Istihbarat Toplantısı

İçerikler

- Finansal
  - Raporlama (L1/L2)
  - Pazar analizi (L1/L2 / L3)
    - Ticaret sermayesi
    - .Değer tarihi
    - EDGAR (SEC)
- Bireysel
  - Çalışan
    - Tarih
    - Sosyal Ağ (SocNet) Profil
    - İnternet Varlığı
    - Fiziksel Konum
    - 1.5 Mobil Ayak İzi
    - "Ücret Için" Bilgi

Kaplı Toplantı

- Kurumsal
  - Konut Toplama
  - Offsite Toplantısı
- HUMINT
  - Sonuçlar

Ayak izi

- Dış Ayak İzleme
  - Müşteri Dış Menzillerini Belirleyin
  - Pasif Keşif
    - WHOIS Aramaları
    - BGP görünümlü gözlük
  - Aktif Ayak İzleme
    - Liman Taraması
    - Pankart Kapma
    - SNP Süpürme
    - Bölge Transferleri
    - SMTP Sıçrama Geri
    - DNS Keşfi
    - İleri / Ters DNS
    - DNS Bruteforce
    - Web Uygulaması Keşfi
    - Sanal Ev Sahibi Tespiti ve Sayım
  - Dış Hedef Listesi Oluşturun
    - Haritalama versiyonları
    - Yama seviyelerini tanımlama
    - Zayıf web uygulamaları aramak
    - Lokavt eşiğinin tanımlanması
- İç Ayak İzleme

Genel

Bu bölüm, bir penetrasyon testinin İstihbarat Toplama faaliyetlerini tanımlar. Bu belgenin amacı, bir hedefe (tipik olarak kurumsal, askeri veya ilgili) karşı keşif yapan pentester için özel olarak tasarlanmış bir standart sağlamaktır. Belge, keşifleri bastırmanın düşünce sürecini ve hedeflerini detaylandırır ve düzgün kullanıldığında, okuyucunun bir hedefe saldırmak için son derece stratejik bir plan üretmesine yardımcı olur.

Arka Plan Kavramları

Seviyeler bu belge için ve bir bütün olarak PTES için önemli bir kavramdır. Pentesting için bir tür olgunluk modelidir. Seviyeleri tanımlamak, zaman, çaba, bilgiye erişim vb. Gibi belirli gerçek dünya kısıtlamaları içindeki beklenen çıktıyı ve faaliyetleri netleştirmemizi sağlar.

İstihbarat Toplama seviyeleri şu anda üç kategoriye ayrılmıştır ve her biri için tipik bir örnek verilir. Bunlar aşağıdaki belgede tekniklerin eklenmesine rehberlik etmelidir. Örneğin, bir facebook profili oluşturmak ve hedefin sosyal ağını analiz etmek gibi yoğun bir etkinlik daha ileri durumlarda uygundur ve uygun düzeyde etiketlenmelidir. Örnekler için aşağıdaki mind haritaya bakın.

Seviye 1 Bilgi Toplama

(düşün: Uyum Saptırma) Esas olarak bir tıklama düğmesi bilgi toplama işlemi. Bu bilgi seviyesi neredeyse tamamen otomatik araçlarla elde edilebilir. Bir PT için IG yaptığınızı söylemek için minimumda.

Acme Corporation'ın PCI / FISMA / HIPAA ile uyumlu olması gerekmektedir. Uyum şartını karşılamak için Seviye 1 bilgi toplama çabası uygun olmalıdır.

Seviye 2 Bilgi Toplaması

(düşün: En İyi Uygulama) Bu seviye, seviye 1 ve bazı manuel analizlerden otomatik araçlar kullanılarak oluşturulabilir. Fiziksel konum, iş ilişkileri, organ çizelgesi vb. Gibi bilgiler de dahil olmak üzere işin iyi anlaşılması.

Widgets Inc'in PCI'ye uygun olması gerekir, ancak uzun vadeli güvenlik stratejileriyle ilgilenir ve birkaç daha küçük widget üreticisi edinir. Seviye 2 bilgi toplama çabası, ihtiyaçlarını karşılamak için uygun olmalıdır.

Seviye 3 Bilgi Toplaması

(Düşün: Devlet Sponsorlu) Daha gelişmiş çatı katı, Redteam, tam kep. Seviye 1 ve seviye 2'den gelen tüm bilgiler ve çok sayıda manuel analiz ile birlikte. SocNet'te ilişki kurmayı düşünün, ağır analiz, iş ilişkilerinin derin anlaşılması, büyük olasılıkla toplantıyı ve korelasyonu gerçekleştirmek için çok sayıda saat.

Bir Ordu Kızıl Ekibi, yabancı bir vatandaş tarafından istismar edilebilecek zayıflıkları bulmak için yabancı bir ülkedeki Ordu ağının bir bölümünü analiz etmek ve saldırmakla görevlendirilir. Bu durumda seviye 3 bilgi toplama çabası uygun olacaktır.

İstihbarat Toplantısı

Ne olduğu

İstihbarat Toplantısı, güvenlik açığı değerlendirmesi ve sömürü aşamalarında hedefe nüfuz ederken kullanılmak üzere mümkün olduğunca fazla bilgi toplamak için bir hedefe karşı keşif yapıyor. Bu aşamada ne kadar çok bilgi toplayabilirseniz, gelecekte o kadar çok saldırı vektörünü kullanabilirsiniz.

Açık kaynak zekası (OSINT), kamuya açık kaynaklardan bilgi bulmayı, seçmeyi ve edinmeyi ve eyleme geçirilebilir istihbarat üretmek için analiz etmeyi içeren bir istihbarat toplama yönetimi biçimidir. [1] (http://en.wikipedia.org/wiki/Open_source_intelligence)

Neden yapıyorsun

Bir organizasyona çeşitli giriş noktalarını belirlemek için Açık Kaynak İstihbaratı toplantısı gerçekleştiriyoruz. Bu giriş noktaları fiziksel, elektronik ve / veya insan olabilir. Birçok şirket, kendi hakkında hangi bilgileri kamuya verdiklerini ve bu bilgilerin kararlı bir saldırgan tarafından nasıl kullanılabileceğini hesaba katmakta başarısız olur. Bunun üzerine, birçok çalışan, kendileri hakkında hangi bilgileri kamuya açık bir şekilde yerleştirdiklerini ve bu bilgilerin kendilerine veya işverenlerine saldırmak için nasıl kullanılabileceğini hesaba katmakta başarısız olur.

Ne değil

OSINT doğru ya da zamanında olmayabilir. Bilgi kaynakları, hatalı verileri yansıtmak için kasıtlı / yanlışlıkla manipüle edilebilir, bilgi zaman geçtikçe eskiyebilir veya sadece eksik olabilir.

Çöplük dalışı veya şirket bilgilerini şirket bilgilerini şirket bilgilerini şirket tarafından üstlenmiyor.

