Güvenlik Açığı Analizi

İçerikler

Test

Güvenlik açığı testi, bir saldırgan tarafından kaldırılabilen sistemlerdeki ve uygulamalardaki kusurları keşfetme işlemidir. Bu kusurlar, ana bilgisayar ve hizmet yanlış yapılandırma veya güvensiz uygulama tasarımından herhangi bir yerde değişebilir. Kusurları aramak için kullanılan süreç değişse ve test edilen belirli bileşene büyük ölçüde bağımlı olsa da, bazı anahtar ilkeler süreç için geçerlidir.

Herhangi bir türde güvenlik açığı analizi yaparken, test cihazı istenen sonucun hedeflerini ve / veya gereksinimlerini karşılamak için geçerli derinlik ve genişlik için testi uygun şekilde ele almalıdır. Derinlik değerleri, bir değerlendirme aracının konumu, kimlik doğrulama gereksinimleri vb. Gibi şeyleri içerebilir. Örneğin; bazı durumlarda, belki de hafifletmeyi doğrulamak için testin amacı yerindedir ve çalışır ve güvenlik açığına erişilebilir değildir; diğer durumlarda, geçerli tüm güvenlik açıklarını keşfetmek için kimlikli erişime sahip uygulanabilir her değişkeni test etme hedefi olabilir. Kapsamınız ne olursa olsun, test hedeflerinize ulaşmak için derinlik gereksinimlerini karşılamak için uyarlanmalıdır. Testin derinliği, değerlendirme sonuçlarının beklentiyi karşıladığından emin olmak için her zaman doğrulanmalıdır (yani tüm makineleri kimlik doğrulaması vb.). Derinliğe ek olarak, güvenlik açığı testi yaparken de genişlik göz önünde bulundurulmalıdır. Breadth değerleri hedef ağlar, segmentler, ev sahipleri, uygulama, envanter vb. Gibi şeyleri içerebilir. En basit haliyle, testiniz bir konak sistemindeki tüm güvenlik açıklarını bulmak olabilir; Diğer durumlarda, belirli bir envanter veya sınırda bulunan ev sahipleri üzerindeki tüm güvenlik açıklarını bulmanız gerekebilir. Ayrıca test kapsamınızı karşıladığınızdan emin olmak için testin genişliği her zaman doğrulanmalıdır (yani, envanterdeki her makine tarama sırasında canlı mıydı? Değilse, neden).

Aktif

Aktif testler, güvenlik açığı için test edilen bileşenle doğrudan etkileşimi içerir. Bu, bir ağ aygıtındaki TCP yığını gibi düşük seviyeli bileşenler olabilir veya böyle bir cihazı yönetmek için kullanılan web tabanlı arayüz gibi yığının üzerinde daha yüksek bileşenler olabilir. Hedef bileşenle etkileşim kurmanın iki farklı yolu vardır: otomatik ve manuel.

Otomatik

Otomatik test, bir hedefle etkileşim kurmak, yanıtları incelemek ve bu yanıtlara dayanarak bir güvenlik açığının var olup olmadığını belirlemek için yazılım kullanır. Otomatik bir süreç, zaman ve işçilik gereksinimlerini azaltmaya yardımcı olabilir. Örneğin, gelen verileri almaya açık olup olmadığını belirlemek için bir sistemdeki tek bir TCP bağlantı noktasına bağlanması kolay olsa da, bu adımı mevcut 65.535 olası bağlantı noktasının her biri için bir kez gerçekleştirmek, manuel olarak yapılırsa önemli miktarda zaman

gerektirir. Böyle bir testin birden fazla ağ adresinde tekrarlanması gerektiğinde, gereken süre, bir tür otomasyon olmadan testin tamamlanmasına izin vermek için çok büyük olabilir. Bu işlevleri yerine getirmek için yazılım kullanmak, test cihazının eldeki görevi yerine getirmesini sağlar ve dikkatlerini verileri işleme ve manuel teste daha uygun görevleri yerine getirmeye odaklar.

Ağ / Genel Güvenlik Açığı Tarayıcılar

Liman Bazlı

Otomatik bağlantı noktasına dayalı bir tarama genellikle geleneksel bir penetrasyon testindeki ilk adımlardan biridir, çünkü hedef ağda veya konakta neler bulunabileceğine dair temel bir genel bakış elde etmeye yardımcı olur. Liman tabanlı tarayıcılar, uzak bir konaktaki bir bağlantı kutusuna sahip olup olmadığını belirlemek için kontrol eder. Genel olarak, bu IP'yi (TCP, UDP, ICMP vb.) kullanan protokolleri içerecektir, Bununla birlikte, diğer ağ protokollerindeki bağlantı noktaları çevreye bağlı olarak da bulunabilir (örneğin, SNA'nın kullanımda olması için büyük ana bilgisayar ortamlarında oldukça yaygındır). Tipik olarak, bir liman iki olası durumdan birine sahip olabilir:

```
    Açık - liman veri alabiliyor
    Kapalı - liman veri alamıyor
```

Bir tarayıcı, belirli bir portun açık veya kapalı olup olmadığını doğru bir şekilde belirleyemiyorsa, “filtreli” gibi diğer durumları listeleyebilir.

