SIZMA TESTİ HİZMETİ VEREN PERSONEL VE FİRMALAR İÇİN YETKİLENDİRME PROGRAMI

İlk yayınlanma: 01.10.2013
R2: 05.01.2014
R3: 24.03.2014
R4: 15.04.2014
R5: 02.05.2014
R6: 16.05.2014
R7: 28.05.2014

Bu dokümana aşağıdaki web sayfasından erişilebilir:

- Türk Standardları Enstitüsü Resmi web sitesi (TSE) (bilisim.tse.org.tr).

İÇİNDEKİLER TABLOSU

0 GİRİŞ

Bilgi, içinde bulunduğumuz iletişim çağında bir kurumun en önemli varlıklarından biridir. Bu kapsamda 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. Bu program dokümanında sızma testi yapan firmalara ve personellere ait kriterler ve şartlar ortaya konulmaktadır.

Sızma testi, bilgisayar ve ağ güvenliğini dışarıdan veya içeriden yapılan bir saldırı ile değerlendirme yöntemidir.

Sızma testlerinin kuruluşlara çeşitli yararları vardır. Bunlardan bazıları aşağıda sıralanmıştır:

- Belirli bir saldırı vektör kümesinin olabilirliğinin belirlenmesi,
- Belirli bir sıralamada kullanılan düşük riskli açıklıkların bir kombinasyonundan kaynaklanan yüksek riskli açıklıkların tespit edilmesi,
- Otomatize ağ veya uygulama açıklık tarama yazılımları ile tespit edilmesi güç veya imkânsız olan açıklıkların tespit edilmesi,
- Başarılı saldırıların, olası iş etkisi ve işletimsel etkilerinin büyüklüğünün anlaşılması ve değerlendirilmesi,
- Ağ koruma cihazlarının ve uygulamalarının saldırıları başarı ile tespit etme ve karşılık verme kabiliyetlerini test etme,
- Güvenlik personeli ve teknolojisine yönelik artan yatırımlara gerekçelendirme sağlanması.

Sızma testleri genellikle tam güvenlik denetimlerinin bir parçası olmakla beraber (örneğin; PCI DSS standardı hem yıllık olarak hem de devamlı olarak (sistem değişikliklerinden sonra) sızma testi gerektirmektedir. Benzer şekilde, ISO/IEC 27001:2005 standardı kapsamı dâhilinde sızma testi yapılması gerekmektedir) tek başına da yapılabilir.

Sızma testlerinde bazı riskler ve dikkat edilmesi gereken noktalar da vardır:

- Test yapılırken, sisteme aşırı yüklenme veya hata oluşturma sonucunda işletimsel sistemde çökme veya hatalı çalışma gibi sorunların yaşanması,
- Kurumsal verilerin kasti veya kasıtsız olarak test esnasında değiştirilmesi,
- Daha önce yaptırılan testlere ait sonuçların, 3.tarafların eline geçerek kötü niyetli olarak kullanılması.

Bu hususlarla ilgili kuruluşlara yönelik olarak bu dokümanda alınması gereken tedbirlere dair bilgilere de yer verilmiştir.

1. KAPSAM VE UYGULAMA ALANI

Bu kriter programı, sistemlerdeki açıklıkları tespit etmek, bu açıklıklardan yararlanılabildiğini göstermek ve bu açıklıkları raporlamak için sızma testi yapan kişi ve kuruluşların sahip olması ve yerine getirmesi gereken kriterleri kapsar. Sızma testi dışında kalan fakat sızma testleri ile ilintili olan; Tersine Mühendislik, Zararlı Yazılım Analizi, Exploit Geliştirme, Zafiyet Araştırma (Vulnerability Research) ve Adli Bilişim gibi konular bu programın kapsamı dahilindedir.

2. ATIF YAPILAN STANDARDLAR VE/VEYA DOKÜMANLAR

EN, ISO, IEC vb.No	Adı (İngilizce)	TS No	Adı (Türkçe)
ISO/IEC 27001:2005	Information technology – Security techniques – Information security management systems - Requirements	TS ISO/IEC 27001:2006	Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler

3. TERİM VE TARİFLER

Bu program için aşağıdaki terim ve tarifler geçerlidir.

3.1. Sızma testi ve türleri

Belirlenen sistemin veya ağın güvenlik açısından analiz edilmesi ve sistemin güvenlik açıklarının ve güvenlik boşluklarının bulunması, bu açıklardan faydalanılarak sistemlere sızılması. Otomatik tarama araçları ile gerçekleştirilen zafiyet taramaları sızma testinin bir aşamasıdır; ancak sızma testi değildir.

3.1.1. Beyaz kutu

Beyaz kutu ağ'daki tüm sistemlerden bilgi sahibi olarak yapılan sızma testi türüdür. Test uzmanının dışarıdan ya da içeriden ağa girmeye ve zarar vermeye çalışmasının simülasyonudur.

3.1.2. Siyah kutu

Siyah kutu testi saldırı yapılacak ağ hakkında hiçbir bilgi sahibi olmadan dışarıdan ağa ulaşmaya çalışan saldırganın verebileceği zararın boyutlarının algılanmasını sağlar.

3.1.3. Gri kutu

Gri kutu testi iç ağda bulunan yetkisiz bir kullanıcının sistemlere verebileceği zararın analiz edilmesini sağlar. Veri çalınması, yetki yükseltme ve ağ paket kaydedicilerine karşı ağ zayıflıkları denetlenir.

3.2. Kuruluş

Sızma testi yaptıran tüzel kişilik.

3.3. Firma

Sızma testi yapan tüzel kişilik.

3.4. Hizmeti aksatma testi (DOS)

Hedef sistemin kaynaklarının ya da bant genişliğinin meşgul edildiği saldırılardır.

3.5. Politika

Yönetim tarafından resmi olarak genel niyetin ve yönün ifade edilmesi.

3.6. Üçüncü taraf

Söz konusu olan konu ile ilgili, taraf bakımından bağımsız olarak kabul edilen kişi ya da kuruluş.

[ISO/IEC Guide 2:1996]

3.7. Tehdit

Bir sistem veya kuruluşta zarara neden olabilecek istenmeyen bir olayın potansiyel nedeni.

[ISO/IEC 13335-1:2004]

3.8. Zayıflık

Bir veya birden fazlar tehdit tarafından istismar edilebilecek bir veya bir grup varlığın zayıf noktaları.

4. KISALTMALAR

DDoS : Distributed Denial-of-Service
DoS : Denial-of-Service
DNS : Domain Name System
FTP : File Transfer Protocol
HTTP : Hyper Text Transfer Protocol
HTTPS : Hyper Text Transfer Protocol Secure
IP : Internet Protocol
ISO : International Organization for Standardization
OWASP : Open Web Application Security Project
PCI-DSS : Payment Card Industry - Data Security Standarts
SCADA : Supervisory Control and Data Acquisition
SSL : Secure Sockets Layer
TSE : Türk Standartları Enstitüsü
TCP/IP : Transmission Control Protocol/Internet Protocol
UDP : User Datagram Protokol

5. SIZMA TESTİ AŞAMALARI

5.1. Planlama

Test sürecinin planlanması aşağıdaki adımlardan oluşmalıdır. Her adımda uyulması gereken hususlar belirtilmiştir.

5.1.1. Test öncesi

Test öncesinde testi yaptıran kuruluş ile koordinasyon sağlanmalıdır. Bu koordinasyon bir sözleşme ve ekinde bir kapsam dokümanı ile belgelenmelidir. Örnek bir kapsam dokümanı Ek-2'de verilmiştir.

Sözleşme ve kapsam dokümanında aşağıdaki hususların olmasına dikkat edilir:

- İşin kapsamı ve tanımı,
- Testin türü (Siyah kutu, beyaz kutu, gri kutu veya belirli zaman aralıkları ile bunların karması olabilir.),
- Sızma testi hizmet türü,
- Testin gerçekleştirileceği sistemlere ait bilgiler (IP, Domain Adı vb.),
- Testin yapılacağı tarih ve saat dilimleri,
- Testi gerçekleştirecek uzmanlara ait bilgiler,

- Hangi ip adresinden testin gerçekleştirileceği,
- Açık bulunduğu taktirde Truva atı yüklenip yüklenemeyeceği,
- Acil Durum Kotarma safhasında iletişime geçilecek personel ve yönetici iletişim bilgileri.

Kuruluş, firma ve testi gerçekleştirecek personel ile bir gizlilik sözleşmesi imzalamalıdır. İmzalanacak olan gizlilik sözleşmesi, İş sözleşmesi kapsamında bazı ek maddeler şeklinde de ele alınabilir fakat gizlilik için ayrı ve detaylı bir sözleşmenin imzalanması tavsiye edilir. Eğer, teklif esnasında gizlilik dereceli bilgilerin paylaşımı söz konusu olacaksa Gizlilik Sözleşmesinin teklif alımından önce yapılması tavsiye edilir.

Firma bu aşamada kuruluştan feragatname isteyebilir. Örnek bir feragatname Ek-3'de verilmiştir.

NOT 1: Gri kutu testlerde testi gerçekleştirmek için gelecek personelin Kuruluşta çalışacağı tarih ve saat dilimleri de kapsam dokümanında belirtilir.

NOT 2: Gri kutu testlerini gerçekleştirmek için gerekli kullanıcı adı ve parola kapsam dokümanında belirtilir. Bu kullanıcı kimliği, firmaya geçici olarak temin edilebilir veya kalıcı bir test hesabının açılarak test dışında "disabled" olacak şekilde ayarlanabilir.

NOT 3: Bu aşamada, kapsam dokümanında yer alan güvenlik uzmanları kuruluş tarafından değerlendirilmeli ve onaylanmalıdır.

5.1.2. Test esnası

Güvenlik testi sürecinde açıklık derecelendirmesi uyarınca acil ya da kritik öneme sahip açıklıkların en kısa sürede kapatılması gerekebilir. Özellikle sızma testi sırasında bu bilgilerin kurum ile paylaşılması veya kapatılması güvenlik testinin bundan sonraki akışını etkileyebileceğinden, firma tarafından daha önce belirlenmiş standart bir form ile bildirimlerin kuruluşa gönderilmesi gerekmektedir.

Güvenlik testlerini yürüten takım ile müşteri kuruluş arasında güvenlik testleri sırasında güvenlik testi kapsamında yapılabilecek olası eklemeler ve güncellemeler için gelen talepler de standart bir form üzerinden yapılmalıdır.

Testler esnasında kuruluş tarafından sistem üzerinde yoğunluk oluşturacak (rapor alma, yığın işleme vb.) herhangi bir işlem yapılmaması tavsiye edilir. Bu tür bir işlem acil olarak gerçekleştirilmesi gerekiyorsa, kuruluş sorumluları firma ile iletişime geçerek, testlerin geçici olarak askıya alınmasını talep etmeleri tavsiye edilir.

5.1.3. Acil durum kotarma

Testler esnasında sistemin işleyişinin kuruluş sorumluları tarafından izlenmesi ve sistemde bir sorun tespit edildiği takdirde, firma sorumlusuna konuyla ilgili bilgi verilerek testlere ara verilmesini istemesi tavsiye edilir. Sistemde tespit edilen sorun uzun süreli veya önemli ise testler daha sonraki bir tarihe ertelenebilir.

