Post Exploitation

İçerikler

Amaç

Post-Sömürü aşamasının amacı, ele geçirilen makinenin değerini belirlemek ve makinenin kontrolünü daha sonra kullanmak üzere korumaktır. Makinenin değeri, üzerinde depolanan verilerin hassasiyeti ve ağın daha fazla ödün vermedeki makinelerin kullanışlılığı ile belirlenir. Bu aşamada açıklanan yöntemler, testçinin hassas verileri tanımlamasına ve belgelenmesine, yapılama ayarlarını, iletişim kanallarını ve ağa daha fazla erişim sağlamak için kullanılabilecek diğer ağ cihazlarıyla olan ilişkileri tanımlamasına ve daha sonraki bir zamanda makineye erişmesi için bir veya daha fazla yöntem oluşturmasına yardımcı olmak içindir. Bu yöntemlerin, Meydana Gelen Yönetmelik Kurallarından farklı olduğu durumlarda, Katılım Kurallarına uyulmalıdır.

Katılım Kuralları

Aşağıdaki Katılım Kuralları, bir penetrasyon testinin İspat Sonrası aşamasına özgüdür ve müşterinin sistemlerinin testçilerin (doğrudan veya dolaylı) eylemleriyle gereksiz riske maruz kalmamasını ve projenin patlama sonrası aşamasında karşılıklı olarak kararlaştırılan bir prosedürün sağlanmasını sağlamayı amaçlamaktadır.

Müşteriyi koruyun

Aşağıdaki kurallar, günlük operasyonların ve müşterinin verilerinin riske maruz kalmamasını sağlamak için bir müşteriyle birlikte oluşturmak için bir kurallar kılavuzu olarak kullanılacaktır:

- Daha önce kararlaştırılmadıkça, müşterinin altyapılarında “kritik” olarak gördüğü hizmetlerin değiştirilmesi olmayacaktır. Bu tür hizmetleri değiştirmenin amacı, müşteriye bir saldırganın nasıl olabileceğini göstermek olacaktır:
  - Ayrıcalıkları tırmandırın
  - Belirli verilere erişim kazanın
  - Hizmet reddine neden olun
- Bir sisteme karşı yürütülen yapılandırma değişiklikleri de dahil olmak üzere tüm değişiklikler belgelenmelidir. Değişikliğin amaçlanan amacını bitirdikten sonra, mümkünse tüm ayarlar orijinal konumlarına döndürülmelidir. Değişiklik listesi, tüm değişikliklerin düzgün bir şekilde geri alındığından emin olmalarına izin vermek için katılımdan sonra müşteriye verilmelidir. Orijinal pozisyonlarına geri dönemeyen değişiklikler, başarılı bir şekilde tersine çevrilen değişikliklerden açıkça ayırt edilmelidir.
- Uzlaşılan sistemlere karşı yapılan eylemlerin ayrıntılı bir listesi tutulmalıdır. Listede alınan eylem ve gerçekleştiği süreyi de içermelidir. Tamamlandığında, bu liste nihai rapora ek olarak dahil edilmelidir.
- Penetrasyon testi sırasında ortaya çıkarılan tüm ve tüm özel ve/veya kişisel kullanıcı verileri (şiranlar ve sistem geçmişi dahil) daha fazla izin almak veya testle ilgili diğer eylemleri yalnızca aşağıdaki koşullar yerine getirilirse gerçekleştirilmek için kaldıraç olarak kullanılabilir:
  - Müşterinin Kabul Edilebilir Kullanım Politikası, tüm sistemlerin müşteriye ait olduğunu ve bu sistemlerde depolanan tüm verilerin müşterinin mülkiyetinde olduğunu belirtir.
  - Kabul Edilebilir Kullanım Politikası, müşterinin ağına olan bağlantısının, bağlı makinenin aranması ve analiz edilmesi için (mevcut tüm veri ve yapılandırmalar dahil) onay olarak kabul edildiğini belirtir.
  - Müşteri, tüm çalışanların Kabul Edilebilir Kullanım Politikasını okuduğunu ve anladığına dair onaylanmıştır.
- Şifreler (kiferifletim formunda olanlar dahil) nihai rapora dahil edilmeyecek veya raporun alıcılarının şifreyi yeniden oluşturamamasını veya tahmin edemeyeceğinden emin olmak için yeterince maskelenmelidir. Bu, şifrelerin ait olduğu kullanıcıların gizliliğini korumak ve korudukları sistemlerin bütünlüğünü korumak için yapılır.
- Tehlike altındaki sistemlere erişimi sürdürmek için kullanılan ve sistemin uygun şekilde çalışmasını etkileyebilecek veya çıkarılması, müşterinin önceden yazılı izni olmadan kesinti süresine neden olabilecek herhangi bir yöntem veya cihaz uygulanmayabilir.
- Tehlike altındaki sistemlere erişimi sürdürmek için kullanılan herhangi bir yöntem veya cihaz, dijital sertifikalar veya giriş istemleri gibi bir kullanıcı kimlik doğrulaması formu kullanmalıdır. Bilinen kontrollü bir sisteme ters bağlantı da kabul edilebilir.
- Testçiler tarafından toplanan tüm veriler testçiler tarafından kullanılan sistemlerde şifrelenmelidir.
- Raporda hassas veriler (ekran görüntüleri, tablolar, rakamlar) içerebilecek herhangi bir bilgi, raporların alıcıları tarafından verileri kalıcı olarak geri kazanılamayan teknikler kullanılarak sterilize edilmeli veya maskelenmelidir.
- Müvekkil nihai raporu kabul ettikten sonra toplanan tüm veriler imha edilecektir. Kullanılmış yöntem ve yıkım kanıtı müşteriye sağlanacaktır.