Tarayıcı, bir bağlantı noktasının açık olduğunu belirlediğinde, tarayıcı tarafından bir güvenlik açığının mevcut olup olmadığı konusunda bir varsayım yapılır. Örneğin, bir bağlantı noktasına dayalı bir tarayıcı TCP bağlantı noktası 23'e bağlanıyorsa ve bu bağlantı noktası dinliyorsa, tarayıcının telnet hizmetinin uzak ana bilgisayarda mevcut olduğunu bildirmesi ve net bir metin kimlik doğrulama protokolü etkin olarak işaretlemesi muhtemeldir.

Hizmet Tabanlı

Hizmet tabanlı bir güvenlik açığı tarayıcısı, uzak bir konakta açık bağlantı noktalarıyla iletişim kurmak için belirli protokolleri kullanan bir araçtır. Bu, bir liman taramasından daha kesindir, çünkü hangi hizmetin çalıştığını belirlemek için yalnızca limana güvenmez. Örneğin, bir bağlantı noktası 8000'in bir konakçıda açık olduğunu tespit edebilir, ancak bu bilgilere dayanarak hangi hizmetin orada çalıştığını tam olarak bilemez. Bir servis tarayıcısı, farklı protokoller kullanarak bağlantı noktasıyla iletişim kurmaya çalışacaktır. 8000 numaralı bağlantı noktasında çalışan hizmet HTTP kullanarak doğru iletişim kurabilirse, web sunucusu olarak tanımlanacaktır.

Banner Kapma

Banner kapma işlemi, belirli bir bağlantı noktasına bağlanma ve o limana bağlı hizmeti / başvuruyu tanımlamak için uzak konakçıdan iade edilen verileri inceleme işlemidir. Genellikle bağlantı sürecinde, yazılım, uygulamanın adı veya yazılımın hangi belirli sürümünün çalıştığına dair bilgileri içerebilecek bir kimlik etiketi sağlayacaktır.

Web Uygulama Tarayıcıları

Genel uygulama kusur tarayıcıları

Çoğu web uygulama taraması bir web sitesi, web uygulaması veya web hizmetinin adresi ile başlar. Tarayıcı daha sonra bağlantıları ve dizin yapılarını takip ederek siteyi sürüner. Bir web sayfaları, kaynaklar, hizmetler ve / veya sunulan diğer medyaların bir listesini derledikten sonra, tarayıcı tarama sonuçlarına karşı testler veya denetimler gerçekleştirecektir. Örneğin, taramada keşfedilen bir web sayfası form alanları varsa, tarayıcı

SQL enjeksiyonu veya siteler arası komut dosyası deneyebilir. Sürünen sayfa hatalar içeriyorsa, tarayıcı hata ayrıntısında görüntülenen hassas bilgileri arayabilir ve benzeri olabilir.

Çürme ve test aşamalarının genel tarama süresini azaltmak için aynı zamanda kademeli olarak yapılabileceği ve gerçekleştirilebileceği belirtilmelidir. Bu, birçok web uygulama tarayıcısı için varsayılan davranıştır.

Dizin Listesi / Kırık Zorlama

Web sitesinde, tarayıcının bağlantıları takip ederek bulamayacağı dizinler olduğunu varsayalım. Kullanıcı tarafından sağlanan bu dizinler hakkında önceden bilgi sahibi olmadan, tarayıcının en az iki ek seçeneği vardır.

Tarayıcı/crawler "ortak" dizinleri arayabilir. Bunlar, yaygın olarak bulunan isimlerin isimleri ve varyantları olan dizinlerdir ve yıllarca süren deneyim ve tarama sonucunda derlenen bir listeye dahil edilir. Çoğu web uygulaması bu tür bir "yerleşik" listesine sahipken, bazı penetrasyon test cihazları kendi özel listelerini korur. Bazen dizin adları, 3rd parti web uygulamasını makul derecede yüksek doğrulukla tanımlamak için kullanılabilecek kadar benzersizdir. Doğru bir dizin listesi genellikle bir web sitesinin "idari" bölümünü bulmanın anahtarı olabilir - çoğu penetrasyon test cihazının keşfedilmekle son derece ilgilenmesi gereken bir bölüm.

