15

Penetrasyon testi

D. Fried CISSP

penetrasyon testi konusuna genel bir giriş yapan ve güvenlik analizi bu özel bölgeyi anlamak için gerekli arka plan ile uzmanına sağlar. Penetrasyon testleri anlayış ve bir bilgisayarın veya ağın güvenliğini artırmak için değerli bir araç aynı zamanda sistem zayıflıklarını ve saldırı sistemleri yararlanmak ve değerli bilgileri çalmak için kullanılabilir.

testleri için gereğini ve bunun kullanımını çevreleyen sorunları ve süreçleri anlayarak, bir güvenlik profesyonel setinin standart bir parçası olarak penetrasyon testi kullanmak daha iyi olacaktır.

kullanımı, uygulama ve süreç açısından penetrasyon testi sunar. Bu penetrasyon özgül sistemleri test etmek özgül tekniklerine derinlemesine bir kılavuz olarak uygun değildir. Penetrasyon testleri beceri büyük bir alan pratik bir sanattır. Doğru ve dikkatli yapılmamışsa, penetrasyon testi (en iyi) geçersiz sayılır edilebilir ve, en aslında hedef sistemlerine zarar. Güvenlik profesyonel penetrasyon test araçları ve teknikleri aşina ise, işe ya kuruluşun güvenlik personeli eğitmek için bu alanda tecrübe büyük bir ile birisiyle anlaşma en iyisidir.

**Penetrasyon Testi Nedir?**

testleri böyle bir saldırıya o sistemin veya kuruluşun direncini test etmek amacıyla bir sistem veya kuruluşun güvenlik atlamasına tasarlanmış prosedürler resmi bir set olarak tanımlandığını olduğunu. Penetrasyon testleri bir sistemin zayıflıklarını ortaya çıkarmak ve sistem potansiyel saldırgan tarafından tehlikeye girebilir yollarını belirlemek için yapılır.

testleri bir test bir hedefe karşı “saldırılar” bir dizi oluşur, genel olarak, farklı biçimlerde (daha sonra ele alınacaktır olan)saldırıya tepki başarı veya saldırıların başarısızlığı ve nasıl testin sonucunu belirleyecektir.

testinin genel amacı düşmanca bir saldırgan tarafından saldırıya dayanacak şekilde deneğin yeteneğini belirlemektir. Bunun gerçek hayatta saldırganın kullanabilir teknikler kullanılarak yapılacaktır. Bu simüle saldırı stratejisi keşfetmek ve gerçek bir keşfeder önce güvenlik zayıf noktaları azaltmak için konuyu verir.

testi var sebebi kuruluşların güvenlik önlemlerinin etkinliğini belirlemek için ihtiyaç vardır. onlar testleri istemek güvenlik bazı de eksiklik olması (ya da keşfetmek istiyorum) olabileceğine inanıyorsanız belirtir. test kendisi güvenlik sorunlarını ortaya çıkarmak olabilir ancak bununla birlikte, test keşfetmek ve test başarılı izin süresi geçerse kaynaklandığı nedeni açıklamak için gayret gösterir. Basitçe tester hassas bilgiler içeren bir binadan başardı belirten oluşturulmasına yeterli değildir. tester atlamalı nöbetçi bekçi veya değerli veya hassas bilgileri onları sağlayacak bekçi personel eğitimi eksikliğinden yetersiz ilgi nedeniyle olduğunu açıklamalıdır.

penetrasyon testi için üç temel gereksinimleri vardır. İlk olarak, test ve belirlenen bir hedefi olmalı ve bu amaç açıkça hedefe c daha spesifik fi o kadar kolay testin başarılı veya başarısız tanımak olacaktır. “İnternetten XYZ girmeye ve araştırma departmanı fi le sunucusuna erişmek.” Gibi kesinlikle ulaşılabilir ise, “XYZ şirket ağı girmeye” olarak kesin değildir Her test tek bir hedefi olmalıdır. tester bir iş güvenliğinden çeşitli yönlerini test etmek CRC Press LLC tarafından

gerçekleşmesini çok olduğu bir sınırlı süre olmalıdır. En penetrasyon testinde metodoloji gerçek dünyada saldırıların türlerini taklit etmektir. Bir saldırganın bir site sızmaya çalıştığı zaman ve enerji bir sonlu miktarda varsaymak mantıklıdır. O zaman bir gün ötesinde bir yıl veya arasında değişebilir; O zaman ulaştıktan sonra saldırganın vazgeçeceğim. Buna ek olarak, korunmakta olan bilgiler “ömür boyu” bir Batılı olarak yararlı olabilir

testi kabul ve bu gerçeği kabul etmelidir. Böylece, test için hedef ifadenin parçası hedeflenen sistemin türü, düzeyde ve bilginin ömrü dayalı makul sayılır bir zaman sınırı içermelidir.

test testin konusu olan örgütün yönetim onayı olmalıdır. Sadece kurumun yönetim ağ ve bilgi sistemleri faaliyetine izin yetkisine sahip gibi bu son derece önemlidir.

testleri ile ilişkili çeşitli terimler vardır. Bu terimler penetrasyon test ve bir penetrasyon testinde yer alan kişileri ve tanımlamak için bu bölümde boyunca kullanılır.

penetrasyon testi gerçekleştiren kişi veya gruptur. test amacı planlamak ve penetrasyon testi yürütmek ve sonuçlarını analiz etmektir. Birçok durumda, test testin konusu olan şirket ya da kuruluşun bir üyesi olacaktır.

bunu kendisini yapmak personele veya uzmanlığa sahip değilse penetrasyon testi yapmak için dışarıdan bir fi

Bir test cihazının gerçek hayattan versiyonudur. tester onun güvenliğini artırmak için bir firma ile çalıştığı yer Ancak, saldırgan kaynakları çalmak için bir şirkete karşı çalışır.

Belirli bir hedefin güvenlik kontrollerini aşmak amacıyla test tarafından gerçekleştirilen faaliyetlerin dizisidir.

usul, veya elektronik oluşabilmektedir.

penetrasyon testi olan kimi üzerine kuruluştur. konu bütün bir şirket olabilir veya bu şirket içinde daha küçük olabilir.

penetrasyon testinin herhangi bir zamanda belirli bir saldırıya maruz sistem veya kuruluştur. Hedef ya da test ediliyor veya olmayabilir. Her iki durumda da, hedef bu girişe karşı kendini korumak için dış dünyaya sunan savunmaların penetrasyon testi test etmek üzere tasarlanmıştır, bu savunmalar olduğunu. Tam penetrasyon testi genellikle bir dizi yönelik saldırıların bir dizi oluşur.

penetrasyon testinde yer alan bir kuruluşun liderlik tanımlamak için kullanılan bir terimdir. test edilen şirketin yönetimi dahil herhangi test çaba, katılan yönetimin çeşitli düzeylerde, hem de bir bütün olarak şirketin üst penetrasyon testi çaba dahil yönetiminin özgül seviyelerinin test kapsamı üzerinde doğrudan etkiye sahip durumda, ancak, test adına çalıştığını varsayılır (ve sponsor) şirket içinde yönetim en az bir seviye.

**penetrasyon testi (** ya da daha basitçe, **Ölçek )** hedef bir simüle saldırı gerçek performansıdır.

sistemleri veya operasyonları üzerinde gerçekleştirilen bir penetrasyon testi isteyecektir çeşitli nedenleri vardır. Fi örgütü yerine koyduğu güvenlik kontrollerinin etkinliğini belirlemektir. Bu kontroller örgütün bilgisayarlar, ağ sistemleri etkileyen, doğada teknik olabilir. Bir şirket kontrol etmek yerinde ve sabit bilgilerinde sahiptir süreç ve ilişkin, doğada operasyonel olabilir. Son olarak, doğada fiziksel olabilir. tester bir site veya şirket yerinde vardır etkinliğini belirlemek için çalışıyor olabilir. Her durumda, test hedefi mevcut kontrolleri çevrelerindeki almaya tarafından fi cient Suf olup olmadığını belirlemek için olacaktır.

bir organizasyon belli bir tehdide sahip açığını belirlemek için çalışıyor olabilir. Her sistem, işlem veya

savunmasız hissediyor hangi tehditlerin belirli bir grubu vardır. İdeal olarak, organizasyon bu tehditlere maruz için adımlar atmış olacağız. test rolü bu karşı önlemlerin etkinliğini belirlemek için ve iyileştirme veya alanlar belirlemek olacak

CRC Press LLC tarafından penetrasyon testi bazen pazarda bir şirketin konumunu güçlendirmek için kullanılabilir. saygın şirket ve deneğin çevre

dayanmış olduğunu belirten tarafından yürütülen bir test, müstakbel müşterilere öznenin ortamı güvenli görünüm vermek için kullanılabilir. o boyutu bile ılımlı ise bir penetrasyon testi deneğin ortamının tüm olası incelemek çünkü kelime “görünüş” Burada önemli. Buna ek olarak, bir işletmenin güvenlik durumu sürekli olarak değişiyor eski, kon fi yapılanışını değişikliği değiştirir ve iş ihtiyaçları geliştikçe. “Çevre” tester inceler müşteri bir birinden çok farklı olabilir. Bir penetrasyon testi amaçları pazarlama için belirli bir çevrenin güvenliği kanıtı kullanılırsa, testi onun sistemleri veya operasyonlarda bulunabilecek güvenlik tehdidine şirketin üst yönetimini uyarmak için kullanılabilir. güvenlik zayıflıkları olduğunu genel bilgi, ya da belirli tehditler ve güvenlik açıklarının özgül bilgi teknik personel arasında mevcut olsa da, bu mesajı hep yönetime iletilen olarak, yönetim tam olarak anlamak veya güvenlik sorunun büyüklüğünü takdir olmayabilir. sistematik yönetimi habersiz olduğu açıklarını ortaya penetrasyon testi var. güvenlik sorunlarının somut delillerin sunulması, bu sorunların şirkete neden olabilir hasar analizi ile birlikte yönetime olabilir ve bilgi güvenliği konularında daha fazla dikkat içine teşvik. Bu uyandırma görüşmesinin bir yan etkisi yönetimi tehdit ve şirket savunmasız

doğasını anlar kez, o tarafından ortaya çıkarılan sadece güvenlik sorunları çözmek için para ve kaynak tüketmek daha istekli olabilir olabilir Test tarafından ek ilgiye ihtiyaç yardımcı güvenlik alanları. Bunlar yan konular genel güvenlik bilinci programı veya güvenlik teknolojisi için ek fon