Hedef Seçimi

Hedefin Tanımlanması ve Adlandırılması

Bir hedef kuruluşa yaklaşırken, bir şirketin bir dizi farklı Üst Düzey Alan (TDL) ve yardımcı işletmeye sahip olabileceğini anlamak önemlidir. Bu bilgilerin kapsayıcılık aşamasında keşfedilmesi gerekirken, katılım öncesi aşamada tartışılan ilk kapsamın bir parçası olmamış olabilecek ek sunucu alanlarını ve şirketlerin tanımlanması o kadar da sıra dışı değildir. Örneğin, bir şirketin .com'un TDL'si olabilir. Ancak, .net .co ve .xxx'e de sahip olabilirler. Bunların revize edilmiş kapsamın bir parçası olması gerekebilir veya limitsiz olabilirler. Her iki durumda da test başlamadan önce müşteri ile temizlenmesi gerekir. Ayrıca, bir şirketin altında bir dizi alt şirkete sahip olması da nadir değildir. Örneğin General Electric ve Proctor ve Gamble, daha küçük şirketlere sahip.

Herhangi bir Katılım Kuralı sınırlaması dikkate alın

Bu noktada, Katılım Kuralları'nı gözden geçirmek iyi bir fikirdir. Bunların bir test sırasında unutulması yaygındır. Bazen, testçiler olarak bulduğumuz şeye ve saldırı olasılıklarına o kadar sarılırız ki hangi IP adreslerine, alan adlarına ve ağlara saldırabileceğimizi unuturuz. Her zaman, testlerinizi odaklamak için Angajman Kurallarına atıfta bulunun. Bu sadece bir yasa perspektifinden önemli değil, aynı zamanda bir kapsam sürünme perspektifinden de önemlidir. Testin temel hedeflerinden her kenara çekildiğinizde size pahalıya mal olur. Ve uzun vadede bu şirket parasına mal olabilir.

Test için zaman uzunluğu düşünün

Toplam test için zaman miktarı, yapılabilecek İstihbarat Toplama miktarını doğrudan etkileyecektir. Toplam sürenin iki ila üç ay olduğu bazı testler vardır. Bu angajmanlarda bir test şirketi, temel iş birimlerinin her birini ve şirketin kişiselliğini aramak için muazzam miktarda zaman harcar. Bununla birlikte, daha kısa kristal kutusu tarzı testleri için hedefler çok daha taktiksel olabilir. Örneğin, belirli bir web uygulamasını test etmek, şirket CEO'sunun finansal kayıtlarını araştırmanızı gerektirmeyebilir.

Testin nihai hedefini düşünün

Her testin aklında bir nihai hedef vardır - kuruluşun kritik olarak gördüğü belirli bir varlık veya süreç. Sonun göz önünde bulundurulması, istihbarat toplama aşaması, nihai hedefi çevreleyen tüm ikincil ve yüksek unsurları içerdiğinden emin olmalıdır. Teknolojileri, 3. tarafları, ilgili personeli vb. desteklemek... Odalının kritik varlıklara tutulmasından emin olmak, daha az ilgili istihbarat unsurlarının analiz sürecine müdahale etmemek için önceliksizleştirildiğini ve kategorize edildiğini garanti eder.

OSINT

Açık Kaynak Zekası (OSINT) üç form alır; Pasif, Yarı pasif ve Aktif.

- **Pasif Bilgi Toplama :** Pasif Bilgi Toplama, yalnızca bilgi toplama faaliyetlerinin hedef tarafından asla tespit edilmemesi konusunda çok net bir gereklilik varsa yararlıdır. Bu tür profillemenin teknik olarak zor olması, çünkü hedef kuruluşa hiçbir zaman ev sahiplerimizden biri veya İnternet'teki "anonim" ev sahiplerinden veya hizmetlerinden herhangi bir trafik göndermiyoruz. Bu, yalnızca arşivlenmiş veya depolanmış bilgileri kullanabileceğimiz ve toplayabileceğimiz anlamına gelir. Bu nedenle, bu bilgiler üçüncü bir taraftan toplanan sonuçlarla sınırlı olduğumuz için güncel veya yanlış olabilir.

- **Yarı-pasif Bilgi** Toplama: Yarı pasif bilgi toplama hedefi, normal İnternet trafiği ve davranışı gibi görünecek yöntemlerle hedefi profillemektir. Bilgi için yalnızca yayınlanan isim sunucularını sorguluyoruz, derinlemesine ters aramalar veya kaba kuvvet DNS isteklerini yerine getirmiyoruz, "casuslanmamış" sunucuları veya dizinleri aramıyoruz. Ağ seviyesi bağlantı noktaları veya tarayıcılar çalıştırmıyoruz ve sadece yayınlanan belgelerde ve dosyalarda meta verilere bakıyoruz; aktif olarak gizli içerik aramamak. Buradaki anahtar, faaliyetlerimize dikkat çekmek değil. Mortem sonrası hedef geri dönüp keşif faaliyetlerini keşfedebilir, ancak faaliyeti kimseye geri atamamalıdır.

- **Aktif Bilgi Toplama** : Aktif bilgi toplama, hedef ve şüpheli veya kötü niyetli davranışlar tarafından tespit edilmelidir. Bu aşamada, ağ altyapısını aktif olarak haritalıyoruz (tam bağlantı noktası taramaları nim1-6535 düşünün), açık hizmetleri aktif olarak sıralayan ve / veya güvenlik açığını tararken, yayınlanmamış dizinler, dosyalar ve sunucuları aktif olarak arıyoruz. Bu aktivitenin çoğu, standart çatınağınız için tipik olarak “kazanç” veya “kandıran” aktivitelerinize girer.

Kurumsal

Fiziksel

Lokasyonlar (L1)

Tam adres, mülkiyet, ilgili kayıtların (şehir, vergi, yasal vb) konum listesine göre, konum için tüm fiziksel güvenlik önlemlerinin tam listesi (kamera yerleşimleri, sensörler, çitler, koruma direkleri, giriş kontrolü, kapı, tanımlama türü, tedarikçi girişi, IP blokları / coğrafi konumlara dayalı fiziksel konumlar, vb. ... Hosts / NOC için: Ev sahiplerinin ve ağların tam CIDR notasyonu, ilgili tüm varlıkların tam DNS listesi, AS'nin tam haritalanması, bakım yolları, CDN tedariki, netblot sahipleri (kimlik verileri), e-posta kayıtları (MX + posta adresi yapısı)

- Sahibi (L1/L2)
- Arazi/vergi kayıtları (L1/L2)
- Paylaşılan/bireysel (L1/L2)
- Saat Dilimleri (L1/L2)
- Ev sahipleri / NOC

Yaygınlık (L1)

Bir hedef kuruluşun birden fazla ayrı fiziksel konuma sahip olması nadir değildir. Örneğin, bir bankanın merkez ofisleri olacak, ancak aynı zamanda çok sayıda uzak şubesi de olacak. Fiziksel ve teknik güvenlik merkezi yerlerde çok iyi olsa da, uzak yerler genellikle zayıf güvenlik kontrollerine sahiptir.

İlişkiler (L1)

İşletme ortakları, gümrük, tedarikçiler, kurumsal web sayfalarında, kiralama şirketlerinde vb. Açıkça paylaşılanlar aracılığıyla analiz. Bu bilgiler, iş veya organizasyonel projeleri daha iyi anlamak için kullanılabilir. Örneğin, hedef kuruluş için hangi ürün ve hizmetler kritiktir?

Ayrıca, bu bilgi başarılı sosyal mühendislik senaryoları oluşturmak için de kullanılabilir.

