Katılım öncesi

İçerikler

Genel Bakış

PTES'in bu bölümünün amacı, bir penetrasyon testinin başarılı bir ön segment adımında yardımcı olan mevcut araç ve teknikleri sunmak ve açıklamaktır. Bu bölümdeki bilgiler, dünyanın en başarılı penetrasyon testçilerinden bazılarının uzun yılların birleşik deneyiminin sonucudur.

Penetrasyon testi arayan bir müşteriyseniz, bu belgenin Genel Sorular bölümüne gitmenizi şiddetle tavsiye ederiz. Bir test başlamadan önce cevaplanması gereken önemli soruları kapsar. Unutmayın, bir penetrasyon testi çatışmacı olmamalıdır. Test cihazının sizi "hackleyip hackleyemeyeceğini" görmek için bir etkinlik olmamalıdır. Bu, iş riskinin belirlenmesi ve saldırı ile ilgili olması gerekir.

Maksimum değer elde etmek için, bu belgedeki soruların kapsandığından emin olun. Ayrıca, Kapsam faaliyeti ilerledikçe, iyi bir test firması kuruluşunuza uyarlanmış ek sorular sormaya başlayacaktır.

Kapsama Giriş

Kapsamı tanımlamak, muhtemelen bir penetrasyon testinin en önemli bileşenlerinden biridir, ancak aynı zamanda en çok göz ardı edilenlerden biridir. Bir ağa erişmek için kullanılabilecek farklı araçlar ve teknikler hakkında birçok cilt yazılırken, penetrasyondan önce gelen konuyla ilgili çok az şey yazılmıştır: hazırlık. Önleme faaliyetlerini düzgün bir şekilde tamamlamayı ihmal etmek, penetrasyon test cihazını (veya firması) kapsam sürünmesi, tatmin edilmemiş müşteriler ve hatta yasal sıkıntılar da dahil olmak üzere bir dizi baş ağrısına açma potansiyeline sahiptir. Bir projenin kapsamı özellikle neyin test edileceğini tanımlar. Testin her yönü nasıl yürütüleceği, Katılım Kuralları bölümünde ele alınacaktır.

Bir angajmanı kapmanın önemli bir bileşeni, test edenlerin zamanlarını nasıl harcamaları gerektiğini özetlemektir. Örnek olarak, bir müşteri, yüz IP adresinin 100.000 $ fiyatı için test edilmesini talep eder. Bu, müşterinin test edilen IP adresi başına 1.000 dolar teklif ettiği anlamına gelir. Bununla birlikte, bu maliyet yapısı sadece bu hacimde etkili olmaya devam etmektedir. Bazı testçilerin içine düştüğü yaygın bir tuzak, test süreci boyunca doğrusal maliyetleri korumaktır. Müşteri sadece bir iş açısından kritik uygulamanın aynı fiyatlandırma yapısında (1.000 $) test edilmesini isteseydi, test cihazı hala sadece tek bir IP'ye saldıracak olsa da, iş hacmi çarpıcı bir şekilde artmıştır. Yapılan işlere göre maliyetleri değiştirmek önemlidir. Aksi takdirde,

bir firma kendilerini hizmetleri için kolayca düşük ücretlendirir, bu da onları tam bir işten daha az yapmaya motive eder.

Sağlam bir fiyatlandırma yapısına sahip olmasına rağmen, süreç tamamen siyah ve beyaz değildir. Bir müşterinin tam olarak ne test edilmesi gerektiğinin tam olarak farkında olmadan nadir değildir. Müşterinin testten beklediklerini etkili bir şekilde nasıl ileteceğini bilmemesi de mümkündür. Anma Öncesi aşamasında, testçinin bir müşteri için keşfedilmemiş bir bölge olabilecek bir rehber olarak hizmet verebilmesi önemlidir. Test cihazı, ciddi bir yoğunluğa sahip tek bir uygulamaya odaklanan bir test ile müşterinin test etmek için çok çeşitli IP adresleri sağladığı bir test arasındaki farkı anlamalıdır ve amaç sadece bir yol bulmaktır.

Zaman Tahmini Metrikler

Zaman tahminleri, belirli bir alanda bir test cihazının deneyimine doğrudan bağlıdır. Bir test cihazının belirli bir testte önemli bir deneyimi varsa, muhtemelen bir testin ne kadar süreceğini indoten indirebilir. Test cihazı bölgede daha az deneyime sahipse, e-postaları yeniden okumak ve önceki benzer testlerden gelen günlükleri taramak, firmanın yaptığı mevcut angajman için zaman gereksinimini tahmin etmenin harika bir yoludur. Test zamanı belirlendikten sonra, zamana %20 eklemek için ihtiyatlı bir uygulamadır.

Zaman değerinin arka ucundaki ekstra% 20'ye dolgu denir. Danışman çevreleri dışında, bu aynı zamanda genel olarak danışman olarak da adlandırılır. Yastık, herhangi bir test için mutlak bir gerekliliktir. Testte herhangi bir kesinti meydana gelirse bir yastık sağlar. Yaygın olarak ortaya çıkan ve test sürecini engelleyen birçok olay vardır. Örneğin, bir ağ segmenti düşebilir veya birçok yönetim seviyesiyle ele alınması gereken birçok toplantı gerektiren önemli bir güvenlik açığı bulunabilir. Bu olayların her ikisi de zaman alıcıdır ve dolgunun yerinde değilse orijinal zaman tahminini önemli ölçüde etkiler.

%20 dolgusu gerekli değilse ne olur? Müşteriyi zamanında işe yaramamak için faturalandırmak son derece etik değildir, bu nedenle, katılım süresi sınırının vurulması durumunda normalde sağlanmamış olabilecek ek değer sağlamak testçilere kalmıştır. Örnekler arasında şirket güvenlik ekibini güvenlik açığından yararlanmak için atılan adımlarla yürümeyi, orijinal teslim edilebilir listenin bir parçası değilse bir yönetici özeti sağlamayı veya ilk test sırasında zor olan bir güvenlik açığını kırmaya çalışmak için biraz daha fazla zaman harcamayı içerir.