şirketin güvenlik orta veya ciddi sorunlar ortaya çıkarır bir penetrasyon testi zamanı etkili haklı çıkarmak için kullanılabilir ve etkili güvenlik önlemleri uygulamak için gerekli gider. şirket tarafından ek ilgiye ihtiyaç testi ile ortaya çıkarılan güvenlik sorunları değil, aynı zamanda yardımcı

sadece ele para ve kaynak tüketmek daha istekli olabilir. Bunlar yan konular genel güvenlik bilinci programı veya güvenlik teknolojisi için ek fon şirketin güvenlik orta veya ciddi sorunlar ortaya çıkarır bir penetrasyon testi zamanı etkili haklı çıkarmak için kullanılabilir ve etkili güvenlik önlemleri uygulamak için gerekli gider. şirket tarafından ek ilgiye ihtiyaç testi ile ortaya çıkarılan güvenlik sorunları değil, aynı zamanda yardımcı sadece ele para ve kaynak tüketmek daha istekli olabilir. Bunlar yan konular genel güvenlik bilinci programı veya güvenlik teknolojisi için ek fon şirketin güvenlik orta veya ciddi sorunlar ortaya çıkarır bir penetrasyon testi zamanı etkili haklı çıkarmak için kullanılabilir ve etkili güvenlik önlemleri uygulamak için gerekli gider.

**Penetrasyon Test Türleri**

testinin tipik görüntü şirketin içine almak için havalandırma şaftı üzerinden günlerce bir şirketin ağı saldıran veya odada oturan yüksek teknoloji bilgisayar uzmanlarından oluşan bir ekibin olduğunu “gizli odaya.” iken bu may farklı (ve çok nonglamorous) çeşitli şekillerde çalışır gerçekte filmlerde kullanılacak bir çekici görüntü, ol.

konunun fiziksel altyapısını içerir. Çoğu zaman, bir şirketin en savunmasız kısımları kendi bilgi ağı ya da bulunan erişim kontrollerinin teknolojisinde bulunmaz. Güvenlik problemleri konu fiziksel güvenliğini

şeklinde bulunabilir. penetrasyon tester bu fiziksel zayıflıkları yararlanmaya çalışacak. Örneğin, bina yeterli sağlar? Bina güvenlik görevlisi var mıdır ve bunlar girebilir veya bir binayı terk olarak gardiyanlar insanları edebilirim? davetsiz misafir bir şirketin binaya kontrolsüz yürümek mümkün değilse, bunlar aradıkları bilgilere fiziksel mümkün olacak. İyi bir test herkesin çalışmak ulaşıyor sabah sırasında binaya yürümek denemektir.

hassas alanlar kilitli ya da başka fiziksel bariyerler tarafından korunmaktadır halinde kez içinde kontrol edin.

zaman fi le dolapları kilitli mi? o telefon ve ağ iletişim bağlantıları sonlandırmak tüm iletişim dolaba girmek nedir? Bir kişinin refakatsiz ve sorgusuz fi ce alanlarının çalışanı içine yürüyebilir mi? Bir binanın tüm güvenli alanları yetkisiz girişlere karşı korunmalıdır. Eğer böyle değilse, test, hassas şirket bilgilerine sınırsız erişim mümkün olacak.

yetkisiz girişlere karşı korumaları inceleyerek içermekle birlikte, penetrasyon testi de yetkisiz çıkış yasaklayan etkinliğini incelemek olabilir. Çalışanlar tesis çıktığınızda şirket duyarlı malzemelerin hırsızlık için kontrol ediyor mu?

bilgisayarlar ya da diğer taşınabilir cihazlar kayıtlı ve girme ve bina çıkarken kontrol ediliyor mu? güvenlik görevlileri türlerini aramak için değil, aynı zamanda bu prosedür önemlidir nasıl ekipman gizli veya maskelenmiş edilebilir üzerinde sadece eğitimli mi?

CRC Press LLC tarafından yardım masası her kullanıcıya gerektiriyorsa yardım kılınabilir önce Örneğin, kişisel veya gizli bilgi vermek baypas çağrıyı cevaplama teknisyen için özellikle inandırıcı “Acıklı bir hikaye” anlatarak bu kontroller? Şirketin karıştırmak” veya elden önce diskleri mıknatısını ise, bu işlemler takip edilir? Değilse Hassas hangi bilgilerin tester

diskler ve bilgisayarlarda nd olacak? Bir şirket birisi basitçe (yani her türlü otorite fiili kanıt olmadan) doğru olduğunu iddia eden olabilir, bir sisteme kimlik veya şifre değişiklikleri başlatmak için gerekli yetkiye ve sıkı politikalara varsa kaldırılır, oluşturulacak bir kimlik neden olabilir veya değişti? Bütün bunlar bir şirket operasyonel süreçlerin karşı saldırılar vardır ve bu tekniklerin tüm bilgisayarlarda giriş kazanır veya hassas bilgilere geçmişte başarıyla kullanılmıştır.

testi fi nal tipi elektronik testtir. Elektronik test bir organizasyonun bilgisayar sistemleri, ağlar, veya iletişim saldırılar oluşmaktadır. Bu elle veya otomatik araçlar kullanmak suretiyle gerçekleştirilebilir. elektronik testinin sistemler konuya tarafından kullanılan veri ağı veya iletişim imkanları sayesinde bir saldırıya karşı olmadığını belirlemektir.

belirli test parametrelerinin bağlı olarak, bir test bir, iki ya da testlerin her üç tip kullanabilir. Testin amacı, belirli birsistemine erişmek ise, test bilgisayarın konsoluna erişmek veya ağ üzerinden makineyi saldırmak için bir elektronik testi fiziksel bir penetrasyon çalışabilir. Yetkisiz personelin değerli bir araştırma verileri elde eğer testin amacı görmeyi ise,

kopyalanan ve bu erişim günlükleri gözden kim olduğunu belirlemek verilen bilgiler izlenir veya günlüğe olup görmek için operasyonel test kullanabilir. Daha sonra test kiti bilgilerinin depolandığı bilgisayarlara erişmek için elektronik

geçiş yapabilir.

**Testleri Ne İşe verir?**

testleri başarılı olmasının birkaç genel nedeni vardır. Birçoğu operasyonel bölgede bulunan; Ancak güvenlik sorunları çıkabilir de fi CIENCIES üç test alanlardan herhangi birinde.

sorunları çok sayıda bilgi güvenliği ve korunması ile ilgili şirket politikaları ve prosedürleri bir şirketin çalışanlarının olmamasından dolayı ortaya çıkmaktadır. Bir şirketin çalışanları ve yüklenicileri özel veya hassas bilgileri uygun prosedürler bilmiyorsanız, onlar çok daha büyük olasılıkla bu bilgilerin korumasız bırakılması için izin hassas şirket bilgileri tartışırken üzerinde şirket politikalarının farkında değilseniz, genellikle basitçe kümesi isteniyor ederek şirketin gelecekteki satış, pazarlama veya araştırma planları hakkında (bazen gönüllü olur. tester farkındalık eksikliğini istismar ve politikaları tanınmış olmadığı gerçeği hesaba test

değiştirir.

durumda, testin denekler şirketin politikaları ve bilgi işleme prosedürleri ile çok tanıdık gelecektir. genellikle insanlar şirketin tarafından tanımlanır standartlaştırılmış prosedürler de fi uymayan çünkü Ancak buna rağmen, penetrasyon testleri çalışır. günlükleri günlük gözden geçirilmesi gerektiğini söylemek de, çoğu yöneticileri rahatsız etmek çok meşgul. İyi idari ve

uygulamaları sistem kon fi yapılanışını kurcalamayı tespit etmek için periyodik olarak kontrol edilmelidir, ancak nadiren de güvenlik politikaları asgari karmaşıklığını ve şifreler için maksimum süre sınırlarını gösterir, ancak birçok site bu uygulamak gerekmez. tester bu güvenlik prosedürel süresi geçerse bilir sonra, açığa çıkarmak kolaydır hale gelir.

operasyonel prosedürleri birbirinden kopuk olması. Bir şirket içinde tek bir kuruluş tarafından kullanılıyor

genellikle con fl başka bir kuruluş tarafından kullanılan süreçlerle ict olabilir. kullanıcıların diğer uygulamalar kullanılan prosedürleri tamamlamak kimliğini doğrulamak için bir uygulama tarafından kullanılan prosedürleri mı, uygulamalar tarafından kullanılıyor farklı standartlar nelerdir? ağda başka bir yerinde daha düşük bir şirketin erişim güvenliği var mı? tüm sistem ve hizmetler için eşit gözden fi les ve denetim kayıtlarını açın veya daha yakından takip bazı sistemler kesildin? Tüm bu kurum ve süreçler arasındaki koordinasyon eksikliği örnekler test cihazı tarafından sömürülen ve test hedefine yaklaşmak için kullanılabilir.

genellikle onlar nd kendilerini fi hangi durumlara ve koşullara yeterli dikkat yoktur çünkü birçok penetrasyon Sosyal mühendisliğin hacker'ın sanatı bu gerçeği dayanır.

