**Milsafe Siber Güvenlik Eğitim ve Danışmanlık**

**Sızma Testi Kapsam ve Bilgi Formu**

| Kuruma Ait Bilgiler | |
| --- | --- |
| Firma Adı |  |
| Firma Adresi |  |
| Yetkili Kişi |  |
| Yetkili Kişi Mail |  |
| Yetkili Kişi Telefon |  |
| Talep Edilen Test Tarihi |  |

## 

## **TALEP EDİLEN HİZMETLER**

**Not**: Test kategorileri hakkında bilgi almak için lütfen kategorilere CTRL tuşu ile birlikte basıp ilgili açıklamaları inceleyiniz.

| Test Kategorileri | Test isteniyor mu? (X: isteniyor) | |
| --- | --- | --- |
| [DIŞ AĞ](#_heading=h.3znysh7) SIZMA TESTLERİ | Evet ( ) Hayır ( ) | |
| WEB UYGULAMALARI SIZMA TESTLERİ | Evet ( ) Hayır ( ) | |
| [MOBİL UYGULAMA](#_heading=h.tyjcwt) SIZMA TESTLERİ | Evet ( ) Hayır ( ) | |
| [SOSYAL MÜHENDİSLİK](#_heading=h.3dy6vkm) TESTLERİ | Evet ( ) Hayır ( ) | |
| [VOIP](#_heading=h.1t3h5sf) AĞLARINA YÖNELİK SIZMA TESTLERİ | Evet ( ) Hayır ( ) | |
| [YEREL AĞ](#_heading=h.4d34og8) SIZMA TESTLERİ | Evet ( ) Hayır ( ) | |
| NAC-802.1x Sızma Testleri de  isteniyor mu? | Evet ( ) Hayır ( ) |
| [KABLOSUZ AĞ](#_heading=h.2s8eyo1) SIZMA TESTLERİ | Evet ( ) Hayır ( ) | |
| SERVİS SONLANDIRMA (DDOS) TESTLERİ | Evet ( ) Hayır ( ) | |
| [ENDÜSTRİYEL KONTROL SİSTEMLERİ](#_heading=h.3rdcrjn) (SCADA) | Evet ( ) Hayır ( ) | |
| BİLGİ GÜVENLİĞİ FARKINDALIK EĞİTİMLERİ | Evet ( ) Hayır ( ) | |

**NOTLAR**

* Yukarıdaki test kategorileri hakkında bilgi almak için “Pentest Hizmeti Detayları” kısmını inceleyiniz
* Yukarıdaki alanda gerçekleştirilmesini istediğiniz test türlerini işaretleyiniz.
* Sosyal Mühendislik Testleri Sızma Testi Projesi Kapsamında 1 senaryo olarak uygulanmaktadır.

## **RAPORLAMA**

**Not**: Rapor dilinin birden fazla seçilmesi daha fazla **efora** neden olup dolayısıyla fiyatı etkileyecektir.

| Raporlama | |
| --- | --- |
| Rapor Dili | Türkçe ( ) İngilizce ( ) |

## **DIŞ AĞ TEST HİZMETİ (İNTERNET ÜZERİNDEN)**

| Dış Ağ Test Hizmeti (Lütfen Bileşen Sayıları Giriniz) | |
| --- | --- |
| Toplam Aktif Sunucu Sayısı (Sanal + Fiziksel) |  |
| Dış Ağ IP Adresleri/Blokları |  |

## **WEB UYGULAMA TEST HİZMETİ**

**Not**: Uygulamalarınız için ne kadar bir **efora** ihtiyaç duyulacağına verilen test hesapları ile sistem analizi ile karar verilmektedir.

| No | URL Adresi | Uygulama Teknolojisi (.Net, PHP, Java) | İnternete Açık mı? | Test Hesabı Verilecek mi? | Test Hesabı  (Kullanıcı /Parola) |
| --- | --- | --- | --- | --- | --- |
| 1 |  |  | E (..) H (..) | E (..) H (..) |  |
| 2 |  |  | E (..) H (..) | E (..) H (..) |  |
| 3 |  |  | E (..) H (..) | E (..) H (..) | E (..) H (..) |
| 4 |  |  | E (..) H (..) | E (..) H (..) | E (..) H (..) |
| 5 |  |  | E (..) H (..) | E (..) H (..) | E (..) H (..) |
| 6 |  |  | E (..) H (..) | E (..) H (..) | E (..) H (..) |
| 8 |  |  | E (..) H (..) | E (..) H (..) | E (..) H (..) |
| 9 |  |  | E (..) H (..) | E (..) H (..) |  |
| 10 |  |  | E (..) H (..) | E (..) H (..) |  |
| 11 |  |  | E (..) H (..) | E (..) H (..) |  |

## **MOBİL UYGULAMA TEST HİZMETİ**

**Not**: Uygulamalarınız için ne kadar bir **efora** ihtiyaç duyulacağına verilen test hesapları ile sistem analizi ile karar verilmektedir.

| No | Uygulama Adı | Platform | İnternete Açık mı? | Test Hesabı Verilecek mi? | Test Hesabı  (Kullanıcı /Parola) |
| --- | --- | --- | --- | --- | --- |
| 1 | [www.example.com](http://www.example.com) | Android (x ) IOS (x ) | E (X) H ( ) | E (x) H( ) | Admin / 1234 |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |

## **İÇ AĞ TEST HİZMETİ (KURUM YEREL AĞINDAN)**

| İç Ağ Test Hizmeti | |
| --- | --- |
| Testin Gerçekleşeceği Yer/Yerler |  |
| Toplam Aktif Sunucu Sayısı |  |
| Toplam Bilgisayar Sayısı |  |
| NAC/802.1X veya FW izni verilmeden de test  isteniyor mu? |  |
| Toplam SSID (Kablosuz Ağ Adı) Sayısı |  |
| Yerel Ağ Vlan Sayısı |  |
| Subnet Bilgileri |  |

## **SOSYAL MÜHENDİSLİK TEST HİZMETİ**

| Sosyal Mühendislik Testi | |
| --- | --- |
| Test Edilecek Kullanıcı Sayısı |  |

# PENTEST HİZMETİ DETAYLARI

**Not**: Ayrıntılı Bilgiye Sızma Testi Yöntem ve Aşamaları dokümanından ulaşılabilir.

## DIŞ AĞ TEST HİZMETİ (İNTERNET ÜZERİNDEN)

Dış ağ üzerinden gerçekleştirilen testlerde Kurum tarafından verilen kapsam dahilinde dış dünyaya açık olan sistemlere yönelik sızma testi gerçekleştirilir. Kuruma ait servis, panel ve diğer kullanıcı giriş alanları aktif, pasif ve OSINT yöntemleri ile elde edilen bilgiler ile test edilir sisteme sızılmaya çalışılır.

## WEB UYGULAMA TEST HİZMETİ

Bu test kategorisinde Kurum tarafından verilen WEB uygulamalarına yönelik sızma testleri gerçekleştirilir Sızma testlerinde **OWASP 4.1** test yönergeleri izlenir. Firmaya ait uygulamalara ve web servislerine yetkili/yetkisiz hesap bilgileri ile giriş yaparak denetimler gerçekleştirilir. Kurum tarafından test hesabı verilmesi durumunda (test hesabı verilmesi şiddetle önerilir, böylece uygulama parametreleri ve fonksiyonları daha kapsamlı bir şekilde test edilmektedir) uygulamalar test hesapları ile kapsamlı bir şekilde test edilirler.

## MOBİL UYGULAMA TEST HİZMETİ

Bu test kategorisinde Kurum mobil uygulamaları OWASP Mobil uygulama test yönergeleri (**MSTG**) kapsamında test edilmektedir. Android ve iOS işletim sistemi için geliştirilmiş mobil uygulamalara yönelik statik ve dinamik güvenlik testlerini içermektedir. Bu test kategorisinde de kullanıcı hesaplı testler daha sağlıklı ve kapsamlı olmaktadır. Gerekli durumlarda kaynak kod denetimi de yapılabilir.

## SOSYAL MÜHENDİSLİK TEST HİZMETİ

Bu test kategorisinde Kurum tarafından verilen e-posta adreslerine veya internet üzerinden bulunan e-posta adreslerine yönelik oltalama saldırıları gerçekleştirilir. Bu test Kurum yetkilileri ile koordineli bir şekilde yürütülür. Test sonrasında detaylı istatistikler Kurum ile paylaşılır.

## VOIP TEST HİZMETİ

VOIP testlerinde Kurum sistemlerine yönelik sızma testleri gerçekleştirilir. İletişim düzeyinde kullanılan şifreleme algoritmaları, yetkisiz çağrı girişimleri, iletişim izlenebilmesi gibi senaryolar gerçekleştirilir.

## İÇ AĞ TEST HİZMETİ

Bu test kategorisinde Kurum sistemlerine yerel ağdan gelebilecek saldırılar canlandırılır. Fiziksel ve yerel ağ erişimi üzerinden senaryolar canlandırılır. Yetkisiz bir Kurum çalışanının kötü niyetli olması durumunda sistemlere ne gibi zararlar verebileceği canlandırılır. Bu test kapsamında verilen tüm sistemlere yönelik kapsamlı bir sızma testi girişimlerinde bulunulur.

## KABLOSUZ AĞ TESTLERİ

Kablosuz ağ testleri kapsamında verilen Kurum kablosuz ağlarına yönelik, kimlik doğrulama, DOS saldırısı, yetkisiz ağ oluşturma gibi senaryolar gerçekleştirilir. Ayrıca ağ üzerinde bulunan Kullanıcılara yönelik sızma girişimlerinde bulunulur.

## SERVİS SONLANDIRMA TESTLERİ

Bu test kapsamında Kurum tarafından dış dünyaya hizmet verilen servislere yönelik DOS/DDOS saldırıları gerçekleştirilir. Saldırı bant genişliği müşteri tarafından seçilmektedir. Yine bu test ile alınan DDOS hizmetinin doğru bir şekilde yapılandırılma durumu test edilmiş olmaktadır. DDOS testi için yaygın olarak kullanılan yöntemler kullanılmaktadır. Kurum tarafından talep edilmesi durumunda ayrıca farklı senaryolar da gerçekleştirilmektedir.

## ENDÜSTRİYEL KONTROL SİSTEMLERİ

Bu test kapsamında Kurum EKS sistemleri fiziksel güvenlik, network güvenliği ve sistem güvenliği testlerine tabi tutulmaktadır. Testler esnasında NESCOR, ISO27001 ve ISO 27019:2013 tarafından önerilen testler uygulanmaktadır.