- İlişkiler (L2/L3)
  Seviye 1'den bilgi veterinerlik yapmak için manuel analiz, ayrıca olası ilişkilere daha derine inin.
- Paylaşılan ofis alanı (L2/L3)
- Paylaşılan altyapı (L2/L3)

- Kiralanan / Kiralanan Ekipman (L2 / L3)

Mantıksal

İş ortakları, müşteriler ve rakipler için birikmiş bilgiler: Her biri için iş adı, iş adresi, ilişki türü, temel finansal bilgiler, temel ev sahipleri / ağ bilgilerinin tam bir listesi.

- İş Ortakları (L1/L2 / L3)
  Target'ın reklamı yapılan iş ortakları. Bazen ana www'de reklamı yapılır.
- İşletme Müşterileri (L1 / L2/3)
  Hedefin reklamı yapılan iş müşterileri. Bazen ana www'de reklamı yapılır.
- Rakipler (L1/L2 / L3)
  Hedefin rakipleri kimler. Bu basit olabilir, Ford vs Chevy veya çok daha fazla analiz gerektirebilir.
- Dokunmatik Grafik (L1)
  Bir dokunuş (insanlar arasındaki sosyal bağlantıların görsel temsili) organizasyondaki insanlar arasındaki olası etkileşimlerin haritalandırılmasına ve onlara dışarıdan nasıl erişileceğinin haritalandırılmasına yardımcı olacaktır (bir dokunuş, harici toplulukları içerdiğinde ve 2'nin üzerinde derinlik seviyesiyle yaratıldığında).
  Temel dokunmatik, şimdiye kadar toplanan bilgilerden elde edilen organizasyon yapısını yansıtmalıdır ve grafiğin daha da genişletilmesi ona dayanmalıdır (genellikle organizasyonel varlıklara odaklanmayı daha iyi temsil ettiği ve olası yaklaşım vektörlerini açıkça ortaya koymalıdır.
- Hoovers profili (L1/L2)
  Ne: yarı açık kaynaklı bir istihbarat kaynağı (genellikle ücretli abonelikler). Bu tür kaynaklar, şirketler hakkında iş ile ilgili bilgilerin toplanması ve işletme hakkında “normalleştirilmiş” bir görüş sağlama konusunda uzmanlaşmıştır.
  Neden: Bilgiler fiziksel konumları, rekabetçi manzarayı, anahtar personeli, finansal bilgileri ve diğer iş ile ilgili verileri içerir (kaynak üzerine bağlı). Bu, hedefin daha doğru bir profilini oluşturmak ve testte kullanılabilecek ek personel ve 3. tarafları belirlemek için kullanılabilir.
  Nasıl: İşletme adı ile sitede basit arama, şirketin tüm profilini ve üzerinde mevcut olan tüm bilgileri sağlar. Onları çaprazlamak ve en güncel bilgileri aldığınızdan emin olmak için birkaç kaynak kullanmanız önerilir. (hizmet için ödenir).
- Ürün hattı (L2/L3)
  Hedefin hizmet sunması durumunda ek analiz gerektirebilecek ürün teklifleri, daha fazla analiz gerektirebilir.
- Piyasa Dikey (L1)
  Hedef hangi sektörde bulunur. yani finansal, savunma, tarım, hükümet vb.
- Pazarlama hesapları (L2/L3)
  Pazarlama faaliyetleri hedefin pazarlama stratejisi hakkında çok sayıda bilgi sağlayabilir
  Hedefin sosyal kişilikleri için tüm sosyal medya ağlarını değerlendirin
  Hedefin geçmiş * pazarlama kampanyalarını değerlendirin
- Toplantılar (L2/L3)

Yayınlanan Tutanaklar mı?
Toplantılar halka açık mı?

- Önemli şirket tarihleri (L1 / L2 / L3)
  Yönetim kurulu toplantıları
  Tatiller
  Yıldönümü
  Ürün / hizmet lansmanı

- İş açılışları (L1/L2)
  Bir organizasyondaki iş açılışlarının bir listesini (genellikle web sitelerinin bir 'bakıcılar' bölümünde bulunarak, kuruluş içinde kullanılan teknoloji türlerini belirleyebilirsiniz. Bir örnek, bir kuruluşun Kıdemli Solaris Sysadmin için bir iş açması durumunda, kuruluşun Solaris sistemlerini kullandığı oldukça açık olmasıdır. Diğer pozisyonlar iş unvanına göre açık olmayabilir, ancak açık bir Junior Network Yöneticisi pozisyonu, Cisco veya Juniper teknolojilerini kullandıklarını söyleyen “CCNA tercih ettiği” veya “JNCIA tercih etti” etkisine bir şey söyleyebilir.

- Yardım kuruluşları ilişkileri (L1/L2 / L3)
  Bir hedef kuruluşun yönetici üyelerinin hayırsever kuruluşlarla ilişkilendirilmesi çok yaygındır. Bu bilgiler, yöneticileri hedeflemek için sağlam sosyal mühendislik senaryoları geliştirmek için kullanılabilir.

- RFP, RFQ ve diğer Kamu Teklifi Bilgileri (L1/L2)
  RFP'ler ve RFQ'lar genellikle bir şirket tarafından kullanılan sistem türleri ve hatta altyapılarıyla ilgili boşluklar veya sorunlar hakkında çok fazla bilgi ortaya çıkarır.
  Mevcut teklif kazananlarının kim olduğunu bulmak, kullanılan sistem türlerini veya şirket kaynaklarının yerinde barındırılabileceği bir konumu ortaya çıkarabilir.

- Mahkeme kayıtları (L2/L3)
  Mahkeme kayıtları genellikle ücretsiz veya bazen bir ücret karşılığında kullanılabilir.
  Dava içeriği, eski çalışan davaları da dahil ancak bunlarla sınırlı olmamak üzere geçmiş şikayetçiler hakkında bilgi ortaya çıkarabilir
  Mevcut ve geçmiş çalışanların suç kayıtları, sosyal mühendislik çabalarının bir listesini sağlayabilir

- Siyasi bağışlar (L2/L3)
  Siyasi bağışları veya diğer finansal çıkarları haritalamak, bariz güç pozisyonlarında olmayan ancak kazanılmış bir çıkarı olan (veya içinde kazanılmış bir akrabası olan) tanımlayan önemli bireyleri tanımlamak için önemlidir.
  Siyasi bağış haritalaması, bilgi edinme özgürlüğüne bağlı olarak ülkeler arasında değişecektir, ancak çoğu zaman diğer ülkelerden gelen bağışlar, orada bulunan veriler kullanılarak geri alınabilir.

- Profesyonel lisans veya kayıtlar (L2/L3)
  Hedeflerinizin bir listesini profesyonel lisans ve kayıt şirketleri toplamak, yalnızca şirketin nasıl işlediğine değil, aynı zamanda bu lisansları korumak için izledikleri yönergeler ve düzenlemeler hakkında bir fikir verebilir. Bunun en önemli örneği, ISO standart sertifikasının bir şirketin belirlenmiş yönergeleri ve süreçleri takip ettiğini gösterebileceği bir şirketlerdir. Bir testçinin bu

süreçlerin farkında olması ve organizasyonda yapılan testleri nasıl etkileyebileceklerinden haberdar olması önemlidir.
Bir şirket genellikle bu ayrıntıları web sitelerinde bir onur rozeti olarak listeler. Diğer durumlarda, bir kuruluşun üye olup olmadığını görmek için verilen dikey için kayıt yaptırmak gerekebilir. Mevcut olan bilgiler, şirketin coğrafi konumu kadar dikey pazara ve aynı zamanda çok bağlıdır. Ayrıca, uluslararası şirketlerin farklı lisanslı olabileceği ve ülkeye bağımlı farklı standartlara veya yasal kuruluşlara kaydolmaları gerekebileceğini de belirtmek gerekir.

