# TÜRK STANDARDLARI ENSTİTÜSÜ

# SIZMA TESTİ TEKNİK KRİTERLERİ PROGRAMI



**Sürüm 1.0**

**01.12.2013**

## Revizyon Tarihçesi

| Sürüm | Tarih | Güncelleme |
|---|---|---|
| 1.0 | 01.12.2013 | İlk sürüm |
| | | |
| | | |
| | | |

Bu dokümana aşağıdaki Web sayfasından erişilebilir:

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

# İÇİNDEKİLER

# 1. Test öncesi

## 1.1 Kapsam belirleme

Kapsam belirleme sızma testinin çok önemli ve genellikle göz ardı edilen bileşenlerinden biridir. Bir ağa erişim için kullanılabilecek farklı araçlar ve teknikler hakkında birçok kitap yazılmıştır. Ancak, teste nasıl hazırlanılacağı konusunda çok az yayın vardır. Bu husus testi icra edenler için kapsamda kontrol dışı değişiklikler ve büyümeler, hukuki konular ve şikayetçi müşteriler gibi alanlarda sorunlara yol açabilir.

Bu bölümün amacı bu gibi tuzaklardan kaçınmanız için sizlere bazı araçlar ve teknikler sağlamaktır. Bu bölümdeki bilgilerin büyük bir kısmı bunları yazan test uzmanlarının tecrübelerinin sonuçlarıdır. Unutulmamalıdır ki, aldığımız derslerin çoğu, zorlukla öğrendiklerimizdir.

Kapsam belirleme spesifik olarak neyi testte tabi tutacağınızla ilgilidir. Testi nasıl yapacağınızı kapsayan bölümden oldukça farklıdır. Testin ne şekilde icra edileceği iş kuralları bölümünde kapsanacaktır.

Bir sızma testi arayışında olan bir müşteri kuruluş konumundaysanız bu dokümanın genel sorular bölümüne bakmanızı öneririz. Bu bölümde bir teste başlamadan önce cevaplanması gereken temel sorular kapsanmaktadır. Bir sızma testinde bir cepheleşmenin olmaması gerekir. Bu test, testi icra edenin sizi “hack”leyip, “hack”leyemeyeceğini görmek için gerçekleştirilen bir faaliyet olmamalıdır. Bu testin amacı bir saldırı ile ilgili olarak ortaya çıkabilecek iş risklerinin belirlenmesi olmalıdır. İyi bir test firması, kapsam belirleme faaliyeti geliştikçe kuruluşa özgü olarak düzenlenmiş ilave sorular sormaya başlar.

## 1.2 Kapsam belirleme nasıl yapılmalıdır?

Bir testin kapsamının belirlenmesinin anahtar bileşenlerinden birisi testin icracısı olarak zamanınızı tam olarak nasıl geçireceğinizi anlamaya çalışmaktır. Örneğin, bir müşteri kuruluş sizden 100 adet IP adresini test etmenizi isteyebilir ve bunun için size sadece 100.000 TL ödemek isteyebilir. Bu ortalama olarak her bir IP başına 1000 TL demektir. Bu durumda sizden çok kritik olan sadece bir uygulamayı test etmeniz istendiğinde bu ücret yapısı uygun olacak mıdır? Sızma testinde ücretler doğrusal olarak belirlenemez.

Sonuç olarak, bazı sızma testlerinde elinizde içlerinden seçerek bir testin bir bölümü kapsamında bir ağa erişim sağlamak üzere teste tabi tutulacak çok sayıda IP adresi bulunacaktır. Aynı zamanda tek bir spesifik uygulama için haftalarınızı harcayacağınız (aylar değilse bile), üst derecede odaklanacağınız testler de olacaktır. Burada anahtar husus aradaki farkı bilmektir. Bu şekildeki bir anlayış ile bir müşteri kuruluşun istediğinin ne olduğunu, müşteri bunu tam olarak ifade edemese de bilmek durumunda olacaksınız.

## 1.3 Zaman tahmini için parametreler

Zaman parametreleriyle ilgili hususlar çoğunlukla testi icra edeceğiniz alandaki tecrübenize bağlı olacaktır. Örneğin, şimdiye kadar herhangi bir uygulama için tam kapsamlı, derinlemesine bir test icra ettiniz mi? Şimdiye kadar geniş bir yelpazedeki IP adreslerini teste tabi tuttunuz mu? Bu iş için geriye

dönerek iletilerinizi ve tarama günlüklerinizi inceleyin. Bulduğunuz zaman değerleri bir yere yazın ve buna asgari %20 ölçüsünde bir süre ilave edin.

Zaman değerine neden %20 ilave ediyoruz? Buna ihtiyaç duyulmasının nedeni her işte testin icrası aşamasında küçük duraksamaların yaşanabileceğidir. Örneğin bir ağ bölütü çökebilir (sizin test faaliyetlerinize bağlı olarak olmaması umulur). Test yapmadan geçen bu süre, aslında size bir test uzmanı maliyeti getirir. Diğer bir örnek toplantıların yavaşlatmasıdır. Çoğu zaman sistemde çok büyük ölçüde bir açıklık tespit edilir ve bu husus müşteri kuruluş ile paylaşılır. Müşteri kuruluş bu durumda sizden üst yönetimle bir toplantıya katılmanızı isteyecektir. Tabii ki siz de katılacaksınız ve bu toplantı sizin genel test sürenizden götürecektir.

Fazladan koyduğunuz %20'lik ek süreye ihtiyaç duymazsanız ne olur? Bu sürenin karşılığında alınan parayı cebe atmak tabii ki etik olmaz. Bunun yerine müşteri kuruluşa test bakımından ilave değerler sağlanır. Firmanın güvenlik timi ile açıklığın istismarına yönelik olarak attığınız adımların üzerinden gidebilirsiniz. Orijinal anlaşmada mevcut değilse, bir yönetici özeti verebilirsiniz ya da başlangıç testi esnasında anlaşılması zor olan bir açıklığı kırmak için ilave biraz zaman harcayabilirsiniz.

Zaman parametrelerinin ve testin icrasının başka bir bileşeni de projenizin kesin bir teslim tarihinin bulunmasıdır. İyi bir projenin bir başlangıcı ve bir sonu olur. Sizin testinizin de olması önerilir. Testin sone ereceği belirli tarihe gelinirse ve iş bitmemişse veya bu tarihten sonra sizden herhangi bir ilave test talebinde bulunulursa yapılacak olan işi ve bu iş için gereken zamanı belirten imzalı bir iş açıklamasının bulunması gerekir.

Bazı test uzmanları bunu yapmakta çok zorlanırlar çünkü maliyetlere ve saatlere gelindiğinde kendilerini baskı altında hissederler. Ancak yazarın tecrübesine göre esas test için olağanüstü bir değer sunduğunuz taktirde müşteri kuruluş sağladığınız ilave hizmet için ödeme yapmada ayak diremeyecektir.

## 1.4 Kapsam belirleme toplantısı

Çoğu zaman kapsam belirleme toplantısı anlaşma imzalandıktan sonra yapılır. Bizim önerimiz gizlilik sözleşmesi imzalanmadan derinlikli, herhangi bir kapsam belirleme görüşmesinin yapılmamasıdır.

Kapsam belirleme toplantısının amacı neyi test edeceğinizi görüşmektir. Bu toplantı işle ilgili kuralları kapsamaz. Bu toplantı maliyetleri de kapsamaz. İşe başlamadan öncesinin konuları olan bu farklı hususlarının ayrı toplantılara ve bölümlere ayrılmasının daha iyi olacağını düşünmekteyiz. Bu düzeyde bir ayrımın yapılmasının nedeni, toplantı hedefleri açık olarak ortaya konmadığında görüşmelerin karmaşık hale gelebilmesidir. Bu husus bir toplantının konuyla ilgisi olmayan konuşmalarla çıkmaza sokulmaması için toplantının kontrol altına alınması ve sürdürülmesinin bir parçasıdır.

Şimdi projenin yaklaşık büyüklüğü hakkında kabaca bir fikre sahip olduğunuza göre müşteri kuruluş ile varsayımların doğrulanması için bir toplantı yapmanın zamanı gelmiştir. Öncelikle müşteri kuruluşa hangi IP aralığının testle ilgili olarak kapsam dahilinde olduğunu açık bir şekilde sormanız gerekecektir. Bazı müşteriler bu noktada geriye çekilerek, aynen kötü adamların yaptığı gibi ağları belirlemenin ve bu ağa saldırıda bulunmanın size bağlı olduğunu söyleyeceklerdir. Test ortamında herhangi bir hukuki kısıtlamanın bulunmaması iyi olur. Ancak test uzmanları olarak bizim doğru sistemleri test ettiğimizi ve doğru sistemlere yönelik saldırıda bulunduğumuzdan emin olmak için daha ileri gitmemiz gerekir. Örneğin, toplantıda müşteri kuruluşun hedef teşkil edecek ortamlara, DNS sunucusuna, e-posta sunucusuna, Web sunucularının üzerinde çalıştığı esas donanıma ve bunların güvenlik duvarı / IDS / IPS çözümlerine sahip olup olmadığı sorulmalıdır.

İlave olarak hedef ortamın hangi ülkelerde işletildiğini belirlememiz gerekir. AB ülkelerinde bireylerin gizliliğini kuşatan bazı çok sıkı kanunlar bulunabilir. Bu hususun işinizin sosyal mühendislik yönü üzerinde bir etkisi olabilir.

## 1.5 Saat başına ücretlendirilen ilave destek

Açık bir şekilde yapılacak işin kapsamına alınmayan herhangi bir şeye dikkatle yaklaşılmalıdır. Bunun birkaç nedeni vardır. Birinci neden, bunun kapsamda kontrol dışı değişiklere ve büyümelere yol açmasıdır. Bu gibi görevler sizin işten elde edeceğiniz karı kolaylıkla yok edebilir ve müşteri kuruluşla aranızda kafa karışıklığına ve sinirlenmelere yol açabilir. Plansız olarak ilave işler alınmasında çoğu test uzmanının düşünmediği başka bir husus ta konunun hukuki bakımdan dallanıp budaklanmasıdır. Plansız olarak yapılan iş isteklerinin çoğu uygun bir şekilde belgelendirilmemişlerdir ve buna bağlı olarak herhangi bir anlaşmazlık ya da hukuki işlem durumunda bu işi kimin istediğini belirlemek güç olacaktır. Dahası elinizdeki sözleşme yapılacak olan işi belirten hukuki bir dokümandır.

Önerimiz, herhangi bir ilave talebin, yapılacak olan işi açık bir şekilde belirten, iş açıklaması biçiminde bir belgeye dökülmesidir. Sözleşmede aynı zamanda ilave işlerin saat başı sabit bir ücret karşılığında yapılacağı ve imzalı ve onaylı bir sözleşme mevcut olmadıkça ilave işlerin tamamlanamayacağı açık bir şekilde belirtilmelidir.

## 1.6 Anketler

Müşteri kuruluşla ilk defa iletişim kurmaya başladığınızda, sızma testinin kapsamını tam olarak belirleyebilmenizden önce cevaplandırılmasına ihtiyaç duyacağınız bir grup soru olacaktır. Bu soruların sorulması çok önemlidir ve sizin için müşteri kuruluşun sızma testinden ne elde etmek istediğini, müşteri kuruluşun kendi ortamına yönelik olarak neden bir sızma testi gerçekleştirilmesini istediğini ve sızma testinin icrası esnasında müşteri kuruluşun belirli türde testlerin yapılmasını isteyip istemediğini daha iyi anlamanıza olanak sağlamalıdır.

Aşağıdaki sorular yapılacak işin müşteri kuruluş için maliyetinin ne olacağının tam olarak belirlenmesi öncesinde cevaplandırılması gerekebilecek bazı sorulardır:

### Genel sorular

### Ağ sızma testi için sorular

1. Müşteri kuruluş neden kendi ortamına yönelik olarak bir sızma testi gerçekleştirilmesini istemektedir?
2. Sızma testine özel bir uygunluk gereksiniminin karşılanmasına yönelik olarak mı ihtiyaç duyulmaktadır?
3. Müşteri kuruluş icra edilecek olan sızma testinin aktif bölümlerinin (tarama, sayma, istismar etme vb.) ne zaman uygulanmasını istemektedir?
4. İş saatleri içerisinde mi?
5. İş saatleri dışında mı?
6. Hafta sonları mı?
7. Toplamda kaç adet IP adresi teste tabi tutulacaktır?
8. Kaç adet iç IP adresi teste tabi tutulacaktır (uygulanabiliyorsa)?
9. Kaç adet dış IP adresi teste tabi tutulacaktır (uygulanabiliyorsa)?

10. Sızma testinin sonuçlarını etkileyebilecek güvenlik duvarı, sisteme izinsiz girişleri tespit/engelleme sistemi, Web uygulaması güvenlik duvarı veya iş yükü dengeleyici gibi araçlar mevcut mudur?
11. Sisteme sızmanın gerçekleşmesi durumunda ne yapmalıyız?:

Gizliliği ihlal edilmiş olan bilgisayarda lokal bir açıklık değerlendirmesi mi gerçekleştirilmelidir? Gizliliği ihlal edilmiş olan bilgisayar üzerinde en üst derecede yetki ayrıcalığı (unix bilgisayarlarda "root", Windows bilgisayarlarında sistem ya da yönetici) mı elde edilmeye çalışılmalıdır? Elde edilen yerel parola karmalarına yönelik olarak; hiç bir saldırı gerçekleştirmemeli miyiz? Yoksa, asgari ölçüde, sözlük destekli olarak veya kapsamlı bir parola saldırısı mı gerçekleştirmeliyiz?

### Web uygulaması sızma testi için sorular

1. Kaç adet Web uygulaması değerlendirmeye tabi tutulmaktadır?
2. Kaç adet oturum açma sistemi değerlendirmeye tabi tutulmaktadır?
3. Kaç adet statik Web sayfası değerlendirmeye tabi tutulmaktadır? (yaklaşık olarak)
4. Kaç adet dinamik Web sayfası değerlendirmeye tabi tutulmaktadır? (yaklaşık olarak)
5. Bakmak için kaynak kodu mevcut olacak mıdır?
6. Herhangi bir dokümantasyon mevcut olacak mıdır? Eğer olacaksa bunlar ne tür dokümantasyon olacaktır?
7. Bu uygulama üzerinde statik analiz gerçekleştirecek miyiz?
8. Müşteri kuruluş bu uygulamaya karşı fuzzing gerçekleştirmemizi istiyor mu?
9. Müşteri kuruluş role dayalı test icra etmemizi istiyor mu?
10. Müşteri kuruluş Web uygulamalarında yetki bilgilerini kullanarak taramalar gerçekleştirmemizi istiyor mu?

### Kablosuz ağ sızma testi için sorular

1. Kaç adet kablosuz ağ mevcuttur?
2. Bir misafir kablosuz ağı kullanılmakta mıdır? Eğer kullanılıyorsa:
3. Misafir kablosuz ağı kimlik sorgulaması gerektirmekte midir?
4. Kablosuz ağlarda hangi tür şifreleme kullanılmaktadır?
5. Kapsama alanının büyüklüğü nedir?
6. Sisteme bağlı olan ancak erişim ve işlem yetkisi olmayan aygıtların sayısını tespit edecek miyiz?
7. Müşteri kuruluşlara karşı gerçekleştirilen kablosuz saldırıları değerlendirmeye tabi tutacak mıyız?
8. Yaklaşık olarak kaç adet kullanıcı kablosuz ağı kullanıyor olacak?

### Fiziki Sızma Testi için sorular

1. Kaç adet lokasyon değerlendirmeye tabi tutulacaktır?
2. Fiziki lokasyon başkaları ile paylaşılmakta olan bir tesis midir? Eğer öyleyse:
3. Kaç bina katı kapsam dahilindedir?
4. Hangi bina katları kapsam dahilindedir?
5. Atlatılması gereken güvenlik görevlileri var mıdır? Eğer varsa:

6. Güvenlik görevlileri üçüncü bir kişi/kuruluş tarafından mı çalıştırılmaktadırlar? Silahlı mıdırlar? Güç kullanma yetkileri var mıdır?
7. Binaya kaç adet giriş vardır?
8. Her kapıyı açan türde anahtarlara müsaade edilmekte midir?
9. Mevcut güvenlik politikalarına ve prosedürlerine uygunluğun teyit edileceği fiziki bir sızma testi mi gerçekleştireceğiz? Yoksa sadece bir denetim mi gerçekleştireceğiz?
10. Kapsam dahilindeki alanın ölçüsü nedir?
11. Tüm fiziki güvenlik tedbirleri dokümante edilmiş midir?
12. Video kameralar kullanılmakta mıdır? Kullanıyorsa bu kameralar müşteri kuruluşa mı aittir?
13. Müşteri kuruluş kamera verilerinin saklanmakta olduğu yere erişim sağlama girişiminde bulunmamızı istiyor mu?
14. Kullanılmakta olan bir alarm sistemi var mıdır? Eğer varsa:
15. Alarm, sessiz bir alarm mıdır?
16. Alarm sistemi hareketle mi tetiklenmektedir?
17. Alarm sistemi kapıların veya pencerelerin açılmasıyla mı tetiklenmektedir?

### Sosyal mühendislik için sorular

1. Müşteri kuruluş, sosyal mühendislik girişiminde bulunabileceğimiz personelin elektronik posta adreslerini bize sağlayacak mıdır?
2. Müşteri kuruluş, sosyal mühendislik girişiminde bulunabileceğimiz personelin telefon numaralarını bize sağlayacak mıdır?
3. Fiziki erişime yönelik olarak sosyal mühendislik girişiminde bulunacak mıyız? Eğer bu yapılacaksa:
4. Kaç kişi hedeflenecektir?

Sızma testinin farklı düzeylerinde iş birim yöneticileri, sistem yöneticileri ve yardım masası personeline yönelik olarak bazı sorulara gerek duyulmayabilir. Ancak aşağıdaki sorular bir kılavuz olarak kullanılabilir.

### İş birimi yöneticileri için sorular

Bir sızma testi icra edilirken iş birimlerinin yöneticileri göz ardı edilemez. Bu kişiler bir hizmet dışı kalma durumu ortaya çıktığı taktirde, bu durumdan en fazla etkilenecek olan kişilerdir.

1. Bir testin uygulanmak üzere olduğunu biliyor musunuz?
2. İfşa edilmesi, bozulması veya silinmesi durumunda kurum için en büyük riskin ortaya çıkacağı esas veriler nelerdir?
3. Kendi iş uygulamalarınızın doğru bir şekilde çalıştığını teyit etmek için test ve doğrulama prosedürleri gerçekleştiriyor musunuz?
4. Kendi kalite güvence test prosedürleriniz mevcut mudur?
5. Uygulama verilerinize yönelik olarak acil kurtarma prosedürleriniz mevcut mudur?

### Sistem yöneticileri için sorular

Sistem yöneticilerinin sızma testi ve güvenlikle ilgili olarak güçleri göz ardı edilemez. Sistem yöneticileri kendi sistemlerini o kurumdaki herkesten çok daha iyi bilirler ve eğer herhangi bir şey yanlış gidiyorsa muhtemelen düzeltici işlemlerin ön safhalarında onlar olacaklardır.

1. Kırılgan olan sistemleri belirtir misiniz? (Çökmeye meyilli olan sistemleri, eski işletim sistemlerinin olup olmadığını veya herhangi bir nedenden ötürü yama yapılmamış sistemleri sorunuz.)
2. Ağda, sistem yöneticisine ait olmayan, ilave onay alınmasını gerektirebilecek sistemler mevcut mudur?
3. Değişim yönetimi prosedürleri mevcut mudur?
4. Sistem kesintilerinde ortalama onarım süresi ne kadardır?
5. Herhangi bir sistem izleme yazılımı mevcut mudur?
6. En kritik sunucularınız ve uygulamalarınız hangileridir?
7. Yedeklemeler düzenli olarak test edilmekte midir?
8. En son ne zaman yedeklemelerden geri yükleme yapılmıştır?

## 1.7 Kapsamdaki kontrol dışı değişikler ve genişleme

Sızma testinin kapsamındaki kontrol dışı değişikler ve büyümeler her şeyi mahvedebilir. Bu husus genellikle bir sızma testi firmasının varlığına son vermesinin en etkili yollarından biridir. Esas olan husus, birçok firmanın ve firma yöneticisinin böyle bir durumun ortaya çıktığını nasıl belirleyebileceğini ya da böyle bir duruma nasıl bir reaksiyon göstereceğini ya hiç bilmemesi ya da çok az şey bilmesidir.

Sızma testinin kapsamındaki kontrol dışı değişikler ve büyümelerle mücadelede akılda tutulması gereken birkaç husus mevcuttur. Bunlardan ilki, iyi bir iş çıkardıysanız müşteri kuruluşun ilave işler talep etmesinin çok yaygın olmasıdır. Müşteri kuruluş sizi ilave iş için ilave para talep etmeniz nedeniyle bırakıyorsa bu müşteri sizi kullanmaya çalışıyordur. Siz de bu sözleşmeyi sürdürmek istemezsiniz zaten.

İkinci husus daha da kritiktir. Mevcut müşteriniz sizden ilave işler talep ederse ondan para sızdırmaya çalışmayın. Fiyatlarınızı düşürmeyi telafi edebilirsiniz. İşin peşinde koşmanız gerekmemiştir. Resmi teklif prosedürlerini takip etmenize gerek kalmamıştır. Bunlara bağlı olarak müşteri kuruluşa %10'luk bir indirim yapmanız size bir şey kaybettirmez. Dahası, ilerdeki işleriniz için en iyi kaynağınız mevcut müşterilerinizdir. Onlara iyi davranırsanız onlar da size döner.

### İşin başlangıç ve bitiş tarihlerini belirleyin

Sızma testinin kapsamındaki kontrol dışı değişikler ve büyümeleri engellemenin anahtar bir bileşeni de işin başlangıç ve bitiş tarihlerinin belirlenmesidir. Test uzmanlarının başını yakan bir husus, yeniden teste tabi tutma işlemidir. Yeniden teste tabi tutma bir sözleşmenin uygulanmasında iyi bir fikirmiş gibi görünmektedir. Ancak çoğu zaman test uzmanları işlerin tamamı bitene kadar ödeme alamayacaklarını unuturlar. Bu işler yeniden teste tabi tutmayı da kapsamaktadır. Bunu halletmenin bir yolu yeniden teste tabi tutma işleminin nihai raporun sunulmasından sonra 30 gün içinde gerçekleşeceğinin sözleşmeye dahil edilmesidir. O zaman yeniden teste tabi tutma işleminin programa alınması konusunda ön ayak olmanız gerekecektir. Müşteri kuruluş bir uzatma talep ederse, sözleşmede belirtilen zaman içerisinde size ödeme yapılması koşuluyla buna olanak tanıyın. İşte o

zaman doğru bir şekilde uygulanan yeniden teste tabi tutma, yapılan işin en önemli kısmı olur. Unutmayın ki, ilerdeki işleriniz için en iyi kaynağınız mevcut müşteri tabanınızdır.

## 1.8 IP aralığının ve etki alanlarının belirlenmesi

Bir sızma testine başlamadan önce sızma girişiminde bulunacağınız hedeflerin neler olduğunu bilmeniz gerekir. Bu hedefler başlangıçtaki anket safhasında, müşteri kuruluştan elde edilebilir. Müşteri kuruluş tarafından hedefler, belirli IP adresleri, ağ sınırları veya etki alanları isimleri biçiminde verilebilir. Bazı durumlarda müşteri kuruluşun size verdiği tek hedef kuruluşun ismi olur ve müşteri kuruluş geri kalanını sizin kendinizin ortaya çıkarmanızı ister. Test uzmanı ile nihai hedef arasındaki güvenlik duvarları ve sisteme izinsiz girişleri tespit/engelleme sistemleri veya ağ donanımının tanımlanması da önemlidir.

### Sınırların doğrulanması

Hedeflere yönelik olarak saldırıya başlamadan önce bu hedeflerin gerçekten sızma testini gerçekleştirdiğiniz müşteri kuruluşa ait olup olmadığının teyit edilmesi zorunludur. Bir bilgisayara saldırı düzenlediniz ve başarılı bir şekilde sızma gerçekleştirdiniz. Ancak daha sonra bu bilgisayarın aslında başka bir kuruma (bir hastane veya bir kamu kurumu gibi) ait olduğunu öğrendiniz. Bu durumda karşılaşabileceğiniz hukuki sonuçları düşünün.

Hedeflerin gerçekten müşteri kuruluşa ait olup olmadığını teyit etmek için hedeflere yönelik olarak bir kimlik sorgulama işlemi gerçekleştirebilirsiniz. Hedefe yönelik olarak bir kimlik sorgulama işlemi gerçekleştirmek için Web'de mevcut olan "Internic" gibi bir kimlik sorgulama aracını kullanabilirsiniz.

## 1.9 Üçüncü taraflarla ilişkiler

Bazı durumlarda sizden üçüncü bir tarafın makinesinde bulunan bir hizmet veya uygulamanın teste tabi tutulması istenebilecektir. Bulut hizmetleri kuruluşlar tarafından daha fazla kullanıldıkça bu husus daha yaygın olarak ortaya çıkmaktadır. Burada akılda tutulması önemli olan husus, sizin test yapmak için müşteri kuruluştan aldığınız bir iznin olabileceği, ancak aynı zamanda üçüncü bir taraftan da izin almanızın gerekebileceğidir. En kötüsü, uluslararası hukuk ile sorun yaşayabilirsiniz. Bazı kuruluşlar bulut hizmetlerinden faydalandıklarını bile bilmiyor olabilirler, ya da bazı uygulamaların başka bir yerdeki ana makinede bulunduğunu unutabilirler. Test esnasında onlara bu gibi bilgileri vermeye hazır olun veya iş açıklamasına, üçüncü taraf kaynaklarının açıklanmadan kullanılmasını kapsayan bir madde koyun.

### Bulut hizmetleri

Bulut hizmetinin test edilmesinde en önemli husus tek bir fiziki ortamda birkaç farklı kuruluşun verilerinin saklanıyor olmasıdır. Çoğu zaman bu farklı verilerin etki alanları arasındaki güvenlik çok gevşektir. Bulut hizmetini sağlayan servis sağlayıcısının test konusunda uyarılması ve testin gerçekleşmekte olduğundan haberdar edilmesi ve servis sağlayıcının test uygulama kuruluşuna test yapma izni vermesi gerekir. İlave olarak, bulutun diğer müşterilerini etkileyebilecek olan bir güvenlik açıklığının tespit edilmesi durumunda doğrudan bağlantı kurulabilecek olan bir güvenlik irtibat noktası bulunması gerekir. Bazı bulut hizmeti sağlayıcılarının, sızma testi uzmanlarının takip etmesi gereken

özel prosedürleri mevcuttur ve bu prosedürler test uzmanlarından bazı formların, sızma testinin zamanının veya açık iznin testin başlamasından önce talep edilmesini gerektirebilir.

Bu, test için külfetli bir onay prosedürü gibi görünebilir, ancak aksi durumda test uzmanları için riskler çok büyüktür.

### İnternet servis sağlayıcısı

İnternet servis sağlayıcısının müşteri kuruluş ile olan hizmet kullanım şartları teyit edilmelidir. Çoğu ticari durumda İnternet servis sağlayıcısı sızma testi için özel hükümler içerir. Bu hükümlerin bir saldırı yapılmadan önce dikkatli bir şekilde gözden geçirilmesi gerekir. İnternet servis sağlayıcısının kötü niyetli olarak belirlediği belirli trafiği dışladığı ve engellediği durumlar söz konusudur. Bu gibi durumlar müşteri kuruluş için kabul edilebilir olabilir ya da olmayabilir. Her iki durumda da bu husus test öncesinde müşteri kuruluş ile açık bir şekilde konuşulmalıdır.

### Web sayfalarının barındırılması

Testin kapsamı ve zamanlamasının Web hizmeti sağlayıcısı ile açık bir şekilde konuşulması gerekir. Aynı zamanda müşteri kuruluş ile doğrudan görüşme esnasında sadece Web açıklıklarını test edeceğinizi açık bir şekilde ifade etmeniz gerekir.

### MSSP

MSSP'de test hakkında bilgilendirilmelidir. MSSP'ye ait olan sistemlerin ve servislerin test edilmesi esnasında özellikle bilgi vermeniz gerekir.

Ancak MSSP'yi bilgilendirmeyeceğiniz bazı durumlar söz konusudur. MSSP'nin yanıtlama süresini test ederken MSSP'nin bilgilendirilmesi testin faydasına olmayacaktır.

Genel bir kural olarak, açık bir şekilde MSSP'ye ait olan bir cihaz veya servis ne zaman teste tabi tutulsa, MSSP bilgilendirilmelidir.

### Sunucuların barındırıldığı ülkeler

Sunucuların barındırıldığı ülkelerin teyit edilmesi de test uzmanının faydasınadır. Ülke teyit edildikten sonra, teste başlamadan önce bu belirli ülkenin mevzuatı incelenmelidir.

Firmanızın hukuk bölümünün bu işlemi sizin için yapmasını ve onların bu işlemi tam bir şekilde yapacağını beklemeyin. Uluslararası hukukun ihlal edilmesi durumunda hiçbir koşulda firmanızın sizin eylemlerinizin sorumluluğunu almasını beklemeyin. Kanunları kendiniz inceleyin. Unutmayın ki, biri hapse girecekse, bu büyük bir olasılıkla hukuku ihlal eden test uzmanı olacaktır.

## 1.10 Kabul edilebilir sosyal mühendislik senaryolarının belirlenmesi

Çoğu kuruluş güvenlik yapılarının güncel saldırılarla aynı seviyedeki bir biçimde test edilmesini isterler. Sosyal mühendislik ve "spear-phishing" saldırıları günümüzde çoğu saldırgan tarafından yaygın olarak kullanılan saldırılardır. Çoğu başarılı saldırıda cinsellik ve uyuşturucu senaryo olarak kullanılsa da bazı

senaryolar iş ortamında kabul edilebilir değildir. Firmanız tarafından test için kullanılmak üzere seçilen senaryoların test başlamadan önce yazılı olarak onaylandığından emin olun.

## 1.11 Hizmet aksatma

İşe başlamadan önce gerilim testi veya hizmet dışı bırakma testi görüşülmelidir. Bu konu testin doğası gereği verebileceği muhtemel zarara bağlı olarak çoğu kuruluşun rahatsız olduğu konulardan biridir. Bir kuruluşun verilerinin gizliliği veya bütünlüğü hakkında tereddütleri yoksa stres testinin yapılması gerekmeyebilir. Ancak kuruluşun aynı zamanda sağladığı hizmetlerin kullanılabilirliği hakkında tereddütleri varsa stres testi üretim ortamına benzer olan ancak üretim yapılmayan bir ortamda icra edilmelidir.

## 1.12 Ödemelerle ilgili hükümler

Test için hazırlanılmasında çoğu test uzmanının unuttuğu bir diğer husus ödemelerin nasıl yapılacağıdır. Sözleşme tarihlerinde olduğu gibi belirli ödeme tarihleri ve ödemeler için de hükümler olmalıdır. Büyük bir kuruluşun test hizmetleri için size ödeme yapmayı mümkün olduğunca ertelemesi olağandışı bir durum değildir.

Aşağıda ödemelerin ne şekilde yapılabileceği ile ilgili birkaç seçenek sunulmaktadır. Bunların sadece birer seçenek olduğu unutulmamalıdır. Sizin firmanızın ve müşteri kuruluşun ihtiyaçlarına uyan bir ödeme yapısı ve planı geliştirebilirsiniz.

### Net 30

Ödeme yapılacak miktarın tamamının nihai raporun teslimini müteakip 30 gün içinde yapılması. Bu ödeme planına genellikle ilave olarak aylık bir gecikme cezası eklenir. Müşteri kuruluşa tanıyabileceğiniz süre değişebilir (45 veya 60 gün gibi).

### Ücretin yarısının önceden alınması

Test başlamadan önce ödenecek tutarın yarısının istenmesi olağandışı bir durum değildir. Bu, özellikle uzun dönemli işlerde çok yaygındır.

### Sürekli ödeme

Sürekli bir ödeme planı da olabilir. Bu daha çok uzun süreli işler içindir. Örneğin bir firmayla bir ya da iki yılı kapsayan bir sözleşme yapabilirsiniz. Müşteri kuruluşun size yıl boyunca düzenli taksitlerle ödeme yapması hiçte olağandışı bir durum değildir.

## 1.13 Sızma testinin amaçları

Her sızma testi amaç odaklı olmalıdır. Sızma testi müşteri kuruluşun işten veya görev hedeflerinden ödün vermesine yol açabilecek belirli açıklıkları belirlemek için yapılmaktadır. Test, yama yapılmamış sistemlerin belirlenmesinden ibaret değildir. Test, kuruluşu olumsuz olarak etkileyebilecek risklerin belirlenmesi ile ilgilidir.

### Temel amaçlar

Bir sızma testinin temel amacı uygunluğa bağlı olarak çıkarılmamalıdır. Bu düşüncenin birkaç farklı gerekçesi vardır. Öncelikle uygunluk güvenliğin dengi değildir. Çoğu kuruluşun uygunluk maksadıyla teste tabi tutulması anlaşılabilir bir durum olsa da uygunluk, sızma testinin esas amacı olmamalıdır. Örneğin bir PCI gerekliliğinin bir kısmını test etmek üzere bir iş alabilirsiniz. Kredi kartı bilgilerini işleme tabi tutan çok sayıda firma vardır. Ancak sizin hedef kuruluşunuzu rekabetçi bir ortamda tek ve benzersiz kılan ve hayatta kalmasını sağlayan özellikler, bu özelliklerden ödün verildiği taktirde hedef kuruluş üzerinde çok büyük bir etki yaratır. Kredi kartı bilgilerinin üçüncü tarafların eline geçmesi çok kötü olabilir. Hedef kuruluşun müşterilerinin tamamının elektronik posta adreslerinin ve kredi kartı numaralarının üçüncü tarafların eline geçmesi ise bir felaket olur.