- Toplanan veriler herhangi bir yasa tarafından düzenlenirse, toplanan ve işlenen verilerin yürürlükteki herhangi bir yasayı ihlal etmediğinden emin olmak için kullanılan sistemler ve konumları müşteri tarafından sağlanacaktır. Sistemler penetrasyon testi ekibi olacaksa, veriler kendi sistemlerine indirilip depolanamayabilir ve yalnızca erişim kanıtı gösterilecektir (Dosya Izinleri, Kayıt Sayısı, dosya adları..etc).
- Şifre kırma için üçüncü taraf hizmetleri kullanılmayacak ve müşterilerin onayı olmadan üçüncü taraflarla başka bir veri türünün paylaşılması da sağlanmayacaktır.
- Değerlendirilen ortamda bulunursa, önceden bir uzlaşma kanıtı varsa, penetrasyon ekibi tarafından yapılan değerlendirme sırasında kaydedilen eylemler ve sürelerle tüm kayıtlar kaydedilir, hash edilir ve müşteriye sağlanacaktır. Müşteri daha sonra olay yanıtına en iyi nasıl yanıt verileceğini belirleyebilir.
- İş sözleşmesinde müşteri tarafından özel olarak yetkili olmadıkça hiçbir günlük kaldırılmamalı, temizlenmeli veya değiştirilmemelidir. İzin verilirse, herhangi bir değişiklikten önce kütükler yedeklenmelidir.

Kendinizi korumak

Bir penetrasyon testinin doğası gereği, müşteriyle ve gerçekleştireceğiniz görevlerle uğraşırken tüm tabanlarınızı kapsadığınızdan emin olmalısınız. Herhangi bir işe başlamadan önce hem müşterinin hem de sağlayıcının rol ve sorumluluklarının net bir şekilde anlaşılmasını sağlamak için müşteriyle aşağıdakileri tartışın.

- Hem müşteri hem de sağlayıcı tarafından imzalanan iş sözleşmesinin ve/veya beyanının, test edilen sistemler üzerinde yapılan eylemlerin müvekkil adına ve temsilinde olmasını sağlayın.
- Katılımı başlatmadan önce şirket sistemlerinin ve altyapısının kullanıcı kullanımını (genellikle "Kabul Edilebilir Kullanım" politikaları olarak anılacaktır) yöneten güvenlik politikalarının bir kopyasını alın. Politikanın karşıladığı doğrulayın:
  - Müşteri sistemleri ve bu verilerdeki sahiplik ve haklar üzerinde kişisel çalışan verilerinin kişisel kullanımı ve kişisel çalışan verilerinin depolanması.
  - Şirket ekipmanlarında depolanan verilerin mülkiyeti.
- Müşteri tarafından sistemlerine göre yönetilen ve kullanılan verileri ve bu verilere uygulanan kısıtlamaları düzenleyen düzenlemeleri ve yasaları doğrulayın.
- Müşteri verilerini alacak ve saklayacak sistemler ve çıkarılabilir medya için tam sürücü şifreleme kullanın.
- Üçüncü bir taraftan bir uzlaşmanın bulunduğu davada takip edilecek prosedürleri müvekkille birlikte tartışın ve belirleyin.
- Ses ve videonun yakalanması ve / veya depolanmasıyla ilgili yasaları kontrol edin, çünkü bu yöntemlerin sömürü sonrası kullanım yerel veya ülke dinleme yasalarının ihlali olarak kabul edilebilir.

Altyapı Analizi

Ağ Yapılandırması

Tehlikeye kapılan bir makinenin ağ yapılandırması, ek alt ağları, ağ yönlendiricileri, kritik sunucular, isim

sunucuları ve makine arasındaki ilişkileri tanımlamak için kullanılabilir. Bu bilgiler, müşterinin ağına daha fazla nüfuz etmek için ek hedefleri belirlemek için kullanılabilir.

Arayüzler

Makinedeki tüm ağ arayüzlerini IP adresleri, alt ağ maskeleri ve ağ geçitleri ile birlikte tanımlayın. Arayüzleri ve ayarları belirleyerek, ağlar ve hizmetler hedefleme için önceliklendirilebilir.

Rota

Diğer alt ağların, filtreleme veya ele alma şemalarının bilgisi, segmentli bir ağdan kaçmak için kullanılabilir ve bu da ek konaklara ve / veya ağların araştırılmasına ve numaralandırılmasına yol açabilir. Bu veriler, aşağıdakiler de dahil olmak üzere bir partiş kıvılcım sunucusu veya ağdaki çeşitli kaynaklardan gelebilir:

- Arayüzler
- Statik ve dinamik rotalar da dahil olmak üzere yuvarlama tabloları
- ARP Tabloları, NetBios veya hizmet ve ev sahibi keşif için kullanılan diğer ağ protokolleri.
- Çok evli ev sahipleri için, yönlendirici olarak hareket edip etmediklerini belirleyin.

DNS Sunucuları

Tüm DNS sunucularını, ana bilgisayar ayarlarını değerlendirerek tanımlayın. DNS sunucuları ve bilgileri daha sonra hedef ağdaki ek ana bilgisayarları ve hizmetleri keşfetmek için bir plan geliştirmek ve yürütmek için kullanılabilir. Bir DNS Sunucusunun ele geçirilmesi durumunda, DNS veritabanı, değerlendirmenin geri kalanı için hedeflere öncelik vermek için kullanılabilecek ana bilgisayarlar ve hizmetler hakkında değerli bilgiler sağlayacaktır. Yeni kayıtların değiştirilmesi ve eklenmesi, DNS'ye bağlı olarak hizmetlerin verilerini engellemek için kullanılabilir.