5.1.4. Test sonrası

Test sonrası aşama en önemli evredir; çünkü sızma testlerini gerçekleştiren test uzmanına tam sızma yapabilme yetkisi verilmiş ise test sonrasında sistemleri tekrar test öncesi aşamadaki durumlarına geri döndürmelidir. Hedef sisteme yüklenen dosyalar, kayıt defteri değişiklikleri ve oluşturulan zayıflıklar temizlenmelidir.

Testin tamamlanmasını müteakiben, bulunan açıklıklar ve başarılı olan sisteme sızma girişimleri ile ilgili olarak firma tarafından bir Sızma Testi Raporu (bk. Madde 5.3) hazırlanmalı ve kuruluşa iletilmelidir.

Sızma testi raporu sadece kuruluşun sorumluları ile paylaşılır. Kuruluşun bulunan açıklıkların kapatılmasına yönelik olarak bir takvim hazırlayarak açıklıkları kapatması gerekmektedir. Açıklıkların kapatılmasına müteakip doğrulama testi, testi gerçekleştiren firma tarafından yapılarak kuruluşa iletilmelidir.

5.1.5. Test periyodu

Sızma testlerinin kuruluş tarafından düzenli olarak en az yılda 1 defa yaptırılması tavsiye edilir. Bunun dışında kritik uygulama ve sistemler daha sık aralıklarla test ettirilebilir. Ayrıca yeni hizmete girecek olan sistem ve uygulamalar için işletime alma öncesinde sızma testleri yaptırılması tavsiye edilir.

5.1.6. Test zamanlaması

Sızma testleri için mümkün olduğu kadar test edilecek sistemde yoğunluk olmayan saatlerin seçilmesi tavsiye edilir. Gün içinde çalışması kritik olan sistem ve yazılımlar için mesai saatleri dışında bir zaman diliminin tercih edilmesi tavsiye edilir. DoS/DDoS saldırı testi düzenlenecek ise, yine mesai saatleri dışının tercih edilmesi tavsiye edilir.

5.2. Uygulama

5.2.1. Sızma testi aşamaları

Sızma testlerini sekiz aşamada ele almak mümkündür. Bunlar;

1. Ön irtibat
2. Bilgi toplama
3. Tehdit modelleme
4. Zafiyet analizi
5. Sızma
6. Sızma Sonrası
7. Raporlama
8. Doğrulama Testi

Sızma testlerinin firmalar tarafından yukarıda belirtilen aşamalarda ele alınması tavsiye edilir.

Firma, bir sızma testi öncesinde o testte yer alacak personeli resmi olarak belirlemeli ve atamalıdır. Herhangi bir personel aynı anda 3 (üç)'ten fazla testte yer alamaz. Sızma testleri, Madde 5'de yer alan test süreci şartlarına uygun şekilde gerçekleştirilir.

Sızma testlerinde test araçlarının kullanımı, sızma testlerini kolaylaştırıcı bir etkendir. Araçların kullanımı uzmanın kendisinin uzun sürede yapabileceği testleri daha kısa sürede tamamlamasını sağlayacaktır. Ne var ki test araçlarının sonuçları güvenilir olmayabilir ve sadece test araçları ile yapılacak testler, kullanılabilir açıklıkları bulmada yetersiz kalacaktır. Bu kriter çerçevesinde firma sadece test araçlarını kullanarak test yapmamalı, dolayısıyla üretilecek olan test sonuç raporu sadece otomatik test araçlarının çıktısı olmamalıdır. İyi bir test yapılabilmesi için öncelikle uzmanlık temeline dayanan testler yapılmalıdır. Bu testlerin test araçlarının kullanımı ile desteklenmesi tavsiye edilir.

Kendi bünyesinde sızma testi yapan kuruluşların da bu standarda uyum sağlaması tavsiye edilir.

Özellikle kritik sistemlerde yapılacak sızma testleri için sigorta yaptırılarak riskin transfer edilmesi tavsiye edilir.

5.2.2. Sızma testi türleri

Sızma testlerinin çeşitli türleri vardır. Bunlardan bu program kapsamında ele alınanlar aşağıda başlıklar halinde belirtilmiştir.

Ağ ve sistem altyapısı sızma testleri
Hedef sistemin ağ ve sistem altyapısına yönelik gerçekleştirilen sızma testleridir. Özellikle aşağıdaki adımların uygulanması tavsiye edilir.

- Yerel ağ sızma testleri
- İnternet sızma testleri
- Güvenlik duvarı sızma testleri
- Saldırı tespit ve/veya engelleme sistemleri sızma testleri

Web uygulamaları ve veritabanları sızma testleri
Hedef sistemde kullanılan platform ve geliştirme dillerinden bağımsız olarak gerçekleştirilen sızma testleridir. Özellikle aşağıdaki adımların uygulanması tavsiye edilir.

- Bilgi toplama
- Yapılandırma yönetim testleri
- Veri doğrulama testleri
- Hizmet aksatma testleri
- İş mantığı testleri
- Oturum yönetimi testleri
- Web hizmetleri testleri
- Kimlik doğrulama testleri
- Yetkilendirme testleri
- Ajax testleri

Mobil uygulamalar sızma testleri
Akıllı telefon, tablet bilgisayar gibi sistemler ve bu sistemlerde çalışan uygulamalar üzerine yapılan sızma testleridir.

Kablosuz ağlar sızma testleri
Kablosuz ağları ve bu ağda yer alan cihazları hedef alan sızma testleridir. Özellikle aşağıdaki adımların uygulanması tavsiye edilir.

- Erişim Noktası (Access Point) cihazlarına yönelik testler
- Şifreleme kullanmayan sistemlere yönelik testler
- Şifreleme (WEP/WPA/WPA2) kullanan sistemlere yönelik testler
- Kablosuz ağa bağlı istemcilere yönelik testler

Endüstriyel kontrol sistemleri sızma testleri
Bir tesiste veya işletmede yer alan tüm ekipmanların merkezi denetleme kontrol ve veri toplama sistemlerine (SCADA) yönelik gerçekleştirilen sızma testleridir.

Hizmeti aksatma saldırıları (DoS/DDoS)
Hizmeti aksatma saldırıları bir sızma testi değildir. Ancak; bilgi güvenliğinin üç ana bileşeninden birisi olan erişilebilirliği doğrudan hedef aldığı ve günümüzde bu konunun önemi arttığı için bu program kapsamında bahsedilmiştir. Yaygın olarak kullanılan test çeşitleri aşağıda verilmiştir;

- Syn Flood Saldırıları
- ACK Flood Saldırıları
- FIN Flood Saldırıları
- TCP Connection Flood Saldırıları

- UDP Flood DDoS Saldırıları
- ICMP Flood DDoS Saldırıları
- HTTP GET, POST Flood Saldırıları
- DNS Flood DDoS Saldırıları
- Botnet Simülasyonu
- Rate Limiting, Karantina Özelliklerinin Test Edilmesi
- Uygulamalara Özel DoS Testleri
- SSL, HTTPS DoS Testleri

Sosyal mühendislik sızma testleri
Sosyal Mühendislik testleri, çeşitli yöntemlerle kullanıcıları aldatmaya yönelik testlerdir. Bu yöntemler telefon konuşması vb. sözlü iletişim ile olabildiği gibi, e-posta ile yapılan oltalama saldırıları gibi teknik araçlar kullanarak da yapılabilir.

Fiziksel sızma testleri
Bilişim sistemlerine yönelik sızma testleri genel olarak ağ iletişimi üzerine odaklansa da çok eski bir yöntem olan fiziksel sızmalar önemini korumaktadır. Fiziksel sızma testi, önemli bir cihaza yerinde müdahale edilmesi olabileceği gibi cihazın bulunduğu konumdan başka bir konuma nakledilmesi de olabilir.

5.3. Raporlama

Sızma Testi Raporu yapılan güvenlik testlerinin sonuçlarının detaylı olarak aktarıldığı belgedir. Genelde şifreli bir medya halinde test öncesi anlaşma yapılan kuruluş yetkilisine teslim edilmelidir. Kuruluş ile müşteri aralarında yaptıkları anlaşmada aksi belirtilmedikçe, testi yapan firma Test Doğrulama aşamasından sonra Sızma Testi Raporunu imha etmelidir. Gerek testi yaptıran gerekse testi yapan firma testin yapıldığına dair bilgileri paylaşmaktan kaçınmalı ve bu şekilde sistemin hedef haline gelmesi engellenmelidir. Sızma Testlerini yapan firmanın test yapılan kuruluşları referans olarak yayınlamaması tavsiye edilir. Bu şekilde hem test yapılan kurum hem de test yapan güvenlik firması risk altına girmekten korunabilir.

Sızma Testi sonuç raporu en az olmak üzere aşağıdaki şartları sağlamalıdır:

- Kapak Sayfası (testlerin yapıldığı zaman dilimini içeren) olmalıdır.
- Yönetici özeti bölümü olmalıdır. Yönetici özeti, özellikle kısa bir okuma ile rapordaki önemli bilgilere ulaşmak isteyen okuyuculara (özellikle yöneticilere) yönelik bir bölümdür. Yönetici özetinin aşağıdaki alt bölümleri içermesi tavsiye edilir:
- Genel Bilgiler
- Kapsam ve IP Adresleri
- Test Ekibi
- Genel Değerlendirme
- Genel Test Metodolojisi
- Risk Derecelendirme
- Genel Bulgular
- Tavsiye Özeti

Teknik Bilgiler bölümü olmalıdır. Teknik bilgiler raporun teknik detaylarının verildiği kapsamlı bir bölümdür. Teknik bilgilerin aşağıdaki alt bölümleri içermesi tavsiye edilir:

- Giriş

- Bilgi Toplama
- Açıklık Analizi
- Kullanma / Açıklık Onayı
- Kullanma Sonrası Etki
- Varsa Diğer Testler (Sosyal Mühendislik/Fiziksel Sızma Testi/DoS/DDoS v.b.)
- Kullanılan Araçlar

Açıklıklara ait bir risk derecelendirmesi olmalıdır. Derecelendirme sayısal olarak veya farklı renklendirme şeklinde yapılmalıdır. Risk derecelendirmesi, kuruluşun, risklerin giderilmesinde önceliklendirme yapmasına imkân vermek üzere hazırlanmalıdır.

Sızma Test Raporu, Madde 6.1.1. de belirtilen Stajyer sızma testi uzmanı dışındaki diğer uzmanlar tarafından hazırlanmalıdır.

Örnek bir Sızma testi sonuç raporu Ek-1'de verilmiştir. Rapor, sızma testi yaptıran müşterinin ihtiyaçlarına göre değiştirilebilir.

6. YETKİNLİK ŞARTLARI

6.1. Personel yetkinlik şartları

Sızma testlerinin başarılı bir şekilde gerçekleştirilmesinde en temel etken uzmanlık olduğundan dolayı testlerin kalitesinde ve tutarlılığında en önemli kriter de testi yapan personelin uzmanlık seviyesi olarak görülmektedir.

6.1.1. Personel yetkinlik seviyeleri

Personel yetkinlik seviyeleri dört başlıkta değerlendirilecektir.

Stajyer Sızma Testi Uzmanı (ST.S.T.U.)
Kayıtlı Sızma Testi Uzmanı (KA.S.T.U.)
Sertifikalı Sızma Testi Uzmanı (SE.S.T.U.)
Kıdemli Sızma Testi Uzmanı (KI.S.T.U.)

