

**SIZMA TESTİ  
KAPSAM FORMU**

**MERKEZ OFİS**

**İçerenköy mah. Ali Nihat Tarlan Cad. Ertaç Sok. Ardil İş Merkezi No:4 Kat:6 Ataşehir/İstanbul - Türkiye**

**(+90) 216 740 00 20**

[**pentest@tetrabilisim.com.tr**](mailto:pentest@tetrabilisim.com.tr)

İçindekiler

[Penetrasyon Testi Bilgi Formu 3](#_Toc137810632)

[Internet (Dış Ağ) Sızma Testi 4](#_Toc137810633)

[Intranet (Yerel Ağ) ve Veri Tabanı Sızma Testi 5](#_Toc137810634)

[Kablosuz Ağ Güvenlik Testi 5](#_Toc137810635)

[Web Uygulama Güvenlik Testi 6](#_Toc137810636)

[EKS/SCADA (Endüstriyel Kontrol Sistemleri) Güvenlik Testleri 7](#_Toc137810637)

[Sosyal Mühendislik ve Son Kullanıcı Farkındalık Testi 7](#_Toc137810638)

[Servis Dışı Bırakma (DOS/DDOS) Testi 8](#_Toc137810639)

[Mobil Uygulama Güvenlik Testi 8](#_Toc137810640)

[Kaynak Kod Analizi 9](#_Toc137810641)

[Test Süreci 9](#_Toc137810642)

[Testler Sırasında Uygulanacak Metodoloji 10](#_Toc137810643)

[Bilgi Toplama Aşaması 10](#_Toc137810644)

[Ağ Topolojisi Çıkarma Aşaması 11](#_Toc137810645)

[Enumerating Aşaması 11](#_Toc137810646)

[Zafiyet Tarama Aşaması 11](#_Toc137810647)

[Hak Elde Etme Aşaması 12](#_Toc137810648)

[Hak Yükseltme Aşaması 12](#_Toc137810649)

[Başka Sistemlere Sızma Aşaması 12](#_Toc137810650)

[Sistemde Kalıcı Olma Aşaması 12](#_Toc137810651)

[Temizlik Aşaması 12](#_Toc137810652)

[Web Uygulama Güvenlik Testleri 13](#_Toc137810653)

[İstemci Tarafı Sızma Testleri 14](#_Toc137810654)

[Servis Dışı Bırakma Testleri 14](#_Toc137810655)

[Veritabanı Zafiyet Testleri 14](#_Toc137810656)

[Kablosuz Ağ Sızma Testleri 15](#_Toc137810657)

[EKS/SCADA (Endüstriyel Kontrol Sistemleri) Güvenlik Testleri 15](#_Toc137810658)

[Raporlama 16](#_Toc137810659)

[Sunum 16](#_Toc137810660)

# Penetrasyon Testi Bilgi Formu

Penetrasyon (Sızma) testi, zafiyet analizinden farklı olarak belirli bir metodoloji dahilinde planlı ve aşamalı olarak gerçekleştirilmektedir. Sahip olunan bilişim sistemlerine ait her türlü zafiyetin dış kaynaklı bir kurum ve/veya bir şirket tarafından teste tabi tutulması, kontrol edilmesi ve raporlanması proaktif güvenliğin ilk adımlarındandır.

Yapılan güvenlik testlerinin temel amacı şirketlerin farkında olmadıkları güvenlik açığına farklı bir bakış ile yaklaşarak ve koordineli çalışarak hedef sistemler üzerinde hizmet kesintisi yaratmaksızın bu zafiyetleri ifşa etmektir, yapılan çalışmanın sonucunda belirlenen bilişim sistemlerindeki mantık hataları ve zafiyetleri tespit edilerek, söz konusu güvenlik açıklıklarının kötü niyetli kişiler tarafından istismar edilmesini önlemek ve sistemleri daha güvenli hale getirmek maksadıyla gerçekleştirilmektir.

TETRA BİLİŞİM tarafından Kurum / Firmanıza yapılacak olan Penetrasyon (Sızma) testleri için aşağıdaki bilgilerin tamamlanmasını tarafınızdan talep ederiz.

