Intro to Defensive Security

Task 1 Introduction to Defensive Security (Defansif Güvenliğe Giriş)

Saldırgan güvenlik tek bir şeye odaklanır: sistemlere sızmak. Sistemlere sızmak, diğer şeylerin yanı sıra hatalardan faydalanarak, güvensiz kurulumları kötüye kullanarak ve uygulanmayan erişim kontrol politikalarından yararlanarak gerçekleştirilebilir. Kırmızı ekipler ve sızma test uzmanları saldırgan güvenlik konusunda uzmanlaşmıştır.

Savunma güvenliği, iki ana görevle ilgilendiği için saldırı güvenliğinin tam tersidir:

İzinsiz girişlerin meydana gelmesini önleme: İzinsiz girişleri meydana geldiklerinde tespit etme ve uygun şekilde yanıt verme

Mavi ekipler savunma amaçlı güvenlik ortamının bir parçasıdır.

Savunma güvenliği ile ilgili görevlerden bazıları şunlardır:

Kullanıcı siber güvenlik farkındalığı: Kullanıcıların siber güvenlik konusunda eğitilmesi, sistemlerini hedef alan çeşitli saldırılara karşı korunmalarına yardımcı olur.

Varlıkların belgelenmesi ve yönetilmesi: Düzgün bir şekilde yönetmek ve korumak için sahip olduğumuz sistem ve cihaz türlerini bilmemiz gerekir.

Sistemlerin güncellenmesi ve yamalanması: Bilgisayarların, sunucuların ve ağ cihazlarının doğru
şekilde güncellendiğinden ve bilinen tüm güvenlik açıklarına (zayıflıklara) karşı yamalandığından emin olmak.

Önleyici güvenlik cihazlarının kurulması: güvenlik duvarı ve saldırı önleme sistemleri (IPS) önleyici güvenliğin kritik bileşenleridir. Güvenlik duvarları hangi ağ trafiğinin içeri girebileceğini ve sistemden veya ağdan nelerin çıkabileceğini kontrol eder. IPS, mevcut kurallar ve saldırı
imzalarıyla eşleşen tüm ağ trafiğini engeller.

Kayıt ve izleme cihazlarının kurulması: Ağın uygun şekilde günlüğe kaydedilmesi ve izlenmesi olmadan, kötü niyetli faaliyetleri ve izinsiz girişleri tespit etmek mümkün olmayacaktır. Ağımızda yeni bir yetkisiz cihaz ortaya çıkarsa, bunu bilebilmeliyiz.

Savunma güvenliğinde çok daha fazlası vardır ve yukarıdaki liste yalnızca birkaç genel konuyu kapsamaktadır.

Bu odada şunları ele alıyoruz:

Security Operations Center (Güvenlik Operasyonları Merkezi) (SOC)

Threat Intelligence (Tehdit İstihbaratı)

Digital Forensics and Incident Response (Dijital Adli Tıp ve Olay Müdahalesi) (DFIR)

Malware Analysis (Kötü Amaçlı Yazılım Analizi)

soru ⇒

Hangi takım savunma güvenliğine odaklanır?

cevap ⇒ **Blue Team**

Task 2 Areas of Defensive Security

Bu görevde, savunma güvenliği ile ilgili iki ana konuyu ele alacağız:

Tehdit İstihbaratını kapsadığımız Güvenlik Operasyon Merkezi (SOC)

Kötü Amaçlı Yazılım Analizini de kapsadığımız Dijital Adli Tıp ve Olay Müdahalesi (DFIR)

Güvenlik Operasyonları Merkezi (SOC)

Güvenlik Operasyon Merkezi (SOC), kötü niyetli siber güvenlik olaylarını tespit etmek için ağı ve sistemlerini izleyen siber güvenlik uzmanlarından oluşan bir ekiptir. Bir SOC için ana ilgi alanlarından bazıları şunlardır:

Güvenlik açıkları: Bir sistem güvenlik açığı (zayıflığı) keşfedildiğinde, uygun bir güncelleme veya yama yükleyerek bunu düzeltmek çok önemlidir. Bir düzeltme mevcut olmadığında, bir saldırganın bunu istismar etmesini önlemek için gerekli

önlemler alınmalıdır. Güvenlik açıklarının giderilmesi bir SOC için hayati önem taşısa da, bu görevin mutlaka onlara verilmesi gerekmez.