Aşağıda bu yetkinlik seviyelerine dair açıklamalar ve şartlar belirtilmiştir:

6.1.1.1. Stajyer Sızma Test Uzmanı

Stajyer Sızma Testi Uzmanı, sektörde çalışmaya başlamış kişileri tanımlamaktadır. Stajyer Sızma Testi Uzmanlarında aşağıdaki şartlar aranmaktadır;

- Bir yıl içerisinde güvenlik konusunda en az bir (1) adet eğitim almış olmak[1],
- 6 ay bilgi güvenliği/bilişim alanında tecrübe veya Yazılı(Teorik) Sınavda Başarılı Olmak

NOT-1: Firmanın çalıştırdığı stajyerleri genel sağlık sigortalı olarak çalıştırmaları kuvvetle önerilmekte olup, gerçekleştirdiği projelerde yer almak suretiyle tecrübe edindiklerini gösterebilmelidir.

[1] Eğitimler TSE'den ya da TSE tarafından yetkilendirilmiş kuruluşlardan alınmalıdır. Eğitim, Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı ile Web Uygulamaları ve Veri tabanları Sızma Testi Uzmanlığı alanlarında kuvvetle önerilmektedir.

NOT-2: Stajyer Test Uzmanlığı için (eğer 6 ay tecrübe yoksa), Yazılı(Teorik) Sınavda 100 üzerinden 50 puan başarılı olmak beklenmektedir.

6.1.1.2. Kayıtlı Sızma Test Uzmanı

Kayıtlı Sızma Testi Uzmanı olabilmek için aşağıdaki şartların yerine getirilmesi gerekmektedir.

Konu hakkında eğitim almış olmak[2],

- TSE tarafından yapılan yazılı ve uygulamalı uzmanlık sınavında başarılı olmak,
- 1 yıl bilgi güvenliği/bilişim alanında çalışmış olmak veya 1 yıl sızma testi yapmış olmak ve bunu belgelendirmek,
- Madde 6.1.2'deki şartları taşımak,
- En az lise mezunu olmak.

Kayıtlı Sızma Testi Uzmanlığı;

- A1-Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı
- A2-Web Uygulamaları ve Veri tabanları Sızma Testi Uzmanlığı
- A3-Endüstriyel Kontrol Sistemleri Sızma Testi Uzmanı
- A4-Sosyal Mühendislik Sızma Testi Uzmanı
- A5-Fiziksel Sızma Testi Uzmanı
- A6-Mobil Uygulamalar Sızma Testi Uzmanı
- A7-Kablosuz Ağlar Sızma Testi Uzmanı
- A8-DOS/DDOS Testi Uzmanı
- A9-Adli Bilişim Uzmanı

olmak üzere 9 (dokuz) ana daldan oluşmakta olup, aşağıdaki notlara göre

Kayıtlı Sızma Testi Uzmanlığı da genel olarak;

- Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı,
- Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı

Sınıflandırılacaktır.

NOT-1: A1, A5, A7, A8, A3 uzmanlık alanları Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı ile ilgili olup, sınavları ve sertifikasyonu ortak yapılacaktır.

NOT-2: A2, A4, A6, A8 uzmanlık alanları Web Uygulamaları ve Veri tabanları Sızma Testi Uzmanlığı ile ilgili olup, sınavları ve sertifikasyonu ortak yapılacaktır.

NOT-3: A9 uzmanlık alanında Sadece Eğitim verilecek olup, sınav yapılmayacak olup, Adli bilişim uzmanı; bilgisayar ve bilişim teknolojileri kullanılarak işlenen suçlarla ilgili olay yerinin analiz edilmesi,

[2] Eğitimler TSE'den ya da TSE tarafından yetkilendirilmiş kuruluşlardan alınmalıdır. Eğitim, Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı ile Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı alanlarında kuvvetle önerilmektedir.

verilerin toplanması, bu verilerin incelenmesi, varsa eğer suç ile ilgili gerekli ilişkilendirmeler yapılarak sonuçların düzenli bir raporlama neticesinde adli makamlara sunulmasını sağlar.

NOT-4: Kayıtlı Test Uzmanlığı için, Teorik (Yazılı) sınav ve Uygulamalı (Pratik) sınav ortalamasının en az 100 üzerinden 50 puan olması gerekmektedir. Teorik Sınav 1/3, Uygulamalı sınav 2/3 ağırlığındadır.

6.1.1.3. Sertifikalı Sızma Test Uzmanı

Sertifikalı Sızma Testi Uzmanı olabilmek için aşağıdaki şartların yerine getirilmesi gerekmektedir:

- Madde 6.1.3'de belirtilen sertifikalardan en az birine sahip olmak ya da TSE tarafından yapılacak yazılı ve uygulamalı sınavda başarılı olmak,
- 2 yıl bilgi güvenliği/bilişim alanında çalışmış olmak veya 2 yıl sızma testi yapmış olmak ve bunu belgelendirmek,
- En az 1 adet ulusal veya uluslararası düzeyde makale yayınlamak veya bir zafiyet keşfinde bulunup TSE'nin zafiyet bildirim programına bildirmek,
- Madde 6.1.2'deki şartları taşımak,
- En az üniversitelerin iki yıllık ön lisans bölümlerinden birinden mezunu olmak.

Sertifikalı Sızma Testi Uzmanlığı;

- Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı,
- Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı

olmak üzere iki ana daldan oluşmaktadır. Her bir uzmanlık için ayrı sertifikalandırma yapılmaktadır.

NOT: Sertifikalı Test Uzmanlığı için, Teorik (Yazılı) sınav ve Uygulamalı (Pratik) sınav ortalamasının en az 100 üzerinden 70 puan olması gerekmektedir. Teorik Sınav 1/3, Uygulamalı sınav 2/3 ağırlığındadır

6.1.1.4. Kıdemli Sızma Test Uzmanı

Kıdemli Sızma Testi Uzmanı olabilmek için aşağıdaki şartların yerine getirilmesi gerekmektedir.

- TSE tarafından yapılan yazılı ve uygulamalı uzmanlık sınavında başarılı olmak,
- 4 yıl bilgi güvenliği alanında çalışmış olmak veya 4 yıl sızma testi yapmış olmak ve bunu belgelendirmek,
- En az 1 adet ulusal veya uluslararası düzeyde makale yayınlamak veya bir zafiyet keşfinde bulunup TSE'nin zafiyet bildirim programına bildirmek.
- Madde 6.1.2'deki şartları taşımak,
- En az üniversitelerin dört yıllık lisans bölümlerinden birinden mezunu olmak.

Kıdemli Sızma Testi Uzmanlığı;

- Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı,
- Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı

Olmak üzere iki ana daldan oluşmaktadır. Her bir Uzmanlık için ayrı sertifikalandırma yapılmaktadır.

Sertifikalı Sızma Testi Uzmanı, Kayıtlı Sızma Testi Uzmanı, Sertifikalı Sızma Testi Uzmanı ve Kıdemli Sızma Testi Uzmanı için eğitim, sınav ve belge geçerlilik süreleri 3 (üç) yıldır. Üçüncü yılın sonunda yetkilendirilmiş personeller yetkilerini devam ettirebilmek için;

- Kayıtlı Sızma Testi Uzmanları, tekrar çoktan seçmeli testte başarılı olmalı,
- Sertifikalı Sızma Testi Uzmanları sahip oldukları sertifikaları devam ettirmeli,
- Kıdemli Sızma Testi Uzmanları çoktan seçmeli ve uygulamalı testte başarılı olmalıdır.

Not-1: Sızma Testi Uzmanları, hizmet verdiği kurum ve kuruluşlardaki gizlilik içermeyen Sızma Testi Rapor Özetlerini E-imza ile imzalayarak, gerektiğinde TSE yetkililerine gönderebilmelidirler.

Not-2: Kıdemli Test Uzmanlığı için, Teorik (Yazılı) sınav ve Uygulamalı (Pratik) sınav ortalamasının en az 100 üzerinden 90 puan olması gerekmektedir. Teorik Sınav 1/3, Uygulamalı sınav 2/3 ağırlığındadır.

6.1.2. Özel şartlar

- Kamu kurumlarında ve kamu kurumu niteliğindeki kurumlarda test yapacak personellerde Türk vatandaşı olma ve kamu haklarından mahrum bulunmama şartları aranır. Bu şartları, kuruluşta takip etmelidir.
- Sızma testi yapacak kişilerin adli sicil kaydı ve/veya adli sicil arşiv kaydı olmamalıdır.

Ayrıca, ihtiyaç duyulan durumlarda kuruluşlar kendi güvenlik düzeylerine göre özel güvenlik, kişi güvenlik ya da klerans gibi belgeleri de isteyebilirler.

6.1.3. Eşdeğerlik çizelgesi[3]

Sertifikalı Sızma Testi Uzmanı belgelendirmelerinde aşağıdaki uluslararası sertifikalar eşdeğer olarak kabul edilecektir. Belirtilen sertifikalar haricinde Madde 6.1.1.3 deki diğer şartların yerine getirilmesi gerekmektedir. Sertifikalı Sızma Testi Uzmanlığı için kabul edilecek sertifikalar Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı ve Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı başlıkları altında iki ayrı tabloda verilmiştir.

Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı Eşdeğerlik Tablosu:

Sertifikalandırma Otoritesi	Sertifika Adı
EC-Council	Licensed Penetration Tester (LPT)
GIAC	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
GIAC	GIAC Penetration Tester (GPEN)
Offensive Security	Offensive Security Certified Professional (OSCP)

Çizelge 1 – Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı Eşdeğerlik Tablosu

Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı Eşdeğerlik Tablosu:

Sertifikalandırma Otoritesi	Sertifika Adı
GIAC	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
GIAC	GWAPT (GIAC Web Application Penetration Tester)
OWASP	OSWE (Offensive Security Web Expert)

[3] Eşdeğerlik çizelgesi, programın yayınlanmasından 18 ay sonra yapılacak düzenleme ile geçerliliğini kaybedecektir.

Çizelge 2 – Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı Eşdeğerlik Tablosu

6.1.4 Genel Şartlar ve Uygulamalar

- Tüm Uzmanlık alanlarında istenen bilgi güvenliği/bilişim/sızma testi tecrübeleri için, daha önceden bilgi güvenliği/siber güvenlik/bilişim/sızma testi alanlarında ilgili eğitimler gün/hafta/ay vb. süre olarak hesaplanıp, tecrübeden sayılabilecektir.
- Stajyer ve Kayıtlı Test Uzmanlıkları için Ön lisans ve Lisans öğrenimlerinde bilgi güvenliği/siber güvenlik/bilişim/sızma testi alanlarında alınan dersler en fazla 1 yıl olarak; Sertifikalı ve Kıdemli Test Uzmanlıkları için ise Yüksek Lisans ve Doktora öğreniminde bilgi güvenliği/siber güvenlik/bilişim/sızma testi alanlarında alınan dersler, gün/hafta/ay vb. süre olarak hesaplanıp en fazla 1 er yıl (Yük. Lisans 1 yıl, Doktora 1 yıl), tecrübeden sayılabilecektir.
- Uygulamalı Eğitim ve Sınavlar genel olarak A1-Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı ve A2-Web Uygulamaları ve Veri tabanları Sızma Testi Uzmanlıklarından yapılacak olup, diğer A3,A4,A5,A6,A7,A8,A9 uzmanlık alanlarından teorik(yazılı) eğitim ve sınav yapılacaktır.