Nakavt DNS Girişleri

Intranet siteleri, yönetim arayüzleri veya harici siteler için oturum açma sayfaları içerebilecek önbellekteki yüksek değerli DNS girişlerini belirleyin. Önbelleğe bağlı arayüzler, hedef ağın ve altyapının daha fazla penetrasyonu için hedeflerin önceliklendirilmesinde kullanılabilecek bilgileri sağlayan ev sahiplerinin ilişkileri ve etkileşimleri hakkında bir görüş sağlayan, ele geçirilen ana bilgisayar tarafından kullanılan en son ve en çok kullanılan ev sahibinden bilgi sağlar. Önbelleğe alınan girişlerin değiştirilmesi, kimlik doğrulama kimlik bilgilerini, kimlik doğrulama jetonlarını yakalamak veya hedef ağın daha fazla nüfuzuna yol açan ele geçirilen ana bilgisayarlar tarafından kullanılan hizmetler hakkında daha fazla bilgi edinmek için kullanılabilir.

Proxy Sunucuları

Ağ ve uygulama seviyesi proxy sunucularını tanımlayın. Proxy sunucuları, müşteri tarafından kurumsal olarak kullanıldığında iyi hedefler koyar. Başvuru vekilleri söz konusu olduğunda, trafiğin akışını veya trafiğin kendisini tanımlamak, değiştirmek ve / veya izlemek mümkün olabilir. Proxy saldırıları genellikle müşteriye etki ve risk göstermek için etkili bir araçtır.

ARP Girişleri

Enumerate önbelleklenmiş ve statik ARP masa girişleri, tehlikeye atılmış makineyle etkileşime giren diğer konakçıları ortaya çıkarabilir. Statik ARP girişleri kritik makineleri temsil edebilir. Değerlendirmenin kapsamı, ARP girişlerini engellemeye ve değiştirmeye izin veriyorsa, bir hizmeti genellikle tespit edilmeyen veya korunmayan bir şekilde bozma, izleme veya tehlikeye atma olasılığını göstermek kolaydır.

Ağ Hizmetleri

Dinleme Hizmetleri

Hedef makine tarafından sunulan tüm ağ hizmetlerini tanımlayın. Bu, ilk tarama ile tanımlanmayan hizmetlerin keşfedilmesine ve diğer makinelerin ve ağların keşfine yol açabilir. Taramada gösterilmeyen hizmetlerin tanımlanması, ağda ve / veya konakta uygulanan olası filtreleme ve kontrol sistemleri hakkında da bilgi sağlayabilir. Buna ek olarak, test cihazı bu hizmetlerden diğer makineleri tehlikeye atmak için kullanabilir. Çoğu işletim sistemi, makineye yapılan ve makineden yapılan TCP ve UDP bağlantılarını tanımlama yöntemini içerir. Her iki bağlantıyı hem ele geçirilmiş bir makineye de kontrol ederek, daha önce bilinmeyen ilişkileri bulmak mümkündür. Hizmetin de dikkate alınması gerektiğinin yanı sıra, bu, standart olmayan limanlarda dinleme hizmetlerini ortaya çıkarabilir ve SSH için anahtarsız kimlik doğrulama gibi güven ilişkilerini gösterebilir.

VPN Bağlantıları

Hedef makineye veya ağ içine ve dışındaki tüm VPN bağlantıları tanımlanmalıdır. Giden bağlantılar, daha önce tanımlanmamış olabilecek yeni sistemlere yollar sağlayabilir. Hem inbound hem de outbound yeni sistemleri ve olası iş ilişkilerini tanımlayabilir. VPN bağlantıları genellikle şifreli trafiğin şifresini çözememeleri veya denetlenmemeleri nedeniyle güvenlik duvarlarını ve izinsiz giriş algılama / önleme sistemlerini atlar. Bu gerçek, VPN'leri saldırıları başlatmak için ideal kılar. Herhangi bir yeni hedef, onlara karşı saldırılar başlatmadan önce kapsam olarak doğrulanmalıdır. Hedef ana bilgisayardaki VPN istemcisinin veya sunucu bağlantılarının varlığı, diğer ana bilgisayarları ve hizmetleri hedeflemek için kullanılabilecek daha önce bilinmeyen kimlik bilgilerine de erişim sağlayabilir.

Dizin Hizmetleri

Hedeflenen bir ev sahibin dizin hizmetleri, ek saldırılarda kullanılabilecek kullanıcı hesaplarını, konakçıları ve / veya hizmetleri numaralandırmak veya güvenlik açığı analizi aşamasında daha önce keşfedilmemiş olabilecek ek hedefler sağlamak için bir fırsat sağlayabilir. Ek olarak, dizin hizmetlerinde bulunan kullanıcıların ayrıntıları Sosyal Mühendislik ve kimlik avı kampanyası saldırıları için kullanılabilir, böylece olası bir yüksek başarı oranı sağlayabilir.