Politika ihlalleri: Bir güvenlik politikasını, ağın ve sistemlerin korunması için gerekli bir dizi kural olarak düşünebiliriz. Örneğin, kullanıcıların gizli şirket verilerini çevrimiçi bir depolama hizmetine yüklemeye başlaması bir politika ihlali olabilir.

Yetkisiz etkinlik: Bir kullanıcının oturum açma adı ve parolasının çalındığı ve saldırganın bunları ağa giriş yapmak için kullandığı durumu düşünün. Bir SOC'nin böyle bir olayı tespit etmesi ve daha fazla zarar verilmeden önce mümkün olan en kısa sürede engellemesi gerekir.

Ağa izinsiz girişler: Güvenliğiniz ne kadar iyi olursa olsun, izinsiz giriş için her zaman bir şans vardır. İzinsiz giriş, bir kullanıcı kötü amaçlı bir bağlantıya tıkladığında veya bir saldırgan genel bir sunucudan yararlandığında meydana gelebilir. Her iki durumda da, bir izinsiz giriş meydana geldiğinde, daha fazla hasarı önlemek için bunu mümkün olan en kısa sürede tespit etmeliyiz.

Güvenlik operasyonları, korumayı sağlamak için çeşitli görevleri kapsar; bu görevlerden biri de tehdit istihbaratıdır.

Tehdit İstihbaratı

Bu bağlamda istihbarat, gerçek ve potansiyel düşmanlar hakkında topladığınız bilgileri ifade eder. Tehdit, bir sistemi bozabilecek veya olumsuz etkileyebilecek herhangi bir eylemdir. Tehdit istihbaratı, şirketin potansiyel düşmanlara karşı daha iyi hazırlanmasına yardımcı olmak için bilgi toplamayı amaçlar. Amaç, tehdide göre bilgilendirilmiş bir savunma elde etmektir. Farklı şirketlerin farklı düşmanları vardır. Bazı düşmanlar bir mobil operatörden müşteri verilerini çalmak isteyebilir; ancak diğer düşmanlar bir petrol rafinerisindeki üretimi durdurmakla ilgilenir. Örnek düşmanlar arasında siyasi nedenlerle çalışan bir ulus-devlet siber ordusu ve finansal amaçlarla hareket eden bir fidye yazılımı grubu yer alır. Şirkete (hedefe) bağlı olarak, düşmanlar bekleyebiliriz.

İstihbaratın veriye ihtiyacı vardır. Veriler toplanmalı, işlenmeli ve analiz edilmelidir. Veri toplama ağ günlükleri gibi yerel kaynaklardan ve forumlar gibi halka açık kaynaklardan yapılır. Verilerin işlenmesi, bunların analiz için uygun bir formatta düzenlenmesini amaçlar. Analiz aşaması saldırganlar ve motivasyonları hakkında daha fazla bilgi bulmayı amaçlar; ayrıca bir öneriler listesi ve eyleme geçirilebilir adımlar oluşturmayı hedefler.

Düşmanlarınız hakkında bilgi edinmek onların taktiklerini, tekniklerini ve prosedürlerini bilmenizi sağlar. Tehdit istihbaratının bir sonucu olarak, tehdit aktörünü (düşmanı) tanımlar, faaliyetlerini tahmin eder ve sonuç olarak saldırılarını hafifletebilir ve bir yanıt stratejisi hazırlayabiliriz.

Dijital Adli Tıp ve Olay Müdahalesi (DFIR)

Bu bölüm Dijital Adli Tıp ve Olay Müdahalesi (DFIR) hakkındadır ve bu konuyu ele alacağız:

Digital Forensics (Dijital Adli Tıp)

Incident Response (Olay Müdahalesi)

Malware Analysis (Kötü Amaçlı Yazılım Analizi)

Digital Forensics (Dijital Adli Tıp);

Adli tıp, suçları araştırmak ve gerçekleri ortaya çıkarmak için bilimin uygulanmasıdır. Bilgisayarlar ve akıllı telefonlar gibi dijital sistemlerin kullanımı ve yaygınlaşmasıyla birlikte, ilgili suçları araştırmak için yeni bir adli tıp dalı doğmuştur: bilgisayar adli bilimi, daha sonra dijital adli bilime dönüşmüştür.