Brute zorlama dizinleri benzer bir yaklaşımdır, ancak statik bir liste kullanmak yerine, bir dizin adının sahip olabileceği her olasılığı belirlemek için bir araç kullanılır. Bu yaklaşımı kullanmanın dezavantajı, web sunucusunu isteklerle çökertme veya susuz kalma potansiyeline sahip olması ve böylece hizmet reddi durumuna neden olmasıdır. Birisi, özellikle bir üretim ayarında, web sunucusunun durumunu yakından takip ederken, dizin kaba kuvvetlendirmeyi gerçekleştirmek için özen gösterilmelidir.

Penetrum test cihazı olarak dizin listeleme yapmak istemenizin nedeni, saldırı alanınızı genişletmek veya hassas bilgiler içerebilecek dizinleri bulmaktır (penettrasyon testinin hedefine bağlı olarak, içinde büyük bir bulguya yol açabilir).

Web Sunucusu Sürümü / Güvenlik Açığı Tanımlama

Birçok web uygulama tarayıcısı, web sunucusunun sürümünü güvenlik tavsiyelerinde bilinen savunmasız sürümlerle karşılaştırmaya çalışacaktır. Bu yaklaşım bazen yanlış pozitiflere yol açabilir; açık kaynaklı web sunucularının çatallandığı veya kopyalandığı ve yeni isimler, afişler verildiği ve farklı sürüm numaraları atandığı bazı durumlar vardır. Web sunucusunun aslında afişin veya web tarayıcı raporlarını çalıştırdığını doğrulamak için ek adımlar atılmalıdır.

Yöntem

Birkaç web sunucusu yöntemi güvensiz olarak kabul edilir ve saldırganların web sunucusu içeriğine farklı erişim seviyeleri kazanmalarını sağlayabilir. Bu yöntemlerin web sunucusu yazılımının bir parçası olması ve web sitesi içeriğinin olmaması, şimdiye kadar tartışılan diğer güvenlik açıklarından ayırt eder. Bazı güvensiz yöntemler şunları içerir:

SEÇENEKLER

HTTP OPTIONS yöntemi kendi başına güvensiz olmasa da, bir saldırganın hedef sunucu tarafından kabul edilen HTTP yöntemlerinin türlerini kolayca numaralandırmasına izin verebilir. Not, OPTIONS yöntemi her zaman doğru değildir ve aşağıdaki yöntemlerin her biri bireysel olarak doğrulanmalıdır.

KORUMA/DELETE

PUT yöntemini kullanarak, bir saldırgan bilgi aktarmak, web içeriğini değiştirmek veya web sunucusuna kötü amaçlı yazılım yüklemek için kullanılabilecek HTML sayfaları gibi kötü amaçlı içerik yükleyebilir.

DELETE yöntemini kullanarak bir saldırgan, bir kişinin ihlalini kaldırabilir veya hizmetin bozulmasına neden olan bir siteyi bozabilir.

Ek olarak, modern REST uygulamaları PUT'u farklı bir şekilde kullanır:

Create->POST Okuma->GET Güncelleme->PUT Silin->DİLGİLİN

WebDAV

WebDAV, Microsoft Internet Information Server'ın (IIS) bir bileşenidir. WebDAV, "Web tabanlı Dağıtılmış Yazarlık ve Sürümleme" anlamına gelir ve düzenleme ve dosya yönetimi için kullanılır. WebDAV uzantıları, IIS Web sunucularında Web içeriğini uzaktan yönetmek ve düzenlemek için yöneticiler tarafından kullanılır ve PROPFID, COPY, MOVE, PROPPATCH, MKCOL, LOCK ve UN LOCK içerebilir. WebDAV, bir sistemi birkaç olası güvenlik açığına maruz bırakabilen çekirdek işletim sistemi bileşenleri ile etkileşime girer. Bu potansiyel risklerden bazıları şunlardır:

```
    Kullanıcı isteklerinin uygunsuz kullanımı nedeniyle tampon taşma koşulları
    Kötü biçimlendirilmiş taleplerden hizmet dışı bırakma koşulları
    Alan tabanlı komut dosyası saldırıları
    Ayrıcalık tırmanışı
    keyfi kodların yürütülmesi
```

İSIM/TRAK

Modern web sunucuları, yetkisiz bilgi açıklamasına yol açabilecek bir kusur içeren TRACE HTTP yöntemini destekler. TRACE yöntemi, web sunucu bağlantılarını hata ayıklamak için kullanılır ve istemcinin istek zincirinin diğer ucunda nelerin alındığını görmesine izin verebilir. Tüm büyük web sunucularında varsayılan olarak etkinleştirilen uzak bir saldırgan, gizlilik kaybına neden olan hassas bilgileri ifşa etmek için HTTP TRACE işlevselliğini kötüye kullanabilir.