CRC Press LLC tarafından o kadar kilitleme veya hassas verileri şifrelemek) ne zaman bilgilerin korunmasına büyük özen insanlar.

gerek “Böyle ve böyle Başkan Yardımcısı” bir çağrı geldiğinde aniden sıkı kullanıcı kimlik doğrulama ve kontrol prosedürleri takip çalışanlar onlar hakkında tüm “unutmak” “derhal.” “Başkan” Does kendisi

sorunları olan teknik destek hattı mı? Muhtemelen hayır, ama insanlar açıkça belirtildiği verilere erişmek için için kişi soran bile hassas bilgilere erişim taleplerini meydan yok, bilgi ihtiyacını sorgulamıyorum, kimliğini kanıtlamak için bir çalışanı sağlayan için tek bir kaynak itimat ve genellikle o kaynak yerleşik bir koruması şirket kendi ortakları için çalışan tanımladı fi katyon (ID) numaraları atamak. Bu rakam şirketin serbestçe istendiğinde henüz işçi rozetleri üzerinde açıkça gösterilir ve birçok hizmetlere erişim sağlar. Başarılı bir test geçerli çalışan geçerli bir çalışan kimlik numarasını elde edilmesi veya üretilmesi için bir yöntem belirleyebilir.

büyük organizasyonlar sağladığı gizli güveniyor. Bir şirket birkaç yüz çalışanı ötesinde büyür sonra, herkes sesli tüm çalışanları bilmek için giderek dif fi kült haline gelir. Böylece, şirketin BT ve İK personeli, şifreler, anahtar yukarıda belirtilen çalışan kimliği numarası olarak kullanıcı kimlik doğrulaması diğer yöntemlerle, güvenmek sistemde, çalışanlar yalnızca kimlik numarası ya da şifre ile anonim varlıkları, tanımladı fi ed olur. Bu daha işçinin kimliği üstlenmek veya bilgileri ifşa insanları kandırmak için sosyal mühendislik kullanımı kolaylaştırır. Tester yapısı içinde gizlemek mümkün olduğunda, keşif korkusu azalır ve test test etmeye devam etmek çok daha iyi olacaktır.

penetrasyon testlerinin başarıyla tamamlanmasının Diğer bir katılımcı en fazla sistem yöneticilerinin kendi sistemlerini güncel altındaki sistemler için en son güvenlik yamaları ve fi xES ile tutmuyorum basit bir gerçektir. Kolayca bir sistem yama konfigürasyonundalardır değişikliği veya prosedürel geçişle kaldırılan olabilirdi açıkları - Sistem hırsızlık büyük bir güvenlik açıklarından yararlanma sonucu meydana gelir. Sistem operatörleri sistemleri güvenliği konfigürasyonundalardır gerisinde izin vermeye devam gerçeği test sürekli sistemlerini nüfuz etmede başarılı olacağı anlamına gelir.

penetrasyon testi için uygun araçlar daha sofistike ve daha geniş bir alana dağıtılmış hale gelmektedir. Bu sistem istismar ve aracın nasıl herhangi bir teknik altyapıya gerek duymadan bunları uygulamak için son derece gelişmiş bile acemi korsanı izin verdi. Genellikle bu araçlar bir anda bir sistemde güvenlik açıkları yüzlerce Yeni delikler bulundukça, hacker araçları hayat daha da sefil ayak uydurmak zorundadır kötü yönetici için serbest bırakabilirsiniz hızlı yazılım şirketleri daha onları istismar. Sonunda, yönetici şey özleyeceğim ve bu şey sisteme girmeye kullanabilirsiniz bir deliktir.

**Saldırı Stratejileri**

testi biraz farklı görevi yaklaşacaktır gerçekleştiren her güvenlik çalışanı ve test tarafından kullanılan gerçek etkileşime kadarki değişecektir. Ancak, çoğu test durumları karşısında ortak olduğu söylenebilir birkaç temel saldırının tek yöntemle güvenmeyin. Farklı durumlar farklı saldırılar için diyoruz. tester bir yerde fiziksel güvenliğini ise, test binada almanın bir yöntemi deneyebilirsiniz; örneğin insanların sabah inrush sırasında kalabalığın yürürken. Bu işe yaramazsa, bir yan kapıya temizlik insanları aşağıdakileri deneyin. Bu işe yaramazsa, başka bir Aynı yöntem elektronik saldırılar için de geçerlidir. bir saldırı çalışmıyor (veya sistem o saldırı duyarlı değildir), deneyin.

yolunu seçin. penetrasyon test de bu yöntemi kullanmalısınız yüzden çoğu gerçek saldırganlar, değerli

rota deneyecektir. Test, bir şirketin ağı nüfuz teşebbüs edilirse, şirketin fi rewall (tabii ki, fi rewall testin

oldu sürece) tüm güvenlik dikkati olacak çünkü nerede saldırıyı başlamak için en iyi yer olmayabilir odaklandı.

lesserguarded alanlarını saldırı deneyin. Alternatif giriş noktaları arayın; örneğin, vb bir şirketin iş ortakları, ağ hizmetlerinde, masaüstü bağlı modemler, bağlantıları Modern kurumsal ağlar sadece fi rewall çok daha noktaları var, bu yüzden tam yararınıza kullanmak.

CRC Press LLC tarafından belirtilen politikalara uygun hale konsantre. Süreçler herkes kurallara uyar zaman iyi çalışabilir, ancak bu veya göz ardı edildiğinde öngörülemeyen sonuçları olabilir. Bir test saldırıyı gerçekleştirirken nedenle, son derece kullanın; Bir Web sitesine 1000 bayt URL girin; log bir ziyaretçilerin içine başkasının adını imzalamak; Bir sistem anormallik veya uyumsuzluk temsil şey deneyin. Gerçek saldırganlar konusu sistemin veya kuruluşun kurallarına ne de tester gerekir.

teknoloji, otomatik saldırılar münhasıran güvenmeyin. bu araçlar kullanmak daha “çekici” (ve kesinlikle daha kolay) zaman bir sistemi giren en etkili yöntem ortaya olmayabilir. teknik olarak gelişmiş olmasa da, önemli güvenlik çıkarabilir ve göz ardı edilmemelidir, “düşük teknolojili” saldırıların vardır. Toplum mühendisliği yaklaşımının bu tip sosyal mühendislik saldırı başlatmak için gerekli olan tek araç tester ses, telefon, ve insanlarla konuşmak yeteneği yöntemin basitliğine rağmen (ya da belki de, bunun için), sosyal mühendislik değerli bilgiler elde etmek için bir son derece etkilidir.

bidonunun dalış” da etkili düşük teknolojili araç olabilir. Çöp bidonunun dalış nd değerli bilgiler fi amacıyla konunun eylemini tanımlamak için kullanılan bir terimdir. En çöp kutularının bulunan tipik bilgiler eski sistem çıktısı, şifre personel bilgileri, raporların taslaklarını ve eski faks nakillerini almaktadır. bir liman çalışan yaklaşık olarak deneğin bilgisayarına tarama, aynı zamanda liman tarama gerektirdiğini teknik beceri herhangi gerektirmez.

kişilerarası iletişimde çok yetenekli olmayabilir test kullanıcılarının o etkili bir araç haline sosyal mühendislik gerekli içeriyor.

test ana hedeflerinden biri, algılama kaçınmaktır. penetrasyon testi temel ilke bilgileri kendi bilgisi veya onayı denekten elde edilebilir olmasıdır. Bir test test suçüstü yakalandı edilirse, bu söz konusu saldırı senaryosuna savunma yeterli olduğunu, de fi, tanımı gereği, anlamına gelmektedir. Aynı şekilde, test algılamak veya bir için kullanılabilir “fi ngerprints” bırakarak kaçınmalıdır. Bunlar fi ngerprints tester ve bir sistemi etrafında dair kanıt bulunmaktadır. fi ngerprints fiziksel (örneğin eksik raporlar, büyük fotokopi faturaları) olabilir ya da örneğin, test ya da bir binaya giriş ve çıkış günlüğü kapı giriş kontrolleri erişimini detaylandırma sistem

iki durumda da, bilgilerin imha yönetimi tarafından (yazılı olarak) testin bir parçası olarak tanımlanır ve onaylanır de fi sistemde herhangi bir şey yok etmeyin. Bir penetrasyon testinin amacı bir sistem veya süreç içinde fl aws ve çıkarmaktır - bilgi yok etmek değil. şirket bilgilerinin gerçek yıkımı sadece onun (potansiyel olarak değerli)

şirketi mahrum, ama aynı zamanda etik olmayan bir davranış olarak yorumlanır ve disiplin veya yasal işlem olabilir. örgütün yönetim testinin bir parçası olarak bilginin gerçek yıkımını gösteren test isterse, test gereksinimi teste tabi tutulan yönetimin yazılı onayını almak için emin olmalıdır. Tabii ki, “fi ngerprints bırakmaz etmek

Tester tester gizleyecekti sistem kayıtları değiştirebilir isteyebilirsiniz. Bu kabul edilebilir olsun ya da olmasın testi

önce test öznenin yönetimi ile görüşmek gereken bir konudur.

kademeli iyileştirme fırsat vermeyen etmeyin. Çoğu penetrasyon testi başarılı olabilmeleri için birçok araç ve kullanılmasını içermektedir. Bu tekniklerin çoğu tamamen bir kuruluşun güvenlik başarısızlığa bir organizasyon veya zayıflık maruz olmayacaktır. Ancak, bu tekniklerin her biri yaklaştıkça testin fi nal hedefine tester hareket edebilir.

