BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI

BİLİŞİM TEKNOLOJİLERİ TEST MÜDÜRLÜĞÜ

SIZMA TESTİ KAPSAMI

GİZLİ /CONFIDENTIAL

Kuruluşun adı	
Adresi	
İrtibattan sorumlu kişi	
Tel.	
E-Posta	

SIZMA TESTİ KAPSAMI

Sızma Testi kapsamı

Kurum bilgi teknolojileri ve internet iletişimi ağı ve bileşenlerinin risk seviyesinin ölçülmesi ve raporlanması amacıyla sızma testleri yapılacaktır.

Bu kapsamda siber suçlular tarafından kullanıldığı bilinen araç ve teknikler kullanılarak Kurum bilgi güvenliği seviyesi değerlendirilecektir. Yapılan çalışmalar sonucunda ortaya çıkan zafiyetler detaylı olarak raporlanacak ve zafiyet giderme önerileri sunulacaktır. Tespit edilen zafiyetlerin giderilmesinden sonra gerekli kontrol testlerinin yapılması da bu işin kapsamındadır.

Test Uyumluluk kapsamı

Bu kapsamda yapılacak testler TS 13638 (Information technology - Security techniques - The requirements for personnel and companies conducting penetration tests) standardına uyumlu olarak gerçekleştirilecektir.

Uygulanacak sızma testi kapsamı hakkında ayrıntılı bilgi aşağıda verilmiştir.

Kapsamdaki testler

Sızma testi kapsamında testler 2 ana vektör üzerinden yapılacaktır:

- İç ağdan yapılacak sızma testleri: Kurum ağının içinde bir erişim noktası kullanılarak yerel ağ ve bu ağa bağlı sistemler test edilecektir.
- Dış ağdan yapılacak sızma testleri: Kurum'a ait ve internet üzerinden erişilebilen sistemlerin test edilecektir.

LÜTFEN YAPTIRMAK İSTEDİĞİNİZ TEST TÜRLERİNİN VE SEÇİMLİ TESTLERİNİN YAYINDAKİ KUTUCUKLARI İŞARETLEYİNİZ.

1. SIZMA TESTİ

Testler sırasında aşağıda temel aşamaları verilmiş yöntemler izlenerek en az aşağıdaki testler yapılacaktır.

1.1. ☐ BEYAZ KUTU

☐ Bilgi işlem personeli desteği ile (Testler esnasında test ekibine gerekli olabilecek bilgiyi sağlamak üzere görevlendirilecek personellerin olması durumu)

☐ Bilgi işlem personeli desteği olmadan

1.1.1. ☐ AĞ

1.1.1.1. Pasif Keşif

- Ağ trafiğini dinleme
- Pasif istihbarat teknikleri ile varlık ve zafiyet tespiti
  - Kurum'un internet üzerindeki varlığının tespit edilmesi
  - Arama motorları kullanımı
- Aktif istihbarat teknikleri ile varlık ve zafiyet tespiti

1.1.1.2. Aktif Keşif (Tarama)

- Aktif cihazların tespiti
- Aktif cihazlarda açık portların tespiti
- İşletim sistemi tespit etme
- Açık portlarda çalışan servisleri ve versiyonlarını tespit etme

1.1.1.3. Zafiyet Tarama

- İçten tarama
- Test eden personelin etki alanına dahil edilerek iç ağ tarama işleminin gerçekleştirilmesidir.
- Dıştan tarama
- Ağdaki istemcilerin ve/veya sunucuların dışarıya açık profilleri taranır.
- Zafiyet tarayıcı ile yapılan tarama ile bir önceki taramada yapılan çıktılar doğrulanır

1.1.1.4. ☐ İstismar Etme

- Cihazların (ftp, ssh, telnet gibi) fabrika çıkışı (default) kullanıcı ve parolaların denenmesi
- Bir önceki aşamada zafiyet tarayıcı ile bulunan zafiyetlerin istismarı için istismar veritabanları ve Metasploit kullanımı
- Windows LM/NTLM zayıflığı tespit etmeye çalışma
- Ağı dinleme ve ortadaki adam saldırısı
- Aktif dinleme

- MAC seli oluşturma
- ARP zehirleme
- DHCP zehirleme
- SSL trafiğini dinleme
- Etki alanı sızma testi aşamaları
- Keşif
- İstismar