Komşular

Bugün ağda birçok hizmet ve işletim sistemi, komşu keşfi için bir dizi protokol kullanır ve hizmetlerin, sorun gidermenin ve yapılandırmanın erişimini daha uygun hale getirir. Protokoller hedef konak türünün türüne bağlı olarak değişir. Ağ ekipmanı, doğrudan kendilerine bağlı veya aynı alt ağda bulunan sistemlere, yapılandırmaları ve diğer ayrıntıları tanımlamak için CDP (Cisco Discovery Protocol) ve LLDP (Link Katma Uzmanı Keşif Protokolü) gibi protokolleri kullanabilir. Benzer şekilde, masaüstü ve sunucu işletim sistemleri, aynı alt ağdaki ana bilgisayarların ve hizmetlerin ayrıntılarını bulmak için mDNS (Multicast Alan Adı Hizmeti) ve NetBios gibi protokolleri kullanabilir.

Hacma

Hallaging, ön değerlendirme aşamasında tanımlanan hedeflerle ilgili hedefli ev sahiplerinden bilgi (yani kişisel bilgiler, kredi kartı bilgileri, şifreler vb. içeren dosyalar) elde etmeyi ifade eder. Bu bilgiler, hedeflerin tatmin edilmesi amacıyla veya ağa daha fazla erişim elde etmek için pivoting sürecinin bir parçası olarak elde edilebilir. Bu verilerin konumu, veri türüne, konakçının rolüne ve diğer koşullara bağlı olarak değişecektir. Yaygın olarak kullanılan uygulamalara, sunucu yazılımına ve ara yazılıma aşinalık çok önemlidir, çünkü çoğu uygulama verilerini birçok farklı formatta ve konumlarda saklar. Hedeflenen verileri bazı sistemlerden elde etmek, çıkarmak veya okumak için özel araçlar gerekli olabilir.

Yüklü Programlar

Başlangıç öğeleri

Çoğu sistem, sistem girişiminde veya kullanıcı oturumunda çalışabilen ve etkileşimde bulunduğu sistem, yazılım ve hizmetlerin amacı hakkında bilgi sağlayabilecek uygulamalara sahip olacaktır. Bu bilgi, bir hedef ağın ve sistemlerinin daha fazla sömürülmesini engelleyebilecek potansiyel karşı önlemleri ortaya çıkarabilir (örneğin. SAKAL / HIPS, Uygulama Beyaz Listeleme, FIM). Toplanması gereken bilgiler şunları içerir:

- Sisteme yüklü uygulamaların ve ilgili sürümlerinin listesi.
- Sisteme uygulanan işletim sistemi güncellemelerinin listesi.

Kurulan Hizmetler

Belirli bir ev sahibindeki hizmetler, ev sahibinin kendisine veya hedef ağdaki diğer ev sahiplerine hizmet edebilir. Hedeflenen her bir ev sahibinin bir profilini oluşturmak, bu hizmetlerin yapılandırılması, amaçları ve değerlendirme hedeflerine ulaşmak veya ağa daha fazla nüfuz etmek için potansiyel olarak nasıl kullanılabileceklerini belirtmek gerekir.

Güvenlik Hizmetleri

Güvenlik hizmetleri, bir saldırganı sistemlerden uzak tutmak ve verileri güvende tutmak için tasarlanmış yazılımı içerir. Bunlar, ağ güvenlik duvarlarını, konak tabanlı güvenlik duvarlarını, IDS / IPS'yi, HIDS / HIPS ve anti-virüsü içerir, ancak bunlarla sınırlı değildir. Hedeflenen tek bir ev sahibinde herhangi bir güvenlik hizmetini tanımlamak, ağdaki diğer makineleri hedef alırken ne bekleyeceği hakkında bir fikir verir. Ayrıca, proje brifinginde müşteriyle tartışılabilecek test sırasında hangi uyarıların tetiklenmiş olabileceğine dair bir fikir verir ve Güvenlik Politikaları, UAC, SELinux, IPSec, pencere güvenlik şablonları veya diğer güvenlik kuralları / yapılandırmalarında güncellemelerle sonuçlanabilir.

Dosya/Printer Hisseleri

Dosya ve baskı sunucuları genellikle hedeflenen veriler içerir veya hedef ağa ve ana bilgisayarlara daha fazla nüfuz etme fırsatı sunar. Hedef alınması gereken bilgiler şunları içerir:

- Dosya Sunucuları tarafından sunulan hisse senetleri - Hedef sistemler tarafından sunulan herhangi bir dosya paylaşımı incelenmelidir. Paylaşımların isimleri ve yorumları bile dahili uygulamaların veya projelerin isimleri hakkında önemli bilgiler sızdırabilir (yani sadece "Fred" ve "Christine" "Hesap" klasörüne erişirse, belki de her ikisi de muhasebe çalışanıdır).
- Paylaşımlar için Erişim Kontrol Listeleri ve izinleri. - Müşteri tarafından, hisseye bağlanmak mümkünse, bağlantının yalnızca okunur / okunursa / yazmanın olup

olmadığını görmek için kontrol edilmelidir. Bir hisse dizin içeriyorsa, farklı dizinler için farklı izinler uygulanabilirse. Sunucu tarafından hem sunucu yapılandırması hem de dosya / yönerge izinleri incelenmelidir.
- Dosya paylaşımı dosyası ve içerik listeleri
- Dosya paylaşımı listelerinden ilgi alan dosyaları belirleyin. Aşağıdaki gibi ilginç veya hedeflenen öğeleri arayın:
  - Kaynak Kodu
  - Yedekler
  - Kurulum Dosyaları
  - Gizli Veriler (e-ebekenlerde finansal veriler, TXT / PDF'deki banka raporları, şifre dosyaları vb.)
- Trojans veya otomatik çalıştırım dosyaları yerleştirin - Akıllıca adlandırma kullanarak veya halihazırda kullanılmakta olan isim sözleşmelerini taklit ederek, kullanıcıların test cihazının ağa daha fazla nüfuz etmesini sağlayarak bu yükleri yürütmeye teşvik edilebilir. Dosya sunucusu günlükleri elde edilebilirse, belirli kullanıcılar bile hedef alınabilir.

