trafik filtreleme, Güvenli Şifreleme Önleme Sistemi (IPS), şifreleme ve güvenli şifreli tünel oluşturma için VPN yetenekleri de dahil olmak üzere yalnızca yönlendirme işlevlerinin yanı sıra birçok güvenlik duvarı özelliğine sahiptir.

**Güvenlik Duvarları**- Cisco Yeni Nesil Güvenlik Duvarları, bir ISR yönlendiricisinin tüm yeteneklerinin yanı sıra gelişmiş ağ yönetimi ve analitiğine sahiptir. Güvenlik duvarı özelliklerine sahip Cisco Adaptive Security Appliance (ASA) Şekil 2'de gösterilmiştir.

**IPS**- Şekil 3'te gösterilen Cisco Next Generation IPS cihazları, izinsiz girişin önlenmesine adanmıştır.

**VPN**- Cisco güvenlik cihazları Sanal Özel Ağ (VPN) sunucusu ve istemci teknolojileri ile donatılmıştır. Güvenli şifreli tünel açma için tasarlanmıştır.

**Malware/Antivirus**- Cisco Gelişmiş Zararlı Yazılım Koruması (AMP), yeni nesil Cisco yönlendiricileri, güvenlik duvarları, IPS aygıtları, Web ve E-posta Güvenliği Araçlarında gelir ve ayrıca ana bilgisayarlara yazılım olarak yüklenebilir.

**Diğer Güvenlik Cihazları**— Bu kategori web ve e-posta güvenlik cihazları, şifre çözme aygıtları, istemci erişim denetim sunucuları ve güvenlik yönetim sistemleri içerir.

# Gerçek Zamanlı Saldırıları Algılama

* **Edge'den Uç Noktasına Gerçek Zamanlı Tarama**- Saldırıları gerçek zamanlı olarak algılamak, güvenlik duvarı ve IDS/IPS ağ aygıtlarını kullanarak saldırıları aktif olarak taramayı gerektirir. Çevrimiçi küresel tehdit merkezlerine bağlantıları olan yeni nesil istemci/sunucu kötü amaçlı yazılım algılaması da kullanılmalıdır. Günümüzde aktif tarama cihazları ve yazılımları, bağlam tabanlı analiz ve davranış algılamayı kullanarak ağ anomalilerini algılamalıdır.
* **DDoS Saldırıları ve Gerçek Zamanlı Yanıt**- DDoS, gerçek zamanlı tepki ve algılama gerektiren en büyük saldırı tehditlerinden biridir. DDoS saldırılarına karşı savunmak yapmak son derece zordur, çünkü saldırılar yüzlerce veya binlerce zombi bilgisayardan kaynaklanır ve saldırılar resimde gösterildiği gibi meşru trafik olarak görünür. Birçok şirket ve kuruluş için, düzenli olarak oluşan DDoS saldırıları Internet sunucularını ve ağ kullanılabilirliğini engeller. DDoS saldırılarını gerçek zamanlı olarak algılamak ve yanıtlamak çok önemlidir.