### İkincil amaçlar

İkincil amaçlar doğrudan uygunlukla ilgili olanlardır. Genellikle bu amaçlar esas amaçlara çok sıkı bir şekilde bağlıdır. Örneğin, kredi kartlarının elde edilmesi ikincil bir amaçtır. Kuruluşun işiyle ilgili verilerin gizliliğinin ihlal edilmesinin veya kuruluşun misyonunu belirleyen prensiplerin bozulmasının denenmesi sızma testinin temel amacıdır.

### İş analizi

Sızma testini uygulamadan önce müşteri kuruluşun güvenlikle ilgili olgunluk düzeyinin belirlenmesi iyi bir fikirdir. Herhangi bir güvenlik olgunluk düzeyi belirlenmeden doğrudan sızma testine geçilmesini isteyen çok sayıda firma mevcuttur. Bu müşteri kuruluşlar için önce bir açıklık analizinin yapılması iyi bir fikirdir. Açıklık analizi çalışmasının yapılmasının kesinlikle kaçınılacak bir tarafı yoktur. Unutulmaması gerekir ki amaç, hedef kuruluşunuza yönelik olan risklerin belirlenmesidir. Bir firma, tam kapsamlı bir sızma testi için hazır değilse, büyük bir ihtimalle yapılacak olan bir açıklık analizinden sızma testine göre çok daha fazla yarar görecektir. Müşteri kuruluş ile önceden sistemler hakkında sizin neleri bilmenizi istediklerinin belirlenmesi gerekir. Bu arada müşteri kuruluştan önceden haberdar oldukları açıklıklar hakkında bilgi almak isteyebilirsiniz. Müşteri kuruluşların önceden bilgileri dahilinde olan hususların yeniden keşfedilerek raporlanmasına gerek kalmaması sizin için zamandan, müşteri kuruluş için paradan tasarruf sağlayacaktır. Uygunluk bakımından kesin bir gereklilik yoksa, tam veya kısmi bir beyaz kutu testi müşteri kuruluş için kara kutu testinden daha fazla fayda sağlayabilir.

Bir iç ağa sızma testi uygulamanız isteniyorsa (bu durumda saldırganın içerden saldırıya başladığını veya zaten orada olduğunu farz etmelisiniz) kapsam hakkında daha fazla bilgi toplamanız gerekir.

## 1.14 İletişim kanallarının tesis edilmesi

Herhangi bir sızma testinin en önemli yönlerinden birisi müşteri kuruluş ile iletişimin sağlanmasıdır. Müşteri kuruluş ile ne sıklıkla etkileşimde bulunduğunuz ve sizin müşteri kuruluşa yaklaşma biçiminiz müşteri kuruluşun tatmin olma duygusunda çok büyük bir fark yaratır. İyi bir konuşmacı olmanız gerekmez. Bu dokümanda sizi bu konuda destekleyecek ve müşteri kuruluşun test faaliyetleri ile ilgili olarak kendisini iyi hissetmesini sağlayacak bir iletişim çerçevesi tanımlanacaktır.

## 1.15 Acil durum irtibat bilgisi

Acil bir durumda müşteri kuruluşla veya hedef kuruluşla temasa geçilebilmesinin hayati olduğu açıktır. Acil durumlar beklenen veya beklenmeyen bir şekilde ortaya çıkabilir ve böyle bir durumda kiminle temasa geçeceğinizi bilmelisiniz.

Bir acil durum temas listesi oluşturun. Bu liste test kapsamındaki tüm taraflarla ilgili iletişim bilgilerini içermelidir. Acil durum temas listesi oluşturulduğunda, listede olan tüm kişilerle paylaşılmalıdır. Hedef kuruluşun müşteriniz olmayabileceğini aklınızda tutun.

Acil bir durumda ulaşılacak kişiler hakkında aşağıdaki bilgileri derleyin:

1. İsmi
2. Unvanı ve operasyonel sorumluluğu
3. Test faaliyetleri ile ilgili olarak detayların görüşülme yetkisi (önceden belirlenmemişse)
4. 7/24 hemen irtibat kurulacak iki kişinin cep telefonu, çağrı cihazı veya ev telefonu (mümkünse)
5. SFTP veya şifrelenmiş e-posta gibi güvenli bir toplu veri aktarımı biçimi

**Not:** Size yardım masası veya harekât merkezi gibi bir grubun isim ve telefon numaraları verilebilir. Bunlar acil durumda irtibat kurulacak bir kişinin yerine sadece buralarda 7/24 personel bulunduruluyorsa geçebilir.

Sızma testinin yapısı acil durumda irtibat kurulacak kişi listesinde kimlerin olması gerektiğini belirler. Sadece siz acil durumda temas bilgilerine ihtiyaç duymazsınız. Müşteri kuruluşlarda acil bir durumda sizinle irtibata geçme ihtiyacı duyabilirler. Bu liste tercihen aşağıdaki kişileri içermelidir:

1. Test için oluşturulan gruptaki tüm test uzmanları
2. Test grubunun yöneticisi
3. Her bir hedef kuruluştan iki teknik bağlantı elemanı
4. Müşteri kuruluş tarafından iki teknik bağlantı elemanı
5. Müşteri kuruluş tarafından bir üst düzey yönetici veya işle ilgili bir bağlantı elemanı

Yukarıdaki listede bazı örtüşmelerin olması mümkündür. Örneğin, hedef kuruluş aynı zamanda müşteri kuruluş olabilir. Test grubunun yöneticisi aynı zamanda testi icra ediyor olabilir. Ya da müşteri kuruluşun teknik bağlantı elemanı aynı zamanda üst düzey yönetici olabilir. Aynı zamanda teste müdahil olan her bir taraf, söz konusu taraflara liderlik eden ve onlar adına sorumluluğu üstlenen tek bir irtibat elemanını belirlemelidir.

## 1.16 Olay raporlama prosedürü

Bir işe başlamadan önce kuruluşun mevcut olaylara tepki yeteneklerinin görüşülmesi birkaç nedenden dolayı önemlidir. Sızma testi sadece kuruluşun mevcut güvenliğinin test edilmesi değildir, aynı zamanda kuruluşun olaylara tepki yeteneklerinin ne olduğunun da tespit edilmesidir. Siz sızma testine başlayıp sonuna kadar gittiğinizde, hedef kuruluş sizin orada olduğunuzun hiç farkında olmazsa, açık bir şekilde kuruluşun güvenlik yapılanmasında önemli bir boşluğu belirlemişsiniz demektir. Teste başlamadan önce, siz testi icra ederken kuruluştan birisinin farkında olup, buna bağlı olarak olay tepki timinin bir saldırıya uğradıklarını veya bilgilerinin çalındığını düşünerek gecenin bir yarısında gerekli kişileri aramaya başlamamasını da garanti altına almak isteyeceksinizdir.

### Olay tanımı

NIST'in tanımlamasına göre, "Bir bilgisayar güvenlik olayı, bilgisayar güvenlik politikalarına, kabul edilebilir kullanım politikalarına veya standart güvenlik uygulamalarına yönelik bir ihlal veya çok yakın bir ihlal tehdididir." Burada bilgisayar mantığının dışında düşünüldüğünde, herhangi birinin bir kuruluşa zorla girmesi ile de fiziki bir olay ortaya çıkar. Teste tabi tuttuğunuz kuruluş farklı tiplerdeki olaylar için farklı kategoriler ve düzeyler belirlemelidir.

### Durum raporu periyodu

Durum raporunun periyodu büyük ölçüde değişkendir. Raporlama zaman planını etkileyen faktörler testin tamamının uzunluğu, testin kapsamı, hedef kuruluşun güvenlik olgunluk derecesi vb. içerir. Müşteri kuruluşun kendisini işin içinde hissetmesine olanak tanıyacak bir zaman planı kararlaştırılmalıdır. Göz ardı edilen müşteri, artık eski bir müşteridir.

Durum raporunun periyodu ve zaman planı bir kere belirlendikten sonra buna bağlı kalınmalıdır. Bir durum raporunun ertelenmesi veya geciktirilmesi gerekli olabilir, fakat bu durum kronikleşmemelidir. Gerekli olduğunda yeni bir zaman planı için müşteri kuruluşun onayı alınmalıdır. Bir durum raporunun tamamen atlanması profesyonel bir davranış değildir ve bundan kaçınılmalıdır.

### PGP protokolü ve diğer alternatifler (Şifreleme seçenekler arasında değildir)

Müşteri kuruluş ile iletişim herhangi bir sızma testi işinin kesinlikle gerekli olan bir yönüdür ve işin hassas doğasına bağlı olarak, hassas bilgiler ve özellikle nihai rapor iletişim esnasında şifrelenmelidir.

Testlerinizi icra etmeye başlamadan önce müşteri kuruluş ile güvenli bir iletişim yolu belirleyin. Yaygın olan birkaç şifreleme yolu aşağıda sunulmaktadır:

1. PGP/GPG protokollerinin her ikisi de e-posta ile haberleşmede ve nihai raporun şifrelenmesinde kullanılır
2. Müşterinin ağında güvenli bir posta kutusu barındırılır
3. Telefon
4. Yüz yüze yapılan toplantılar
5. Nihai raporun teslimatında, raporu AES şifreli arşiv dosyasında da saklayabilirsiniz. Ancak arşiv hizmetinizin AES şifrelemesini desteklediğinden emin olmalısınız
6. Aynı zamanda hangi bilgilerin yazılı hale getirilebileceğini ve hangi bilgilerin sadece sözlü olarak iletilmesi gerektiğini sormalısınız. Siz onaylasanız da onaylamasanız da bazı kuruluşların bazı güvenlik bilgilerinin kendilerine yazılı olarak aktarılmasında sınırlama getirmeleri için çok iyi gerekçeleri vardır.

Müşteri kuruluş ile güvenli bir iletişim yolunun önceden tesis edilmesi ve aynı zamanda bu yolun müşteri kuruluşun yetenekleri dahilinde olması ve müşteri kuruluşun kendini rahat hissetmesinin sağlanması önemlidir.

## 1.17 İş kuralları

Kapsam neyi test edeceğinizi tanımlarken, iş kuralları test işleminin ne şekilde gerçekleştirileceğini tanımlamaktadır. Bunlar birbirinden bağımsız olarak ele alınması gereken iki farklı hususdur.

## Zaman çizelgesi

Test için açık bir zaman çizelgeniz olmalıdır. Kapsamda başlangıç ve bitiş zamanları tanımlanırken şimdi başlangıç ve bitiş zamanlarının arasındaki her şeyin tanımlanmasının zamanı gelmiştir. Test ilerledikçe zaman çizelgesinin değişmesi anlaşılabilir bir durumdur. Bir zaman çizelgesi yaratmaktaki amaç kesin, değişmez bir zaman çizelgesine sahip olmak değildir. Aslında bir zaman çizelgesi sizin için ve müşteri kuruluş için başlangıçta yapılması gereken işlerin açık bir şekilde belirlenmesi ve işlerden kimlerin sorumlu olacağının tespit edilmesine olanak sağlar. Genellikle yapılacak işin ve işin her bir belirli bölümünün alacağı zamanın belirlenmesinde GANTT çizelgeleri ve iş dökümü yapısı kullanılmaktadır. Zaman planının dökümünün bu şekilde görülmesi sizin için tahsis edilmesi gerekecek kaynakların belirlenmesinde ve müşteri kuruluş için test esnasında karşılaşılabilecek muhtemel engellerin belirlenmesinde yardımcı olacaktır.

İnternette kullanıma açık olan çok sayıda GANTT çizelgesi aracı mevcuttur. Sizin için en iyi olanını bulun ve bir testin yol haritasını oluştururken yoğun olarak kullanın. Bu araç, hedef kuruluşun üst yönetimi ile aranızda mükemmel bir iletişim ortamı sağlayacaktır.

## Lokasyonlar

Müşteri kuruluş ile test için nerelere seyahat etmeniz gerekeceğini görüşmeniz de önemlidir. Bu en basitinden yerel otellerin belirlenmesi, en karmaşık anlamda ise belirli bir hedef ülkenin kanunlarının belirlenmesi içindir.

Bazı durumlarda bir kuruluşun çok sayıda lokasyonu mevcuttur ve sizin birkaç örnek lokasyonu belirlemeniz gerekebilir. Bu gibi durumlarda müşteri kuruluşun tüm lokasyonlarına seyahat etmekten kaçınmaya çalışmalısınız. Çoğu zaman testte kullanmak üzere Yerel Alan Ağı bağlantıları mevcut olur.

## Hassas bilgilerin açıklanması

Amaçlarınızdan birisi hassas bilgilere erişim sağlamak olsa da, aslında bu bilgileri görmek veya indirmek istemeyebilirsiniz. Bu yeni test uzmanları için biraz tuhaf gelebilir ancak hedef bilgilerin sisteminizde bulunmasını istemeyeceğiniz çok sayıda durum vardır. Çoğu durumda test sisteminizin bir güvenlik duvarı ya da sistemde çalışmakta olan bir anti-virüs uygulaması yoktur. Bu gibi durumlar kişisel kimlik bilgilerinizi bilgisayarınızın yakınında bir yerde bulundurmayı istemeyeceğiniz durumlardır.

Bu durumda soru şuna dönüşmektedir; “Verileri elde etmeden erişim sağladığımı nasıl ispat edeceğim?” Verileri göstermeksizin erişim sağladığınızı ispat etmenin birçok yolu mevcuttur. Örneğin, bir veri tabanı şeması gösterebilirsiniz, erişim sağladığınız sistemlerin izinlerini gösterebilirsiniz veya içeriği göstermeden dosyaları gösterebilirsiniz.

Testlerinizde geçerli olmasını istediğiniz paranoya düzeyi, müşteri kuruluşla birlikte karar vermeniz gereken bir husustur. Her durumda testlerin arasında test bilgisayarınızda bulunan sonuçları temizlemek isteyeceksiniz. Bu husus aynı zamanda kullanacağınız raporlama şablonu için de geçerlidir.

Özel bir ek bilgi olarak, kanun dışı içerikle (çocuk pornosu vb.) karşılaştığınız durumlarda derhal emniyet güçlerini ve daha sonra müşteri kuruluşu belirtilen sıra dahilinde bilgilendirmelisiniz. Müşteri kuruluşu bilgilendirip ondan konuyla ilgili talimat almayınız. Bu gibi içeriğin en basit şekliyle izlenmesi dahi suç teşkil eder.

### Kanıtların kullanılması

Bir testin kanıtlarının kullanılmasında, raporun farklı aşamalarında verilere büyük bir özen gösterilmesi inanılmaz ölçüde önemlidir. Daima şifrelemeyi kullanınız ve testlerin arasında test için kullandığınız bilgisayarı temizleyiniz. Güvenlik toplantılarında içinde test raporlarının bulunduğu USB çubuklarını hiçbir şekilde başkasına teslim etmeyiniz. Ve ne yaparsanız yapın, başka bir müşterinin raporunu bir şablon olarak yeniden kullanmayınız. Bir dokümanınızda başka bir kuruluşa ait referansların bulunması hiçte profesyonelce bir davranış olmaz.

### Düzenli durum toplantıları

Test prosedürü boyunca müşteri kuruluş ile düzenli toplantılar yapılarak onların testin genel gidişatı konusunda bilgilendirilmesi kritik bir hususdur. Bu toplantılar günlük olarak düzenlenmeli ve mümkün olduğunca kısa tutulmalıdır. Genel olarak toplantılar üç basit hususu kapsar: planlar, ilerleme ve problemler.

Planlar bölümünde o gün için neyi yapmayı planladığınızı tanımlarsınız. Bunun maksadı bir değişim veya hizmet dışı kalma esnasında test icra etmeyeceğinizden emin olunmasıdır.

İlerleme bölümünde bir önceki toplantıdan beri neleri tamamladığınız hususunda bilgi vermelisiniz.

Problemler bölümünde testin genel olarak zamanlamasını etkileyecek her konu müşteri kuruluş ile görüşülmelidir. Herhangi bir durumu düzeltmek üzere belirlediğiniz belirli kişiler varsa, probleme yönelik çözümü toplantıda tartışmamalısınız.

Durum toplantılarında amaç 30 dk. veya daha az süreli bir toplantı yapmak ve geri kalan görüşmeleri sadece problemi çözmek için gerekli olan kişilerle çevrimdışı olarak yapmaktır.

### Günün hangi saatlerinde test yapılacağı

Çoğu müşteriler bakımından günün bazı saatlerinde testin icra edilmesi diğer saatlere göre daha iyidir. Maalesef bu sızma testi uzmanları için çoğu zaman gece geç saatler demektir. Testin başlamasından önce testin uygulanacağı saatlerin müşteri kuruluş ile görüşüldüğünden emin olunuz.

### Saldırılardan sakınma

Saldırılardan sakınmanın tamamen kabul edilebilir olduğu zamanlar ve saldırılardan sakınmanın testin ruhuna uygun olmadığı zamanlar vardır. Örneğin, eğer uyguladığınız test sadece teknolojinin değil ama aynı zamanda hedef kuruluşun güvenlik ekibinin yeteneklerinin teste tabi tutulduğu bir kara kutu testi ise saldırılardan sakınmak tamamen uygundur. Ancak çok sayıda sistemi hedef kuruluşun güvenlik ekibiyle koordineli olarak teste tabi tutuyorsanız saldırılardan sakınılması testin faydasına olmayacaktır.

### Test için izin

Bu doküman test yaparken alabileceğiniz muhtemelen en önemli belgedir. Bu belge testin kapsamını belgelendirir ve müşteri kuruluşun güvenlik açıklıkları bakımından teste tabi tutulacakları ve sistemlerinin üçüncü şahısların kontrolüne geçebileceği gerçeğini imza altına aldıkları belgedir. İlave olarak, bu izin belgesi açık bir şekilde testin sistemde dengesizliklere yol açabileceğini ve proses esnasında test uzmanları tarafından sistemlerin çökertilmemesi için her türlü ihtimamın gösterileceğini ifade eder. Ancak testin icrası dengesizliklere yol açabileceğinden, müşteri kuruluş test uzmanlarını herhangi bir sistem dengesizliği veya çökmesinden sorumlu tutamaz.

Bu doküman müşteri kuruluş tarafından imzalanmadan testin başlamaması çok önemlidir.

İlave olarak bazı servis sağlayıcıları kendi sistemlerinin test edilmesine başlanmadan önce bir ön bildirimde bulunulmasını ve/veya ayrı bir izin alınmasını isterler. Örneğin, Amazon'da doldurulması gereken çevrimiçi bir talep formu mevcuttur ve kendi bulutlarındaki herhangi bir makinenin taranmasından önce bu isteğin onaylanması gerekir.

### Hukuki mülahazalar

Sızma testlerinde yaygın olan bazı faaliyetler bazı yerel kanunlara aykırı olabilir. Bu nedenle yaygın olarak kullanılan sızma testi görevlerinin çalışmanın gerçekleştirileceği yerdeki hukuka uygunluğunun kontrol edilmesi tavsiye edilir. Örneğin, sızma testi esnasında İnternet üzerinden yapılan herhangi bir aramanın yakalanması bazı bölgelerde telefon dinleme olarak değerlendirilebilir.

## 1.18 Mevcut yetenekler ve teknoloji

İyi bir sızma testi sadece yama yapılmamış sistemleri aramaz. Bu testler aynı zamanda hedef kuruluşun yeteneklerini de test eder. Buradan hareketle aşağıda test esnasında nirengi noktası olarak kullanılabilecek hususların bir listesi verilmektedir:

1. Bilgi toplamanın tespit edilmesi ve buna karşılık verilmesi
2. Ayırt edici özelliklerin araştırılmasının tespit edilmesi ve buna karşılık verilmesi
3. Tarama yapılmasının ve açıklık analizi yapılmasının tespit edilmesi ve buna karşılık verilmesi
4. Sisteme sızmanın (saldırılar) tespit edilmesi ve buna karşılık verilmesi
5. Verilerin biriktirilmesinin tespit edilmesi ve buna karşılık verilmesi
6. Verilerin dışarı sızdırılmasının tespit edilmesi ve buna karşılık verilmesi

Bu bilgiler izlenirken zaman bilgisinin de alındığından da emin olunmalıdır. Örneğin, bir tarama faaliyeti tespit edilirse size bilgi verilmeli ve hangi düzeyde bir tarama gerçekleştirildiği belirtilmelidir.

# 2. Bilgi toplama

## 2.1 Genel

Bu bölümde sızma testinin bilgi toplama faaliyetleri tanımlanmaktadır. Bu dokümanın maksadı özellikle bir hedefe (tipik olarak bir firma, askeri kuruluş veya ilgili diğer kuruluşlar) yönelik olarak keşif faaliyeti gerçekleştiren sızma testi uzmanları için geliştirilmiş bir doküman sağlamaktır. Bu dokümanda düşünce aşaması ve sızma testi keşfinin amaçları detaylandırılmaktadır ve uygun bir şekilde

kullanıldığında bu doküman okuyucusuna bir hedefe saldırı icra etmek için yüksek düzeyde stratejik bir plan hazırlamasında yardımcı olur.

## 2.2 İstihbarat toplama

### Nedir?

- İstihbarat toplama, bir hedefe sızma gerçekleştirirken, açıklık değerlendirmesi ve istismar etme safhalarında faydalanmak üzere mümkün olduğu kadar çok bilgi toplamak için bir hedefe yönelik olarak keşif faaliyeti gerçekleştirmektir. Bu aşamada ne kadar çok bilgi toplayabilirseniz daha sonra o kadar çok saldırı vektörü kullanabilirsiniz.
- Açık kaynak istihbaratı kamuya açık kaynaklardan bilgilerin bulunması, seçilmesi ve elde edilmesini ve bu bilgilerin eyleme dönüştürülebilir istihbarat üretmek için analiz edilmesini içeren bir istihbarat toplama yönetim biçimidir.

### Neden yapılmaktadır?

- Açık kaynak istihbaratı toplama faaliyetini bir kuruluşun çeşitli giriş noktalarını belirlemek için gerçekleştiririz. Bu giriş noktaları fiziki noktalar, elektronik noktalar ve/veya insanlar olabilir. Çoğu firmalar kendileri hakkında hangi bilgileri herkese açtıklarını ve bu bilgilerin azimli bir saldırgan tarafından ne şekilde kullanılabileceği hususlarını gözden kaçırırlar. Bunun da ötesinde çoğu çalışanlar kendileri hakkında hangi bilgileri herkese açık hale getirdiklerini ve bu bilgilerin onlara veya işverenlerine karşı ne şekilde kullanılabileceği hususlarını göz ardı ederler.

### Ne değildir?

- Açık kaynak istihbaratı toplama faaliyetinde elde edilen bilgiler doğru ve zamanlı olmayabilir. Bilgi kaynakları kasten/kazara yanlış bilgiler yansıtmak üzere manipüle edilebilir. Zaman geçtikçe bilgiler eskimiş olabilir veya basit bir şekilde bilgiler eksik olabilir.
- Bu istihbarat faaliyetleri işe yarayacak bir şeyler bulmak amacıyla yapılan çöp karıştırmayı ya da tesis içerisinde bulunan fiziki nesnelerden firma hakkında bilgi çıkarılmasını kapsamaz.

## 2.3 Hedef seçimi

### Hedefin belirlenmesi ve adlandırılması

Bir hedef kuruluş ele alınırken, firmanın çok sayıda farklı TDL ve ikincil işlerinin olabileceğinin bilinmesi önemlidir. Bu bilgiler kapsam belirleme safhasında belirlenmiş olsa da işe başlamadan önce başlangıçta görüşülmüş olan kapsamda olmayabilen ilave sunucuların, etki alanlarının ve firmaların belirlenmesi alışılmadık bir durum değildir. Örneğin bir firmanın “.com” şeklinde bir üst düzey etki alanı olabilir. Ancak aynı firmanın “.net, .co ve .xxx” şeklinde etki alanları da olabilir. Bu etki alanları düzeltilmiş kapsamın bir kısmını oluşturabilir ya da sınırların dışında tutulabilir. Her iki durumda da testin başlamasından önce bu hususun müşteri kuruluş ile açıklığa kavuşturulması gerekir. Bir firma için firmanın altında yer alan çok sayıda alt firmanın olması da alışılmadık bir durum değildir.

### İş kurallarındaki kısıtlamaların dikkate alınması

Bu noktada iş kurallarının gözden geçirilmesi iyi bir fikir olabilir. Test esnasında bunların unutulması oldukça yaygın bir durumdur. Bazen test uzmanları olarak bulduklarımıza ve saldırı imkânlarına kendimizi kaptırıp hangi IP adreslerine, etki alanlarına ve ağlara saldırı gerçekleştirebileceğimizi unuturuz. Testinizin odaklanmasını muhafaza etmek için daima iş kurallarına başvurunuz. Bu sadece hukuksal bakımdan değil aynı zamanda test kapsamında kontrol dışı değişikler ve büyümeler olmaması bakımından da önemli bir husustur. Esas hedeflerden sapmanız sizin için zaman kaybına ve uzun dönemde firmanız için para kaybına mal olacaktır.

### Testin süresinin dikkate alınması

Testin tamamının süresi, gerçekleştirilebilecek istihbarat toplama faaliyetinin miktarını doğrudan etkiler. Bazı testlerde toplam süre iki ila üç aydır. Bir test firması bu gibi işlerde oldukça büyük bir zamanı esas iş birimlerini ve firmanın personelini araştırmak için harcar. Ancak daha kısa süreli testlerde hedefler daha taktik olabilir. Örneğin, spesifik bir Web uygulamasının teste tabi tutulmasında firmanın genel müdürünün finansal kayıtlarının araştırılmasına gerek görülmeyebilir.

### Testin nihai amacının dikkate alınması

### Bilgi toplama safhasından ne elde etmek istediğinizin belirlenmesi

### Sonuç almak için plan yapılması

## 2.4 Açık kaynak istihbaratı

Açık kaynak bilgilerinin üç biçimi vardır; pasif, yarı pasif ve aktif.

- **Pasif istihbarat toplama**: Pasif istihbarat toplama sadece, istihbarat toplama faaliyetlerinin hedef tarafından tespit edilmemesi gibi çok açık bir gereklilik varsa kullanışlıdır. Hedef kuruluşa ne kendimiz ne de kendi makinelerimizden, anonim makinelerden veya İnternet genelindeki servislerden hiçbir trafik gönderilmediğinden bu tür bir profil çıkarma işleminin teknik olarak gerçekleştirilmesi güçtür. Bu sadece arşive alınan veya saklanan bilgileri toplayabileceğimiz anlamına gelmektedir. Sadece üçüncü taraflardan toplanan sonuçlarla kısıtlandığımıza bağlı olarak bu bilgiler zamanı geçmiş veya yanlış bilgiler olabilmektedir.

- **Yarı pasif istihbarat toplama**: Yarı pasif istihbarat toplamanın amacı, normal İnternet trafiği veya normal çalışma davranışları gibi görünen yöntemlerle hedefin profilinin çıkarılmasıdır. Bilgi için sadece açıklanmış olan sunucuları sorgularız, derinlikli tersine aramalar gerçekleştirmeyiz veya brute force DNS isteklerinde bulunmayız, açıklanmamış sunucularda veya dizinlerde arama yapmayız. Ağ düzeyinde port taraması yapmayız veya gezginleri çalıştıramayız ve sadece yayınlanmış dokümanlar ve dosyalardaki meta verilere bakarız. Aktif olarak gizlenmiş içerik araştırmayız. Burada anahtar husus faaliyetlerimizin dikkat çekmemesidir. İşlem sonrasında hedef geriye dönük olarak keşif faaliyetlerini tespit edebilir fakat bu faaliyeti kimseye isnat edemez.

- **Aktif istihbarat toplama**: Aktif istihbarat toplama, şüpheli ve kötü niyetli davranışlar hedef tarafından tespit edilmelidir. Bu aşamada aktif olarak ağ yapısını çıkarırız, aktif bir şekilde açık

servisleri listeleriz ve/veya açıklık analizi taraması yaparız. Açıklanmamış dizinlerde, dosyalarda ve sunucularda aktif olarak arama yaparız. Bu faaliyetlerin çoğu standart sızma testinin tipik keşif veya tarama faaliyetleridir.

### Firma

### Fiziki bilgiler

### Lokasyonlar

Her bir lokasyonun için açık adres, mülkiyet, ilgili diğer bilgilerin (şehir, vergi, hukuki vb.) listelenmesi. Lokasyondaki tüm fiziki güvenlik tedbirlerinin (kamera yerleri, sensörler, tel örgüler, devriyeler, giriş kontrolü, kapılar, kimlik türü, tedarikçi girişi, IP bloklarına/konum belirleme servislerine dayalı fiziki lokasyonlar vb.) listelenmesi.

- Sahibi
- Arazi/vergi kayıtları
- Paylaşımlı/müstakil
- Saat dilimleri
- Makineler/Ağ operasyon merkezi

### Firmanın yayılması

Bir hedef kuruluş için çok sayıda birbirinden ayrı fiziki lokasyonun bulunması alışılmadık bir durum değildir. Örneğin bir bankanın merkez ofisleri vardır ancak aynı zamanda çok sayıda uzak şubeleri de bulunmaktadır. Merkez lokasyonlarda fiziki ve teknik güvenlik çok iyi olabilirken, uzak lokasyonların güvenlik denetimleri çoğunlukla zayıftır.

### İlişkiler

İş ortakları, gümrükçüler, tedarikçiler, firmanın Web sayfasında açık olarak paylaşılanlar yoluyla analiz edilenler, kiralama firmaları vb. Bu bilgiler işle ilgili veya kurumsal projelerin daha iyi anlaşılmasında kullanılabilir. Örneğin, hedef kuruluş için hangi ürünlerin ve hizmetlerin kritik olduğu gibi.

Bu bilgiler aynı zamanda başarılı sosyal mühendislik senaryolarının yaratılmasında da kullanılabilir.

- İlişkiler
- Paylaşılan ofis alanları
- Paylaşılan altyapı
- Kiralanmış/finansal olarak kiralanmış teçhizat

### Mantıksal bağ kurma

Ortaklar, müşteriler ve rakipler hakkında toplanan bilgiler: Her biri için ticari unvanı, iş adresi, ilişki türü, temel finansal bilgiler, ana makineleri/ağ bilgisinden oluşan tam bir liste.

### İş ortakları

- Hedefin ilan edilmiş iş ortakları. Bazen esas İnternet sitesinde ilan edilir.

### İş müşterileri

- Hedefin ilan edilmiş müşterileri. Bazen esas İnternet sitesinde ilan edilir.

### Rakipler

- Hedefin rakipleri kimlerdir? Bunun tespiti basit olabilir veya ileri bir analiz gerektirebilir.

### İrtibat çizelgesi

- İrtibat çizelgesi (insanlar arasındaki sosyal bağların görsel bir sunumu) kuruluş içerisindeki kişilerin potansiyel etkileşimlerini ortaya çıkarmada ve bu kişilere dışarıdan (irtibat çizelgesi dış toplulukları içerdiğinde ve iki seviyeden daha yukarıda bir derinlikte oluşturulduğunda) nasıl erişim sağlanabileceğinin belirlenmesinde size yardımcı olur.
- Temel irtibat çizelgesi o ana kadar derlenmiş olan bilgilerden çıkarılan kurumsal yapıyı yansıtmalıdır ve ilave olarak çizelgede yapılacak müteakip genişlemeler de bu bilgilere dayalı olmalıdır (irtibat çizelgesi genellikle kurumsal olarak odaklanılan varlıkları daha iyi gösterdiğinden ve muhtemel yaklaşma vektörlerini açığa çıkardığından).

### Hoovers profili

- **Nedir?** Yarı kullanıma açık bir istihbarat kaynağıdır (genellikle ödemeli abonelik ile). Bu gibi kaynaklar firmalar hakkında işle ilgili bilgilerin toplanması konusunda ve iş hakkında normalize edilmiş bir bakış açısı sağlamada uzmanlaşmışlardır.
- **Neden kullanılır?** Bilgiler fiziki lokasyonları, rekabet ortamını, anahtar personeli, finansal bilgileri ve işle ilgili diğer bilgileri içerir (kaynağa bağlı olarak).
- **Nasıl kullanılır?** Web sitesinde ticari unvan kullanılarak yapılacak bir arama firmanın tam bir profilini ve firma hakkında mevcut olan tüm bilgileri çıkarır. Bilgilerin birkaç kaynak kullanmak suretiyle çapraz olarak sorgulamasının yapılması ve en güncel bilgilerin elde edildiğinden emin olunması önerilir.

### Üretim hattı

- Hedef kuruluşun sunduğu ürünler ve kuruluş hizmet üretiyorsa bu hizmetler hakkında ilave bir analiz yapılması gerekebilir.

### Dikey pazar

- Hedef kuruluşun hangi endüstri kolunda faaliyet gösterdiği (finans, savunma, tarım, kamu vb.)

### Pazarlama hesapları

- Pazarlama faaliyetleri hedefin pazarlama stratejileri hakkında zengin bilgiler sağlar.
- Hedef kuruluşun sosyal bağlantılarını belirlemek için tüm sosyal medya ağları incelenmelidir.

- Hedef kuruluşun geçmişteki pazarlama kampanyaları incelenmelidir.

### Toplantılar

- Toplantı tutanakları yayınlanıyor mu?
- Toplantılara halka açık mı?

### Firma için önemli tarihler

- Yönetim kurulu toplantıları
- Tatiller
- Yıldönümleri
- Ürün/hizmet başlangıçları

### İş olanakları

- Bir kuruluşun iş olanakları listelerini (genellikle kuruluşun Web sitesinin kariyer bölümünde bulunurlar) incelemek suretiyle kuruluş içerisinde ne tür teknolojilerin kullanılmakta olduğunu belirleyebilirsiniz. Örneğin bir kuruluşta "Solaris Sysadmin" gibi bir iş olanağı olması, kuruluşun "Solaris systems" kullandığını çok açık bir şekilde gösterir.

### Hayır kurumları ile bağlar

- Bir hedef kuruluşun yöneticilerinin hayır kurumları ile ilişkilerinin bulunması çok yaygın olarak görülür. Bu bilgiler yöneticiler hedeflendiğinde sağlam sosyal mühendislik senaryolarının yaratılması için kullanılabilir.