Veritabanı Sunucuları

Veritabanı, bir değerlendirmede hedef alınabilecek çok sayıda bilgi içerir.

- Veritabanı - Veritaban adlarının bir listesi, düzenleyicinin veritabanının amacını ve veritabanının içerebileceği veri türlerini belirlemesine yardımcı olabilir. Birçok veri tabanına sahip bir ortamda, bu hedeflere öncelik vermede yardımcı olacaktır.
- Tablolar - Masa adları ve yorumlar, sütun adları ve türleri gibi meta veriler de değerlendiricinin hedefleri seçmesine ve hedeflenen verileri bulmasına yardımcı olabilir.
- Tablo İçeriği, düzenlenmiş içerik için satır sayımı
- Sütunlar - Birçok veri tabanında, tüm masaların tüm sütun adlarını tek bir komutla aramak mümkündür. Bu, hedeflenen verileri bulmak için kaldıraçlı olabilir (örneğin. Kredi kartı verileri bir Oracle veritabanında hedeflenirse, *adı = '%CCN%';* orada *all_tab_columns'tan belirli * uygulamayı* deneyin.
- Veritabanı ve Masa Izinleri
- Veritabanı Kullanıcıları, Şifreler, Gruplar ve Roller

Veritabanlarında barındırılan bilgiler, riski göstermek, değerlendirme hedeflerine ulaşmak, hizmetlerin yapılandırılması ve işlevini belirlemek veya bir müşteri ağına ve ana bilgisayarlara daha fazla nüfuz etmek için de kullanılabilir.

Yönetmenlik Sunucuları

Bir dizin hizmetinin ana hedefleri, referans veya/ve kimlik doğrulama için hizmetlere ve ev sahiplerine bilgi sağlamaktır. Bu hizmetin uzlaşması, hizmete bağlı tüm ev sahiplerinin kontrolünün sağlanmasına izin verebilir ve bir saldırıyı ilerletmek için kullanılabilecek bilgiler sağlayabilir. Bir dizin hizmetinde aranacak bilgiler şunlardır:

- Nesnelerin listesi (Kullanıcılar, şifreler, Makineler.etc)
- Sistemle bağlantılar

- Protokollerin ve güvenlik seviyesinin tanımlanması

İsim Sunucuları

İsim sunucusu, sunucuların kayıt türlerine bağlı olarak barındırma ve hizmetlere çözüm sağlar. Kayıtların ve kontrollerin numaralandırılması, bir müşteri ağına ve ev sahiplerine daha fazla nüfuz etmek için öncelik vermek ve saldırmak için bir hedef ve hizmet listesi sağlayabilir. Kayıtları değiştirme ve ekleme yeteneği, hizmetlerin reddedilme riskini göstermek için kullanılabilir ve bir müşteri ağındaki trafik ve bilgilerin ele alınmasına yardımcı olur.

Dağıtım Hizmetleri

Dağıtım hizmetlerinin tanımlanması, aşağıdakilerin erişimine ve numaralandırılmasına izin verir:

- Katılımsız cevap dosyaları
- Dosyalarda izin
- Dahil güncellemeler
- Uygulamalar ve sürümler

Bu bilgiler bir müşteri ağına ve ev sahiplerine daha fazla nüfuz etmek için kullanılabilir. Hizmetin depolarını ve yapılandırmasını değiştirme yeteneği izin verir

- Arka kapı kurulumu
- Onları saldırıya karşı savunmasız hale getirmek için hizmetlerin değiştirilmesi

Sertifika Yetkisi

Tazminatlı bir müşteri ev sahibi üzerinde Sertifika Yetkisi hizmetlerinin tanımlanması, erişime izin verecektir

- Kök CA
- Kod İmza Sertifikaları
- Şifreleme ve İmza Sertifikaları

Hizmetin kontrolü de izin verecektir

- Çeşitli görevler için yeni sertifikaların oluşturulması
- Sertifikaların iptali
- Sertifika İptal Listesinin Değiştirilmesi
- Kök CA Sertifikasının Eklenmesi

Hizmetlerin kontrolü riski gösterir ve bir müşterinin ağı ve ev sahiplerinde veri ve hizmetlerin tehlikeye girmesine izin verir.

Kaynak Kod Yönetimi Sunucusu

Zorunlu olan ev sahibinde veya hizmetin müşteri kısmı üzerinde çalışan hizmet aracılığıyla kaynak kod yönetim sistemlerinin tanımlanması:

- Sayıda projeler - Proje adları şirket projelerinde hassas bilgileri verebilir.
- Kaynak kod dosyalarına erişimi doğrulayın
- Kaynak kod dosyalarını değiştirin - Kapsamda izin verilirse, kaynak kodunun değiştirilmesi, bir saldırganın sistemi etkileyecek değişiklikler yapabileceğini kanıtlamaktadır.
- Enumerate geliştiriciler - Geliştiricilerin ayrıntıları, sistemin diğer alanlarına saldırmak için girişlerin yanı sıra sosyal mühendislik saldırıları için kullanılabilir
- Sayım yapılandırması

Dinamik Ana Bilgisayar Konfigürasyon Sunucusu

Dinamik ana bilgisayar yapılandırma hizmetinin tanımlanması veya hizmetin tehlikeye atılmış ana bilgisayar tarafından kullanılması aşağıdakilere izin verir:

- Sayım kiralamaları verildi
- Enumerasyon yapılandırması
- Sayım Seçenekleri
- Yapılandırmanın değiştirilebilir
- Tüm kiralamaların tüketimi

Hizmetin kontrolü, hizmet reddi riskini göstermek ve yardım edilen ağdaki ev sahiplerinin ve hizmetlerin orta saldırılarında insanda kullanılmak üzere kullanılabilir.