6.2. Firma yetkinlik şartları

Aşağıdaki çizelgede personel sayıları ve uzmanlıkları temelinde firma seviyeleri ve ISO/IEC 27001:2005 şartı olup olmadığı verilmiştir.

Firma Seviyesi	KI.S.T.U.	SE.S.T.U.	KA.S.T.U.	ST.S.T.U.	ISO/IEC 27001:2005 Uyumluluğu
A	1	1	1	2	Kısmen
B		1	1	1	Kısmen
C			1		Kısmen

Çizelge 3 – Personel Sayılarına ve Uzmanlıklarına göre firma seviyeleri

A, B ve C seviyelendirmesi firmaların personel kapasiteleri göz önüne alınarak yapılmıştır. Bu seviyelendirme ile sızma testi yaptıran kuruluşların kendi büyüklüklerine uygun firmaları tercih edebilmesi amaçlanmaktadır.

Bu program da belirtilen şartlara uyum sağladığını iddia eden firmalar TSE'ye başvurarak uyumlarını belgelendirirler. Firmalar, TSE tarafından yıllık olarak denetime tabii tutulur ve belgeleri yenilenir.

Firmalar için ISO/IEC 27001:2005 sertifikasyonu zorunlu olmamakla birlikte, ISO/IEC 27001:2005 in aşağıda yer alan ek kontrol maddelerine uyum sağlamaları gerekmektedir.

Madde No	Kontrol	Zorunluluk		
		A	B	C
A.5 Güvenlik Politkası				
A.5.1 Bilgi güvenliği politkası				
A.5.1.1	Bilgi güvenliği politika dokümanı	X	X	X

A.5.1.2	Bilgi güvenliği politikasını gözden geçirme	X	X	X
A.6 Bilgi güvenliği organizasyonu				
A.6.1 İç organizasyon				
A.6.1.1	Yönetimin bilgi güvenliğine bağlılığı	X	X	
A.6.1.2	Bilgi güvenliği koordinasyonu	X	X	
A.6.1.3	Bilgi güvenliği sorumluluklarının tahsisi	X	X	
A.6.1.4	Bilgi işleme tesisleri için yetki prosesi	X	X	
A.6.1.5	Gizlilik anlaşmaları	X	X	X
A.6.1.6	Otoritelerle iletişim	X	X	X
A.6.1.7	Özel ilgi grupları ile iletişim	X	X	X
A.6.1.8	Bilgi güvenliğinin bağımsız gözden geçirmesi			
A.6.2 Dış taraflar				
A.6.2.1	Dış taraflarla ilgili riskleri tanımlama	X	X	X
A.6.2.2	Müşterilerle ilgilenirken güvenliği ifade etme	X	X	X
A.6.2.3	Üçüncü taraf anlaşmalarında güvenliği ifade etme	X	X	X
A.7 Varlık yönetimi				
A.7.1 Varlıkların sorumluluğu				
A.7.1.1	Varlıkların envanteri	X	X	
A.7.1.2	Varlıkların sahipliği	X	X	
A.7.1.3	Varlıkların kabul edilebilir kullanımı	X	X	
A.7.2 Bilgi sınıflandırması				
A.7.2.1	Sınıflandırma kılavuzu	X	X	
A.7.2.2	Bilgi etiketleme ve işleme	X	X	
A.8 İnsan kaynakları güvenliği				
A.8.1 İstihdam öncesi				
A.8.1.1	Roller ve sorumluluklar	X	X	
A.8.1.2	Tarama	X	X	
A.8.1.3	İstihdam koşulları	X	X	
A.8.2 Çalışma esnasında				
A.8.2.1	Yönetim sorumlulukları	X	X	
A.8.2.2	Bilgi güvenliği farkındalığı, eğitim ve öğretimi	X	X	
A.8.2.3	Disiplin prosesi	X	X	
A.8.3 İstihdamın sonlandırılması veya değiştirilmesi				
A.8.3.1	Sonlandırma sorumlulukları	X	X	
A.8.3.2	Varlıkların iadesi	X	X	
A.8.3.3	Erişim haklarının kaldırılması	X	X	
A.9 Fiziksel ve çevresel güvenlik				
A.9.1 Güvenli alanlar				
A.9.1.1	Fiziksel güvenlik çevresi			
A.9.1.2	Fiziksel giriş kontrolleri	X	X	
A.9.1.3	Ofisler, odalar ve olanakları korumaya alma	X	X	
A.9.1.4	Dış ve çevresel tehditlere karşı koruma	X	X	
A.9.1.5	Güvenli alanlarda çalışma	X	X	
A.9.1.6	Açık erişim, dağıtım ve yükleme alanları			
A.9.2 Teçhizat güvenliği				

A.9.2.1	Teçhizat yerleştirme ve koruma	X	X	
A.9.2.2	Destek hizmetleri			
A.9.2.3	Kablolama güvenliği	X	X	
A.9.2.4	Teçhizat bakımı			
A.9.2.5	Kuruluş dışındaki teçhizatın güvenliği	X	X	X
A.9.2.6	Teçhizatın güvenli olarak elden çıkarılması ya da tekrar kullanımı	X	X	X
A.9.2.7	Mülkiyet çıkarımı	X	X	
A.10 Haberleşme ve işletim yönetimi				
A.10.1 Operasyonel prosedürler ve sorumluluklar				
A.10.1.1	Dokümante edilmiş işletim prosedürleri	X	X	
A.10.1.2	Değişim yönetimi	X	X	
A.10.1.3	Görev ayrımları	X	X	
A.10.1.4	Geliştirme, test ve işletim olanaklarının ayrımı	X	X	X
A.10.2 Üçüncü taraf hizmet sağlama yönetimi				
A.10.2.1	Hizmet sağlama	X	X	
A.10.2.2	Üçüncü taraf hizmetleri izleme ve gözden geçirme	X	X	
A.10.2.3	Üçüncü taraf hizmetlerdeki değişiklikleri yönetme	X	X	
A.10.3 Sistem planlama ve kabul				
A.10.3.1	Kapasite planlama			
A.10.3.2	Sistem kabulü			
A.10.4 Kötü niyetli ve mobil koda karşı koruma				
A.10.4.1	Kötü niyetli koda karşı kontroller	X	X	X
A.10.4.2	Mobil koda karşı kontroller	X	X	X
A.10.5 Yedekleme				
A.10.5.1	Bilgi yedekleme	X	X	X
A.10.6 Ağ güvenliği yönetimi				
A.10.6.1	Ağ kontrolleri	X	X	
A.10.6.2	Ağ hizmetleri güvenliği	X	X	
A.10.7 Ortam işleme				
A.10.7.1	Taşınabilir ortam yönetimi	X	X	
A.10.7.2	Ortamın yok edilmesi	X	X	
A.10.7.3	Bilgi işleme prosedürleri	X	X	
A.10.7.4	Sistem dokümantasyonu güvenliği	X	X	X
A.10.8 Bilgi değişimi				
A.10.8.1	Bilgi değişim politikaları ve prosedürleri	X	X	X
A.10.8.2	Değişim anlaşmaları	X	X	X
A.10.8.3	Aktarılan fiziksel ortam	X	X	
A.10.8.4	Elektronik mesajlaşma	X	X	X
A.10.8.5	İş bilgi sistemleri	X	X	
A.10.9 Elektronik ticaret hizmetleri				
A.10.9.1	Elektronik ticaret			
A.10.9.2	Çevrimiçi işlemler			
A.10.9.3	Herkese açık bilgi			
A.10.10 İzleme				
A.10.10.1	Denetim kaydetme	X	X	

A.10.10.2	Sistem kullanımını izleme	X	X	
A.10.10.3	Kayıt bilgisinin korunması	X	X	
A.10.10.4	Yönetici ve operatör kayıtları	X	X	
A.10.10.5	Hata kaydı	X	X	
A.10.10.6	Saat senkronizasyonu	X	X	
A.11 Erişim kontrolü				
A.11.1 Erişim kontrolü için iş gereksinimi				
A.11.1.1	Erişim kontrolü politikası	X	X	
A.11.2 Kullanıcı erişim yönetimi				
A.11.2.1	Kullanıcı kaydı	X	X	
A.11.2.2	Ayrıcalık yönetimi	X	X	
A.11.2.3	Kullanıcı parola yönetimi	X	X	
A.11.2.4	Kullanıcı erişim haklarının gözden geçirilmesi	X	X	
A.11.3 Kullanıcı sorumlulukları				
A.11.3.1	Parola kullanımı	X	X	X
A.11.3.2	Gözetimsiz kullanıcı teçhizatı	X	X	
A.11.3.3	Temiz masa ve temiz ekran politikası	X	X	X
A.11.4 Ağ erişim kontrolü				
A.11.4.1	Ağ hizmetlerinin kullanımına ilişkin politika	X	X	
A.11.4.2	Dış bağlantılar için kullanıcı kimlik doğrulama	X	X	
A.11.4.3	Ağlarda teçhizat tanımlama	X	X	
A.11.4.4	Uzak tanı ve yapılandırma portu koruma	X	X	
A.11.4.5	Ağlarda ayrım	X	X	
A.11.4.6	Ağ bağlantı kontrolü	X	X	
A.11.4.7	Ağ yönlendirme kontrolü	X	X	
A.11.5 İşletim sistemi erişim kontrolü				
A.11.5.1	Güvenli oturum açma prosedürleri	X	X	X
A.11.5.2	Kullanıcı kimlik tanımlama ve doğrulama	X	X	X
A.11.5.3	Parola yönetim sistemi	X	X	
A.11.5.4	Yardımcı sistem programlarının kullanımı	X	X	
A.11.5.5	Oturum zaman aşımı	X	X	X
A.11.5.6	Bağlantı süresinin sınırlandırılması	X	X	
A.11.6 Uygulama ve bilgi erişim kontrolü				
A.11.6.1	Bilgi erişim kısıtlaması	X	X	
A.11.6.2	Hassas sistem yalıtımı	X	X	
A.11.7 Mobil bilgi işleme ve uzaktan çalışma				
A.11.7.1	Mobil bilgi işleme ve iletişim	X	X	
A.11.7.2	Uzaktan çalışma	X	X	
A.12 Bilgi sistemleri edinim, geliştirme ve bakımı				
A.12.1 Bilgi sistemlerinin güvenlik gereksinimleri				
A.12.1.1	Güvenlik gereksinimleri analizi ve belirtimi			
A.12.2 Uygulamalarda doğru işleme				
A.12.2.1	Giriş verisi geçerleme			
A.12.2.2	İç işleme kontrolü			
A.12.2.3	Mesaj bütünlüğü			