Zaman ve test metriklerinin bir başka bileşeni, her projenin kesin bir ölü tarihe sahip olması gerektiğidir. Tüm iyi projeler iyi tanımlanmış bir başlangıç ve sona sahiptir. Çalışmayı ve testin sona ereceği belirli bir tarihe vardığınız süreyi veya bu tarihten sonra herhangi bir ek test veya çalışma talep edilip edilmediğini belirten imzalı bir çalışma beyanına sahip olmanız gerekecektir. Bazı testçiler bunu yaparken zor zamanlar geçirirler, çünkü maliyet ve saatler söz konusu olduğunda çok fazla acı çektiklerini hissederler. Bununla birlikte, yazarın deneyimi olmuştur ki, ana test için olağanüstü bir değer sağlarsanız, müşterinin ek iş için size ödeme yapmayacağıdır.

Kapsamlı Toplantı

Çoğu durumda, sözleşme imzalandıktan sonra kapsam toplantısı gerçekleşecektir. Durumlar, sözleşme imzalanmadan önce kapsamla ilgili konuların birçoklarının tartışılabileceği yerlerde gerçekleşir, ancak çok az ve çok uzaktır. Bu durumlar için, herhangi bir derinlemesine kapsam tartışması gerçekleşmeden önce bir gizlilik anlaşmasının imzalanması önerilir.

Kapsam toplantısının amacı neyin test edileceğini tartışmak. Bu toplantıda angajman ve maliyet kuralları karşılanmayacaktır. Bu konuların her biri, her parçanın bu toplantının odak noktası olduğu toplantılarda ele alınmalıdır. Bu yapılır, çünkü odak açıkça belirtilmediği takdirde tartışmalar kolayca karıştırılabilir ve karıştırılabilir. Moderatör olarak hareket etmek ve tartışmaları konulu tutmak, teğetleri önlemek ve

gerektiğinde bazı konuları çevrimdışı tartışma için daha uygun ilan etmek önemlidir.

Artık proje için zorlu bir büyüklük sırası (ROM) değeri kurulduğuna göre, varsayımları doğrulamak için müşteriyle bir toplantı yapma zamanıdır. İlk olarak, giriş için hangi IP aralıklarının kapsamında olduğu açıkça kurulması gerekir. Bir müşterinin dirençli olması ve testçinin ağını tanımlamasının ve ona saldırmasının, testi mümkün olduğunca gerçekçi hale getirmesinin doğrulayıcı olduğunu varsayması nadir değildir. Bu gerçekten de ideal bir durum olacaktır, ancak olası yasal sonuçların her şeyden önce düşünülmesi gerekir. Bu nedenle, bir müşteriye bu endişeleri iletmek ve onlara örtük bir kepçelemenin önemini vermek test cihazının sorumluluğundadır. Örneğin, toplantıda, müşterinin aşağıdakiler de dahil olmak üzere tüm hedef ortamlara sahip olduğu doğrulanmalıdır: DNS sunucusu, e-posta sunucusu, web sunucularının çalıştırdığı gerçek donanım ve güvenlik duvarı / IDS / IPS çözümü. Bu cihazların yönetimini üçüncü taraflara dış kaynak sağlayacak bir dizi şirket var.

Ek olarak, hedef ortamların faaliyet gösterdiği ülkeler, iller ve devletler tanımlanmalıdır. Yasalar bölgeden bölgeye değişir ve testler bu yasalardan çok etkilenebilir. Örneğin, Avrupa Birliği'ne ait ülkelerin, bir sosyal mühendislik katılımının yürütülme şeklini önemli ölçüde değiştirebilecek bireylerin mahremiyetini çevreleyen çok katı yasalara sahip oldukları bilinmektedir.

Saatlik Orana Göre Ek Destek

Nişan kapsamında açıkça örtülmeyen her şey çok dikkatli bir şekilde ele alınmalıdır. Bunun ilk nedeni kapsam sürünmesidir. Kapsam genişledikçe, kaynaklar tüketilir, test cihazı için karları keser ve hatta müşterinin karı oluşturabilir. Birçok testçinin ad-hoc temelinde ek çalışmalar yaparken düşünmediği başka bir konu daha var: yasal sonuçlar. Birçok ad-hoc talebi doğru bir şekilde belgelenmez, bu nedenle bir anlaşmazlık veya yasal işlem durumunda kimin ne söylediğini belirlemek zor olabilir. Ayrıca, sözleşme yapılacak olan işi belirten yasal bir belgedir. Notu test etme iznine sıkıca bağlı olmalıdır.

Orijinal kapsamın dışındaki herhangi bir talep, yapılacak işi açıkça tanımlayan bir çalışma beyanı şeklinde belgelenmelidir. Ayrıca, sözleşmede saatte sabit bir ücret karşılığında ek iş yapılacağının açıkça belirtilmesini ve imzalanmış ve karşı imzalı bir KÖKÜM yerine gelene kadar ek işlerin tamamlanamayacağını açıkça belirtmesini öneriyoruz.

Anketler

Müşteri ile ilk iletişim sırasında, müşterinin katılım kapsamı için cevaplaması gereken birkaç soru doğrulanabilir. Bu sorular, müşterinin penetrasyon testinden ne elde etmek istediğini, müşterinin neden çevrelerine karşı bir penetrasyon testi yaptırmak istediğini ve penetrasyon testi sırasında belirli test türlerini isteyip istemediklerini daha iyi anlamak için tasarlanmıştır. Aşağıdakiler, bu aşamada sorulabilecek örnek sorulardır.

Genel Sorular

Ağ Penetrasyon Testi

1. Müşteri neden nüfuz testine sahip olmak onların çevresine karşı yapılıyor?
2. Penetrasyon testi belirli bir uyum şartı için gerekli midir?
3. Müşteri, yapılan penetrasyon testinin aktif kısımlarını (skorku, numaralandırma, sömürü vb.) ne zaman istiyor?