1.1.1.5. ☐ Zayıf şifrelerin kırılması

- Sözlük saldırısı
- Bir sözlükteki bütün kelimelerin sistemde kullanıp kullanılmadığını test eder. Sözlük kuruma özel anahtar kelimeleri de içerir.
- Bütünleşik kaba kuvvet saldırısı
- Sözlük saldırısındaki kelimelere rakam ya da sembolik karakterlerin eklenmesi ile hedef sistemin şifreleri test edilir. (Örneğin password yerine p@ssw0rd denenmesi)
- Kaba kuvvet saldırısı
- Belli bir uzunluğa kadar mümkün olan tüm şifreleri ve karşılığı olan hash özetlerini test etmemizi sağlar.
- Gökkuşağı tabloları
- Belli bir uzunluktaki şifrelerin her bir karakteri için test edilmesini içerir.

1.1.1.6. ☐ İstismar Sonrası İşlemler

- Yetki yükseltme ve erişimi sürdürme (Etki alanını ele geçirme)
- Veri toplama (AD Explorer ile)
- İç ağın haritasını çıkarmaya başlama
- Pivoting ile yeni sistemler istismar etme

1.1.1.7. Durum Kayıtlarını Temizleme

- Log kayıtlarının sistem yöneticisi tarafından silinmesi
- Sızma testi makinelerinin test yapan personeller tarafından temizlenmesi

1.1.2. ☐ KABLOSUZ AĞ TARAMA

Bu bölümde 802.1 a/b/g/n kanallarında çalışan sadece kurum kablosuz cihazları taranır.

- Kablosuz tarayıcının menzilinde bulunan yetkisiz kablosuz cihazları teşhis etmek
- Lokasyon tespiti ve kablosuz sinyalin sınırlarını belirleme. Sokaklara, kamuya açık bölgelere yakınlığı kısaca insanların yoğun olduğu yerlerden izolesi gerekir.
- Potansiyel arka kapı ve diğer güvenlik ihlallerini bulmak

- Tarama ile tespit edilen cihazlarda zafiyet taranması: Kablosuz cihazların güvenlik yapılandırmasının kontrolü (auth mekanizması, data encryption, admin erişimi eğer bu bilgiler başka şekilde elde edilemediyse)
- Kullanılan kriptoloji algoritması tespiti WEP/WPA2
- *Misafir Ağı ile yerel ağa geçiş ve atlatma testleri*
- *WEP, WPA, WPA2 anahtarı kırma testleri*
- *WPS destekli kablosuz ağlara yönelik keşif çalışmaları ve PIN numarası testleri*
- Sahte erişim noktası ile kullanıcıları aldatma
- Servis engelleme saldırıları

1.1.3. ☐ WEB UYGULAMALARI TESTİ

1.1.3.1. Bilgi toplama ve ayar yönetimi

- Sunucu, sanal sunucu ve teknoloji bilgisi (web sunucu, CMS, Veritabanı)
- IP-sunucu-versiyon bilgisi eşleşmesi çıkarma
- WHOIS sorgusu (port 43) ile domain sahipliği, subdomain, ip blokları, eposta vb
- Nslookup ile www ve www'suz sorgu yapma
- Alt domainleri sıralama
- Framework ve uygulama izini sürme
- Herkese online olan uygulamaları bulma
- Açık kaynak ya da ticari olsun kaynak koda erişim ile bulma
- Özelleşmiş uygulamaların izini sürme
- Kaynakları sıralama (Alt domainler, website yapısı, gizli dosyalar, yapılandırma dosyaları)
- *Arama moturu keşfi ve arama motorunun kötüye kullanımı*
- http method bilgisi analizi
- SSL/TLS bilgisi: versiyonları ve algoritmaları
- Uygulama dizin yapısı analizi
- Yönetici arayüzü erişimi
- Minimum bilgi prensibine aykırı durumları tespit etme
- Yardım ve hata sayfaları
- Unutulmuş html açıklama satırları
- E-posta ve kullanıcı toplama
- Sosyal ağlar, arama motorları
- Yedeklenmiş ve unutulmuş dosyalar
- Bilinen açıklıklar bulma
- Oturum bilgilerini kullanarak zafiyet tarayıcı ile tarama