A.12.2.4	Çıkış verisi geçerleme			
A.12.3 Kriptografik kontroller				
A.12.3.1	Kriptografik kontrollerin kullanımına ilişkin politika	X	X	X
A.12.3.2	Anahtar yönetimi	X	X	X
A.12.4 Sistem dosyalarının güvenliği				
A.12.4.1	Operasyonel yazılımın kontrolü			
A.12.4.2	Sistem test verisinin korunması			
A.12.4.3	Program kaynak koduna erişim kontrolü			~~X~~
A.12.5 Geliştirme ve destekleme proseslerinde güvenlik				
A.12.5.1	Değişim kontrol prosedürleri			
A.12.5.2	İşletim sistemindeki değişikliklerden sonra teknik gözden geçirme			
A.12.5.3	Yazılım paketlerindeki değişikliklerdeki kısıtlamalar			
A.12.5.4	Bilgi sızması			
A.12.5.5	Dışarıdan sağlanan yazılım geliştirme			
A.12.6 Teknik açıklık yönetimi				
A.12.6.1	Teknik açıklıkların kontrolü			
A.13 Bilgi güvenliği ihlal olayı yönetimi				
A.13.1 Bilgi güvenliği olayları ve zayıflıklarının rapor edilmesi				
A.13.1.1	Bilgi güvenliği olaylarının rapor edilmesi	X	X	
A.13.1.2	Güvenlik zayıflıklarının rapor edilmesi	X	X	
A.13.2 Bilgi güvenliği ihlal olayları ve iyileştirmelerin yönetilmesi				
A.13.2.1	Sorumluluklar ve prosedürler	X	X	
A.13.2.2	Bilgi güvenliği ihlal olaylarından öğrenme	X	X	X
A.13.2.3	Kanıt toplama	X	X	X
A.14 İş sürekliliği yönetimi				
A.14.1 İş sürekliliği yönetiminin bilgi güvenliği hususları				
A.14.1.1	Bilgi güvenliğini iş sürekliliği yönetim prosesine dahil etme			
A.14.1.2	İş sürekliliği ve risk değerlendirme			
A.14.1.3	Bilgi güvenliğini içeren süreklilik planlarını geliştirme ve gerçekleştirme	X	X	
A.14.1.4	İş sürekliliği planlama çerçevesi			
A.14.1.5	İş sürekliliği planlarını test etme, sürdürme ve yeniden değerlendirme			
A.15 Uyum				
A.15.1 Yasal gereksinimlerle uyum				
A.15.1.1	Uygulanabilir yasaları tanımlanma	X	X	X
A.15.1.2	Fikri mülkiyet hakları (IPR)	X	X	X
A.15.1.3	Kurumsal kayıtların korunması	X	X	X
A.15.1.4	Veri koruma ve kişisel bilgilerin gizliliği	X	X	X
A.15.1.5	Bilgi işleme olanaklarının kötüye kullanımını önleme			
A.15.1.6	Kriptografik kontrolleri düzenleme	X	X	
A.15.2 Güvenlik politikaları ve standardlarla uyum ve teknik uyum				
A.15.2.1	Güvenlik politikaları ve standardlarla uyum	X	X	
A.15.2.2	Teknik uyum kontrolü	X	X	
A.15.3 Bilgi sistemleri denetim hususları				
A.15.3.1	Bilgi sistemleri denetim kontrolleri	X	X	
A.15.3.2	Bilgi sistemleri denetim araçlarının korunması	X	X	

Çizelge 4 – ISO/IEC 27001:2005 Ek kontrol maddelerinin bir alt kümesi

Uygunluğu kontrol etmek için yapılan faaliyetlerin kayıtları tutulmalıdır.

Bütün kayıtlar okunaklı olmalı, zarar görmelerini veya bozulmalarını ve kaybolmalarını önlemek için uygun şartları sağlayabilecek mekanlarda kolayca ulaşılabilecek şekilde saklanmalı ve muhafaza edilmelidir. Kayıtların muhafaza edilme süreleri belirlenmelidir.

Not - Kayıtlar, basılı kopya veya elektronik kayıt gibi herhangi bir ortamda olabilir.

Saklanması gereken bütün kayıtlar, emniyetli bir şekilde ve gizlilik içinde muhafaza edilmelidir.

6.2.1. Kuruluş ile iletişim şartları

Sızma testlerinde olumsuz durumlar ile karşılaşılmaması (işletimsel sistemlerin göçmesi, dışarıya veri sızması vb.) ve testlerin etkin ve zamanlı bir biçimde gerçekleştirilmesinde kuruluş ile etkin iletişim çok önemli rol oynar. Hem sızma testi öncesinde hem de sızma testi esnasında kuruluş ile sürekli iletişim halinde olmak gerekir. Firma, sızma testi gidişatına göre verilmesi gereken kritik bazı kararlarda (Hizmet Aksatma testini devam ettirip ettirmeme vb.) mutlaka kuruluşun görüşünü almalıdır.

Sızma testleri esnasında, kuruluş gerçek siber saldırılara da maruz kalabilmektedir. Bu noktada kuruluşun, sızma testlerini izleyerek, testler ile siber saldırılar arasında ayrım yapabilmesi ve firma ile iletişim kurarak, testi durdurmasını istemesi önem arz etmektedir. Testin siber saldırı esnasında durdurulması, hem sistemi korumak açısından hem de sonradan yapılacak olan adli bilişim analiz çalışmasını da kolaylaştırması açısından önemlidir.

Aşağıdaki hususlara dikkat edilmelidir:

- Firma, sızma testine başlamadan önce kuruluşunun irtibat noktasını bilgilendirmelidir.
- Firma, kuruluş ile gizlilik dereceli veya hassas bilgilerin elektronik ortamdan paylaşımında yeterli seviyede güvenlik kontrollerini (dosyayı şifreli gönderme, e-postayı şifreli, elektronik imzalı gönderme, güvenli ftp vb.) uygulamalıdır.
- Firmanın, sızma testi öncesinde kuruluş ile çevrimiçi veya karşılıklı olarak bir toplantı yapması ve sızma testlerinde karşılaşılabilecek riskler ve alınabilecek önlemler konusunda kuruluşu bilgilendirmesi tavsiye edilir.
- Firma sızma testi öncesinde kapsamı net şekilde belirlemeli ve buna uygun olarak testleri gerçekleştirmelidir. Test esnasında kapsamın genişletilmesi söz konusu olursa firma bu kararı kuruluş ile görüşerek ve kuruluşun yazılı onayına istinaden alabilir ve buna göre testlerin kapsamını genişletebilir veya daraltabilir.

6.2.2. Gizlilik ve kayıt saklama şartları

Sızma testi ile ilgili gerek kuruluş tarafından doldurulan anket, form vb. dokümanlar gerekse firma tarafından üretilen sızma testi sonuç raporu vb. dokümanlar gizlilik derecesine haiz dokümanlardır. Bu tür dokümanlar üretim, kullanım ve saklama aşamalarında hassasiyetle ele alınmalı ve çalınma, yetkisiz erişim, kaybolma vb. risklere karşı korunmalıdır.

Test raporlarının saklanmasında kuruluşunun görüşü alınmalı ve buna göre hareket edilmelidir. Önceki yapılan testlere ait raporlar saklanacak ise, bu raporlar firma personelinin taşınabilir bilgisayarlarında veya taşınabilir ortamlarda (harici disk, flash disk vb.) bulundurulmamalı, gerek yazılı kopyaları gerekse elektronik kopyaları mutlaka güvenli bir ortamda saklanmalıdır.

Raporlar özellikle sunumlarda kullanılmamalı ve örnek mahiyetinde diğer kuruluşlara gösterilmemelidir. Raporların saklanması, bir sonraki testte daha önce bulunan açıklıkların kapatılıp kapatılmadığını anlamak açısından firma için yararlı olacaktır. Ne var ki raporların ele geçirilmesi veya çalınması da firma için yüksek bir güvenlik riski teşkil etmektedir.

Firma belirli bir teste ait sızma testi raporunu saklayabilmesi için testi yaptıran kuruluştan mutlaka resmi nitelikte yazılı olarak izin almalıdır. Bu izne binaen firma sızma testi raporlarını saklayabilir.

Firma, hangi personelinin hangi testlerde görev aldığını dair kayıtları tutmalı ve en az 2 yıl süre ile bu kayıtları saklamalıdır. Ayrıca sızma testlerinde yer alan personelin isimleri de Sızma testi raporunda belirtilmelidir.

Test raporlarına erişim, bilmesi gereken prensibine göre verilmeli, yetkilendirilmeli ve kontrol edilmelidir. Raporlara erişim sadece testi yapan veya doğrudan yöneten kişiler ile kısıtlı kalmalı ve bunlar haricinde erişim olmamalıdır. Bir önceki testin devamı niteliğinde yeni bir test yapılacak ise bu durumda yeni testi yapacak olan personel eski test raporuna erişmek üzere yetkilendirilebilir. Bu durumda yetkilendirmenin yetkili kişi tarafından onaylanması gerekir.

Yukarıdaki kriterler temelinde örneğin; firmanın muhasebe müdürü veya iş geliştirme müdürünün test raporlarına erişimi olmamalıdır. Yeni yapılacak bir sızma testi için atanan proje yöneticisi, sızma testi yapacak olan personele aynı kuruluşun bir önceki sızma testine dair erişim için yetkilendirebilir.

Firmanın farklı iş kollarında faaliyet göstermesi durumunda ISO/IEC 27001:2005 ek maddelerine uyum sadece ilgili birimi için aranır. İlgili birimin, diğer birimlerle çalışma alanı ve bilgi paylaşımı v.b. durumları söz konusu olduğunda gizlilik şartlarına uygunluk sağlanır.

6.2.3. Kapanış işlemleri

Firma yasal olarak faaliyetlerine son vermesi durumunda, kendisinde bulunan sızma testi sonuç raporlarını geri dönülemez şekilde imha etmelidir.

6.2.4. Bildirim şartları

TSE tarafından yetkilendirilmiş personeller, firma değiştirmeleri veya çalıştıkları firmadan ayrılmaları durumunda en geç 15 takvim günü içinde bu durumu TSE'ye bildirmelidirler. Aynı şekilde firmalar da, yetkilendirilmiş bir personel firmadan ayrıldığında veya firmada göreve başladığında bu durumu TSE'ye bildirmelidirler.

Firmadan ayrılan personel, firmanın belgelendirme sınıfı ile ilgili değişikliğe neden oluyor ise ayrılış tarihini müteakip iki (2) ay içerisinde eşdeğer yetkinliği sahip bir personel istihdam edilmelidir.

6.2.5. Yabancı uzman çalıştırma ile ilgili şartlar

Kamu kurumlarında ve kamu kurumu niteliğindeki kurumlarda test yapacak personellerde Türk vatandaşı olma ve kamu haklarından mahrum bulunmama şartları aranır. Bu şartları, kuruluşta takip etmelidir.

Sızma testlerinde çalışan uzmanların ne renk şapka taktıkları çok net olmayabildiğinden, özellikle çeşitli kötü niyetli organizasyonların hedefi haline gelebildiklerinden ve bu alanda yüksek meblağlar söz konusu olduğundan dolayı, yabancı uzman çalıştırma konusu hassasiyetle ele alınmalıdır.

Bu noktada her ne kadar yukarıdaki koşullar yerli uzmanlar açısından da geçerli olsa bile, hukuksal açıdan bakıldığında, kanunsuz bir davranış neticesinde ülke kanunlarının uygulanması uluslararası kanunlara göre çok daha kolay ve caydırıcı etkiye sahiptir. Ayrıca; teknik olarak bakıldığında yurtdışından yapılan saldırıların takip edilmesi de yine yurtiçinden yapılan saldırılara göre çok daha zor olabilmektedir.

Bu nedenle firmalar kamu kurum ve kuruluşlarına yaptıkları sızma testlerinde yabancı uzman çalıştırmamalıdırlar. Özel sektör kuruluşlarına yapılan testlerde de yabancı uzman çalıştırılmaması tavsiye edilir. Özel durumlarda (yurtiçinde belli bir alanda uzman bulunamıyor ise vb.) yabancı uzman çalıştırma yoluna gidilebilir fakat firmanın bunu net bir şekilde ve delilleri ile gerekçelendirebilmesi gerekmektedir. Gerekçelendirme delili, firmanın ilgili pozisyon için ilana çıkması ve ilanın en az 2 (iki) hafta askıda kalması fakat eleman bulamamasıdır.

