Evrak Tarih ve Sayısı: 26.09.2022-E.36459

YAZILIM VE BİLİŞİM SİSTEMLERİNDE GÜVENLİK TARAMASI TESTLERİ HİZMET ALIMI ŞARTNAMESİ

2022, T.C. Hakkari Üniversitesi, Bilgi İşlem Daire Başkanlığı

İÇİNDEKİLER

1. TANIMLAR ve KISALTMALAR

İdare	:	T.C. Hakkâri Üniversitesi Bilgi İşlem Daire Başkanlığı
Kurum	:	T.C. Hakkari Üniversitesi
İstekli	:	Teklif veren
Yüklenici	:	Sözleşme yapılan istekli
DDos (Distributed Denial of Service)	:	Birden fazla bilgisayardan yoğun trafik oluşturularak hedeflenen servisi yavaşlatmak ya da çökertmek için yapılan sanal saldırılardır.
Dos (Denial of Service)	:	İnternete bağlı bir hostun hizmetlerini geçici veya süresiz olarak aksatarak, bir makinenin veya ağ kaynaklarının asıl kullanıcılar tarafından ulaşılamamasını hedefleyen bir siber saldırıdır.
DNS (Domain Name System)	:	İnternet uzayını bölümlemeye, bölümleri adlandırmaya ve bölümler arası iletişimi organize etmeye yarayan sistemdir.
Web Uygulaması	:	Çeşitli araçlarla (Visual Studio, Web Expression, Dreamviewer) ve teknolojilerle (PHP, ASP, ASP.NET) geliştirilmiş ve Web Sunucu lar üzerinde duran, Internet Tarayıcı programlar aracılığı ile ulaşılıp kullanılabilen uygulamalardır.
Sızma Testi (Pentest / Penetrasyon Testi)	:	Bilişim sisteminin güvenliğini değerlendirmek üzere bir bilgisayar sistemi üzerinde gerçekleştirilen yetkilendirilmiş temsili bir siber saldırıdır.
Exploit	:	Bir bilgisayar programı veya betiktir, bilgisayar programlarında bulunan zayıflık veya hatalar için kullanılır.

2. KONU ve KAPSAM

2.1. Bu şartname İdare tarafından kullanılan tüm bilişim sistemlerinin (sunucuların, ağ cihazlarının, güvenlik ürünlerinin) güvenlik kontrollerinin yapılmasını amaçlanmaktadır.

2.2. Yapılacak güvenlik testi Kurum tarafından kullanılan tüm bilişim sistemlerini (sunucular, ağ cihazları, güvenlik ürünleri vb.) kapsar.

2.3. Güvenlik testi bir kez yapılacak ve sonunda kapsamlı bir rapor kuruma teslim edilecektir.

3. KOŞULLAR

3.1. Projede görev alacak tüm uzmanların T.C. vatandaşı olmaları ve hizmetin tümüyle Türkiye Cumhuriyeti sınırları içerisinde verilmesi gerekmektedir.

3.2. Test ve inceleme hizmetlerini yürütecek personelin/personellerin güncel olan CEH, ECSA/LPT, OSCP, TSE Beyaz Şapkalı Hacker sertifikalarından en az birine sahip olması gerekmektedir.

3.3. Penetrasyon testini sağlayacak yüklenici ISO27001 ve ISO20000-1 sertifikasyonlarına veya Pentest firması unvanına sahip olmalıdır.

3.4. İçeride yapılacak testlerde kullanılacak (notebook, PC vb.) cihazlar yüklenici tarafından temin edilecektir.

3.5. Yapılacak tüm sızma testleri (özellikle DOS testleri), çalışmakta olan sistemleri, mesai saatlerinde kesintiye uğratmayacak şekilde gerçekleştirilecektir.

3.6. İstemsiz bir kesinti yaşanması durumunda ise yüklenicinin acil durum destek hizmetlerini yürütecek nitelikli personelleri sağlaması gerekmektedir.

3.7. İdare, testlerin yapılması için belirlediği kapsama yönelik uygun test altyapısını hazırlayacaktır.