    1. İş saatleri içinde mi?
    2. İş saatlerinden sonra mı?
    3. Hafta sonları mı?
4. Kaç tane IP adresi test ediliyor?
    1. Uygunsa kaç dahili IP adresi?
    2. Varsa kaç harici IP adresi?
5. Güvenlik duvarı, saldırı tespiti / önleme sistemi, web uygulaması güvenlik duvarı veya yük bakkaliye gibi bir penetrasyon testinin sonuçlarını etkileyebilecek herhangi bir cihaz var mı?
6. Bir sisteme nüfuz edilir durumda, test ekibi nasıl ilerlemelidir?
    1. Ele geçirilen makinede yerel bir güvenlik açığı değerlendirmesi yapın?
    2. Ele geçirilen makinede en yüksek ayrıcalıkları (Unix makinelerinde, SISTEM'in veya Windows'taki Yöneticide) temellerini kazanmaya çalışmak?
    3. Elde edilen yerel şifre karmalarına (örneğin, /etc / shadow) karşı hayır, minimum, sözlük veya kapsamlı şifre saldırıları yapın?

Web Uygulama Penetrasyon Testi

1. Kaç tane web uygulaması değerlendiriliyor?
2. Kaç tane oturum açma sistemi değerlendiriliyor?
3. Kaç tane statik sayfa değerlendiriliyor? (yaklaşık)
4. Kaç tane dinamik sayfa değerlendiriliyor? (yaklaşık)
5. Kaynak kodu kolayca temin edilebilir mi?
6. Herhangi bir belge olacak mı?
    1. Eğer evet, ne tür belgeler?
7. Bu uygulamada statik analiz yapılacak mı?
8. Müşteri bu uygulamaya karşı bu musluk yapılmasını istiyor mu?
9. Müşteri bu uygulamaya karşı rol tabanlı test yapılmasını istiyor mu?
10. Müşteri, web uygulamalarının güvenilir taramalarını istiyor mu?

Kablosuz Ağ Penetrasyon Testi

1. Kaç tane kablosuz ağ mevcut?
2. Misafir kablosuz ağ kullanılır mı? Eğer öyleyse:
    1. Konuk ağ kimlik doğrulaması gerektiriyor mu?
    2. Kablosuz ağlarda ne tür şifreleme kullanılır?
    3. Kapsamın kare görüntüleri nedir?
    4. Rogue cihazların numaralandırılması gerekli olacak mı?
    5. Ekip müşterilere karşı kablosuz saldırıları değerlendirecek mi?
    6. Kablosuz ağı yaklaşık kaç müşteri kullanacak?

Fiziksel Penetrasyon Testi

1. Kaç yer değerlendiriliyor?
2. Bu fiziksel konum ortak bir tesis mi? Eğer öyleyse:
    1. Kapsamında kaç kat var?
    2. Hangi katlar kapsamda?
3. Bypass edilmesi gereken güvenlik görevlileri var mı? Eğer öyleyse:
    1. Güvenlik görevlileri 3. parti aracılığıyla istihdam ediliyor mu?
    2. Onlar silahlı mı?
    3. Güç kullanmalarına izin veriliyor mu?
4. Binaya kaç giriş var?
5. Kilitleme turlarının veya tümsek tuşlarının kullanımına izin veriliyor mu? (Ayrıca yerel yasaları da göz önünde bulundurun)
6. Bu testin amacı mevcut politikalara ve prosedürlere uygunluğu doğrulamak mı yoksa denetim yapmak mı?
7. Alanın kare görüntüleri nedir?
8. Tüm fiziksel güvenlik önlemleri belgelendi mi?
9. Video kameralar kullanılıyor mu?
    1. Kameralar müşteriye ait mi? Eğer öyleyse:
        1. Ekip, video kamera verilerinin depolandığı yere erişmeye çalışmalı mı?
10. Silahlı alarm sistemi kullanılıyor mu? Eğer öyleyse:
    1. Alarm sessiz bir alarm mı?
    2. Alarm hareketle tetiklenir mi?
    3. Alarm kapıların ve pencerelerin açılmasıyla tetiklenir mi?

Sosyal Mühendislik

1. Müşterinin, bir Sosyal Mühendislik saldırısının karşı yapılmasını istedikleri e-posta adreslerinin bir listesi var mı?
2. Müşterinin, karşı yapılacak bir Sosyal Mühendislik saldırısından hoşlanacakları telefon numaralarının bir listesi var mı?
3. Sosyal Mühendislik yetkisiz fiziksel erişim kazanmak amacıyla onaylanır mı? Eğer öyleyse:
    1. Kaç kişi hedef alınacak?

Farklı test seviyelerinin bir parçası olarak, İş Birimi Yöneticileri, Sistem Yöneticileri ve Masa Personeli Yardımı için soruların gerekli olmayabileceğini belirtmek gerekir. Ancak bu soruların gerekli olması durumunda aşağıda bazı örnek sorular bulunabilir.

İş Birimi Yöneticileri için Sorular

1. Yönetici bir testin gerçekleştirilmek üzere olduğunun farkında mı?
2. Açıkta kalırsa, yozlaşmış veya silinirse örgüt için en büyük riski yaratacak ana veri nedir?

3. İş uygulamalarının düzgün çalıştığını doğrulamak için test ve doğrulama prosedürleri mi?
4. Test cihazları, uygulamanın ilk geliştirildiği zamandan itibaren Kalite Güvence testi prosedürlerine erişebilecek mi?
5. Uygulama verileri için Afet Kurtarma Prosedürleri yerinde mi?

Sistem Yöneticileri için Sorular

1. Kırılgan olarak nitelendirilebilecek sistemler var mı? (Çökme eğilimleri, eski işletim sistemleri veya yamalanmamış sistemler)
2. Ağın üzerinde müşterinin sahip olmadığı, test etmek için ek onay gerektirebilecek sistemler var mı?
3. Değişim Yönetimi prosedürleri yerinde mi?
4. Sistem kesintilerini onarmak için ortalama zaman nedir?
5. Herhangi bir sistem izleme yazılımı yerinde midir?
6. En kritik sunucular ve uygulamalar nelerdir?
7. Yedekler düzenli olarak test edilir mi?
8. Yedekler en son ne zaman restore edildi?

Kaplı Sürünme

Kapsam sürünmesi, bir penetrasyon test firmasını işten çıkarmanın en etkili yollarından biridir. Sorun şu ki, birçok şirket ve yönetici bunu nasıl tanımlayacakları veya gerçekleştiğinde buna nasıl tepki vereceği hakkında çok az fikre sahip.