Org Grafiği (L1)

- Pozisyon tanımlama
  - Organizasyonda önemli kişiler
  - Bireyler özellikle hedef alacak
- İşlemler
  - Organizasyon içindeki değişikliklere eşleştirme (promosyonlar, yanal hareketler)
- İştirakler
  - İşletmeye bağlı olan bağlı kuruluşların haritalanması

Elektronik

Belge Meta Verileri (L1/L2)

- - Ne var? Meta veri veya meta içerik, kapsamdaki veriler / belge hakkında bilgi sağlar. Yazar / yaratıcı adı, saat ve tarih, kullanılan/referanslı standartlar, bir bilgisayar ağındaki konum (iyileştirici / klasör / yönerge yolu / vb. bilgileri) gibi bilgilere sahip olabilir. Bir görüntü için meta verileri renk, derinlik, çözünürlük, kamera yapımı / tip ve hatta koordinatlar ve konum bilgileri içerebilir.
- Neden yapmalısın ki? Metadata önemlidir, çünkü dahili ağ, kullanıcı adları, e-posta adresleri, yazıcı konumları vb. hakkında bilgi içerir ve konumun bir planı oluşturmaya yardımcı olacaktır. Ayrıca ilgili belgelerin oluşturulmasında kullanılan yazılımlar hakkında bilgi içerir. Bu, bir saldırganın bir profil oluşturmasını ve / veya ağlarda ve kullanıcılarda dahili bilgi ile hedefli saldırılar gerçekleştirmesini sağlayabilir.
- Bunu nasıl yapardın? FOCA (GUI tabanlı), metagoofil (piton bazlı), meta-ekstratör, exiftool (düz tabanlı) gibi dosyadan (pdf / kelime / görüntü) çıkarmak için araçlar mevcuttur. Bu araçlar, sonuçları HTML, XML, GUI, JSON vb. olarak farklı formatlarda ayıklama ve görüntüleme yeteneğine sahiptir. Bu araçlara yapılan giriş çoğunlukla ‘müşteri’nin kamu varlığından indirilen ve daha sonra daha sonra hakkında daha fazla bilgi edinmek için analiz edilen bir belgedir. FOCA, belgeleri aramanıza yardımcı olur, GUI arayüzü aracılığıyla hepsini indirin ve analiz eder.

Pazarlama İletişimi (L1/L2)

- Geçmiş pazarlama kampanyaları, hala erişilebilir olabilecek emekli olabilecek

projeler için bilgi sağlar.
- Mevcut pazarlama iletişimleri, çoğunlukla dahili olarak da kullanılan tasarım bileşenleri (Renkler, Yazılar, Grafikler vb.) içerir.
- Dış pazarlama organizasyonları da dahil olmak üzere ek iletişim bilgileri.

Altyapı Varlıkları

sahip olduğu ağ blokları (L1)

- Kuruluşun sahip olduğu Ağ Blokları, tüm aramaları yapmaktan pasif olarak elde edilebilir. DNSStuff.com bu tür bilgileri elde etmek için tek duraktır.
- IP Adresleri için Açık Kaynak aramaları, hedefteki altyapı türleri hakkında bilgi verebilir. Yöneticiler genellikle çeşitli destek sitelerinde yardım talepleri bağlamında adres bilgilerini yayınlarlar.

E-posta adresleri (L1)

- E-posta adresleri, geçerli kullanıcı adları ve etki alanı yapısının potansiyel bir listesini sağlar
- E-posta adresleri, kuruluşların web sitesi de dahil olmak üzere birçok kaynaktan toplanabilir.

Dış altyapı profili (L1)

- Hedefin dış altyapı profili, dahili olarak kullanılan teknolojiler hakkında muazzam bilgiler sağlayabilir.
- Bu bilgiler hem pasif hem de aktif olarak birden fazla kaynaktan toplanabilir.
- Profil, dış altyapıya karşı bir saldırı senaryosu oluşturmada kullanılmalıdır.

Kullanılan teknolojiler (L1/L2)

- Destek forumları, posta listeleri ve diğer kaynaklar aracılığıyla yapılan OSINT aramaları, hedefte kullanılan teknolojilerin bilgilerini toplayabilir
- Tespit edilen bilgi teknolojisi organizasyonuna karşı Sosyal mühendisliğin kullanımı
- Ürün satıcılarına karşı sosyal mühendislik kullanımı

Satın alma anlaşmaları (L1/L2 / L3)

- Satın alma anlaşmaları, hedefte donanım, yazılım, lisans ve ek somut varlık hakkında bilgi içerir.

Uzaktan erişim (L1/L2)

- Çalışanların ve / veya müşterilerin uzaktan erişim için hedefe nasıl bağlandığına dair bilgi edinmek, potansiyel bir giriş noktası sağlar.
- Çoğu zaman uzaktan erişim portalına bağlantı hedefin ana sayfasından kullanılabilir
- Uzaktan kullanıcılar için bağlanmak için uygulamaları / prosedürleri ortaya

çıkarmak için belgeler nasıl

Uygulama kullanımı (L1/L2)

Hedef kuruluş tarafından kullanılan bilinen başvurunun bir listesini toplayın. Bu genellikle halka açık dosyalardan meta veriler çıkarılarak elde edilebilir (daha önce tartışıldığı gibi)

Savunma teknolojileri (L1/L2/L3)

Kullanılmış parmak izi savunma teknolojileri, kullanımdaki savunmalara bağlı olarak çeşitli şekillerde elde edilebilir.

Pasif parmak izi

- Hedef kuruluşun teknisyenlerinin sorunları tartışıyor olabileceği veya kullanımdaki teknoloji hakkında yardım isteyebileceği arama forumları ve halka açık bilgilere
- Hedef organizasyon için arama pazarlama bilgilerinin yanı sıra popüler teknoloji satıcıları
- Satıcı referans sayfalarında veya pazarlama materyalinde listelenip listelenmediğini görmek için hedef organizasyon logosunu kullanarak Tin-eye (veya başka bir görüntü eşleştirme aracı) araması

Aktif parmak izi

- Engellemedeki kalıpları test etmek için halka bakan sistemlere uygun sonda paketlerini gönderin. Belirli WAF tiplerinin parmak izi için çeşitli araçlar vardır.
- Başlık bilgileri hem hedef web sitesinden gelen yanıtlarda hem de e-postalar içinde genellikle yalnızca kullanımdaki sistemlerde değil, aynı zamanda etkinleştirilen belirli koruma mekanizmalarında da bilgi gösterir (örneğin. E-posta ağ geçidi Anti-virüs tarayıcıları)

İnsan kapasitesi (L1 / L2 / L3)

Bir hedef organizasyonun savunmacı insan kapasitesini keşfetmek zor olabilir. Hedef teşkilatın güvenliğini yargılamaya yardımcı olabilecek birkaç önemli bilgi parçası vardır.