### Teklif/Fiyat teklifi alma ve diğer kamu ihale bilgileri

- Teklif/Fiyat teklifi alma faaliyetleri firma tarafından kullanılan sistemlerin tipleri hakkında ve altyapılarındaki potansiyel eksikler hakkında çok miktarda bilgi gösterir.

- İhaleleri kazananların kimler olduğunun belirlenmesi kullanılmakta olan sistemlerin tiplerini veya firma kaynaklarının kuruluşun dışında bulundurulduğu bir lokasyonu gösterebilir.

### Mahkeme kayıtları

- Mahkeme kayıtları genellikle ya serbestçe kullanılabilir durumdadır ya da bir ücret karşılığı alınabilir.
- Eski çalışanların açtığı davaları içeren ancak bunlarla sınırlı olmayan davaların içeriği firmadan şikayetçi olanlar hakkında bilgiler verebilir.
- Mevcut ve eski çalışanlar hakkındaki sabıka kayıtları sosyal mühendislik gayretleri için bir dizi hedef sağlayabilir.

## Bağışlar

- Bağışlar ve diğer finansal katkıların belirlenmesi güçlü bir pozisyonda olmayabilen ancak firmanın mevcut bir çıkarı bulunan önemli kişilerin belirlenmesi bakımından önemlidir.
- Bağışların çıkarılması ülkeden ülkeye bilgi edinme özgürlüğüne bağlı olarak değişir fakat çoğu durumda başka ülkelerden yapılan yardımlar mevcut veriler kullanılmak suretiyle geriye doğru takip edilebilir.

## Mesleki lisanslar ve tesciller

Hedef kuruluşunuzun mesleki lisanslarının ve tescillerinin elde edilmesi sadece firmanın nasıl çalıştığı hakkında değil aynı zamanda bu lisansları muhafaza etmek için takip ettikleri kılavuzlar ve düzenlemeler hakkında da bir bakış sağlar. Buna iyi bir örnek olarak, bir firmanın ISO Standardları sertifikası firmanın belli kılavuzları ve prosesleri takip ettiğini gösterir. Test uzmanı açısından bu proseslerin ve bu proseslerin kuruluşta gerçekleştirilmekte olan testlere nasıl bir etkisi olacağının farkında olunması önemlidir.

Bir firma genellikle bu gibi detayları Web sayfalarına bir onur işareti olarak koyar. Aksi durumda dikey bir pazarda, kuruluşun bu pazarın bir üyesi olup olmadığının anlaşılması için tescillerin araştırılması gerekebilir. Kullanılabilir olan bilgiler büyük ölçüde dikey pazara ve aynı zamanda firmanın coğrafi konumuna bağlıdır. Uluslararası firmaların farklı bir şekilde lisanslandırılmış olabileceğine ve ülkeye bağlı olarak farklı standardlarla veya yasal organlarla tescil edilmelerinin gerekebileceğine de dikkat edilmelidir.

## Firmanın organizasyon şeması

### Görev tanımları

- Kuruluştaki önemli kişiler
- Özellikle hedeflenecek kişiler

### İşlemler

### İştirakler

## Elektronik

## Doküman meta verileri

- **Nedir?** Meta veri bir verinin/dokümanın kapsamı hakkında bilgi verir. Yazarı/oluşturanın ismi, tarih ve saat, kullanılan/başvurulan standardlar, bir bilgisayar ağındaki yeri (yazıcı/dosya/dizin/yol vb. bilgiler), coğrafi etiket vb. gibi bilgileri içerebilir. Bir resim için meta veri renk, derinlik, çözünürlük, kameranın yapısı/türü ve hatta koordinat ve konum bilgilerini içerebilir.
- **Meta veri niçin kullanılır?** Meta veri önemlidir çünkü iç ağ, kullanıcı isimleri, e-posta adresleri, yazıcıların konumları vb. bilgileri içerir ve lokasyonun bir planının çıkarılmasına yardımcı olur. Meta veri aynı zamanda ilgili dokümanların yaratılmasında kullanılan yazılım hakkında bilgileri de içerir. Bu, saldırıyı gerçekleştirenin bir profil yaratmasını ve/veya ağlar ve kullanıcılar hakkındaki dahili bilgilerle özel amaçlı saldırılar icra etmesini mümkün kılar.
- **Nasıl elde edilir?** Dosyadan (pdf/word/resim) meta verileri çıkaran “FOCA (GUI-tabanlı)”, “metagoofil (python- tabanlı)”, “meta-extractor”, “exiftool (perl-tabanlı)” gibi araçlar mevcuttur. Bu araçların meta verileri çıkarma ve sonuçları “HTML, XML, GUI, JSON” vb. gibi formatlarda sunma

yetenekleri vardır. Bu araçlarda kullanılacak olan girdiler çoğu zaman müşterilerin kamuya açık varlıklarından indirilen ve daha sonra hakkında daha fazla bilgi edinmek için analiz edilen bir belgedir. Belgeleri aramanıza, indirmenize ve analiz etmenize yardımcı olan “FOCA” olsa da tüm bunlar “FOCA”nın “GUI” arayüzü aracılığıyla gerçekleştirilir.

### Pazarlama iletişimleri

- Geçmiş pazarlama kampanyaları yürürlükten kalkmış olabilen ancak halen erişilebilir olan projeler hakkında bilgi sağlar.
- Güncel pazarlama iletişimleri, çoğu dahili olarak kullanılan tasarım bileşenlerini de (renkler, fontlar, grafikler vb.) içerir.
- Dış pazarlama kuruluşları gibi ilave iletişim bilgileri.

### Altyapı varlıkları

### Sahip olunan ağ blokları

- Kuruluş tarafından sahip olunan ağ blokları “WHOIS” aramaları gerçekleştirmek suretiyle pasif olarak elde edilebilir. “DNSStuff.com” bu gibi bilgilerin doğrudan elde edilebileceği bir yerdir.
- IP adreslerine yönelik olarak gerçekleştirilen aramalar hedefteki altyapının tipi hakkında bilgiler verebilir. Yöneticiler genellikle IP adresi bilgilerini çeşitli destek sitelerindeki yardım istekleri bağlamında gönderirler.

### E-posta adresleri

- E-posta adresleri geçerli kullanıcı adlarının ve etki alanı yapısının potansiyel bir listesini sağlar.
- E-posta adresleri kuruluşun Web sitesi de dahil olmak üzere birçok kaynaktan toplanabilir.

### Dış altyapı profili

- Hedefin dış altyapı profili dahili olarak kullanılan teknoloji hakkında geniş bilgi sağlayabilir.
- Bu bilgiler çeşitli kaynaklardan pasif ya da aktif bir şekilde toplanabilir.
- Profil, dış altyapıya yönelik olarak bir saldırı senaryosunun oluşturulmasında kullanılmalıdır.

### Kullanılan teknolojiler

- Destek forumları, posta listeleri ve diğer kaynaklarda yapılan açık kaynak istihbarat aramalarıyla hedefte kullanılan teknolojiler hakkında bilgi toplanabilir.
- Belirlenen bilgi teknolojileri kuruluşuna karşı sosyal mühendislik kullanılmalıdır.
- Ürün satıcılarına karşı sosyal mühendislik kullanılmalıdır.

### Satın alma anlaşmaları

- Satın alma anlaşmaları donanım, yazılım, lisanslar ve hedefte mevcut olan ilave fiziki varlıklar hakkında bilgi içerir.

### Uzaktan erişim

- Çalışanların ve/veya müşterilerin uzaktan erişim için hedef kuruluşa nasıl bağlı olduğu hakkında bilgi elde edilmesi potansiyel bir giriş noktası sağlar.
- Çoğu zaman uzaktan erişim portalına bağlantı hedef kuruluşun ana sayfasında bulunur.
- Nasıl yapılır (How To) dokümanları, uzaktaki kullanıcılara uygulamaları/prosedürleri gösterir.

### Uygulama kullanımı

Hedef kuruluş tarafından kullanılan bilinen uygulamaların bir listesini oluşturun. Bu, genellikle herkesin erişimine açık olan dosyalardan meta verilerin çıkarılması ile yapılabilir (önceden bahsedildiği gibi).

### Savunma teknolojileri

Kullanımda olan savunmaya yönelik teknolojilerin ayırt edici özelliklerinin belirlenmesi, kullanımda olan savunma sistemlerine bağlı olarak birkaç yolla yapılabilir.

### Pasif bir şekilde ayırt edici özelliklerinin belirlenmesi

- Hedef kuruluşun teknisyenlerinin bazı konuları tartışmaları veya kullanımda olan teknolojilerle ilgili yardım istemeleri muhtemel olan forumlarda ve kamuya açık olarak erişilebilir olan bilgilerde arama yapın.
- Hedef kuruluşa ve aynı zamanda popüler teknoloji satıcılarına yönelik pazarlama bilgilerini araştırın.
- “Tin-eye” programını (veya başka bir resim eşleme aracını) kullanarak hedef kuruluşun logosunun satıcıların referans sayfalarında veya diğer pazarlama materyalinde bulunup bulunmadığına yönelik olarak bir arama yapın.

### Aktif bir şekilde ayırt edici özelliklerinin belirlenmesi

- Hedefin halka yönelik sistemlere engellenen örüntüleri test etmek için uygun sorgulama paketleri gönderin. Belirli Web uygulaması güvenlik duvarı tiplerinin ayırt edici özelliklerini belirlemek için birkaç araç mevcuttur.
- Hem hedef kuruluşun Web sitesinden gelen yanıtların, hem de e-postaların üst bilgileri genellikle hem kullanılmakta olan sistem hakkında hem de devreye alınmış olan özel güvenlik mekanizmaları hakkında bilgiler verir.

### İnsan kaynaklarının yetenekleri

Hedef bir kuruluşun insan kaynaklarının savunmaya yönelik yeteneklerinin tespit edilmesi güçtür. Hedef kuruluşun güvenliğinin sorgulanmasında yardımcı olabilecek birkaç anahtar bilgi mevcuttur.

- Firma genelinde SOME timlerinin bulunup bulunmadığını kontrol edin.
- Güvenlikle ilgili bir pozisyon için ne sıklıkla personel arandığını görmek için iş ilanlarını kontrol edin.
- Güvenlikle ilgili olmayan işlerde (örneğin, geliştiriciler) güvenliğin bir gereklilik olarak belirtilip belirtilmediğini görmek için iş ilanlarını kontrol edin.

- Hedef kuruluşun güvenliğinin kısmen veya tamamen dış kaynaklardan karşılanıp karşılanmadığını görmek için dış kaynak kullanım anlaşmalarını kontrol edin.
- Firma için çalışmakta olan, güvenlik çalışanlarının arasında olması muhtemel belirli kişileri araştırın.

### Finansal hususlar

### Raporlama

Hedef kuruluşun finansal raporları büyük ölçüde kuruluşun lokasyonuna bağlıdır. Raporlama her bir münferit şube tarafından değil de kuruluşun genel merkezi aracılığıyla yapılıyor olabilir.

### Pazar analizi

### Ticari sermaye

### Hedef kuruluşun tarihsel olarak finansal değeri

### Kişiler

### Çalışanlar

### Tarihsel bilgiler

- **Mahkeme kayıtları**
  - **Nedir?** Mahkeme kayıtları ilgilenilen bir kişi ya da kuruluşun lehine veya aleyhine olarak, suçlarla ve/veya şikâyetlerle, davalarla veya diğer hukuki işlemlerle ilgili kamusal kayıtlardır.
  - **Niçin araştırılır?** Mahkeme kayıtları potansiyel olarak münferit bir çalışanla ya da tüm firmayla ilgili hassas bilgiler gösterebilirler. Bu bilgilerin kendisi faydalı olabilir veya ilave bilgi elde etmek için bir araç teşkil edebilirler. Bu bilgiler sızma testinin sonraki aşamalarında sosyal mühendislik veya başka maksatlarla da kullanılabilirler.
  - **Nasıl elde edilir?** Bu bilgilerin çoğu İnternette herkese açık mahkeme Web siteleri ve kayıt veri tabanları aracılığıyla elde edilebilir. Bazı ilave bilgiler “LEXIS/NEXIS” gibi ücretli servisler aracılığıyla elde edilebilir. Bazı bilgiler kayıtların talep edilmesiyle veya şahsi müracaatla elde edilebilir.

- **Bağışlar**
  - **Nedir?** Bağışlar bir kişinin kendine ait parasını belirli bir siyasi adaya, siyasi partilere veya özel bir ilgi sahasındaki kuruluşlara yönlendirmesidir.
  - **Niçin araştırılır?** Bağışlar potansiyel olarak bir kişi hakkında faydalı bilgiler sunabilir. Bu bilgiler söz konusu kişilerle politikacılar, siyasi adaylar ve siyasi kuruluşlar arasındaki bağlantıları ortaya çıkarmada yardımcı olmak üzere sosyal ağ analizinin bir parçası olarak kullanılabilir. Bu bilgiler aynı zamanda sızma testinin ileriki aşamalarında sosyal mühendislik veya diğer maksatlarla da kullanılabilir.

- **Nasıl elde edilir?** Bu bilgilerin çoğu günümüzde İnternette kişi bazında siyasi bağışları takip eden halka açık Web siteleri (örneğin, http://www.opensecrets.org/) aracılığıyla elde edilebilmektedir.

- **Mesleki lisanslar ve tesciller**
  - **Nedir?** Mesleki lisanslar veya tesciller belirli bir lisans hakkı kazanmış olan veya bir topluluğun belirli bir düzeyde mensubu olan kişiler hakkında üye listelerini ve diğer ilgili bilgileri içeren bilgi depolarıdır.
  - **Niçin araştırılır?** Ticari lisanslar potansiyel olarak bir kişi hakkında faydalı bilgiler gösterebilir. Bu bilgiler bir kişinin güvenilirliğini teyit etmek için (gerçekten iddia ettikleri gibi belirli bir sertifikaya sahip midirler?) veya kişilerle başka kuruluşlar arasındaki bağlantıları ortaya çıkarmada yardımcı olmak üzere sosyal ağ analizinin bir parçası olarak kullanılabilir. Bu bilgiler aynı zamanda sızma testinin sonraki aşamalarında sosyal mühendislik veya diğer maksatlarla da kullanılabilir.
  - **Nasıl elde edilir?** Bu bilgilerin çoğu günümüzde İnternette halka açık Web siteleri aracılığıyla elde edilebilmektedir. Tipik olarak her kuruluş kendi tescil bilgilerini çevrimiçi olarak elde edilebilir şekilde muhafaza etmektedir ya da belki de bu bilgilerin toplanması için ilave bazı adımlar atmak gerekebilir.

**Sosyal ağ profili**

- **Meta verilerden sızdırılan bilgiler**
  - Fotoğraf meta verileri aracılığıyla lokasyonun bilinmesi
- **İletişim tonu**
  - İletişimde kullanılan tonun öznel olarak belirlenmesi – saldırgan, pasif, sempatik, övücü, aşağılayıcı, küçümseyen, kibirli, seçkinci, mazlum, lider, destekçi, taklit edici vb.
- **Yayınların periyodu**
  - Yayınların periyodunun belirlenmesi (saatte/günde/haftada bir vb.). İlave olarak iletişimin günün hangi saatinde, haftanın hangi gününde olmasına yönelik bir meyil olduğu.
- **Lokasyon tespiti**
  - Bing Map Apps
  - Foursquare
  - Google Latitude
  - Yelp
  - Gowalla

- **Hedefin sosyal medyadaki mevcudiyeti**

- Hangi siteleri kullanıyorlar?

### Hedefin İnternetteki mevcudiyeti

- **E-posta adresi**
  - **Nedir?** E-posta adresleri kullanıcıların genel posta kutusu kimlikleridir.
  - **Niçin araştırılır?** E-posta adreslerinin toplanması veya araştırılması önemlidir çünkü birçok maksatla kullanılırlar. E-posta adresleri daha sonra erişim için bir brute force saldırısına tabi tutulabilecek muhtemel bir kullanıcı kimliği sağlar ama daha da önemlisi özel amaçlı istenmeyen e-postaların gönderilmesine yarar. Bu istenmeyen e-postalar istismar öğeleri, zararlı kodlar vb. içerebilir ve bir kullanıcıya özel spesifik bir içerikten bahsedebilir.
  - **Nasıl elde edilir?** E-posta adresleri çeşitli Web sitelerinde, gruplarda, bloglarda, forumlarda, sosyal medya portallarında vb. aranabilir ve çıkartılabilir. Bu e-posta adresleri çeşitli teknik destek Web sitelerinden de elde edilebilir. Bir etki alanı ile eşleşen e-posta adreslerine yönelik olarak arama yapan e-posta toplama araçları da mevcuttur (ihtiyaç duyulduğu taktirde).

- **Kişisel tanıtıcılar/takma adlar**
- **Kayıtlı kişisel etki alanı adları**
- **Atanmış statik IPler/ağ bölümü (IP aralığı)**

### Fiziki lokasyon

- Hedefin fiziki lokasyonunu elde edebilirsiniz

### Telefon bilgi taraması

- Telefon numarası
- Cihazı türü
- Kullanım
- Kurulmuş uygulamalar
- Telefonun sahibi/yöneticisi

### Ödeme karşılığı elde edilecek bilgiler

- Geçmiş sorgulaması
- Linked-In
- LEXIS/NEXIS

## 2.5 Örtülü bilgi toplama

### Firmanın yerinde bilgi toplama

Fiziki güvenlik denetlemeleri

Kablosuz ağ taraması / Radyo frekans taraması

Çalışan davranışları eğitimlerinin denetlenmesi

Girilebilir / Komşu tesisler (ortak alanlar)

Bir şeyler bulmak amacıyla yapılan çöp karıştırması

Kullanılan teçhizat tipleri

### Dışarıdan bilgi toplama

Veri merkezi lokasyonları

Ağ hizmeti sağlama/sağlayıcısı

### İnsanlar hakkında bilgi toplama

İnsan hakkında bilgi toplama başka bir yolla elde edilemeyecek bilgiler sağladığından hedef varlık hakkında daha pasif bir anlayışla yapılan bilgi toplamayı bütünler ve aynı zamanda istihbarat resmine daha kişisel (duygular, tarih, anahtar kişiler arasındaki ilişkiler, atmosfer vb.) yönler ekler.

İnsan istihbaratının elde edilmesi metodolojisi daima fiziki ya da sözlü olarak doğrudan teması içerir. Bilgi toplama faaliyeti optimal ölçüde bilginin açığa çıkması ve sorgulama esnasında hedef varlığın işbirliğinin sağlanmasına yönelik olarak özel bir takma kimlikle yapılmalıdır.

İlave olarak, daha hassas hedeflerden istihbarat toplanması, fiziksel olarak yerinden ya da elektronik/uzaktan erişim araçları (kapalı devre kamera sistemleri, Web kameraları vb.) kullanmak suretiyle gözlemden faydalanmak suretiyle gerçekleştirilebilir. Bu gözlemler genellikle davranışsal paternleri (ziyaret sıklıkları, kıyafet zorunluluğu, erişim yolları, kafeler gibi ilave erişim sağlayabilecek anahtar lokasyonlar gibi) ortaya çıkarmak maksadıyla gerçekleştirilir.

### Sonuçlar

Anahtar çalışanlar

Ortaklar/Tedarikçiler

Sosyal mühendislik

## 2.6 Bilgi tarama

**NEDİR?** Dışarıdan bilgi toplama, bilgi toplamanın “footprinting” olarak ta adlandırılan, bilgi edinmek maksadıyla kuruluşun dışından bir bakış açısıyla hedefle yapılan etkileşimleri içeren bir safhasıdır.

**NEDEN YAPILIR?** Çoğu bilgiler hedeflerle etkileşme girilerek toplanabilir. Bir servisi ya da cihazı sorgulamak suretiyle genellikle bu servis ya da cihazın ayırt edici özelliklerini tespit edebileceğiniz senaryolar yaratabilirsiniz. Hatta daha basit olarak cihazı tanımlayacak bir “banner” satın alabilirsiniz. Bu adımda hedefleriniz hakkında daha çok bilgi toplamanız gerekmektedir. Bu aşamanın sonunda amacınız önceliklendirilmiş bir hedef listesi elde etmektir.

## Dış bilgi tarama

### Müşteri kuruluşun dış sınırlarının belirlenmesi

Bir sızma testi esnasında istihbarat toplamanın temel amaçlarından biri kapsam dahilinde olacak makinelerin belirlenmesidir. Hedefin etki alanlarındaki ve sınırlarının içerisindeki sistemlerin belirlenmesinde ters DNS aramaları, DNS "brute force" saldırıları, "WHOIS" aramaları gibi kullanılabilecek çok sayıda teknik mevcuttur. Belirtilen bu teknikler ve diğerleri aşağıda açıklanmaktadır.

## Pasif keşif

### "WHOIS" aramaları

Dış bilgi tarama için öncelikle peşinde olduğumuz bilginin hangi "WHOIS" sunucularında içerildiğinin belirlenmesine ihtiyaç vardır. Buradan hareketle hedefin etki alanının en üst düzey etki alanını bilmemiz, daha basit olarak hedefin etki alanının kayıtlı olduğu kayıt yetkilisinin konumunu belirlememiz gerekmektedir.

"WHOIS" bilgisi ağaç şeklinde bir hiyerarşiye dayanır. ICANN tüm en üst düzey etki alanları için kayıt yetkilisidir ve tüm manuel "WHOIS" sorgulamaları için önemli bir başlangıç noktasıdır.

### "WHOIS" araması

- ICANN - http://www.icann.org
- IANA - http://www.iana.com
- NRO - http://www.nro.net
- AFRINIC - http://www.afrinic.net
- APNIC - http://www.apnic.net
- ARIN - http://ws.arin.net
- LACNIC - http://www.lacnic.net
- RIPE - http://www.ripe.net

Kayıt yetkilisi sorgulandığında etki alanı kayıt bilgisini elde edebiliriz. "WHOIS" bilgilerini veren çok sayıda İnternet sitesi mevcuttur. Ancak belgelendirmede kesinliğin sağlanması maksadıyla sadece uygun kayıt yetkilisinin kullanılması gerekir.

- InterNIC - http://www.internic.net/ http://www.internic.net]

ARIN'da (American Registry for Internet Numbers – Amerikan İnternet numaraları kayıt defteri) yapılacak basit bir "WHOIS" araması doğru kayıt yetkilisini verecektir.

## BGP aynaları

BGP'ye dâhil olan ağların otonom sistem numarasının belirlenmesi mümkündür. BGP yolları dünya genelinde ilan edilmiştir ve BGP4 ve BGP6 aynaları kullanılmak suretiyle bunlar tespit edilebilir.

- BGP4 - http://www.bgp4.as/looking-glasses
- BPG6 - http://lg.he.net/

## Aktif bilgi tarama

### Port taraması

Port taraması teknikleri, test için elde mevcut olan zamana ve testin gizli olarak icra edilmesi gerekliliğine bağlı olarak değişir. Sistemler hakkında hiçbir bilgi yoksa, sistemlerin belirlenmesinde hızlı bir "ping" taraması kullanılabilir. İlave olarak kullanılabilir durumda olan yaygın olarak kullanılan portların tespit edilmesi için "ping" doğrulamasız, hızlı bir tarama çalıştırılmalıdır. Bundan sonra daha kapsamlı bir tarama çalıştırılabilir. Bazı test uzmanları sadece açık TCP portları ve aynı zamanda UDP portlarına bakarlar.

"http://nmap.org/nmap_doc.html" adresindeki doküman, port taraması tiplerini detaylı olarak açıklamaktadır. "Nmap", ağ denetimi/taraması için fiili olarak geçerli olan standarttır. "Nmap" hem Linux hem de Windows işletim programlarında çalışır.

Nmap'in kullanılması hakkında detaylı bilgiyi "Sızma Testi Teknik Kılavuzunda" (http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines#Nmap_.28Windows.2FLinux.29) bulabilirsiniz.

"Nmap"te düzinelerce seçenek bulunmaktadır. Bu bölüm port taraması ile ilgili olduğundan bu bölümde bu görevin yerine getirilmesi için gerekli olan komutlara odaklanılacaktır. Kullanılan komutların esas olarak eldeki zamana ve taramaya tabi tutulan portların sayısına bağlı olacağının bilinmesi önemlidir. Bu görevlerin yerine getirileceği ne kadar çok port varsa veya elde ne kadar az zaman varsa, makineyi o kadar daha az bir süre araştırabiliriz. Mevcut seçeneklerden bahsedildikçe bu husus daha açık hale gelecektir.

### "Banner Grabbing"

"Banner Grabbing" uygulaması bir ağa bağlı bilgisayar sistemleri ve bu bilgisayarların açık portlarında çalışmakta olan servisler hakkında bilgi toplamak için kullanılan bir listeleme tekniğidir. "Banner Grabbing" ağdaki uygulamaların sürümlerini ve hedef makinenin çalıştığı işletim sistemini belirlemek için kullanılır.

"Banner Grabbing" genellikle HTTP, FTP ve SMTP protokollerinin, sırasıyla 80, 21, ve 25 portlarında gerçekleştirilir. "Banner Grabbing" uygulanmasında yaygın olarak kullanılan araçlar "Telnet", "nmap" ve "Netcat"tir.

### "SNMP Sweeps"

"SNMP sweeps" belirli bir sistem hakkında çok fazla bilgi sağladığı için uygulanır. SNMP protokolü durum bilgisi kullanmaz ve datagram uyumlu bir protokoldür. Ancak SNMP sunucuları geçersiz dizilerle yapılan sorgulara cevap vermez ve kullandığı UDP protokolü, kapalı UDP portlarını eksiksiz bir şekilde raporlamaz. Bu nedenle sorgu gönderilen bir IP adresinden cevap alınamaması, aşağıdaki hususlardan biri nedeniyle olabilir:

- Makine erişilebilir değildir
- SNMP sunucusu çalışmamaktadır
- Hatalı bir sorgu dizisi gönderilmiştir
- Cevap datagramı henüz ulaşmamıştır

### Alan transferleri

DNS alan transferi, ya da bilinen diğer adıyla AXFR bir tür DNS işlemidir. DNS alan transferi bir dizi DNS sunucusu üzerindeki DNS verilerini içeren veri tabanlarının kopyasının çıkarılması için geliştirilmiş olan bir mekanizmadır. Alan transferleri iki çeşittir: tam alan transferi (AXFR) ve artan alan transferi (IXFR). DNS alan transferi gerçekleştirme yeteneğinin test edilmesinde kullanılabilecek olan çok sayıda araç mevcuttur. Alan transferlerinin gerçekleştirilmesinde yaygın olarak kullanılan araçlar "host", "dig" ve "nmap"tir.

### SMTP Bounce Back

Aynı zamanda, teslim edilmedi raporu/alındısı (NDR), (başarısız) ileti durum raporu (DSN) iletisi, iletilmedi bildirimi (NDN) veya basitçe "bounce" olarak ta adlandırılan "SMTP bounce back", bir e-posta sisteminden gelen bir iletinin göndericisini, iletisinin adresine teslim edilmesi ile ilgili bir problem yaşandığına dair bilgilendiren, otomatik olarak yaratılan bir elektronik iletidir. Bir "bounce" iletisi, yazılım ve sürümler dahil olmak üzere kullanılan SMTP sunucusu hakkında bilgi içeriyor olabileceğinden, bir saldırgan için SMTP sunucusunun ayırt edici özelliklerinin tespit edilmesinde yardımcı olabilir.

Bu basit bir şekilde hedefin etki alanı içerisinde sahte bir adres yaratmak suretiyle gerçekleştirilebilir. Örneğin, "asDFADSF_garbage_address@target.com", "target.com"u test etmek üzere kullanılabilir. Gmail, test uzmanlarının seçimini kolaylaştıracak şekilde, sayfa başlığı bilgilerine tam erişim olanağı sağlamaktadır.

### DNS keşfi

DNS keşfi, etki alanının yetkili ad sunucusunun "WHOIS" kayıtlarına bakmak için gerçekleştirilir. İlave olarak, asıl etki alanı adındaki değişiklikler kontrol edilmeli ve Web sitesinde hedefin denetiminde olabilecek başka etki alanlarına atıfta bulunulup bulunulmadığı da kontrol edilmelidir.

### Düz/TersDNS

Ters DNS, bir kuruluş içerisinde kullanımda olan geçerli sunucu isimlerinin elde edilmesi için kullanılabilir. Verilen bir IP adresinden, bir adın çözümlenebilmesi için IP adresinin "PTR (ters) DNS" kaydını içeriyor olması gerekir. Çözümleme yapılırsa sonuçlar döndürülür. Bu işlem genelde sunucunun çeşitli IP adresleri ile test edilmesi ve herhangi bir sonuç döndürüp döndürmediğine bakılması ile gerçekleştirilir.

### DNS Bruteforce

İstemci etki alanı/etki alanları ile ilgili tüm bilgiler belirlendikten sonra DNS sorguları yapılır. DNS, IP adresleri ile alan adlarını eşleştirmek ve bu işlemin tersi için kullanıldığından, bu uygulamanın güvenlik açıkları içerecek şekilde mi yoksa güvenlik açıkları içermeyecek şekilde mi yapılandırıldığını belirlemek gerekir. Burada güvenlik açıkları söz konusu ise istemci hakkında daha fazla bilgi edinebilmek için DNS kullanılabilir. DNS'in hatalı yapılandırılması sonucu ortaya çıkacak en ciddi durum, DNS'in İnternet kullanıcılarına bir DNS alan transferi yapma olanağı sağladığı durumdur. DNS'in alan transferine olanak sağlayıp sağlamadığını belirlemek ve bunun yanında bilinmeyen ilave alan adlarını tespit edebilmek için kullanılabilecek olan birçok araç mevcuttur.

### Web uygulaması keşfi

Sızma testi sırasında zayıf Web uygulamalarının belirlenmesi özellikle yararlı bir işlem olabilir. Aranması gerekenler, yanlış olarak konfigüre edilmiş olan OTS uygulamaları, fonksiyonellik eklentisi yapan OTS uygulamaları (eklentiler çoğu zaman esas uygulamaya göre saldırılara karşı daha hassas kodlar içerir) ve isteğe göre uyarlanmış uygulamalardır. İyi bir sonuç elde etmek için WAFP gibi, Web uygulamalarının ayırt edici özelliklerini tespit eden uygulamalar kullanılabilir.

### Sanal makinelerin tespiti ve sıralanması

Web sunucuları genellikle fonksiyonelliği pekiştirmek maksadıyla birkaç sanal makine barındırır. Birkaç sunucu aynı DNS adresini işaret ediyorsa bunlar aynı sunucuda barındırılıyor olabilirler. Bir IP adresini bir sanal makine kümesi ile eşleştirmek için MSN araması gibi araçlar kullanılabilir.

### Dış hedef listesinin oluşturulması

Yukarıdaki faaliyetler tamamlandıktan sonra, bir kullanıcılar, e-postalar, etki alanları, uygulamalar, makineler ve servisler listesi derlenmelidir.

### Sürümlerin tespiti

Uygulama bilgisinin belirlenmesinin hızlı bir yolu, sürümün kontrolüdür. Servislerin sürümlerinin ayırt edici özellikleri “nmap” kullanılmak suretiyle bir dereceye kadar elde edilebilir ve Web uygulamalarının sürümleri çoğu zaman rastgele bir Web sayfasının kaynağına bakılmak suretiyle elde edilebilir.

### Yama düzeylerinin belirlenmesi

Servislerin yama düzeylerinin belirlenmesinde, sistemi sürümleri arasındaki farklılıklar bakımından sorgulayan yazılımların kullanılması dikkate alınmalıdır. Sızma testinin bu aşamasında müşteri kuruluşun kabul etmesi koşuluyla yetki bilgileri kullanılabilir. Açıklık tarayıcıları yama düzeylerinin uzaktan, yetki bilgileri kullanılmadan belirlenmesinde özellikle etkindirler.

### Kilitlenme eşiğinin belirlenmesi

Bir kimlik doğrulama servisinin kilitlenme eşiğinin belirlenmesi, sızma testi esnasında yapılacak olan brute force saldırıları nedeniyle geçerli kullanıcıların hesaplarının kilitlenmemesini garantiye alma olanağı sağlar. Ortamdaki birbirinden ayrı tüm kimlik doğrulama servisleri belirlenmeli ve en masumane olduğu düşünülen münferit bir kullanıcı hesabı kilitlenmeye yönelik olarak test edilmelidir. Çoğu zaman geçerli bir kullanıcının hesabında yapılacak olan 5-10 deneme, servisin kullanıcıların hesabını kilitleyip kilitlemediğinin belirlenmesi için yeterli olur.

### Hataya dayalı olarak
### Saldırı için zayıf portların belirlenmesi

Zayıf portların belirlenmesi “banner grabbing”, “nmap” kullanılarak ve kullanıcının sağduyusunu kullanması ile gerçekleştirilebilir. Çoğu port ve servisler, sürümleri hakkında yanlış bilgi verirler veya yanlış yönlendirmeler yaparlar.

**Eski sistemler**

**Sanal makinelere karşı sanallaştırma platformları**

**Bellek yapısı**

## İç bilgi tarama

### Pasif keşif

Bir test uzmanının iç ağa erişimi mevcutsa, paket dinleme önemli miktarda bilgi sağlayabilir. Sistemlerin belirlenmesinde pasif işletim sistemi ayırt edici özelliklerin belirlenmesi aracında (p0f - passive OS fingerprinting) uygulanan teknikler gibi tekniklerin kullanılması gerekir.

### Müşteri kuruluşun iç sınırlarının belirlenmesi

Testin icrasında önce yerel alt ağ tespit belirtilmelidir. Yerel alt ağ belirtildikten sonra adreste küçük değişiklikler yapmak suretiyle buradan diğer alt ağlar bulunabilir. Aynı zamanda bir iç makinenin yönlendirme tablosuna bakılması da özellikle çok şey anlatır. Aşağıda kullanılabilecek birkaç teknik verilmektedir.