Savunma amaçlı güvenlikte, dijital adli bilişimin odak noktası bir saldırının ve faillerinin kanıtlarını ve fikri mülkiyet hırsızlığı, siber casusluk ve yetkisiz içerik bulundurma gibi diğer alanları analiz etmeye kayar. Sonuç olarak, dijital adli bilişim aşağıdaki gibi farklı alanlara odaklanacaktır:

Dosya Sistemi: Bir sistemin depolama alanının dijital adli tıp görüntüsünün (düşük seviyeli kopya) analiz edilmesi, yüklü programlar, oluşturulan dosyalar, kısmen üzerine yazılan dosyalar ve silinen dosyalar gibi birçok bilgiyi ortaya çıkarır.

Sistem belleği: Saldırgan kötü amaçlı programını diske kaydetmeden bellekte çalıştırıyorsa, sistem belleğinin adli görüntüsünü (düşük seviyeli kopyasını) almak, içeriğini analiz etmenin ve saldırı hakkında bilgi edinmenin en iyi yoludur.

Sistem günlükleri: Her istemci ve sunucu bilgisayar, neler olup bittiğiyle ilgili farklı günlük dosyaları tutar. Günlük dosyaları bir sistemde neler olduğu hakkında birçok bilgi sağlar. Saldırgan izlerini temizlemeye çalışsa bile bazı izler kalacaktır.

Ağ günlükleri: Bir ağdan geçen ağ paketlerinin günlükleri, bir saldırının gerçekleşip gerçekleşmediği ve neleri içerdiği hakkında daha fazla soruyu yanıtlamaya yardımcı olacaktır.

Incident Response (Olay Müdahalesi);

Bir olay genellikle bir veri ihlali veya siber saldırı anlamına gelir; ancak bazı durumlarda yanlış yapılandırma, izinsiz giriş girişimi veya politika ihlali gibi daha az kritik bir şey olabilir. Siber saldırı örnekleri arasında bir saldırganın ağımızı veya sistemlerimizi erişilemez hale getirmesi, genel web sitesini tahrif etmesi (değiştirmesi) ve veri ihlali (şirket verilerini çalması) sayılabilir. Bir siber saldırıya nasıl yanıt verirsiniz? Olay müdahalesi, böyle bir durumla başa çıkmak için izlenmesi gereken metodolojiyi belirtir. Amaç, hasarı azaltmak ve mümkün olan en kısa sürede iyileşmektir. İdeal olarak, olay müdahalesi için hazır bir plan geliştirirsiniz.

Olay müdahale sürecinin dört ana aşaması şunlardır:

Hazırlık: Bu, olaylarla başa çıkmak için eğitilmiş ve hazır bir ekip gerektirir. İdeal olarak, olayların ilk etapta meydana gelmesini önlemek için çeşitli önlemler alınır.

Tespit ve Analiz: Ekip, herhangi bir olayı tespit etmek için gerekli kaynaklara sahiptir; ayrıca, tespit
edilen herhangi bir olayın ciddiyetini öğrenmek için daha fazla analiz edilmesi esastır.

Kontrol Altına Alma, Yok Etme ve Kurtarma: Bir olay tespit edildiğinde, diğer sistemleri etkilemesini önlemek, ortadan kaldırmak ve etkilenen sistemleri kurtarmak çok önemlidir. Örneğin, bir sisteme bilgisayar virüsü bulaştığını fark ettiğimizde, virüsün diğer sistemlere yayılmasını durdurmak (kontrol altına almak), virüsü temizlemek (ortadan kaldırmak) ve sistemin düzgün bir şekilde kurtarılmasını sağlamak isteriz.

Olay Sonrası Faaliyet: Başarılı bir kurtarma işleminden sonra bir rapor hazırlanır ve gelecekte benzer olayların önlenmesi için öğrenilen ders paylaşılır.

Malware Analysis (Kötü Amaçlı Yazılım Analizi);

Malware, kötü amaçlı yazılım anlamına gelir. Yazılım, bir diske kaydedebileceğiniz veya ağ üzerinden gönderebileceğiniz programları, belgeleri ve dosyaları ifade eder. Kötü amaçlı yazılımlar, aşağıdakiler gibi birçok türü içerir:

Virüs, kendisini bir programa ekleyen bir kod parçasıdır (bir programın parçası). Bir bilgisayardan diğerine yayılmak üzere tasarlanmıştır; ayrıca, bir bilgisayara bulaştığında dosyaları değiştirerek, üzerine yazarak ve silerek çalışır. Sonuç, bilgisayarın yavaşlamasından kullanılamaz hale gelmesine kadar değişir.

Truva Atı, arzu edilen bir işlevi gösteren ancak altında kötü niyetli bir işlevi gizleyen bir programdır. Örneğin, bir kurban şüpheli bir web sitesinden saldırgana sistemi üzerinde tam kontrol sağlayan bir video oynatıcı indirebilir.