örgütün güvenliğini gösterecektir tek zayıflık veya güvenlik açığı için bakarak, tester, birleştirildiğinde, aynı derecede birçok önemli, daha küçük zayıflıkları göz ardı edilebilir. Gerçek saldırganlar sonlu sabırla olabilir; böylece test taktik değiştirerek hazır olun. Her deney çalışacak değil, her teknik başarılı olacaktır. Çoğu penetrasyon test çalışmasına tekniklerin standart “araç seti” var. Ancak, farklı sistemler, farklı saldırılarına açıktır ve farklı test gerektirebilir. test akım bir çalışmıyorsa, başka bir yöntem geçmek için hazırlanmış olmalıdır. Bir elektronik saldırı sonuçlar veren değilse, fiziksel veya işlevsel saldırıya geçin. girişimleri bir şirketin ağ bağlantısı çalışmayan şekilde ise şirketin çevirmeli bağlantılar aracılığıyla ağa erişmeyi deneyin. son kez çalıştı saldırı konusu aynı bu kez başarılı olmayabilir.

CRC Press LLC tarafından keşfetmek için çok daha iyi bir konumda bulunuyor.

**Planlama**

penetrasyon testi gerçekleşebilir önce, açık bir test planı hazırlanmalıdır. test planı hedefleri ve test hedefleri detay parametreleri özetlemektedir ve test ekibi ve hedef organizasyonun yönetiminde hem beklentilerini anlatacağız.

penetrasyon testi planlama en önemli parçası hedef organizasyonun yönetiminin katılımıdır. yönetim onayı Penetrasyon testleri etik olmayan olmasının yanı sıra, makul “casusluk” olarak kabul edilir ve çoğu bölgelerde yasa tester tam ayrıntılı olarak test nişan belgelemek ve devam etmeden önce yönetimden yazılı onay ekibi konusu organizasyonun parçasıysa, organizasyonun yönetim ekibinin çabaları bilir ve bunlardan önemlidir. test ekibi organizasyon yapısının dışında ve testi yapıyorsa “kiralık” testi gerçekleştirmek için yönetimin organizasyonu ve hedef örgüt arasındaki sözleşmenin bir parçası olarak dahil edilmelidir. Her durumda, testi yönetimi böyle onay vermek yetkisine sahip olduğundan emin olun. Penetrasyon testleri bir organizasyonun altyapısına saldırıları içermektedir. Bu tip faaliyetler onaylanmış veya açıkça bunu yapmak için yetkisi yok birileri üstlenilen edilmemelidir.

gereği, penetrasyon testleri o sistemi veya kuruluşun nüfuz niyetiyle bir sistem veya organizasyon üzerinde kullanımını içerir. faaliyetin Bu tip zorunlu olarak, konu organizasyonda birisi test farkında olmasını ihtiyacı olanlar, aslında, faaliyet biliyoruz test hakkında bilmek emin olun. Ancak, mutlak minimuma testin listesini tutmak. çok fazla insan test hakkında biliyorsanız, hedefin faaliyetleri ve operasyonlar değişmiş bilmeyerek) ve test çaba sonuçlarını inkâr edilebilir. fi t beklentilerine davranış bu değişiklik davranışları edildiğini fark edince çalışanlar Batı Electric'in Hawthorne fabrikasında, bir ünlü çalışmanın adını Hawthornebilinir,

test sırasında, test gerçekleştirecek etkinliklerin çoğu gerçek yaşam saldırganlar sistemlerini nüfuz

aynı kişilerdir. Hedef örgütün personel bu faaliyetleri bulursa, onlar (haklı olarak) gerçek bir saldırı için testi saldırganı” yakalayabilir. Uygun yönetim personeli test faaliyetlerinin farkında olduğundan emin yaparak, meşruiyetini doğrulamak mümkün olacak.

alınması gereken önemli etik not penetrasyon testleri eylemi kasten güvenlik zayıflıkları belirlemek amacıyla konu ihlal içerir olmasıdır. Bu, aynı araçları ve gerçek yaşam saldırganlar kullanmak yöntemlerin çoğunu test gerektirir. Ancak, gerçek hacker bazen kanuna aykırı veya saldırılarını gerçekleştirmek için son derece davranışlarda. penetrasyon testi güvenlik profesyonel bir şirketin güvenlik prosedürlerini ve sistemlerini atlayarak ve ihlal arasındaki çizgiyi çizmek bekleniyor. Bu ayrımlar testin başlamasından önce yönetimi ile tartışılan ve da yasal sorunlar testin yürütülürken çıkarsa tekrar ele alınmalıdır. penetrasyon testi vermeyi kabul edildikten sonra, testin parametreleri kurulmalıdır. test parametreleri test türü belirleyecektir, testlerin amaçları ve test nasıl çalıştırıldığını fi ne de olacaktır işletim sınırları. Birincil karar olarak ne belirlemektir. Bu tanımını uzun ( “şirket ağına girmeye yeteneğini test”) geniş bir yelpazedeki son XYZ son ürün hakkında teknik bilgi kaybı riskini belirlemek”) yapabilirsiniz. Bu testin başarılı ya da başarısız kolay olur Genel olarak, daha fazla özgül test de Tanımlar tercih edilir. tester teknik spesifik fi katyonlarının bir üretmek mümkün olup olmadığını İkinci örnekte durumunda, test açıkça başardı. fi ilk örnekte söz konusu ağ sisteminde logging hareket yapar başarı oluştururlar veya test şebekesinden alınan gerçek veri üretmek Böylece, başarı ya da başarısızlık için özgül kriterleri açıkça de fi ned olmalıdır.

test planı ve belirlenen bir zaman sınırı olmalıdır. Testin süresi uzunluğu gerçek hasım sistemi girmeye

beklenebilir süreyi ve aynı zamanda makul ilgili olmalıdır CRC Press LLC tarafından

test ekibi veya yönetim biri tarafından testinde yerleştirilen herhangi sınırları açıklamalıdır. Takım

için istekli olduğunu “hasar” miktarını sınırlamak ahlaki hususlar varsa tester (belki yasal veya sözleşmeye erişmesi yasaktır sistem veya işlemin alanlar varsa, ya da bu açıkça olmalıdır Test planında açıkladı. Yine teste

kurallara uymayan gerçek yaşam saldırganlar ve saldırganlar gibi davranmaya çalışacaktır. yönetim test belirli etmek istiyorsa, bu açıkça de fi ned olmalıdır. test planı da test sırasında “yakalanma” nin usul ve etkilerini koymalıdır. Ne de fi nes “yakalanmadan” ve bu test de planda açıklanmalıdır nasıl etkilediğini.

parametreleri Tanımlanmış olmuştur kez test planı test için “senaryo” odaklanmalıdır. senaryo test, test şirket içinde üstlenecek pozisyondur. Test Şirket içerisindekiler (çalışanları, yüklenicileri, geçici çalışanlar vs.)

belirlemek için çalışıyor Örneğin, test şirket içinde geçici iş verilebilir. Test kuruluşa dış tehdit düzeyini

tasarlanmış ise, tester bir pozisyonunu üstlenecek “yabancı.” senaryosu olacak testin genel hedefi ne de de fi. şirketin bilgisayar veya tesislerin basit penetrasyon var mı? konu fiziksel veya elektronik saldırılara yoluyla fikri

kaybından endişe duyduğunu mı? Onların Web sitesine vandalizm endişe ediyorsunuz, Onların elektronik ticaret dolandırıcılık veya reddi hizmet saldırılarına karşı koruma? Tüm bu faktörler testi senaryosunu belirlenmesine

bir saldırı planlamak ve yürütmek durması amacıyla son derece önemlidir.

**Yapılması** tamamlandıktan sonra, test senaryoları kurulmuştur ve test test metodolojisini belirlemiştir, testiiçin zamanı. Birçok yönlerden, bir penetrasyon testi planının icra sonuçlanan askeri bir yürütme ile

Böyle bir kampanya olarak, üç ayrı fazlar vardır: keşif, saldırı ve (isteğe bağlı olarak) işgal.

keşif” faz olarak da adlandırılır) keşif aşamasında, test genellikle testin “sahnesini” anket olacaktır. tester fiziksel bir

planlıyorsa, keşif aşaması herhangi bir yetersizlik ya da güvenlik açıkları için teklif edilen yeri inceleyerek oluşacaktır.