Ağ Güvenlik Açığı Tarayıcılar / Özel Protokoller

VPN

Geleneksel güvenlik açığı değerlendirme araçları, İnternet Anahtar Değişimine (IKE) hizmet veren VPN cihazlarıyla doğru protokol görüşmelerini gerçekleştiremez. IKE'nin kullanımda olduğu durumlarda, doğru parmak izi, geri alma kalıpları geri alma ve kullanımda olan kimlik doğrulama mekanizmalarını tanımlama gibi işlevleri yerine getirebilen ek araç setleri kullanmak gerekecektir. Bir VPN cihazının bu özelliklerini belirleyerek, iletken kod sürümlerinin yanı sıra statik önceden paylaşılan tuşlar gibi kimlik doğrulama türlerinde zayıflıklar tanımlanabilir.

Sesli Ağ Tarayıcıları

Savaş Tecrit

Birçok kuruluş hala telefon hatları üzerinden bant erişiminden yararlanmaktadır. Savaş-sözleşmeyi yürütmek için tasarlanmış güvenlik açığı değerlendirme araçlarını kullanmak, kimlik doğrulama ve ağ mimarisindeki zayıflıkları belirleyebilir.

VoIP

IP üzerine ses teknolojileri artık çoğu kuruluşta bol miktarda bulunur. VoIP altyapılarının güvenlik açığı analizini yapmak için birçok araç geliştirilmiştir. Bu araçları kullanarak, VoIP ağlarının düzgün bir şekilde bölümlenip segmente edilmediğini ve bu ağlardan çekirdek altyapı sistemlerine erişmek veya bir hedef ağdaki telefon konuşmalarını kaydetmek için kullanma potansiyellerinin varsayılarak tanımlanabilir.

Manuel Doğrudan Bağlantılar

Herhangi bir otomatik süreç veya teknolojide olduğu gibi, hata payı her zaman vardır. Sistemlerdeki, ağ cihazlarındaki ve ağ bağlantısındaki açıklar, test sırasında yanlış sonuçlar verebilir. Otomatik testin sonuçlarını doğrulamak ve tüm potansiyel saldırı vektörlerini ve daha önce tanımlanamayan zayıflıkları belirlemek için bir hedef sistemde bulunan her protokole veya hizmete manuel doğrudan bağlantıların yürütülmesi her zaman önerilir.

Kafası tıkanıklığı

Birden Fazla Çıkış Düğüm

Güvenlik izleme ve savunma sistemleri, belirli bir IP adresinden kötü niyetli faaliyetin tanımlanması bahanesiyle çalışır. İntution Tespit sistemlerinin konuşlandırıldığı ve faaliyeti izlediği durumlarda, birden fazla IP adresinden kaynak değerlendirmesi ve saldırı faaliyetlerinin daha doğru sonuçlar vermesi ve bir hedef ağdaki izleme cihazının tanımlanması ve yanıt verme fırsatını azaltması. TOR proxyleri gibi teknolojiler, tek bir IP adresinden kaynaklanmadan değerlendirme faaliyetleri yürütmek için bir araç sağlayabilir.

IDS Kaçış

IDS teknolojilerinin konuşlandırıldığı hedef ortama karşı değerlendirme faaliyetleri yürütürken, kaçınma yapmak gerekebilir. İskeleme manipülasyonu, polimorfizm, oturum eklemesi ve parçalanma gibi yöntemleri kullanarak, IDS cihazlarında uygulanan imza eşleştirme kalıplarını atlarken daha doğru sonuçlar sağlayabilir.

Pasif

Meta Veri Analizi

Meta veri analizi, dosya verilerinin kendisinin aksine, bir dosyayı tanımlayan verilere bakmayı içerir. Örneğin, bir Microsoft Office belgesi, belgenin en son kaydedildiği zaman, belgenin ne zaman oluşturulduğunda belgeyi, şirketi listeleyebilir. Birçok belge, özel meta verilerin girişine bile izin verir. Bu, potansiyel olarak dahili adresler ve sunuculara giden yollar, dahili IP adresleri ve bir penetrasyon test cihazının ek erişim veya bilgi elde etmek için kullanabileceği diğer bilgileri içerebilir.