Lütfen gerçekleştirilmesini talep ettiğiniz hizmet türü için kutucuklar içerisine «X» yazınız.

|  |  |
| --- | --- |
| **Test Talep Bilgileri** | |
| Kurum / Firma Ünvanı |  |
| İlgili Kişi |  |
| İlgili Kişi Ünvanı |  |
| İletişim Bilgileri |  |

|  |  |
| --- | --- |
| **Test Ekibi** | |
| Kurum / Firma Ünvanı | TETRA SİBER GÜVENLİK |
| İlgili Kişi |  |
| İlgili Kişi Ünvanı |  |
| İletişim Bilgileri |  |

Penetrasyon testlerinde amaç sadece güvenlik açıklıklarını belirlemek değil, bu açıklıklar kullanılarak hedef sistemler üzerinde gerçekleştirilebilecek ek işlemlerin belirlenmesidir.

White Box, Gray Box, Black Box olmak üzere genel kabul görmüş üç çeşit sızma testi vardır.

|  |  |
| --- | --- |
| **Test Türleri** | |
| White Box (Beyaz Kutu) Testleri | Güvenlik testi ekibi, sistemin kendisi ve arka planda çalışan ilave teknolojiler hakkında tam bilgi sahibidir. Black Box tekniğine göre kurum ve firmaya daha büyük fayda sağlar. Hata ve zafiyetleri bulmak kolaylaşacağından bunlara tedbir alınma süresi de azalacaktır. Sistemin zarar görme riski çok azdır. |
| Gray Box (Gri Kutu) Testleri | Güvenlik testi ekibi, bu yaklaşımda, sistem ile ilgili bilgileri kısmen bilgi sahibidir. Örneğin; IP adres listesi, sunucu sistem ile ilgili versiyon bilgisi vb. Bilgiler güvenlik testi yapacak ekibe önceden sağlanır. Black Box yaklaşımına göre daha kısa zaman alır. Kontrolü ve testi istenen IP adresleri belli olduğundan sistemin, istem dışı zarar görme ihtimali de azalmış olur. |
| Black Box (Siyah Kutu) Testleri | Güvenlik testi ekibi, bu yaklaşımda, başlangıçta güvenlik testi yapılacak sistemle ilgili bir bilgi yoktur. Tamamen bilinmeyen bir sistem ile ilgili bilgi toplanacak ve testler yapılacaktır. Bu yöntemde test ekibinin sistem ile ilgili bilgi düzeyi hiç olmadığından, yanlışlıkla sisteme zarar verme ihtimalleri de yüksektir. Bilgi toplama safhası oldukça zaman alır. Süre bakımından en uzun süren yaklaşım tarzıdır. |

|  |
| --- |
| **Talep Edilen Hizmetler** |
| Internet (Dış Ağ) Sızma Testi  Intranet (Yerel Ağ) ve Veri Tabanı Sızma Testi  Kablosuz (Wireless) Ağ Zafiyet Testi  Web Uygulama Güvenlik Testi  Sosyal Mühendislik ve Son Kullanıcı Farkındalık Testi  Servis Dışı Bırakma (DOS/DDOS) Testi  Mobil Uygulama Güvenlik Testi  EKS/SCADA (Endüstriyel Kontrol Sistemleri) Güvenlik Testleri  Kaynak Kod Analizi |

## Internet (Dış Ağ) Sızma Testi

Dış test olarak adlandırılan bu test hedef networke internet üzerinden gelebilecek olan saldırıların gerçek zamanlı simülasyonudur. Erişim profili internet olduğundan kötü niyetli kişilerin gerçekleştirdiği saldırıların en yaygın olduğu alandır, çalışmalar süresince siber saldırgan gözüyle sistemler tüm detaylarıyla incelenerek yetkili onayı dahilinde çıkan açıklıklar istismar edilerek sızma denemeleri gerçekleştirilir, verebileceği zararlar tespit edilerek raporlanır.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Internet (Dış Ağ) Sızma Testi** | | | | |
| Test Edilecek IP/SUBNET Bilgileri |  | | | |
| Test Edilecek Domain (Alan Adı) Bilgisi  [Sub Domain (Alt Alan Adı) ile birlikte] |  | | | |
| DMZ Alanında Bulunan Sunucu Sayısı |  | | | |
| Test Edilecek Sunucu Bilgileri | Web Sunucu: | DNS Sunucu: | | Firewall/VPN: |
| Mail Sunucu: | FTP Sunucu: | | Diğer: |
| Mail Sunucusu Lokasyon |  | |  | |
| Web Sunucusu Lokasyon |  | |  | |