Sanallaştırma

Kimlik doğrulama sanallaştırma hizmetleri veya istemci yazılımı aşağıdakilere izin verir:

- Enumerate Virtual Machines (isim, yapılandırmalar, işletim sistemi)
- İdare sistemleri için komut şifreleri ve dijital sertifikaları sayın.
- Enumrate virtualization yazılım yapılandırması
- Host'ların yapılandırılması
- VM eyaletinin kontrolü ile hizmet reddi riskini gösterin
- VM'lerde barındırılan verilere erişim
- Ele geçirilen ev sahibine ev sahipliği yapan sanal ev sahiplerinin veya hizmetlerin trafiğinin ele geçirilmesi

Mesajlaşma

Mesajlaşma için hizmetlerin veya istemci yazılımlarının tanımlanması fırsat sağlar

- Yönerkesi Hizmetlerini Tanımlayın
- Kimlik bilgilerinin karşılaştırılması
- Gizli bilgilere erişim
- Ana bilgisayarların ağda tanımlanması
- Sistem ve iş ilişkileri

Tüm bu bilgiler ve eylemler, bir müşterinin ağına ve ev sahiplerine daha fazla nüfuz etmek için kullanılabilir.

İzleme ve Yönetim

Hizmetlerin veya istemci yazılımının izlenmesi ve / veya yönetimi amacıyla tanımlanması, hedef ağdaki ek sunucuların ve hizmetlerin tanımlanmasını sağlayabilir, ayrıca kazanılan yapılandırma parametreleri diğer hedeflere erişim sağlayabilir ve test cihazı tarafından hangi eylemlerin gerçekleştirildiğini belirlemek için istemci tarafından tespit edilebilir. Arayabileceğiniz bazı hizmetler:

- SNMP (Uygulamalı Ağ Yönetimi Protokolü)
- Syslog'un

Kimlik bilgilerini almak, ev sahibini belirlemek ve diğer hizmetlere erişmek için aramak için bazı Yönetim Hizmetleri ve Yazılımları şunlar olabilir:

- SSH Sunucu / Müşteri
- Telnet Sunucusu / Hillit
- RDP (Uzaktan Masaüstü Protokolü) İstemcisi
- Terminal Sunucu
- Sanal Ortam Yönetim Yazılımı

Yedekleme Sistemleri

Verileri yedeklemek amacıyla hizmetlerin veya müşteri yazılımının tanımlanması, bir saldırgana büyük bir fırsat sağlar, çünkü bu sistem bir saldırgan sağlamak için ihtiyaç duydukları verilere ve sistemlere erişim gerektirir:

- Ev sahiplerinin ve sistemlerin numaralandırılması
- Hizmetlerin verilmesi
- Ev sahibi ve/veya hizmetlerine yönelik kimlik bilgileri
- Yedek verilere erişim

Hizmetten edinilen bilgiler, sistemin ve bilgilerine gizlilik, bütünlük ve erişime yönelik riski göstermek için kullanılabilir. Yedeklere erişim, müşteri sistemlerine yanlış yapılandırma, savunmasız yazılım veya arka kapılarda tanıtma fırsatı da sağlayabilir.

Ağ hizmetleri (RADIUS,TACACS..etc)

Hizmetlerin tanımlanması veya ağ hizmetleri kullanımı aşağıdakilere izin verir:

- Kullanıcıların numaralandırılması
- Ev sahiplerinin ve sistemlerin numaralandırılması
- Kimlik bilgilerinin karşılaştırılması
- Alternatif yöntemler mevcut değilse hizmet reddi riskini gösterin

Hassas Veriler

Anahtar-loglama

Anahtar vuruşları izleyerek, şifreler ve PII dahil olmak üzere hassas bilgileri tespit etmek mümkündür -

Kullanıcı şirket yazılımını kullanırken özel IM'de sohbet ederken sohbet ediyorsa bunun yasallığının ne olduğunu bilmiyor musunuz, bilen var mı? Şirket, ağdaki tüm verilerin izlenebileceğini söylüyorsa, bu iyi olmalıdır. Protect Yourself'teki ikinci mermi noktası mevcutsa ve ekipmanın kullanımının izlenebileceğini ve kişisel kullanıma izin verilmediğini belirtirse, politika kişisel kullanıcıyı veya veri sahipliğini kapsamazsa, hayır. Ayrıca Network'ü de kapsayacak şekilde genişletilmelidir.

Ekran yakalama

Ekran yakalama, uzlaşma kanıtı göstermek ve ekranda gösterilebilecek bilgilere erişim ve diğer yollarla erişmek mümkün değildir. Müşterinin müşterilerinin çalışanlarının özel verilerini veya gösterilmesi için ekran yakalama ile toplanan verilerle büyük özen gösterilmelidir.