- Şirket çapında bir CERT / CSSR / PSTT ekibinin varlığını kontrol edin
- Bir güvenlik pozisyonunun ne sıklıkta listelendiğini görmek için reklamı yapılan işleri kontrol edin
- Güvenliğin güvenlik dışı işler için bir gereklilik olarak listelenip listelenmediğini görmek için reklamı yapılan işleri kontrol edin (örneğin geliştiriciler)
- Hedefin güvenliğinin kısmen veya tamamen dış kaynaklı olup olmadığını görmek için dış kaynak anlaşmalarını kontrol edin
- Güvenlik camiasında aktif olabilecek şirket için çalışan belirli kişileri kontrol edin

Finansal

Raporlama (L1/L2)

Hedef finansal raporlama büyük ölçüde kuruluşun bulunduğu yere bağlı olacaktır. Raporlama, her şube için değil, organizasyon merkezi aracılığıyla da yapılabilir. 2008 yılında SEC, ABD'de Uluslararası Finansal Raporlama Standartlarının (IFRS) kabulü için önerilen bir yol haritası yayınladı.

Ülke Başına UFRS Benimsenme --> http://www.iasplus.com/en/resources/use-of-ifrs

Pazar analizi (L1 / L2 / L3)

- Analist kuruluşlarından (Gartner, IDC, Forrester, 541, vb.) pazar analizi raporları alın. Bu, pazar tanımının ne olduğunu, pazar sınırını, rakipleri ve genel olarak değerleme, ürün veya şirketteki büyük değişiklikleri içermelidir.

Ticaret sermayesi

- Tanımlama, kuruluşun herhangi bir ticaret sermayesi tahsis ettiği ve genel değerleme ve serbest sermayenin yüzde kaçta olduğunu tespit eder. Bu, kuruluşun piyasa dalgalanmalarına ne kadar duyarlı olduğunu ve değerleme ve nakit akışının bir parçası olarak dış yatırıma bağlı olup olmadığını gösterecektir.

Değer tarihi

- Organizasyonun zaman içinde değerlemesinin, dış ve iç olaylar arasında korelasyon oluşturmak ve değerleme üzerindeki etkileri için grafik.

EDGAR (SEC)

- EDGAR (Elektronik Veri Toplama, Analiz ve Alma sistemi) ABD'nin bir veritabanıdır. Yasanın dosyalanması gereken tüm şirketlerin (hem yabancı hem de yerli) kayıt beyanlarını, periyodik raporları ve diğer bilgilerini içeren Güvenlik ve Borsalar Komisyonu (SEC).
- EDGAR verileri önemlidir, çünkü finansal bilgilere ek olarak, bir şirketin web sitesinden veya diğer kamu varlığından başka bir şekilde dikkat çekici olmayan bir şirket içindeki kilit personeli tanımlar. Ayrıca, büyük ortak hisse senedi sahiplerinin yöneticilerinin beyanlarını, isimleri ve adreslerini, şirkete karşı yasal işlemlerin bir özetini, ekonomik risk faktörlerini ve diğer potansiyel olarak ilginç verileri içerir.
- Nasıl elde edilir: Bilgiler SEC'in EDGAR web sitesinde (http://www.sec.gov/edgar.shtml) mevcuttur. Özellikle ilgi duyulan raporlar arasında 10-K (yıllık rapor) ve 10-Q (çocak rapor) yer alıyor.

Bireysel

Çalışan

Tarih

- Mahkeme Kayıtları (L2/L3)

    - Nedir: Mahkeme kayıtları, bir kişi veya çıkar örgütü için veya kuruluşuna karşı cezai ve / veya sivil şikayetler, davalar veya diğer yasal eylemlerle ilgili tüm kamu kayıtlarıdır.
    - Bunu neden yaparsınız: Mahkeme kayıtları, bireysel bir çalışanla veya bir bütün olarak şirketle ilgili hassas bilgileri potansiyel olarak ortaya çıkarabilir. Bu bilgi kendi başına yararlı olabilir veya ek bilgi edinmek için sürücü olabilir. Ayrıca daha sonra penetrasyon testinde sosyal mühendislik veya diğer amaçlar için de kullanılabilir.
    - Nasıl yapacağınız: Bu bilgilerin çoğu artık halka açık mahkeme web siteleri ve kayıt veritabanları aracılığıyla İnternet'te mevcut. Bazı ek bilgiler LEXIS / NEXIS gibi ödeme hizmetleri aracılığıyla kullanılabilir. Bazı bilgiler kayıt talebi veya kişi istekleri yoluyla kullanılabilir.
- Siyasi Bağışlar (L2/L3)
    - Siyasi bağışlar, belirli siyasi adaylara, siyasi partilere veya özel çıkar örgütlerine yönelik bir bireyin kişisel fonlarıdır.
    - Neden yaparsınız: Siyasi bağışlarla ilgili bilgiler potansiyel olarak bir bireyle ilgili yararlı bilgileri ortaya çıkarabilir. Bu bilgi, bireyler ve politikacılar, siyasi adaylar veya diğer siyasi örgütler arasında bağlantı kurmaya yardımcı olmak için sosyal ağ analizinin bir parçası olarak kullanılabilir. Ayrıca daha sonra penetrasyon testinde sosyal mühendislik veya diğer amaçlar için de kullanılabilir.
    - Nasıl yaparsınız: Bu bilgilerin çoğu artık çevrimiçi olarak siyasi bağışları izleyen herkese açık web siteleri (i.e., http://www.opensecrets.org/) aracılığıyla İnternet'te mevcuttur. Belirli bir devletin yasalarına bağlı olarak, belirli bir miktar üzerindeki bağışların genellikle kaydedilmesi gerekir.
- Profesyonel lisans veya kayıtlar (L2/L3)
    - Nedir: Profesyonel lisanslar veya kayıtlar, belirli bir lisansa veya bir topluluk içindeki belirli bir bağlantı ölçüsüne sahip bireyler için üyelerin ve diğer ilgili bilgilerin listelerini içeren bilgilerin depolarıdır.
    - Bunu neden yaparsınız: Profesyonel lisanslarla ilgili bilgiler potansiyel olarak bir bireyle ilgili yararlı bilgileri ortaya çıkarabilir. Bu bilgiler, bir bireyin güvenilirliğini doğrulamak için kullanılabilir (iddia ettikleri gibi gerçekten belirli bir sertifikaya sahipler mi) veya bireyler ve diğer kuruluşlar arasında bağlantı kurmaya yardımcı olmak için sosyal ağ analizinin bir parçası olarak kullanılabilir. Ayrıca daha sonra penetrasyon testinde sosyal mühendislik veya diğer amaçlar için de kullanılabilir.
    - Nasıl yapacağınız: Bu bilgilerin çoğu artık halka açık web siteleri aracılığıyla İnternet'te mevcut. Tipik olarak, her kuruluş çevrimiçi olarak mevcut olabilecek veya toplamak için ek adımlar gerektirebilecek kendi bilgi kayıtlarını korur.

Sosyal Ağ (SocNet) Profili

- Meta Verim Sızıntısı (L2/L3)
    - Fotoğraf Meta Verileri üzerinden konum farkındalığı
- Ton (L2 / L3)
    - Beklenen teslim edilebilir: iletişimde kullanılan tonun öznel tanımlanması - agresif, pasif, çekici, satış, övme, demlenme, alçaltıcı, kibir, elitist, underdog, lider, takipçi, taklit, vb. ...