## Intranet (Yerel Ağ) ve Veri Tabanı Sızma Testi

İç test olarak da bilinen bu test, hedef networke içeriden gelebilecek olan saldırıların gerçek zamanlı simülasyonudur. Şirket çalışanlarının ve/veya ağa dahil olan bir saldırganın vereceği zararlar çalışmalar süresince siber saldırgan gözüyle hedef sistemler tüm detaylarıyla incelenerek yetkili onayı dahilinde çıkan açıklıklar istismar edilir ve sızma denemeleri gerçekleştirilir, verebileceği zararlar tespit edilerek raporlanır.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Intranet (Yerel Ağ) ve Veri Tabanı Sızma Testi** | | | | | | | |
| Test Edilecek Sunucu Bilgileri | Sunucu: | | DNS Sunucu: | | | Firewall/VPN: | |
| Mail Sunucu | | SFTP Sunucu: | | | Veri Tabanı: | |
| Domain Controller: | | Router/Switch: | | | Diğer: | |
| Veritabanı Sistemleri |  |  | |  | | |  |
| Test Edilecek Toplam Sunucu Sayısı  (Fiziksel + Sanal Sunucu) |  | | | | | | |
| (Kurumun burada verdiği bilgiler fiyat çalışması için önemlidir; istemci, sunucu, dmz, cihaz, vs..) | | | | | | | |
| Kablosuz Ağ Güvenliği |  | | | |  | | |
| Çalışma Lokasyon |  | | | |  | | |
| Lokasyon Adres – 1 |  | | | | | | |
| Lokasyon Adres – 2 |  | | | | | | |
| Lokasyon Adres – 3 |  | | | | | | |
| Lokasyon Adres – 4 |  | | | | | | |
| İşletim Sistemleri |  | | | | | | |
| İstemci Sayısı |  | | | | | | |
| Test Edilecek IP Aralıkları |  | | | | | | |
| DMZ IP Aralıkları |  | | | | | | |
| Toplam IP Alan Cihaz Sayısı |  | | | | | | |
| Diğer Bilgiler | Forma yazılamayan/yazılacak alan bulunamayan bilgiler bu alana yazılacaktır. | | | | | | |

## Kablosuz Ağ Güvenlik Testi

Kablosuz ağ güvenlik testi kablosuz ağların, erişim kontrollerinin, yapılandırmalarının ve kullanıcılarının davranışlarının değerlendirilmesi, parola kırma testleri, erişim sağlanan kablosuz ağlar üzerinden kurum ağına gerçekleştirilebilecek saldırıların test edilmesi, bulgu/çözüm önerilerinin raporlanması ve hizmet kapsamı dahilinde talep edildiğinde doğrulanması faaliyetlerini içeren güvenlik testlerinin gerçekleştirilmesidir.

|  |  |  |
| --- | --- | --- |
| **Kablosuz Ağ Güvenlik Testi** | | |
| Test Edilecek SSID Sayısı |  | |
| Test Yapılacak Lokasyon Sayısı |  | |
| Hotspot Testleri İsteniliyor mu? |  |  |

## Web Uygulama Güvenlik Testi

Web Uygulama Güvenlik Testi hedef web uygulamasına gelebilecek olan içeriden veya dışarıdan saldırıların gerçek zamanlı simülasyonudur. Çalışmalar süresince siber saldırgan gözüyle hedef web uygulama evrensel olarak kabul görmüş metodolojiler kullanılarak incelenir yetkili onayı dahilinde çıkan açıklıklar istismar edilerek sızma denemeleri gerçekleştirilir, verebileceği zararlar tespit edilerek raporlanır.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Web Uygulama Güvenlik Testi** | | | | | |
| Sunucu Sayısı |  | | | | |
| Web Uygulama Sayısı |  | | | | |
| Test Alan Adı |  | | | | |
| Sunucu Erişim Noktası ve Web Uygulamalarına Ait URL'ler | INTERNET (DIŞ AĞ): | | INTRANET (YEREL AĞ): | | |
| Test Edilecek Uygulama IP Adresleri |  | | | | |
| Teknoloji |  |  | | |  |
| Demo Hesap Sağlanacak mı? |  | | |  | |
| Kullanıcı Profil Sayısı |  | | | | |

## EKS/SCADA (Endüstriyel Kontrol Sistemleri) Güvenlik Testleri

Endüstriyel kontrol sistemlerinde sızma testi, sistemin güvenlik açıklarını belirlemek, zayıf noktaları tespit etmek ve istenmeyen erişim girişimlerini önlemek için yapılan bir test sürecidir. Bu testler, ağ bağlantılarını, güncelleme eksikliklerini, zayıf parola politikalarını ve diğer potansiyel güvenlik açıklarını değerlendirir. Ayrıca, yetkisiz erişim girişimlerini simüle ederek sistemin güvenlik düzeyini değerlendirir ve önlem alınması gereken alanları belirler.