Meta veriler, bir şirketin iç ağında bulunan belgelerde oldukça yaygın olsa da, şirketler belgeleri halka veya halka açık İnternet'te sunmadan önce meta verileri temizlemeye özen göstermelidir. Bu nedenle, bir saldırganın pasif olarak erişebileceği herhangi bir meta veri, (hedefe doğrudan saldırmadan) bir güvenlik sorunu olarak kabul edilmelidir.

Trafik İzleme

Trafik izleme, bir iç ağa bağlanma ve çevrimdışı analiz için verileri yakalama kavramıdır. Rota zehirlenmesi, bular ağda "gürültü" oluşturduğu ve kolayca tespit edilebildiği için bu aşamadan hariç tutulur. "Kayıtlı" bir ağdan ne kadar hassas verilerin toplanabileceği genellikle şaşırtıcıdır. Anahtarlanmış bir ağa bu "verilerin sızdırılması" aşağıdaki gibi kategorize edilebilir:

ARP / MAC önbellek taşması, anahtarlı paketlerin yayınlanmasına neden olur - bu, uygun olmayan ARP / MAC önbellek zamanlama konfigürasyonlarına sahip Cisco anahtarlarında yaygındır.

Etherleak - bazı eski ağ sürücüleri ve bazı gömülü sürücüler, ARP paketlerini doldurmak için sistem belleğinden veri kullanacak. Yeterli ARP paketi toplanabilirse, iç bellekten hassas bilgiler yakalanabilir

Yanlış yapılandırılmış kümeler veya yük dengeleyiciler

Hubslar ağa takıldı Bu kategorilerin bazılarının yalnızca tek bir alt ağa veri sızıntısına neden olduğunu, diğerlerinin ise çok daha büyük ağ segmentlerine sızmaya neden olabileceğini unutmayın.

Doğrulama

Araçlar Arasındaki Korelasyon

Birden fazla araçla çalışırken, bulguların korelasyonuna duyulan ihtiyaç karmaşık hale gelebilir. Korelasyon, öğelerin belirli ve kategorik korelasyonu olan iki farklı stile ayrılabilir, her ikisi de belirli bir hedef üzerinde toplamaya çalıştığınız bilgi, metrik ve istatistik türüne göre yararlıdır.

Spesifik korelasyon, güvenlik açığı kimliği, CVE, OSVDB, satıcı indeksleme sayıları, bir yazılım ürünü ile bilinen sorun vb. gibi belirli bir tanımlanabilir sorunla ilgilidir ve ana bilgisayar adı, IP, FQDN, MAC Adresi vb. Bunun bir örneği, aynı sorunu birden fazla araçta endeksleyecekleri için CVE numarasına göre bulguların geliştirilmesi olacaktır.

Kategorik korelasyon, uyum çerçevelerinde olduğu gibi konular için kategorik bir yapı ile ilgilidir (yani. NIST SP 800-53, DOD 5300 Serisi, PCI, HIPPA, OWASP Listesi vb.) Kırılganlık türleri, yapılandırma sorunları vb. Gibi makro faktörlere göre ürün gruplandırmanıza izin verir. Bunun bir örneği, varsayılan şifreleri olan ev sahipleri için tüm bulguları NIST 800-53 (IA-5) içinde şifre karmaşıklığı için bir gruba ayırmak olacaktır.

Çoğu durumda, penetrasyon test cihazları, aynı konaktaki birden fazla araç arasında fazlalık içinde bulunan belirli güvenlik açıklarının mikro sorunlarına odaklanacaktır. Bu fazlalık, test çıktısındaki istatistiksel sonuçları çarpıtabilir ve yanlış bir artan risk profiline yol açabilir.

Bunun tersi, makro korelasyonda (yani en iyi 10/20 listelerinde) aşırı bir azalma veya basitleştirme ile ilgilidir, çünkü sonuçlar yanlış bir azaltılmış risk profili ile sonuçlanan çıktıyı çarpıtabilir.

Manuel Test / Protokol Spesifik

VPN

Parmak izi

Parmak izi, VPN cihazının türünü ve serbest bırakılan kodun doğru sürümünü belirlemek için yararlıdır. Cihazın parmak izini doğru bir şekilde parmak izi alarak, uygun araştırma ve analiz daha sonra hedef sisteme karşı yapılabilir.

Kimlik doğrulaması

VPN cihazları çeşitli kimlik doğrulama biçimleri ile çalışabilir. Geleneksel güvenlik açığı değerlendirme araçlarının bir parçası olmayan VPN araç setlerini kullanmak, kimlik doğrulama mekanizmalarının uygun şekilde tanımlanmasına ve önceden paylaşılan tuşlar veya varsayılan grup kimlikleri gibi var olabilecek zayıflıkları belirlemesine olanak tanır.