çalıştırdığı şekilde fark edilebilir kalıpları için bakmak gerekir. insanlar gelip düzenli aralıklarla gidiyor mu? Koruma

ne kadar yakından insanların girip siteden ayrılmadan incelemek mı? onlar normal çalışma saatleri sonrasında

daha yapın ve düzenli zamanlarda yapılan bu mermi vardır? Farklı zamanlarda işgal sitenin farklı alanlarda

birbirlerini tanımak, ya da birbirlerine yabancı gibi görünüyor yapmak insanlar görünüyorum. fiziki takibin amacı olduğunca hedef konumu ile olduğu gibi tamamen aşina olmak ve sitenin davranışlarında tekrarlanabilir kalıpları kalıpları anlamak ve onlara karıştırma testinin önemli bir parçası olabilir. testi ediliyorsa, test mümkün olduğunca hedef çevre hakkında çok fazla bilgi edinmek için keşif aşamasını eşleme ve gözetim bir takım teknikler içerecektir. tester fiziksel olarak hedef konumunu gözlemlemek olamaz

çevrenin elektronik sondalama kullanılmalıdır. tester hedef sistemi veya ağın bir elektronik “harita” geliştirerek Nasıl ağ dışarı atılır? Ne ana erişim noktaları vardır ve ne tür donanım ağını yönetiyor? Çeşitli barındıran tanımladımusunuz ve ne çalıştıran işletim sistemleri veya platformlar? Başka hangi ağların da buna bağlanır? çevirmeli ağ kullanılabilir hizmet mıdır ve dial-out hizmeti dışında almak için kullanılabilir?

öznenin çevrenin doğrudan gözetim şeklinde olmak zorunda değildir. Ayrıca daha dolaylı diğer yollarla

Örneğin, konu hakkında bilgi edinmek için bazı iyi yerlerdir:da hoşnutsuz çalışanlar bilgisayar gösterileri bilgisayar kulüp toplantıları listeleri, örgüt yapıları başvurusu bildiriler ve turlar

yiyecek ve içeceklerin teslim Satıcıları CRC Press LLC tarafından

kullanabileceği istismar edecektir. Ayrıca henüz halka açık forumlarda içine yapılmış değil yeni saldırılar olabilir.

güvenmek zorundadır tester önceki testlerde elde edilen ve bilgi güvenliği alanında çalışan güncel olayların bilgisi muhtemel caddeleri takip etmek.

temel yöntem, yaşanabilecek çeşitli önlemler ve bu önlemler için kullanılabilir yanıtları kullanımı (en azından belirlemelidir.

adım, hedef çevre üzerindeki fiili saldırıdır. saldırı sitesine veya sisteme girmeye ve yerinde olabilecek bir kısıtlamalarını aşmak için keşif aşamasında bulunan zayıflığını istismar oluşacaktır. tester keşif aşamasında yaptıysa, saldırı aşaması çok daha kolay hale gelir.

aşamasında Zamanlama kritik önem taşıyabilir. Orada tester bir saldırı çalıştırmak için zaman lüksüne sahip ve bu, arama testi ve açığa çıktıkça çevreye uyum sağlamak için büyük fl esneklik sağlayan edilebilir.

durumda, zaman bolluğu kullanılamaz. tester sahibinin öğlen saatinde fi les gelen bilgi toplamaya

bekçi mermi arasında bir bina girmeye çalışan veya bilinen bir alarm takıldı ve sistemin izinsiz tepkisi ara saldırıyı tamamlamayı deneyen bu durumda olabilir (a penetrasyon tanınması ve yanıt ya da önlem arasındaki süre) ulaşılır.

saldırı sırasında, yeni bir bilgisayar veya ağa test kazançları girişi, test saldırının işgal aşamasına geçmemiz Meslek test harekât üssü olarak hedeflemislerdir belirtmek için kullanılan terimdir. tester bilgi toplama veya durumunu izleme veya tester diğer hedeflere karşı saldırı için bir üs olarak hedef kullanmak isteyebilir hedefte daha

geçirmek istiyor, çünkü bu olabilir. tester o hedef ortamında mukim olduğu zaman süresince tespiti maruz işgal aşaması, belki test için en büyük tehlike sunuyor. tester işgal safhasına girmek seçerse, adımlar kadar tester varlığı belirlenemeyen yapmak alınmalıdır.

penetrasyon testi testin tamamlanmasından önce keşif / saldırısı / işgal döngüyü defalarca tekrarlamak dikkat etmek yeni saldırı hazırlanarak piyasaya gibi, test saldırı sonuçlarına tepki ve test planının bir sonraki adıma geçmek saldırıyı terk edip saldırının başka bir türü için keşif başlamak için karar vermelidir. Bu döngünün tekrarlanması uygulama sayesinde, test sonunda testi tamamlayacak.

elektronik - - iki temel test türlerinin her biri farklı araçları ve metodolojileri vardır. güçlü ve her tür zayıflıkların penetrasyon testi yürütülürken muazzam yardımcı olacaktır. Örneğin, fiziksel girmeler genellikle teknik bilgi bilgi gerekmez. bazı uzman teknik deneyim (örneğin, alarm sistemleri atlayarak) gerektirebilir zaman, fiziksel operasyonlar güvenlik, bina ve site operasyonlar, insan doğası ve sosyal etkileşim alanında beceri gerektirir.

penetrasyon sırasında kullanılan “araçlar” her test cihazı ile değişir ama genel olarak iki genel alana ayrılır:

sistemlerinin kötüye kullanma ve sosyal etkileşim kötüye. koruma sistemlerinin kötüye örnekleri bilgi istemini toplayıp masalarında açıkça sol bilgiyi kopyalama, yanlışlıkla kilitli bir fi le odası erişen, (erişim kontrollü aşağıdaki birisini) bindirme, geçmiş dikkatsiz güvenlik görevlisi yürüyen içerir. Koruma sistemleri tipik ve normal

hedefi korumak için kurulur. Hedefin operasyonel prosedürlerin Bilgi normal ve anormal tehditler hem karşısında etmek mümkün test senaryolarını geliştirmeye test sağlayacaktır.

güvenlik bilincinin eksikliği herhangi bir başarılı bir fiziksel penetrasyon testinde büyük rol oynayabilir.

bilginin değerinin farkında değilseniz, düzgün onu korumak için daha az olasıdır. hassas bilgileri saklamak politika ve prosedürlerin farkındalık eksikliği birçok şirket bol miktarda bulunur. penetrasyon test aksi olmalıdır bilgilere erişmek için bu yararlanabilir.

sosyal mühendislik belki etkili penetrasyon testleri için mükemmel bir araçtır. Toplum mühendisliği, fizik ve kontrollerinde açıklarını istismar “içeriden” yardım elemanı ekler ve

CRC Press LLC tarafından

penetrasyonlar, diğer taraftan, genellikle fiziksel girmeler benden daha derinlemesine teknik bilgi gerektirir.

yaşam saldırganlar durumunda, bu bilgi kendi olabileceği gibi başka birinden “ödünç”. Son yıllarda, birçok yeni

teknik özellikler internette penetrasyon ve saldırı araçlarının yüksek kullanılabilirlik, bu araçların gelişmişliği ile

azalmış görünmektedir. Böylece, aracın geliştiricisinin ve fl içinde bilginin bir hedefe büyük zarar ict “ödünç”

büyük bir olmadan kimse için nispeten basit hale geldi. Orada hala beceriyle teknik olarak gelişmiş

çok sayıda bir sisteme karşı başarılı bir saldırı başlatmak için, ancak, vardır.

saldırıda kullanılan aletler genellikle otomatik analiz veya saldırı özellikleri sağlamak olanlardır. Örneğin, birçok serbestçe

ve ağ güvenliği analiz araçları bir sistemin açıklarını keşfetmek için otomatik bir yöntem ile test cihazı sağlamaktır.

test fi elle nd mümkün olabilir açıklarını, ama otomatik araçların kullanımı çok daha büyük ef fi verimliliğini sağlar. Aynı

tarayıcıları gibi araçlar (yani bir hedef ana bilgisayarda kullanımda olan hangi portların test anlatmak), ağ “koklayıcıların”

için bir ağ üzerinde o rekor tra fi c) ve “savaş dialer” (yani sistematik için telefon numaralarını aramak ) erişilebilir

keşfetmek tester bu zayıflıkları yararlanmaya almalı hedef sistemdeki zayıflıklar ve olası caddeleri ile ilgili bilgi zenginliği ile test

sistemi, sistem konfigürasyonundalardır ve sistem diğer sistemlere sahiptir ilişki: elektronik testleri yürütürken

temel alanları vardır. İşletim sistemine karşı saldırılar henüz yönetici veya platformun üreticisi tarafından yamalı

platformda böcek veya delikler istismar. Sistem konfigürasyonundalardır karşı saldırılar değil son sistem bültenleri

sistem kayıtlarını kontrol kullanılmayan hesapları veya sistem elemanlarının uygunsuz konfigürasyonundalardır

kaldırarak gibi rutin görevleri göz ardı etmek aşırı çalışan yöneticilerin doğal bir eğilim kullanmaya çalışabilir. Son olarak,

hangi saygı diğer sistemlerle bir sistem vardır ilişkisini kullanması olabilir. Bir hedef sistemine sahip bir güven

tester başka makineden hedef makinede yönetici hakları tesis edebilir? Birçok durumda, başarılı bir penetrasyon

hedef makinesini saldırmasını değil sonuçlanacaktır, ancak desteklendiği ilk başarıyla hedef makineye “ilişki” çeşit

saldıran.