|  |  |
| --- | --- |
| EKS/SCADA (Endüstriyel Kontrol Sistemleri) Güvenlik Denetim Hizmeti | |
| Demo Hesap Sağlanacak mı? |  |
| Üretimdeki sistemler üzerinde de test yapılması isteniyor mu? |  |
| EKS/SCADA Sistem Bilgileri (IP/Erişim Adres Bilgileri dahil) |  |
| Test kapsamında değerlendirilecek sunucu sayısı? |  |
| Test kapsamında değerlendirilecek uygulama sayısı? |  |
| EKS sisteminde kaç farklı tipte RTU kullanılmaktadır? | …..Farklı Tipte RTU kullanılmaktadır. |
| EKS sisteminde kaç farklı tipte PLC kullanılmaktadır? | …..Farklı Tipte PLC kullanılmaktadır. |
| EKS sisteminde kaç farklı tipte Röle kullanılmaktadır? | …..Farklı Tipte Röle kullanılmaktadır. |
| Demo Hesap Sağlanacak mı? |  |
| Test Edilecek Uygulama IP Adresleri |  |
| EKS sisteminde kablosuz ağ teknolojileri kullanılmakta mıdır? |  |

## Sosyal Mühendislik ve Son Kullanıcı Farkındalık Testi

Bu test "Güvenlik zincirindeki en zayıf halka’nın bulunması ve bu yol ile sistemlere sızıntı sağlanacak mı sorusunun cevabının bulunması amacıyla internet üzerinden belirlenen kullanıcı listesine senaryo dahilinde sahte bir e-mail gönderilerek mail içerisinde bulunan bağlantı yoluyla kullanıcıları sahte sayfaya yönlendirerek bilgiler girmesi istenmektedir.

|  |  |
| --- | --- |
| **Sosyal Mühendislik ve Son Kullanıcı Farkındalık Testi** | |
| E-posta Gönderilecek Kullanıcı Sayısı |  |
| Varsa, talep edilen senaryolar ve ilave bilgi |  |
| İstenen Sosyal Mühendislik Testi |  |

## Servis Dışı Bırakma (DOS/DDOS) Testi

Bu testte hedef sisteme yönelik dışardan gelebilecek olan servis dışı bırakma saldırıları belirli bir süre dahilinde en yaygın kullanılan atak yöntemleri ile test edilir.

|  |  |
| --- | --- |
| **Servis Engelleme (DOS/DDOS) Testi** | |
| IP Sayısı |  |
| Sunucu Sayısı |  |
| Bant Genişliği | MBit |
| DDoS Koruması var mı? |  |

## Mobil Uygulama Güvenlik Testi

Mobil Uygulama Güvenlik Testi hedef mobil uygulamasına gelebilecek olan saldırıları simüle eder. Bu test hackerların yaptığı gerçek saldırıları göz önünde bulundurarak, verecebilecekleri zararları tespit ederek raporlar.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mobil Uygulama Güvenlik Testi** | | | | |
| Mobil Uygulama Sayısı |  | | | |
| Platform |  |  | |  |
| Demo Hesap Sağlanacak mı? |  | |  | |
| Erişim adresi (App Store, Google Play Store, vb.) |  | |  | |
| Uygulama Ekran Sayısı |  | | | |
| Kullanıcı Profil Sayısı |  | | | |

## Kaynak Kod Analizi

|  |  |  |
| --- | --- | --- |
| **Kaynak Kod Analizi** | | |
| Test edilecek uygulama sayısı |  | |
| Dinamik Kod Analizi isteniyor mu? |  |  |
| Uygulamanın geliştirildiği yazılım dili |  |  |
| Teknoloji |  | |
| Uygulama toplam kod satır sayısı |  | |
| Sayfa sayısı |  | |

# Test Süreci

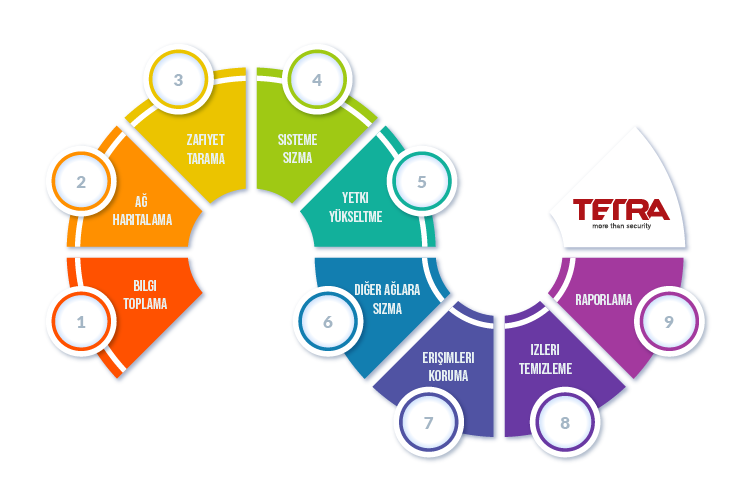
|  |  |
| --- | --- |
| **ACİL DURUM KOTARMA** | |
| Acil durum kotarma safhasında iletişime geçilecek kurum yetkili personel bilgileri. | |
| Ad, Soyad | Telefon Numarası |
|  |  |