3.8. İdare, yüklenicinin kurum içinden ve dışından testleri yapabilmesi için uygun seviyede erişim izinlerini tanımlayacaktır.

3.9. Yüklenici, aşağıda maddelenmiş olan hizmetleri eksiksiz bir şekilde vermeyi taahhüt eder:

- İletişim Alt Yapısı ve Aktif Cihazlar Testleri
- Kablosuz Ağ Sistemleri Testleri
- Dağıtık Servis Dışı Bırakma Testleri
- DNS Testleri

- Veri tabanı Sistemleri Denetim
- Web Uygulaması Testleri
- Sosyal Mühendislik Testleri

3.10. Fiyat araştırma ve/veya fiyat teklifi alınma esnasında yapılacak testler için fiyatın belirlenmesi adına istenilecek bilgiler, 3. kişilere teklif verecek istekli tarafından paylaşılmamak taahhüttü ile idare tarafından sağlanacaktır.

3.11. Bu teknik şartname kapsamında alınacak hizmet sürecinde ISO/IES 27001 ve/veya ISO 20000-1 standardında yapılabilecek güncellemelere göre yüklenici, proje planında ve proje uygulamasında yeni standarda göre değişiklikler yapabilecek ve İdare tarafından istenirse yeni standarda göre projeyi tamamlayacaktır.

3.12. Hizmet Gizliliği: Yüklenici şartnamede tanımlanan aşamalara ait işlerle ilgili tespit ettiği hiçbir bilgiyi İdareden saklamayacak, İdare tarafından belirlenen personele tüm bilgileri istenildiği zaman verecektir. İdare ortamından öğrenilen tüm bilgiler GİZLİ statüsünde olup, yüklenici idare ile ilgili öğrendiği hiçbir bilgiyi hizmet süresince ve/veya sözleşme süresi sonrasında 3 üncü şahıslar ile paylaşmayacağını taahhüt edecektir. Bu hizmet aşamasında çalışacak bütün personel ile hizmet başlamadan önce üzerinde karşılıklı olarak anlaşılacak özel gizlilik sözleşmesinin imzalanması istenecektir. Türk yargı mercilerinin kararları saklı kalmak kaydıyla sözleşmenin amaçları doğrultusunda herhangi bir ifşa ve yayımlama/yayınlama gerekliliği konusunda bir uzlaşmazlık ortaya çıkarsa, idarenin bu konudaki kararı nihai olacaktır. Gizlilik yükümlülüğü, sözleşmenin herhangi bir nedenle sona ermesinden sonra da devam eder. Yüklenici sözleşmenin imzalanmasına müteakip Gizlilik Sözleşmesini imzalayarak idareye sunacaktır.

4. TEMEL SIZMA TESTLERİ

4.1.Temel Sızma Testi Adımları

4.1.1. Temel sızma testi adımları aşağıda tanımlanan Sistem Tespiti, Servis Tespiti ve Açıklık Taraması/Araştırması adımlarından oluşmaktadır.

a) **Sistem Tespiti:** Sunucu veya aktif/pasif ağ cihazlarının sistem/yapılandırma bilgilerinin tespit edilmeye çalışıldığı adımdır.

b) **Servis Tespiti:** Kurum Bilgi Sistemlerinde yer alan varlıkların port taramasının gerçekleştirildiği ve dış dünyaya/genel erişime açık olan portların sunduğu servislerin tespit edilmeye çalışıldığı adımdır.

c) **Açıklık Taraması/Araştırması:** Kurumun bileşenleri ve bu bileşenlerin sunduğu servislerin açıklık tarayıcıları ile güncel açıklıklara karşı tarandığı ve muhtemel güvenlik açıklıklarının belirlenmeye çalışıldığı adımdır. Bu adımda ayrıca, tespit edilen muhtemel açıklıklar için açıklık veri tabanları gibi kaynaklar kullanılarak bu açıklıkların bileşenlere ve bileşenlerin etkileşimde olduğu sistemlere güvenlik açısından etkileri araştırılır.