1.1.3.2. Kimlik Denetimi

- Kimlik doğrulama türü
- Giriş-çıkış işlevi ve cache yönetimi

- Kullanıcı adı ve şifre politikaları

1.1.3.3. Yetkilendirme Denetimi

- *Kullanıcı hesaplarına yönelik sözlük saldırıları*
- *Kullanıcı hesaplarının tespitine yönelik testler*
- *Savunmasız parola hatırlatma ve parola sıfırlama testi*
- *Kimlik doğrulama şemasını atlatmaya yönelik testler*
- *Brute Force (Kaba Kuvvet testi)*
- *CAPTCHA testi*
- *Çok faktörlü kimlik doğrulama testi*

1.1.3.4. Oturum Yönetimi

- *Oturum yönetim şeması testi*
- *CSRF – Siteler arası istek sahteciliği testi*
- Session *Fixation – sabit oturum testi*
- *Çerez niteliklerinin testi*

1.1.3.5. Girdi-çıktı alanı tespiti ve istismarı

- *XSS – (Cross site scripting) Çapraz site betik yönlendirme testleri*
- *SQL Injection Atakları*
- *LDAP Injection Atakları*
- *Path Injection Atakları*
- *Kod Çalıştırma Atakları*
- File Inclusion zafiyetleri

1.2. ☐ KARA KUTU

Sızma testlerinin kara kutu olarak yapılması halinde aşağıdaki adımlar uygun olduğu sürece denetlenir:

- Kurumun Harici Altyapısının Envanterinin Çıkarılması *(Kurumsal Bilgi Toplama)*
- Ağın Topolojik Haritasının Oluşturulması
- Hedeflerin IP Adreslerinin Belirlenmesi
- WEB Sunucularına Giden Trafik Rotalarının Tespiti
- Hedefe Giden TCP ve UDP Trafiğinin Takibi
- Hedef Sunucuların Fiziksel Konumlarının Belirlenmesi
- IP Bilgisi için Etki Alanı Kayıtlarının Sorgulanması
- Hedef Hakkındaki IP Blok Bilgisinin Bulunması
- İstemcinin İnternet Servis Sağlayıcısının Tespiti
- Açık Portların Listelenmesi
- Kapalı Portların Listelenmesi
- Hedef Ağdaki Tüm Portların Taranması
- Hedefe Yönelik SYN Taraması ve Cevabın Analiz Edilmesi
- Hedefe Yönelik Connect Taraması ve Cevabın Analiz Edilmesi
- Hedefe Yönelik FIN Taraması ve Cevabın Analiz Edilmesi
- Standart ve Standart Olmayan Protokollerin Kullanımının İncelenmesi