Ağ trafiği yakalama

Ağ trafiği yakalama ağın kontrollerine bağlı olarak kullanılabilir ve yakalama için kullanılan ortam aşağıdakiler için kullanılabilir:

- Ağdaki ev sahiplerini tanımlayın
- Kesişme verileri
- Hizmetlerin tanımlanması
- Ağdaki ev sahipleri arasındaki ilişkileri belirlemek
- Kimlik bilgilerinin yakalanması

Sadece angajman kapsamında kapsanan trafiği yakalamak için özen gösterilmelidir ve yakalanan bilgilerin Voice Over IP çağrılarının ele geçirilmesi gibi yerel yasaların kontrolü altına girmez. Müşterinin müşterisini ve / veya çalışan kişisel ve gizli verilerini korumak için tutulan ve gösterilen bilgiler filtrelenmelidir.

Önceki Denetim raporları

Kullanıcı Bilgileri

Bu bölümde ana odak, sistemde bulunan veya uzaktan bağlanmış olan kullanıcı hesaplarıyla ilgili hedef sistemde bulunan bilgiler üzerindedir ve değerlendirmeyi gerçekleştiren personelin daha fazla penetrasyon için toplanıp analiz edebileceği veya değerlendirmenin istenen hedefini sağlayabileceği bir iz bırakmıştır.

Sistem Üzerine

Uzlaşılmış bir sistemde toplanabilecek genel bilgiler şunlardır:

- Tarih dosyaları - Tarih dosyaları, kullanıcının yürüttüğü son komutları saklar. Bunlar aracılığıyla okumak, sistem yapılandırma bilgilerini, önemli uygulamaları, veri konumlarını ve diğer sistemleri ortaya çıkarabilir * hassas bilgileri.
- Şifreleme Anahtarları (SSH, PGP / GPG)
- İlginç Belgeler (.doc/x, .xls/x, şifre. *) - Kullanıcılar genellikle şifreleri ve diğer hassas bilgileri net metin belgelerinde saklar. Bunlar, şifre.txt gibi ilginç kelimeler için dosya adlarını aramak veya belgelerin kendi üzerinden arama yapmak için iki şekilde bulunabilir. İndeks hizmetleri buna yardımcı olabilir, örneğin Linux find veritabanı.
- Kullanıcıya özel uygulama yapılandırma parametreleri

- Bireysel Uygulama Geçmişi (Yalnızca MRU Windows, tarih dosyaları..etc)
- Çıkarılabilir medyayı numaralandırın
- Enumerate ağ paylaşımları / alan adı izni (düzgün)

Web Tarayıcılar

Diğer konakçıları ve sistemleri tanımlamak için kullanılabilen ve bir müşterinin ağına ve ana bilgisayarlarına daha fazla nüfuz etmek için bilgi sağlayan web tarayıcılarından toplanabilecek bilgiler şunlardır:

- Tarayıcı Tarihi
- Yer İşaretleri
- Tarih İndir
- Kimlik bilgileri
- Vekiller
- Eklentiler / Ömürler

Bir web tarayıcısından gelen bilgiler müşterinin çalışanının gizli ve özel verilerini içerebileceğinden, yalnızca etkileşim için kapsamdaki verilerin yakalanması büyük özen gösterilmelidir. Bu veriler iade edilen verilerden filtrelenmeli ve rapor edilmelidir.

IM Müşterileri

IM Müşterilerinden tehlikeye atılmış bir sistem üzerinde toplanabilecek bilgiler şunlardır:

- Sayıda Hesap Yapılandırması (Kullanıcı, Şifre, Sunucu, Proxy)
- Sohbet Günlükleri

Bir web tarayıcısından gelen bilgiler müşterinin çalışanının gizli ve özel verilerini içerebileceğinden, yalnızca etkileşim için kapsamdaki verilerin yakalanması büyük özen gösterilmelidir. Bu veriler iade edilen verilerden filtrelenmeli ve rapor edilmelidir.

Sistem Yapılandırma

Şifre Politikası

Sistem şifresi politikasını numaralandırarak, mors kuvvet ve çatlak şifreleri kabalaştırma ve çatlak şifreler çok daha verimli hale gelir, örneğin minimum şifre uzunluğunun 8 karakter olduğunu bilerek, 8 karakterden daha az bir kelimeyi sözlükten kaldırabilirsiniz.

Güvenlik Politikaları

Yapılandırılmış Kablosuz Ağlar ve Anahtarlar

Hedefleri kablosuz bilgi olarak bularak, sahadayken şirketler aracılığıyla fiziksel saldırılar başlatmak mümkün olur. Ayrıca, siteden uzaktayken bağlantı kurmak için hedefleri cezbetmek için sahte bir AP kurulmasına izin verebilir.

Yüksek Değer / Profil Hedefleri

Yüksek değer / profil hedefleri, ele geçirilen sistemlerden toplanan verilerin analizi ve bu sistemlerin etkileşimleri ve üzerinde çalışan hizmetlerin analizi ile bu yüksek değer / profilli hedeflerin işleyişi ve etkileşimleri sayesinde bu yüksek değer / profilli hedeflerin bu bakışı, işletmeye kazanılabilecek etkinin belirlenmesinde ve ölçülmesinde ve müşterinin altyapının genel bütünlüğüne göre daha da genişletilebilir.

Veri Kaydırımı

Olası tüm sızdırmazlık yollarının haritalanması

Erişimin sağlandığı alanların her birinden tam bir sızdırma yolu oluşturulmalıdır. Bu, dış dünyaya ulaşmanın ikincil ve yükseklikli yollarını içerir (farklı erişilebilir alt vb.) Haritalama sağlandıktan sonra, gerçek sızdırma testi başlatılmalıdır.