4.2. Dış Ağdan Gerçekleştirilecek Temel Sızma Testleri:

4.2.1. Kurum ağından bağımsız bir lokasyondan, kurumun internet üzerinde sahip olduğu IP ağı taranarak temel sızma testi adımları gerçekleştirilir.

4.3. İç Ağdan Gerçekleştirilecek Temel Sızma Testleri:

4.3.1. Kurumun iç ağında "Temel Sızma Testi Adımlarının" yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:

a) Kurum yerel ağ haritası tespiti

b) Belirlenen açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma testlerinin gerçekleştirilmesi

c) Yerel alan ağı içerisinde zafiyet taraması yapılması

d) Kurum yerel ağında araya girme teknikleri ile hassas bilgilerin elde edilmeye çalışılması

e) Elde edilen bilgiler ışığında kullanıcı bilgisayarları, sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırılarının gerçekleştirilmesi

f) Ele geçirilen sunucu ve kullanıcı bilgisayarları üzerinden daha kritik bilgilere ulaşılmaya çalışılması

5. SIZMA TESTLERİ KAPSAMINDA GERÇEKLEŞTİRİLECEK GÜVENLİK TESTLERİ

5.1. Temel sızma testlerinin tamamlanması sonrası, sızma testleri kapsamında gerçekleştirilmesi gereken ikinci kısım, güvenlik testleridir. Sızma testleri kapsamında gerçekleştirilecek güvenlik testleri asgari olarak aşağıdaki testleri kapsar.

5.1.1. İletişim Alt Yapısı ve Aktif Cihazlar

5.1.1.1. Kurumun ağ altyapısı ve aktif ağ cihazlarına yönelik asgari olarak aşağıdaki testler gerçekleştirilir:

a) Kurumda kullanılan ağ cihazlarının genel mimari içindeki yeri incelenir.

b) Tüm ağ cihazları açıklık bulma araçları ile taranır.

c) Tespit edilen açıkların uygulanabilirlikleri sınanır.

d) Ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenir.

e) Aktif cihaz üzerindeki port güvenliği, VLAN ve trunk yapısı incelenir.

f) Ağ topolojisi ve segmentasyonu incelenerek kullanıcı-sunucu ağları arasında erişim kontrolünün olup olmadığı kontrol edilir.

g) Paket dinlemesi yoluyla ağ üzerinden geçebilecek VoIP paketleri yakalanmaya ve konuşmalar dinlenmeye çalışılır.

h) Aktif cihaz üzerinde çalışan servisler incelenir.

i) Kullanılan servislerin servis dışı bırakılmayla sonuçlanabilecek saldırılara karşı (ARP zehirlemesi, CDP DoS, DHCP DoS, SNMP DoS vb.) durumu incelenir.

j) Cihazlar üzerinde açık olan Telnet, HTTP, FTP, SNMP, TFTP, SSH servislerine sözlük saldırısı veya kaba güç kullanılarak erişim sağlanmaya çalışılır.

k) Erişim sağlanan cihazlar üzerinden alınan bilgilerle diğer cihazlara erişilmeye çalışılır.

l) Aktif cihazlar için uzak/yerel erişim kontrolü, yönetim, kayıt ve kimlik doğrulama mekanizmaları incelenir.

m) Cihazların merkezi şekilde yönetilmesini ve gözetlenmesini sağlayan yönetim sistemlerinin varlığı araştırılır ve bu sistemlere sızma girişimlerinde bulunulur.

n) Cihazlarda ortak parolanın kullanılıp kullanılmadığı test edilir.

o) Kurum çalışanları için kullanılan içerik filtreleme sistemleri atlatılmaya çalışılır.

p) Kurum içinden dışarı tünel kurulmasıyla, kurum dışından kurum içine yetkisiz bağlantı gerçekleştirilmeye çalışılır.

q) Kurum dışına açık yönetim ara yüzlerinin varlığı kontrol edilir.