Kapsam sürünmesiyle mücadele ederken hatırlanması gereken birkaç şey var. Birincisi, bir müşteri belirli bir etkileşim üzerinde yapılan işten memnunsa, ek iş talep etmeleri çok yaygındır. Bunu bir iltifat olarak alın ve harcanan ekstra süreyi telafi etmek için ek fon istemekten çekinmeyin. Bir müşteri ekstra iş için ödeme yapmayı reddederse, bu işi yapmak için neredeyse asla kalmaya değmez.

İkinci nokta daha da kritik. Mevcut müşterilerle uğraşırken, fiyatları düşük tutmaya özen gösterin. Fiyat oyma ile iyi bir durumdan yararlanmak, tekrarlanan işleri ortadan kaldırmanın kesin bir yoludur. Firma, müşterinin resmi RFP süreci ve müşterinin kendisi için avlanma gibi müşteriyi edinmenin maliyetlerinden kaçındığı için fiyatların düşürülebileceğini göz önünde bulundurun. Ayrıca, gelecekteki işler için en iyi kaynak mevcut müşteriler aracılığıyladır. Onlara iyi davranın ve geri dönecekler.

Başlangıç ve Bit Tarihlerini Belirtin

Kapsam sürünmesini yenen bir başka önemli bileşen, başlangıç ve bitiş tarihlerini açıkça belirtmektedir. Bu da projenin kesin bir son verilmesini sağlar. Kapsam sürünmesinin gerçekleştiği en yaygın alanlardan biri yeniden test sırasındadır. Yeniden test etmek, bir sözleşmeden sonra giderken her zaman iyi bir fikir gibi gelir. Firmanın şefkatli ve gayretli olduğunu, müşterinin mümkün olduğunca güvenli olmasını sağlamaya çalıştığını gösterir. Sorun, tamamlanana kadar işin ödenmediği unutulması unutulması başladığında başlar. Buna yeniden test de dahil.

Bu riski azaltmak için, sözleşmeye, tüm yeniden testlerin nihai rapor sunumundan sonra belirli bir zaman dilimi içinde yapılması gerektiğinden bahseden basit bir açıklama ekleyin. Daha sonra yeniden test etme çabasına öncülük etmek testçilerin sorumluluğu haline gelir. Müşteri bir uzatma isterse, her zaman ödemenin

belirtilen tarihte yerine getirilmesi koşuluyla buna izin verin. Son olarak ve en önemlisi, kaliteli bir yeniden test yapın. Unutmayın, gelecekteki işler için en iyi kaynak mevcut müşteri tabanınızdır.

IP Menzilleri ve Alan Alanlarını Belirtin

Penetrasyon testine başlamadan önce, tüm hedefler tanımlanmalıdır. Bu hedefler ilk anket aşamasında müşteriden alınmalıdır. Hedefler, müşteri tarafından belirli IP adresleri, ağ aralıkları veya alan adları şeklinde verilebilir. Bazı durumlarda, müşterinin sağladığı tek hedef kuruluşun adıdır ve test edenlerin geri kalanını kendi başlarına tanımlayabilmelerini bekler. Test cihazı ile nihai hedef arasında bulunan güvenlik duvarları ve IDS / IPS veya ağ ekipmanı gibi sistemlerin de kapsamın bir parçası olup olmadığını tanımlamak önemlidir. Yukarı akış sağlayıcıları ve diğer 3. parti sağlayıcıları gibi ek unsurlar tanımlanmalı ve kapsamda olup olmadıkları tanımlanmalı.

Aralıklarını Doğrulayın

Hedeflere saldırmaya başlamadan önce, aslında teste karşı yaptığınız müşteriye ait olduklarını doğrulamanız zorunludur. Bir makineye saldırmaya başlarsanız ve yalnızca makinenin aslında başka bir kuruluşa (hastane veya devlet kurumu gibi) ait olduğunu öğrenmek için başarılı bir şekilde nüfuz ederseniz karşılaşabileceğiniz yasal sonuçları düşünün.

Üçüncü Taraflarla Başa Çıkmak

Bir nişanın bir hizmeti veya üçüncü bir tarafın ev sahipliği yaptığı bir başvuruyu test etmeyi içereceği bir dizi durum vardır. Bu, "bulut" hizmetleri daha popüler hale geldikçe son yıllarda daha yaygın hale geldi. Hatırlanması gereken en önemli şey, müşteri tarafından izin verilmiş olsa da, üçüncü taraf sağlayıcıları için konuşmadıklarıdır. Bu nedenle, barındırılan sistemlerin test edilmesi için onlardan da izin alınmalıdır. Uygun izinleri elde edememek, her zaman olduğu gibi, sonsuz baş ağrılarına neden olabilecek yasayı ihlal etme olasılığını beraberinde getirir.

Bulut Hizmetleri

Bulut servisini test etmedeki en büyük sorun, tek bir fiziksel ortamda depolanan birden fazla farklı kuruluştan gelen veriler olmasıdır. Genellikle bu farklı veri alanları arasındaki güvenlik çok gevşektir. Bulut hizmetleri sağlayıcısının teste uyarılması ve testin gerçekleştiğini kabul etmesi ve test kuruluşuna test izni vermesi gerekiyor. Ayrıca, bulut servis sağlayıcısında, diğer bulut müşterilerini etkileyebilecek bir güvenlik açığının keşfedilmesi durumunda temasa geçilebilecek doğrudan bir güvenlik teması olmalıdır. Bazı bulut sağlayıcıları, penetrasyon test cihazlarının takip etmesi için özel prosedürlere sahiptir ve test başlamadan önce talep formları, planlama veya açık izin gerektirebilir.