Fermuarlı çıkış yollarını test etmek

Sıfiltrasyon yolları haritalama başına, verilerin test edilmesinden itibaren imha edilmelidir. Bu, önceden Pre-engagementkatılım kapsamına alınmalı ve yeterli altyapı, müşterinin kabul edilebilir katılım politikasına bağlı olan kurulum olmalıydı (yani sızdırılan veriler genellikle test cihazının tam kontrolündeki bir sunucuya sızdırılır ve test edilen kuruluşa doğrudan erişir ve sahiplenilecektir). Sıfatın kendisi, örgütle ilgili Tehdit Modelleme Standardına karşılık gelen tehdit aktörleri tarafından kullanılan gerçek dünya yoklama stratejilerini simüle etmelidir (yani, verilerin zip/7z şifreli dosyaların içinde arşivlendiği ağ içindeki bir sahneleme alanı kullanılarak çoğunlukla "standart" yokuş filitrasyonu varsa, daha sofistike bir tehdit aktörü kullanırsa, o zaman daha sofistike bir tehdit aktörü kullanırsa, bu stratejileri simüle etmek anlamına gelir).

Kontrol güçlü yönlerini ölçmek

Alkış testi yaparken, testin ana amacı, hassas bilgilerin kuruluştan ayrılmasından kaynaklanan tespit ve engellemeye yönelik mevcut kontrollerin gerçekten işe yarayıp yaramadığını ve bu tür uyarılara nasıl tepki verdikleri ve olayların nasıl soruşturulduğu ve hafifletildiği konusunda herhangi bir şey tespit edilmişse, yanıt ekiplerini kullanıp kullanmadığını görmektir.

Kalıcılık

- Kimlik doğrulaması gerektiren arka kapının kurulumu.
- Sisteme geri bağlanmak için hizmetlerin kurulumu ve / veya değiştirilmesi. Kullanıcı ve karmaşık şifre minimum olarak kullanılmalıdır; sertifikaların kullanımı veya kriptografik anahtarlar mümkün olduğunda tercih edilir. (SSH, kanın, RDP). Tek bir IP ile sınırlı ters bağlantılar kullanılabilir.
- Karmaşık şifreli alternatif hesapların oluşturulması.
- Mümkün olduğunda arka kapı yeniden başlatmalardan kurtulmalıdır.

Altyapıya Daha Fazla Penetrasyon

Pivoting, testçinin, müşterinin altyapısındaki diğer sistemlere daha fazla yerleşmek ve erişmek için tehlikeye atılmış sistem üzerindeki varlığını kullanacağı eylemdir. Bu eylem, ele geçirilmiş sisteme yüklenen yerel

kaynak veya araçlar kullanılarak kendi başına emredilmiş ev sahibinden gerçekleştirilebilir.

Uzlaşmalı Sistemden

Uğraştırılmış bir sistemden alınabilecek eylemler:

- Aletleri yükleyin
- Yerel sistem araçlarını kullanın
- ARP Taraması
- Ping Sweep'in
- Dahili ağın DNS Artırılması
- Dizin Hizmetleri Sayım
- Kaba kuvvet saldırıları
- Yönetim Protokolleri ve tehlikeye atılmış kimlik bilgileri (WinRM, WMI, SMB, SNMP.etc)
- Tehlike altındaki kimlik bilgilerinin ve anahtarların kötüye kullanımı (Webpages, Databases..etc)
- Uzaktan İtkili İstismarlar

Yürütülecek eylem, belirli riski göstermek ve / veya müşterinin ağına ve ev sahiplerine daha fazla nüfuz etmek için gereken bilgilere bağlı olacaktır. Düzenli planlama oturumlarının, toplanan bilgilerin yeniden değerlendirilmesi ve belirlenen hedefler karşılanana kadar post sömürüye devam etmek için en iyi yaklaşımı belirlemesi önerilir.

İpli Uzlaşmalı Sistem

Uzlaşılmış bir sistem aracılığıyla yapılabilecek eylemler:

- Liman İlerleme
- Dahili bir ağa (SSH)
- İç ağdan VPN'e
- Uzaktan Sömürüsü Yürütün
- Tehlike altındaki kimlik bilgilerinin ve anahtarların kötüye kullanımı (Webpages, Databases..etc)

Yürütülecek eylem, belirli riski göstermek ve / veya müşterinin ağına ve ev sahiplerine daha fazla nüfuz etmek için gereken bilgilere bağlı olacaktır. Düzenli planlama oturumlarının, toplanan bilgilerin yeniden değerlendirilmesi ve belirlenen hedefler karşılanana kadar post sömürüye devam etmek için en iyi yaklaşımı belirlemesi önerilir.

Temizlik

Temizleme işlemi, penetrasyon testi tamamlandıktan sonra sistemlerin temizlenmesi gereksinimlerini karşılar. Bu, test sırasında kullanılan tüm kullanıcı hesaplarını ve ikilileri içerecektir.

- Tüm yürütülebilir, komut dosyalarını ve geçici dosyaları tehlikeye atılmış bir sistemden çıkarın. Mümkünse dosyaları ve klasörleri kaldırmak için güvenli silme yöntemi.

- Değerlendirme sırasında değiştirildiği durumlarda orijinal değerler sistem ayarlarına ve uygulama yapılandırma parametrelerine geri dönün.
- Tüm arka kapı ve/veya rootkitleri yüklü çıkarın.
- Uzlaşma sistemlerine geri bağlamak için oluşturulan tüm kullanıcı hesaplarını kaldırın.

" http://www.pentest-standard.org/index.php'den alındınız mı? başlık = Post_Disloitasyon&oldid=947"