**Sonuçlar**

testinde fi nal adım yönetimine testin bulgular rapor etmektir. Raporun genel amacı ve sesi aslında bir test

sonucun kendi beklenti yönetimin ifadesiyle nişan başında ayarlanmalıdır. Gerçekte, ne test belirleyecektir için

raporu bakmak istenir. tester bir şirketin genel fiziksel güvenliğini incelemek istenir, raporda fl vb şirketin

kullandığı çeşitli güvenlik önlemlerinin genel bir bakış açısı yeniden olacaktır. tester belirli bir bilgisayar sistemi

kontrolleri değerlendirmek istenir, raporda büyük olasılıkla o makineden ayrıntılı analizini içerecektir.

penetrasyon testi sonucunda üretilen rapor konusu vardır açıkları ve bu güvenlik açıklarından yararlanmak için

kesin saldırılarla ilgili son derece hassas bilgiler içermektedir. penetrasyon test raporu sadece bir ihtiyaç

hedefin yönetimi içinde olanlara dağıtılır sağlamak için büyük özen gerekir. Raporda şirketin yüksek hassasiyet

işaretlenmiş olmalıdır. özellikle hassas veya gizlilik dereceli bilgilerinin söz konusu olduğunda, belirli bir fonksiyonel

sadece bilgi içeren her sürümü ile raporun çeşitli sürümleri olabilir.

belgelenmiş halindeki test angajman rövanşı ile yönetimini sağlamalıdır. Test sırasında yaşananların

Bu hedefin açıkları bir listesini yönetim sağlar ve gelecekteki saldırılara karşı korumak için kullanılan

değerlendirmek için onları tanır.

testin ilk hedefleri belgelenmelidir. Bu test egzersizin amacı ve niyeti aşina hale orijinal karar verme sürecinin

değildi kimse yardımcı olacaktır. Daha sonra, test sırasında kullanılan metodoloji tarif edilmelidir. Bu, kullanılan

hakkında bilgi, bu saldırıların başarılı veya başarısız ve test test sırasında yaşanan dif fi zorluklardan ve içerecektir. aşırı açıklayıcı ve (bazı durumlarda) tehlikeli olabilir kullanılan hassas yöntemler hakkında çok detay sunarken, test ekibi tarafından kullanılan genel yöntemler ve prosedürler rapora dahil edilmelidir. Bu sisteme girmek için test takımı için ne kadar kolay veya dif fi kült bir fikir edinmek için önemli bir araç olabilir.

CRC Press LLC tarafından metodoloji ve prosedürler bir saldırı ev bilgisayarındaki İnternet bağlantısı fiyatına internetten başlatılabilir olduğunu Ancak, şirket hedefini güvence içine daha fazla kaynak koymak isteyebilirsiniz.

Raporda ayrıca test sırasında bulunan bilgileri listelenmelidir. Bu o nasıl bulunduğunu, bulunan ve dif fi büyük onu nding fi vardı nerede, bulunmuştur hakkında bilgi içermelidir. Bu bilgiler yönetimini testi ile ortaya çıkarılan sorunlarının derinlik ve genişlik hissi vermek önemlidir. Bulunan öğelerin listesi yalnızca bir veya iki ürün uzunsa, sürece elbette test sadece bu bir veya iki öğe arıyordu) fonksiyonlarını yerine getiremezler. Liste birkaç uzunluğunda Ancak, şirketin güvenlik politikaları ve prosedürleri de dramatik iyileştirmeler yapmak içine yönetimini

analizi için bazı bilinen miktarla karşılaştırıldığında hedefin güvenlik genel bir özetini vermelidir. Örneğin,

bilgisayarlarda şifreleri yüzde 10 kolay tahmin edildiğini bulmalarına olabilir. Ancak, önceki araştırmalar veya tester

internet veya diğer istemciler üzerinde ortalama bilgisayar yüzde 30 kolay tahmin şifreler içerdiğini

Böylece, şirket aslında sektörü norm daha iyi yapıyor. Raporda şirketin binalarda korumaları yüzde 25'i test rozetleri kontrol etmediğini göstermektedir Ancak, bu büyük olasılıkla yüksek kabul ve daha fazla eylem için ayrıca fi nal sonucuna testin ilk hedefleri karşılaştırmak gerekir. Test yönetimi tarafından belirlenen gereksinimlerini

Sonuçlar beklenen veya beklenmeyen ve ne dereceye kadar mıydı? Test hedeflenen alanda problemleri ortaya mı, diğer ilişkisiz alanlarda bulundu? yönetimin özgün beklentileri ile uyum içinde testlerin maliyeti veya karmaşıklık oldu

rapor ayrıca deneğin güvenliğin geliştirilmesi için öneriler içermelidir. öneriler penetrasyon testinin bulgularının edilmiş alanların güvenliğini artırmaya yardımcı olabilecek sadece testin kapsadığı alanlar, aynı zamanda bulunmaktadır edilmelidir. Örneğin, tutarsız sistem konfigürasyonundalardır daha sıkı değişim kontrol süreci gösterebilir. tester iyi bir kullanıcı kimlik doğrulama gereksinimlerine yol açabilecek şirketin yardım masasından için izin Başarılı sosyal mühendislik girişimi.

saldırganlar faaliyetlerini paralel görünse de, penetrasyon testi, aslında, kendi sistemlerinde mevcut gerçek tehlikelere ağların sahiplerini uyarmak için hizmet vermektedir. Böyle otomatikleştirilmiş liman tarama, savaş arama ve değerlendirmeleri gibi diğer risk analiz faaliyetleri, bir sistemde var olabilecek teorik açıklarını işaret etmek bilgisayarın sahibinin bu faaliyetler birinden çıkış bakmak ve bu delikler temsil asıl tehdit aldığını iyice sistemde delikleri ve zayıf noktalar bir listesini göreceksiniz. Etkili bir penetrasyon testi, ancak, aynı sistem delikler ele alınmamıştır oluşabilir gerçek hasarı gösterir. Bu ön plana bir sistem veya siteye erişmek için teknikler getirir ve daha fazla dikkat gerektiren açık alanları yapar. (Standart risk analizleri ve bertaraf stratejileri ek

penetrasyon testi teknikleri uygulayarak, güvenlik profesyonel öznenin kuruluş tam bir güvenlik görüntü

CRC Press LLC tarafından

Stephen James

**Ödemek**

organizasyonlar internete kendi iç ağlarını bağlamak devam ederken, sistem yöneticileri ve yöneticileri sistemlerini güvence altına almak ihtiyacının giderek daha duyarlı hale gelmektedir. kendini kesmek denetim (SHA) onlar bir

hacker tarafından keşfedilir önce bir ağda güvenlik zayıflıkları belirlemek ve ortadan kaldırmak için korsan yöntemlerini kullanan bir yaklaşımdır. Bu makale, bilgisayar kaynaklarına erişmek için yetkisiz kişilerin izin ve ağ

güvenliğini artırmak için ağ yöneticileri için adımları sağlar en sık görülen korsan teknikleri anlatılmaktadır.

**Giriş**

Bugünün elektronik ortamda, saldırıya uğrama tehdidi birkaç talihsiz kuruluşlarda meydana gelen artık pek mümkün olaydır. Hacker olaylar ve tehlikeye sistemlerin yeni raporlar hemen her gün görünür. organizasyonlar

internete kendi iç ağlarını bağlamak devam ederken, sistem yöneticileri ve yöneticileri sistemlerini güvence altına

ihtiyacının giderek daha duyarlı hale gelmektedir. Temel şifre kontrolleri uygulamak artık verilere yetkisiz erişime karşı korumak için yeterlidir. Organizasyonlar artık değerlendirmek ve sistemlerini korumak için daha fazla

güncel teknikleri arıyoruz. Gelişmekte olan en popüler ve pratik tekniği kendini kesmek denetim (SHA) 'dir. SHA bir hacker tarafından keşfedilir önce bir ağda güvenlik zayıflıkları belirlemek ve ortadan kaldırmak için korsan yöntemlerini kullanan bir yaklaşımdır.

Bu makale SHA için metodolojiyi ve hacker geçmişte çeşitli sistemlerin nüfuz sağladı popüler

korsan bir takım teknikler sunar. Her bir açıklama tür saldırıları önlemek için izlenmesi gereken

önerdi sistem yönetimi adımlar veya önlemler bir dizi izler. tartışılan konuların bazılarını UNIX

sistemlerine özgü olsa da, kavramlar, genel olarak tüm sistemlere uygulanabilir.

**Kendinden Hack Denetim Amaçları**

temel amacı yetkisiz kişilerin sisteme erişmek için izin verebilir tüm potansiyel kontrol

zayıflıklarını tespit etmektir. Ağ yöneticisi tanıdık ve sistem güvenliğini aşmak için bilinen tüm korsan

teknikleri kullanmalıdır. Denetimin yapısına bağlı olarak, objektif (erişim yok olabilir) ya da (yani,

sabotaj) sistemini yok erişimin bir kullanıcının mevcut seviyelerini uzatmak ya olabilir.

**Kendinden Hack Denetim Metodolojisi Bakış**

yararlı bir SHA gerçekleştirmek için, hacker farklı tespit ve anlaşılmalıdır. dünyanın uzak bir bölgesinde bir laboratuarda oturan parlak bir bilgisayar bilimi mezunu olarak bir hacker klişe tehlikeli bir yanılgıdır. Böyle hacker mevcut olmasına rağmen, güvenlik ihlalleri çoğunluğu hareket görülen örgüt personeli tarafından yapılmaktadır. Hackerlar dört tip olarak kategorize edilebilir:

sisteme erişim yetkisi bir kuruluş içindeki kişiler. Bir örnek Hesaplar Ödenecek uygulama

menüsü fonksiyonları erişimi olan Muhasebe departmanında meşru personel olabilir.