ISS'NIN

Müşteri ile ISS hizmet şartlarını doğrulayın. Birçok ticari durumda ISS, test için özel hükümlere sahip olacaktır. Bir saldırı başlatmadan önce bu terimleri dikkatlice gözden geçirin. ISS'lerin kötü niyetli olarak kabul edilen bazı trafiği engelleyip engelleyeceği durumlar vardır. Müşteri bu riski onaylayabilir, ancak başlamadan önce her zaman açıkça iletilmelidir. Web Hosting Diğer tüm üçüncü taraflarda olduğu gibi, testin kapsamının ve zamanlamasının web barındırma sağlayıcısıyla açıkça iletilmesi gerekir. Ayrıca, müşteriyle iletişim kurarken, testin yalnızca web güvenlik açıklarını arayacağını açıkça ifade ettiğinizden emin olun. Test, uygulamanın tehlikeye atılması için hala bir yol sağlayabilecek altta yatan altyapıdaki güvenlik açıklarını ortaya çıkarmayacaktır.

MSP'ler

Yönetilen Güvenlik Hizmeti Sağlayıcılarının da testten haberdar edilmesi gerekebilir. Özellikle, sahip oldukları sistem ve hizmetler test edildiğinde haberdar edilmeleri gerekecektir. Ancak MSP'nin bildirilmeyeceği durumlar vardır. MSP'nin gerçek yanıt süresini belirlemek testin bir parçasıysa, MSSP'nin bildirilmesi için testin bütünlüğünün kesinlikle yararına değildir. Genel bir kural olarak, MSSP'nin açıkça sahip olduğu bir cihaz veya hizmet test edildiğinde, bunların bildirilmesi gerekecektir.

Sunucuların barındırıldığı Ülkeler

Ayrıca, sunucuların barındırıldığı ülkeleri doğrulamak test cihazının yararınadır. Ülkeyi doğruladıktan sonra, teste başlamadan önce belirli ülkenin yasalarını gözden geçirin. Firmanın hukuk ekibinin testçiler için yerel yasaların tam bir özeti sağlayacağı varsayılmamalıdır. Ayrıca, firmanın testçileri tarafından ihlal edilen herhangi bir yasa için yasal sorumluluk alacağı varsayılmamalıdır. Teste başlamadan önce test ettikleri her bölge için yasaları doğrulamak her testçinin sorumluluğundadır, çünkü sonuçta herhangi bir ihlal için cevap vermek zorunda kalacak olan test cihazı olacaktır.

Kabul Edilebilir Sosyal Mühendislik Bahanelerini Tanımlayın

Birçok kuruluş, güvenlik duruşlarının mevcut saldırılarla uyumlu bir şekilde test edilmesini isteyecektir. Sosyal mühendislik ve mızrak kimlik avı saldırıları şu anda birçok saldırgan tarafından yaygın olarak kullanılmaktadır. Başarılı saldırıların çoğu seks, uyuşturucu ve rock and roll (sırasıyla porno, Viagra ve ücretsiz iPod) gibi bahaneler kullanırken, bu bahanelerin bazıları kurumsal bir ortamda kabul edilemez. Teste başlamadan önce test için seçilen herhangi bir bahanenin yazılı olarak onaylandığından emin olun.

DoS Testi

Angajman başlamadan önce stres testi veya Hizmetin Reddi testleri tartışılmalıdır. Testin potansiyel olarak zarar verici doğası nedeniyle birçok kuruluşun rahatsız olduğu bir konu olabilir. Bir kuruluş sadece verilerinin gizliliği veya bütünlüğü konusunda endişeliyse, stres testi gerekli olmayabilir; Bununla birlikte, kuruluş hizmetlerinin mevcudiyetinden de endişe duyuyorsa, stres testi üretim ortamıyla aynı olan üretim dışı bir ortamda yapılmalıdır.

Ödeme Koşulları

Birçok testçinin tamamen unuttuğu bir teste hazırlanmanın bir başka yönü de nasıl ödenmesi gerektiğidir. Sözleşme tarihleri gibi, ödemeler için belirli tarihler ve şartlar olmalıdır. Daha büyük kuruluşların ödemeyi mümkün olduğunca uzun süre geciktirmesi nadir değildir. Aşağıda birkaç yaygın ödeme yöntemi bulunmaktadır. Bunlar sadece örnektir. Her kuruluşun müşterilerinin ve kendilerinin ihtiyaçlarına daha uygun bir şekilde uyacak şekilde kendi fiyatlandırma yapısını oluşturması ve değiştirmesi kesinlikle tavsiye edilir. Önemli olan, test başlamadan önce bir tür yapının yerinde olmasıdır.

Net 30

Nihai raporun tesliminden sonraki 30 gün içinde toplam miktar ödenir. Bu genellikle ödeme yapılmaması

için aylık yüzde bir ceza ile ilişkilidir. Bu, müşterilerinize (yani 45 veya 60) vermek istediğiniz herhangi bir gün olabilir.

Yarı Ön

Test başlamadan önce toplam faturanın yarısının peşin olarak ödenmesi nadir değildir. Bu, daha uzun vadeli angajmanlar için çok yaygındır.

Tekrarlayan

Tekrarlayan bir ödeme programı, uzun vadeli angajmanlar için daha yaygın olarak kullanılır. Örneğin, bazı angajmanlar bir veya iki yıla kadar uzanabilir. Müşterinin yıl boyunca düzenli taksitlerde ödeme yapması hiç de nadir değildir.

Hedefler

Her penetrasyon testi hedef odaklı olmalıdır. Bu, testin amacının, müşterinin iş veya görev hedeflerinin tehlikeye girmesine yol açan belirli güvenlik açıklarını belirlemek olduğunu söylemektir. Bu, yamalanmamış sistemler bulmakla ilgili değildir. Bu, organizasyonu olumsuz yönde etkileyecek olan riski belirlemekle ilgilidir.

Birincil

Bir testin birincil hedefi uyum tarafından yönlendirilmemelidir. Bu akıl yürütmenin bir dizi farklı gerekçesi var. İlk olarak, uyum eşit güvenlik değildir. Birçok kuruluşun uyum nedeniyle testten geçtiği anlaşılsa da, testin ana hedefi olmamalıdır. Örneğin, PCI-DSS gereksinimlerinin bir parçası olarak bir penetrasyon testini tamamlamak için bir firma işe alınabilir.