7. Kişisel bilgilerin gizliliği

Firma yaptığı testler esnasında kuruluş çalışanlarının kişisel bilgilerine ulaşması durumunda, bu bilgileri kuruluş ile paylaşmamalı, sızma testi sonuç raporuna eklememeli ve bir kopyasını kendisine almamalıdır. Sızma test raporunda kullanıcı adı ve parolaları maskelenmelidir.

8. Kanunlara ve mevzuata uyum

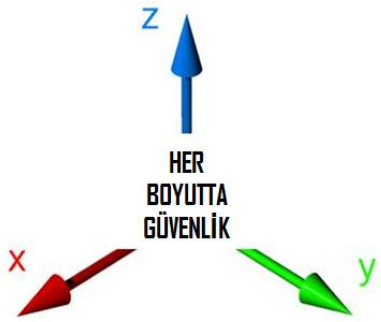
Testler yasadışı araçları veya yöntemleri içermemelidir. Örnek: DDOS için Botnet kiralama vb. Ayrıca; testler esnasında kuruluş ile sözleşmede veya teknik şartnamede belirlenmiş olan kapsam dışına kuruluşun yazılı izni olmadan çıkılmamalıdır.

Sızma testleri esnasında firma, sadece kuruluşa ait içeriklere erişim sağlanabildiğini göstermeli, bunun dışında kuruluşa ait içeriklerin tamamına erişim sağlayarak tüm içeriği kopyalamamalı ve üçüncü taraflar ile paylaşmamalıdır. Firmanın içeriklere erişim sağlandığını gösterebilmesi için gerekiyorsa örnek olarak birkaç kayıt kopyalayabilir.

Program kapsamında yetkilendirilen personeller için taahhütname, firmalar için ise belge kullanım sözleşmesi imzalanacaktır. Yetkilendirilmiş personel ve firmalar imzaladıkları taahhütname ve sözleşmedeki şartlara uymadıkları takdirde yetkilendirme belgeleri TSE tarafından geri alınır.

EK-1

ÖRNEK BİR SIZMA TESTİ SONUÇ RAPORU



XYZ LTD. ŞTİ.

ABC KURUMU

SIZMA TESTİ RAPORU

XYZ Bilgi Güvenliği Limited Şirketi
Cumhuriyet Mah. Demokrasi Sok. No: 17/6 ÇANKAYA/ANKARA
Telefon : 0 312 123 45 67
Faks : 0 312 123 45 68

1 Ocak – 31 Ocak 2013

İçindekiler

UYARI

Rapor içeriği gizli olup iki tarafın yazılı mutabakatı olmadan üçüncü taraflara basılı olarak ya da elektronik ortamda transfer edilemez veya paylaşılamaz.

Rapor, tarama süresi içinde varlığı bilinen veya tarafımızdan tespit edilen güvenlik açıklıklarını içerecektir. Tarama işlemi bittikten sonra rapor teslim edilene kadar geçen süre içerisinde çıkabilecek yeni güvenlik açıklarına dair eksikliklerden dolayı raporu hazırlayan firma sorumlu tutulamaz.

Rapor içinde yer alan çözüm önerilerine konu hakkında fikir verme amaçlı yer verilmiştir. Çözüm önerilerinin uygulanması sebebi ile çıkabilecek problemlerden raporu hazırlayan firma sorumlu tutulamaz. Önerilerde sunulan değişikliklerden gerçekleştirilmeden önce konu hakkında uzman kişilerden destek alınması tavsiye edilir.

1. YÖNETİCİ ÖZETİ

1.1. GENEL BİLGİLER

Bu rapor, XYZ Ltd. Şti. tarafından ABC Kurumu sistemleri üzerindeki güvenlik açıklarını ortaya çıkarmak amacı ile 1 Ocak - 31 Ocak 2013 tarihleri arasında gerçekleştirilen sızma testleri ve güvenlik değerlendirmeleri çalışmalarının detaylı sonuçlarını içermektedir.

Sızma testi kapsamında ABC Kurumu altyapısı ve sunucularının çalışmasını etkileyecek araçlar kurum yetkililerinin bilgisi olmadan kullanılmamış, hizmetin aksamasına neden olabilecek herhangi bir işlem gerçekleştirilmemiştir.

Bilgi sistemleri, intranet ve internet olmak üzere iki ayrı taramaya tabii tutulmuştur. Internet üzerinden gerçekleştirilen testler, sistemler hakkında herhangi bir bilgisi olmayan personel tarafından gerçekleştirilmiştir. Intranet üzerinden gerçekleştirilen testlerde çeşitli seviyede yetkilendirilmiş kullanıcı hakları kullanılarak sistemler test edilmiş ve bunlardan doğabilecek riskler raporun ilerleyen kısımlarında açıklanmıştır.

Test ile sunucular üzerinde bulunabilecek muhtemel güvenlik açıklıklarının kötü niyetli saldırganlardan önce ortaya çıkartılması ve önlem alınması amaçlanmaktadır.

Rapor, bulunan her güvenlik açığının risk derecesini, açık hakkında açıklamaları, daha detaylı bilgi bulabileceğiniz bağlantıları, güvenlik açığının nasıl kapatılabileceği hakkında gerekli bilgiyi, açığın nasıl kötüye kullanılabileceği hakkında örnekleri ve uzman personelin yorum ve önerilerini içermektedir.

Açıklıkların kapatılmasında izlenecek sırayı belirlerken teknik raporda belirtilen açıklık önem dereceleri öncelikli rol oynamalıdır.

Rapor okuyucunun TCP/IP ve kullanılan teknoloji hakkında temel bilgilere sahip olduğu düşünülerek hazırlanmıştır. Bu sebeple raporlarda kullanılan terimler ile ilgili her hangi bir açıklama yapılmayacaktır.

1.2. KAPSAM VE IP ADRESLERİ

Bu tarama kapsamında taramayı yaptıran ABC Kurumu tarafından belirlenen ve aşağıda listelenen sunuculara yönelik saldırı ve sızma testi gerçekleştirilmiştir. Bu testler esnasında, test edilen sunucular tarafından verilen hizmetlerin sekteye uğratılmaması amacıyla Denial of Service (DoS) saldırıları ayrı yapılmıştır. Denial of Service (DoS) saldırıları ile ilgili bilgi raporun ilerleyen kısımlarında özel bölüm olarak verilmiştir. Test edilen IP adresleri aşağıda listelenmiştir.

212.125.85.1-212.125.85.255 adres aralığı internet tarafında taranmıştır.

Sunucu Adı	IP Adresi	DNS Adı	Açıklama
MAIL	212.125.85.6	mail.abc.gov.tr	E-posta sunucusu
WEB	212.125.85.100	www.abc.gov.tr	Web Sunucusu
WEB	212.125.85.104	www.kml.gov.tr	Web Sunucusu
DNS	212.125.85.150	dns.abc.gov.tr	DNS Sunucusu

192.168.100.0-192.168.100.255 adres aralığı yerel ağ tarafında taranmıştır.

Sunucu Adı	IP Adresi	DNS Adı	Açıklama
DC	192.168.100.10	dc.abc.gov.tr	Etki Alanı Sunucusu
WEB	192.168.100.100	www.abc.net.tr	Intranet Uygulama Sunucusu
DNS	192.168.100.150	dns.abc.net.tr	DNS Sunucusu
SQL	192.168.100.101	Sql.abc.net.tr	Intranet Veri tabanı Sunucusu

1.3. TEST EKİBİ

Ahmet CAN	Kıdemli Sızma Testi Uzmanı*
Nur ÖZDEMİR	Sertifikalandırılmış Sızma Testi Uzmanı*
Cem ALPUN	Kayıtlı Sızma Testi Uzmanı*
Meryem YILMAZ	Stajyer Sızma Testi Uzmanı*
Ümit GÜZEL	Stajyer Sızma Testi Uzmanı*

* TSE XXX programına uygun uzmanlık seviyesidir.

1.4. GENEL DEĞERLENDİRME

Gerçekleştirilen kontroller, özellikle web uygulamalarının güvenlik açısından son derece sorunlu kodlara sahip olduğunu göstermiştir. Bu da testler neticesinde SQL Injection gibi önemli ve tehlikeli güvenlik açıklarının tespit edilmesine yol açmıştır. Kullanıcı tarafından yollanan verilerin, uygulama tarafından kullanılmadan önce sorun oluşturacak karakterler için kontrol edilmemesi SQL Injection, XSS (CrossSiteScripting) gibi web uygulama problemlerinin ortaya çıkmasına neden olmaktadır. Tespit edilen bu açıklar, yetkisiz kullanıcıların rahatlıkla web sitesine ait içeriği değiştirmesine, veri tabanında tutulan tüm kayıtlara erişim sağlamasına veya sunucu üzerinde istedikleri komutları çalıştırmasına izin verecek niteliktedir. Bu açıklardan başarı ile faydalanan bir saldırgan veri tabanının bulunduğu ağa erişim sağlayabilir. Elde edilen test sonuçları internet üzerinden bu açıklar sayesinde yerel ağa erişimin mümkün olduğunu göstermiştir. Yine web sunucuları üzerindeki yapılandırmada hatalar bulunması, detaylı hata mesajları vasıtası ile uygulama kaynak kodları gibi önemli bilgilerin elde edilmesine izin vermiştir.

Güncel olmayan işletim sistemleri sunucuların sağlıklı çalışmasını tehdit eden unsurlardan bir tanesidir. Sunucunun tamamen başkasının eline geçmesine kadar giden bu açıklıklar zamanında önlenmediği taktirde büyük sorunlara yol açmaktadır.

1.5. GENEL TEST METODOLOJİSİ

Günümüz bilgi güvenliğinde iki tür yaklaşım vardır. Bunlardan kabul göreni proaktif yaklaşımdır. Sızma testleri (pentest) ve zayıflık tarama (vulnerability assessment) konusu proaktif güvenliğin en önemli bileşenlerinden biridir.

Sızma testleri ve zayıflık tarama birbirine benzeyen fakat farklı kavramlardır. Zayıflık tarama hedef sistemdeki güvenlik açıklıklarının çeşitli yazılımlar kullanarak bulunması ve raporlanması işlemidir. Sızma testi çalışmalarında amaç sadece güvenlik açıklıklarını belirlemek değil, bu açıklıklar kullanılarak hedef sistemler üzerinde gerçekleştirilebilecek ek işlemlerin (sisteme sızma, veritabanı bilgilerine erişme) belirlenmesidir.

Zayıflık tarama daha çok otomatize araçlar kullanılarak gerçekleştirilir ve kısa sürer. Sızma testi çalışmaları zayıflık tarama adımını da kapsayan ileri seviye tecrübe gerektiren bir süreçtir ve zayıflık tarama çalışmalarına göre çok daha uzun sürer.

1.6. RİSK DERECELENDİRME

Sızma testi çalışmalarında bulunan açıklar 5 risk seviyesinde değerlendirilmişlerdir. Bu değerlendirmede, PCI-DSS güvenlik tarama prosedürleri dokümanında[4] kullanılan beş seviye risk değerleri kullanılmıştır.