- Hedef Sistemin Çalışma Süresinin İncelenmesi
- Farklı Hedeflerce Kullanılan İşletim Sistemlerinin İncelenmesi
- İşletim Sistemlerine Uygulanan Yamaların İncelenmesi
- Etki Alanındaki DNS Kayıtlarının Tespiti ve DNS Hijacking Denemesi
- Kurumun WEB Sitesinden Uygulamaların İndirilmesi ve Tersine Mühendislik Saldırıları
- Hedef Sunucudaki Programlama Dillerinin ve Çeşitli Programların Oluşturulmasında Kullanılan Uygulama Yazılımlarının Listelenmesi
- Hataların ve Özel WEB Sayfaların Aranması
- Farklı Alt Alan Adlarının Tahmini ve Cevapların Analiz Edilmesi
- Oturumların Ele Geçirilmesi
- Sunucu Tarafından Üretilen Çerezlerin İncelenmesi
- WEB Sunucu Tarafından Kullanılan Erişim Kontrollerinin İncelenmesi
- URL İnjeksiyonları ve Oturum Tanımlayıcıları için Kaba Kuvvet Saldırıları
- WEB Sayfalarının Dizin Tutarlılığının ve Sayfa İsimlendirme Kurallarının Kontrol Edilmesi
- WEB Sayfa Kaynak Kodunda Hassas Bilgi Aranması
- WEB Sayfalarında URL Encoding Denemesi
- Girdi Alanlarında Bellek Taşırma Saldırılarının Denenmesi
- Girdi Alanlarında Geçersiz Aralıkların Aranması
- Boş Karakter İnjeksiyonu Saldırılarının Denenmesi
- Siteler Arası Betik Çalıştırma (XSS) Saldırılarının Denenmesi
- Hedef WEB Sunucusu Trafiğinin Kaydedilmesi, Tekrarlanması ve Cevapların Not Edilmesi
- Çeşitli SQL İnjeksiyonu Saldırılarının Denenmesi
- Gizli Alanların İncelenmesi
- Server Side Includes İncelenmesi
- WEB Sunucu Tarafından Yapılan E-Ticaret ve Ödeme Geçitlerinin İncelenmesi
- Karşılama, Hata ve Hata Ayıklama Mesajlarının İncelenmesi
- Sunucunun SMTP Mail Bouncing Tarafından Sorgulanması
- HTTP Sunucusunun Banner Bilgisinin Ele Geçirilmesi
- SMTP Sunucusunun Banner Bilgisinin Ele Geçirilmesi
- POP3 Sunucusunun Banner Bilgisinin Ele Geçirilmesi
- FTP Sunucusunun Banner Bilgisinin Ele Geçirilmesi
- Sunucuda Kullanılan WEB Uzantılarının Belirlenmesi
- HTTPS Tunelleme ile Trafiğin Sarmalanması Denemesi
- Hedef Sunucuların İşletim Sistemleriyle İlgili Bilgi Toplanması
- ICMP Cevaplarının Kontrolü (Type 3 Port Unreachable)
- ICMP Cevaplarının Kontrolü (Type 8 Echo Request)
- ICMP Cevaplarının Kontrolü (Type 13 Time-Stamp Request)
- ICMP Cevaplarının Kontrolü (Type 15 Information Request)
- ICMP Cevaplarının Kontrolü (Type 17 Subnet Address Mask Request)
- Broadcast Adresinden Dönen ICMP Cevaplarının Kontrolü
- DNS Sunucularının Port Taraması (TCP/UDP 53)
- TFTP Sunucularının Port Taraması (Port 69)

- NTP Portlarının Test Edilmesi (Port 123)
- SNMP Portlarının Test Edilmesi (Port 161 ve 162)
- Telnet Portlarının Test Edilmesi (Port 23)
- LDAP Portlarının Test Edilmesi (Port 389)
- NetBIOS Portlarının Test Edilmesi (Port 135-139 ve 445)
- SQL Server Portlarının Test Edilmesi (Port 1433 ve 1434)
- Citrix Portlarının Test Edilmesi (Port 1495)
- Oracle Portlarının Test Edilmesi (Port 1521)
- NFS Portlarının Test Edilmesi (Port 2049)
- Compaq, HP Inside Manager Portlarının Test Edilmesi (Port 2301 ve 2381)
- Uzak Masaüstü Portlarının Test Edilmesi (Port 3389)
- Sybase Portlarının Test Edilmesi (Port 5000)
- SIP Portlarının Test Edilmesi (Port 5060)
- VNC Portlarının Test Edilmesi (Port 5800 ve 5900)
- X11 Portlarının Test Edilmesi (Port 6000)
- JetDirect Portlarının Test Edilmesi (Port 9100)
- FTP Data Port Taraması (Port 20)
- WEB Sunucularının Port Taraması (Port 80)
- SSL Sunucularının Port Taraması (Port 443)
- Kerberos-Active Directory Port Taraması (Port TCP/UDP 88)
- SSH Sunucularının Port Taraması (Port 22)

2. ☐ UYGUNLUK DENETİMİ

Cihazlar üzerindeki kimlik bilgileri ile ilgili cihazlara bağlanarak iç güvenliğinin uygunluğu denetlenir. Uygunluk denetimi cihazın yapılandırma dosyası verilmek suretiyle yapılan taramadır.

3. ☐ ZAFİYET ANALİZİ

Ağ, web ve kablosuz ağ olmak üzere 3 başlık altında yapılabilir. Sızma testinden farklı olarak istismar ve sonrası aşamalar gerçekleştirilmez.

4. ☐ DİĞER TESTLER (İSTEĞE BAĞLI)

Bu kısımda size sunulan testler haricinde yaptırmak istediğiniz testleri belirtebilirsiniz. Ancak belirtilen testler laboratuvar yetenekleri kapsamında değerlendirilecek olup yetkili personel tarafından yapılabilir.

