Istismar

İçerikler

Amaç

Bir penetrasyon testinin sömürü aşaması, yalnızca güvenlik kısıtlamalarını atlayarak bir sisteme veya kaynağa erişim sağlamaya odaklanır. Önceki aşama, güvenlik açığı analizi düzgün bir şekilde yapılırsa, bu aşama iyi planlı ve hassas bir grev olmalıdır. Ana odak noktası, kuruluşa ana giriş noktasını belirlemek ve yüksek değerli hedef varlıkları belirlemektir.

Güvenlik açığı analiz aşaması düzgün bir şekilde tamamlandıysa, yüksek değerli bir hedef listesine uyulmamış olmalıydı. Sonuçta, saldırı vektörü, organizasyon üzerindeki başarı olasılığını ve en yüksek etkisini dikkate almalıdır.

Karşı önlemler

Karşı önlemler, bir istismar yolunu başarıyla tamamlama yeteneğini engelleyen önleyici teknoloji veya kontroller olarak tanımlanır. Bu teknoloji, Host Bazlı İtici Engelleme Sistemi, Güvenlik Görevlisi, Web Uygulama Güvenlik Duvarı veya diğer önleyici yöntemler olabilir. Bir istismar gerçekleştirirken, çeşitli faktörler dikkate alınmalıdır. Önleyici bir teknoloji olması durumunda, bir atlatma tekniği düşünülmelidir. Bunun mümkün olmadığı durumlarda, alternatif istismar yöntemleri düşünülmelidir.

Genel olarak, argüman, alarmlar takılırsa, denklemin seviyesi azaltılabilirse, organizasyona saldırırken gizli kalmaktır. Mümkünse, istismarı tetiklemeden önce karşı önlemler alınmalıdır. Bu, saldırının kuru koşularını yaparak veya teknolojiyi sıralayarak yapılabilir.

Anti-Virüs

Anti-virüs, kötü amaçlı yazılımların sistemde konuşlandırılmasını önlemeyi amaçlayan bir teknolojidir. Bir penetrasyon testçisi olarak bu tür anti-virüs teknolojilerini tanımlayabilmeli ve bunlara karşı koruma sağlayabilmeliyiz. Anti-virüs, örneğin konak tabanlı saldırı önleme sistemleri, web uygulaması güvenlik duvarları ve diğer önleyici teknolojiler gibi mevcut olabilecek tüm farklı önleyici önlemlerin küçük bir alt kümesidir.

Kodlama

Kodlama, dağıtılan kod parçasını aynı görünmemesini sağlayacak şekilde verileri gizleme yöntemidir. Kodlama ile, karışıklık genellikle bilgiyi karıştırarak ve uygulamanın gerçekte ne yaptığını gizlemek için yeniden düzenleyerek ortaya çıkar.

Paketleme

Ambalaj, uygulamayı sıkıştırmak veya "paketlemek" için verileri yeniden düzenlemeye çalıştığı için kodlamaya benzer. Bunun umutları, teslim edilen idam edilebilir veya kod parçasının, anti-virüs teknolojileri tarafından alınmayacağı şekilde gizlenmesidir.

Şifreleme

Şifreleme, Kodlama ve Ambalaj gibi şifreleme, amaçlanan çalıştırılabilir kodu manipüle etmenin başka bir yöntemidir, böylece tanınabilir veya muayene için kullanılabilir değildir. Sadece bellek içi (paketlemeye benzer yöntemlerle) şifresini çözdükten sonra gerçek kod ilk kez açığa çıkar - umarım güvenlik mekanizmaları izin verdikten ve şifre çözüldükten hemen sonra yürütülür.

Whitelist Bypass

Beyaz listeleme teknolojileri, bir seferde belirli bir sistemde görülen uygulamalar için güvenilir bir modelden yararlandı. Teknoloji, sistemin bir temelini alır ve yabancı bir şeye karşı sistemde çalıştırılmasının normal olanı tanımlar. Penettrasyon test cihazı beyaz liste teknolojilerini atlatabilmelidir. En yaygın yöntemlerden biri doğrudan hafıza erişiminden geçer. Whitelisting, hafızayı gerçek zamanlı olarak izleme kapasitesine sahip değildir ve bir hafıza sakini programı çalışırsa ve diske dokunmuyorsa, verilen teknoloji tarafından tespit edilmeden çalışabilir.