Aşağıdaki tablo **Tablo** kullanılan seviyelendirmeyi açıklamaktadır.

Risk	Seviyesi	Risk Puanı	Detay Açıklama
	**ACİL**	5	Acil öneme sahip açıklıklar, niteliksiz saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Depolanmış XSS, SQL enjeksiyonu ve RFI/LFI, ayrıca müşteri bilgisi ifşasına yol açabilecek açıklık vektörleri bu kategoriye girerler.
	**KRİTİK**	4	Kritik öneme sahip açıklıklar, nitelikli saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Ayrıca yansıtılan ve DOM tabanlı XSS açıklık vektörleri bu kategoriye girer.
	**YÜKSEK**	3	Yüksek öneme sahip açıklıklar, uzaktan gerçekleştirilen ve kısıtlı hak yükseltilmesi (mesela, yönetici hakları olmayan bir işletim sistemi kullanıcısı veya e-posta sahteciliği) veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan ataklara sebep olan açıklıkları içermektedir.
	**ORTA**	2	Orta öneme sahip açıklıklar, yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan ataklara sebep olan açıklıkları içermektedir.
	**DÜŞÜK**	1	Düşük öneme sahip açıklıklar ise etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin (best practices) izlenmemesinden kaynaklanan eksikliklerdir.

Tablo 1- Raporda kullanılan risk seviyelendirmesi

[4] https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf

1.7. GENEL BULGULAR

1.7.1. SQL Injection Güvenlik Açıklıkları

SQL Injection web uygulamasında kullanılan parametrelere, kendi sorgulamalarımızı ekleyerek arka plandaki veri tabanına erişmemize ve SQL sorgulamaları yapmamıza olanak tanıyan açıktır. Genellikle web uygulaması üzerindeki formlar veya URL içindeki parametreler kullanılarak bu açıktan yararlanılır. Eğer web uygulamasının herhangi bir veri tabanı ile bağlantısı var ve uygulama üzerinde gerekli önlemler alınmamış ise bu tip saldırılar yapmak mümkün olabilir. Bu tip saldırılar neticesinde sistem üzerinde tam yetki sahibi olmak, yerel ağdaki sistemlere sızmak veya veri tabanı üzerinde tutulan kayıtlara erişmek ve değiştirmek mümkün olabilir.

1.7.2. Güncel Olmayan Sunucular

Sunucular, hizmetlerin sunulduğu genel platformlar olarak çeşitli işletim sistemleri koşturmaktadır. İşletim sistemleri, çıkan yama programlar ile zaman zaman güncellenmektedir. Güncelleştirmeler takip edilmediği taktirde telafi edilemeyen sorunlara yol açmaktadır.

1.7.3. Cross Site Scripting (XSS)

Dinamik olarak oluşturulan web sayfalarında, kullanıcı tarafından sağlanan bilgiler uygulama tarafından düzgün bir şekilde işlenemediği veya kontrol edilemediği durumlarda, yetkisiz kişileri istedikleri script kodlarının görüntülenecek sayfada çalışmasını sağlayabilirler. Söz konusu problem Cross Site Scripting (XSS) olarak adlandırılmaktadır. Bu tip saldırıların hedefi direkt olarak sunucuya bağlanan kullanıcılardır. Uygulamalardaki XSS açıklıkları kullanılarak, bağlanan kullanıcıların session id, cookie gibi bilgileri çalınmaya çalışır.

1.8. TAVSİYE ÖZETİ

Sızma testi neticesinde özellikle sql injection ve güncel olmayan sunucular tespit edilmiştir.

Yazılım geliştirme sürecini müteakip, yazılımı devreye almadan önce yapılacak kod analizlerinin sql injection açıklıklarını önleme de büyük fayda sağlamaktadır. Yazılımı geliştiren personele güvenli kod geliştirme eğitimlerinin temin edilmesi bu sürecin daha sağlıklı yürütülmesine ciddi derece de katkı sağlamaktadır.

Güncel olmayan işletim sistemleri her zaman sorun olmuştur. Güncelleştirme uyarıları halka açık olarak yayınlandığı için art niyetli kişiler tarafından da kolaylıkla takip edilip zafiyetler kullanılabilmektedir. Güncelleştirmelerin takip edilmesini sağlayan bir politika ve prosedür kurulması ile bu konudan kaynaklanan risklerin asgari seviyeye indirgendiği görülmektedir.

2. TEKNİK BİLGİLER

2.1. GİRİŞ

Güvenlik taramaları internet üzerinden erişilebilir sunucular için kurumdan en az bilgi temin edilerek gerçekleştirilmiş olup, sıradan bir kullanıcının ne gibi aktiviteler gerçekleştirebileceğini göstermektedir. Intranet üzerinden gerçekleştirilen sızma testlerinde kurum tarafından temin edilen çeşitli seviyelerde yetkilendirilmiş kullanıcı hakları kullanılmıştır. Testler sırasında çeşitli ticari tarama ürünleri, herkes tarafından temin edilebilecek açık kaynak kodlu programlar ve uzmanlarımız tarafından geliştirilmiş yardımcı program ve araçlar kullanılmıştır. Bu araçların listesi "Kullanılan Araçlar" bölümünde yer almaktadır.

2.2. BİLGİ TOPLAMA

2.2.1. Domain Sorgusu ve Whois Sorgusu

Bu aşamada domain sorgusu, dns sunucudan alan transferi ve whois veritabanı taramaları gerçekleştirildi.

2.2.2. Web Sitesi Analizi

Kurumun hangi dış bağlantıları ve etki alanlarının kullandığını belirlemek amacı ile kurumun web siteleri genel olarak incelendi. Daha sonra yapılacak detaylı incelemelere temel teşkil edecek bilgiler toplandı.

2.2.3. Arama Motorları

Arama motorları kullanılarak kurum ve kurum personeli hakkında araştırmalar yapıldı. Bu araştırmalar neticesinde kritik personelin üye olduğu gruplar sosyal paylaşım siteleri tespit edilerek kurum hakkında bilgi edinme çalışılması yapıldı. Bu çalışma kapsamında kurum hakkında yapılmış haberler de incelenerek faydalı olabilecekler ayıklandı.

2.2.4. Ağ Haritasının Çıkarılması

Bilgi toplamanın en önemli kısmı elde edilen bilgilerin birleştirilmesidir. Bu aşamada elde edilen bilgiler birleştirilerek kuruma ait güvenlik duvarı, uygulama sunucusu, veritabanı yönetimi sunucusu, aktif ağ cihazları gibi cihazların ip adresleri ve birbirleri ile olan bağlantıları tespit edildi.

2.2.5. Sosyal Mühendislik Çalışması

Kurumlara yapılan saldırıların en zayıf halkası genelde kullanıcılar olabilmektedir. Kurumda bilgi alınabilecek her türlü personel ile iletişme geçilerek (sahte e-postalar, telefon görüşmeleri veya benzer vasıtalar ile) temasa geçilerek bilgi edinim çalışması gerçekleştirildi.

2.2.6. Tahmin Çalışması

Kurumun faaliyet alanı, yapısı ve sistemleri temel alınarak, kurumda olabilecek servis ve uygulamaların bir listesi testte kullanılmak amacı ile oluşturuldu.

2.3. AÇIKLIK ANALİZİ

Bu kısımda açıklık analizi yapılan açıklıklar risk seviyesine göre sıralanır.

AÇIKLIK 1

Risk Seviyesi	Acil/Kritik/Yüksek/Orta/Düşük
Erişim Ortamı	İnternet/Intranet
Kullanıcı Profili	Internet Kullanıcısı/Intranet Kullanıcısı/Sistem Kullanıcısı/Diğer
Kullanılan Araçlar	Sqlmap
Zafiyet Türü	Web Uygulaması Açıklıkları/Hizmetler/Windows Açıklıkları
Zafiyet Adı	SQL Injection/OpenSSH Rastgele Komut İşletim Zafiyeti/Cross site scripting (XSS)
Etkilenen Sistemler ve portlar	212.125.85.100 - 5521
Tanım	Bazı uygulama yazılımlarında sql injection açıklıklarının olduğu tespit edilmiştir.
Çözüm önerileri	Kod geliştirme esnasında sql injection neden olabilecek hususlara dikkat edilmelidir. Uygulama kodlarına müdahale edilemeyen uygulamalar için uygulama katmanı güvenlik duvarı (web application firewall) kullanılmalıdır.
Referanslar ve İyi Uygulama Örnekleri	https://www.owasp.org/index.php/SQL_Injection

NOT: Tanım kısmında açıklık/zafiyet ile ilgili elde edilen ekran görüntüleri paylaşılabilir.

AÇIKLIK 2

Risk Seviyesi	Acil/Kritik/Yüksek/Orta/Düşük
Erişim Ortamı	İnternet/Intranet
Kullanıcı Profili	Internet Kullanıcısı/Intranet Kullanıcısı/Sistem Kullanıcısı/Diğer
Kullanılan Araçlar	Nessus
Zafiyet Türü	Web Uygulaması Açıklıkları/Hizmetler/Windows Açıklıkları
Zafiyet Adı	SQL Injection/OpenSSH Rastgele Komut İşletim Zafiyeti/Cross site scripting (XSS)
Etkilenen Sistemler ve portlar	172.16.32.25 - 5522
Tanım	Bazı Windows sistemlerinin güncel olmadığı belirlenmiştir.
Çözüm önerileri	Tüm sistemler için gerekli güncellemelerin yapılmış olduğundan emin olunmalı, güncelleştirmelerin düzenli olarak yapılması için gerekli düzenlemeler yapılmalıdır.
Referanslar ve İyi Uygulama Örnekleri	http://windowsupdate.microsoft.com http://www.microsoft.com/technet/security/default.mspx

NOT: Açıklıkların analizinde aşağıdaki çizelge de yer alan değerler kullanılabilir.

Risk Seviyesi	Erişim Ortamı	Kullanıcı Profili	Zafiyet Türü	Zafiyet Adı
Acil	İnternet	Internet Kullanıcısı	Web Uygulamaları	SQL Injection
Kritik	Intranet	Intranet Kullanıcısı	Windows Açıklıkları	OpenSSH Rasgele Komut İşletim Zaafiyeti
Yüksek	Kablosuz Ağ	Sistem Kullanıcısı	Linux Açıklıkları	Cross site scripting (XSS)
Orta	Mobil Ağ	Sistem Yöneticisi	Ağ Yapılandırmaları	Mantıksal Açıklık
Düşük	Diğer……	Diğer……	Diğer……	Girdi Doğrulama Zafiyeti
				Kimlik Doğrulama Zafiyeti
				Oturum Yönetimi Zafiyeti
				Yetkilendirme Zafiyeti
				AJAX Zafiyeti
				Diğer……

2.4. KULLANMA/AÇIKLIK ONAYI

AÇIKLIK 1

8 Ocak 2013 tarihli İdare yazısı ile açıklıktan nasıl faydalanılabileceğinin açıklanması amaçlı testin ilerletilmesi talep edilmiştir.