No	Test Açıklaması
1	
2	

5. ☐ KONTROL TESTLERİ

Sızma testleri sırasında tespit edilen zafiyetlerin Kurum personeli tarafından giderilmesinin ardından aşağıda listelenmiş işlemler "kontrol testleri" kapsamında yapılır. Kurum, kontrol testlerinin ilk raporun tesliminden sonra 6 ay içinde yapılabilmesi için gerekli çalışmaları yürütecektir. İlk testin üzerinden 6 aydan fazla süre geçmesi halinde sistemlerin yeniden test edilmesi gerekir.

- Giderildiği belirtilen zafiyetin istismar edilmesi
- Varsa; güncellenen işletim sisteminin zafiyet taramasının yapılması
- Varsa; güvenlik cihazları üzerinde yapılan değişikliklerin gözden geçirilmesi
- Varsa; yeni zafiyetlere neden olabilecek noktaların belirlenmesi
- Kontrol testi sonuçlarının raporlanması

6. GENEL SORULAR

Testi yaptırmadaki amacınız nedir?		
Testlerin tarafınızdan planlanan başlama tarihi		
Bütün testler mesai saatleri içerisinde yapılabilir mi?	Evet ☐	Hayır ☐
Testlerin Yeri	Uzaktan erişim ile ☐	TSE dışında (Müşteri sahasında) ☐
Kaç tane alan adınız (domain) mevcut? Bunlardan kaçının taranmasını istiyorsunuz?		

Sızma Testi Kapsamı

(Test türünde beyaz kutu seçildiyse aşağıdaki soruyu cevaplandırınız) Ağ sistemleri planı nedir? (Segmentler, Router, Switch, DMZ, IDS, IPS, Firewall, web sunucular vb.)
Ağınızda IPv6 yapısı mevcut mu? Mevcutsa IPv6 adresli istemci veya sunucuların güvenlik testini istiyor musunuz?
Test kapsamı dışında tutulmasını istediğiniz bileşenleriniz var mı?(Sunucu, Kişisel bilgisayar, uygulama, printer vb.) Sunucu ve bilgisayarlar için ip adresi, uygulama için ip ve port adresi verilebilir.

Test edilecek istemcilerin bulunduğu ağ adresi ve adedi nedir? (Örnek 192.168.24.0/24 ağ adresinde 50 adet istemci test edilecek gibi)
Test edilecek sunucuların bulunduğu ağ adresi ve adedi nedir?

7. Çıktılar

Testlerin sonucunda Kurumunuza aşağıdaki başlıkları içeren ayrıntılı bir rapor sunulacaktır:

- Yönetici özeti: Raporun kritik bulgularının ve uygulamanın genel durumunun değerlendirilmesi
- Yapılan testler ve elde edilen sonuçlar: Yapılan testlerin sırasıyla ele alındı ve test sonucunda elde edilen sonuçların raporlanması

- Tespit edilen güvenlik zafiyetleri: Test sonuçları arasında “saldırgan tarafından kullanılabilir” ve/veya uygulamanın güvenliğini tehdit eden bulgular
- Zafiyetlerin giderilmesi için öneriler: Tespit edilen zafiyetlerin giderilmesi için öneriler
- Yorumlar: Testler sırasında uygulanabilir olmadığı için ele alınamamış ve ilerleyen dönemlerde risk oluşturabilecek noktalar.
- Ham veriler: tarama ve test sırasında oluşan verilerin ham kayıtlarıdır

Bulgular aşağıda verilen “Bulgu Önem Dereceleri” tablosuna uygun olarak derecelendirilir.

Önem Derecesi	**Açıklama**
Acil	Niteliksiz saldırgan tarafından dış ağdan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Kritik	Nitelikli saldırgan tarafından dış ağdan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Yüksek	Dış ağdan gerçekleştirilen ve kısıtlı hak yükseltilmesi veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan saldırılara sebep olan açıklıklardır.
Orta	Yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan saldırılara sebep olan açıklıklardır.
Düşük	Etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.

Başvuran Kuruluş Adına	
Yetkili Adı Soyadı	
(Firma) Kaşe ve İmzası	
Tarih	