Proses Enjeksiyonu

İşlem enjeksiyonu, zaten çalışan bir sürece enjekte edilmesi için bir yöntemdir. Bir sürece enjekte edilerek, uygulamanın bilgileri normalde doğada güvenilecek bir süreçte gizlenebilir. Önleyici ölçüm teknolojisinin çalışma süreçlerini denetlemesi çok zordur ve uygulamanın güvenilir bir süreç olduğunu düşüneceği farklı bir süreçte neredeyse her zaman saklanabilir.

Tamamen Hafıza Sakini

Hafıza yerleşik saldırıları genellikle en çok tercih edilendir, çünkü çoğu teknoloji hafızayı incelemez. Bir saldırgan olarak, hafızada yaşamanın bir yolunu bulmak tamamen arzu edilir olurdu. Diske yazarken, çoğu uygulama potansiyel olarak kötü amaçlı yazılım taramaları, temel çizgileri ve diğer kimliklerini gerçekleştirecektir. Diske yazarken tespit edilebilmesi önemli ölçüde daha da artar.

İnsan

Sömürü gerçekleştirirken, doğrudan bir istismardan veya bir uygulama kusurundan geçmek her zaman en iyi yol değildir. Bazen insan unsuru bir örgüte saldırmak için daha iyi bir yol olabilir. Doğru saldırı caddesini anlamak ve kaldırdığımız yöntemin alınması gereken en iyi yol olduğundan emin olmak önemlidir.

Veri Yürütme Önlemesi (DEP)

Sömürü gerçekleştirirken, birçok önleyici tedbirler birime oyuna girebilir. Veri Yürütme Önleme, çoğu işletim sistemine uygulanan bir savunma önlemidir ve bellekte bir yazın meydana geldiğinde yürütme iznini önler. DEP'in arkasındaki düşünce süreci, bir saldırganın hafızayı yeniden yazmasını durdurmak ve ardından bu kodu yürütmektir. Veri yürütme önlemeyi atlamak için çok sayıda yöntem vardır ve daha sonra PTES'in sömürü aşamasında tartışılır.

Adres Uzay Düzeni Randomizasyonu

Bir tampon taşma kırılganlığı sırasında (veya belleği kontrol ettiğimiz herhangi bir şey sırasında), bellek adresleri, shellcode'umuza yeniden yönlendirme uygulaması için sabitlenir. ASLR durumunda, bir saldırganın para kodu uygulamak için her zaman nereye gidebileceğini tahmin etmesini önlemek için belirli baytlar randomize edilir.

Web Uygulama Güvenlik Duvarı (WAF)

Web uygulaması güvenlik duvarları, web tabanlı uygulama saldırılarına karşı korunmak için bir uygulama ile çevrimiçi olarak oturan bir teknolojidir. Web uygulaması güvenlik duvarları, belirli bir web uygulamasına yönelik potansiyel olarak tehlikeli veya malformasyonları tanımlamaya ve bunları önlemeye çalışır. Web

uygulaması güvenlik duvarları için bir dizi bypass tekniği vardır ve penetrasyon testi sırasında test edilmelidir.

Kaçış

Kaçakçılık, bir penetrasyon testi sırasında tespitten kaçmak için kullanılan tekniktir. Bu, bir gardiyan tarafından görülmemek üzere bir kamera sistemini atlatmak, İHA Tevazılık Tespit Sistemleri (IDS) veya İHA'yı Önleme Sistemlerinden (IPS) kaçmak için yüklerinizi gizlemek veya web uygulaması güvenlik duvarlarını aşmak için talep / yanıtları kodlamak için yüklerinizi gizlemek olabilir. Genel olarak, bir teknolojiden veya kişiden kaçınmak için düşük riskli bir senaryo belirleme ihtiyacı, istismardan önce formüle edilmelidir.