- Frekans (L2 / L3)
  - Beklenen teslim edilebilir: Yayınların sıklığının tanımlanması (saat / gün / hafta, vb. ...). Ek olarak - iletişimin gerçekleşmeye eğilimli olduğu gün / haftanın zamanı.
- Konum farkındalığı (L2/L3)
  Çeşitli kaynaklardan profillenen kişi için konum geçmişini haritalayın, ister uygulamalarla ve sosyal ağlarla doğrudan etkileşim yoluyla veya fotoğraf meta verileri yoluyla pasif katılım yoluyla.
  - Bing Harita Uygulamaları
  - Dört sualtı
  - Google Latitude
  - Yelp
  - Gowalla
- Sosyal Medya Varlığı (L1/L2/L3)
  Hedefin sosyal medya hesabını/varlığını Doğrula (L1). Ve ayrıntılı analiz sağlayın (L2 / L3)

İnternet Varlığı

- E-posta Adresi (L1)
  - - Ne var? E-posta adresleri, kullanıcıların halka açık posta kutusu kimlikleridir.
  - Neden yapmalısın ki? E-posta adresi toplama veya arama, birden fazla amaca hizmet verdiği için önemlidir - daha sonra erişim için kaba olarak zorlanabilen, ancak daha da önemlisi hedefli spam göndermeye ve hatta otomatik botlara göndermeye yardımcı olan olası bir kullanıcı-yaapması formatı sağlar. Bu spam e-postalar istismarlar, kötü amaçlı yazılımlar vb. içerebilir ve özellikle bir kullanıcıya özel içerikle ele alınabilir.
  - Bunu nasıl yapardın? E-posta adresleri çeşitli web sitelerinden, gruplardan, bloglardan, forumlardan, sosyal ağ portallarından vb. Aranabilir ve çıkarılabilir. Bu e-posta adresleri çeşitli teknoloji destek web sitelerinden de mevcuttur. Belirli bir etki alanına (gerekirse) eşleştirilmiş e-posta adreslerini aramak için hasat ve örümcek araçları vardır.
- Kişisel Kopyalar / Nikeller (L1)
- Kişisel Alan Adı Kayıtlı (L1/L2)
- Asate Statik IP'ler / Netblocks (L1/L2)

Fiziksel Konum

- Fiziksel Konum
  - Hedefin fiziksel konumunu türeyebilir misiniz

Mobil Ayak İzi

- Telefon numarası (L1 / L2 / L3)
- Cihaz tipi (L1 / L2 / L3)
- Kullanım (L1 / L2 / L3)

- Yüklü uygulamalar (L1/L2/L3)
- Sahibi/yöneticisi (L1/L2/L3)

"Ödeme İçin" Bilgi

- Arka plan kontrolleri
- Ödeme Bağlantılı -In
- LEXIS/NEXIS

Örtülü Toplanma

Kurumsal

Konut Toplantısı

Yerinde toplanma için belirli yerleri seçmek ve daha sonra zaman içinde keşif yapmak (yalnızca desenleri sağlamak için en az 2-3 gün). Yerinde istihbarat toplama yaparken aşağıdaki unsurlar aranır:

- Fiziksel güvenlik denetimleri
- Kablosuz tarama / RF frekans taraması
- Çalışan davranış eğitimi denetimi
- Erişilebilir/bitişik tesisler (parçalanmış alanlar)
- Damper dalışı
- Kullanmakta olan ekipman türleri

Site dışı toplanma

Site dışı yerleri ve organizasyonla ilgili önem/ilgilerini belirlemek. Bunlar hem mantıklı hem de aşağıdakilere göre fiziksel konumlardır:

- Veri merkezi konumları
- Ağ tedariki / sağlayıcı

HUMINT

İnsan zekası, başka türlü elde edilemeyen bilgiler sağladığı için varlık üzerinde daha pasif bir şekilde toplanmasını tamamlar ve zeka resmine daha fazla "kişisel" bakış açıları ekler (düşmanlar, tarih, anahtar bireyler arasındaki ilişkiler, "atmosfer" vb.)

İnsan zekası elde etme metodolojisi her zaman doğrudan etkileşimi içerir - ister fiziksel ister sözlü olsun. Toplanma, söz konusu varlığın en uygun bilgi maruziyetini ve işbirliğini elde etmek için özel olarak oluşturulacak varsayılan bir kimlik altında yapılmalıdır.

Ek olarak, daha hassas hedefler üzerinde istihbarat toplanması, yalnızca gözlemi kullanarak gerçekleştirilebilir - tekrar fiziksel olarak veya elektronik / uzaktan araç (CCTV, web kameraları vb.)

aracılığıyla gerçekleştirilebilir. Bu genellikle davranış kalıpları oluşturmak için yapılır (ziyaret sıklığı, kıyafet kodu, erişim yolları, kahve dükkanları gibi ek erişim sağlayabilecek kilit konumlar gibi).

Sonuçlar

- Anahtar Çalışanlar
- Ortaklar/Tedarikçiler
- Sosyal Mühendislik

Ayak izi

NEDİR: Ayak izi olarak da bilinen dış bilgi toplama, organizasyona dış perspektiften bilgi edinmek için hedefle etkileşimden oluşan bir bilgi toplama aşamasıdır.

NEDEN: Hedeflerle etkileşim kurarak çok fazla bilgi toplanabilir. Bir hizmeti veya cihazı araştırarak, genellikle çubuğunun veya daha basit bir şekilde, cihazı tanımlayacak bir afişin temin edilebileceği senaryolar oluşturabilirsiniz. Hedefleriniz hakkında daha fazla bilgi toplamak için bu adım gereklidir. Bu bölümden sonra hedefiniz öncelikli bir hedef listesidir.

Dış ayak izi

Müşteri Harici Aralıklarını Belirleyin

Bir penetrasyon testi sırasında istihbarat toplanmasının en büyük hedeflerinden biri, kapsamda olacak ev sahiplerini belirlemektir. Sistemleri tanımlamak için kullanılabilecek bir dizi teknik vardır, ters DNS aramaları, DNS bruting, SONOF alanlarda ve aralıklarda aramalar dahil. Bu teknikler ve diğerleri aşağıda belgelenir.

Pasif Keşif

WHOIS Lookups'ın

Dış ayak izi için, önce DSÖIS sunucularından hangisinin peşinde olduğumuz bilgileri içerdiğini belirlememiz gerekir. Hedef alan için TLD'yi bilmemiz gerektiği göz önüne alındığında, hedef alan adının kayıtlı olduğu Kayıt Defteri'ni bulmak zorundayız.

WHOIS bilgileri bir ağaç hiyerarşisine dayanır. ICANN (IANA) tüm TLD'ler için yetkili kayıttır ve tüm manuel WHOIS sorguları için harika bir başlangıç noktasıdır.

- ICANN - http://www.icann.org
- IANA - http://www.iana.com
- NRO - http://www.nro.net
- AFRINIC - http://www.afrinic.net
- APNIK - http://www.apnic.net
- ARIN - http://ws.arin.net
- LACNIC - http://www.lacnic.net

- RIPE - http://www.ripe.net

Uygun Kayıt şirketi sorgulandıktan sonra, Kayıt Defter bilgilerini elde edebiliriz. WHOIS bilgilerini sunan çok sayıda site vardır; ancak belgelerde doğruluk için yalnızca uygun Kayıt Defteri kullanmanız gerekir.