Kredi kartı bilgilerini işleyen şirket sıkıntısı yoktur. Bununla birlikte, hedef organizasyonu rekabetçi bir pazarda benzersiz ve uygulanabilir kılan özellikler, tehlikeye girerse en büyük etkiye sahip olacaktır. Kredi kartı sistemlerinin tehlikeye girmesi kesinlikle ciddi bir sorun olacaktır, ancak kredi kartları numaraları, ilgili tüm müşteri verilerinin sızdırılmasıyla birlikte felaket olacaktır.

İkincil

İkincil hedefler doğrudan uyum ile ilgilidir. Birincil ve ikincil hedeflerin çok yakından ilişkili olması nadir değildir. Örneğin, PCI-DSS güdümlü test örneğinde, kredi kartlarını almak ikincil hedeftir. Bu veri ihlalini organizasyonun işletmesine veya misyon sürücülerine bağlamak birincil hedeftir. İkincil hedefler uyum ve / veya BT için bir şey ifade eder. Birincil hedefler üst yönetimin dikkatini çeker.

İş Analizi

Bir penetrasyon testi yapmadan önce, müşterinin güvenlik duruşunun olgunluk seviyesini belirlemek faydalıdır. İlk önce bu olgunluk seviyesini değerlendiren bir penetrasyon testine atlamayı seçen bir dizi kuruluş vardır. Çok olgunlaşmamış bir güvenlik programı olan müşteriler için, önce bir güvenlik açığı analizi yapmak genellikle iyi bir fikirdir.

Bazı testçiler, Güvenlik Açabilirlik Analizi (VA) çalışmalarını çevreleyen bir damgalama olduğuna inanıyor. Bu testçiler, amacın hedef organizasyondaki riskleri belirlemek olduğunu unuttular, sözde “rockstar” yaşam

tarzını sürdürmekle ilgili değil. Bir şirket tam bir penetrasyon testi için hazır değilse, iyi bir VA'dan bir penetrasyon testinden çok daha fazla değer elde edeceklerdir.

Müşteri ile önceden sağlayacakları sistemler hakkında hangi bilgileri sağlayın. Ayrıca, zaten belgelenmiş olan güvenlik açıkları hakkında bilgi istemek de yararlı olabilir. Bu, testçilerin zamanını kazandıracak ve bilinen sorunlarla test keşiflerini üst üste çıkarmayarak müşteri parasını kurtaracaktır. Aynı şekilde, tam veya kısmi bir beyaz kutu testi, uygunluk tarafından kesinlikle gerekli değilse, müşteriye bir kara kutu testinden daha fazla değer getirebilir.

İletişim Hatları Oluşturun

Herhangi bir penetrasyon testinin en önemli yönlerinden biri müşteri ile iletişimdir. Müşteri ile ne sıklıkta etkileşime girdiğiniz ve onlara nasıl yaklaşma şekliniz, memnuniyet duygularında büyük bir fark yaratabilir. Aşağıda, müşterinin test faaliyetleri konusunda rahat hissetmesine yardımcı olacak bir iletişim çerçevesi bulunmaktadır.

Acil Durum İletişim Bilgileri

Açıkçası, acil bir durumda müşteri veya hedef kuruluşla temasa geçebilmek hayati önem taşır. Acil durumlar ortaya çıkabilir ve bunları ele almak için bir temas noktası oluşturulmuş olmalıdır. Acil durum irtibat listesi oluşturun. Bu liste, test kapsamında tüm taraflar için iletişim bilgilerini içermelidir. Oluşturulduktan sonra, acil durum kişi listesindeki tüm kişilerle paylaşılmalıdır. Unutmayın, hedef organizasyon müşteri olmayabilir.

Her acil durum irtibatı hakkında aşağıdaki bilgileri toplayın:

1. Tam adı
2. Başlık ve operasyonel sorumluluk
3. Test faaliyetlerinin ayrıntılarını tartışmak için yetkilendirme, daha önce belirtilmemişse
4. Mümkünse cep telefonu, çağrı cihazı veya ev telefonu gibi iki 7/24 anında iletişim şekli
5. SFTP veya şifreli e-posta gibi güvenli toplu veri aktarımının bir şekli

Not: Yardım masası veya operasyon merkezi gibi bir grubun sayısı bir acil durum temasının yerini alabilir, ancak yalnızca 7/24 personele sahipse. Her penetrasyon testinin doğası, acil durum iletişim listesinde kimin olması gerektiğini etkiler. Müşteri için iletişim bilgileri ve hedeflerin yalnızca kullanılabilir hale getirilmesi gerekmez, aynı zamanda acil bir durumda test cihazlarıyla da iletişime geçmeleri gerekebilir. Liste tercihen aşağıdaki kişileri içermelidir:

1. Nişan için test grubundaki tüm penetrasyon test cihazları
2. Test grubunun yöneticisi
3. Her hedef organizasyonda iki teknik temas
4. Müşteriye iki teknik bağlantı
5. Müşteriye bir üst yönetim veya iş bağlantısı

Yukarıdaki listede bir miktar örtüşme olması mümkündür. Örneğin, hedef kuruluş müşteri olabilir, test grubunun yöneticisi de penetrasyon testini yapıyor olabilir veya bir müşterinin teknik teması üst yönetimde olabilir. Ayrıca, ilgili taraf başına, onu yöneten ve onun adına sorumluluk alan tek bir irtibat kişisini tanımlaması önerilir.

Olay Raporlama Süreci

Örgütün mevcut olay müdahale yeteneklerini tartışmak, çeşitli nedenlerden dolayı bir angajmandan önce yapılması önemlidir. Bir penetrasyon testinin bir kısmı sadece bir kuruluşun bulunduğu güvenliği değil, aynı zamanda olay müdahale yeteneklerini de test etmektir.

Hedefin iç güvenlik ekiplerinin fark etmesi olmadan tüm bir angajman tamamlanabilirse, güvenlik duruşunda büyük bir boşluk tespit edilmiştir. Test başlamadan önce, hedef kuruluştaki birinin testlerin ne zaman yapıldığının farkında olmasını sağlamak da önemlidir, böylece olay müdahale ekibi gece yarısı üst yönetimin her üyesini aramaya başlamaz, çünkü saldırı altında olduklarını veya tehlikeye atıldıklarını düşünürler.