# En İyi Güvenlik Uygulamaları

* **Risk Değerlendirmesi Gerçekleştir**— Koruduğunuz şeyin değerini bilmek, güvenlik harcamalarının haklı çıkarılmasına yardımcı olacaktır.
* **Güvenlik İlkesi Oluşturma**— Şirket kurallarını, iş görevlerini ve beklentileri açıkça gösteren bir ilke oluşturun .
* **Fiziksel Güvenlik Önlemleri**— Ağ dolaplarına, sunucu konumlarına ve yangın önleme işlevlerine erişimi kısıtlayın.
* **İnsan Kaynakları Güvenlik Önlemleri**— Çalışanlar arka plan kontrolleri ile düzgün bir şekilde araştırılmalıdır.
* **Yedekleme Yapma ve Test Etme**- Düzenli yedeklemeleri gerçekleştirin ve yedeklerden veri kurtarma testi yapın.
* **Güvenlik Yamalarını ve Güncelleştirmelerini Koruma**— Sunucu, istemci ve ağ aygıtı işletim sistemlerini ve programlarını düzenli olarak güncelleyin.
* **Erişim Denetimlerini Çalıştırma**— Güçlü kullanıcı kimlik doğrulamasının yanı sıra kullanıcı rollerini ve ayrıcalık düzeylerini yapılandırın.
* **Olay Yanıtını Düzenli olarak Test Edin**— Bir olay yanıt ekibi istihdam edin ve acil yanıt senaryolarını test edin.
* **Ağ İzleme, Analiz ve Yönetim Aracı Uygulayın**- Diğer teknolojilerle bütünleşen bir güvenlik izleme çözümü seçin.
* **Ağ Güvenliği Aygıtlarını Uygulama**— Yeni nesil yönlendiricileri, güvenlik duvarlarını ve diğer güvenlik aygıtlarını kullanın.
* **Kapsamlı Uç Nokta Güvenlik Çözümü Uygulama**— Kurumsal düzeyde kötü amaçlı yazılımdan koruma ve virüsten koruma yazılımı kullanın.
* **Kullanıcıları eğitin —**Kullanıcıları ve çalışanları güvenli prosedürlerde eğitin.
* **Verileri şifreleyin**— E-posta dahil tüm hassas şirket verilerini şifreleyin.

# Siber güvenlik eğitimi için en yaygın bilinen ve saygın kuruluşlardan biri SANS Enstitüsüdür.

# Botnet

# Bir botnet, İnternet üzerinden bağlanmış, kötü niyetli bir birey veya grup tarafından kontrol edilebilen bir grup bottur.

# Bir botnet on binlerce hatta yüz binlerce bot içerebilir. Bu botlar kötü amaçlı yazılım dağıtmak, DDoS saldırıları başlatmak, istenmeyen e-posta dağıtmak veya kaba kuvvet şifre saldırıları yürütmek için etkinleştirilebilir.

# Siber Savunmada Ölüm Zinciri

# Siber güvenlikte, Kill Chain (Ölüm Zinciri veya Öldürme Zinciri) bir bilgi sistemleri saldırısının aşamalarıdır.

**1. Aşama: Keşif**- Saldırgan hedef hakkında bilgi toplar.

**2. Aşama: Silahlanma** - Saldırgan hedefe göndermek için bir istismar ve kötü amaçlı yük oluşturur.

**3. Aşama: Teslimat** - Saldırgan, istismar ve kötü amaçlı yükü hedefe e-posta veya başka bir yöntemle gönderir.

**4. Aşama: İstismar** - istismar yürütülür.

**5. Aşama : Kurulum** - Hedefe kötü amaçlı yazılım ve arka kapılar yüklenir.

**6.Aşama. Komut ve Kontrol** - Hedefin uzaktan kontrolü bir komut ve kontrol kanalı veya sunucu aracılığıyla elde edilir.

**7.Aşama. Eylem** - Saldırgan bilgi hırsızlığı gibi kötü amaçlı eylemler gerçekleştirir veya Kill Chain aşamalarında tekrar çalışarak ağdaki diğer cihazlara ek saldırılar gerçekleştirir.

Siber Öldürme Zincirine dayanan bir şirketin güvenlik savunmaları hakkında bazı sorular şunlardır:

• Öldürme Zincirinin her aşamasındaki saldırı göstergeleri nelerdir?

• Her aşamada saldırı göstergelerini tespit etmek için hangi güvenlik araçlarına ihtiyaç vardır?

• Şirketin bir saldırıyı tespit etme yeteneğinde boşluklar var mı?