DHCP sunucuları sadece yerel bilgiler için değil, önemli makinelerin uzak IP aralığı ve diğer detayları konusunda da potansiyel bir kaynaktır. Çoğu DHCP sunucuları yerel bir IP geçit adresi ve aynı zamanda DNS ve WINS sunucularının adreslerini sağlar. Windows tabanlı ağlarda DNS sunucuları, aktif dizin etki alanı denetleyicisi olmak durumundadırlar ve bu nedenle de ilgi alanındadırlar.

## Aktif bilgi tarama

### Port taraması

Iç port taraması dış port taramasından farklıdır çünkü daha geniş bir bant genişliği kullanılabilir ve daha fazla yetenek söz konusudur.

### “Banner Grabbing”

“Banner Grabbing” uygulaması bir ağa bağlı bilgisayar sistemleri ve bu bilgisayarların açık portlarında çalışmakta olan servisler hakkında bilgi toplamak için kullanılan bir listeleme tekniğidir. “Banner Grabbing” ağdaki uygulamaların sürümlerini ve hedef makinenin çalıştığı işletim sistemini belirlemek için kullanılır.

“Banner Grabbing” genellikle HTTP, FTP ve SMTP protokollerinin, sırasıyla 80, 21, ve 25 portlarında gerçekleştirilir. “Banner Grabbing” uygulanmasında yaygın olarak kullanılan araçlar “Telnet”, “nmap” ve “Netcat”tir.

### “SNMP Sweeps”

“SNMP sweeps” belirli bir sistem hakkında çok fazla bilgi sağladığı için uygulanır. SNMP protokolü durum bilgisi kullanmaz ve datagram uyumlu bir protokoldür. Ancak SNMP sunucuları geçersiz dizilerle yapılan sorgulara cevap vermez ve kullandığı UDP protokolü, kapalı UDP portlarını eksiksiz bir şekilde raporlamaz.

### Alan transferleri

DNS alan transferi, ya da bilinen diğer adıyla AXFR bir tür DNS işlemidir. DNS alan transferi bir dizi DNS sunucusu üzerindeki DNS verilerini içeren veri tabanlarının kopyasının çıkarılması için geliştirilmiş olan bir mekanizmadır. Alan transferleri iki çeşittir: tam alan transferi (AXFR) ve artan alan transferi (IXFR). DNS alan transferi gerçekleştirme yeteneğinin test edilmesinde kullanılabilecek olan çok sayıda araç mevcuttur. Alan transferlerinin gerçekleştirilmesinde yaygın olarak kullanılan araçlar "host", "dig" ve "nmap"tir.

### SMTP Bounce Back

Aynı zamanda, teslim edilmedi raporu/alındısı (NDR), (başarısız) ileti durum raporu (DSN) iletisi, iletilmedi bildirimi (NDN) veya basitçe "bounce" olarak ta adlandırılan "SMTP bounce back", bir e-posta sisteminden gelen bir iletinin göndericisini, iletisinin adresine teslim edilmesi ile ilgili bir problem yaşandığına dair bilgilendiren, otomatik olarak yaratılan bir elektronik iletidir. Bir "bounce" iletisi, yazılım ve sürümler dahil olmak üzere kullanılan SMTP sunucusu hakkında bilgi içeriyor olabileceğinden, bir saldırgan için SMTP sunucusunun ayırt edici özelliklerinin tespit edilmesinde yardımcı olabilir.

Bu basit bir şekilde hedefin etki alanı içerisinde sahte bir adres yaratmak suretiyle gerçekleştirilebilir. Örneğin, "asDFADSF_garbage_address@target.com", "target.com"u test etmek üzere kullanılabilir. Gmail, test uzmanlarının seçimini kolaylaştıracak şekilde, sayfa başlığı bilgilerine tam erişim olanağı sağlamaktadır.

### DNS keşfi

DNS keşfi, etki alanının yetkili ad sunucusunun "WHOIS" kayıtlarına bakmak için gerçekleştirilir. İlave olarak, asıl etki alanı adındaki değişiklikler kontrol edilmeli ve Web sitesinde hedefin denetiminde olabilecek başka etki alanlarına atıfta bulunulup bulunulmadığı da kontrol edilmelidir.

### Düz/Ters DNS

Ters DNS, bir kuruluş içerisinde kullanımda olan geçerli sunucu isimlerinin elde edilmesi için kullanılabilir. Verilen bir IP adresinden, bir adın çözümlenebilmesi için IP adresinin "PTR (ters) DNS" kaydını içeriyor olması gerekir. Çözümleme yapılırsa sonuçlar döndürülür. Bu işlem genelde sunucunun çeşitli IP adresleri ile test edilmesi ve herhangi bir sonuç döndürüp döndürmediğine bakılması ile gerçekleştirilir.

### DNS Bruteforce

İstemci etki alanı/etki alanları ile ilgili tüm bilgiler belirlendikten sonra DNS sorguları yapılır. DNS, IP adresleri ile alan adlarını eşleştirmek ve bu işlemin tersi için kullanıldığından, bu uygulamanın güvenlik açıkları içerecek şekilde mi yoksa güvenlik açıkları içermeyecek şekilde mi yapılandırıldığını belirlemek gerekir. Burada güvenlik açıkları söz konusu ise istemci hakkında daha fazla bilgi edinebilmek için DNS kullanılabilir. DNS'in hatalı yapılandırılması sonucu ortaya çıkacak en ciddi durum, DNS'in İnternet kullanıcılarına bir DNS alan transferi yapma olanağı sağladığı durumdur. DNS'in alan transferine olanak sağlayıp sağlamadığını belirlemek ve bunun yanında bilinmeyen ilave alan adlarını tespit edebilmek için kullanılabilecek olan birçok araç mevcuttur.

### Web uygulaması keşfi

Sızma testi sırasında zayıf Web uygulamalarının belirlenmesi özellikle yararlı bir işlem olabilir. Aranması gerekenler, yanlış olarak konfigüre edilmiş olan OTS uygulamaları, fonksiyonellik eklentisi yapan OTS uygulamaları (eklentiler çoğu zaman esas uygulamaya göre saldırılara karşı daha hassas kodlar içerir) ve isteğe göre uyarlanmış uygulamalardır. İyi bir sonuç elde etmek için WAFP gibi, Web uygulamalarının ayırt edici özelliklerini tespit eden uygulamalar kullanılabilir.

### Sanal makinelerin tespiti ve sıralanması

Web sunucuları genellikle fonksiyonelliği pekiştirmek maksadıyla birkaç sanal makine barındırır. Birkaç sunucu aynı DNS adresini işaret ediyorsa bunlar aynı sunucuda barındırılıyor olabilirler. Bir IP adresini bir sanal makine kümesi ile eşleştirmek için MSN araması gibi araçlar kullanılabilir.

### Sürümlerin tespiti

Uygulama bilgisinin belirlenmesinin hızlı bir yolu, sürümün kontrolüdür. Servislerin sürümlerinin ayırt edici özellikleri “nmap” kullanılmak suretiyle bir dereceye kadar elde edilebilir ve Web uygulamalarının sürümleri çoğu zaman rastgele bir Web sayfasının kaynağına bakılmak suretiyle elde edilebilir.

### Yama düzeylerinin belirlenmesi

Servislerin yama düzeylerinin belirlenmesinde, sistemi sürümleri arasındaki farklılıklar bakımından sorgulayan yazılımların kullanılması dikkate alınmalıdır. Sızma testinin bu aşamasında müşteri kuruluşun kabul etmesi koşuluyla yetki bilgileri kullanılabilir. Açıklık tarayıcıları yama düzeylerinin uzaktan, yetki bilgileri kullanılmadan belirlenmesinde özellikle etkindirler.

### Zayıf Web uygulamalarının aranması

Sızma testi sırasında zayıf Web uygulamalarının belirlenmesi özellikle yararlı bir işlem olabilir. Aranması gerekenler yanlış olarak konfigüre edilmiş olan OTS uygulamaları, fonksiyonellik eklentisi yapan OTS uygulamaları (eklentiler çoğu zaman esas uygulamaya göre saldırılara karşı daha hassas kodlar içerir) ve isteğe göre uyarlanmış uygulamalar. Burada iyi bir sonuç elde etmek için WAFP gibi Web uygulamalarının ayırt edici özelliklerini tespit eden uygulamalar kullanılabilir.

### Kilitlenme eşiğinin belirlenmesi

Bir kimlik doğrulama servisinin kilitlenme eşiğinin belirlenmesi, sızma testi esnasında yapılacak olan brute force saldırıları nedeniyle geçerli kullanıcıların hesaplarının kilitlenmemesini garantiye alma olanağı sağlar. Ortamdaki birbirinden ayrı, tüm kimlik doğrulama servisleri belirlenmeli ve en masumane olduğu düşünülen münferit bir kullanıcı hesabı kilitlenmeye yönelik olarak test edilmelidir. Çoğu zaman geçerli bir kullanıcının hesabında yapılacak olan 5-10 deneme, servisin kullanıcıların hesabını kilitleyip kilitlemediğinin belirlenmesi için yeterli olur.

### Saldırı için zayıf portların belirlenmesi

Zayıf portların belirlenmesi “banner grabbing” ve “nmap”in kullanılmasıyla ve kullanıcının sağduyusunu kullanması ile gerçekleştirilebilir. Çoğu port ve servisler sürümlerinin detayları hakkında yanlış bilgi verirler veya yanlış yönlendirmeler yaparlar.

### Eski sistemler

### Sanal makinelere karşı sanallaştırma platformları

### Bellek yapısı

## 2.7 Koruma mekanizmalarının belirlenmesi

### Ağa dayalı korumalar

Basit paket filtreleri

Trafik şekillendirme aygıtları

Veri kaybından korunma (DLP) sistemleri

Şifreleme/tünelleme

### Makineye dayalı korumalar

Yığın/alt yığın korumaları

Güvenli uygulamalar listesi teşkili

Anti-Virüs/Filtreleme/Davranışsal analiz

Veri kaybından korunma sistemleri

### Uygulama düzeyindeki korumalar

Uygulama korumalarının belirlenmesi

Kodlama seçenekleri

Potansiyel baypas yolları

Güvenli listesine alınan sayfalar

### Bellek korumaları

HBA - Makine düzeyi

LUN maskeleme

Bellek denetimcisi

iSCSI CHAP Secret

### Kullanıcı korumaları

# 3. Tehdit modellemesi

## 3.1 Genel

Bu bölümde doğru bir sızma testi uygulaması için gerekli olan, tehdit modellemesi yaklaşımı tanımlanmaktadır. Standard belirli bir tehdit modelini kullanmaz ancak kullanılan modelin tehditleri, bu tehditlerin yeteneklerini, teste tabi tutulan kuruluş bazında tehditlerde aranacak nitelikleri ve tehditlerin gelecekteki testlerde tekrar tekrar kullanılması kabiliyetini göstermesi bakımından aynı sonuçlarla tutarlı olmasını gerektirir.

Standard geleneksel tehdit modellemesinin iki anahtar öğesine odaklanmaktadır: değerli varlıklar ve saldırgan (tehdit). Değerli varlıklar, iş varlıkları ve iş prosesleri, saldırgan ise tehdit zümreleri ve bunların kabiliyetleri şeklinde alt dallara ayrılır.

Her sızma testi için asgari olarak bu dört öğenin tamamı açık bir şekilde tanımlanmalı ve yazılı olarak belgelenmelidir.

Saldırgan tarafının modellenmesinde, tehdit zümresi (çoğu zaman anlamsal olan ve kuruluşun SWOT analizine bağlı olan) ve yeteneklerinin (çoğu zaman teknik olan) üzerinde, saldırı motivasyonu modellemesinin ilave yönleri de verilmelidir. Bu ilave yönler esas olarak hedefteki kullanılabilir olan farklı varlıkların değerini dikkate alır ve bu varlıkların elde edilmesinin maliyeti ile birleştirir. Belirlenen varlıkların her birine yönelik olarak, “bu varlık kaybedilirse ne olur?” şeklindeki daha doğru bir bakış açısı sağlamak maksadıyla tamamlayıcı bir model olarak kuruluş için etki modellemesi de gerçekleştirilebilir. Bu modelleme varlıkların net değerini, gerçek değerini ve bir kayıp durumunda doğacak diğer dolaylı maliyetleri dikkate alır.

**Üst düzey tehdit modellemesi prosesi**

1. İlgili dokümanlar toplanır
2. Öncelikli ve ikincil varlıklar belirlenir ve kategorilendirilir
3. Tehditler ve tehdit zümreleri belirlenir ve kategorilendirilir
4. Öncelikli ve ikincil varlıklara yönelik tehdit zümreleri belirlenir

**Örnek**

Sızma testi değerlendirmesi göz önüne alındığında sistemde yerleşik olarak bulunan CRM uygulaması kapsam dahilinde olabilir. Arka uç veri tabanında saklanmakta olan müşteri bilgileri kapsam dahilindeki uygulama ile doğrudan bağlantılı olduğundan, kolaylıkla belirlenebilen önemli bir varlıktır. Ancak veri tabanı sunucusunun teknik tasarımı incelenmek suretiyle, aynı veri tabanı sunucusunun arka ucunda saklanmakta olan HR veri tabanı da ikinci bir değerli varlık olarak belirlenebilir. Bir saldırgan CRM uygulamasını çalışan bilgilerini elde etmek için bir sıçrama tahtası olarak kullanabilir. Temel bir tehdit modellemesi uygulamasında belirli tehdit zümreleri CRM uygulaması ile eşleştirildiğinde ilgi alanı dışında olarak değerlendirilebilir. Ancak ikincil değerlerin belirlenmesi ile tehdit manzarası aniden değişir.

## 3.2 İş değer analizi

Tehdit modellemesi uygulamasının iş değer analizi kısmında kapsam dahiline alınan tüm değerler ve bu değerlerin desteklediği iş prosesleri üzerinde değer eksenli bir bakış açısı uygulanır. Sızma testi uzmanı toplanan dokümanların analiz edilmesi ve kuruluş içerisindeki ilgili personelle görüşmeler yapmak suretiyle, bir saldırgan tarafından hedef alınması en çok muhtemel olan değerleri, bunların kıymetinin ne olduğunu ve bunların (kısmen) kaybı durumunda etkilerinin neler olabileceğini belirleyebilir.

### Kurumsal veriler

### Politikalar, planlar ve prosedürler

Kuruluş içi politikalar, planlar ve prosedürler kuruluşun nasıl iş yaptığını ortaya koyar. Bu dokümanlar bir kuruluş içerisindeki anahtar konumdaki rollerin ve bir firmanın çalışmaya devam edebilmesini sağlayan iş proseslerinin belirlenmesine yardımcı olabildiğinden özel önem taşır.

### Ürün bilgisi (ticari sırlar, ar-ge verileri )

Ürünle ilgili bilgiler patentler, ticari sırlar, geleceğe yönelik planlar, kaynak kodları, ürünün pazar değerini doğrudan etkileyen destek sistemleri, algoritmalar ve kuruluşun söz konusu ürünün iş başarısına yönelik olarak anahtar faktör olarak dikkate aldığı diğer bilgileri içerir.

### Pazarlama bilgileri (planlar, yol haritaları vb.)

Bunlar promosyonlar, yeni ürün çıkarılması, ürün değişimleri, pazar konumlaması, ortaklıklar, üçüncü taraf tedarikçilere yönelik pazarlama planları, kuruluşun içerisinde ve dışarısında sürdürülen faaliyetlerle ilgili iş planlarıdır. İlave olarak, kamuoyu araştırmalarıyla ilgili bilgiler, ortaklarla, raporlayıcılarla, danışma şirketle ilgili detaylar ve bu gibi varlıklarla yapılan her türlü yazışmalar da yüksek ölçüde talep gören bilgiler olarak değerlendirilir.

### Finansal bilgiler (banka, krediler, tasarruf hesapları )

Finansal bilgiler genellikle bir kuruluşun sahip olduğu en iyi korunan bilgileridir. Bu bilgiler banka hesap bilgilerini, kredi kartı bilgilerini ve/veya kredi kartı numaralarını, yatırım hesaplarını ve diğer bilgileri içerebilir.

### Teknik bilgiler

Kuruluş ve kuruluşun faaliyetleri hakkındaki teknik bilgiler sızma testi uzmanı için çok önemli bilgilerdir. Bu gibi bilgiler bir sızma testinden beklenen sonuçlar değildir. Ancak bu bilgilerin başka alanlarda kullanılmasıyla testin icra edilmesi süreci kolaylaşır. Örneğin, altyapı tasarım bilgileri istihbarat toplama prosesi için değerli bilgiler sağlayabilir.

- **Altyapı tasarım bilgileri**

Altyapı tasarımıyla ilgili bilgiler tüm ana teknolojilerle ve kuruluşun çalışmasında kullanılan tesislerle ilgili bilgilerdir. Bina projeleri, elektrik hatları ve bağlantı çizelgeleri, bilgisayar donanımı/ağ tasarımları ve uygulama düzeyindeki bilgi işlem faaliyetlerinin tamamı altyapı tasarımıyla ilgili bilgiler olarak değerlendirilir.

- **Sistem konfigürasyon bilgileri**

Sistem konfigürasyon bilgileri konfigürasyon temel dokümanlarını, konfigürasyon kontrol çizelgelerini ve güçlendirme prosedürlerini, grup politikası bilgilerini, işletim sistemi imajlarını, yazılım envanterini vb. içerir. Bu bilgiler açıklıkların keşfedilmesine yardımcı olabilir (örneğin konfigürasyon hataları veya eski yazılım kurulumları bilgisi sayesinde açıklık tespit edilmesi).

- **Kullanıcı hesabı yetki bilgileri**

Kullanıcı hesabı yetki bilgileri, bir kimlik denetimi aracı (VPN, Web portalı vb.) mevcut olduğunda, bilgi sistemine ayrıcalıklı olmayan bir düzeyde erişimin kolaylaştırılmasına yardımcı olur.

- **Ayrıcalıklı kullanıcı hesabı** yetki **bilgileri**

Ayrıcalıklı kullanıcı hesabı yetki bilgileri, bir kimlik denetimi aracı (VPN, Web portalı vb.) mevcut olduğunda, bilgi sistemine yüksek düzeyde erişimin kolaylaştırılmasına yardımcı olur. Ayrıcalıklı kullanıcı hesabı yetki bilgilerinin elde edilmesi genellikle teste tabi tutulan bilgi sisteminin üçüncü kişilerin ele geçmesine yol açar.

## Çalışan bilgileri

Bu bölümde bir saldırgan tarafından elde edildiği taktirde kuruluş üzerinde doğrudan bir etkisi olabilecek olan çalışan bilgileri analiz edilmektedir. Bu gibi bilgilerin kaybı veya açıkta bırakılması durumunda ceza uygulamaya rıza gösteren kuruluşlar, bu şekildeki bilgi kayıplardan doğrudan etkileneceği açık olan aday kuruluşlardır. Aynı zamanda çalışanları kritik varlıklar olarak değerlendirilebilecek olan kuruluşlar da (özel devlet organları, ticari sırlarla ilgili uzman çalışanlar/bölümler vb.) bu gibi bir incelemeye tabi tutulabilirler.

- Vatandaşlık numaraları
- Kişisel kimlik bilgileri
- Korunan sağlık bilgileri
- Finansal bilgiler (banka, kredi hesapları)

## Müşteri verileri

Çalışan bilgilerine benzer şekilde tehdit modellemesi sürecinde müşteri verileri de, kuruluşu doğrudan/dolaylı olarak bir kayba maruz bırakması söz konusuysa, bir iş değeri olarak değerlendirilir. Bu noktada düzenleme/uyma gerekliliğinin (cezalara dayalı olan) üzerinde ilave bir faktör söz konusu olur. Bu gibi bilgiler dolandırıcılık yapılmasında kullanıldığında, kuruluş bu bilgilerin kaybından sorumlu tutulabilir ve dolandırıcılıkla ilgili olarak dava edilebilir (dolandırıcılığın yapılmasını mümkün kılan müşteri bilgilerinin kaybına dayalı olarak). Aşağıdaki listede ilgili müşteri verilerini kapsayan ve tehdit modellemesi bakımından iş varlıkları olarak değerlendirilebilecek bu gibi bilgi alanları örnekleri verilmektedir.

- Vatandaşlık numaraları

- Kişisel kimlik bilgileri
- Korunan sağlık bilgileri
- Finansal bilgiler (banka, kredi hesapları)
- Tedarikçi verileri

Kuruluş için kritik olarak değerlendirilen tedarikçilerle ilgili bilgiler (kritik bileşenlerin üreticileri, ticari bir sırrın bir parçasını teşkil edebilecek olan tedarikçilerle yapılan anlaşmalar, tedarik edilen bileşenlerin maliyet analizleri) ve aynı zamanda kuruluşun tedarikçileri aracılığıyla yürüttüğü iş faaliyetlerini etkilemek için kullanılabilecek olan her tür bilgi iş varlığı olarak değerlendirilir.

- Ortaklara ait veriler
- Bulut servisi hesap bilgileri

### İnsan varlıkları

Bir kuruluşun insan varlıklarının belirlenmesinde akılda tutmamız gereken husus, bu varlıkların elde edilmesinin kuruluşun bilgilerinin ele geçirilmesi gibi daha büyük bir gayretin bir parçası olmasıdır. Böyle olunca, iş varlığı olarak belirlenen insan varlıkları, bilgilerin ifşa edilmesine yönelik olarak kaldıraç olarak kullanılabilecek olanlar, karar almada manipüle edilebilecek olanlar veya eylemleri kuruluşu olumsuz olarak etkileyebilecek veya bir saldırganın varlıkları daha ileri derecede ele geçirmesine olanak sağlayabilecek olan insanlardır. İnsan varlıklarının kuruluşun hiyerarşik yapısı içerisinde en üstteki kişiler olması gerekmez. Daha çok önceden belirlenmiş olan iş varlıklarıyla ilgili olan anahtar personel veya bu gibi varlıklara erişim için olanak sağlayacak konumdaki personel olması gerekir. İnsan varlıkları aynı zamanda normalde erişimi kısıtlı olan firma varlıklarına erişimle ilgili olmayabilen, ancak güvenliğin veya prosedürlerin atlatılmasını kolaylaştıracak şekilde firmaya fiziki olarak erişim sağlayabilecek konumda olan çalışanları içerebilir. Aşağıdaki liste bu gibi varlıklar için bazı örnekler vermektedir ve bu liste teste tabi tutulan kuruluşa göre uyarlanabilir.

- Üst yönetim
- Yönetici asistanları
- Orta düzey yönetim
- İdari asistanlar
- Teknik/Takım liderleri
- Mühendisler
- Teknisyenler
- İnsan kaynakları

## 3.3 İş proses analizi

Bir iş para kazanmıyorsa iş değildir. İş, ham malzemelerin veya bilginin çeşitli proseslerden geçirilerek değerinin yükseltilmesi veya ilave değer yaratılması suretiyle gerçekleşir. Bu da gelir yaratır. İş prosesleri ve varlıkları (insan, teknoloji, para) kuruluşlar için değer zincirlerinin yaratılmasında destek olur. Bu proseslerin ortaya çıkarılması, kritik olan ve olmayan proseslerin belirlenmesi ve nihayet bu proseslerdeki hataların bulunması ile işin nasıl yürüdüğünü, neyin para kazandırdığını ve nihayet belirli tehdit zümrelerinin kuruluşların para kaybetmesini nasıl sağlayabildiklerini anlayabiliriz.

İş prosesi analizinde kritik prosesler ve kritik olmayan prosesler birbirinden ayrılır. Her bir kategori için analiz aynıdır ve bazı öğeleri dikkate alır. Esas farklılık kritik bir iş prosesine yöneltilen tehdit ile buna karşı kritik olmayan bir iş prosesine yöneltilen tehdidin ağırlıklarındadır. Ancak birkaç kritik olamayan iş prosesinin toplamının bir tehdit senaryosu içerisinde birleştirilerek bir öğenin/prosesin içerisinde kritik bir kusur yaratılabileceğinin de akılda tutulması gerekir. Bu gibi tehdit senaryoları da bu safhada belirlenmeli ve sızma testinin sonraki aşamalarında kullanılması planlanmalıdır.

### Prosesi destekleyen teknik altyapı

İş prosesleri genellikle bilgi teknolojileri altyapısı (bilgisayar ağları, işlem gücü, bilgi girişleri ve iş prosesleri yönetim bilgisayarları) tarafından desteklendiğinden, tüm bu bilgi teknolojileri öğeleri belirlenmeli ve planı çıkarılmalıdır. Çıkarılan bu plan, daha sonra tehdit modelinin açıklıkların belirlenmesi ve istismara çevrilmesinde kullanılmak üzere yeterince açık olmalıdır.

### Prosesi destekleyen bilgi varlıkları

Teknik altyapının aksine bilgi varlıkları, referans olarak ya da destek materyali (karar alma, hukuki, pazarlama vb.) olarak kullanılan, kuruluştaki mevcut bilgi tabanlarıdır. Bu gibi varlıklar genellikle önceden iş prosesinde belirlenmiştirler ve teknik altyapının ve bu bilgi varlıklarını destekleyen ilave teknik altyapının yanı sıra çıkarılan plana dahil edilmelidirler.

### Prosesi destekleyen insan varlıkları

İş analizine dahil olan insan kaynaklarının belirlenmesi proses analiziyle (yazılı olan veya olmayan) bağlantılı olarak yapılmalıdır ve herhangi bir şekilde müdahil (belirli bir bilgi varlığı veya teknik altyapı öğesi ile ilgisi olmasa da) olan herkes listelenmeli ve prosese yerleştirilmelidir. Bu insan kaynakları varlıkları genellikle bir onaylama alt prosesinin, bir doğrulama alt prosesinin bir kısmını ve hatta bir referansın (hukuki danışmanlık gibi) bir kısmını teşkil eder. Bu gibi varlıklar (özellikle bilgi varlıkları veya teknik altyapı ile herhangi bir ilgisi olmayanlar) daha sonra doğaları gereği teknikten ziyade sosyal saldırı vektörleriyle eşleştirilebilirler.

### Prosese üçüncü tarafların katılması ve/veya prosesin üçüncü taraflarca kullanılması

Prosesi destekleyen insan varlıklarına benzer şekilde iş prosesine herhangi bir şekilde müdahil olan her üçüncü taraflar da belirlenmelidir. Bu kategori hem insan varlıklarını hem de bilgi/teknik varlıkları içerebileceğinden, planının çıkarılması incelik gerektirebilir.

## 3.4 Tehdit unsurları/zümresi analizi

İlgili tehdit zümrelerinin ve unsurlarının tanımlanmasında, tehdidin lokasyonu (kuruluşun içinden veya dışından gelmesi), lokasyondaki belirli zümreler ve belirli bir tehdit unsuru veya zümresi için bir yetenekler/motivasyon profili yaratılmasında destek olabilecek ilave bilgiler anlamında tehdit açık bir şekilde tanımlanmalıdır. Mümkünse özel tehdit unsurları belirtilmelidir. Aksi taktirde daha genel bir

zümre çerçevesi (destekleyen materyal ve istihbaratla birlikte) çizilmelidir. Aşağıda bazı tehdit unsuru/zümresi örnekleri verilmektedir:

| İç | Dış |
|---|---|
| Çalışanlar | İş ortakları |
| Yönetim (üst yönetim, orta düzey yönetim) | Rakipler |
| Yöneticiler (ağ, sistem, sunucu) | İş üstlenicileri |
| Geliştiriciler | Tedarikçiler |
| Mühendisler | Devletler |
| Teknisyenler | Organize suç örgütleri |
| İş üstlenicileri (dışardaki kullanıcılarıyla birlikte) | İnternet korsanları |
| Genel kullanıcı zümresi | “Script kiddies” (eğlence olsun diye yapanlar/rastgele “hack”leyenler) |
| Uzaktaki destek unsurları/zümreleri | |

## Çalışanlar

Doğrudan firma için, tam zamanlı veya yarı zamanlı olarak çalışan kişiler. Genelde bu kişilerin çoğu geçimleri bakımından bu firmaya bağlı olduklarından, onlara iyi davranıldığı sürece, firmayı incitmekten çok onu korumaya meyilli olacakları farz edilerek, firma için ciddi bir tehdit teşkil etmeyecekleri kabul edilir. Bu kişiler çoğunlukla veri kaybı olaylarına veya kazara bilgilerin üçüncü tarafların eline geçmesi olaylarına karışırlar. Nadiren dışarıdan birileri tarafından izinsiz olarak sisteme girişlere yardımcı olmaları için motive edilebilirler veya kendi kendilerine zararlı bazı eylemler gerçekleştirirler. Bu kişilerin yetenekleri değişken olmakla birlikte, genellikle düşük ile orta düzey arasında yetenektedirler.

### Yönetim (Üst, orta)

Yukarıda tanımlandığı gibi doğrudan firma adına çalışan kişilerdir. Firma içerisindeki konumları ve fonksiyonları dikkate alındığında genellikle ayrıcalıklı bilgilere erişimleri mevcuttur.

## 3.5 Tehdit yetenek analizi

Bir tehdit zümresi tanımlandığında, bu zümrenin kuruluş üzerinde başarılı bir eylemde bulunma ve kuruluşun bilgilerini ele geçirme ihtimalini yansıtacak doğru bir tehdit modeli oluşturmak için, söz konusu tehdit zümresinin yetenekleri de analiz edilmelidir. Bu analiz hem teknik analiz, hem de fırsat analizi (yapılması mümkün olduğunda) yapılmasını gerektirir.

### Kullanılan araçların analizi

Tehdit zümresinin/unsurunun kullanabileceği bilinen her türlü araç buraya dahil edilmelidir. İlave olarak serbest olarak kullanılabilir olan araçlar da, bu araçların kullanılabilmesi için gerekli olan beceri seviyesinden bu araçların mevcut potansiyeline kadar analiz edilmeli ve tehdit yeteneğine dahil edilmelidir.

### Kuruluşla ilgili ortamlara yönelik istismarların kullanılabilirliği

Tehdit zümresi/unsuru, kuruluşla ilgili olan ortamlara yönelik istismarda bulunma veya istismar geliştirme yetenekleri bakımından da analiz edilmelidir. İlave olarak bu gibi istismarlara üçüncü taraflar, iş ortakları veya yeraltı toplulukları aracılığıyla erişim sağlanması da bu analizde dikkate alınmalıdır.

### İletişim yöntemleri

Kuruluşa yönelik saldırıların karmaşıklığının değerlendirilmesi bakımından tehdit unsuru/zümresinin kullanımında olan iletişim yöntemlerinin bir analizi yapılmalıdır. Bu iletişim yöntemleri, şifreleme gibi basit ve açık olarak kullanılabilir olan teknolojilerden, saldırıların icrasında ve kaynak bilgilerinin maskelenmesinde “bulletproof hosting”, “drop-sites kullanımı” ve bilinen ya da bilinmeyen “botnet”lerin kullanımı gibi uzmanlara özel araçlara ve servislere kadar uzanır.

## 3.6 Saldırı motivasyonunun modellenmesi

Daha ileri analizlerde tehdit unsurları veya zümrelerinin muhtemel motivasyon kaynakları dikkate alınmalıdır. “Anonymous” ve “Antisec” gibi gruplar tarafından gerçekleştirilen bilgisayar korsanlığı türü saldırıların artmasından da anlaşılacağı üzere saldırganların motivasyon kaynakları sürekli olarak değişmektedir. Her kuruluş ve/veya dikey pazara yönelik özgün motivasyon kaynaklarında hafif farklılıklar mevcuttur. Yaygın olan bazı saldırı motivasyon kaynakları aşağıda belirtilmektedir:

- Kar elde etmek (doğrudan ya da dolaylı olarak)
- Bilgisayar korsanlığı
- Doğrudan kin

- Eğlence veya ün sağlamak
- Ortak olarak kullanılan/bağlı olunan sitemlere daha ileri düzeyde erişim sağlamak

## 3.7 Bilgileri ele geçirilen kıyaslanabilir kuruluşlarla ilgili haberlerin bulunması

Eksiksiz bir tehdit modelinin sağlanması maksadıyla aynı dikey endüstri içerisindeki diğer kuruluşlarla bir karşılaştırma verilmelidir. Bu karşılaştırma ilgili her türlü olayı, bu kuruluşlarla ilgili haberleri ve karşılaştıkları güçlükleri içermelidir. Bu şekildeki bir karşılaştırma, tehdit modelinin doğrulanması ve kuruluşun kendini karşılaştırması için bir dayanak sağlanması maksadıyla kullanılır (herkese açık olan bu bilgilerin, karşılaştırma yapılan firmanın gerçekte yüz yüze kaldığı tehdit ve olayların sadece bir kısmını göstereceği dikkate alınmalıdır).

# 4. Açıklık analizi

## 4.1 Açıklık Testi

Açıklık testi bir saldırgan tarafından kaldıraç olarak kullanılabilecek, sistemlerdeki ve uygulamalardaki kusurların keşfedilmesi prosesidir. Bu kusurlar makine ve servisin yanlış konfigüre edilmesinden, güvenli olmayan uygulama tasarımına kadar uzanabilir. Kusurların tespitinde kullanılan prosesler değişse ve büyük ölçüde teste tabi tutulan özel bileşene bağlı olsa da, proseste bazı anahtar prensipler uygulanır.

Test uzmanı, her türden açıklık analizinin gerçekleştirilmesinde, istenen sonuçlara yönelik amaçların ve/veya gerekliliklerin karşılanması maksadıyla, açıklık testini derinlik ve genişlik bakımından uygun bir şekilde kapsamlandırılmalıdır. Derinlikle ilgili değerler, değerlendirme aracının konumu, kimlik doğrulama gereklilikleri vb. gibi şeyleri ihtiva edebilir. Örneğin bazı durumlarda testin amacı tehdit hafifletme mekanizmasının mevcut ve çalışır durumda olduğunun ve açıklığın erişilebilir olmadığının teyit edilmesi olabilirken, diğer bazı durumlarda testin amacı uygulanabilir tüm açıklıkların keşfedilmesi maksadıyla, uygulanabilir her değişkenin, kimlik doğrulamalı bir erişimle test edilmesi olabilir. Kapsam ne olursa olsun, amaçlara ulaşmak için test işlemi derinlik gereksinimlerinin karşılanacağı şekilde uyarlanmalıdır. Değerlendirme sonuçlarının beklentileri karşılamasının (“Tüm makineler kimlik doğrulaması yaptı mı?” vb. gibi) mümkün kılınması bakımından testin derinliği daima teyit edilmelidir. Derinliğe ilave olarak açıklık testinin uygulanmasında genişlik te dikkate alınmalıdır. Genişlikle ilgili değerler hedef ağlar, bölütler, makineler, uygulamalar, envanterdekiler vb. şeyleri içerebilir. Yapacağınız test en basit şekliyle bir makinedeki tüm açıklıkları bulunması olabileceği gibi, diğer bazı durumlarda verilen bir sınır dahilindeki veya envanterdeki tüm makinelerdeki açıklıkların bulunması olabilir. İlave olarak testin genişliği, test kapsamınızın karşılanması bakımından daima teyit edilmelidir (“Tarama sırasında envanterde bulunan tüm makineler çalışır vaziyette miydi?”. Değilse, “neden?”).