5.1.2. DNS Servisleri

5.1.2.1. Kurumun DNS servislerine yönelik asgari olarak aşağıdaki testler gerçekleştirilir:

a) DNS sunucuların topolojik konumu incelenir.

b) DNS Sunucusunun alan yapılandırmasında yer alan kayıtlar ortaya çıkarılmaya çalışılır. Bu kapsamda;

1) Sunucu üzerinden alan transferi (zone transfer) yapılmaya çalışılır.

2) NXT ve NSEC kaynak kayıtları üzerinden bilgi elde edilmeye çalışılır.

3) Netcraft, Google, Whois sorguları yapılarak Kurum alanında yer alan sunucular tespit edilmeye çalışılır.

4) DNS sunucular için ön bellek zehirlemesi gerçekleştirilmeye çalışılır.

5) DNS sunucular üzerindeki kaynak kayıt girdileri incelenir.
6) DNS sunucular üzerindeki ters kaynak kayıt girdileri incelenir.
7) DNS sunucuların sürüm bilgisi elde edilmeye çalışılır.
8) Kurum dışı alan isimleri sorgulanmaya çalışılır.
9) Sunucular üzerinde DNS dışında bir servisin çalışıp çalışmadığı incelenir.
10) Güvenlik Duvarında DNS sunucular için izin verilen portlar incelenir.
11) DNS sunucuları güvenlik taramasına tabi tutulur.
12) DNS servisini veren yazılımın açıklıkları araştırılır.

5.1.3. Veritabanı Sistemleri

5.1.3.1. Veri tabanı sistemlerine yönelik asgari olarak aşağıdaki testler gerçekleştirilir:

a) Sistemdeki veri tabanı uygulamaları ve bu uygulamaları üzerinde barındıran işletim sistemleri tespit edilerek, tespit edilen bu sistemlere erişimin açık olup olmadığı denetlenir ve erişimin açık olması halinde çeşitli tarama araçlarıyla veri tabanı versiyonu, üretici adı vb, bilgiler ele geçirilmeye çalışılır.

b) Elde edilen veri tabanı sistem bilgileri kullanılarak, bu sistemlere yönelik kullanıcı adı ve parola deneme saldırıları yapılır. Bu saldırılar sırasında, ön tanımlı kullanıcı adı ve parolaların denenmesinin yanında, kuruma özel olabilecek ve tahmin edilebilir kullanıcı adı ve parolalar da denenir.

c) Veri tabanı kullanıcı adı ve parola saldırılarının başarısız olması durumunda, işletim sistemi seviyesinden erişim denemeleri yapılır. Windows, Linux vb. ortamlar üzerinden sistem kullanıcıları ile veri tabanı uygulamasına bağlanılmaya çalışılır.

d) Parola deneme saldırılarının başarılı olması durumunda tespit edilen erişim bilgileriyle sistemlere bağlanılır. Bağlanılan sistemlerde hangi hassas verilerin bulunduğu, kullanıcı adı, parola ve parolalara ait karmaşıklaştırılmış özet verilerinin bulunup bulunmadığı denetlenir.

e) Görüntülenebilen kullanıcı adı ve parola özet bilgileri çeşitli araçlarla tespit edilmeye çalışılarak zayıf olarak belirlenmiş parolalar tespit edilir.

f) Erişilebilen sistemlerde yama bilgisi kontrol edilir. Bilinen açıklıkları içeren ve gerekli güncellemeleri yapılmamış sistemlerde hak yükselme vb. saldırılarla erişim sağlanan kullanıcının hakları genişletilmeye çalışılır.

g) Erişilebilen sistemlerden diğer erişilemeyen sistemlere tanımlanmış bağlantılar varsa bu bağlantılar kullanılarak diğer veritabanı uygulamalarına geçilmeye çalışılır.

h) Hassas verileri ihtiva eden sistemlere erişile bilinmesi halinde yetki seviyesi arttırılmaya çalışılır. Erişim bilgisi elde edilecek sistemlerin sayısı arttıkça, her sistem için yukarda bahsi geçen adımlar tekrarlanır ve mevcut tüm veri tabanlarının güvenliğibu şekilde kontrol edilir.