# Behavior-Based Security

# Davranış tabanlı güvenlik, bilinen kötü amaçlı imzalara dayanmayan ancak ağdaki anormallikleri algılamak için bilgi bağlamı kullanan bir tehdit algılama biçimidir. Davranış tabanlı algılama, yerel ağdaki bir kullanıcı ile yerel veya uzak bir hedef arasındaki iletişim akışını yakalamayı ve analiz etmeyi içerir. Bu iletişimler, yakalanıp analiz edildiğinde, anomalileri tespit etmek için kullanılabilecek bağlam ve davranış kalıplarını ortaya koymaktadır. Davranışa dayalı algılama, normal davranıştan bir değişiklikle saldırının varlığını keşfedebilir.

* **Bal Küpü (Honeypot)** - Honeypot, ilk olarak saldırganın öngördüğü kötü niyetli davranış modeline hitap ederek ilgisini çeken davranışa dayalı bir algılama aracıdır. Ardından, bal küpünün içindeyken, ağ yöneticisi saldırganın davranışını yakalayabilir, günlüğe kaydedebilir ve analiz edebilir. Bu, bir yöneticinin daha fazla bilgi kazanmasına ve daha iyi bir savunma yapmasına olanak tanır.
* **Cisco'nun Siber Tehdit Savunma Çözümü Mimarisi** - Bu, daha fazla görünürlük, bağlam ve kontrol sağlamak için davranış tabanlı algılama ve göstergeler kullanan bir güvenlik mimarisidir. Amaç saldırının kim, ne, nerede, ne zaman ve nasıl gerçekleştiğini bilmektir. Bu güvenlik mimarisi, bu hedefe ulaşmak için birçok güvenlik teknolojisini kullanır.

# NetFlow

# NetFlow teknolojisi, bir ağ üzerinde akan veriler hakkında bilgi toplamak için kullanılır.

# Ağınızdaki kimlerin ve hangi cihazların olduğunu, kullanıcıların ve cihazların ağınıza ne zaman ve nasıl eriştiğini gösterir.

# NetFlow, davranış tabanlı algılama ve analizde önemli bir bileşendir. NetFlow ile donatılmış anahtarlar, yönlendiriciler ve güvenlik duvarları, ağa giren, çıkan ve ağ üzerinden transfer edilen veriler hakkında bilgi raporlayabilir.

# Ağ veri akışları hakkında bilgi toplayarak, NetFlow 90'dan fazla farklı öznitelikte temel davranışlar kurabilir.

# CSIRT

# bilgisayar güvenliği olay raporlarını almak, incelemek ve yanıtlamak için bir Bilgisayar Güvenliği Olay Yanıt Ekibi (CSIRT) vardır. CSIRT'in birincil görevi, bilgisayar güvenliği olaylarıyla ilgili kapsamlı araştırmalar yaparak şirket, sistem ve veri koruma sağlamaya yardımcı olmaktır.

# Security Playbook

# Tüm bu bilgiler bir güvenlik başucu kitabında (security playbook) derlenmelidir. Güvenlik başucu kitabı, güvenlik olayı veri kaynaklarına karşı, olay tespiti ve yanıtına yol açan tekrarlanabilir sorguların (raporların) bir koleksiyonudur.

* Kötü amaçlı yazılım bulaşmış makineleri algılayın.
* Şüpheli ağ etkinliğini algılayın.
* Düzensiz kimlik doğrulama girişimlerini algılayın.
* Gelen ve giden trafiği tanımlar ve anlar.
* Eğilimler, istatistikler ve sayımlar dahil olmak üzere özet bilgileri sağlayın.
* İstatistiklere ve metriklere kullanılabilir ve hızlı erişim sağlayın.
* Etkinlikleri tüm ilgili veri kaynaklarıyla ilişkilendirin.

# Olay Önleme ve Algılama Araçları

* **SIEM**
* — Güvenlik Bilgileri ve Olay Yönetimi (SIEM) sistemi, ağ üzerindeki güvenlik cihazlarından güvenlik uyarılarını, günlükleri ve diğer gerçek zamanlı ve geçmiş verileri toplayan ve analiz eden bir yazılımdır.