Hassas Grev

Bir penetrasyon testinin ana odak noktası, örgüte karşı simüle edilmiş bir saldırıyı temsil etmek için bir saldırganı simüle etmektir. Bir penetrasyon testi yoluyla getirilen değer genellikle saldırıların doğada gürültülü olduğu ve her istismarı deneme girişiminde olduğu parçalama ve kapma teknikleri ile değildir. Bu yaklaşım, örgütün olay tepkisi seviyesini ölçmek için bir penetrasyon testinin sonunda özellikle yararlı olabilir, ancak çoğu durumda sömürü aşaması, hedefle ilgili belirli bir araştırma birikimidir.

Özelleştirilmiş Sömürü Bulvarı

Her saldırı genellikle sömürü yolunun nasıl gerçekleştiğinde aynı olmayacaktır. Bu aşamada başarılı olmak için saldırı senaryoya göre uyarlanmış ve özelleştirilmiş olmalıdır. Örneğin, bir kablosuz penetrasyon testi yapıldıysa ve belirli bir teknoloji kullanılıyorsa, bunların hangi teknolojilerin bulunduğuna göre tanımlanması ve saldırıya uğraması gerekir. Her bir senaryoyu net bir şekilde anlamak ve bir istismarın uygulanabilirliği, penetrasyon testinin bu aşamasının en önemli yönlerinden biridir.

Özel Sömürüler

Birkaç kez internette halka açık olan istismarlar, başarılı bir şekilde tamamlamak için bazı çalışmalara ihtiyaç duyabilir. Çoğu durumda, bir istismar Windows XP SP2 için tasarlanmışsa, saldırının Windows XP SP3 aracılığıyla başarılı olabilmesi için istismarda özel değişiklikler gerekecektir. Penetrum test cihazı, saldırıyı başarılı bir şekilde tamamlamak için bir istismarı ve anında değişme yeteneğini özelleştirebilecek bilgiye sahip olmalıdır.

Özelleştirmeyi ömürü

Bir saldırı durumunda, sömürü aşamasının başarılı olmasını sağlamak için mağdurların altyapısını simüle etmek genellikle gereklidir. Bilgi toplama aşamasında kaldıraçlanan teknikler her zaman yardımcı olabilir, ancak çalışan bir altyapıya ve sistemlerin yerinde olması, tedarik aşamasını çok daha kolay hale getirecektir. Özel bir istismar durumunda, penetrasyon test cihazı, bir sisteme başarılı bir şekilde saldırmak için zaten kamu istismarlarını özelleştirebilmelidir. Sömürüler için ortak bir tema, işletim sistemlerinin veya uygulamalarının belirli sürümlerini hedeflemektir. Bunun nedeni, hizmet paketlerine ve / veya işletim sisteminin yeni sürümlerine dayalı bellek adreslerinin değişmesidir. Test cihazı, farklı işletim sistemlerine başarılı bir şekilde konuşlandırmak ve sistemi başarıyla tehlikeye atmak için bu istismarları özelleştirebilmelidir.

Sıfır Gün Açısı

Çoğu durumda, sıfır günlük açı genellikle çoğu penetrasyon test cihazı için son çaredir. Bu tür bir saldırı genellikle normal saldırı yöntemleriyle örgüte karşı odaklanmış bir saldırıyı ele alabilecek son derece gelişmiş bir organizasyonu temsil eder. Bazı senaryolarda, keşfedilmemiş güvenlik açıklarının mühendisliğini tersine çevirmek, fuzz veya gelişmiş keşif yapmak için araştırmalar yapılabilir. Bu tür bir saldırının uygulanabilir olması durumunda, saldırganların en iyisine çevrenin karşı önlem teknolojisini içerecek şekilde yeniden üretildiğinden emin olun.

Sıfır günlük istismarların başarılı olabilmesi (veya bu konuda herhangi bir istismar) ve aynı işletim sistemine, yamalara ve karşı önlemlere sahip olmak başarı konusunda oldukça önemlidir. Bazen bu bilgiler, meydana gelen erişim veya sayım düzeyine bağlı olarak mevcut olmayabilir.