- InterNIC - http://www.internic.net/ http://www.internic.net]

Tipik olarak, ARIN'e karşı basit bir kim sizi doğru kayıt memuruna yönlendirir.

BGP görünümlü gözlükler

Border Gateway Protokolü'ne (BGP) katılan ağlar için Özerk Sistem Numarasını (ASN) belirlemek mümkündür. BGP rota yolları dünya çapında ilan edildiğinden, bunları bir BGP4 ve BGP6 görünümlü cam kullanarak bulabiliriz.

- BGP4 - http://www.bgp4.as/Look-glasses (http://www.google.com/url?q=http%3A%2F%2Fwww.bgp4.as%2Flooking-glasses&sa=D&sntz=1&usg=AFQjCNGJNLNRaL6xeGcya4mZ9NPyOFd8Tg)
- BPG6 - http://lg.he.net/ (http://lg.he.net/)

Aktif Ayak İzi

Liman Taraması

Liman tarama teknikleri, test için mevcut olan süreye ve gizli olma ihtiyacına göre değişecektir. Sistemler hakkında sıfır bilgi varsa, sistemleri tanımlamak için hızlı bir ping taraması kullanılabilir. Buna ek olarak, ping doğrulaması olmadan hızlı bir tarama (n haritasında - PN) en yaygın limanları tespit etmek için çalıştırılmalıdır. Bu tamamlandıktan sonra, daha kapsamlı bir tarama yapılabilir. Bazı testçiler sadece açık TCP bağlantı noktalarını kontrol eder, UDP'yi de kontrol ettiğinizden emin olun. http://nmap.org/nmap_doc.html belge bağlantı noktası tarama tiplerini detaylandırır. Nmap ("Network Mapper"), ağ denetimi / tarama için fiili standarttır. Nmap hem Linux hem de Windows'ta çalışır.

PTES Teknik Kılavuzunda (http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines#Nmap_.28Windows.2FLinux.29) Nmap'ın bu amaçla kullanımı hakkında daha fazla bilgi bulabilirsiniz (http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines#Nmap_.28Windows.2FLinux.29)

Nmap'ın onlarca seçeneği var. Bu bölüm liman taramasıyla uğraştığı için bu görevi yerine getirmek için gereken komutlara odaklanacağız. Kullanılan komutların esas olarak taranan ana bilgisayarların zamanına ve sayısına bağlı olduğunu belirtmek önemlidir. Bu görevleri yerine getirmek için ne kadar çok ev sahibiniz varsa veya daha az zaman, ev sahibini o kadar az sorgulayacağız. Bu, seçenekleri tartışmaya devam ettikçe belirginleşecek.

IPv6 da test edilmelidir.

Banner Kapma

Banner Kapma, bir ağdaki bilgisayar sistemleri ve açık limanlarını çalıştıran hizmetler hakkında bilgi toplamak için kullanılan bir numaralandırma tekniğidir. Banner kapma, ağ, hedef akranın çalıştığı uygulamaların ve işletim sisteminin kullanımını tanımlamak için kullanılır.

Banner kapma genellikle Hyper Text Transfer Protocol (HTTP), Dosya Aktasyonu Protokolü (FTP) ve Basit

Posta Transfer Protokolü (SMTP) üzerinde yapılır; bağlantı noktaları sırasıyla 80, 21 ve 25. Afiş kapma işlemini gerçekleştirmek için yaygın olarak kullanılan araçlar Telnet, harita ve Netcat'tir.

SNP Süpürme

SNMP süpürmeleri, belirli bir sistem hakkında tonlarca bilgi sunduğu için de gerçekleştirilir. SNMP protokolü vatansız, verigram odaklı bir protokoldür. Ne yazık ki SNMP sunucuları taleplere geçersiz topluluk dizeleriyle yanıt vermiyor ve altta yatan UDP protokolü kapalı UDP limanlarını güvenilir bir şekilde rapor etmiyor. Bu, sondalanan bir IP adresinden gelen "cevap yok" aşağıdakilerden herhangi biri anlamına gelebileceği anlamına gelir:

- makineye ulaşılamaz
- SNMP sunucusu çalışmıyor
- Geçersiz topluluk ipi
- Yanıt verigramı henüz gelmedi

Bölge Transferleri

AXFR olarak da bilinen DNS bölgesi transferi, bir DNS işlemi türüdür. DNS verilerini bir dizi DNS sunucusunda içeren veritabanlarını çoğaltmak için tasarlanmış bir mekanizmadır. Bölge transferi iki lezzette gelir, tam (AXFR) ve artımlı (IXFR). DNS bölgesi aktarımını gerçekleştirme yeteneğini test etmek için mevcut çok sayıda araç vardır. Bölge transferlerini gerçekleştirmek için yaygın olarak kullanılan araçlar konak, kazma ve haritadır.

SMTP Sıçrama Geri

SMTP, teslimatsız Rapor / Makbuz (NDR), (başarısız) bir Teslimat Bildirimi (DN) mesajı, Teslimatsız Bildirim (NDN) veya basitçe bir sıçrama olarak da adlandırılan SMTP geri dönüşü, bir posta sisteminden bir teslimat sorunu hakkında başka bir mesajın göndereni bilgilendiren otomatik bir elektronik posta mesajıdır. Bu, SMTP sunucusunun parmak izin parmak izinde bir saldırgana yardımcı olmak için kullanılabilir, çünkü yazılım ve sürümler de dahil olmak üzere SMTP sunucu bilgileri bir sıçrama mesajında dahil edilebilir.

Bu, hedefin etki alanında sahte bir adres oluşturarak yapılabilir. Örneğin, asDFADSF_garbage_address@target.com, target.com test etmek için kullanılabilir. Gmail, başlıklara tam erişim sağlar ve test cihazları için kolay bir seçim yapar.

DNS Keşif

DNS keşfi, etki alanının yetkili adakçısı için WHOIS kayıtlarına bakarak gerçekleştirilebilir. Ek olarak, ana alan adının varyasyonları kontrol edilmelidir ve web sitesi, hedefin kontrolü altında olabilecek diğer alan adlarına referanslar için kontrol edilmelidir.

İleri / Ters DNS

Ters DNS, bir organizasyon içinde kullanımda geçerli sunucu adlarını elde etmek için kullanılabilir. Bir adı, sağlanan bir IP adresinden bir adı çözmesi için bir PTR (ters) DNS kaydına sahip olması gerektiğine dair bir uyarı vardır. Eğer karar verirse, sonuçlar geri verilir. Bu genellikle herhangi bir sonuç döndürüp döndürmediğini görmek için sunucuyu çeşitli IP adresleriyle test ederek gerçekleştirilir.

DNS Bruteforce

Müşteri etki alanıyla ilişkili tüm bilgileri belirledikten sonra, artık DNS sorgulamaya başlama zamanıdır. DNS, IP adreslerini ana bilgisayarlara haritalamak için kullanıldığından ve bunun tersi de güvenli bir şekilde yapılandırılıp yapılandırılmadığını görmek isteyeceğiz. Müşteri hakkında ek bilgi vermek için DNS'yi kullanmaya çalışacağız. DNS'yi içeren en ciddi yanlış yapılandırmalardan biri, İnternet kullanıcılarının bir DNS bölgesi aktarımı gerçekleştirmesine izin vermektir. DNS'yi numaralandırmak için kullanabileceğimiz birkaç araç var, sadece bölge transferlerini gerçekleştirme yeteneğini kontrol etmekle kalmaz, aynı zamanda yaygın olarak bilinmeyen ek ana bilgisayar adlarını da keşfedebilirsiniz.