# DLP

# — Veri Kaybı Önleme Yazılımı (DLP), hassas verilerin bir ağdan çalınmasını veya kaçmasını engellemek için tasarlanmış bir yazılım veya donanım sistemidir. DLP sistemi dosya erişim yetkilendirmesi, veri alışverişi, veri kopyalama, kullanıcı etkinliği izleme ve daha fazlasına odaklanabilir. DLP sistemleri üç farklı durumda verileri izlemek ve korumak için tasarlanmıştır: kullanımda veri, hareket halinde veri ve dinlenme halinde veri. Kullanılan veriler istemciye odaklanır, hareket halinde veriler ağ üzerinden geçerken verilere atıfta bulunur ve geri kalan veriler veri depolama anlamına gelir.

# Cisco ISE ve TrustSec

# — Cisco Identity Services Engine (Cisco ISE) ve Cisco TrustSec, ağa erişimi (misafirler, mobil kullanıcılar, çalışanlar) daha fazla karmaşıklık olmadan segmente eden rol tabanlı erişim denetimi ilkeleri oluşturarak ağ kaynaklarına erişimi zorlar. Trafik sınıflandırması kullanıcı veya cihaz kimliğine dayanır.

# IDS ve IPS

# Saldırı Algılama Sistemi (IDS), özel bir ağ aygıtı veya bir sunucu ya da güvenlik duvarındaki kötü amaçlı trafik arayan verileri bir kurallar veritabanına veya saldırı imzalarına karşı tarayan birkaç araçtan biridir.

# Saldırı Tespit Sistemi bir eşleşme tespit ettiğinde harekete geçmez, bu nedenle saldırıların gerçekleşmesini engelleyemez. IDS'nin işi sadece algılamak, günlüğe kaydetmek ve rapor etmektir.

# IDS tarafından gerçekleştirilen tarama ağı yavaşlatır (gecikme süresi olarak bilinir). Ağ gecikmesini önlemek için IDS genellikle normal ağ trafiğinden ayrı olarak çevrimdışı olarak yerleştirilir.

# Saldırı Önleme Sistemi (IPS), pozitif bir kural veya imza eşlemesine dayanarak trafiği engelleme veya reddetme yeteneğine sahiptir. En iyi bilinen IPS/IDS sistemlerinden biri Snort'dur. Snort'un ticari sürümü Cisco’nun Sourcefire’ıdır. Sourcefire gerçek zamanlı trafik ve port analizi, günlüğe kaydetme, içerik arama ve eşleştirme yapma yeteneğine sahiptir ve sondaları (probes), saldırıları ve port taramalarını algılayabilir. Ayrıca raporlama, performans ve günlük analizi için diğer üçüncü taraf araçlarıyla da bütünleşir.

# KAVRAMLAR

# açık bağlantı noktaları için bir bilgisayar, sunucu veya başka bir ağ ana bilgisayarını sondalama işlemi: port tarama

# hangi trafiğe izin verildiğini kontrol ederek ağı korur, hem de izin verilir: güvenlik duvarı

# Doğru ya da Yanlış. Bugün bir kuruluşun tüm ağ güvenlik ihtiyaçlarını çözecek tek güvenlik cihazları bulunmaktadır.: yanlış

# Bu saldırı, sunucuları ve sahte trafiğe sahip ağ aygıtlarını basitçe ezerek hizmetleri bozar.: DdoS

# ağ dolaplarına, sunucu konumlarına ve yangın önleme erişimini kısıtlayan bir güvenlik önlemi türü: Fiziksel Güvenlik

# Doğru ya da Yanlış. Bir botnet on binlerce hatta yüz binlerce bot olabilir.: doğru

# bir bilgi sistemleri saldırısının aşamalarının kavramsal bir taslağı: Öldürme Zinciri

# pozitif bir kural veya imza eşleşmesine dayanarak trafiği engelleme veya reddetme yeteneğine sahip bir güvenlik cihazı: IPS/IDS

# ağ üzerinden akan veriler hakkında bilgi toplamak için kullanılan bir araç: NetFlow