Sızma Testi Hizmeti

Sistemlerinizi Daha Güvenilir Kılmak için
En Az Yılda Bir Sızma Testinizi Biz Yapalım

Bilgi'nin temel güvenlik özellikleri olan Gizlilik, Bütünlük ve Erişilebilirlik özelliklerinin korunması çok kritik ve kaçınılmazdır. Bu özelliklerden herhangi birinin zarar görmesi etki seviyesine göre kuruma zarar verir. Bu sebeple bilginin işlendiği sistemler ve uygulamalar düzenli olarak güvenlik testlerine tabi tutulmak suretiyle dışarıdan ve içeriden gelebilecek saldırılara karşı, bu sistem ve uygulamalardaki zafiyetler tespit edilerek kapatılmalıdır.

Bilgi Birikim Sistemleri 30 yıldır bilişim sektöründe hizmet veren, ülkemizin önde gelen Bilgi Teknolojileri sistem entegratörlerindendir. Güvenlik konusunda TSE A Tipi Sızma Testi Sertifikasına sahip nadir firmalardan biridir. Bu sertifikasyona sahip olmak için tüm şirket kurucu ortakları ve Sızma Testi personelleri TSE güvenlik kontrolleri ve sıkı testlerinden geçmişlerdir. Zorlu bir süreç sonrası alınan bu belge gereği her yıl TSE tarafından düzenli olarak yapılan denetimlerden de geçme zorunluluğu vardır.

Kamu kurum ve kuruluşlar ile özel sektör firmaların Sızma Testi Şartnamelerinde yer alan TSE A Tipi Sızma Testi Sertifikası şartını yerine getirerek birçok projeler alınmış ve başarıyla tamamlanmıştır. BBS Sızma Testi Ekibi bu projelerden edindiği tecrübelerle kendini her daim geliştirmekte ve yetkinlik düzeyini sürekli artırmaktadır.

Hizmet İçeriği

- Internet (Dış Ağ) Sızma Testi
- Intranet (Yerel Ağ) ve Veri Tabanı Sızma Testi
- Kablosuz (Wireless) Ağ Zafiyet Testi
- Web Uygulama Güvenlik Testi
- Sosyal Mühendislik ve Son Kullanıcı Farkındalık Testi
- Servis Dışı Bırakma (DOS/DDOS) Testi
- Mobil Uygulama Testi
- Doğrulama Testi

Uygulanan Metodoloji

BBS Güvenlik Değerlendirmesi Raporu hazırlanırken konu hakkındaki uluslararası standartlar incelenmiş ve azami ölçüde faydalanılmıştır. OWASP Testing Guide v3, OSSTM, ISSAF, NIST, Gerçekleştirilen testler uluslararası standart ve yönetmeliklere (ISO/IEC 27001, ISAE 3402, NIST, SoX, SAS 70) tam uyumludur.

Bilgi Toplama Aşaması

Kapsamlı bir güvenlik değerlendirmesi için hedef hakkında olası tüm bilgileri toplamak adına İnternet üzerinden teknik (whois/dns sorguları) ve teknik olmayan (arama motorları, haber grupları, e-posta listeleri sosyal ağlar vb.) yöntemler kullanılarak, hedef şirket veya sistem hakkında bilgi sağlanır.

Ağ Topolojisi Çıkarma Aşaması

Hedef sistem üzerinde port ve servis taraması, açık sistemlerin belirlenmesi, açık sistemler üzerindeki açık portların ve servislerin belirlenmesi, sistemler üzerinde hangi işletim sistemlerinin ve servislerin çalıştığının belirlenmesi, işletim sistemlerine, servislere ve uygulamalara ait versiyon bilgilerinin tespiti, sistemlerde kullanılan donanım/yazılımların ve versiyonlarının tespit edilmesi, Router, Firewall, IPS gibi ağ cihazlarının tespiti gerçekleştirilerek detaylı bir ağ haritası çıkarılır.