## 4.2 Aktif açıklık testi

Aktif açıklık testi güvenlik açıklıkları bakımından teste tabi tutulan bileşenle doğrudan etkileşime girilmesini içerir. Bu bileşen, ağ aygıtındaki TCP yığını gibi düşük seviyede bir bileşen olabilir ya da bir aygıtı yönetmek için kullanılan Web tabanlı bir arayüz gibi, yığının üst düzeylerindeki bileşenler olabilir. Hedef bileşenle etkileşime girmek için iki ayrı yol mevcuttur: otomatik ve manuel.

**Otomatik**

Otomatik test, hedefle etkileşime girmede yazılımdan faydalanır, aldığı yanıtları inceler ve bu yanıtlara göre bir açıklığın bulunup bulunmadığını belirler. Otomatik bir proses, gereken zamanın ve işçiliğin azaltılmasında yardımcı olabilir. Örneğin, bir sistemdeki bir TCP portunun gelen verileri almaya açık olup olmadığını belirlemek için bu porta bağlanmak basit bir işlemken, bu işlemin mevcut 65 535 adet muhtemel portun her biri için bir kere gerçekleştirmek, manuel olarak yapıldığı taktirde, önemli ölçüde zaman gerektirecektir. Bu şekildeki bir testin çok sayıda ağ adresinde tekrarlanması zorunlu olduğunda gereken zaman o kadar fazla olur ki, testin bazı otomasyon biçimleri kullanılmadan tamamlanması mümkün olmayabilir.

**Ağ/Genel açıklık tarayıcıları**

**Porta dayalı açıklık tarayıcıları**

Otomatikleştirilmiş, porta dayalı bir tarama genellikle geleneksel bir sızma testinin ilk adımlarından biridir, çünkü bu tarama hedef ağ veya makinede nelerin kullanılabilir durumda olduğu hakkında temel bir düşünce elde edilmesine yardımcı olur. Porta dayalı bir tarama uzak bir makinedeki bir portun bağlantı kabul edip etmediğini belirlemek için kontrol yapar. Genellikle bu tarama IP kullanan protokolleri içerir (TCP, UDP, ICMP vb. gibi). Ancak başka ağ protokollerinde ortama bağlı olan portlar mevcut olabilir (örneğin, geniş çerçeveli ortamlarda SNA'nın kullanımda olması oldukça yaygındır). Tipik olarak bir port aşağıdaki iki muhtemel durumdan birinde olabilir:

- Açık – Port veri girişine müsaittir.
- Kapalı - Port veri girişine müsait değildir.

Bir tarayıcı bir portun "açık mı?" yoksa "kapalı mı?" olduğunu tam olarak belirleyemezse, portun "filtrelendiği" gibi başka durumlar belirtebilir.

Bir tarayıcı bir portun açık olduğunu belirlediğinde, bir açıklık olup olmadığı hakkında bir tahminde bulunulur. Örneğin, porta dayalı tarayıcı bir TCP 23 portuna bağlanır ve bu port dinleme durumundadır. Bu durumda tarayıcı muhtemelen uzak makinede telnet servisinin kullanımda olduğunu raporlayacak ve bu portu "açık metin kimlik sorgulaması protokolünün devrede olduğu" şeklinde işaretleyecektir.

**Servise dayalı açıklık tarayıcıları**

Servise dayalı bir açıklık tarayıcısı, bir portta çalışmakta olan servis hakkında daha fazla bilgi edinmek maksadıyla, uzak bir makinedeki açık portlarla iletişim kurmak için belirli protokollerden faydalanan bir tarayıcıdır. Bu, bir port taramasından daha kesin sonuç verir. Çünkü hangi servisin çalışmakta olduğunun belirlenmesinde sadece porta dayanmaz. Örneğin, bir port taraması bir makinedeki TCP 8000 portunun açık olduğunu belirleyebilir fakat sadece bu bilgiye dayalı olarak bu portta hangi servisin çalışmakta olduğunu bilemez. Bir servis tarayıcısı farklı protokolleri kullanmak suretiyle portla iletişim kurma girişiminde bulunur. Portta çalışmakta olan servis HTTP'yi kullanarak doğru bir şekilde iletişim kurabilirse bu durumda servis bir Web sunucusu olarak belirlenir.

**Banner Grabbing**

Banner grabbing belirli bir porta bağlanılarak, uzak makineden döndürülen verilerin bu porta bağlı olan servis/uygulamanın belirlenmesi maksadıyla incelenmesi prosesidir. Yazılım bağlantı esnasında

genellikle, uygulamanın ismi veya yazılımın hangi sürümünün çalıştığı hakkında bilgiler içerebilen bir kimlik dizisi verir.

### Web uygulaması tarayıcıları

#### Genel uygulama hata tarayıcıları

Çoğu Web uygulaması taraması, Web sitesinin, Web uygulamasının veya Web servisinin adresiyle taramaya başlar. Tarayıcı daha sonra, linkleri ve dizin yapılarını takip etmek suretiyle sitede yavaş yavaş ilerler. Tarayıcı Web sayfaları, kaynaklar, servisler ve sunulan diğer ortamların bir listesini derledikten sonra testleri icra eder veya sitedeki ilerlemesinin sonuçlarına yönelik olarak inceleme yapar. Örneğin sitede ilerleme esnasında bir Web sayfasının form alanları içerdiği tespit edilirse, tarayıcı SQL enjeksiyonu veya çapraz site sorgulaması girişiminde bulunabilir. Sitede ilerlenen sayfada hatalar mevcutsa, tarayıcı hata detaylarında hassas bilgileri arayabilir ve bu şekilde devam eder.

Sitede ilerleme ve test icra etme safhaları kademelendirilebilir ve genel tarama süresini azaltmak maksadıyla aynı esnada gerçekleştirilebilir. Bu uygulama birçok Web uygulaması tarayıcısı için varsayılan çalışma davranışıdır.

### Dizinlerin listelenmesi/Brute force saldırısı

Web sitesinde tarama yaparak ilerleyen bir kişinin, linkleri takip etmek suretiyle tespit edemediği kullanılabilir dizinlerin mevcut olduğunu farz edelim. Tarayıcının bu dizinlerden önceden haberi olmaması durumunda asgari iki ilave seçeneği mevcuttur.

Tarayıcı/sitede ilerleyen kişi, yaygın olan dizinleri araştırabilir. Bu dizinler genelde yaygın olarak bulunan isimler ve isim varyantlarına sahip olan dizinlerdir ve yılların tecrübesinin ve taramaların sonucunda derlenmiş olan bir listeye dahil edilirler. Çoğu Web uygulamasında bu çeşit bir liste yapısal olarak mevcut olsa da, bazı sızma testi uzmanları isteklerine göre uyarladıkları, kendi listelerini kullanırlar. Bazı durumlarda dizin isimleri özeldir ki, bu isimler kullanılarak üçüncü taraf bir Web uygulaması yüksek bir doğrulukla belirlenebilir. Genellikle, doğru bir dizin listesi bir Web sitesinin yönetimsel kısımlarının, sızma testi uzmanlarının keşfetmekle yakından ilgili olabildiği kısımların, bulunmasında anahtar olabilir.

Brute force saldırısı dizinleri de benzer bir yaklaşımla, statik bir liste kullanmak yerine, dizin ismi olma ihtimali olan her seçeneği birer birer sıralayan bir araç kullanılır. Bu yaklaşımın kullanılmasının dezavantajı, yapılan isteklerle Web sunucusunun çökertilmesi veya tıkanmasının mümkün olması ve bu şekilde bir hizmet dışı kalma durumunun ortaya çıkabilmesidir. Dizin brute force saldırısının yapılmasında dikkatli olunmalı ve özellikle saldırı üretimle ilgili bir ortamda gerçekleştiriliyorsa, birisi Web sunucusunun durumunu yakından takip etmelidir.

Sızma testi uzmanı olarak dizinlerin listelenmesini istemenizdeki neden, saldırı alanınızı genişletmek veya hassas bilgiler içeren dizinleri bulmaktır.

### Web sunucusunun sürümünün/açıklığının belirlemesi

Çoğu Web uygulaması tarayıcıları, Web sunucusunun sürümünü, saldırılara karşı açıklığı bulunduğu bilinen güvenlik önerilerindeki sürümlerle karşılaştırma girişiminde bulunurlar. Bazı durumlarda açık kaynak Web sunucuları dallara ayrıldığından veya kopyalandığından ve yeni isimler, “banner”lar verildiği ve farklı sürüm numaraları tahsis edildiğinden bu yaklaşım bazen yanlış sonuçlara götürebilir.

Web sunucusunun gerçekten de banner veya Web tarayıcısı tarafından bildirilen Web sunucusu olduğunun teyit edilmesi için ilave adımların atılmalıdır.

**Yöntemler**

Birkaç Web sunucusu yöntemi güvensiz olarak değerlendirilmektedir ve saldırganların Web sunucusunun içeriğine değişen düzeylerde erişim elde etmesine olanak tanıyabilirler. Gerçek olan, bu yöntemlerin Web sunucusu yazılımının bir parçası olduğu ve Web sitesi içeriğinin buraya kadar bahsedilen diğer açıklıklarından bunun ayırt edilemeyeceğidir. Güvenli olmayan bazı yöntemler aşağıdakileri içerir:

**OPTIONS**

HTTP OPTIONS yönteminin kendisi güvensiz değildir, bu yöntem bir saldırgana hedef sunucu tarafından kabul edilen HTTP yöntemlerini kolaylıkla belirleme olanağı sağlayabilir. OPTIONS yönteminin her zaman doğru olmadığına ve aşağıda belirtilen her yöntemin münferit olarak doğrulanması gerektiğine dikkat edilmelidir.

**PUT/DELETE**

Bir saldırgan, PUT yöntemini kullanarak HTML sayfaları gibi bilgilerin aktarılması, Web içeriğinin değiştirilmesi veya Web sunucusuna zararlı bir yazılımın yüklenmesi için kullanılabilen zararlı bir içeriği yükleyebilir. Bir saldırgan, DELETE yönteminin kullanarak içeriği kaldırabilir veya hizmette aksamaya sebep olacak şekilde bir Web sitesinin görünüşünü değiştirebilir.

İlave olarak, modern REST uygulamaları, PUT yöntemini farklı bir tarzda kullanır:

Create->POST Read->GET Update->PUT Delete->DELETE

**WebDAV**

WebDAV Microsoft İnternet bilgi sunucusunun (IIS - Internet Information Server) bir bileşenidir. WebDAV (Web-based Distributed Authoring and Versioning), Web tabanlı olarak yayılan yazarlık ve sürümlendirme anlamına gelmektedir ve metin düzenleme ve dosya yönetimi için kullanılmaktadır. WebDAV uzantıları yöneticiler tarafından IIS Web sunucularındaki Web içeriğinin uzaktan idare edilmesi ve düzenlenmesinde kullanılır ve PROPFIND, COPY, MOVE, PROPPATCH, MKCOL, LOCK ve UNLOCK'ı içerir. WebDAV bir sistemi çeşitli muhtemel açıklıklara maruz bırakabilen ana işletim sistemi bileşenleri ile etkileşime girer. Potansiyel risklerin bazıları aşağıda belirtilmektedir:

- Kullanıcı isteklerinin uygun olmayan bir biçimde işlenmesinden kaynaklanan arabellek aşımı durumları
- Hatalı oluşturulmuş isteklerden kaynaklanan hizmet dışı kalma durumları
- Etki alanı tabanlı komut yazma saldırıları
- Ayrıcalıkların askıya alınması
- Gelişigüzel kod uygulanması

**TRACE/TRACK**

Modern Web sunucuları, yetkisiz olarak bilgilerin açığa çıkarılmasına yol açabilen bir kusur içeren TRACE HTTP yöntemini desteklemektedir. TRACE yöntemi, Web sunucusu bağlantılarındaki hataları

yakalar ve istemcinin istek zincirinin öteki ucunda ne alınmakta olduğunu görmesine olanak sağlar. Tüm yaygın Web sunucularında varsayılan olarak devreye alınan HTTP TRACE fonksiyonelliği, bir saldırgan tarafından, gizlilik kaybıyla sonuçlanacak şekilde, hassas bilgilerin ifşa edilmesi için kötü maksatlı olarak kullanılabilir.

**Ağ açıklık tarayıcıları / Özel protokoller**

**Sanal Özel Ağ**

Geleneksel açıklık değerlendirme araçlarının İnternet anahtar değişim protokolü (IKE - Internet Key Exchange) VPN cihazları ile doğru protokol görüşmeleri icra etme yeteneği yoktur. IKE'nin kullanımda olduğu durumlarda kesin ayırt edici özelliklerin belirlenmesi, geri alma paternleri ve kullanımda olan kimlik doğrulama yöntemlerinin belirlenmesi gibi fonksiyonları gerçekleştiren ilave araç takımlarının kullanılması gerekecektir. Bir VPN cihazının bu öz niteliklerini belirlemek suretiyle, çalışan kod sürümlerindeki ve önceden paylaşımlı anahtarlar gibi kimlik doğrulama türlerindeki zayıflıklar belirlenebilir.

**Sesli ağ tarayıcıları**

**War Dialing (Otomatik numara çevirme)**

Çoğu kuruluş halen telefon hatları aracılığıyla, bant dışı erişimden faydalanmaktadır. Otomatik numara çevirmeyi uygulamak üzere geliştirilmiş olan açıklık değerlendirme araçlarının kullanılmasıyla kimlik doğrulamadaki ve ağ mimarisindeki zayıflıklar belirlenebilir.

**VoIP**

VoIP, IP üzerinden ses verisi gönderilmesi teknolojisi günümüzde çoğu kuruluşta bol miktarda kullanılmaktadır. VoIP altyapılarının açıklık analizinin yapılması için çok sayıda araç geliştirilmiştir. Bu araçların kullanılması suretiyle, VoIP ağlarının uygun bir şekilde bölümlendirilip bölümlendirilmediği ve VoIP altyapılarının ana altyapı sistemlerine erişimde veya hedef ağdaki muhtemel telefon konuşmalarının kaydedilmesinde kullanılabilme potansiyeli belirlenebilir.

**Manuel direkt bağlantılar**

Her otomatikleştirilmiş proses veya teknolojide olduğu gibi, hata payı her zaman mevcuttur. Sistemlerdeki, ağ cihazlarındaki ve ağ bağlantısındaki dengesizlikler test esnasında doğru olmayan sonuçlar verebilir. Hedef bir sistemde kullanımda olan her bir protokol veya servise, otomatikleştirilmiş test sonuçlarının, potansiyel saldırı vektörlerinin ve önceden belirlenmemiş olan zayıflıkların teyit edilmesi maksadıyla manuel direkt bağlantıların yapılması her zaman önerilmektedir.

**Örtülü**

**Çok sayıda çıkış düğümü**

Güvenlik izleme ve savunma sistemleri belirli bir IP adresinden gelen kötü niyetli bir eylemi belirleme görevini yerine getirir. Sisteme izinsiz girişleri tespit sistemlerinin görevlendirildiği ve faaliyetleri izlediği durumlarda, çok sayıda IP adresinden yapılan kaynak bulma değerlendirmesi ve saldırı eylemleri daha doğru sonuçlar sağlar ve hedef ağdaki bir izleme aygıtının bunu belirlemesi ve yanıt vermesi olanağını zayıflatır. TOR vekil sunucuları gibi teknolojiler tek bir IP adresinden kaynaklama yapmaksızın değerlendirme faaliyetlerini yürütmek için bir yol sağlamaktadır.

**IDS sistemlerinden kaçınma**

IDS teknolojilerinin görevlendirildiği bir hedef ortama yönelik olarak değerlendirme faaliyetleri icra edilirken bu sistemlerden kaçınılması gerekebilir. IDS aygıtlarında uygulanmakta olan imza eşleştirme paternlerinin baypas edilmesi esnasında dizi manipülasyonu, çok biçimlilik, oturum bölümleme ve parçalama daha doğru sonuçlar verebilir.

## 4.3 Pasif açıklık testi

**Meta veri analizi**

Meta veri analizi bir dosyadaki verilere değil, bir dosyayı tarif eden verilere bakılmasını içerir. Örneğin bir Microsoft Office dokümanı, belgenin yazarını, firmayı, belgenin en son ne zaman kaydedildiğini ve buna benzer bilgileri listeleyebilir. Hatta çoğu doküman isteğe bağlı meta verilerin girilmesine olanak sağlar. Bu bilgiler potansiyel olarak iç adresleri ve sunuculara giden yolları, iç IP adreslerini ve bir sızma testi uzmanının ilave erişim veya ilave bilgiler elde etmek için kullanabileceği diğer bilgileri içerebilir.

Meta veriler bir firmanın iç ağında bulunan dokümanlarda oldukça yaygın olduğundan firmaların dokümanın kamunun kullanımına açılması veya kamunun kullanımında olan İnternete konulması öncesinde meta verilerinin boşaltılmasına özel ihtimam göstermelidir. Bu nedenle, bir saldırganın erişim elde edebileceği her meta veri bir güvenlik konusu olarak ele alınmalıdır.

**Trafik izleme**

Trafik izleme bir iç ağa bağlanarak, çevrimdışı analiz maksadıyla verilerin yakalanması konseptidir. “Route poisoning” ağda gürültü yarattığından ve kolaylıkla tespit edilebileceğinden bu safhanın dışında tutulmaktadır. Anahtarlanmış bir ağdan elde edilebilen hassas bilgilerin miktarı genellikle şaşırtıcı ölçüde fazladır.

## 4.4 Doğrulama

**Araçlar arasındaki korelasyon**

Birkaç araçla çalışıldığında bulgular arasındaki korelasyon gerekliliği karmaşık hale gelebilir. Korelasyon iki ayrı biçime ayrılabilir; öğelerin özel ve kategorik korelasyonu. Belirli bir hedeften toplamaya çalıştığınız bilgilerin, metriklerin ve istatistiklerin türüne bağlı olarak bu biçimlerin her ikisi de kullanışlıdır.

Özel korelasyon açıklık kimliği, CVE, OSVDB, satıcı indeks numarası, bir yazılım ürünü hakkında bilinen hususlar vb. gibi belirli, tanımlanabilir hususlarla ilgilidir ve makine adı, IP, FQDN, MAC adresi vb. gibi mikro faktörlere göre gruplandırılabilir. Buna bir örnek x makinesi için bulguların CVE numarası ile gruplandırılması (CVE numaraları birçok araçta aynı hususu indekslenmiş olabileceğinden) olabilir.

Kategorik korelasyon, öğeleri açıklık türleri, konfigürasyon hususları vb. gibi makro faktörlerine göre gruplamanıza olanak sağlayan, uygunluk çerçevelerindeki (örneğin, NIST SP 800-53, DoD 5300 Series, PCI, HIPPA, OWASP List vb.) gibi kategorik bir yapı ile ilgilidir. Buna bir örnek makineler için

varsayılan parolalarla elde edilen tüm bulguların, NIST 800-53 (IA-5) içindeki bir parola karmaşıklığı grubunda gruplanması olabilir.

Sızma testi uzmanları çoğu durumda aynı makinedeki birkaç araç arasında çok miktarda bulunan, belirli açıklıkların mikro hususları üzerine odaklanırlar. Bu çokluk, test çıktılarındaki istatistiksel sonuçları çarpıtabilir ve hatalı olarak yükseltilmiş bir risk profili ortaya çıkarabilir.

Bunun tersi, sonuçların çıktı sonuçlamasını hatalı olarak düşük bir risk profili olarak çarpıtabildiği, makro korelasyondaki aşırı azaltma veya basitleştirmedir (örneğin, ilk 10/20 listeleri).

**Manuel test/Protokole özel test**

**Sanal özel ağ**

**Ayırt edici özelliklerin belirlenmesi**

Ayırt edici özelliklerin belirlenmesi, VPN cihazının türünün ve kurulu olan kodun kesin sürümünün belirlenmesi bakımından kullanışlıdır. Cihazın doğru bir şekilde ayırt edici özelliklerin belirlenmesi suretiyle hedef sisteme yönelik olarak uygun bir araştırma ve analiz icra edilebilir.

**Kimlik doğrulama**

VPN cihazları kimlik doğrulamanın çeşitli biçimleriyle çalışabilirler. Geleneksel açıklık değerlendirmesi araçlarının bir parçası olmayan VPN araç takımlarının kullanılması, kimlik doğrulama mekanizmalarının doğru bir şekilde belirlenmesine ve ön paylaşımlı anahtarlar veya varsayılan grup kimlikleri gibi mevcut olabilecek zayıflıkların belirlenmesine olanak sağlar.

**“Citrix”**

**Sıralama**

Çoğu varsayılan kurulumlar ve kötü bir şekilde konfigüre edilmiş olan Citrix aygıtları, yayınlanan uygulamaları listelemek ve cihaza kimlik doğrulaması için konfigüre edilmiş olan geçerli kullanıcı adlarını belirlemek için bir yol sağlar. Bu bilgiler brute force saldırıları esnasında ve yetkili kullanıcılar için önceden tanımlanmış profillerin çıkarılması girişimlerinde çok önemli hale gelir.

**DNS (Etki alanı isim sistemi)**

Etki alanı isim sistemi uygun şekilde kullanılmadığı zaman bir saldırgana çok miktarda bilgi sunar. Sürüm bilgisi, doğru tanımlama ve doğru araştırma analizi yapma olanağı sağlar. Alan transferleri gibi zayıflıklar, saldırı için ilave hedeflerin tamamlayıcı bir listesini ve aynı zamanda hedef kuruluşla ilgili potansiyel olarak hassas verilerde bilgi sızıntısı sağlar.

**Web**

Web servisleri bir saldırgan için geniş bir alan sağlar. Çoğu diğer protokol ve servislerin aksine Web servisleri çoğu zaman münferit bir sistemin birçok portunda çalışır vaziyette bulunabilir. Yöneticiler güçlendirme faaliyetlerini Web servisleri için yaygın olarak kullanılan portlara veya yayınlanmış olan dizinlere odaklayabilirler ve ilave özniteliklerin güçlendirilmesini ihmal edebilirler. Otomatikleştirilmiş araçlar servislerdeki çoğu zayıflıkları belirleme yeteneğinde olmadıklarından, Web servisleri daima manuel olarak incelenmelidir.

#### E-posta

E-posta sunucuları hedef kuruluş hakkında çok miktarda bilgi verebilir. Hedef cihazda var olan fonksiyonların kullanılması suretiyle geçerli kullanıcı hesaplarının teyidi yapılabilir ve aynı zamanda diğer sistemlere yönelik olarak gerçekleştirilecek ilave saldırılar için potansiyel bir kullanıcı adları listesi geliştirilebilir. E-posta aktarması gibi açıklıklar kuruluşa yönelik olarak "phishing" gibi ilave saldırıların gerçekleştirilmesinde kaldıraç olarak kullanılabilir. Çoğu zaman e-posta sunucuları brute force saldırılarında hedeflenebilecek olan uzaktan erişim için bir Web arayüzü sağlarlar.

#### Saldırı kulvarları

#### Ağaç dalları şeklinde saldırı yapılanmalarının yaratılması

Bir güvenlik değerlendirmesi sırasında, nihai raporun doğruluğu bakımından test işleminin tamamı boyunca test ilerledikçe ağaç dalları şeklinde bir saldırı yapılanmasının geliştirilmesi çok önemlidir. Yeni sistemler, servisler ve potansiyel açıklıklar tanımlandıkça ağaç dalları şeklindeki bu saldırı yapılanması geliştirilmeli ve güncellenmelidir. Bu husus, somutlaştırılan bir giriş noktasının, ağaç dalları şeklindeki saldırı yapılanmasının geliştirilmesi esnasında belirlenen diğer saldırı vektörlerinde de tekrar edilebileceğinden, test işleminin istismar etme safhalarında özellikle önemlidir.

#### İzole edilmiş laboratuvar testi

İzole edilmiş bir laboratuvarda, benzer ortamların kurulması durumunda açıklık analizi ve istismarın doğruluk derecesi çok daha büyük olur. Çoğu zaman sistemler belirli kontrol setleri veya ilave koruma mekanizmaları ile güçlendirilebilir. Hedef kuruluşu taklit eden bir laboratuvarın tasarlanmasıyla, istenen hedeflere yönelik olarak tanımlanan açıklıklar ve istismar girişimlerinin güvenilirliğini kesinleştirilebilir, doğru olmayan sonuçların elde edilmesi veya sistemin işlememesi olasılığını azaltabilir.

#### Görsel olarak doğrulama

#### Manuel bağlantıyla kontrol etme

Uygun korelasyon yanlış bulguların azaltılmasına yardımcı olur ancak doğruluğun yükseltilmesinde genel olarak hedef sistemin görsel olarak kontrol edilmesinin yerini hiçbir şey tutmaz. Bir protokol/servis bağlantısının sonuçlarını veya yanıtlarını kontrol etmek ve bu sonuçları bilinen açıklık işaretleri ile karşılaştırmak için değerlendirme araçları geliştirilmiştir. Ancak araçlar yaygın olmayan portlardaki servislerin veya bir uygulamada yapısal olarak bulunabilen "custom logic"in belirlenmesinde her zaman kesin doğru sonuç vermez. Bir test uzmanı hedef sistemin kullanılabilir olan servislerini ve bu servisler için fonksiyonellik sağlayan uygulamaları manuel olarak değerlendirmek suretiyle, hedef sistemin doğrulamasının ve açıklık tanımlamasının uygun bir şekilde yapılmasını sağlayabilir.

## 4.5 Araştırma

#### Kamu araştırması

Hedef sistemde bir açıklık rapor edildiğinde, açıklık hususunun tanımlamasının doğru yapıldığının belirlenmesi ve sızma testi kapsamında bu açıklığın istismar edilebilme potansiyelinin araştırılması gerekir. Çoğu durumda raporlanan açıklık, ticari veya açık kaynak bir yazılım paketindeki yazılım açıklıktır. Diğer durumlarda ise raporlanan açıklık, iş prosesindeki bir hata veya yanlış konfigürasyon veya varsayılan parolaların kullanılması gibi yaygın bir idari hatadır.

**Açıklık veri tabanları**

Açıklık veri tabanları, otomatikleştirilmiş bir araç tarafından raporlanan bir hususun teyit edilmesinde veya hedef uygulamadaki açıklığın manuel olarak kontrol edilmesinde kullanılabilir. Çoğu araç söz konusu bir açıklık için özet bilgilere veya CVE veri tabanındaki diğer kaynaklara bağlantı veren linklere erişim için kullanılabilen CVE belirleyicisini kullanır. CVE aynı zamanda OSVDB ve Bugtraq gibi açıklık veri tabanlarındaki veya istismar veri tabanlarındaki ve çerçevelerindeki hususları araştırmak için de kullanılabilir.

Açıklık veri tabanları rapor edilen bir hususun doğruluğunu teyit etmek için kullanılabilir. Örneğin, Windows'ta bir Apache Web sunucusu hatası bulunabilir, fakat aynı hata Linux'ta bulunmayabilir. Bu durum otomatikleştirilmiş bir tarayıcı tarafından dikkate alınmayabilir.

**Satıcı önerileri**

Satıcı tarafından yayınlanan güvenlik önerileri ve değişim günlükleri herhangi bir otomatikleştirilmiş araç tarafından raporlanmayan açıklık bilgilerine yönelik işaretler verebilir. Çoğu ana yazılımın satıcıları, dahili olarak tespit ettikleri hususlar ve bir açıklığın ortaya çıkarılması için bağımsız bir araştırmacıyla işbirliği yapıkları durumlarındaki hususlar hakkında sınırlı bilgiler verirler. Araştırmacı açıklığın detayları hakkında sessiz kalmayı tercih ederse bu durumda satıcı tavsiyeleri genellikle kullanılabilir olacak tek veri olur. Başka araştırmacılar da bağımsız olarak daha fazla detay tespit edebilir ve bu detayları açıklık veri tabanlarına ilave edebilirler. Bir satıcı önerisinde kullanılan CVE'nin araştırılması, potansiyel olarak istismar edilebilir bir husus hakkında daha fazla detayı ortaya çıkarabilir.

Değişim günlükleri, sürümler arasındaki farklılıkların sabit olan ancak yaygın olarak bilinmeyen bir açıklığı gösterdiği (bunun sonucu olarak belki de yükseltme veya kurulum için ayrıcalık tanınmamış olan), özellikle açık kaynak ürünlerindeki ilave araştırmalar için kılavuzluk sağlar.

**İstismar veri tabanları ve çerçeve modülleri**

Çoğu istismar veri tabanları aktif olarak tutulmaktadır ve İnternette herkesin erişimine açıktır. Güvenlik araştırmacıları ve istismar yazarları istismar kodlarını her zaman çok sayıda Web sitesine vermezler. Bu nedenle birkaç Web sitesine aşina olunması ve potansiyel olarak istismara karşı hassas olan uygulamalara karşı kullanılmak üzere bu sitelerin her birinde istismar kodu kontrolü yapılması tavsiye edilmektedir. Bazı açıklık veri tabanları kullanılabilecek olan istismarları takip etse de kapsadıkları alan genellikle tam değildir ve eksiksiz oldukları düşünülmemelidir.

Ticari ve açık kaynak istismar çerçevelerinin de açıklıkların araştırılmasında kullanışlı oldukları kanıtlanmıştır. Çoğu durumda kullanılabilir istismar modülleri herkese açık olan Web sitelerinde listelenmektedir ve bir konunun istismar edilebilirliği bakımından değerli bir gösterge olabilir.

**Yaygın olarak kullanılan/varsayılan parolalar**

Yöneticiler ve teknisyenler genelde zayıf parolalar seçerler, varsayılan parolaları hiç değiştirmezler veya hiç parola kullanmazlar. Çoğu yazılım ve donanım ait kullanma kılavuzları çevrimiçi olarak kolaylıkla bulunabilir ve bu kılavuzlarda varsayılan yetki bilgileri verilebilir. İnternetteki forumlardan ve resmi satıcı e-posta listelerinden belgelenmemiş hesap bilgileri, yaygın olarak kullanılan parolalar ve sıklıkla yanlış olarak konfigüre edilen hesaplar elde edilebilir. Nihayet, çoğu Web sitesinde varsayılan/sisteme izinsiz erişim giriş parolaları yazılmaktadır ve tanımlanan her sistem için bu parolalar kontrol edilmelidir.

### Güçlendirme kılavuzları / Yaygın olan hatalı konfigürasyonlar

Sızma testinin esas amaçlarından birisi de gerçek bir saldırganın taktiklerinin ve davranışlarının simüle edilmesidir. Otomatikleştirilmiş taramalar bir test için gereken zamanı kısaltsa da hiçbir tarayıcı bir insan gibi davranamaz. Güçlendirme kılavuzları bir sızma testi uzmanı için çok değeli bir referans olabilir. Güçlendirme kılavuzları sadece bir sistemin en zayıf taraflarını vurgulamaz, aynı zamanda kaç adet önerinin uygulanmış olduğunu teyit etmek suretiyle, bir yöneticinin ne kadar dikkatli ve tedbirli olduğu hakkında bir fikir sahibi olursunuz. Her sızma testi sırasında, yönetici tarafından mevcut olarak bırakılan açıklıkları tespit etmek maksadıyla her ana sistem ve bu sisteme yönelik olarak önerilen güçlendirme ayarlarının gözden geçirilmesine zaman harcanmalıdır.

Kullanıcı forumları ve e-posta listeleri sistemler ve yöneticilerin bu sistemleri konfigüre ederken ve güvenliğini sağlarken yaşadıkları çeşitli hususlar hakkında önemli bilgiler sağlayabilir. Bir sızma testi uzmanı kendisi sanki bir sistem kuracakmış gibi sistemleri araştırmalı ve baş ağrıtabilecek noktaların ve muhtemel konfigürasyon hatalarının nerelerde yattığını keşfetmelidir.

### Özel araştırma

#### Tıpatıp bir ortamın kurulması

Sanallaştırma teknolojileri bir güvenlik araştırmacısının geniş bir çeşitlilikteki işletim sistemlerini ve uygulamalarını bunlar için atanmış bir donanım olmaksızın çalıştırmasına olanak sağlamaktadır. Hedef bir işletim sistemi veya uygulaması tanımlandığında hedefi taklit etmek için hızlı bir şekilde sanal bir makine ortamı yaratılabilir. Test uzmanı konfigürasyon parametrelerini ve uygulamalarının çalışma davranışlarını keşfetmek için hedefe doğrudan bağlanmaksızın, bu sanal makineyi kullanır.

#### Test konfigürasyonları

Sanal bir test makinesi Windows XP, Vista, 7, Server 2003 and Server 2008, Debian, Ubuntu, Red Hat ve mümkünse Mac OS X dahil olmak üzere, yaygın olarak kullanılan tüm işletim sistemleri için temel imajları içermelidir. Her bir servis paketi düzeyi için ayrı imajların tutulması hedef ortamının yeniden yaratılmasını kolaylaştırır. Klonlamayı destekleyen, sanal makine ortamıyla kombinasyon halindeki tam bir sanal makine kitaplığı test uzmanının dakikalar içerisinde yeni sanal makine hedefleri geliştirmesine olanak sağlar. İlave olarak anlık ekran görüntüsü alma özelliği daha etkin olarak çalışma ve program hatalarının aynısını üretme olanağı sağlar.