Olay tanımı

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), bir olayı şöyle tanımlıyor: "Bilgisayar güvenlik politikalarının ihlal edilmesi veya yakın bir ihlali, kabul edilebilir kullanım politikaları veya standart güvenlik uygulamalarının ihlali tehdidi." (Bilgisayar Güvenliği Olayı Ele Alma Kılavuzu - Özel Yayın 800-61 Rev 1). Bir olay fiziksel düzeyde de ortaya çıkabilir, burada bir kişi herhangi bir yolla bir alana izinsiz fiziksel erişim kazanır. Hedef teşkilat, farklı olaylar türleri için farklı kategorilere ve seviyelere sahip olmalıdır.

Durum Raporu Frekansı

Durum raporlama sıklığı çok çeşitli olabilir. Raporlama programını etkileyen bazı faktörler, testin genel uzunluğunu, test kapsamını ve hedefin güvenlik olgunluğunu içerir. Etkili bir program, müşterinin meşgul hissetmesini sağlar. Göz ardı edilen bir müşteri eski bir müşteridir.

Durum raporlarının sıklığı ve programı belirlendikten sonra, yerine getirilmelidir. Bir durum raporunu ertelemek veya geciktirmek gerekli olabilir, ancak kronik hale gelmemelidir. Müşteriden gerekirse yeni bir programı kabul etmesi istenebilir. Bir durum raporunu tamamen atlamak profesyonel değildir ve mümkünse kaçınılmalıdır.

PGP ve Diğer Alternatifler

Şifreleme isteğe bağlı değildir. Müşteri ile iletişim, herhangi bir penetrasyon testi katılımının kesinlikle gerekli bir parçasıdır ve katılımın hassas doğası nedeniyle, hassas bilgilerin iletişimi, özellikle nihai raporda şifrelenmelidir. Test başlamadan önce, müşteri ile güvenli iletişim aracı kurulmalıdır. Birkaç yaygın şifreleme yolu aşağıdaki gibidir:

1. PGP / GPG hem e-posta üzerinden iletişim kurmak hem de nihai raporu şifrelemek için kullanılabilir (konundan satır satırların düz metinden geçirildiğini unutmayın)
2. Müşterinin ağında barındırılan güvenli bir posta kutusu
3. Telefon
4. Yüz yüze toplantılar
5. Nihai raporu sunmak için, raporu bir AES şifreli arşiv dosyasında da saklayabilirsiniz, ancak arşiv yardımcı programınızın CBC kullanarak AES şifrelemesini desteklediğinden emin olun.

Ayrıca ne tür bilgilerin yazılı olarak alınabileceğini ve hangilerinin sadece sözlü olarak iletilmesi gerektiğini sorun. Bazı kuruluşların, hangi güvenlik bilgilerinin kendilerine iletildiğini yazılı olarak sınırlamak için çok iyi nedenleri vardır.

Katılım Kuralları

Kapsam ne test edileceğini tanımlarken, katılım kuralları bu testin nasıl gerçekleşeceğini tanımlar. Bunlar birbirinden bağımsız olarak ele alınması gereken iki farklı yöndür.

Zaman Çizelgesi

Nişan için net bir zaman çizelgesi oluşturulmalıdır. Kapsam, bir angajmanın başlangıcını ve sonunu tanımlarken, angajman kuralları aradaki her şeyi tanımlar. Test ilerledikçe zaman çizelgesinin değişeceği anlaşılmalıdır. Bununla birlikte, katı bir zaman çizelgesine sahip olmak, bir tane yaratma hedefi değildir. Aksine, bir testin başında bir zaman çizelgesine sahip olmak, ilgili herkesin yapılacak işi ve söz konusu işten sorumlu olacak kişileri daha net bir şekilde tanımlamasına izin verecektir. GANTT Grafikleri ve İş Dökümü Yapıları genellikle işi ve çalışmanın her bir parçasının alacağı süreyi tanımlamak için kullanılır. Programın bu şekilde parçalandığını görmek, kaynakların nereye uygulanması gerektiğini belirlemede yer alanların yardımcı olur ve müşterinin test sırasında karşılaştığı olası engelleri belirlemesine yardımcı olur.

İnternette bir dizi ücretsiz GANTT Grats aracı mevcuttur. Birçok yemlik bu araçlarla yakından özdeşleşir. Bu nedenle, bir hedef organizasyonun üst yönetimi ile iletişim kurmak için mükemmel bir ortamdır.

Konumlar

Müşteri ile önceden kurulması gereken herhangi bir etkileşimin bir başka parametresi, testçilerin test sırasında seyahat etmesi gereken herhangi bir destinasyondur. Bu, yerel otelleri tanımlamak kadar basit olabilir veya belirli bir hedef ülkenin geçerli yasalarını tanımlamak kadar karmaşık olabilir.

Bir kuruluşun birden fazla yerde ve bölgede faaliyet göstermesi nadir değildir ve test için birkaç seçkin sitenin seçilmesi gerekecektir. Bu durumlarda, her müşteri konumuna seyahatten kaçınılmalıdır, bunun yerine, sitelere VPN bağlantılarının uzaktan test için mevcut olup olmadığı belirlenmelidir. Hassas Bilgilerin Açıklanması

Belirli bir katılımın hedeflerinden biri hassas bilgilere erişmek olsa da, bazı bilgiler aslında görüntülenmemeli veya indirilmemelidir. Bu, yeni testçilere garip geliyor, ancak test edenlerin hedef verilere sahip olmamaları gereken bir dizi durum var. Örneğin, Sağlık Sigortası Taşınabilirlik ve Hesap Verebilirlik Yasası (HIPAA) kapsamında Kişisel Sağlık Bilgileri (PHI), bu verilerin korunması gerekir. Bazı durumlarda hedef sistemin onu koruyan bir güvenlik duvarı veya anti-virüs (AV)ı olmayabilir. Bu tür bir durumda, test edenlerin herhangi bir kişisel olarak Tanımlanabilir Bilgiye (PII) kesinlikle önlenmesi gerekir.