Kategori: Citrix

Sayım

Birçok varsayılan kurulum ve kötü yapılandırılmış Citrix cihazları, yayınlanan uygulamaları numaralandırmak ve cihaza doğrurayacak şekilde yapılandırılmış geçerli kullanıcı adlarını belirlemek için bir araç sağlar. Bu bilgi, kaba kuvvet saldırıları sırasında çok önemli hale gelir ve yetkili kullanıcılar için önceden tanımlanmış profillerden kurtulma girişimleri.

DNS

Alan Adı Sistemleri, bir saldırgana düzgün bir şekilde sertleşmediğinde bol miktarda bilgi sunabilir. Sürüm bilgileri uygun tanımlama ve doğru araştırma analizine izin verir. Bölge transferleri gibi zayıflıklar, saldırı için ek hedeflerin kapsamlı bir listesinin yanı sıra hedef kuruluşla ilgili potansiyel olarak hassas verilerin bilgi sızıntısını da sağlar.

Web

Web hizmetleri bir saldırgan için büyük bir manzara sağlar. Diğer protokollerin ve hizmetlerin çoğundan farklı olarak, web hizmetleri genellikle tek bir sistemin birden fazla limanında çalışır. Yöneticiler, sertleşmelerini web hizmetleri veya yayınlanmış dizinler için ortak limanlara odaklayabilir ve ek nitelikleri düzgün bir şekilde sertleştirmeyi ihmal edebilirler. Web hizmetleri her zaman manuel bir şekilde gözden geçirilmelidir, çünkü otomatik değerlendirme araçları hizmetlerindeki en zayıflıkları tanımlayamaz.

Posta

Posta sunucuları bir hedef kuruluş hakkında çok sayıda bilgi sağlayabilir. Hedef cihazdaki doğal işlevleri kullanarak, geçerli hesapların onaylanması ve diğer sistemlere ek saldırılar için potansiyel kullanıcı adlarının bir listesinin geliştirilmesi. Posta röleleme gibi güvenlik açıkları, kimlik avı gibi organizasyona ek saldırılar için kaldıraçlanabilir. Genellikle, posta sunucuları, kaba kuvvet kampanyalarında hedeflenebilecek uzaktan erişim için bir web arayüzü sağlayacaktır.

Saldırı Bulvarları

Saldırı ağaçlarının oluşturulması

Bir güvenlik değerlendirmesi sırasında, angajman boyunca test ilerledikçe bir saldırı ağacı geliştirmek için nihai raporun doğruluğu için çok önemlidir. Yeni sistemler, hizmetler ve potansiyel güvenlik açıkları tespit edildiğinden; bir saldırı ağacı geliştirilmeli ve düzenli olarak güncellenmelidir. Bu, özellikle katılımın sömürü aşamalarında önemlidir, çünkü gerçekleşen bir giriş noktası, saldırı ağacının gelişimi sırasında haritalandırılan diğer vektörler arasında tekrarlanabilir.

İzole Laboratuar Testi

Güvenlik açığı analizinin ve sömürüsünün doğruluğu, çoğaltılan ortamlar izole bir laboratuvarda kurulduğunda önemli ölçüde daha yüksektir. Çoğu zaman, sistemler belirli kontrol setleri veya ek koruma mekanizmaları ile sertleştirilebilir. Danışman, hedef organizasyonunu taklit eden bir laboratuvar tasarlayarak, istenen hedeflere karşı tespit edilen ve istismar edilen güvenlik açıklarının güvenilir olmasını sağlayabilir ve yanlış sonuçlar veya sistem çalışmamazlık fırsatını azaltabilir.

Görsel Onay

İnceleme ile Manuel Bağlantı

Uygun korelasyon yanlış bulguları azaltmaya ve genel doğruluğu artırmaya yardımcı olabilirken, bir hedef sistemi görsel olarak incelemenin yerini almaz. Değerlendirme araçları, bir protokol / hizmet bağlantısının sonuçlarını veya yanıtı gözden geçirmek ve bilinen güvenlik açıklarının imzalarıyla karşılaştırılmak üzere tasarlanmıştır. Bununla birlikte, uygun olmayan portlardaki hizmetleri veya bir uygulamaya dahil edilebilecek

özel mantıkta tanımlamada araçlar her zaman doğru değildir. Bir hedef sistemi, mevcut hizmetleri ve bu hizmetler için işlevsellik sağlayan uygulamaları manuel olarak değerlendirerek, bir test cihazı uygun doğrulama ve güvenlik açığı tanımlamasının tamamlandığından emin olabilir.