### Fuzzing

Fuzzing ya da hata enjeksiyonu, uygulamalara programlanabilir biçimde geçerli, rastgele veya beklenmeyen girdiler göndermek suretiyle, uygulamanın kusurlarını bulmak için yapılan bir brute force saldırısı tekniğidir. Temel proses hedef uygulamaya bir hata ayıklayıcı eklemek ve daha sonra belirli girdi alanlarına yönelik olarak fuzzing program parçacıklarını çalıştırmak ve herhangi bir çökme olup olmadığını takip etmek suretiyle programın durumunu analiz etmektir. Bazı test uzmanları belirli hedefler için kendi fuzzing uygulamalarını yazsalar da fuzzing uygulamalarının çoğu erişilebilirdir.

### Potansiyel saldırı kulvarlarının / vektörlerinin belirlenmesi

Komutları veya diğer girdi alanlarını belirlemek için hedef ağ uygulamasında oturum açılmalı veya ağa bağlanılmalıdır. Hedef dosyaları ve/veya Web sayfalarını okuyan masaüstü bir uygulamaysa, veri girişi kulvarları için kabul edilir olan dosya biçimleri analiz edilmelidir. Bazı basit testler bir çökme yaratmak için geçersiz karakterlerin veya uzun karakter dizileri girilmesini içerir. Başarılı olan bir çökme durumunda programın durumunu analiz etmek için bir hata ayıklayıcı eklenmelidir.

**Kodlarına ayırma ve kod analizi**

Bazı programlama dilleri, makine dilinin kaynak koduna dönüştürülmesine olanak tanır ve bazı belirli uygulamalar hata ayıklama için sembollerle derlenir. Bir sızma testi uzmanı program akışını analiz etmek ve potansiyel açıklıkları belirlemek için bu özelliklerden faydalanabilir. Açık kaynak uygulamalarda kaynak kodu hatalara yönelik olarak analiz edilmelidir. PHP'de yazılan Web uygulamaları aynı açıklıkların çoğunu paylaşmaktadır ve bu Web sayfalarının kaynak kodları sızma testinin bir bölümü olarak incelenmelidir.

# 5. İstismar etme

## 5.1 Maksat

Bir sızma testinin istismar safhası sadece güvenlik kısıtlamalarını baypas etmek suretiyle bir sisteme veya kaynağa erişim sağlamaya odaklıdır. Daha önceki safha olan açıklık analizi uygun bir şekilde gerçekleştirildiyse, bu aşama iyi planlanmış ve tam isabetli olabilir. Odaklanılan esas husus kuruluşa asıl giriş noktasının ve yüksek değerdeki hedef varlıkların belirlenmesidir.

Açıklık analizi safhası uygun bir şekilde tamamlandıysa, bir kritik hedef listesi derlenmiş olmalıdır. Sonuç olarak, saldırı vektörü başarı ihtimalini ve kuruluş üzerinde en yüksek etkiyi dikkate almalıdır.

## 5.2 Karşı tedbirler

Karşı tedbirler bir istismar kulvarının başarılı olarak teşkil edilmesi yeteneğini engelleyen koruyucu teknoloji veya denetimler olarak tanımlanır. Bu teknoloji makineye kurulu olan sisteme izinsiz girişleri engelleme sistemi, güvenlik muhafızı, Web uygulaması güvenlik duvarı veya diğer koruyucu yöntemler olabilir. Bir istismarın gerçekleştirilmesinde birkaç faktör dikkate alınmalıdır. Koruyucu bir teknolojinin varlığı durumunda bir aldatma tekniği dikkate alınmalıdır. Bunun mümkün olmadığı durumlarda alternatif istismar yöntemleri dikkate alınmalıdır.

Genel olarak amaç, kuruluşa saldırı gerçekleştirirken gizli kalmaktır. Alarmlar harekete geçirilirse değerlendirmenin düzeyi azaltılabilir. Eğer mümkünse, istismarın başlatılmasından önce karşı tedbirler sıralanmalıdır. Bu işlem saldırı provalarının yapılması veya teknolojilerin listelenmesi ile yapılabilir.

**Anti-virüs**

Anti-virüs sisteme zararlı yazılımların yerleştirilmesini önlemeyi amaçlayan bir teknolojidir. Bir sızma testi uzmanı bu tür anti-virüs teknolojilerini belirleyebilmeli ve bunlardan sakınabilmelidir. Anti-virüs mevcut olabilecek tüm farklı koruyucu tedbirlerin (örneğin, makineye kurulu izinsiz girişleri engelleme sistemi, Web uygulaması güvenlik duvarları ve diğer koruyucu teknolojiler) küçük bir alt kümesidir.

**Kodlama**

Kodlama, uygulanan kod parçasının verilerle aynı şekilde görünmemesini sağlayacak şekilde verilerin gizlenmesi yöntemidir. Kodlamada gizleme genellikle uygulamanın gerçekte ne yaptığının gizlenmesi maksadıyla bilgilerin karıştırılması ve yeniden düzenlenmesi suretiyle yapılır.

### Sıkıştırma

Sıkıştırma, uygulamayı sıkıştırmak için verilerin yeniden düzenlenmesi bakımından kodlamanın benzeridir. Bundan umulan, verilen çalıştırılabilir bir kodun veya bir kod parçacığının herhangi bir anti-virüs teknolojisi tarafından alınamayacak bir biçimde gizlenmesidir.

### Şifreleme

Şifreleme, kodlama ve sıkıştırma gibi, hedeflenen çalıştırılabilir kodun tanınamayacak veya incelenmek üzere kullanılamayacak bir biçimde manipüle edilmesinin başka bir yöntemidir. Sadece hafızada şifrenin çözülmesinden (sıkıştırmaya benzer yöntemlerle) sonra, ve tercihen güvenlik mekanizmalarının buna izin vermesinden sonra gerçek kod ilk olarak ortaya çıkar ve şifresinin çözülmesinden sonra hemen uygulanır.

### Güvenli adresler listesinin baypas edilmesi

Güvenli adresler listesi teknolojileri belirli bir sistemde genelde görülen uygulamalar için güvenli bir model geliştirmiştir. Teknoloji, sistemin ana hatlarını çıkarır ve sistemde neyin çalıştırılmasının normal olduğunu ve buna karşın sistem için neyin yabancı olduğunu belirler. Sızma testi uzmanı güvenli adresler listesi teknolojilerini atlatabilmelidir. En yaygın olan yöntemlerden birisi doğrudan belleğe erişimdir. Güvenli adresler listesi teknolojilerinin gerçek zamanlı olarak hafızayı izleme yeteneği yoktur ve bellekte yerleşik olan bir program çalışıyorsa ve diskle teması yoksa, program söz konusu teknoloji tarafından tespit edilmeksizin çalışabilir.

### Proses enjeksiyonu

Proses enjeksiyonu basit olarak zaten çalışmakta olan bir prosese enjeksiyonda bulunma yöntemidir. Bir prosese enjeksiyonda bulunmak suretiyle uygulama bilgileri normalde doğası gereği güvenilir olan bir prosesin içerisine saklanabilir. Koruyucu tedbir teknolojisinin çalışmakta olan prosesleri denetlemesi çok güçtür ve her durumda, çalışmakta olan proses, uygulamanın güvenilir olduğunu düşündüğü başka bir proses içerisine saklanabilir.

### Tamamen bellekte yerleşik saldırılar

Bellekte yerleşik saldırılar çoğu teknolojiler belleği denetleyemediğinden genelde en çok tercih edilen saldırılardır. Bir saldırgan olarak bellekte yaşamanın bir yolunu bulmak en çok istenen durumdur. Çoğu uygulamalar diske kayıt yaparken potansiyel olarak zararlı yazılımlara yönelik olarak taramalar, ana hatların çıkarılması ve diğer kimlik saptama uygulamalarını icra eder. Diske kayıt yaparken tespit edilme olasılığı çok daha büyük olur.

### İnsan

Bir istismar gerçekleştirmede doğrudan bir istismar veya uygulama hatası üzerinden gitmek her zaman en iyi yol değildir. Bazen insan öğesi bir kuruluşa yönelik saldırı icra etmenin daha iyi bir yolu olabilir.

Doğru saldırı kulvarının bilinmesi ve geliştirmekte olduğumuz yöntemin takip edilecek en iyi yol olduğundan emin olmamız önemlidir.

### Veri uygulamasının önlenmesi

Bir istismarın icra edilmesinde çok sayıda koruyucu tedbir ön plana çıkar. Veri uygulanmasının önlenmesi çoğu işletim sistemlerinde uygulanmakta olan savunmaya yönelik bir tedbirdir ve bellekte bir üzerine yazma durumu ortaya çıktığında bunun uygulanması önler. Veri uygulanmasının önlenmesinin ardındaki düşünce bir saldırganın belleğe yeniden kayıt yapmasını ve daha sonra bu kodu uygulamasını engellemektir. Veri uygulanmasının önlenmesini baypas etmek için birkaç yöntem mevcuttur ve daha ileride sızma testinin istismar safhasında açıklanmaktadır.

### Adres boşluğu düzeninin rastgele hale getirilmesi

Bir arabellek aşımı açıklığı esnasında (veya belleği denetlediğimiz herhangi bir açıklıkta) bellek adresleri uygulama akışının kabuk kodumuza yönlendirilmesi maksadıyla belleğin içine gömülü olarak kodlanmışlardır. Adres boşluğu düzeninin rastgele hale getirmek suretiyle, bir saldırganın kabuk kodu çalıştırmak için her zaman nereye gidebileceğini kestirmesini önlemek için belirli baytlar rastgele hale getirilir.

### Web uygulaması güvenlik duvarı

Web uygulaması güvenlik duvarları Web tabanlı uygulama saldırılarına karşı korunmak maksadıyla bir uygulama ile aynı hatta bulunan bir teknolojidir. Web uygulaması güvenlik duvarları belirli bir Web uygulamasına yönelik potansiyel olarak tehlikeli veya bozucu saldırıları belirlemeye ve Web uygulamasını bunlardan korumaya çalışır. Web uygulaması güvenlik duvarlarının baypas edilmesi için birkaç teknik mevcuttur ve sızma testi esnasında bu teknikler denenmelidir.

## 5.3 Kaçınma

Kaçınma, bir sızma testi esnasında tespit edilmekten kaçınmak maksadıyla kullanılan bir tekniktir. Bu teknikler güvenlik görevlileri tarafından görülmemek için bir kamera sisteminin atlatılması, izinsiz girişleri tespit veya engelleme sistemlerinden kurtulmak maksadıyla veri yüklerinizin gizlenmesi veya Web uygulaması güvenlik duvarlarının atlatılması maksadıyla isteklerin/yanıtların kodlanması olabilir. Genel olarak bir teknoloji veya bir kişiden kaçınılması için düşük riskli bir senaryonun belirlenmesi ihtiyacı istismar öncesinde formüle edilmelidir.

## 5.4 İsabet doğruluğu

Bir sızma testinin odaklandığı esas nokta kuruluşa yönelik olarak simule edilmiş bir saldırının gösterilmesi maksadıyla bir saldırganın simule edilmesidir. Bir sızma testinin sağladığı değer genelde doğası gereği saldırıların gürültülü olduğu dağıtma veya zorla gasp etme teknikleri aracılığıyla ve her istismarın denenmesi yoluyla elde edilmez. Bu yaklaşım belki sızma testinin sonunda kuruluşun olaylara verdiği yanıtın ölçülmesi girişiminde faydalı olabilir ancak çoğu durumda istismar safhası hedefe yönelik spesifik araştırmaların bir birikimidir.

## 5.5 İsteğe göre uyarlanmış istismar kulvarı

İstismar kulvarının gerçekleşmesi bakımından her saldırı tipik olarak aynı olmayacaktır. Bu safhada başarılı olmak maksadıyla saldırı senaryoya dayalı olarak uyarlanmış ve isteğe bağlı olarak düzenleniş olmalıdır. Örneğin, kablosuz olarak bir sızma testi gerçekleştiriliyorsa ve belirli bir teknoloji kullanımdaysa bu teknolojilerin belirlenmesi ve mevcut olan bu teknolojilere dayalı olarak saldırının icra edilmesi gerekir. Her bir senaryonun ve istismarın uygulanabilirliğinin tam olarak anlaşılması sızma testinin bu safhasının en önemli hususlarından biridir.

## 5.6 Uygun hale getirilmiş istismarlar

Çoğu durumda İnternette herkesin erişimine açık olan istismarların başarılı olarak gerçekleştirilmesi maksadıyla bazı düzenlemelerin yapılması gerekir. Çoğu durumda, bir istismar Windows XP SP2 için geliştirilmişse, Windows XP SP3 aracılığıyla yapılacak bir saldırının başarılı olması için istismarda belirli modifikasyonların yapılması gerekir. Sızma testi uzmanı bir istismarı isteğe göre uyarlayabilmek için gereken bilgiye ve saldırıyı başarılı bir şekilde gerçekleştirmek maksadıyla anında değişiklik yapma yeteneğine sahip olmalıdır.

## 5.7 İstismarın isteğe göre uyarlanması

Bir saldırı durumunda istismar safhasının başarılı olmasını sağlamak maksadıyla saldırının mağdurunun altyapısının simule edilmesi gerekir. Bilgi toplama safhasında geliştirilen teknikler her zaman yardımcı olur ancak çalışma altyapısının ve mevcut sistemlerin bilinmesi istismar safhasını çok daha kolaylaştıracaktır. Uygun hale getirilmiş istismarla ilgili olarak, sızma testi uzmanı bir sisteme başarılı bir saldırıda bulunabilmek maksadıyla herkese açık olan istismarları kendi isteğine göre uyarlayabilmelidir. İstismarlar için yaygın olan bir husus, işletim sistemlerinin ve uygulamaların belirli sürümlerinin hedeflenmesidir. Bunun nedeni servis paketlerine ve/veya işletim sisteminin yeni sürümlerine bağlı olarak bellek adreslerinin değişmesidir. Sızma testi uzmanı farklı işletim sistemlerinde kullanmak ve sistemi başarılı bir şekilde ele geçirmek için bu istismarları kendine göre uyarlayabilmelidir.

## 5.8 Sıfırıncı gün

Çoğu zaman sıfırıncı gün saldırısı bir sızma testi uzmanının başvuracağı son şeydir. Bu tür bir saldırı genellikle bir kuruluşa yönelik olarak normal saldırı yöntemleriyle odaklanmış bir saldırı gerçekleştirebilme becerisindeki üst düzeyde gelişmiş bir kuruluşu işaret eder. Bazı özel durumlarda tersine mühendislik, fuzzing veya keşfedilmemiş olan ileri derecede açıklıkların keşfedilmesi maksadıyla araştırma yapılabilir. Bu tür bir saldırının uygulanabilir olduğu durumlarda, karşı tedbir teknolojilerinin olaya katılmasını sağlamak için ortamın saldırganın bilgisi dahilinde yeniden yaratılması sağlanmalıdır.

Sıfırıncı gün istismarlarında aynı işletim sistemi, yamalar ve karşı tedbirlere sahip olunması başarı bakımından çok önemlidir. Bazen bu bilgiler erişimin düzeyine veya gerçekleşen sıralamaya bağlı olarak kullanılabilir olmayabilir.

## Fuzzing

Fuzzing bir protokol veya uygulamanın canlandırılması ve uygulamaya bir açıklığı tespit etme niyetiyle veri gönderme girişiminde bulunulması yeteneğidir. Çoğu zaman test uzmanının beklentisi, uygulamada bir çökme belirlemek ve buradan belirli bir istismar yaratmaktır. Fuzzing olayında saldırgan daha önce keşfedilmemiş olan bir şeyden belirli bir açıklık yaratmaya çalışır. Sızma testi esnasında herhangi bir saldırı kulvarı belirlenememişse veya sızma testi sıfırıncı gün araştırması gerektiriyorsa fuzzing teknikleri potansiyel olarak hassas olan zayıflıkların belirlenmesinde sızma testinin bir parçası olarak kullanılabilir.

## Kaynak kodu analizi

Kaynak kodu kullanılabilir durumdaysa veya açık kaynak olarak erişilebiliyorsa sızma testi uzmanının eline kullanılabilir olan başka saldırı kulvarları geçer. Test uzmanı kaynak koduna bakma ve uygulamaların içerisindeki hataları belirleme yeteneğine sahipse bu yöntemler aracılığıyla sıfırıncı gün zayıflıklarını da belirleyebilir.

## İstismarların türleri

Bir sızma testi esnasında belirlenebilen, sıfırıncı gün olarak kategorilendirilebilecek birkaç tür istismar mevcuttur. Bunlardan bazıları bu bölümde listelenmektedir.

## Arabellek aşımları

Arabellek aşımları uygun olmayan kodlama tekniklerine bağlı olarak gerçekleşir. Bu durum özellikle bir program bir arabelleğe veri kaydettiğinde ve daha sonra arabelleğin sınırlarını aştığında ve bellek bölümlerinin üzerine yazmaya başladığında ortaya çıkar. Arabellek aşımı istismarlarında saldırganların amacı bir çökmeyi beklemek ve söz konusu sistem üzerinde kod uygulama ayrıcalığını elde etmektir. Bir arabellek aşımı istismarında yaygın olan tekniklerden birisi de belirli bir kaydın üzerine yazmak ve kabuk koda atlamaktır.

## Yapısal özel durum işlemesi üzerine yazma

Yapısal özel durum işlemesinin üzerine yazma, yapısal özel durum işleyicinin bir uygulamayı kapatmaya başlamasıyla ortaya çıkar. Saldırgan yapısal özel durum işlemesinin çalışma şeklini manipüle edebilir, yapısal özel durum işleyicinin esas adresinin üzerine yazabilir ve yapısal özel durum işlemesi aracılığıyla uygulama akışının denetimini elde edebilir. Bu durum arabellek aşımı açıklığı ve yapısal özel durum işlemesiyle uyumlu uygulamalarla güçlendirilen yaygın bir saldırıdır.

## Geriye dönüşe yönelik programlama

Geriye dönüşe yönelik programlama kullanıcının uygulama akışı üzerinde denetimi olduğu, ancak veri uygulamasının önlenmesi veya diğer önleyici savunma mekanizmalarının mevcut olabildiği bölümler esnasında kullanılan bir tekniktir. Veri uygulamasının önlenmesinin etkinleştirildiği durumlarda saldırganın belirli kurgu talimatlarını uygulamak için doğrudan erişimi bulunmaz ve bu nedenle

saldırgan belirli Windows API çağrılarına veya veri uygulamasının önlenmesini devre dışı bırakma veya atlatma tekniklerine hazırlanmak maksadıyla geriye dönüşe yönelik bir programlama aygıtı yapılandırır.

### Trafik analizi

Trafik analizi ne tür bilgilerin gönderildiğinin belirlenmesi ve bu trafiğin anlaşılması ve manipüle edilmesi yeteneği tekniğidir. Bir sızma testi uzmanı bir protokolün nasıl çalıştığını ve bir saldırının güçlendirilmesi maksadıyla nasıl manipüle edilebileceğini anlayabilmelidir.

### Fiziksel olarak erişim

Bir sızma testi esnasında fiziksel olarak erişim, fiziki güvenlik denetimlerinin atlatılması ve yetki dışı erişim elde edilmesi maksadıyla uygulanabilir bir saldırı yöntemi olabilir. Bir sızma testi esnasında değerlendirici potansiyel olarak hatalı güvenlik denetimlerini belirleyebilmeli ve testin kapsamı dahilinde ise tesise erişim sağlama girişiminde bulunmalıdır.

### İnsan yönü

Bir sızma testi esnasında en belirgin olan yollardan bazıları tesise yönelik olarak sosyal mühendislik yapılması ve erişim elde edilmesi olabilir. Bu, kuruluşun ne şekilde iş yaptığı hakkında önemli ölçüde bilgi ve istihbarat toplama safhasından öğrendiğiniz her şeyi gerektirir.

### Bilgisayar erişimi

Fiziki erişim bir bilgisayara bırakılmışsa sızma testi uzmanı bu bilgisayara saldırı icra edebilmeli ve sisteme erişime olanak sağlayabilen birkaç yöntem aracılığıyla erişim sağlamalıdır.

### Yakın erişim (wifi)

Kablosuz iletişim radyo frekans türü iletişim aracılığıyla erişim elde etmeye yönelik saldırılar için bir kulvardır. Sızma testi uzmanı hedefin kullanımda olan spektrum frekanslarına kayıtlı olup olmadığını görmek için radyo frekans listesini gözden geçirmelidir.

### WİFİ saldırıları

Protokole bakılmaksızın WEP, WPA, WPA2, EAP-FAST, EAP-LEAP ve diğer kulvarlarda çok sayıda saldırı mümkündür. Saldırgan çeşitli şifreleme protokollerine ve standartlarına aşina olmalı ve devreye sokulan denetimlerin çevresinde uygulamayı etkin bir şekilde test edebilmelidir.

### Kullanıcıya saldırı

Hedefe saldırı için hileli erişim noktalarından faydalanılması genellikle faydalı ve uygulanabilir bir saldırı yöntemidir. İstismarları güçlendirmek veya hassas bilgileri çalmak maksadıyla hedefi kandırmak için hileli bir erişim noktasından faydalanılması kablosuz bir değerlendirme esnasında icra edilmelidir.

Bunun için yaygın olarak kullanılan birkaç teknik mevcuttur ancak en yaygın olanı saldırganın aynı isimle veya hedefin bağlanmasını sağlayacak ikna edici bir isimle kablosuz bir erişim noktası kurgulamasıdır.

## 5.9 Örnek saldırı kulvarları

Her durumda saldırılar sızma testinin kapsamı içerisindeki bir senaryoya dayanmalıdır. Aşağıda senaryoya bağlı olarak dikkate alınabilecek birkaç saldırı kulvarının listesi verilmektedir ancak bu liste hiçbir şekilde kapsamlı bir liste değildir.

Web uygulaması saldırıları, sosyal mühendislik, fiziki saldırı kulvarları, belleğe dayalı istismarlar (arabellek/yığın aşımları, bellek bozulmaları, “use-after-free”). İki bağlantı noktası arasındaki bağlantıyı izinsiz izleme, “VLAN Hopping”, USB bellek sürücüsü yerleştirme, tersine mühendislik, sıfırıncı gün saldırıları, kullanıcının şifrelemesine saldırı, grafik işleme biriminin kırılması, trafik analizinin kırılması, “Firewire” yönlendirme protokolleri, çalışanları taklit etme senaryosuyla “phishing”.

Tekrar belirtmek gerekirse bu örnekler sadece kuruluş için uyguladığınız senaryoya bağlı olan saldırı için temel kulvarlardır. Bir sızma testinin değeri yaratıcılığından ve zayıflıkların belirlenmesi ve bu zayıflıkların kusursuz bir biçimde istismar edilmesi yeteneğinden gelmektedir.

## 5.10 Nihai hedef

Sızma testi öncesinde, etkileşim safhasında sızma testinin nihai hedefleri açık ve seçik bir biçimde müşteri kuruluşla görüşülmelidir. İstismar safhasındaki en büyük zorluk kuruluşa tespit edilmeden giriş için en kolay yolunun belirlenmesi ve kuruluşun gelir yaratma kabiliyetinde en büyük etkinin yaratılmasıdır.

Önceki safhaların uygun bir şekilde icra edilmesiyle kuruluşun nasıl çalıştığı ve para kazandığı nispeten açık bir şekilde anlaşılabilir. Kuruluşun kendisine yönelik bir saldırı ile uğrayacağı önemli ölçüdeki kayıplara nasıl dayanabildiğini göstermek maksadıyla istismar safhasından istismar sonrası safhasına kadar saldırı vektörleri sadece güvenlik denetimlerinin atlatılması görevine dayanmalıdır.

# 6. İstismar sonrası

## 6.1 Maksat

İstismar sonrası safhasının amacı ele geçirilen bilgisayarın değerinin belirlenmesi ve bilgisayarın daha sonra kullanmak üzere denetiminin sürdürülmesidir. Bilgisayarın değeri bu bilgisayar üzerinde saklanmakta olan verilerin hassaslığı ve bilgisayarın ağın ele geçirilmesi safhasında sağlayacağı fayda ile belirlenir. Bu safhada tarif edilen yöntemler test uzmanına hassas verilerin belirlenmesi ve belgelenmesinde, konfigürasyon ayarlarının, iletişim kanallarının ve ağa daha ileri erişim elde etmek için kullanılabilecek olan diğer ağ aygıtlarıyla ilişkilerin belirlenmesinde ve daha sonraki bir zamanda bilgisayara erişimde kullanılabilecek bir ya da daha fazla yöntemin kurulmasında yardımcı olmayı amaçlar. Bu yöntemlerin üzerinde anlaşılan angajman kurallarından farklı olması durumunda angajman kurallarına uyulmalıdır.

## 6.2 Angajman kuralları

Aşağıda belirtilen angajman kuralları bir sızma testinin istismar sonrası safhasına özeldir ve müşteri kuruluşun sisteminin test uzmanlarının eylemleriyle (doğrudan veya dolaylı) gereksiz risklere maruz kalmamasını sağlamayı ve projenin istismar sonrası safhasında karşılıklı olarak üzerinde anlaşılan bir prosedürün takip edilmesinin sağlanmasını amaçlamaktadır.

### Müşteri kuruluşun korunması

Aşağıdaki kurallar günlük faaliyetlerin ve müşteri kuruluşun verilerinin riske maruz bırakılmaması için müşteri kuruluşla karşılıklı olarak oluşturulacak bir kurallar kılavuzu olarak kullanılmalıdır:

- Önceden üzerinde anlaşılmadığı sürece müşteri kuruluşun kendi altyapısı bakımından kritik olarak gördüğü servislerde hiçbir modifikasyon yapılmamalıdır. Bu gibi servislerde yapılacak modifikasyonların maksadı müşteri kuruluşa bir saldırganın ne şekilde:
  - Ayrıcalıklarını yükseltebileceğini,
  - Belirli verilere erişim elde edebileceğini,
  - Hizmet dışı kalmaya neden olabileceğini göstermektir.
- Konfigürasyon değişiklikleri dahil olmak üzere sisteme yönelik olarak uygulanan bütün modifikasyonlar belgeye dökülmelidir. Modifikasyonun amaçlanan maksadına ulaşılmasından sonra mümkünse tüm ayarlar orijinal durumlarına döndürülmelidir. Sızma testi sonrasında değişikliklerin bir listesi, tüm değişikliklerin geriye döndürüldüğünü görmelerine olanak sağlamak maksadıyla müşteri kuruluşa verilmelidir. Orijinal durumlarına döndürülemeyen değişiklikler, başarılı bir şekilde orijinal durumuna döndürülen değişikliklerden açık bir şekilde ayrılmalıdır.
- Ele geçirilen sisteme yönelik olarak atılan adımların ayrıntılı bir listesi muhafaza edilmelidir. Listede atılan adım ve bunun gerçekleştiği zaman dilimi içerilmelidir. Sızma testi tamamlandıktan sonra bu liste nihai rapora bir ek olarak dahil edilmelidir.
- Sızma testi esnasında açığa çıkarılan herhangi bir özel ve/veya kişisel veri (parolalar ve sistem geçmişi dahil) sadece aşağıdaki durumlarda daha geniş kapsamlı izinler elde etmek veya testle ilgili diğer eylemleri uygulamak maksadıyla bir kaldıraç olarak kullanılabilir:
  - Kabul edilebilir kullanım politikası müşteri kuruluş tarafından sahip olunan tüm sistemlerin ve bu sistemlerde saklanmakta olan tüm verilerin müşteri kuruluşun mülkiyetinde olduğunu belirtmektedir.
  - Kabul edilebilir kullanım politikası müşteri kuruluşun ağına yapılacak bağlantının, bağlanılan bilgisayarda arama ve analiz (mevcut tüm veriler ve konfigürasyonlar dahil) yapmak için bir izin olarak değerlendirileceğini belirtmektedir.
  - Müşteri kuruluş tüm çalışanların kabul edilebilir kullanım politikasını okuyup anladıklarına dair teyidi almıştır.
- Parolalar (şifrelenmiş biçimleri dahil) nihai raporda bulunmayacaktır ya da raporun alıcılarının parolaları yeniden yaratamayacakları veya parolaları tahmin edemeyecekleri ölçüde maskelenmelidir. Bu işlem parolaların ait olduğu kullanıcıların gizliliğinin korunması ve aynı zamanda parolalarla korunan sistemlerin bütünlüğünün muhafaza edilmesi maksadıyla yapılmaktadır.

- Ele geçirilen sisteme erişimi sürdürmek maksadıyla kullanılan, sistemin düzgün çalışmasını etkileyebilecek olan herhangi bir yöntem ya da cihaz veya sistemden çıkarılması sistemde aksaklık nedeniyle durmaya neden olabilecek herhangi bir yöntem ya da cihaz müşteri kuruluşun önceden alınmış yazılı izni olmaksızın uygulanmamalıdır.
- Ele geçirilen sistemlere erişimi sürdürmek maksadıyla kullanılan herhangi bir yöntem ya da cihazda sayısal sertifikalar veya giriş komutları gibi bir kullanıcı kimlik sorgulama biçimi kullanılmalıdır.
- Test uzmanları tarafından toplanan tüm veriler test uzmanları tarafından kullanılan sistemlerde şifrelenmelidir.
- Rapora dahil edilen, hassas veri (anlık ekran görüntüleri, tablolar, rakamlar) içeren tüm bilgiler veriyi kalıcı olarak kurtarılamayacak duruma getiren teknikler kullanılmak suretiyle sterilize edilmeli veya maskelenmelidir.
- Müşteri kuruluş nihai raporu kabul eder etmez toplanan tüm veriler yok edilecektir. Verilerin yok edilmesinde kullanılan yöntem ve kanıtlar müşteri kuruluşa verilecektir.
- Toplanan veriler herhangi bir kanun gereği düzenlenmekteyse, toplanan ve işlenen verilerin uygulamada olan herhangi bir kanunu ihlal etmemesini garantiye almak için müşteri kuruluş tarafından kullanılan sistemler ve bu sistemlerin lokasyonları verilmelidir. Sistemler test uzmanları tarafından kullanılan sistemler olacaksa veriler bu sistemler indirilmeyebilir ve saklanmayabilir. Sadece erişildiğinin kanıtları gösterilir (dosya izinleri, kayıt sayısı, dosya isimleri vb.).
- Müşteri kuruluştan önceden alınmış bir izin olmaksızın, ne şifre kırmada üçüncü taraf hizmeti kullanılır, ne de herhangi bir tür veri üçüncü taraflarla paylaşılır.
- Değerlendirilen ortamda sistemin önceden ele geçirilmiş olduğuna dair bir kanıt bulunursa, sızma testi uzmanlarının değerlendirmesi esnasında kaydedilen tüm günlükler eylemler ve zamanlarıyla birlikte kaydedilir ve müşteri kuruluşa verilir. Müşteri kuruluş daha sonra olaya verilen tepkinin ne kadar iyi olduğunu belirleyebilir.
- Sızma testi sözleşmesi/iş açıklamasında müşteri kuruluş tarafından özellikle yetki verilmedikçe hiçbir günlük çıkarılamaz, silinemez veya değiştirilemez. Yetki verilmişse günlükler herhangi bir değişiklik öncesinde yedeklenmelidir.

## Kendinizin korunması

Sızma testinin doğasına bağlı olarak müşteri kuruluşla ve gerçekleştireceğiniz görevlerle ilgilenirken tüm detayları kapsadığınızdan emin olmalısınız. Herhangi bir çalışmaya başlamadan önce her iki tarafın görev ve sorumluluklarının tam olarak anlaşılmasını sağlamak için müşteri kuruluşla aşağıdaki hususlar görüşülmelidir.

- Müşteri kuruluş ve hizmet sağlayıcı arasında imzalanan sözleşme ve/veya iş açıklaması gereği teste tabi tutulan sistemler üzerinde yürütülen eylemlerin müşteri kuruluşun adına ve onu temsilen yapıldığını kesinleştirin.
- İşe başlamadan önce firmanın sistemlerinin ve altyapısının kullanımını düzenleyen güvenlik prensiplerinin bir suretini elde edin. Prensiplerin aşağıdakileri kapsadığından emin olun:
    - Teçhizatın kişisel kullanımı ve çalışanlara ait kişisel verilerin müşteri kuruluşun sistemlerinde saklanması ve bu veriler üzerindeki mülkiyet ve haklar.
    - Firmaya ait donanımda saklanmakta olan verilerin mülkiyeti.
- Müşteri kuruluş tarafından, müşteri kuruluşun sistemlerinde yönetilen ve kullanılan verileri düzenleyen düzenlemeler ve kanunların teyit edilmesi ve bu gibi verilere uygulanan kısıtlamalar.

- Bu sistemler ve müşteri kuruluşun verilerini alan ve saklayan hareketli ortamlar için diskin tamamının şifrelenmesi işlemini uygulayın.
- Üçüncü bir tarafın sistemi ele geçirme girişimi tespit edildiğinde takip edilecek olan prosedür müşteri kuruluşla görüşülmeli ve geliştirilmelidir.
- Ses ve görüntülerin yakalanması ve/veya saklanması ile ilgili kanunları gözden geçirin. Çünkü istismar sonrasında bunların kullanılması, konuşmaların gizlice dinlenmesiyle ilgili yerel kanunların ihlali olarak değerlendirilebilir.

## 6.3 Altyapı analizi

### Ağ konfigürasyonu

Ele geçirilen bir bilgisayarın ağ konfigürasyonu, ilave alt ağların, ağ yönlendiricilerinin, kritik sunucuların ve bilgisayarlar arasındaki ilişkilerin belirlenmesinde kullanılabilir. Bu bilgiler müşteri kuruluşun ağında daha ileri derecede sızma gerçekleştirmek için ilave hedeflerin belirlenmesinde de kullanılabilir.

### Arayüzler

Bilgisayardaki bütün ağ arayüzlerini, IP numaraları, alt ağ maskeleri ve ağ geçitleri ile birlikte belirleyin. Arayüzlerin ve ayarların belirlenmesi suretiyle ağlar ve servisler hedefleme bakımından önceliklendirilebilirler.