|  |  |
| --- | --- |
| **DOĞRULAMA TESTİ İSTENİYOR MU?** | |
| **Doğrulama Testi**: Zafiyetler kurum tarafından kapatıldıktan sonra tespit edilen bulguların kontrol edilmesidir. | |
| Evet : | Hayır : |

## Testler Sırasında Uygulanacak Metodoloji

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

Gerçekleştirilecek sızma testine ilişkin detaylar aşağıda yer almaktadır.



## Bilgi Toplama Aşaması

Bilgi toplama kapsamlı bir güvenlik değerlendirmesi yapabilmek için hedef hakkında olası tüm bilgileri toplamak için kullanılan evredir. İnternet üzerinden teknik (whois/dns sorguları) ve teknik olmayan (arama motorları, haber grupları, e-posta listeleri sosyal ağlar vb.) yöntemler kullanılarak, hedef şirket veya sistem hakkında bilgi sağlanabilir. Bu safhanın amacı mümkün olan her saldırı yolunu keşfederek hedef ve uygulamalarının kapsamlı bir görünümünü elde etmektir. Bu sayede hedef üzerinde bilgi güvenliğiyle ilgili her vektörün test edilebilmesine olanak sağlanır. Bu adım metodolojinin genellikle göz ardı edilen ilk ve en önemli adımlarından biridir. Diğer tüm aşamalarda olabildiğince kapsamlı ilerlenmesini sağlar.

## Ağ Topolojisi Çıkarma Aşaması

Birinci bölümün ardından hedefle ilgili tüm olası bilgiler edinildiğinde, hedef network ve kaynaklarını analiz etmek için daha teknik bir yaklaşım uygulanır. Network haritalama aktif bir bilgi toplama aşamasıdır. Bu evrede amaç; hedef sistemin muhtemel bir network topolojisinin üretmek ve network yapısının detaylandırılmasıdır. Bu aşamada; hedef sistem üzerinde port ve servis taraması, açık sistemlerin belirlenmesi, açık sistemler üzerindeki açık portların ve servislerin belirlenmesi, sistemler üzerinde hangi işletim sistemlerinin ve servislerin çalıştığının belirlenmesi, işletim sistemlerine, servislere ve uygulamalara ait versiyon bilgilerinin tespiti, sistemlerde kullanılan donanım/yazılımların ve versiyonlarının tespit edilmesi, Router, Firewall, IPS gibi ağ cihazlarının tespiti gerçekleştirilerek detaylı bir network haritası çıkarılır. Network haritalama bilgi toplama aşamasından elde edilen bilgilerin doğrulanmasına yardımcı olarak, hedef sistemler ile ilgili daha detaylı bilgi elde edilmesini sağlayacaktır.

## Enumerating Aşaması

Bu aşamada bir önceki adımda canlı olduğu tespit edilen sistemler üzerinde TCP/UDP port tarama işlemi gerçekleştirilir. Açık olduğu tespit edilen portları hangi servislerin kullandığı, bu servislerin hangi üreticiye ait servisler olduğu, versiyonları gibi bilgiler “banner grabbing” olarak adlandırılan yöntem ile öğrenilir ve manuel testler ile bu bilgilerin doğruluğundan emin olunduktan sonra bu bilgiler ışığında zafiyet veritabanları taranır ve bilinen zafiyetler sonraki aşamalarda kullanılmak üzere not alınır.

Tespit edilen canlı sistemler içinde router, switch gibi aktif ağ cihazlarının yer alması durumunda bu cihazlar üzerinde çalışan işletim sistemleri, bu işletim sistemlerinin versiyonları, bu cihazlar üzerindeki servisler, yönlendirme protokolleri, yönetimsel amaçlı servisler ve versiyonları tespit edilmeye çalışılır ve bu bilgiler ışığında zafiyet veritabanında inceleme yapılarak sonraki aşamalarda kullanılmak üzere not alınır. Ayrıca bu cihazlar üzerinde koşan gereksiz servislerin, ön-tanımlı kullanıcı adı veya şifre bilgilerinin ya da yönetim için kullanılan güvensiz protokollerin tespiti halinde bu zafiyetler yapılandırma problemleri başlığı altında rapora yansıtılır.