© 2004 CRC Press LLC tarafından gibi personelini kapsayabilir.

sisteme erişim yetkisi bir kuruluşun dışında kişiler. Bir örnek kuruluşun yazılım satıcıları bir

uzaktan sistem destek kişi olabilir.

sistemine erişmek için yetkiniz olmayan bir kuruluşun dışında kişiler. Bir örnek örgütü ile

hiçbir bağlantısı yoktur denizaşırı bir ülkede bir internet kullanıcısı.

SHA amacı sistem güvenliğini tehlikeye herhangi akla yöntemi kullanmaktır. Dört korsan türlerinin

biri tam olarak tüm olası güvenlik risklerini değerlendirmek için düşünülmelidir.

**Popüler Hacker Teknikleri**

Aşağıdaki bölümlerde teknikler en yaygın çeşitli kurumsal sistemlere erişim sağlamak için hackerlar

tarafından kullanılan tanımlar. Her bölüm korsan tekniğini tartışır ve bu riskleri azaltmaya yardımcı olmak uygulanabilecek temel kontrolleri önermektedir. Ağ yöneticisi bu tekniklerin her biri çalışmalıdır ve kuruluşun belirli bir çevreye uyum sağlayan prosedürleri belirlemelidir.

**Log-in erişme İstemi**

Bir bilgisayar sistemine yasa dışı erişim sağlamanın bir yöntemi, giriş-in istemi geçer. Hacker tesis

fiziksel olarak veya bir çevirme bağlantısı üzerinden sisteme erişmeye çalışan olduğunda bu

durum ortaya çıkabilir.

**Fiziksel erişim.**

kurumsal bilgi sistemleri güvenliğini önemli bir adım bilgisayar kaynaklarına fiziksel erişim

yeterli sınırlı olduğunu sağlamaktır. Bir terminale fiziksel erişim sağlayan herhangi bir iç veya dış kişi

oturum açma isteminde oturum açma girişiminde fırsatı verilir.

kuruluşun tesis içinde bir terminal yoluyla yetkisiz sistem erişimi için potansiyelini azaltmak için,

yöneticisi temin etmelidir:

Terminaller fiziksel olarak güvenli ortamlarda bulunur.

Uygun erişim kontrol cihazları bilgisayar donanımı bulunduğu alanlara erişmek için kullanılabilir

tüm kapı ve pencereler yüklenir.

ağlara bağlanan Kişisel bilgisayarlar şifre korumalı onlar serbest alanlar bulunuyorsa bulunmaktadır.

sisteme erişmeye çalışan bir korsan oturum açma istemini erişim sağlamasını önce meşru bir

parola tahmin etmek gerekecektir.

Kullanıcılar veya onların çalışma alanları yakınında şifrelerini yazmayın.

**Çevirme erişimi.**

istemindeki log-erişmek için bir başka yöntem konakçıya olarak çevirmektir. Birçok “Daemon dialer” Internet üzerinde kolayca kullanılabilir. çevirmek için bir dizi numara verildiğinde Bu programlar, geçerli modem numaralarını

tanımlayabilir. Bir hacker bulduğunda bir

© 2004 CRC Press LLC tarafından

çevirmeli ağ erişimi yoluyla güvenlik ihlalleri için olasılığını en aza indirmek için, ağ yöneticisi

etmelidir:

Yeterli kontroller böyle çevirmeli oturumları için, kullanılmadığı zaman modemi kapatarak geri arama tesisi kullanarak ya da bu tür bir kerelik şifre olarak, kimlik doğrulama ekstra seviye gerektiren çevirmeli oturumların için yerinde .

Hacker erişilmiş hangi sistemin bilmez ki kuruluşun logosu ve adı günlük ekran kaldırılır.

Bir uyarı mesajı bir suçtur ve bunların faaliyetleri kaydedilebilir olabileceğini sisteme erişmek

yetkisiz kişilerin uyarır. Bu, bazı ülkelerde yasal bir gerekliliktir.

**Şifreleri elde edilmesi**

Hacker bir kuruluşun erişim kazandı sonra log-in istemi, o sistemde oturum açmayı

deneyebilirsiniz. Bu prosedür geçerli bir kullanıcı kimliği ve parola birleşimi gerektirir.

**Brute Force Saldırıları.**

Kaba kuvvet saldırıları geçerli şifreleri tahmin etmek manuel ya da otomatik girişimleri içerir.

Programı tahmin basit bir şifre C kod yaklaşık 60 hatları veya PERL 40 hatlarında yazılabilir. Birçok şifre tahmin programları internette mevcuttur. Çoğu hacker otomatik olarak çeşitli sisteme atanan varsayılan şifreleri topluluğudur Yüklendiklerinde zaman hesapları bir “şifre isabet listesi” var. Örneğin, çoğu UNIX sistemlerinde konuk hesabı için varsayılan parola “misafir” dir.

ağı yetkisiz erişime karşı korumak için, ağ yöneticisi temin etmelidir:

Tüm kullanıcı hesapları şifre ile korunmaktadır.

Şifre değerlerin uygun tahmin önlemek için seçilir.

Sistem kurulduktan sonra Varsayılan şifreleri değiştirilir.

Başarısız log-in girişimleri kaydedilir ve uygun olarak takip edilmektedir.

Kullanıcı hesapları oturum açma başarısızlık önceden tanımlanmış sayıdan sonra dışarı kilitlenir.

Kullanıcılar tahmin etmek zor şifreler seçmek zorunda kalıyor.

Kullanıcılar, yıl boyunca periyodik olarak şifrelerini değiştirmeleri zorlanmaktadır.

Kullanılmayan kullanıcı hesapları devre dışı bırakılır.

Kullanıcılar eğitimli ve uygun parola yönetimi ve seçimin önemi hakkında düzenli olarak

hatırlatılır.

© 2004 CRC Press LLC tarafından

Çoğu UNIX siteleri adlı bir dosyada ilgili kullanıcı hesapları ile birlikte şifrelenmiş parolaları saklamak / etc / passwd. Bir hacker bu dosyaya erişmek durumunda, o sadece böyle Crack gibi bir şifre kırma programı çalıştırabilirsiniz. UNIX sistemleri (denilen kript) tarafından kullanılan aynı şifreleme algoritması ile standart bir sözlüğü şifreleyerek eserlerini Crack. Bir eşleşme bulana kadar sonra şifre dosyasındaki girdileri karşı her şifreli sözlük kelimesi karşılaştırır. Çatlak gelen isimsiz bir File Transfer Protocol üzerinden serbestçe kullanılabilir ftp.cert.org /

araçlar / köründe.

şifre kırma yazılımı hacker'ın kullanımını mücadele etmek için, ağ yöneticisi temin etmelidir:

Şifreli şifreler gölge şifre dosyası ve dosyanın yeterince korunduğunu saklanır.

Tüm “zayıf” şifreleri şifre dosyası karşı Crack çalıştırarak tanımlanır.

Böyle Npasswd veya Passwd + olarak Yazılım tahmin etmek zor şifreler seçmek için kullanıcılar zorlamak için kullanılır.

Kullanıcılar veya çalışma ortamlarına yakın şifrelerini yazmayın.

Kullanıcıların sadece az sayıda kopyalama riskini en aza indirmek için komut satırından erişebilir / etc /

passwd dosya.

**Tuş Günlüğü.**

Bu oturum açma oturumları yakalamak için kısa bir senaryo yazmak için en az 30 saniye sürer. Bir

hacker bir iş istasyonunda bir tuş-günlük programını yüklemek için bir disketi kullanabilir. Bu Truva atı kurulduktan sonra, bu tetikleyici anahtar kelimelere dayalı, arka planda çalışır ve her oturum açma oturumunda yakalar. Hacker uzak bir yerden yakalanan tuş vuruşlarını okuma ve sisteme erişebilir. Bu teknik çok basit ve hemen hemen her zaman farkedilmez.

Bir tuş-günlük programı yoluyla sisteme hacker'ın erişimini engellemek için ağ yöneticisi temin

etmelidir:

Ayrıcalıklı hesabı (örneğin kök) bir kerelik şifreleri gerektirir.

Ev sahibi dosya sistemi ve bireysel kullanıcıların iş istasyonları periyodik tuş-günlüğü

programlarını içerebilir Truva Atları taranır.

Bilgisayar donanımı için yeterli fiziksel erişim kısıtlamaları Truva Atları yüklenmesini kişileri

engellemek için vardır.

**Paket Sniffing.**

İnternet ağ analizörleri ve dahil olmak üzere ağ izleme araçları geniş bir yelpazede sunuyor “paket

koklayıcıları.” Onlar bir iletişim segmenti boyunca iletilir olarak veri paketlerini yakalayarak Bu araçlar işi. Bir hacker bu yazılım bir LAN ve yüklere bağlı bir PC'ye fiziksel erişim sağlayan sonra, o da yerleri arasında transfer gibi verileri takip edebiliyor. Alternatif olarak, korsan ofis ve yakalama veri paketleri halinde bir ağ bağlantı noktasına bir dizüstü ekleyebilirsiniz.

Bu ağ trafiği genellikle şifreli değil hatırlamak, korsan özellikle arasındaki, geçerli bir kullanıcı

hesabı ve şifre kombinasyonları yakalamak dair yüksek şans

© 2004 CRC Press LLC tarafından

isimsiz FTP üzerinden serbestçe kullanılabilir ftp.ee.lbl.gov en

tcpdump2.2.1.tar.z.

paket izleyiciler aracılığıyla hesap ve şifre sızıntıları olasılığını azaltmak için, ağ yöneticisi

etmelidir:

Haberleşme hatları pratik olduğu kadar segmente edilmiş bulunmaktadır.