Ancak, veriler fiziksel veya sanal olarak elde edilemezse, testçilerin gerçekten bilgiye eriştiği nasıl kanıtlanabilir? Bu sorun çeşitli şekillerde çözülmüştür. Tonoz kapısının paranın hiçbirini almadan açıldığını kanıtlamanın yolları vardır. Örneğin, veritabanı şeması ve dosya izinlerinin bir ekran görüntüsü alınabilir veya dosyaların kendileri, dosyaların kendi dosyalarında görünmediği sürece içeriği görüntülemek için açmadan görüntülenebilir.

Testlerin belirli bir katılımda ne kadar temkinli olması gerektiği, müşteriyle tartışılması gereken bir parametredir, ancak test yapan firma, müşteri görüşüne bakılmaksızın kendilerini yasal anlamda koruyacaklarından her zaman emin olmalıdır. Hassas verilere maruz kalmanın gerekli olduğu bir öneme bakılmaksızın, tüm rapor şablonları ve test cihazı makineleri her bir etkileşimden sonra yeterince temizlenmelidir. Özel bir yan not olarak, testçiler tarafından yasadışı veriler (yani çocuk pornografisi) keşfedilirse, uygun kolluk kuvvetlerine derhal bildirilmeli, ardından müşteri tarafından bilgilendirilmelidir. Müşteriden yön almayın.

Kanıtlar Ele Alınması

Bir testin kanıtlarını ve raporun farklı aşamalarını ele alırken, verilere aşırı özen göstermek inanılmaz derecede önemlidir. Her zaman şifreleme kullanın ve test makinenizi testler arasında sterilize edin. Güvenlik konferanslarında test raporlarıyla USB bellekleri asla dağıtmayın. Ve ne yaparsanız yapın, başka bir müşteri katılımından bir raporu şablon olarak yeniden kullanmayın! Belgenizdeki başka bir kuruluşa referans bırakmak çok profesyonel değil.

Düzenli Durum Toplantıları

Test süreci boyunca, müşterinin testin genel ilerlemesini bildiren düzenli toplantılar yapmak kritik öneme sahiptir. Bu toplantılar günlük olarak yapılmalı ve mümkün olduğunca kısa olmalıdır. Toplantılar üç konsepte tutulmalıdır: planlar, ilerleme ve problemler.

Planlar genellikle tartışılır, böylece testler planlanmamış büyük bir değişiklik veya kesinti sırasında yapılmaz. İlerleme, müşteriye şimdiye kadar neler yapıldığına dair bir güncellemedir. Sorunlar bu toplantıda da tartışılmalıdır, ancak kısalık yararına, çözümlerle ilgili konuşmalar neredeyse her zaman çevrimdışı hale getirilmelidir.

Test için günün zamanı

Bazı müşteriler tüm testlerin iş saatleri dışında yapılmasını gerektirir. Bu, çoğu testçi için geç geceler anlamına gelebilir. Test başlamadan önce müşterinin günlük gereksinimlerin iyi bir şekilde belirlenmesi gerekir.

Shunning ile anlaşmak

Sfonun mükemmel bir şekilde kabul edilebilir olduğu zamanlar vardır ve testin ruhuna uymayabileceği zamanlar vardır. Örneğin, testiniz sadece teknolojiyi değil, hedef kuruluşun güvenlik ekibinin yeteneklerini test ettiğiniz tam bir kara kutu testi olacaksa, kaçınılması tamamen iyi olacaktır. Bununla birlikte, hedef kuruluşun güvenlik ekibiyle koordineli olarak çok sayıda sistemi test ederken, saldırılarınızı engellemek için testin yararına olmayabilir.

Test için izin

Penetrasyon testi için elde edilmesi gereken en önemli belgelerden biri, Teste İzin belgesidir. Bu belge kapsamı belirtir ve testçilerin faaliyetleri hakkında farkındalık tanıyan bir imza içerir. Ayrıca, testin sistem istikrarsızlığına yol açabileceğini ve testçi tarafından bu süreçte sistemleri çökertmemek için tüm bakım verildiğini açıkça belirtmelidir. Bununla birlikte, test istikrarsızlığa yol açabilir, çünkü müşteri test cihazını herhangi bir sistem istikrarsızlığı veya çöküşten sorumlu tutmaz. Bu belge müşteri tarafından imzalanana kadar testlerin başlamaması kritik öneme sahiptir.

Buna ek olarak, bazı servis sağlayıcıları sistemlerini test etmeden önce önceden bildirim ve / veya ayrı izin gerektirir. Örneğin, Amazon'un tamamlanması gereken bir çevrimiçi istek formu vardır ve talebin bulutlarındaki herhangi bir ana bilgisayarı taramadan önce onaylanması gerekir. Bu gerekliyse, belgenin bir parçası olmalıdır.

Yasal Değerlendirmeler

Penetrasyon testlerinde yaygın olan bazı faaliyetler yerel yasaları ihlal edebilir. Bu nedenle işin yapılacağı yerdeki ortak çatı katılık görevlerin yasallığını kontrol etmesi tavsiye edilir. Örneğin, penetrasyon testi sırasında yakalanan herhangi bir VOIP çağrısı bazı alanlarda dinleme olarak kabul edilebilir.

Yetenekler ve Teknoloji Yerinde

İyi penetrasyon testleri sadece yamalanmamış sistemleri kontrol etmez. Hedef organizasyonun yeteneklerini de test ediyorlar. Bu amaçla, aşağıda test yaparken kıyaslayabileceğiniz şeylerin bir listesi bulunmaktadır.

1. Bilgi toplamayı tespit etme ve bunlara yanıt verme becerisi
2. Ayak baskısını tespit etme ve yanıt verme yeteneği
3. Tarama ve vulan analizi tespit etme ve bunlara yanıt verme becerisi
4. Sızdırmazlığı tespit etme ve bunlara yanıt verme becerisi (saldırılar)
5. Veri toplamayı tespit etme ve bunlara yanıt verme yeteneği
6. Verileri tespit etme ve bunlara yanıt verme yeteneği

Bu bilgileri takip ederken zaman bilgisi topladığınızdan emin olun. Örneğin, bir tarama tespit edilirse size bildirilmeli ve o sırada hangi tarama seviyesini tahmin ettiğinizi belirtmelidir.

" http://www.pentest-standard.org/index.php'den alındınız mı? başlık = Önceden katılım&oldid=940 "