### Yönlendirme

Diğer alt ağlar, filtreleme veya adresleme planları bölümlendirilmiş bir ağdan çıkmak için kaldıraç olarak kullanılabilir. Bu da ilave makinelerin ve/veya ağların araştırılmasına ve sıralanmasına yol açar. Bu gibi veriler belirli bir makineden veya ağdaki aşağıdakileri içeren çeşitli kaynaklardan alınabilir:

- Arayüzler
- Statik ve dinamik yolları içeren yönlendirme tabloları
- Servis ve makine keşfinde kullanılan ARP çizelgeleri, NetBios veya diğer ağ protokolleri.
- Çok merkezli makineler için bu makinelerin bir yönlendirici olarak çalışıp çalışmadıkları belirlenmelidir.

### DNS sunucuları

Makine ayarlarını değerlendirmek suretiyle kullanımda olan tüm DNS sunucularını belirleyin. Daha sonra DNS sunucuları ve bilgileri, hedef ağdaki ilave makine ve servislerin keşfedilmesine yönelik olarak yapılacak olan bir planın geliştirilmesinde ve uygulanmasında kullanılabilir. DNS sunucusunun ele geçirilmesi durumunda DNS veri tabanları makineler ve servisler hakkında, değerlendirmenin geri kalan bölümünde hedeflerin önceliklendirilmesinde kullanılabilecek olan değerli bilgiler sunar. DNS'ye bağlı olarak, servis verilerinin kestirilip yakalanmasında, kayıtların değiştirilmesi veya yeni kayıtların eklenmesi kullanılabilir.

### Ön belleğe atılan girdiler

Ön bellekteki intranet siteleri oturum açma sayfalarını, yönetici arayüzlerini veya dış siteleri içerebilen kritik DNS girdilerini belirleyin. Önbelleklenen arayüzler, ele geçirilen makineler tarafından kullanılan, makinelerin ilişkileri ve etkileşimleri hakkında bir bakış açısı sağlayan, hedef ağ ve altyapıya yönelik daha ileri derecedeki sızmalar için hedeflerin önceliklendirilmesinde kullanabilecek bilgileri sağlayan en yeni ve en çok kullanılan makine bilgilerini verir. Müsaade edildiyse, ön belleğe atılan girdilerin değiştirilmesi, kimlik doğrulama yetki bilgilerinin, kimlik doğrulama işaretlerinin yakalanmasında veya ele geçirilen makineler tarafından kullanılan servisler hakkında hedef ağda daha ileri derecede bir sızma sağlayan daha detaylı bilgilerin elde edilmesinde kullanılabilir.

### Vekil sunucular

Ağ düzeyindeki ve uygulama düzeyindeki vekil sunucularını belirleyin. Vekil sunucuları müşteri kuruluş tarafından kuruluş genelinde kullanılmakta olduğunda iyi bir hedef teşkil eder. Uygulama vekil sunucuları bakımından, trafik akışının veya trafiğin kendisinin belirlenmesi, izlenmesi ve/veya değiştirilmesi mümkün olabilir. Vekil sunucu saldırıları genellikle müşteri kuruluşa etki ve riskin gösterilmesinin etkin bir yoludur.

### ARP (Address Resolution Protocol - adres çözümleme protokolü) girdileri

Ele geçirilen makine ile etkileşime giren diğer makineleri gösterebilen önbelleklenen girdiler ve statik ARP çizelgesi girdileri sıralanmalıdır. Statik ARP girdileri kritik makineleri gösterebilir. Değerlendirmenin kapsamı ARP girdilerini kestirip yakalamaya ve değiştirmeye olanak tanıyorsa, bir servisin bozulma, izlenme veya ele geçirilme ihtimalini genellikle tespit edilemeyen veya engellenemeyen bir tarzda göstermek kolaydır.

### Ağ servisleri

### Dinleme servisleri

Hedef makine tarafından sunulan tüm ağ servisleri belirlenmelidir. Bu başlangıç taraması esnasında tespit edilememiş servislerin keşfedilmesine ve aynı zamanda başka makine ve ağların keşfedilmesine yol açabilir. Taramada gösterilmeyen servislerin belirlenmesi ağ ve/veya makinede uygulanmakta olan filtreleme ve denetim sistemleri hakkında bilgiler de sunabilir. İlave olarak test uzmanı diğer makineleri ele geçirmek için bu servisleri kaldıraç olarak kullanabilir. Çoğu işletim sistemi makineden veya makineye doğru yapılan TCP ve UDP bağlantıları için bir belirleme yöntemi içerir. Ele geçirilen makineden veya makineye doğru yapılan bağlantıların her ikisinin de kontrol edilmesi suretiyle önceden bilinmeyen ilişkilerin bulunması mümkündür. Makinenin yanı sıra servis te dikkate alınmalıdır. Bu standart olmayan portlarda dinleme yapan servisleri gösterebilir ve güvenli kabuk için anahtarsız kimlik sorgulama gibi güvene dayalı ilişkileri belirtebilir.

### Sanal özel ağ bağlantıları

Makineye/ağa ve makineden/ağdan yapılan tüm sanal özel ağ bağlantıları belirlenmelidir. Giden bağlantılar daha önce belirlenmemiş olabilen yeni sistemlere doğru yollar sağlayabilir. Hem gelen,

hem de giden bağlantılar yeni sistemleri ve muhtemel iş ilişkilerini tanımlayabilir. Sanal özel ağ bağlantıları çoğu zaman, şifre çözme veya şifrelenmiş trafiği izleme yetenekleri olmayan güvenlik duvarlarını ve izinsiz giriş tespit/engelleme sistemlerini baypas eder. Bu gerçek sanal özel ağları onlar aracılığıyla saldırı düzenleme bakımından ideal hale getirir. Herhangi bir yeni hedefin, bu hedefe yönelik bir saldırı düzenlenmeden önce kapsam dahilinde olduğunun teyit edilmelidir. Hedef makinede sanal özel ağ istemcisinin veya sunucu bağlantılarının mevcudiyeti önceden bilinmeyen, başka makine ve servislerin hedeflenmesinde kullanılabilecek yetki bilgilerine erişimi de sağlayabilir.

### Dizin servisleri

Hedeflenen bir makinede çalışan dizin servisleri ilave olarak gerçekleştirilecek saldırılarda kullanılabilecek kullanıcı hesaplarının, makinelerin ve/veya servislerin listelenmesi olanağını veya önceden açıklık analizi safhasında keşfedilmemiş olabilen ilave hedefleri sağlayabilir. İlave olarak dizin servislerinde bulunan kullanıcılara ait detaylar sosyal mühendislik ve phishing saldırılarında kullanılabilir ve böylece daha yüksek bir başarı oranı sağlanabilir.

### Komşular

Günümüzdeki ağlardaki birçok servis ve işletim sistemi, servislere erişim, arıza giderme ve konfigürasyonu daha kullanışlı bir hale getirme gayretleri dahilinde komşuların keşfedilmesi maksatlı birkaç protokol kullanır. Bu protokoller hedef makinenin türüne bağlı olarak değişir. Ağ aygıtları kendilerine doğrudan bağlı olan veya aynı alt ağda mevcut bulunan makinelerin sistemleri, konfigürasyonları ve diğer detaylarını belirlemek için CDP ve LLDP gibi protokolleri kullanabilirler. Benzer şekilde masa üstü ve sunucu işletim sistemleri aynı alt ağdaki makineler ve servislerin detaylarını bulmak için mDNS ve NetBios gibi protokolleri kullanabilirler.

## 6.4 Pillaging (soygunculuk)

Pillaging hedeflenen makinelerden değerlendirme öncesi safhasında tanımlanan amaçlarla ilgili bilgileri (kişisel bilgileri içeren dosyalar, kredi kartı bilgileri, parolalar vb.) elde etmek anlamına gelmektedir. Bu bilgiler amaçların karşılanması maksadıyla veya ağa daha ileri düzeyde erişim elde etmek için bir eksen oluşturmanın bir parçası olarak elde edilebilir. Bu bilgilerin yeri verinin türüne, makinenin görevine ve diğer durumlara göre değişir. Çoğu uygulamalar verilerini birçok farklı biçimde ve yerde sakladığından, yaygın olarak kullanılmakta olan uygulamalar, sunucu yazılımı ve aracı yazılımlar hakkında bilgi sahibi olmak ve bunlara temel düzeyde aşina olmak çok önemlidir.

### Kurulu programlar

### Sistem açılış öğeleri

Çoğu sistemler, sistemin açılışında veya kullanıcının oturum açmasında çalışabilen, etkileşime girdiği sistem, yazılım ve servisler hakkında bilgi sağlayabilen uygulamalara sahiptir. Bu bilgiler bir hedef ağın ve bu ağın sistemlerinin daha ileri derecede istismar edilmesini engelleyebilecek muhtemel potansiyel karşı tedbirleri (örneğin, HIDS/HIPS, Güvenilir uygulamalar listesi oluşturulması, FIM) gösterebilir. Toplanması gereken bilgiler aşağıdakileri içerir:

- Sistemde kurulu uygulamaların ve bunlarla ilişkili sürümlerin listesi.

- Sisteme uygulanan işletim sistemi güncellemelerinin listesi.

### Kurulu servisler

Belirli bir makinenin üzerindeki servisler makinenin kendisine veya hedef ağdaki diğer makinelere hizmet eder. Her bir hedef makine için, servislerinin konfigürasyonlarını, makinelerin maksatlarını ve bu makinelerin değerlendirme amaçlarına ulaşılmasında veya ağda daha ileri derecede bir sızma için potansiyel olarak ne şekilde kullanılabileceğini dikkate alan bir profilin yaratılması gereklidir.

### Güvenlik servisleri

Güvenlik sistemleri bir saldırganı sistemlerden uzak tutmak ve verileri güvende tutmak için geliştirilmiş bir yazılım içerir. Bu güvenlik servisleri ağ güvenlik duvarlarını, makineye yerleşik güvenlik duvarlarını, IDS/IPS, HIDS/HIPS ve anti-virüs programlarını içerir, ancak bunlarla sınırlı değildir. Hedeflenen tek bir makinedeki güvenlik servislerinin belirlenmesi ağdaki diğer makineler hedeflendiğinde nelerle karşılaşılabileceği hususunda bir fikir verir. Bu güvenlik servislerinin belirlenmesi aynı zamanda test esnasında hangi alarmların tetiklenebileceği hakkında da bir fikir verir. Bu husus proje hakkında bilgi verme sırasında müşteri kuruluş ile görüşülmelidir. Bu görüşme sonucunda güvenlik politikalarında, UAC, SELinux, IPSec, windows güvenlik şablonları ve diğer güvenlik kuralları/konfigürasyonlarında güncelleme yapılabilir.

### Dosya/Yazıcı paylaşımı

Dosya ve yazıcı sunucuları genellikle hedeflenen verileri içerirler veya hedef ağ ve makinelerde daha ileri derecede sızma fırsatını sağlarlar. Hedeflenmesi gereken bilgiler aşağıdakileri içerir:

- Dosya sunucuları tarafından önerilen paylaşımlar – Hedef sistemler tarafından önerilen herhangi bir dosya paylaşımı incelenmelidir. Paylaşımlardaki sadece isimler ve yorumlar bile iç uygulamalar ve projeler hakkında önemli bilgileri sızdırabilir.
- Paylaşımlar için erişim kontrol listeleri ve izinler – İstemci tarafından gelen paylaşımlarda, paylaşıma bağlanmak mümkünse bu durumda bağlantının salt okunur mu yoksa okuma/yazma şeklinde mi olduğunu görmek için paylaşım kontrol edilmelidir. Unutulmamalıdır ki, bir paylaşım dizinler içeriyorsa, bu durumda farklı dizinlere farklı izinler uygulanabilir. Sunucu tarafından gelen paylaşımlarda, hem sunucunun konfigürasyonu hem de dosya/dizin izinleri incelenmelidir.
- Dosya paylaşım dosyası ve içerik listeleri
- Dosya paylaşım listelerindeki ilgilenilen dosyalar belirlenmelidir. Aşağıdakiler gibi ilginç veya hedeflenen öğelere bakılmalıdır:
    - Kaynak kodu
    - Yedeklemeler
    - Kurulum dosyaları
    - Gizli veriler (hesap tablosu şeklindeki finansal veriler, TXT/PDF formatındaki banka raporları, parola dosyaları vb.)
- Truva atlarının veya otomatik çalıştırma dosyalarının yerleştirilmesi – Akıllı isimlendirmenin kullanılması veya halen kullanımda olan isimlendirme usullerinin taklit edilmesi suretiyle kullanıcılar, test uzmanının ağa daha ileri derecede sızmasına olanak sağlayacak veri yüklerini

uygulamaya cesaretlendirilebilir. Dosya sunucusu günlükleri elde edilebilirse belirli kullanıcılar bile hedeflenebilir.

### Veri tabanı sunucuları

Veri tabanları bir değerlendirmede hedeflenebilecek zengin bilgiler içerirler.

- Veri tabanları – Veri tabanları isim listesi, veri tabanının maksadının ve veri tabanında içerilen verilerin türünün belirlenmesinde değerlendiriciye yardımcı olabilir. Bu, çok sayıda veri tabanının mevcut olduğu bir ortamda hedeflerin önceliklendirilmesinde yardımcı olur.
- Çizelgeler – Çizelge isimleri ve yorumlar, sütun isimleri ve türler gibi meta veriler de değerlendiriciye hedeflerin seçilmesinde ve hedeflenen verilerin bulunmasında yardımcı olur.
- Çizelge içeriği, düzenlenen içerik için satır sayısı
- Sütunlar – Çoğu veri tabanında tüm sütun isimlerinin ve tüm çizelgelerin tek bir komutla aranması mümkündür. Bu hedeflenen verilerin bulunmasında kaldıraç olarak kullanılabilir.
- Veri tabanı ve çizelge izinleri
- Veri tabanı kullanıcıları, parolalar, gruplar ve görevler

Veri tabanlarında bulundurulan bilgiler de riskin gösterilmesi, değerlendirme amaçlarına ulaşılması, servislerin konfigürasyonlarının ve fonksiyonlarının belirlenmesi veya bir müşteri kuruluşun ağı veya makinesine daha ileri derecede sızma için kullanılabilir.

### Dizin sunucuları

Bir dizin servisinin esas amacı servisler ve makineler için referans olarak başvurmak ve/veya kimlik doğrulaması için bilgi sağlamaktır. Bu servisin ele geçirilmesi bu servise dayalı olan tüm makinelerin denetimine olanak sağlar ve aynı zamanda daha sonraki bir saldırıda kullanılabilecek bilgileri sağlar. Bir dizin servisinde aranacak bilgiler aşağıdadır:

- Nesne listeleri (kullanıcılar, parolalar, bilgisayarlar vb.)
- Sistem bağlantıları
- Protokollerin ve güvenlik düzeyinin tanımı

### Ad sunucuları

Ad sunucusu kayıtların türüne bağlı olarak makine ve servislerin çözümlenmesini sağlarlar. Kayıtların ve denetimlerin sıralanması, bir müşteri kuruluşun ağ ve makinelerine daha ileri derecede sızma için önceliklendirilecek ve saldırı yapılacak bir hedefler ve servisler listesi sağlayabilir. Kayıtların değiştirilmesi ve eklenmesi yeteneği hizmet dışı kalma riskini göstermek için ve aynı zamanda bir müşteri kuruluşun ağındaki trafiğin ve bilgilerin kestirilip yakalanmasında yardımcı olarak kullanılabilir.

### Görevlendirme servisleri

Görevlendirme servislerinin tanımlanması aşağıdakilere erişimi ve bunların sıralanmasını sağlar:

- İşletmensiz cevap dosyaları
- Dosyalara yönelik izinler

- Dahil edilen güncellemeler
- Uygulamalar ve sürümler

Bu bilgiler bir müşteri kuruluşun ağ ve makinelerine daha ileri derecede sızma için kullanılabilir. Servisin veri havuzlarının ve konfigürasyonunun değiştirilmesi yeteneği aşağıdakiler için olanak sağlar:

- Sisteme izinsiz erişim kurulumu
- Saldırılara hassas hale getirmek için servislerin modifikasyonu

### Sertifika makamı

Ele geçirilen bir müşteri kuruluş makinesindeki sertifika makamı servislerinin belirlenmesi aşağıdakilere erişime olanak sağlar:

- Kök sertifika makamı
- Kod imzalama sertifikaları
- Şifreleme ve imzalama sertifikaları

Servisin kontrolü aynı zamanda aşağıdakiler için olanak sağlar:

- Birkaç görev için yeni sertifikaların yaratılması
- Sertifikaların iptali
- Sertifika iptal listesinin değiştirilmesi
- Kök sertifika makamı sertifikasının eklenmesi

Servislerin kontrolü riski gösterir ve bir müşteri kuruluşun ağ ve makinelerindeki veriler ve servislerin ele geçirilmesine olanak sağlar.

### Kaynak kodu yönetim sunucusu

Ele geçirilen makinede çalışan servis veya servisin müşteri kuruluş tarafı aracılığıyla kaynak kodu yönetim sistemlerinin tanımlanması aşağıdakiler için fırsat sunar:

- Projelerin sıralanması – Proje isimleri firma projeleri hakkında hassas bilgiler verebilir.
- Kaynak kodu dosyalarına erişimin onaylanması.
- Kaynak kodu dosyalarında değişiklik yapılması – Kapsam dahilinde müsaade edilmişse kaynak kodunun değiştirilmesi bir saldırganın sistemi etkileyecek değişiklikler yapabileceğini kanıtlar.
- Geliştiricilerin sıralanması – Geliştiriciler hakkındaki detaylar sosyal mühendislik saldırılarında ve aynı zamanda sistemin diğer alanlarına yapılacak saldırılarda girdi olarak kullanılabilir.
- Konfigürasyonun sıralanması.

### Dinamik makine konfigürasyonu sunucusu

Dinamik makine konfigürasyonu servisinin tanımlanması veya servisin ele geçirilen makine tarafından kullanılması aşağıdakilere olanak sağlar:

- Yapılan kiralamaların sıralanması
- Konfigürasyonun sıralanması
- Seçeneklerin sıralanması

- Konfigürasyonun modifikasyonu
- Kiralamaların bitirilmesi

Servisin kontrolü ele geçirilen ağdaki makineler ve servislerin hizmet dışı kalma riskini göstermek ve iki bağlantı noktası arasındaki bağlantıyı izinsiz izleme saldırılarında kullanılabilir.

### Sanallaştırma

Sanallaştırma servislerinin veya yazılımının tanımlanması aşağıdakilere olanak sağlar:

- Sanal bilgisayarların sıralanması (isim, konfigürasyonlar, işletim sistemleri)
- Yönetim sistemleri için parolaların ve sayısal sertifikaların sıralanması
- Sanallaştırma yazılımı konfigürasyonunun sıralanması
- Makinelerin konfigürasyonları
- Sanal bilgisayarların durumunun kontrol edilmesi suretiyle hizmet dışı kalma riskinin gösterilmesi
- Sanal bilgisayarlarda bulundurulan verilere erişim
- Ele geçirilen makinede bulundurulan sanal makinelerin ve servislerin trafiğinin kestirilip yakalanması.

### İleti sistemi

Mesajlaşma servislerinin veya yazılımının tanımlanması aşağıdakiler için fırsat yaratır:

- Dizin servislerinin belirlenmesi
- Yetki bilgilerinin ele geçirilmesi
- Gizli bilgilere erişim
- Ağdaki makinelerin tanımlanması
- Sistem ve iş ilişkileri

Bu bilgilerin ve eylemlerin tamamı riskin gösterilmesi ve bir müşteri kuruluşun ağ ve makinelerine daha ileri derecede sızma için kullanılabilir.

### İzleme ve yönetim

İzleme ve/veya yönetim amaçlı servislerin veya yazılımın tanımlanması hedef ağdaki ilave sunucuların ve servislerin tanımlanmasını sağlayabilir. İlave olarak elde edilen konfigürasyon parametreleri başka hedeflerin makinesine erişimi ve test uzmanının hangi eylemlerinin müşteri kuruluş tarafından tespit edilebileceğinin belirlemesini sağlayabilir. Aranacak bazı servisler aşağıdadır:

- SNMP
- Syslog

Yetki bilgilerinin elde edilmesi, makinenin belirlenmesi ve diğer servislere erişim elde edilmesine yönelik olarak aranacak bazı yönetim servisleri ve yazılımı şunlar olabilir:

- SSH sunucusu/istemcisi
- Telnet sunucusu/istemcisi
- RDP istemcisi

- Terminal sunucusu
- Sanal ortam yönetim yazılımı

### Yedekleme sistemleri

Verilerin yedeklenmesi amaçlı servislerin veya yazılımın tanımlanması bir saldırgan için büyük bir fırsat sunar.

- Makinelerin ve sistemlerin sıralanması
- Servislerin sıralanması
- Makine ve/veya servisler için yetki bilgileri
- Yedeklenmiş verilere erişim

Servisten elde edilen bilgiler sistem ve sistem bilgilerine yönelik gizlilik, bütünlük ve erişim risklerini göstermede kullanılabilir. Yedeklemelere erişim aynı zamanda eksik konfigürasyonların, hassas yazılımların veya müşteri kuruluşun sistemlerindeki izinsiz giriş noktalarının ortaya çıkarılmasını da sağlayabilir.

### Ağ servisleri (RADIUS,TACACS vb.)

Servislerin tanımlanması veya ağ servislerinin kullanımı aşağıdakilere olanak sağlar:

- Kullanıcıların sıralanması
- Makine ve sistemlerin sıralanması
- Yetki bilgilerinin ele geçirilmesi
- Alternatif yöntemler mevcut değilse hizmet dışı kalma riskinin gösterilmesi

### Hassas veriler

### Tuşlarla oturum açma

Tuş darbelerinin izlenmesi suretiyle parolalar ve kişisel kimlik bilgileri gibi hassas bilgilerin tespit edilmesi mümkündür.

### Ekran görüntüsü alma

Ekran görüntüsü alma sistemin ele geçirildiğine dair kanıt göstermede ve aynı zamanda ekranda gösterilebilen ve başka yollarla erişimin mümkün olmadığı bilgilere erişimde kullanılabilir. Ekran yoluyla derlenen bilgilerin müşteri kuruluşun müşterilerinin çalışanlarına ait özel verileri içermemesine dikkat edilmelidir.

### Ağ trafiğinin yakalanması

Ağ trafiğinin yakalanması, ağdaki kontrollere ve yakalama için kullanılan ortama bağlı olarak aşağıdakiler için kullanılabilir:

- Ağdaki makinelerin belirlenmesi

- Verilerin kestirilip yakalanması
- Servislerin belirlenmesi
- Ağdaki makineler arasındaki ilişkilerin belirlenmesi
- Yetki bilgilerinin yakalanması

Sadece sızma testinin kapsamı dahilindeki ağ trafiğinin yakalanmasına ve yakalanan bilgilerin yerel kanunların denetimi altında olmamasına (İnternet üzerinden sesli iletişim gibi) dikkat edilmelidir. Alıkonan ve gösterilen bilgiler müşteri kuruluşun müşterilerinin ve/veya çalışanlarının kişisel bilgilerini ve gizli bilgileri içermemesine yönelik olarak filtrelenmelidir.

### Önceki denetim raporları

### Kullanıcı bilgileri

Bu bölümde esas olarak odaklanılan husus, hedef sistemde bulunan, sistemde mevcut olan veya uzaktan bağlanan, değerlendirmeyi gerçekleştiren personelin toplayabileceği ve daha ileri derecedeki sızma için analiz edebileceği veya değerlendirmenin istenen amacını sağlayacak bazı izler bırakan kullanıcıların hesapları ile ilgili bilgilerdir.

### Sistemdeki bilgiler

Ele geçirilen bir sistemden toplanabilecek genel bilgiler:

- Geçmiş dosyaları – Geçmiş dosyaları kullanıcının uygulamış olduğu eski komutları saklar. Bunların okunması sistem konfigürasyon bilgilerini, önemli uygulamaları, veri lokasyonlarını ve diğer hassas sistem bilgilerini açığa çıkarabilir.
- Şifreleme anahtarları (SSH, PGP/GPG)
- İlgi çekici belgeler – Kullanıcılar sıklıkla parolaları ve diğer hassas bilgileri açık metin dosyalarında saklarlar. Bunlar iki yolla bulunabilir; dosya isimlerinde ilgi çekici kelimelerin aranmasıyla veya dokümanlarının kendilerinde arama yapılmasıyla. İndeksleme servisleri de bu konuda yardımcı olabilir.
- Kullanıcıya özel uygulama konfigürasyon parametreleri
- Kişisel uygulama geçmişi
- Kaldırılabilir ortamların sıralanması
- Ağ ortaklarının / etki alanı izinlerinin sıralanması

### Web sunucuları

Web sunucularından toplanabilecek bilgiler diğer makinelerin ve sistemlerin belirlenmesinde ve aynı zamanda bir müşteri kuruluşun ağ ve makinelerine daha ileri derecede sızma için bilgi sağlamada kullanılabilir. Bu bilgiler:

- Sunucu geçmişi
- Sık kullanılanlar
- Dosya indirme geçmişi
- Yetki bilgileri
- Vekil sunucular

- Eklentiler / Uzantılar

Bir Web sunucusundan gelen bilgiler müşteri kuruluşun çalışanlarının gizli ve kişisel bilgilerini içerebileceğinden, sadece sızma testinin kapsamında bulunan verilerin yakalanmasına özel önem gösterilmelidir. Bu verilerden geri getirilen ve raporlanan veriler ayıklanmalıdır.

### Anlık ileti kullanıcıları

Ele geçirilen bir sistemdeki anlık ileti kullanıcılarından toplanabilen bilgiler:

- Hesap konfigürasyonlarının sıralanması (kullanıcı, parola, sunucu, vekil sunucu)
- İleti kayıtları

Bir Web sunucusundan gelen bilgiler müşteri kuruluşun çalışanlarının gizli ve kişisel bilgilerini içerebileceğinden, sadece sızma testinin kapsamında bulunan verilerin yakalanmasına özel önem gösterilmelidir. Bu verilerden geri getirilen ve raporlanan veriler ayıklanmalıdır.

### Sistem konfigürasyonu

### Parola politikası

Sistemlerin parola politikalarının sıralanması suretiyle brute force saldırısı düzenleme ve parolaların kırılması çok daha etkin hale gelir. Örneğin, asgari parola uzunluğunun 8 karakter olduğunun bilinmesiyle 8 karakterin altındaki kelimeleri sözlük dışına atabilirsiniz.

### Güvenlik politikaları

### Konfigüre edilmiş kablosuz ağlar ve anahtarlar

Hedefin kablosuz bağlantı bilgilerinin bulunması suretiyle firmaların bulunduğu yerden, firmaların kablosuz bağlantıları aracılığıyla fiziki saldırılar düzenlenmesi mümkün olur.

## 6.5 Kıymetli/kritik hedefler

Ele geçirilen sistemlerden ve bu sistemlerde çalışan sistemler ve servisler arasındaki etkileşimlerden derlenen verilerin analiz edilmesi yoluyla kıymetli/kritik hedefler belirlenebilir ve ilave olarak sızma testi öncesi toplantılarda belirlenen hedefler genişletilebilir. K kıymetli/kritik hedeflerin etkileşimleri iş üzerinde, veriler ve prosesler üzerinde ve müşteri kuruluşun altyapısının ve servislerinin genel bütünlüğü üzerindeki etkinin tanımlanmasında ve ölçülmesinde yardımcı olur.

## 6.6 Verilerin dışarı sızması

### Muhtemel tüm veri sızma yollarının belirlenmesi

Erişimin sağlandığı her bir alandan, verilerin dışarı sızması için bir yol yaratılabilir. Bu dış dünyaya erişimin (farklı, erişilebilir alt ağlar vb. aracılığıyla) ikincil ve üçüncül yollarını içerir. Verilerin dışarı sızma yollarının belirlenmesi yapıldıktan sonra verilerin dışarı sızması testi başlatılabilir.

### Verilerin dışarı sızma yollarının test edilmesi

Teste tabi tutulan kuruluştan belirlenen her dışarı sızma yolu kullanılarak dışarı veri sızdırılmalıdır. Bu husus önceden sızma testi öncesi kapsamlama safhasında kapsanmış olmalı ve müşteri kuruluşun kabul edilebilir angajman politikasına bağlı olan yeterli altyapı kurulmuş olmalıdır (bu şu anlama gelmektedir; dışarı sızdırılan veriler genellikle test uzmanının tam denetimde olan ve teste tabi tutulan kuruluşun erişiminde ve mülkiyetinde olan bir sunucuya sızdırılır). Verilerin dışarı sızdırılma işleminin kendisi kuruluşla ilgili tehdit modelleme standardına uyan tehdit aktörleri tarafından gerçek hayatta kullanılan veri sızdırma stratejilerini simule etmelidir.

### Kontrol gücünün ölçülmesi

Verilerin dışarı sızdırılması testi uygulanırken esas amaç hassas bilgilerin kuruluşun dışına çıkmasının tespit edilmesi ve engellenmesi için mevcut olan kontrollerin çalışıp çalışmadığının görülmesi ve aynı zamanda tepki ekiplerinin bu gibi alarm durumlarına ne şekilde reaksiyon gösterdikleri, olayları ne şekilde inceledikleri ve olayları yatıştırdıklarının denenmesidir.

## 6.7 Kalıcılık

- Kimlik doğrulaması isteyen, sisteme izinsiz giriş noktalarının kurulması
- Sisteme geri bağlanmak için servislerin kurulması ve/veya değiştirilmesi. Asgari olarak kullanıcı adı ve karmaşık parola kullanımı; mümkünse sertifikaların veya kriptografik anahtarların kullanımı tercih edilir (SSH, ncat, RDP). Tersine bağlantıların sadece tek bir IP ile kısıtlanması kullanılabilir.
- Karmaşık parolalı alternatif kullanıcı hesaplarının yaratılması
- Mümkün olduğunda sisteme izinsiz giriş noktasının yeniden başlatmalarda yerinde kalması.

## 6.8 Altyapıya yönelik daha ileri derecede sızma

“Pivoting” test uzmanının ele geçirilen sistemdeki varlığını, daha ileri derecede sızma maksadıyla müşteri kuruluşun altyapısındaki diğer sistemlerin sıralanması ve bunlara erişim sağlanmasında kullandığı bir eylemdir. Bu eylem ele geçirilen makineden ele geçirilen sisteme yüklenen yerel kaynakların ve araçların kullanılması suretiyle uygulanabilir.

### Ele geçirilen sistemden yapılacak eylemler

Ele geçirilen bir sistemden yapılacak eylemler:

- Araçların yüklenmesi
- Yerel sistem araçlarının kullanılması
- ARP taraması
- Ping Sweep

- DNS iç ağın sıralanması
- Dizin servislerinin sıralanması
- Brute force saldırıları
- Yönetim protokolleri ve ele geçirilen yetki bilgileri aracılığıyla sıralama ve yönetim (WinRM, WMI, SMB, SNMP vb.)
- Ele geçirilen yetki bilgileri ve anahtarların kötüye kullanılması (Web sayfaları, veri tabanları vb.)
- Uzaktan istismarların uygulanması

Uygulanacak olan eylem belirli risklerin gösterilmesi ve/veya müşteri kuruluşun ağ ve makinelerinde daha ileri derecede sızma için ihtiyaç duyulan bilgiye bağlı olacaktır. Toplanan bilgilerin yeniden değerlendirilmesi ve konulan hedeflere ulaşılana kadar istismar sonrasında sürdürülecek en iyi yaklaşıma karar verilmesi için düzenli planlama oturumlarının yapılması önerilir.

### Ele geçirilen sistemin içinde yapılacak eylemler

Ele geçirilen bir sistem içerisinde yapılacak eylemler:

- Port yönlendirme
- Iç ağa yönelik vekil sunucu
- Iç ağa yönelik sanal özel ağ
- Uzaktan istismar uygulanması
- Ele geçirilen yetki bilgileri ve anahtarların kötüye kullanılması (Web sayfaları, veri tabanları vb.)

Uygulanacak olan eylem belirli risklerin gösterilmesi ve/veya müşteri kuruluşun ağ ve makinelerinde daha ileri derecede sızma için ihtiyaç duyulan bilgiye bağlı olacaktır. Toplanan bilgilerin yeniden değerlendirilmesi ve konulan hedeflere ulaşılana kadar istismar sonrasında sürdürülecek en iyi yaklaşıma karar verilmesi için düzenli planlama oturumlarının yapılması önerilir.

## 6.9 İz temizleme

İz temizleme prosesi sızma testi tamamlandıktan sonra sistemlerin temizlenmesine yönelik gereklilikleri kapsar. İz temizleme test esnasında kullanılan tüm kullanıcı hesaplarını ve ikilileri kapsar.

- Uygulanabilir tüm diziler ve geçici dosyaların ele geçirilen sistemden kaldırılması. Mümkünse dosya ve klasörlerin kaldırılmasında güvenli silme yönteminin kullanılması.
- Değerlendirme esnasında değişiklik yapıldıysa, sistem ayarlarının ve uygulama konfigürasyon parametrelerinin orijinal haline döndürülmesi.
- Kurulan tüm sisteme izinsiz giriş noktalarının ve/veya gizli korsanlık amaçlı programların kaldırılması.
- Ele geçirilen sisteme tekrar geri bağlanmak için yaratılan tüm kullanıcı hesaplarının kaldırılması.

# 7 Raporlama

## 7.1 Giriş

Sızma testinin önemli aşamalarından biri ve son aşaması da raporlama aşamasıdır. Bu bölüm sızma testi sonuçlarının raporlanması için temel kriterleri belirlemek amacıyla hazırlanmıştır. Her sızma testine göre uygun format kullanılarak rapor hazırlanabileceği gibi, bir sızma testi raporunda bulunması gereken temel öğeler ile okuyucular tarafından daha iyi anlaşılabilmesi için raporun sahip olması gereken yapısı hakkındaki temel bilgiler aşağıda sunulmuştur.