5.1.4. Web Uygulamaları

5.1.4.1. Web uygulamalarına yapılacak testler sisteme zarar vermeyecek şekilde, idare tarafından yüklenici için her bir uygulama adına oluşturulacak kullanıcı profilleri kullanılarak gerçekleştirilir. Yapılacak testler kapsamında, sunucular üzerinde çalışan servislerin ya da işletim sistemlerinin bilinen açıklıklarının araştırılmasının yanında, sistemdeki uygulamalara has güvenlik açıklıkları da araştırılır ve asgari olarak aşağıda listelenen açıklık ve zafiyetlerin varlığına ilişkin testler gerçekleştirilir.

a) Veri Denetimi
b) Yetersiz Girdi Denetimi
c) Yetersiz Çıktı Denetimi
d) XSS Enjeksiyonu (XSS Injection)
e) SQL Enjeksiyonu (SQL Injection)
f) Diğer Enjeksiyonlar (XPATH, LDAP v.b.)
g) HTTP Yanıt Bölme (HTTP ResponseSplitting)
h) Kontrolsüz URL Yönlendirmeleri

5.1.4.2. Oturum Yönetimi;

a) Oturum Sabitleme (SessionFixation)
b) Çerez Etiketlerinin Kullanılmaması
c) Yetersiz Oturum Sonlandırma Fonksiyonu
d) Oturum Bilgisinin URL İçinde Taşınması
e) Siteler Arası istek Sahteciliği (Cross-Site RequestForgery, CSRF)

5.1.4.3. Kimlik Doğrulama ve Yetkilendirme;

a) Yetki Arttırımı, Yetkilendirmenin Atlatılması
b) Eksik Hesap/Parola Yönetimi ve Yetersiz Parola Politikası
c) Kimlik Doğrulamanın Atlatılması
d) Tersine yol (PathTraversal)
e) Uygulama Mantığı Hatları (Application LogicFlaw, Business LogicFlaw)

5.1.4.4. Bilgi Sızdırma ve Ayar Yönetimi;

a) Minimum Bilgi Prensibine Aykırı Yardım Sayfaları, HTML Yorumları, HataMesajları, Hata Sayfaları ve Durumlar
b) Veri İletiminde SSL Kullanılmaması
c) Zayıf veya Geçersiz SSL Sertifikası Kullanılması
d) Sunucu Bilgisinin Kısıtlanmaması
e) Kullanılan Teknoloji Bilgisinin Kısıtlanmaması
f) Yedeklenmiş ve Unutulmuş Dosyaların Varlığı
g) Yönetici Ara yüzüne Erişim
h) Hizmet Dışı Bırakma
i) Kaba Kuvvet Saldırısına Açık Ekranlarda Risk Azaltıcı Metotlar kullanılmaması

5.1.5. Kablosuz Ağ Sistemleri

5.1.5.1. Kurumda kullanılan kablosuz ağ cihazlarının genel mimari içindeki yeri incelenir.

5.1.5.2. Kablosuz ağlardan kurum içi ağlara erişim olup olmadığı incelenir ve kablosuz ağlardan kurum ağına sızılmaya çalışılır.

5.1.5.3. İstemcilerin kablosuz ağ yapılandırmaları incelenir.

5.1.5.4. Kurumda bulunan kablosuz ağlar taranarak özellikleri keşfedilmeye çalışılır.

5.1.5.5. Kablosuz ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenir.

5.1.5.6. Kablosuz ağlarda kullanılan şifreleme ayarları incelenir.

5.1.5.7. WEP ve WPA/WPA2 şifreleme kullanılan ağlarda kablosuz ağ şifresi ele geçirilmeyeçalışılır.

5.1.5.8. Sahte kablosuz ağ erişim noktaları oluşturularak kurumda bulunan istemciler ele geçirilmeye çalışılır.

5.1.5.9. İstemciler üzerinden kablosuz ağ taraması yapılarak, kurum etrafında bulunan diğerkablosuz ağlar keşfedilmeye çalışılır.