Bulanıklık

Bulmaca, bir protokolü veya uygulamayı yeniden oluşturma ve bir güvenlik açığının tanımlanması umuduyla uygulamaya veri göndermeye çalışma yeteneğidir. Çoğu zaman bir fuzzer umutları, bir uygulamadaki bir kazayı tanımlamak ve ondan belirli bir istismar oluşturmaktır. Bulma durumunda, saldırgan daha önce keşfedilmemiş bir şeyden belirli bir güvenlik açığı yaratmaya çalışıyor. Bir penetrasyon testinin bir parçası olarak, angajman sırasında herhangi bir yer tespit edilmezse veya angajman sıfır günlük araştırma için çağrıda bulunur; potansiyel olarak savunmasız maruziyetleri tanımlamak için bulanıklama teknikleri kaldırılmalıdır.

Kaynak Kodu Analizi

Bir penetrasyon test cihazının mevcut olduğu diğer yollar, kaynak kodunun mevcut olması veya açık kaynaklı olmasıdır. Test cihazı kaynak koduna bakma ve uygulama içindeki kusurları belirleme yeteneğine sahipse, bu yöntemlerle sıfır günlük maruz kalmalar da tanımlanabilir.

İtici Uçurum Çeşitleri

Bir penetrasyon testi sırasında sıfır gün olarak sınıflandırılabilecek birkaç istismar türü vardır. Bazıları bu bölümde listelenmiştir.

Tampon Taşıyor

Tampon taşmaları, uygunsuz kodlama teknikleri nedeniyle ortaya çıkar. Spesifik olarak, bu genellikle bir program bir tampona veri yazdığında ve daha sonra tamponun sınırını aştığı ve hafızanın bazı bölümlerini yazmaya başladığında ortaya çıkar. Tampon taşması istismarlarında saldırganların hedefi bir çarpışmayı kontrol etmek ve verilen sistemde kod uygulaması kazanmaktır. Bir tampon taşma istismarında, daha yaygın olanlardan biri, belirli bir kaydın üzerine yazmak ve kabuk koduna "atlamak"tır.

SEH Üstesinden Yazıyor

SEH'nin üzerindeki yazılar, yapılandırılmış istisna işleyicinin bir uygulamayı zarif bir şekilde kapatmaya başlamasıyla ortaya çıkar. Saldırgan, SEH'nin nasıl çalıştığını manipüle edebilir, SEH işleyicisinin temel adresini yazabilir ve SEH'den yürütme akışının kontrolünü ele geçirebilir. Bu, tampon taşma kırılganlığı ve SEH ile uyumlu uygulamalarla çalışan yaygın bir saldırıdır.

Dönüş Yönlü Programlama

Return Oriented Programming (ROP), kullanıcının yürütme akışının kontrolünü ele geçirdiği bir kısımda kullanılan bir tekniktir, ancak veri yürütme önleme (DEP) veya diğer önleyici savunma mekanizmaları yerinde olabilir. DEP'in etkinleştirildiği durumda, saldırganın belirli montaj talimatlarını yerine getirmek için doğrudan erişimi yoktur, böylece saldırgan, DER'yi devre dışı bırakmak veya DEP'yi devre dışı bırakmak için belirli Windows API aramaları veya teknikleri hazırlamak için ROP cihazı inşa eder. Yaygın bir yöntem, yazı İşlemcilik Çağrısını, yığından gelen verileri daha sonra yürütülebilecek yazılı bir hafıza alanına kopyalamaktır.

Trafik Analizi

Trafik analizi, ne tür bilgilerin gönderildiğini ve bu trafiği anlama ve manipüle etme yeteneğini belirleme tekniğidir. Bir penetrasyon test cihazı, bir protokolün nasıl çalıştığını ve bir saldırıdan yararlanmak için nasıl manipüle edilebileceğini anlamalıdır.

Fiziksel Erişim

Bir penetrasyon testi sırasında fiziksel erişim, fiziksel güvenlik kontrollerini aşmaya ve yetkisiz erişim sağlamaya çalışmak için uygun bir saldırı yöntemi olabilir. Bir penetrasyon testi sırasında, değerlendirici potansiyel olarak kusurlu fiziksel güvenlik kontrollerini tanımlayabilmeli ve kapsam dahilindeyse tesise erişmeye çalışabilmelidir.