## Zafiyet Tarama Aşaması

Hedef sisteme ait bilgi toplama ve network haritasının çıkarılmasının ardından, elde edilen bilgiler değerlendirilerek zafiyet analizi gerçekleştirilir. Bu aşamanın amacı, daha önce elde edilen bilgileri kullanarak zafiyetlerin varlığını teknik olarak değerlendirmektir. Zafiyet tanımlaması; network, sunucular, uygulamalar ve diğer bileşenlerdeki zafiyetleri bulmak için elde edilen verileri, çıkarılan network topolojisini değerlendirerek gerçekleştirilen güvenlik denetimini bir adım ileriye taşır. Bu aşamada hedef sisteme zarar vermeyecek şekilde zafiyetleri tanımlamak ve tanımlanan zafiyetleri bilinen istismarlarla sömürmek için çeşitli otomatize zafiyet tarama araçlarıyla taramalar gerçekleştirilebilir. Zafiyet tarama araçlarının ayarları ön tanımlı olarak kullanılmamakta ve hedef sisteme göre yapılandırma sağlanmaktadır. Tarama sonuçları Sızma Testi Uzmanı tarafından değerlendirilerek false positive ve false negatif sonuçlar elenmektedir. Zafiyet tanımlaması ve analizi sonucunda hedef sisteme sızma yolları ve senaryoları belirlenmektedir.

## Hak Elde Etme Aşaması

Zafiyet analizi sonrası tanımlanan zafiyetler istismar edilmeye çalışılarak, hedef sistem ve güvenliği üzerinde denemeler gerçekleştirilir. Hedef sistem üzerindeki güvenlik önlemlerini aşılarak erişim elde edilmeye ve erişim mümkün olduğunca bağlantı (reverse, bind) sağlanmaya çalışılır. Tanımlanan zafiyetlerin istismarı için uygun PoC kodları/araçları kullanılarak veya yazılarak hedef sistem üzerinden testler gerçekleştirilir. İstismar için kullanılacak olan exploit halka açık kaynaklardan elde edilmişse hedef sistem üzerinde kullanılmadan önce klonlanmış ortamında test edilmekte ve hedef sisteme zarar verilecek işlemlerden kaçınılmaktadır.

## Hak Yükseltme Aşaması

Erişim kazanmak bir sızma testinin odak noktasını oluşturur. Tanımlanan zafiyetler istismar edilerek hedef sistem üzerin de erişim elde edilmeye çalışılır. Erişim elde etmek için hedef sistem üzerinde tespit edilen servislerde kullanıcı adı/parola kombinasyonlarının keşfi, sistem hesaplarına yönelik boş veya varsayılan parolaların bulunması, kullanılan uygulama ve donanım cihazlarının varsayılan ayarlarda bulunması gibi zafiyetler istismar edilebilir. Hedef sisteme düşük yetkilerle dahi olsa erişim sağlandıktan sonra hak ve yetki yükseltilmeye çalışılır.

Hak ve yetki yükseltmek için erişilen hesap üzerinden çeşitli exploitler denenerek root, administrator, SYSTEM gibi yetkili kullanıcı profiline geçilmeye çalışılır.

## Başka Sistemlere Sızma Aşaması

Erişim yapılan sistemlerden şifreli kullanıcı bilgilerinin alınarak daha hızlı bir ortamda denenmesi. Sızılan sistemde zehirleme araçları çalıştırılabiliyorsa ana sisteme erişim yapan diğer kullanıcı/sistem bilgilerinin elde edilmesi. Sistemde bulunan çevresel değişkenler ve çeşitli network bilgilerinin kaydedilerek sonraki süreçlerde kullanılması.

## Sistemde Kalıcı Olma Aşaması

Sisteme girildiğinin başkaları tarafından belirlenmemesi için bazı önlemlerin alınmasında fayda vardır. Test süresince yetkili sistemler üzerine arka kapılar yerleştirilmesi, fark edilmeyecek şekilde yetkili hesaplar tanımlanması gibi aşamalardır.

## Temizlik Aşaması

Hedef sistemlere bırakılmış arka kapılar, test amaçlı scriptler, sızma testleri için eklenmiş tüm veriler not alınarak test bitiminde sistem akışını tamamıyla eski haline getirmeyi hedefleyen aşamadır.