Oturum açma oturumları ve diğer hassas veriler Kerberos gibi yazılımları kullanılarak şifrelenmiş biçimde iletilmektedir.

Ayrıcalıklı hesabı (örneğin kök) bir kerelik şifreleri kullanarak işaret.

iletişim hatları ve bilgisayar donanımı fiziksel erişim kısıtlanır.

**Sosyal mühendislik.**

Hackerlar genellikle zaman (genellikle yaklaşık iki hafta) süreyle kullanılmamış bir kullanıcı hesabı

ve yönetici sesle tanımak olası değildir bir kullanıcıya ait olduğundan emin olun. Bilgisayar korsanları

genellikle başka bir binada devletlerarası kullanıcılara veya kullanıcılara ait hesapları hedef alır. Onlar bir seçtikten sonra, bir kullanıcının kimliğini üstlenecek ve onların şifrelerini unuttuysanız açıklayan, yönetici yardım masası arayın. Çoğu durumda, yönetici veya yardım masası telefonla hacker için şifreler sıfırlar.

infiltrasyon bu tür güvenli ağı tutmak için bir çaba, ağ yöneticisi temin etmelidir:

Tüm personel düzenli hatırlattı ve veri güvenliğinin önemi hakkında ve doğru şifre yönetimi

konusunda eğitimli.

Organizasyon belgelenmiş ve telefonla şifreleri sıfırlamak için prosedürleri kontrol etti.

Personel sosyal mühendislik saldırıları kurbanı yoktur. Personeli Bir hacker bilgi sistemleri

departmanı bir üyesi olarak kendisini yanlış ve şifre isteyebilir olasılığının farkında olmalıdır.

**Genel Erişim Yöntemleri**

Hackerlar başka bir sistemden bir ana bilgisayar sistemine erişmek için çeşitli yöntemler kullanırlar.

**Internet Protokol Adresi Sızdırma.**

Tipik bir ağda, bir konak (Bir kullanıcı hesabı ve şifre kombinasyonunu gerektirmeden, yani) kimlik

doğrulaması gerektirmeden onunla iletişim kurmak için diğer “güvenilir” ana sağlar. gibi dosyaları yapılandırarak güvenilen olarak Sunucular tanımlanır. rhost ve

hosts.equiv Dosyalar. o iletişim bağlantıları kurmak için izin verilmeden önce kimlik doğrulaması sağlaması gerekir güvenilen olarak tanımlananlar dışındaki herhangi konak.

İnternet Protokolü (IP) sızdırma güvenilmeyen ana ağa bağlanma ve güvenilir bir ev sahibi gibi

davranarak içerir. Bu erişim güvenilen konağın buna IP numarasını değiştirerek korsanı tarafından

sağlanır. Başka bir deyişle, izinsiz konak kimlik doğrulaması için zorlu değil, yerel ağdaki ana aptallar.

güvenlik bu tür ihlalleri önlemek için ağ yöneticisi temin etmelidir:

© 2004 CRC Press LLC tarafından içinde güvenilir olarak sadece uygun barındıran tanımlanmıştır / etc / hosts.equiv, ve bu dosyanın üzerine dosya izinleri

yeterli.

Sadece uygun barındıran kullanıcıların / 'içinde tanımlanır. rhost Dosyalar. Pratik ise, bu dosyalar çıkarılmalıdır.

**Katılımsız Terminaller.**

Böyle öğle saatinde olarak uzun süre için açık ve sahipsiz imzalanan sol kullanıcı terminalleri bulmak

oldukça yaygındır. Bilgisayar korsanı kullanıcıların çalışma alanlarına fiziksel erişebilir varsayarsak (veya korsan içeriden olduğunu varsayarak), bu durum sistemin güvenliğini tehlikeye karşı bir hacker için mükemmel bir fırsattır.

hacker, yıkıcı bir virüs indirmek, bir Truva atı yerleştirin yetkisiz işlemleri gerçekleştirmek için katılımsız terminali kullanmak kullanıcının değiştirebilir. rhost dosya veya korsan sonradan oturum böylece kullanıcının şifresini değiştirin.

Ağ yöneticisi sağlayarak gözetimsiz terminalleri ile erişimden tehlikesini en aza indirmek için:

Kullanıcı oturumları otomatik hareketsizlik önceden belirlenen bir saatte zaman aşımına uğrar veya parola korumalı ekran koruyucular çağrılır.

Kullanıcılar düzenli eğitimli ve onlar sahipsiz onların çalışma alanları bırakmak bekliyoruz zaman kendi

oturumlarını kapalı imzalama önemi hakkında hatırlatılır.

Yeterli kontroller kullanıcıların çalışma alanlarında fiziksel erişimi yetkisiz kişilerin önlemek için

vardır.

**Yazılabilir Seti Kullanıcı Kimliği Dosyaları.**

UNIX çalıştırılabilir dosyaları dosya izinleri ayarlamak kullanıcı kimliği (SUID) kök yaparak kök yetki

verilmek istenen verir. Hacker'lar genellikle tüm SUID dosyaları tespit etmek ve yazılabilir olup olmadığını belirlemek için dosya sistemi üzerinden arama. yürütüldüğünde sonraki sefer, yazma, böylece onlar yazılabilir

olmalı, korsan SUID programı dahilinde basit bir kod satırı ekleyebilirsiniz / etc / passwd dosya ve bu root haklarını kazanmak için korsanı sağlayacaktır. Aşağıdaki UNIX komut tüm dosya sistem boyunca SUID kök dosyalarını arayacaktır: / -Kullanıcı kök -perm -4000 -print bulmak

Ağ yöneticisi sağlayarak SUID dosyalar arasında yasadışı erişim imkanı azaltabilir:

programların en az sayıda SUID dosya izinlerini atanır.

SUID olan programlar kök dışında kullanıcılar tarafından yazılabilir değil.

onlar etkili SUID kök çünkü sistem cron tabloları (özellikle kök cron tablo) içinde tanımlanmış Çalıştırılabilirler kök dışında kullanıcılar tarafından yazılabilir değil.

**Bilgisayar Acil Müdahale Ekibi Danışmanlar.**

Bilgisayar Acil Müdahale Ekibi (CERT) yeni bir güvenlik poz saptanmıştır zaman uyarıları

veren. Bu riskler sıklıkla yetkisiz kullanıcıların sistemlerine kök erişmek için izin verir. Hackerlar her

zaman en son CERT uyarılarına takip © 2004 CRC Press LLC tarafından

Ağ yöneticisi temin etmelidir:

Tüm CERT uyarılarının gözden geçirilerek bir kontrollü ve zamanında gereği yapılmıştır.

Checksum'ları uygulama öncesinde CERT yamalar bütünlüğünü sağlamak için kullanılır.

**Hacker Bülten tahtaları.**

İnternet sistem güvenliği değerli bir bilgi kaynağı olarak hareket korsan ilan panoları ve

forumlarda çok sayıda vardır. En popüler korsan ilan tahtası “2600” tartışması grubudur. genellikle

çeşitli sistemlere ilişkin Dünya değişimi güvenlik bilgisi yerinden ve Hackerlar belirli programlara ilişkin

kuruluşlar veya korsan teknikleri ile ilgili güvenlik hassas bilgileri yayımlamak.

Ağ yöneticisi kurumun veri güvenlik görevlisi düzenli kuruluşun sistem ortamına ile ilgili

olabilecek yeni teknikler ve bilgiler tespit etmek korsan bülten panoları gözden emin olmalıdır.

**İnternet Yazılım.**

İnternet, bilgisayar kaynakları güvence veri güvenliği görevlileri ve yöneticileri yardımcı olabilir

SATAN, POLİSLER ve ISS gibi yararlı araçlar, çok sayıda sunar. Bu araçlar güvenlik risklerini tespit

etmek, kurumsal sistemlerini tarayın. Ancak, bu araçlar da korsanlara mevcuttur ve sistemleri nüfuz onlara yardımcı olabilir.

Olası güvenlik sorunlarını belirlemek ve gidermek için, ağ yöneticisi temin etmelidir:

Her güvenlik programının son sürümü elde edilmiş ve düzenli bir şekilde yürütülmektedir. Her

tespit poz derhal çözülmelidir.

Sistem veri güvenlik görevlisi ve bağımsız dış danışmanları ikisi tarafından düzenli güvenlik

denetimleri tabidir.

**Sonuç**

Hacker aktivite işletmelerin internete kendi iç kurumsal ağlarını bağlamak artmaya devam edecek

gerçek ve sürekli tehdit oluşturuyor. Bu makale, bilgisayar kaynaklarına erişmek için yetkisiz kişilerin

en sık görülen korsan teknikleri anlatmıştır. kendini kesmek denetim algılanır ve zamanında

çözülmediği takdirde, hackerlar kurumsal sistemine nüfuz edebilme izin verebilir, güvenlik zayıflıkları

tanımlamak için giderek kritik bir teknik haline geliyor. Sistem yöneticileri ve veri güvenlik görevlileri

düzenli bütün CERT yayınları ve hacker bülten panoları okuyarak son korsan teknikleri takip etmelidir.

**Yazar Biyografileri**

Stephen James

Stephen James UNIX ve İnternet güvenliği yanı sıra, hacker çalışmalarında uzmanlaşmış Avustralya'nın önde

bilgisayar güvenlik uzmanları biridir. O Price Waterhouse (Sidney) ile üst düzey bir danışman.

© 2004 CRC Press LLC tarafından