Enumerating Aşaması

Canlı olduğu tespit edilen sistemlerde TCP/UDP port tarama işlemi gerçekleştirilir. Açık portları hangi servislerin kullandığı, bu servislerin hangi üreticiye ait olduğu, versiyonları gibi bilgiler “banner grabbing” yöntemi ile öğrenilir ve emin olunduktan sonra zafiyet veri tabanları taranır ve bilinen zafiyetler tespit edilir.

Router, switch gibi aktif ağ cihazların üzerinde çalışan işletim sistemleri, bu işletim sistemlerin versiyonları, cihazlar üzerindeki servisler, yönlendirme protokolleri, yönetimsel amaçlı servisler ve versiyonları tespit edilmeye çalışılır ve zafiyet veri tabanında inceleme yapılır. Cihazlar üzerinde koşan gereksiz servislerin, ön-tanımlı kullanıcı adı veya şifre bilgileri veya yönetim için kullanılan güvensiz protokollerin tespiti raporlanır.

Zafiyet Tarama Aşaması

Hedef sisteme zarar vermeyecek zafiyetler tanımlamak ve bilinen istismarlarla sömürmek için çeşitli otomatik zafiyet tarama araçlarıyla taramalar gerçekleştirilir; Hedef sistemlere sızma yolları ve senaryoları belirlenir.

Hak Elde Etme Aşaması

Hedef sistem üzerindeki güvenlik önlemleri aşılarak erişim elde edilmeye ve mümkün olduğunca bağlantı (reverse, bind) sağlanmaya çalışılır. Tanımlanan zafiyetlerin istismarı için uygun PoC kodları/araçları kullanılarak veya yazılarak hedef sistem üzerinden testler gerçekleştirilir.

Hak Yükseltme Aşaması

Hedef sistem üzerinde tespit edilen servislerde kullanıcı adı/parola kombinasyonlarının keşfi, sistem hesaplarına yönelik boş veya varsayılan parolaların bulunması, kullanılan uygulama ve donanım cihazlarının varsayılan ayarlarda bulunması gibi zafiyetler istismar edilerek hedef sistem üzerinde erişim elde edilir. Hedef sisteme erişim sonrası çeşitli exploitler denenerek root, administrator, SYSTEM gibi yetkili kullanıcı profiline geçilmeye çalışılır.

Başka Sistemlere Sızma Aşaması

Erişim yapılan sistemlerden şifreli kullanıcı bilgilerin alınarak daha hızlı bir ortamda denenir. Sızılan sistemde zehirleme araçları çalıştırılabiliyorsa ana sisteme erişim yapan diğer kullanıcı/sistem bilgileri elde edilir.

Sistemde Kalıcı Olma Aşaması

Sisteme girişin başkaları tarafından belirlenmemesi için test süresince yetkili sistemler üzerine arka kapılar yerleştirilir, fark edilmeyecek şekilde yetkili hesaplar tanımlanır.

Temizlik Aşaması

Hedef sistemlere bırakılmış arka kapılar, test amaçlı script’ler, sızma testleri için eklenmiş çalışmalar temizlenir ve sistem akışı ilk haline getirilir.

İstemci Sızma Testi

İstemcilerin yapılandırmaları incelenerek mantık hataları ve eksiklikler kontrol edilir.

Veritabanı Zafiyet Testi

Veri tabanlarına özel güvenlik taramaları gerçekleştirilir. Varsayılan konfigürasyondan kaynaklı zafiyetlerden eksik güncellemelere, ön tanımlı şifrelerin tespitine kadar birçok veri tabanı sistemlerine özel açıklar tespit edilir.

Kablosuz Ağ Sızma Testi

Opsiyonel olarak sunulan bu test adımında kapsamındaki wireless sistemleri için asgari aşağıdaki güvenlik denetimleri gerçekleştirilir.

- WLAN Şifre Tespiti ve Şifre Kırma
- WLAN Dinleme ve Araya Girme
- WLAN Zayıflık Tarama
- WLAN Yapılandırma Kontrolü

Adres: Yeni Sahra Mah. Fatih Cad. No: 8 Ataşehir / İstanbul P.K 34746
T: +90 (216) 373 98 00
F: +90 (216) 373 99 93