Web Uygulaması Keşfi

Zayıf web uygulamalarını tanımlamak, bir penetrasyon testi sırasında özellikle verimli bir etkinlik olabilir. Aranacak şeyler arasında yanlış yapılandırılmış OTS uygulamaları, eklenti işlevselliğine sahip OTS uygulaması (dalgalar genellikle taban uygulamadan daha savunmasız kod içerir) ve özel uygulamalar bulunur. WAFP gibi web uygulama parmak izleri burada büyük bir etki için kullanılabilir.

Sanal Evre Algılama ve Sayım

Web sunucuları genellikle tek bir sunucuda işlevselliği pekiştirmek için birden fazla "sanal" ana bilgisayar barındırır. Birden fazla sunucu aynı DNS adresine işaret ederse, aynı sunucuda barındırılabilir. MSN araması gibi araçlar, bir ip adresini bir dizi sanal ana bilgisayara haritalamak için kullanılabilir.

Dış Hedef Listesi Oluşturun

Yukarıdaki faaliyetler tamamlandıktan sonra, kullanıcılar, e-postalar, etki alanları, uygulamalar, ev sahipleri ve hizmetlerin bir listesi derlenmelidir.

Haritalama versiyonları

Sürüm kontrolü, uygulama bilgilerini tanımlamanın hızlı bir yoludur. Bir dereceye kadar, hizmetlerin sürümleri harita kullanılarak parmak izi alınabilir ve web uygulamalarının sürümleri genellikle keyfi bir sayfanın kaynağına bakarak toplanabilir.

Yama seviyelerinin tanımlanması

Hizmetlerin yama seviyesini dahili olarak tanımlamak için, sürümler arasındaki farklar için sistemi sorgulayacak yazılım kullanmayı düşünün. Müşterinin kabul etmesi koşuluyla, penetrasyon testinin bu aşaması için kimlik bilgileri kullanılabilir. Güvenlik açığı tarayıcıları, yama seviyelerini kimlik bilgileri olmadan uzaktan tanımlamada özellikle etkilidir.

Zayıf web uygulamaları aramak

Zayıf web uygulamalarını tanımlamak, bir penetrasyon testi sırasında özellikle verimli bir etkinlik olabilir. Aranacak şeyler arasında yanlış yapılandırılmış OTS uygulamaları, eklenti işlevselliğine sahip OTS uygulaması (dalgalar genellikle taban uygulamadan daha savunmasız kod içerir) ve özel uygulamalar bulunur. WAFP gibi web uygulama parmak izleri burada büyük bir etki için kullanılabilir.

Lokavt eşiğinin tanımlanması

Bir kimlik doğrulama hizmetinin kilitleme eşiğinin belirlenmesi, kaba kuvvet saldırılarınızın testiniz sırasında geçerli kullanıcıları kasıtlı olarak kilitlemediğinden emin olmanızı sağlayacaktır. Çevredeki tüm farklı kimlik doğrulama hizmetlerini belirleyin ve lokavt için tek, zararsız bir hesabı test edin. Genellikle 5 - 10 geçerli bir hesabın denemesi, hizmetin kullanıcıları kilitleyip kilitlemeyeceğini belirlemek için yeterlidir.

Dahili Ayak İzi

Pasif Keşif

Test cihazının dahili ağa erişimi varsa, paket koklama çok fazla bilgi sağlayabilir. Sistemleri tanımlamak için panf'de uygulanan teknikler gibi teknikleri kullanın.

Müşteri İç Menzillerini Tanımlayın

Dahili testler yaparken, önce yerel alt ağınızı numaralandırın ve adresi hafifçe değiştirerek oradan diğer alt ağlara tahmin edebilirsiniz. Ayrıca, bir iç ev sahibinin rotasyon masasına bir bakış özellikle anlatabilir. Aşağıda kullanılabilecek bir dizi teknik bulunmaktadır.

DHCP sunucuları sadece yerel bilgilerin değil, aynı zamanda uzak IP aralığının ve önemli ana bilgisayarların ayrıntılarının da potansiyel bir kaynağı olabilir. DHCP sunucularının çoğu, yerel bir IP ağ geçidi adresinin yanı sıra DNS ve WINS sunucularının adresini de sağlayacaktır. Windows tabanlı ağlarda, DNS sunucuları Active Directory etki alanı denetleyicileri ve dolayısıyla ilgi çekici olma eğilimindedir.

Aktif Keşif

Dahili aktif keşif, harici bir kişinin tüm unsurlarını içermelidir ve ek olarak aşağıdaki gibi intranet işlevselliğine odaklanmalıdır:

- Dizin hizmetleri (Aktif Dizin, Novell, Güneş vb.)
- İşletme işlevselliği sağlayan Intranet siteleri
- Kurumsal uygulamalar (ERP, CRM, Muhasebe vb.)
- Hassas ağ segmentlerinin tanımlanması (konut, Ar-Ge, pazarlama vb.)
- Üretim ağlarına erişim (veranticenters)
- VoIP altyapısı
- Kimlik doğrulaması (kerberos, çerez jetonları vb.)
- Proxying ve internet erişim yönetimi

Koruma Mekanizmalarını Tanımlayın

Aşağıdaki unsurlar, kapsamda ilgili konum/grup/taşıyıcılara göre tanımlanmalı ve haritalandırılmalıdır. Bu, gerçek saldırıyı gerçekleştirirken kullanılacak güvenlik açığı araştırma ve sömürüsünün doğru uygulanmasını sağlayacaktır - böylece saldırının verimliliğini en üst düzeye çıkararak ve tespit oranını en aza indirecektir.

Ağ Tabanlı Korumalar

- "Basit" paket filtreler
- Trafik Şekillendirme Cihazları
- DLP Sistemleri
- Şifreleme / Tünelleme

Ev Sahibi Tabanlı Korumalar

- Yığın / Ağartma Korumaları
- Uygulama Beyaz Listeleme
- AV/Boşlama/Davranış Analizi
- DLP Sistemleri

Uygulama Seviyesi Korumaları

- Uygulama Korumalarını Belirleyin
- Kodlama Seçenekleri
- Potansiyel Bypass Caddeleri
- Beyaz Listeye Alınan Sayfalar

Depolama Korumaları

- HBA - Ev Sahibi Seviyesi
- LUN Maskeleme
- Depolama Denetleyicisi
- iSCSI CHAP Sırrı

Kullanıcı Korumaları

- AV/Spam Filtreleme Yazılımı
  Sömürülebilirliği sınırlayan SW Yapılandırma antispam / antiAV olarak kabul edilebilir

" http://www.pentest-standard.org/index.php'den alındınız mı? başlık = Intelligence_Gathering&oldid=953 "

Bu sayfa en son 6 Ekim 2014 tarihinde 20:21 tarihinde düzenlenmiştir.

İçerik, aksi belirtilmedikçe GNU Serbest Dokümanlık Lisansı 1.2 kapsamında mevcuttur.