## Web Uygulama Güvenlik Testleri

Kapsam dahilinde kurumun internet ve intranet ortamında yayın yapan web sunucuları ve web uygulamaları test edilir. Web uygulamalarının aşağıdaki zafiyet türlerine göre dayanıklılığı tespit edilmeye çalışır. Kapsam dahilinde, internet bankacılığı, banka kurumsal sayfası gibi dışarı yayın yapan sunucu ve uygulamalar öncelikle test edilerek zafiyetler tespit edilmeye çalışır.

* Bilgi Toplama (Information Gathering)
  + Spider, Robots, Crawlers
  + Search Engine Discovery/Reconnaissance (Arama Moturu Keşfi ve Arama Motorunun Kötüye Kullanımı)
  + Identify Application Entry Points (Uygulama Girdi Noktalarının Tespiti)
  + Web Application Fingerprint (Uygulama İzlerinin Tespiti)
  + Application Discovery (Uygulamanın Keşfi ve Haritalama)
  + Analysis of Error Codes (Hata Kodlarının Analizi)
* Yapılandırma Yönetimi Testleri (Configuration Management Testing)
  + SSL/TLS Testing
  + DB Listener Testing
  + Infrastructure Configuration Management Testing (Altyapı Yapılandırma Yönetimi Testi)
  + Application Configuration Management Testing (Uygulama Yapılandırma Yönetimi Testi)
  + Testing for File Extensions Handling (Dosya Uzantılarını İşleme Testi)
  + Old, Backup and Unreferenced Files (Eski, Yedeklenen ve Referanslanmayan Dosya Testleri)
  + Infrastructure and Application Admin Interfaces (Altyapı ve Uygulama Yönetim Paneli Testi)
  + Testing for HTTP Methods and XST (HTTP ve XST Metod Testleri)
* Yetkilendirme Testleri
  + Credentials Transport Over an Encrypted Channel (Kimlik Bilgilerinin Şifreli Kanallar Üzerinden Taşınması Testleri)
  + Testing for User Enumeration (Kullanıcı Hesaplarının Tespitine Yönelik Testler)
  + Testing for Guessable (Dictionary) User Account (Kullanıcı Hesaplarına Yönelik Sözlük Saldırıları)
  + Brute Force Testing (Kaba Kuvvet Testi)
  + Testing for Bypassing Authentication Schema (Kimlik Doğrulama Şemasını Atlatma Testleri)
  + Testing for Vulnerable Remember Password and PWD Reset (Savunmasız Parola Hatırlatma ve Parola Sıfırlama Testi)
  + Testing for CAPTCHA
  + Testing Multiple Factors Authentication (Çok Faktörlü Kimlik Doğrulama Testi)
* Oturum Yönetimi Testleri
  + Testing for Session Management Schema (Oturum Yönetimi Şeması Testi)
  + Testing for Cookies Attributes (Çerez Niteliklerinin Testi)
  + Testing for Session Fixation (Sabit Oturum Testi)
  + Testing for CSRF (CSRF – Siteler Arası İstek Sahteciliği Testi)
* Kimlik Doğrulama Testleri
  + Testing for Path Traversal (Dizin Gezinme Testi)
  + Testing for Bypassing Authorization Schema (Yetki Şemasını Atlatma Testi)
  + Testing for Privilege Escalation (Hak ve Yetki Yükseltme Testi)
* Veri Değerlendirme Testleri
  + XSS (Cross Site Scripting-Çapraz Site Betik Yönlendirme) Testleri
    - Reflected XSS
    - Stored XSS
    - DOM Based XSS
  + SQL Injection
  + Path Injection
  + LDAP Injection
  + Code Execution
    - OS Code Execution

## İstemci Tarafı Sızma Testleri

Gerçekleştirilecek denetimlerde “İstemci Tarafı Sızma Testleri” kapsamında istemcilerin yapılandırmaları incelenerek mantık hataları ve eksiklikleri kontrol edilmektedir.

## Servis Dışı Bırakma Testleri

Bu kapsamda gerçekleştirilecek testler ile penetrasyon testi kapsamındaki sunucuların ve servislerin olası servis dışı bırakma saldırılarına karşı ne kadar korunaklı oldukları tespit edilmeye çalışılır. Kontrollü bir şekilde gerçekleştirilecek bu servis bırakma saldırıları hem uygulama katmanında hem de network katmanında yapılır.