Risk Seviyesi	Acil/Kritik/Yüksek/Orta/Düşük
Erişim Ortamı	İnternet/Intranet
Kullanıcı Profili	Internet Kullanıcısı/Intranet Kullanıcısı/Sistem Kullanıcısı/Diğer
Kullanılan Araçlar	Sqlmap
Zafiyet Türü	Web Uygulaması Açıklıkları/Hizmetler/Windows Açıklıkları
Zafiyet Adı	SQL Injection/OpenSSH Rastgele Komut İşletim Zafiyeti/Cross site scripting (XSS)
Etkilenen Sistemler ve portlar	212.125.85.100 – 5521
Tanım	Bazı uygulama yazılımlarında sql injection açıklıklarının olduğu tespit edilmiştir.
Çözüm önerileri	Kod geliştirme esnasında sql injection neden olabilecek hususlara dikkat edilmelidir. Uygulama kodlarına müdahale edilemeyen uygulamalar için uygulama katmanı güvenlik duvarı (web application firewall) kullanılmalıdır.
Referanslar ve İyi Uygulama Örnekleri	https://www.owasp.org/index.php/SQL_Injection

2.5. KULLANMA SONRASI ETKİ

AÇIKLIK 1

Açıklık üzerinde yapılan testler ilerletilerek aşağıdaki personel bilgileri ve intranet uygulama kullanıcı adı ve parolaları elde edilmiştir. Ayrıca, web sunucusunun bu veri tabanını kullandığı tespit edildiğinden gerekli değişiklikler yapılarak web sayfası üzerinde görülmesi sağlanmıştır.

S. No	Adı Soyadı	Görevi	Kullanıcı Adı	Parola
1	*Yüksel UÇAR*	*Sağlık Mem.*	****	****
2	*Handan GÖKDEMİR*	*Tıbbi Teknolog*	****	****
3	*Cevahir KESEN ÜLKÜ*	*Ebe*	****	****
4	*Züleyha KAPLAN*	*Diyetisyen*	****	****

2.6. DENIAL of SERVICE (DoS) SALDIRILARI

DoS/DDoS testleri sırasında kurumun iş akışını aksatmamak amacıyla Kurum personeli ile koordineli bir çalışma yürütülmüştür. Bu çalışma kapsamında testler hafta sonu saat 02:00-04:00 arasında gerçekleştirilmiştir.

DoS/DDoS saldırıları yapılan sunucular aşağıda listelenmiştir.

Sunucu Adı	IP Adresi	DNS Adı	Açıklama
MAIL	212.125.85.6	mail.abc.gov.tr	E-posta sunucusu
WEB	212.125.85.100	www.abc.gov.tr	Web Sunucusu
DNS	212.125.85.150	dns.abc.gov.tr	DNS Sunucusu

Günümüz dünyasında şirketlerin internete olan bağlantıları hayati önem kazanmış durumdadır. Internet bağlantısının önem kazanmasıyla paralel olarak Internet dünyasının en eski ve etkili saldırı yöntemlerinden biri olan DoS saldırıları da tehdit sınıflandırmasında en üst sıralara yükselmiştir. DoS/DDoS saldırılarının birçok çeşidi bulunmaktadır. ABC Kurumu tarafından aşağıdaki saldırı çeşitlerinin yapılması istemiştir.

ABC Kurumu tarafından talep edilen DoS/DDoS saldırı çeşitleri:

- Syn flood ddos saldırıları
- ACK flood ddos saldırıları
- FIN flood ddos saldırıları
- TCP flood ddos saldırıları
- ICMP flood ddos saldırıları
- HTTP GET flood
- HTTP Post Flood
- UDP Flood
- DNS flood
- Fragmentatin flood

Bu testler neticesinde kurumun aşağıdaki DoS/DDoS çeşitlerine karşı herhangi bir korumasının olmadığı tespit edilmiştir:

- HTTP GET flood
- HTTP Post Flood
- UDP Flood
- DNS flood
- Fragmentatin flood

2.7. KULLANILAN ARAÇLAR

Raporda detayları sunulan sunuculara doğru gerçekleştirilen testlerde aşağıdaki listelenen ticari ve açık kaynak kodlu araçlar kullanılmıştır.

2.7.1. Ağ Tarayıcıları

Nessus – Açık kaynak kodlu zafiyet tarayıcısıdır. *http://www.nessus.org/*

Nmap – Nmap ("Network Mapper") network haritasının çıkartılmasında ve güvenlik denetiminde kullanılan açık kaynak kodlu bir araçtır. *www.insecure.org/nmap/*

2.7.2. Uygulamaya Yönelik Araçlar

AppTool - Uygulama düzeyindeki güvenlik açıklarının çıkartılmasında ve çözüm önerilerinin sunulmasında kullanılan lisanslı bir araçtır.

http://www.appsecurity.com/software/products/tr/tr/apptool-source/

2.7.3. Diğer Araçlar

Nemesis – Paket üreticisi bir program.

Ripe.net – Kamuya açık web sitesi.

EK-2

SIZMA TESTİ KAPSAM BELİRLEME FORMU ÖRNEĞİ

Bu form gerçekleştirilecek olan güvenlik testlerinin kapsamını belirlenmesi için hazırlanmıştır. Lütfen mümkün olduğu kadar detaylı şekilde doldurunuz. Lütfen gerekli yerleri **(x)** şeklinde işaretleyiniz.

Test yapılmasını istediğiniz sistemler arasında kuruluş dışında barındırılan sistemler var ise bu durum testi yapan firmaya bildirilmelidir.

Testin gerçekleştirileceği

Tarih aralığı : ...../...../..... - ...../...../.....

IP aralığı: ..... - .....

Talep Edilen Test Türü			
( ) Beyaz Kutu Testi ( ) Siyah Kutu Testi ( ) Gri Kutu Testi Gri Kutu Testi ..... saatleri arasında yapılmalıdır. Siyah Kutu Testi ..... saatleri arasında yapılmalıdır. Beyaz Kutu Testi ..... saatleri arasında yapılmalıdır.			
Talep Edilen Hizmetler			
( ) Internet Üzerinden Güvenlik Denetim Hizmeti ( ) Web Uygulamalarına Yönelik Güvenlik Denetim Hizmeti ( ) Yerel Ağ İçinden Güvenlik Denetim Hizmeti ( ) Diğer.....			
Internet Üzerinden Ağ Cihazları ve Sunucu Güvenlik Denetim Hizmeti			
Test Edilecek IP'ler ve Açıklama		"1.1.1.1 (DNS)" gibi	
Firmaya Ait Test Edilecek Alan Adı			
Internet Üzerinden Test Edilecek Toplam Aktif Sunucu Sayısı			
Web Uygulamalarına Yönelik Güvenlik Denetim Hizmeti			
Test Edilecek Web Uygulama ve Sunucu Sayısı			
Test Edilecek Web Uygulamalarına Ait	Uygulama URL'i	Teknoloji	Test Hesabı Verilecek

URL'ler		(.NET,PHP,JAVA)	mi?*
Yerel Ağ İçinden Gerçekleştirilecek Güvenlik Denetim Hizmeti Bilgileri			
Yerel Ağ İçinden Gerçekleştirilecek Güvenlik Denetim Hizmeti Bilgileri	Web Sunucu:	DNS Sunucu:	Firewall/VPN:
	Mail Sunucu:	SFTP Sunucu:	Veri Tabanı:
	Diğer:	Diğer:	Diğer:
Test Edilecek İstemci Sayıları ve Türü			
Test Edilecek IP'ler ve Açıklama		"1.1.1.1 (DNS)" gibi	
Çalışmanın Gerçekleştirileceği Lokasyon			
Wireless Ağlara Sızma Testleri			
Test Edilecek Cihaz Sayısı			
Kimlik Doğrulama Yöntemleri			
İstenilen Testler		( ) WiFi Ağını İçeriden ve Dışarıdan Dinleme Testleri	
		( ) WiFi Hotspot Testleri	
		( ) Erişim Sağlanması Durumunda Diğer Sistemlere Erişim Testleri	
		( ) Şifreleme Türünün Tespit Ve Kırılma Testleri	
Acil Durum Kotarma İletişim Bilgileri			
Firma		**Müşteri Kuruluş**	

İdari		**İdari**	
Teknik		**Teknik**	

EK-3

SIZMA TESTİ ÖNCESİ

MÜŞTERİ FERAGATNAMESİ ÖRNEĞİ

Test Tarihleri: <gg.aa.yy> - <gg.aa.yy>

İşbu Sızma Testi Öncesi Müşteri Feragatnamesi ("Feragatname") <gg.aa.yy> tarihinde, <adres> adresinde mukim <müşteri tam adı> ("Müşteri") ile <adres> adresinde mukim yüklenici <firma> ("Firma") arasında imzalanmış olan hizmet alımına ilişkin sözleşmeye ek olmak üzere düzenlenerek taraflarca imzalanmıştır.

Müşteri işbu Feragatname ile firma tarafından Müşteri'ye verilecek saldırı simülasyonu hizmetleri ("Hizmet") kapsamında işbu Feragatname'yi imzalamayı kabul, beyan ve taahhüt eder. Saldırı simülasyonu kötü amaçlı bir saldırganın Müşteri sistemlerine verebileceği zararı Müşterinin görebilmesi ve gerekli tedbirleri alabilmesi için yapılan simülasyonudur.

1. Firma tarafından Müşteri'ye verilecek Hizmet'in ön hazırlıkları sırasında, saldırı simülasyonları öncesi ve saldırı simülasyonları sırasında eğer varsa tüzel ve/veya gerçek üçüncü kişileri, haberdar etmek, gerekiyorsa onlardan yazılı ve/veya sözlü olarak gerekli her türlü izni almak ve simülasyonlar sırasında gözlemlerini yaptırtmaktan Müşteri sorumludur. Bilgi verilmemiş, izin alınmamış veya gözlem yaptırılmamış tüzel ve/veya gerçek üçüncü kişilerle çıkacak anlaşmazlıklardan, bu üçüncü kişilerin taleplerinden ve bu sebeple doğabilecek doğrudan ve/veya dolaylı zararlardan dolayı firmanın sorumlu olmadığını Müşteri kabul eder. Müşteri firmayı bu anlaşmazlıklardan, taleplerden ve zararlardan ari tutacaktır.
2. Firmanın ağır kusuru ile sebep olduğu haller hariç olmak üzere, saldırı simülasyonları sırasında Müşteri'nin DoS, DDoS veya test sistemlerinin zarar görmesi ve bunun hizmet kesintisine sebep olması halinde firmanın sorumlu olmayacağını Müşteri kabul eder.
3. Saldırı simülasyonları sırasında oluşabilecek, hizmet kesintisi, sistem yüklenmeleri gibi durumlardan firmanın kesinlikle sorumlu olmayacağını Müşteri kabul eder.
4. İşbu Feragatname, Müşteri'nin yetkili kişileri tarafından imza edilmekle geçerli ve bağlayıcıdır.

İşbu Feragatname iki nüsha olarak <gg.aa.yy> tarihinde imzalanmış olup, 01.09.2013 <gg.aa.yy> tarihi itibarıyla geçerli ve bağlayıcı olmak üzere yürürlüğe girmiştir.

Firma Müşteri Kuruluş

9. Kaynakça

[1] TS ISO/IEC 27001:2005, Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler

[2] TS EN ISO/IEC 17025, Deney ve kalibrasyon laboratuvarlarının yeterliliği için genel şartlar

[3] Burlu, K. (2010). Bilişimin Karanlık Yüzü

[4] SAĞIROĞLU, Ş., VURAL, Y., Kurumsal Bilgi Güvenliğinde Güvenlik Testi ve Öneriler, Gazi Üniv. Müh. Mim. Fak. Der., Cilt 26, No 1, 89-103, 2011

[5] www.owasp.org