Araştırma

Kamusal Araştırmalar

Bir hedef sistemde bir güvenlik açığı bildirildikten sonra, konunun tanımlanmasının doğruluğunu belirlemek ve penetrasyon testi kapsamında güvenlik açığının potansiyel istismar edilebilirliğini araştırmak gerekir. Çoğu durumda, güvenlik açığı, ticari veya açık kaynaklı bir yazılım paketinde bildirilen bir yazılım güvenlik açığı olacaktır ve diğer durumlarda güvenlik açığı bir iş sürecinde bir kusur veya yanlış yapılandırma veya varsayılan şifre kullanımı gibi yaygın bir idari hata olabilir.

Güvenlik Veritabanı Veritabanları

Güvenlik açığı veritabanları, otomatik bir araç tarafından bildirilen bir sorunu doğrulamak veya bir hedef uygulamanın güvenlik açığını manuel olarak incelemek için kullanılabilir. Çoğu araç, CVE veritabanındaki özet bilgilere ve diğer kaynaklara erişmek için kullanılabilecek belirli bir güvenlik açığı için CVE tanımlayıcısını kullanacaktır. CVE ayrıca, sorunu OSVDB ve Bugtraq gibi güvenlik açığı veritabanlarında veya istismar veritabanlarında ve çerçevelerde aramak için de kullanılabilir.

Bildirilen bir sorunun doğruluğunu doğrulamak için güvenlik açığı veritabanları kullanılmalıdır. Örneğin, bir Apache web sunucusu kusuru Windows'ta var olabilir, ancak otomatik bir tarayıcı tarafından dikkate alınmayabilecek Linux'ta değil.

Satıcı Danışmanları

Satıcı tarafından verilen güvenlik tavsiyeleri ve değişiklik günlükleri, herhangi bir otomatik araçla bildirilemeyen güvenlik açığı bilgilerine işaretçiler sağlayabilir. Birçok büyük yazılım satıcısı, bağımsız bir araştırmacının bir güvenlik açığının açıklanmasını koordine ettiği dahili olarak keşfedilen konular ve konular hakkında sınırlı ayrıntılar bildirmektedir. Araştırmacı, güvenlik açığının ayrıntılarına sessiz kalmayı seçerse, satıcı danışmanlığı genellikle mevcut tek veridir. Bu durumlarda, diğer araştırmacılar bağımsız olarak daha fazla ayrıntı keşfedebilir ve ayrıntıları güvenlik açığı veritabanlarına ekleyebilirler. Bir satıcı danışmanlığında kullanılan CVE'yi aramak, potansiyel olarak sömürülebilir bir sorun hakkında daha fazla ayrıntı ortaya çıkabilir.

Değişiklik günlükleri, özellikle açık kaynaklı ürünlerde, versiyonlar arasındaki bir diffün sabit ancak yaygın olarak bilinmeyen ve belki de sonuç olarak yükseltme veya kurulum için öncelik verilmeyen bir güvenlik açığı ortaya çıkarabileceği ek araştırmalar için rehberlik sağlayabilir.

Veritabanı ve Çerçeve Modüllerini Sömürme

Birçok istismar veri tabanı, internette aktif olarak korunur ve herkese açıktır. Güvenlik araştırmacıları ve istismar yazarları, istismar kodlarını her zaman birden fazla siteye sunmaz, bu nedenle birkaç siteye aşina olmaları ve potansiyel olarak savunmasız uygulamalara karşı kullanmak için istismar kodu için her birini kontrol etmeleri önerilir. Bazı güvenlik açığı veritabanları istismar kullanılabilirliğini takip ederken, kapsama alanları genellikle eksiktir ve kapsamlı olarak kabul edilmemelidir.

Ticari ve açık kaynaklı istismar çerçeveleri, güvenlik açıklarını araştırmada da yararlı olabilir. Çoğu durumda, mevcut istismar modülleri halka açık web sitelerinde listelenir ve bir sorunun istismar edilebilirliğinin değerli bir göstergesi olabilir.

Ortak / Temerrüt Şifreler

Sık sık, yöneticiler ve teknisyenler zayıf şifreleri seçer, asla varsayılanı değiştirmez veya herhangi bir şifre belirlemezler. Çoğu yazılım ve donanım için kılavuzlar çevrimiçi olarak kolayca bulunabilir ve varsayılan kimlik bilgilerini sağlar. İnternet forumları ve resmi satıcı posta listeleri, belgesiz hesaplar, yaygın olarak kullanılan şifreler ve sıklıkla yanlış yapılandırılmış hesaplar hakkında bilgi sağlayabilir. Son olarak, birçok web sitesi varsayılan / arka kapı şifrelerini belgelemektedir ve tanımlanan her sistem için kontrol edilmelidir.