İnsan Açısı

Fiziksel bir penetrasyon testi sırasında, en belirgin yollardan bazıları, tesise girme ve erişim elde etmek için sosyal mühendislik yapmak olacaktır. Bu, organizasyonun iş nasıl işlediği ve istihbarat toplama aşamasından öğrendiğiniz her şey hakkında önemli bir bilgi gerektirir.

PC Erişimi

Bir PC'ye fiziksel erişim verilirse, penetrasyon test cihazı PC'ye saldırabilir ve sisteme erişime izin verecek birden fazla yöntemle erişebilir.

Yakınlık Erişimi (WiFi)

Kablosuz iletişim, RF tipi iletişim yoluyla erişim sağlamak için saldırılar için bir yoldur. Penettrasyon test cihazı, hedefin kullanımda kayıtlı spektrum frekanslarına sahip olup olmadığını görmek için FCC radyo frekans listesini görüntülemelidir.

WiFi Saldırıları

Protokol ne olursa olsun, WEP, WPA2, EAP-FAST, EAP-LEAP ve diğer caddeler için bir dizi saldırı vardır. Saldırgan, çeşitli şifreleme protokollerine ve standartlarına aşina olmalı ve uygulamaya konulan kontroller etrafındaki uygulamayı etkili bir şekilde test edebilmelidir.

Kullanıcıya Saldırmak

Kurbana saldırmak için haydut erişim noktalarından yararlanmak genellikle faydalı ve uygun bir saldırı yöntemidir. Sömürülerden yararlanmak veya hassas bilgileri çalmak için mağdurları ikna etmek için haydut bir erişim noktasından yararlanmak, kablosuz bir değerlendirme sırasında yapılmalıdır. Bunun kullanımında

birkaç yaygın teknik vardır, ancak en yaygın olarak saldırgan, kurbanın bağlanması için aynı adı taşıyan bir kablosuz erişim noktası veya cazip bir isim kuracaktır.

Kategori: Saldırının Örnek Bulvarları

Her bir senaryoda, saldırılar angajmanın kapsamı içindeki senaryoya dayanmalıdır. Aşağıda, senaryoya dayanarak dikkate alınması gereken birkaç saldırı yolunun bir listesi bulunmaktadır, ancak hiçbir şekilde kapsamlı bir liste değildir.

Web Uygulama Saldırıları Sosyal-mühendislik Fiziksel Saldırı Caddeleri Hafızaya Dayalı İspatlar (yani tampon / yığın taşmalar, bellek yolsuzlar, kullanım süresi dışında). Adam içinde orta VLAN Hopping USB / Flash Drive Dağıtımı Ters Mühendislik Sıfır Gün Açısı Kullanıcıya saldırmak Şifreleme Çatlağı Grafik İşleme Birimi (GPU) Çatlama Trafik Analizi Ateş telleri Protokolleri Yönlendirme Pretexting ile kimlik avı Çalışan Takliti

Yine bu örnekler, organizasyon için gerçekleştirdiğiniz senaryoya dayanarak sadece saldırı için temel yollardır. Bir penetrasyon testinden elde edilen değer, yaratıcılıktan ve maruz kalmaları tanımlama ve onları kesin bir şekilde kullanma yeteneğinden gelir.

Genel Amaç

Müşteri ile etkileşim öncesi etkileşim aşamasında, penetrasyon testinin genel hedeflerinin net bir tanımı iletilmeliydi. Sömürü aşaması durumunda, en büyük zorluk, tespit edilmeden organizasyona en az direnç yolunu belirlemek ve kuruluşların gelir elde etme yeteneği üzerinde en fazla etkiye sahip olmaktır.

Önceki aşamaları düzgün bir şekilde gerçekleştirerek, kuruluşun nasıl çalıştığına ve para kazandığının net bir şekilde anlaşılması nispeten anlaşılmalıdır. Sömürü aşamasından ve patlama sonrası aşamaya kadar, saldırı vektörleri, örgütün örgüte karşı hedefli bir saldırı yoluyla nasıl önemli kayıplar alabileceğini temsil etmek için yalnızca güvenlik kontrollerini aşma misyonuna güvenmelidir.