## Veritabanı Zafiyet Testleri

Bu test adımında veritabanlarına özel güvenlik taramaları gerçekleştirilir. Yapılan zafiyet taramaları sırasında veritabanları üzerindeki varsayılan konfigürasyondan kaynaklı zafiyetlerden eksik güncellemelere, ön tanımlı şifrelerin tespitine kadar birçok Veritabanı sistemlerine özel açıklıklar tespit edilebilmektedir.

## Kablosuz Ağ Sızma Testleri

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

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

## EKS/SCADA (Endüstriyel Kontrol Sistemleri) Güvenlik Testleri

* Bilgi Toplama: Hedeflenen EKS/SCADA sistemleri hakkında ayrıntılı bilgi toplanır. Bu adımda, ağ altyapısı, kullanılan teknolojiler, sistem bileşenleri, bağlantı noktaları, erişim yönetimi ve güvenlik politikaları gibi bilgiler analiz edilir.
* Tehdit Modellemesi: Sistemdeki potansiyel tehdit senaryoları belirlenir ve bunların etkileri değerlendirilir. Bu adımda, saldırganların nasıl bir saldırı düzenleyebileceği, hedeflenen zayıf noktalar ve olası etkileri üzerine odaklanılır.
* Zayıf Nokta Tespiti: Sistemdeki güvenlik açıkları ve zayıf noktalar belirlenir. Bu adımda, ağ taraması, güvenlik açığı taraması ve konfigürasyon denetimleri gibi teknikler kullanılarak potansiyel riskler ve eksiklikler tespit edilir.
* Yetkilendirme ve Erişim Kontrolü Analizi: Sistemdeki yetkilendirme mekanizmaları, parola politikaları ve erişim kontrolü yöntemleri analiz edilir. Bu adımda, güçlü şifreleme, iyi parola yönetimi uygulamaları ve gereksiz erişim izinlerinin kaldırılması gibi önlemler üzerinde durulur.
* Saldırı Simülasyonu: Sistemde saldırı senaryoları simüle edilir. Bu adımda, saldırganların hedef sistemlere nasıl sızabileceği veya hizmeti kesintiye uğratabileceği gibi durumlar modellenir. Bu sayede, sistemin güvenlik önlemlerinin ne kadar etkili olduğu değerlendirilir.
* Raporlama ve Öneriler: Sızma testi sonuçları detaylı bir rapor haline getirilir. Bu raporda, tespit edilen güvenlik açıkları, zayıf noktalar ve riskler ayrıntılı olarak açıklanır. Ayrıca, bu açıkları gidermek için öneriler ve iyileştirme adımları sunulur.

EKS/SCADA güvenlik testleri, endüstriyel kontrol sistemlerinin güvenliğini değerlendirmek, potansiyel riskleri belirlemek ve önleyici önlemler almak için önemli bir adımdır.

## Raporlama

Gerçekleştirilen güvenlik denetiminden sonra takip eden 10 (on) iş günü içerisinde yapılan testlerin tamamının tek rapor sureti olmak üzere hazırlanarak parola korumalı durumda kuruma e-posta yolu ile teslim edilir.

Teslim edilecek rapor aşağıdakileri içerir;

* Gerçekleştirilen güvenlik denetim çalışmasına ve bulgulara ilişkin yönetici özeti
* Test sırasında tespit edilen zafiyetlerin kritiklik seviyelerini, hangi sistemlerde bu zafiyete rastlandığını gösteren ve zafiyeti ortadan kaldırmaya yönelik çözüm önerilerinin bulunduğu zafiyet kimlik kartları
* Kategori şekilde Risk Seviyesi Özet Dağılımını içeren tablolama

Teslim edilecek raporların yanında zafiyetlerin giderilip giderilmediğinin takibini kolaylaştırmak adına tespit edilen zafiyetlerin ve bu zafiyetlerin bulunduğu sistemlerin bilgisinin yer aldığı bir Excel dokümanı kuruma verilir ve doğrulama denetiminde bu dokümandaki bilgiler baz alınır. Kurum onayı ile doğrulama denetimine kadar gerçeleştirilen sızma testi raporu saklanmaktadır. Doğrulama testi sonrası ise geri getirilemez şekilde temizlenmektedir.

## Sunum

Raporların tesliminden sonra istenmesi halinde kurum personeline, gerçekleştirilen sızma testine ilişkin özet mahiyetinde bir sunum yapılır. Bu sayede kurum personeli, sızma testini gerçekleştiren uzmanlarımızla test ile ilgili görüş alışverişinde bulunabilme imkânı kazanırlar.