Sertleştirme Kılavuzları / Ortak Yanlış Yapılandırmalar

Penetrasyon testinin birincil hedeflerinden biri, gerçek bir saldırganın taktiklerini ve davranışlarını simüle etmektir. Otomatik tarama bir testin zaman penceresini azaltabilirken, hiçbir tarayıcı bir insan gibi davranamaz. Sertleştirme kılavuzları bir penetrasyon test cihazı için paha biçilmez bir referans olabilir. Bunlar sadece bir sistemin en zayıf kısımlarını vurgulamakla kalmaz, aynı zamanda kaç tavsiyenin uygulandığını doğrulayarak bir yöneticinin çalışkanlığı duygusunu kazanabilirsiniz. Her penetrasyon testi sırasında, yönetici tarafından belirlenen güvenlik açıklarını keşfetmek için her büyük sistemi ve önerilen sertleştirme ayarlarını gözden geçirmek için zaman alınmalıdır.

Kullanıcı forumları ve posta listeleri, sistemler ve yöneticilerin bunları yapılandırma ve güvence altına almada sahip oldukları çeşitli konular hakkında değerli bilgiler sağlayabilir. Bir test cihazı, hedef sistemlerini kendisi kuruyormuş gibi araştırmalı ve ağrı noktalarının ve olası yapılandırma hatalarının nerede yatacağını keşfetmelidir.

Özel Araştırmalar

Bir replika ortam oluşturmak

Sanallaştırma teknolojileri, bir güvenlik araştırmacısının özel donanım gerektirmeden çok çeşitli işletim sistemleri ve uygulamaları çalıştırmasına izin verir. Hedef işletim sistemi veya uygulaması tanımlandığında hedefi taklit etmek için bir sanal makine (VM) ortamı hızlı bir şekilde oluşturulabilir. Test cihazı, doğrudan hedefe bağlanmadan, uygulamanın parametrelerini ve davranışlarını yapılandırmak için bu VM'yi kullanabilir.

Yapılandırmaları Test Edin

Bir test VM laboratuvarı, mümkün olduğunda Windows XP, Vista, 7, Server 2003 ve Server 2008, Debian, Ubuntu, Red Hat ve Mac OS X dahil olmak üzere tüm yaygın işletim sistemleri için temel görüntüler içermelidir. Her servis paketi seviyesi için ayrı görüntülerin korunması, hedefin çevresini yeniden yaratma sürecini kolaylaştıracaktır. Klonlamayı destekleyen bir VM ortamı ile birlikte eksiksiz bir VM kütüphanesi, bir test cihazının dakikalar içinde yeni bir hedef VM getirmesine izin verecektir. Ek olarak, bir anlık görüntü özelliği kullanmak daha verimli çalışmasına ve hataları yeniden üretmesine olanak sağlayacaktır.

Bulanıklık

Bulanıklık veya arıza enjeksiyonu, uygulamaya programsal olarak geçerli, rastgele veya beklenmedik girdiler göndererek uygulama kusurlarını bulmak için kaba kuvvet tekniğidir. Temel süreç, hedef uygulamaya bir hataşı eklemeyi ve daha sonra bulanıklaştırma rutinini belirli giriş alanlarına karşı çalıştırmayı ve daha sonra herhangi bir çöküşten sonra program durumunu analiz etmeyi içerir. Birçok burkulma uygulaması mevcuttur, ancak bazı testçiler belirli hedefler için kendi tüy izlerini yazar.

Potansiyel caddeleri / vektörlerin tanımlanması

Komutları ve diğer giriş alanlarını belirlemek için bir hedef ağ uygulamasına giriş yapın veya bağlantı kurun. Hedef, dosyaları ve/veya web sayfalarını okuyan bir masaüstü uygulamasıysa, veri girişinin yolları için kabul edilen dosya biçimlerini analiz edin. Bazı basit testler, bir kazaya neden olmak için geçersiz karakterler veya çok uzun karakter dizilerini göndermeyi içerir. Başarılı bir kaza durumunda program durumunu analiz etmek için bir hata ayıklama takın.

sökülmesi ve kod analizi

Bazı programlama dilleri ayrışmaya izin verir ve bazı özel uygulamalar hata ayıklama için sembollerle derlenir. Bir test cihazı, program akışını analiz etmek ve potansiyel güvenlik açıklarını belirlemek için bu özelliklerden yararlanabilir. Açık kaynak uygulamaları için kaynak kodu kusurlar için analiz edilmelidir. PHP'de yazılan web uygulamaları aynı güvenlik açıklarının çoğunu paylaşır ve kaynak kodları herhangi bir testin bir parçası olarak incelenmelidir.