5.1.5.10. İstemciler üzerinden kablosuz ağ kullanılarak kurum dışına bağlantı yapılıp yapılamayacağı incelenir.

5.1.6. Dağıtık Servis Dışı Bırakma Testleri

5.1.6.1. Dağıtık servis dışı bırakma(DDOS) testlerinde amaç, kurumların bu kapsamdaki saldırılara karşı kullandığı savunma mekanizmalarının etkinliğini değerlendirmektir. DDOS testleri, kurumun en az servis verdiği saatlerde ve sistem yöneticileri ile koordine olarak gerçekleştirilir. Bu kapsamda asgari olarak ağıdaki testler gerçekleştirilir.

5.1.6.2. IP Seviyesinde Gerçekleştirilecek DDOS Testleri;

a) DNS sunucularına yönelik dağıtık aşırı paket gönderimi ile trafiğin üzerinden geçtiği güvenlik duvarı gibi aktif cihazlara yönelik yük testi gerçekleştirilir.

b) Web sunucularına yönelik dağıtık aşırı paket gönderimi ile trafiğin üzerinden geçtiği güvenlik duvarı gibi aktif cihazlara yönelik yük testi gerçekleştirilir.

c) Herkese hizmet veren servisler tespit edilerek, bu servislere yönelik dağıtık aşırı paket gönderimi ile trafiğin üzerinden geçtiği güvenlik duvarı gibi aktif cihazlara yönelik yük testi gerçekleştirilir.

5.1.6.3. Uygulama Seviyesinde Gerçekleştirilecek DDOS Testleri;

a) DNS sunucularına yönelik rastgele istek gönderimi ile DNS sunucu yük testi gerçekleştirilir.

b) Web sunucularına yönelik aşırı paket gönderimi ile web sunucu yük testi gerçekleştirilir.

5.1.7. Sosyal Mühendislik Testleri

5.1.7.1. Sosyal Mühendislik Testleri kapsamında, insanların zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışma işlemlerinin bütünüdür. Bu kapsamda;

a) Bilgi toplama

b) Zayıflık tarama

c) Sisteme sızma

d) Erişim koruma

e) İzleri temizleme testleri yapılır.

6. SIZMA VE GÜVENLİK TESTLERİ RAPORLAMA

6.1. Yöneticilere ve teknik çalışanlara ayrı olmak koşuluyla iki farklı raporun düzenlenmesi gerekmektedir.

6.2. Raporlar okunabilir ve anlaşılabilir olmalıdır.

6.3. Yüklenici, raporları idareye teyit ettirdikten sonra imzalı şekilde teslim etmelidir.

6.4. Günlük olarak yapılan işlemler mesai bitiminde raporlanmalıdır.

6.5. Test sırasında zayıflıklar ve Exploitler raporlanmalıdır.

6.6. Test sırasında yetkisiz veriye ulaşılması durumu mevcut ise bu durum raporlanmalıdır.

6.7. Test sırasında trafik anormallikleri raporlanmalıdır.

6.8. Raporlarda bulunan güvenlik zafiyetlerinin özet tablosu, kategori/risk seviyesi özet dağılım tablosu ayrıca bulunan güvenlik açıklarının risk seviyeleri, kategorileri, etki biçimleri, bulgu sebepleri vb. yöntemlere göre dağılım tabloları grafiksel ve metinsel sunulmalıdır.

6.9. Sonuçların basit açıklıklar olarak değil, bir risk haritası kapsamında idareye sunulması gerekmektedir.

6.10. Her bir açıklığın kimin ilgi alanına girdiğinin hazırlanacak raporun sonuç bölümünde belirtilmesi gerekmektedir.

6.11. İdare tarafından belirlenen sistem yöneticileri ve/veya yazılımcılar ile toplantı yapılıp sonuçların paylaşılması sağlanmalıdır.

Ömer ÇİÇEK
Bilgisayar Teknikeri

Öğr.Gör. Gülşen ERTUŞ