Fidye yazılımı, kullanıcının dosyalarını şifreleyen kötü amaçlı bir programdır. Şifreleme, şifreleme parolası bilinmeden dosyaları okunamaz hale getirir. Saldırgan, kullanıcı bir "fidye" ödemeye razı olursa kullanıcıya şifreleme parolasını sunar.

Kötü amaçlı yazılım analizi, çeşitli araçlar kullanarak bu tür kötü amaçlı programlar hakkında bilgi edinmeyi amaçlar:

Statik analiz, kötü niyetli programı çalıştırmadan inceleyerek çalışır. Bu genellikle assembly dili (işlemcinin komut seti, yani bilgisayarın temel talimatları) hakkında sağlam bilgi gerektirir.

Dinamik analiz, kötü amaçlı yazılımı kontrollü bir ortamda çalıştırarak ve faaliyetlerini izleyerek çalışır. Kötü amaçlı yazılımın çalışırken nasıl davrandığını gözlemlemenizi sağlar.

soru⇒

Bir ağı ve sistemlerini kötü niyetli olaylara karşı izleyen siber güvenlik uzmanlarından oluşan bir ekibe ne ad verirsiniz(ipucu= SOC)?

cevap ⇒ **Security Operations Center**

soru ⇒

DFIR ne anlama geliyor?

cevap ⇒ **Digital Forensics and Incident Response**

soru ⇒

Hangi tür kötü amaçlı yazılım, kullanıcının dosyalarına yeniden erişim sağlamak için para ödemesini gerektirir?

cevap ⇒ **ransomware**

Task 3 Practical Example of Defensive Security (Savunmacı Güvenliğe Pratik Bir Örnek)

Bir güvenlik analisti olarak yapacağınız tipik bir görev ne olabilir? Bayrağı alana kadar takip etmek için "Siteyi Görüntüle "ye tıklayın. (İlk kez bayrak alıyorsanız, bayrak bir görevi tamamladığınızda aldığınız bir metin dizisi olarak görülebilir. Örnek bir bayrak FLAG{WORDS_AND_MORE} şeklindedir).

Bir bankanın korunmasından sorumlu bir Güvenlik Operasyon Merkezi'nin (SOC) parçasısınız. Bu bankanın SOC'si bir Güvenlik Bilgi ve Olay Yönetimi (SIEM) sistemi kullanmaktadır. Bir SIEM, çeşitli kaynaklardan güvenlikle ilgili bilgi ve olayları toplar ve bunları tek bir sistem üzerinden sunar. Örneğin, başarısız bir oturum açma girişimi veya beklenmedik bir coğrafi konumdan oturum açma girişimi olduğunda bilgilendirilirsiniz. Dahası, makine öğreniminin ortaya çıkmasıyla, bir SIEM, genellikle yalnızca çalışma saatlerinde oturum açan bir kullanıcının gece 3'te oturum açması gibi olağandışı davranışları tespit edebilir.

Bu alıştırmada, ağımızdaki ve sistemlerimizdeki farklı olayları gerçek zamanlı olarak izlemek için bir SIEM ile etkileşime gireceğiz. Olaylardan bazıları tipik ve zararsızdır; diğerleri ise bizim daha fazla müdahalemizi gerektirebilir. Kırmızı ile işaretlenmiş olayı bulun, not alın ve daha fazla inceleme için üzerine tıklayın.

Ardından, şüpheli etkinlik veya olay hakkında daha fazla bilgi edinmek istiyoruz. Şüpheli olay, yerel bir kullanıcı, yerel bir bilgisayar veya uzak bir IP adresi gibi bir olay tarafından tetiklenmiş olabilir. Posta göndermek ve almak için fiziksel bir adrese ihtiyacınız vardır; benzer şekilde, İnternet üzerinden veri göndermek ve almak için bir IP adresine ihtiyacınız vardır. IP adresi, İnternet üzerinden iletişim kurmanızı sağlayan mantıksal bir adrestir. Olayın gerçekten kötü niyetli olup olmadığını doğrulamak için tetikleyicinin nedenini inceleriz. Kötü niyetliyse, SOC'deki başka birine bildirmek ve IP adresini engellemek gibi gerekli önlemleri almamız gerekir.

soru ⇒

Takip ederek elde ettiğiniz bayrak nedir?

cevap ⇒ **THM{THREAT-BLOCKED}**