Raporlama aşamasında sızma testi sonuçlarını açıklayan detaylı bir rapor üretilerek müşteri kuruluşa iletilir. Hazırlanan raporda temel amaç müşteri kuruluşun rapordan azami şekilde fayda sağlayabilmesi olmalıdır. Dolayısıyla müşteri kuruluşun sızma testleri ile ilgili olarak yeterli teknik bilgiye sahip personeli olmasa bile, raporu doğru bir şekilde yorumlayabilmesi gerekmektedir. Bunun için gerekli şartlar öncelikle raporda bir "Yönetici özeti" olması ve raporun mümkün olduğu kadar teknik detayları açıklayıcı tarzda yazılmasıdır. Rapor, tespit edilen açıklıkları kritikliklerine göre seviyelendirmeli ve müşteri kuruluşun bu seviyelendirmeye göre açıklıkların kapatılmasını önceliklendirebilmesini sağlamalıdır. Ayrıca raporda açıklıkların kapatılmasına dair yöntem ve önerilere de yer verilmelidir.

Bir sızma testi raporu, doğası itibarıyla hassas ve gizlilik derecesine sahip bir dokümandır. Bu nedenle raporların müşteri kuruluş ile paylaşılmasında gizlilik şartlarına dikkat etmek gerekmektedir. Rapor mümkünse, müşterinin irtibat noktasına elden teslim edilmeli, bu mümkün olmuyorsa (farklı şehir veya ülkelerdeki firmalar vb.) elektronik ortamda müşteri kuruluş ile önceden üzerinde anlaşılmış şifreleme teknikleri uygulanarak paylaşılmalıdır. Örneğin sftp, sertifika (PKI) tabanlı şifreleme ve paylaşım, e-posta şifreleme (S/MIME) yoluyla paylaşım gibi teknikler kullanılabilir.

Raporlar ile ilgili saklama, gizlilik ve diğer tüm şartların detaylarına TSE Sızma testi yapan firmalara ait kriterler dokümanından ulaşılabilir.

## 7.2 Raporun Yapısı

Rapor yapısı, sızma testinin hedefleri, izlenen yöntemler ve sonuçların derlenmesi için iki temel bölüme ayrılmıştır:

## 7.3 Yönetici Özeti

Raporun bu bölümü; Sızma testinin belirgin hedefleri ile işletilen testlerin üst düzeydeki sonuçlarını okuyucuya sunmak üzere tasarlanmıştır. Raporun hedef okuyucu kitlesi; kurum yöneticileri, güvenlik programı ile ilgili çalışanları ile belirlenen/doğrulanan tehditlerden etkilenme ihtimali bulunan dış kuruluşlara ait çalışanlar olabilir. Raporun uygulama ile ilgili özet bölümünde aşağıdaki hususlar yer alır:

**Temel bilgiler**

Bu bölüm, yapılan testlerin genel olarak amaçlarını açıklamalıdır. Test öncesi bölümünde tanımlanan riskler; karşı tedbirler ve test hedefleri ile ilgili detaylar; genel test amaçları ve sonuçlarının okuyucu tarafından anlaşılabilmesi için bu bölümde sunulmalıdır.

(Örnek: MÜŞTERİ, sızma testi uzmanıından, ...tesisinde konuşlu sistemlerinin iç/dış açıklık analizlerini ve sızma testlerini yapmalarını talep eder. Söz konusu sistemlerde ... risk sınıfına göre risklerin

bulunduğu ve yetkisiz olarak erişim sağlanırsa MÜŞTERİYE'ye zarar verebilecek materyalleri içeren ... veri sınıflandırma seviyesinde veri bulundurduğu tespit edilmiştir. MÜŞTERİNİN doğrudan ya da dolaylı saldırılara karşı koyabilme yeteneğini test etmek için sızma testi uzmanı; ağ açıklık taraması, Açıklık doğrulama (burada üzerinde mutabık kalınan saldırılar verilmelidir), zayıf hizmetlerin kullanılabilme analizi, istemci tarafı saldırıları, browser tarafı saldırıları gibi analizleri gerçekleştirir. Bu değerlendirmenin amacı, MÜŞTERİ tarafından uygulanan güvenlik kontrollerinin etkinliğinin doğrulanması ve bu sayede işle ilgili kritik bilgilerin korunduğundan emin olunmasıdır. Bu rapor söz konusu değerlendirmenin sonuçlarını ve MÜŞTERİNİN kendi güvenliğini iyileştirmek için önerileri içerir.

- Test aşamasında hedeflerde bir değişiklik söz konusu olursa bu değişikliklerin tamamı raporun bu bölümünde verilmelidir. Buna ek olarak bu değişiklikler raporun ekine eklenebilir ve bu durumda bu bölümden atıf yapılarak belirtilmelidir.

**Genel Değerlendirme:**

Bu bölüm testin etkinliğinin ve ön hazırlık aşamasında belirlenen hedeflere sızma testi uzmanının ulaşma yeteneğinin kısa bir değerlendirmesini içerir.

**Risk Derecelendirme/Risk Profili:**

Genel bir risk derecelendirme/profili/skoru bu bölümde tanımlanır ve açıklanır. Ön sözleşme aşamasında sızma testi uzmanı bir skor oluşturma mekanizması tanımlayacak ve risk izleme/derecelendirme için ayrıca bir mekanizma oluşturacaktır. FAIR, DREAD ve diğer derecelendirmelerden elde edilecek farklı yöntemler tanımlanacak ve çevresel faktörlere bağlı olarak bir araya getirilecektir.

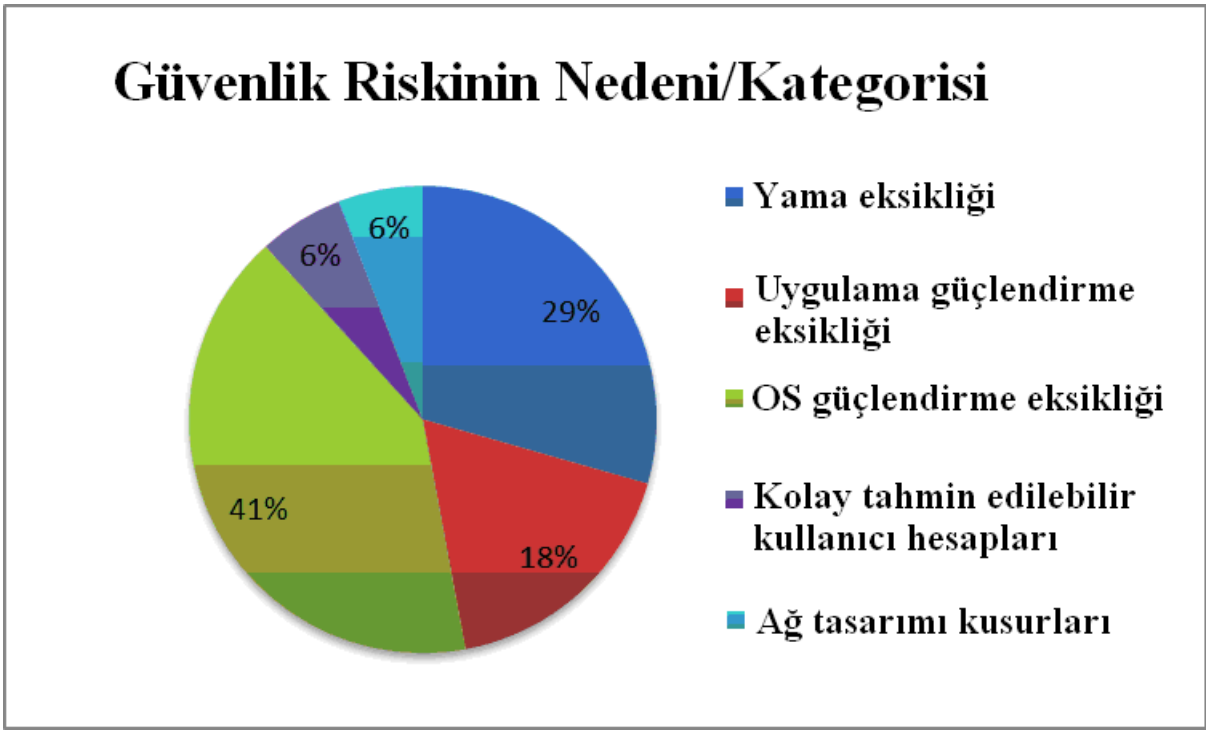
| Bilgi Güvenliği Risk Derecelendirme Ölçeği | |
|---|---|
| Aşırı Yüksek 13-15 | Güvenlik kontrollerinde aşırı yüksek riskler: felaket seviyesinde finansal kayıp oluşturma olasılığı vardır. |
| Yüksek 10-12 | Güvenlik kontrollerinde yüksek riskler: önemli seviyede finansal kayıp oluşturma potansiyeli vardır. |
| Yükselmiş 7-9 | Güvenlik kontrollerinde yükseltilmiş riskler: finansal kayıp oluşturma potansiyeli vardır. |
| Orta 4-6 | Güvenlik kontrollerinde orta seviye riskler: sınırlı finansal kayıp oluşturma olasılığı bulunur. |
| Düşük 1-3 | Güvenlik kontrollerinde düşük riskler: ölçülebilir negatif etki ile sonuçlanır. |

Bir MÜŞTERİ için "Genel Risk Skoru" yedidir (7). Bu derecelendirme YÜKSELTİLMİŞ güvenlik kontrolleri riskleri için maddi finansal kayıp potansiyelinin bulunduğu anlamına gelir. Uzman kişi, doğrudan bir saldırının başarılı olması durumunda birçok orta seviye risk açıklıkları ile bir tane yüksek

seviye risk olduğu temeline dayanarak bu derecelendirmeyi yapmıştır. Tespit edilen en ciddi açıklık; kurumsal halka açık Web sayfasında varsayılan parolaların kullanılmasıdır. Bu husus birçok hassas dokümana erişime ve cihaz üzerindeki içerikleri kontrole izin vermektedir. Bu açıklık kullanıcı hesaplarının çalınmasına, hassas bilginin sızdırılmasına ya da tüm sistemin ele geçirilmesine sebep olabilir. Bunun dışındaki birçok daha az hassas açıklık, kullanıcı hesabı yetki bilgilerinin çalınmasına ve bilgi sızdırılmasına olanak sağlayabilir.

**Genel Bulgular:**

Genel bulgular bölümü; sızma testi sırasında elde edilen hususların basit ve istatistiksel formatta bir özetini içermelidir. Ön anlaşma aşamasında belirlenen test edilen hedefler, test sonuçları, süreçleri saldırı senaryoları, başarı oranları ve diğer dikkate değer diğer hususların grafiksel gösterimi sunulmalıdır. Bunlara ek olarak tespit edilen hususların nedenleri hakkında da bilgi kolay okunabilir bir formatta sunulmalıdır (Örneğin kullanılabilen açıklıkların temel nedenlerini gösteren bir grafik verilmesi gibi).




Ön sözleşme aşamasında belirlenmişse, bu alan kullanım ortamındaki karşı tedbirlerin etkinliğini gösteren metrikleri de içermelidir (Örneğin x saldırısı uygulandığında IPS y'yi engellemiştir. Diğer karşı tedbirler tasarım ve etkinlik anlamında benzer metrikleri içermelidir).

**Önerilerin Özeti:**

Raporun öneriler bölümü; okuyucu tarafından kolaylıkla anlaşılabilecek şekilde belirlenen risklerin çözümü için gerekli görevleri ve önerilen yöntemin uygulanması için gerekli efor seviyesini sunmalıdır. Bu bölüm aynı zamanda önerilen yol haritasının nasıl önceliklendirildiği ile ilgili hususları da içermelidir.

**Stratejik Yol Haritası:**

Yol haritası güvensiz olduğu tespit edilen öğelerin iyileştirilmesi için önceliklendirilmiş bir plan içermeli ve bu plan iş hedefleri/ potansiyel etki seviyesi göz önünde bulundurularak hazırlanmalıdır. Bu bölüm

belirlenen hedefler ile tespit edilen tehditleri eşleştirmelidir. Bu bölümde temel hedefler ile gerçekleştirme zamanları göz önüne alınarak izlenmesi gereken yol açıklanmalıdır. Örneğin

| **Bu Değerlendirme Esnasında Tamamlanan Hususlar** |
|---|
| **Görev** |
| **Kurum içerisinde güvenlikle ilgili iletişim noktası tanımlanması**<br>• Kurum içerisinde güvenlikle ilgili sorunların çözümü için ayrılmış kaynakların belirlenmesi. İyileştirme sürecinin etkin bir şekilde yönetilebilmesi için ilgili personelce sahiplenilmeli ve desteklenmelidir.<br>• Program ve üçüncü taraf değerlendirmelerinin güvenliğinin sağlanması gereklidir. |
| **Güvenlikle ilgili mevcut durumun belirlenmesi**<br>• Bu görev işletim esnasında gerçekleştirilecektir. |
| **1-3 Ay Arasında Yapılacaklar** |
| **Görev** |
| **İyileştirme Stratejisinin Belirlenmesi**<br>• Sızma testi sırasında elde edilen bilgiler kullanılarak iyileştirme stratejisi geliştirilmelidir.<br>Bu eylem için değerlendirme raporu bir temel teşkil edecektir. Bu nedenle raporun MÜŞTERİ Güvenlik Ekibi tarafından resmi hale getirilmesi ve onaylanması gereklidir. |
| **Bilgi Güvenliği Konseyi/Eylem Ekibinin Oluşturulması**<br>• Uygulamadaki süreçlerde güvenliğin ve iyileştirmenin daha iyi sağlanması için MÜŞTERİ özel bir ISEC konseyi oluşturmalı ve her ekip üyesinin iyileştirmeye yeterince katkı sağlaması sağlanmalıdır.<br>• Konsey her iş biriminden yöneticilerin katılması ile oluşturulmalıdır.<br>• ….. |
| **Bilgi Güvenliği Proje Planlamasına Başlanması**<br>• MÜŞTERİ için güvenlik yürütücülerin atanması yapılmalıdır.<br>• **….** |
| **İyileştirme Faaliyetlerinin Önceliklendirilmesi**<br>• Belirlenen risklerin çözümlenebilmesi için gerçekleştirilmesi gereken faaliyetlerin daha iyi anlaşılması için Sızma Testi sonuçlarının detaylı incelemesi yapılmalıdır.<br>• Belirlenen risklerin azaltılması ve en yüksek etliye sahip risklerin öncelikli olarak etkilerinin azaltılması için iyileştirme faaliyetlerinde öncelikler belirlenmelidir.<br>• Ortam güvenliğinin hızlıca artırılması için sunucuların yamaların yapılması ile sürece başlanmalıdır. |
| **Yama hizmetleri**<br>• Onarılması gereken hususlar ve nasıl onarılacağı…<br>• |
| **Hizmetlerin Güçlendirilmesi**<br>• **…** |
| **3-12 Ay Arasında Yapılacaklar** |
| **Görev** |
| **Kurum içerisinde güvenlik değerlendirmesi**<br>Bilginin ve bu bilgiyi işleyen sistemleri uygun seviyede güvenliğinin sağlanması, temelde yönetimin sorumluluğudur. MÜŞTERİ çalışanları, bilgi güvenliği programının mevcut durumunu anlamalı ve riskleri kabul edilebilir bir seviyeye çekmek için gerekli faaliyetler hakkında bilgi sahibi olmalıdır. MÜŞTERİ'nin kendi kurumu içerisinde gerçekleştireceği bir öz değerlendirme, çalışanların uygulanan bilgi güvenliği programını daha iyi anlamaları için bir araç olacak ve gerekli olması durumunda bir iyileştirme hedefinin oluşturulmasına yardımcı olacaktır. |
| **12 aydan sonra yapılacaklar** |

| Görev |
| --- |
| **Üçüncü tarafların Bilgi Güvenliği Yaklaşımlarının değerlendirilmesi ve 27001/2 ile uyumlarının analizinin yapılması**<br>• MÜŞTERİ'nin; genel ataklara ve özel saldırılara karşı koyma yeteneğinin geniş çerçevede değerlendirilmesi yapılmalıdır.<br>• Uygunsuzluk bölgelerinin temel nedenleri belirlenmelidir.<br>• Elde edilen sonuçların temel olarak kullanılması sağlanarak bir strateji oluşturulmalıdır. |

## 7.4 Teknik Rapor

Bu bölüm okuyucuyu testin teknik detayları ve ön irtibat aşamasında anahtar başarı göstergeleri olarak üzerinde anlaşılan tüm hususlar/bileşenler konusunda bilgilendirir. Teknik rapor bölümü, testin kapsamı, bilgileri, saldırı yolu, etkisini ve iyileştirme önerilerini detaylı şekilde açıklamalıdır

**Giriş:**

Teknik raporun giriş bölümü aşağıdakilerle ilgili ön bilgi verilmesi amacını taşır:

- Hem müşteri kuruluş hem de sızma testi ekibinden teste katılan personeller
- İrtibat bilgisi
- Testte söz konusu olan varlıklar
- Testin amaçları
- Testin kapsamı
- Testin kuvveti
- Yaklaşım
- Tehdit/derecelendirme yapısı

Bu bölüm teste yer alan özel kaynaklara ve testin genel kapsamına referans vermelidir.

**Bilgi toplama:**

Bilgi toplama ve bilgi değerlendirme iyi bir sızma testinin temellerini oluşturur. Sızma testi uzmanı ortam hakkında ne kadar bilgi sahibi ise testin sonuçları o kadar iyi olacaktır. Bu bölümde, bilgi toplama aşaması sonucunda elde edilen açık ve özel bilgilerin boyutlarının müşteri kuruluşa gösterilmesi için bazı hususlar yazılı hale getirilmelidir. Tespit edilen sonuçlar asgari olarak, dört temel kategoride sunulmalıdır:

**Pasif bilgi toplama:**

Bu bölüm DNS, IP/altyapı ile ilgili bilgilere yönelik Google araması gibi dolaylı analizlerden elde edilen bilgileri kapsar. Bu bölüm varlıklara herhangi bir doğrudan trafik göndermeden müşteri kuruluşun ortamındaki teknolojinin profilinin çıkarılmasında kullanılan teknikler üzerinde yoğunlaşır.

**Aktif bilgi toplama:**

Bu bölümde, altyapı eşleştirme, port tarama, mimari değerlendirme ve diğer izleme faaliyetleri gibi görevlerin yöntemleri ve sonuçları gösterilir. Bu bölüm varlıklara doğrudan trafik göndererek müşteri kuruluşun ortamındaki teknolojinin profilinin çıkarılmasında kullanılan teknikler üzerinde yoğunlaşır.

**Kuruluşla ilgili bilgi toplama:**

Kuruluşun yapısı, iş birimleri, piyasa payı, dikey ve diğer kuruluş fonksiyonları ile ilgili bilgiler hem iş süreçleri hem de test edilen daha önce tespit edilmiş fiziksel varlıklar ile eşleştirilmelidir.

**Personel ile ilgili bilgi toplama:**

Kullanıcılar ile müşteri kuruluşu eşleştiren, bilgi toplama aşamasında bulunan herhangi bir bilgi ve tüm bilgiler bu bölümde yer almalıdır. Bu bölüm, genel/özel çalışan veri tabanları, e-posta depoları, organizasyon şemaları ve çalışan/şirket bağlantısına giden diğer unsurlar gibi bilgi sağlamak için kullanılan teknikleri göstermelidir.

**Açıklık değerlendirme:**

Açıklık değerlendirme, bir test çerçevesinde olası açıklıkların tespit edilmesi ve her bir tehdidin tehdit sınıflandırmasının yapılması faaliyetidir. Bu bölümde açıklığın tespit edilmesinde kullanılan yöntemlerin bir tanımı ve açıklığın kanıtı/sınıflandırması yer almalıdır. İlave olarak bu bölüm aşağıdakileri içermelidir:

- Açıklık Sınıflandırma seviyeleri
- Teknik Açıklıklar
    - OSI katman açıklıkları
    - Bulunan açıklık tarayıcı
    - Elle tespit edilen
    - Genel açıklık sahası
- Mantıksal açıklıklar
    - OSI dış açıklıklar
    - Açıklıkların tipi
    - Nasıl/Nerede bulunduğu
    - Açıklık sahası
- Sonuçların özeti

**Kullanma / Açıklık Onaylama:**

Kullanım veya açıklık onaylama, hedefteki varlığa belirli bir seviyede erişim sağlamak için önceki bölümlerde tespit edilen açıklıkların kullanılması faaliyetidir. Bu bölüm, tanımlanan açıklıkları onaylamak için atılan tüm adımları ve aşağıdakileri detaylı bir şekilde ele almalıdır:

- Kullanım zaman çizelgesi
- Kullanım için seçilen hedefler
- Kullanım faaliyetleri
    - Yönlendirilmiş Saldırı

        - Kullanılamayan hedef makineler
        - Kullanılabilen hedef makineler
            - Tekil makine bilgisi
            - Yürütülen saldırılar
            - Başarılı Saldırılar
            - Verilen erişim + yükseltme yolu seviyesi
            - İyileştirme
                - Açıklık bölüm referansına bağlantı
                - Ek azaltma tekniği
                - Karşılayıcı kontrol önerisi
- Dolaylı saldırı
    - Oltalama
        - Saldırının zaman çizelgesi/detayları
        - Tespit edilen hedefler
        - Başarı/Başarısızlık oranı
        - Verilen erişim seviyesi
    - İstemci tarafı
        - Saldırının zaman çizelgesi /detayları
        - Tespit edilen hedefler
        - Başarı/Başarısızlık oranı
        - Verilen erişim seviyesi
    - Tarayıcı tarafı
        - Saldırının zaman çizelgesi /detayları
        - Tespit edilen hedefler
        - Başarı/Başarısızlık oranı
        - Verilen erişim seviyesi

**Kullanma sonrası:**

Tüm testlerde en kritik unsurlardan biri, testin test edilen müşteri kuruluş üzerindeki gerçek etkisi ile olan bağlantısıdır. Yukarıdaki bölümler, açıklığın teknik doğası ve hatadan başarılı bir şekilde yararlanma kabiliyetini ortaya koyarken, kullanım sonrası bölümü kullanım kabiliyetini gerçek iş riskine bağlamalıdır. Bu alanda aşağıdaki unsurlar, ekran görüntüleri, zengin içerik elde etme ve gerçek ortam ayrıcalıklı kullanıcı erişimlerinden örnekler kullanılarak gösterilmelidir:

- Ayrıcalık yükseltme yolu
- Kullanılan teknik
- Müşteri kuruluş tarafından tanımlanan kritik bilgilerin elde edilmesi
- Bilginin değeri
- Ana iş sistemlerine erişim
- Uyumluluk korumalı veri kümlerine erişim

- Erişilen ek bilgiler/sistemler
- Süreklilik yeteneği
- Dışarı sızdırılabilme yeteneği
- Karşı tedbir etkinliği
    - Tespit yeteneği
        - FW/WAF/IDS/IPS
        - İnsan
        - DLP
        - Log
    - Müdahale ve Etkinlik

**Risk/Açıklık Sahası:**

İşe doğrudan etki, açıklık, kullanma ve kullanma sonrası bölümlerindeki mevcut kanıtlar vasıtası ile ölçüldüğünde, risk miktarı belirlenebilir. Bu bölümde yukarıdaki sonuçlar, ön irtibat bölümünden gelen risk değerleri, bilgilerin kritikliği, kuruluşun değeri ve hesaplanan işe etkisi ile birleştirilir. Bu müşteri kuruluşa test boyunca bulunan açıklıkların tespit edilmesi, görselleştirilmesi ve finansal kaynak ayırma kabiliyetini ve çözümün etkin bir şekilde müşteri kuruluşun iş amaçları doğrultusunda değerlendirilmesini sağlayacaktır. Bu bölüm, iş risklerini aşağıdaki alt bölümler dahilinde içermelidir:

- İhlal olayı sıklığının değerlendirilmesi
    - Olası olay sıklığı
    - Tehdit yeteneğinin kestirilmesi (3 – tehdit modellemeden)
    - Kontrol kuvvetinin kestirilmesi (6)
    - Açıklıkları birleştir (5)
    - Gerekli olan yetenek seviyesi
    - Gerekli olan erişim seviyesi
- İhlal olayı başına kayıp büyüklüğünün kestirilmesi
    - Birincil kayıplar
    - İkincil kayıplar
    - Risk kök neden analizinin tespit edilmesi
        - Kök neden hiçbir zaman bir yama değildir.
        - Başarısız olan süreçlerin tespit edilmesi
- Riskin Belirlenmesi
    - Tehdit
    - Açıklık
    - Örtüşme

**Sonuç**

Bu bölüm gerçekleştirilen teste son genel bir bakış sağlar. Bu bölüm testin bölümlerinin genel bir değerlendirmesini yansıtmalı ve buna ek olarak kuruluşun güvenlik çerçevesinin gelişimini desteklemelidir. Bölümün kuruluşun güvenlik programının geliştirilmesi açısından destek ve kılavuzluk

sağlayacak ve gelecekteki test/güvenlik faaliyetlerini özendirecek bir ifade ile tamamlanması tavsiye edilir.

# EK A

# Sızma testi aşamaları kontrol listesi

**Etik Hackerlığa Giriş**

| | | | |
|---|---|---|---|
| Bilgi Güvenliğinin Önemi | ( ) | ( ) | ( ) |
| Bilgi Güvenliğinin Tanımlanması | ( ) | ( ) | ( ) |
| Güvenlik üçgeni | ( ) | ( ) | ( ) |
| Hacker' a dair herşey. | ( ) | ( ) | ( ) |
| Hactivizm | ( ) | ( ) | ( ) |
| Güvenlik Uzmanlığı | ( ) | ( ) | ( ) |

**Footprinting, Keşif ve Arama**

| | | | | | |
|---|---|---|---|---|---|
| Google Advanced Search Option | ( ) | ( ) | ( ) | ( ) | ( ) |
| Sitenin Ana Sayfasından Bilgi Edinme | ( ) | ( ) | ( ) | ( ) | ( ) |
| Lokasyon Bilgisi | ( ) | ( ) | ( ) | ( ) | ( ) |
| Çalışanların Bilgileri | ( ) | ( ) | ( ) | ( ) | ( ) |
| Her Türlü İletişim Bilgisi | ( ) | ( ) | ( ) | ( ) | ( ) |
| Partner Firmalar | ( ) | ( ) | ( ) | ( ) | ( ) |
| Waybackmachine | ( ) | ( ) | ( ) | ( ) | ( ) |

| | | | | | |
|---|---|---|---|---|---|
| İnternette Bulunabilecek Dokümanlar | ( ) | ( ) | ( ) | ( ) | ( ) |
| Sosyal Ağlar | ( ) | ( ) | ( ) | ( ) | ( ) |
| GHDB (Google Hacking Data Base) | ( ) | ( ) | ( ) | ( ) | ( ) |
| Traceroute (Farklı araç ve yöntemler ile) | ( ) | ( ) | ( ) | ( ) | ( ) |
| IANA Whois Servisi | ( ) | ( ) | ( ) | ( ) | ( ) |
| ARIN IP Servisi | ( ) | ( ) | ( ) | ( ) | ( ) |
| WHOIS | ( ) | ( ) | ( ) | ( ) | ( ) |
| Exiftool Metadata Analizi | ( ) | ( ) | ( ) | ( ) | ( ) |
| FOCA Metadata Analizi | ( ) | ( ) | ( ) | ( ) | ( ) |
| Wget İle Siteyi İndirip İnceleme | ( ) | ( ) | ( ) | ( ) | ( ) |
| Theharvester | ( ) | ( ) | ( ) | ( ) | ( ) |
| Maltego | ( ) | ( ) | ( ) | ( ) | ( ) |

**Tarama**

| | | | | | |
|---|---|---|---|---|---|
| TOR Proxy Kurulumu ve Kullanımı | ( ) | ( ) | ( ) | ( ) | ( ) |
| Ping Uygulaması | ( ) | ( ) | ( ) | ( ) | ( ) |
| Super Scan | ( ) | ( ) | ( ) | ( ) | ( ) |
| Hping | ( ) | ( ) | ( ) | ( ) | ( ) |

| | | | | | |
|---|---|---|---|---|---|
| NMAP (Host , Port , OS taraması ) | ( ) | ( ) | ( ) | ( ) | ( ) |
| Netcat | ( ) | ( ) | ( ) | ( ) | ( ) |
| Nessus Zafiyet Tarayıcısı | ( ) | ( ) | ( ) | ( ) | ( ) |
| Nexpose Zafiyet Tarayıcısı | ( ) | ( ) | ( ) | ( ) | ( ) |
| OpenVAS Zafiyet Tarayıcısı | ( ) | ( ) | ( ) | ( ) | ( ) |

**Servislerden Bilgi Alma**

| | | | | | |
|---|---|---|---|---|---|
| Superscan (NetBIOS Enumeration) | ( ) | ( ) | ( ) | ( ) | ( ) |
| SNMP Enumeration | ( ) | ( ) | ( ) | ( ) | ( ) |
| SMTP Enumeration | ( ) | ( ) | ( ) | ( ) | ( ) |
| SMB Enumeration | ( ) | ( ) | ( ) | ( ) | ( ) |
| DNS Enumeration | ( ) | ( ) | ( ) | ( ) | ( ) |
| Dnsenum | ( ) | ( ) | ( ) | ( ) | ( ) |
| Fierce | ( ) | ( ) | ( ) | ( ) | ( ) |
| Nslookup | ( ) | ( ) | ( ) | ( ) | ( ) |
| DIG | ( ) | ( ) | ( ) | ( ) | ( ) |
| Nmap Versiyon OS Taramaları | ( ) | ( ) | ( ) | ( ) | ( ) |

| | | | | | |
|---|---|---|---|---|---|
| Nmap Scriptleri | ( ) | ( ) | ( ) | ( ) | ( ) |
| Netcat | ( ) | ( ) | ( ) | ( ) | ( ) |
| LDAP Enumeration | ( ) | ( ) | ( ) | ( ) | ( ) |
| Sqlmap İle Enumeration | ( ) | ( ) | ( ) | ( ) | ( ) |
| **Sistemlere Giriş** | | | | | |
| Exploit Kullanımı | ( ) | ( ) | ( ) | ( ) | ( ) |
| Exploit Düzenleme | ( ) | ( ) | ( ) | ( ) | ( ) |
| Windows Hacking | ( ) | ( ) | ( ) | ( ) | ( ) |
| Linux Hacking | ( ) | ( ) | ( ) | ( ) | ( ) |
| Client Side Atakları | ( ) | ( ) | ( ) | ( ) | ( ) |
| Metasploit Framework | ( ) | ( ) | ( ) | ( ) | ( ) |
| MSF Komut Satırı | ( ) | ( ) | ( ) | ( ) | ( ) |
| MSF Konsol | ( ) | ( ) | ( ) | ( ) | ( ) |
| MSF Web | ( ) | ( ) | ( ) | ( ) | ( ) |
| Meterpreter | ( ) | ( ) | ( ) | ( ) | ( ) |
| Binary Payloadlar | ( ) | ( ) | ( ) | ( ) | ( ) |

# EK B

# Kısaltılmış terimler

Aşağıdaki kısaltmalar, bu dokümanın bir ya da birden fazla bölümünde kullanılmaktadır. Kısaltmaların karşılarında İngilizce açılımları ve yaygın olarak kullanılan Türkçe karşılıkları verilmektedir.

| | | |
|---|---|---|
| AES | Advanced encryption standard | Gelişmiş şifreleme standardı |
| API | Application programming interface | Uygulama programlama arayüzü |
| ARP | Address resolution protocol | Adres çözümleme protokolü |
| BGP | Border gateway protocol | Sınır geçit protokolü |
| CDP | Cisco discovery protocol | Cisco keşif protokolü |
| CERT | Computer emergency response team | Siber olaylara müdahale ekibi (SOME) |
| CRM | Customer relationship management | Müşteri ilişkileri yönetimi |
| CSIRT | Computer security incident response team | Bilgisayar güvenliği olay müdahale ekibi |
| CVE | Common vulnerabilities and exposures | Yaygın açıklıklıklar ve zayıflıklar |
| DHCP | Dynamic host configuration protocol | Dinamik bilgisayar konfigürasyonu protokolü |
| DLP | Data loss prevention | Veri kaybından korunma |
| DNS | Domain name system | Alan adı sistemi |
| DSN | Delivery status notification | İleti durum raporu |
| FTP | File transfer protocol | Dosya aktarım protokolü |
| GPG | GNU privacy guard | |
| GUI | Graphical User Interface | Grafiksel Kullanıcı Arayüzü |
| HBA | Host bus adapter | |
| HIDS | Host-based intrusion detection systems | Kullanıcı tabanlı izinsiz girişleri tespit sistemi |
| HIPS | Host-based intrusion prevention systems | Kullanıcı tabanlı izinsiz girişleri engelleme sistemi |
| HR | Human resources | İnsan kaynakları |
| HTTP | Hyper text transfer protocol | Hipermetin aktarma protokolü |
| ICANN | Internet corporation for assigned names/numbers | İnternet tahsisli numaralar ve isimler kurumu |
| ICMP | Internet control message protocol | İnternet kontrol mesaj iletişim kuralı |
| IDS | Intrusion detection systems | İzinsiz girişleri tespit sistemi |
| IP | Internet Protocol | İnternet protokolü |
| IPS | Intrusion prevention systems | İzinsiz girişleri engelleme sistemi |
| ISO | International Organization for Standardization | Uluslararası standardlar teşkilâtı |
| LLDP | Link layer discovery protocol | |

| | | |
|---|---|---|
| mDNS | Multicast Domain Name Service | Çoklu gönderim alan adı servisi |
| MSSP | Managed security service provider | Yönetilen güvenlik servis sağlayıcısı |
| NDN | Non-delivery notification | İletilmedi bildirimi |
| NDR | Non-delivery report/receipt | Teslim edilmedi raporu/alındısı |
| NIST | National institute of standards and technology | Ulusal standard ve teknoloji enstitüsü |
| Nmap | Network Mapper | |
| OSI | Open Systems Interconnection | Açık sistemler bağlantısı |
| OSINT | Open source intelligence | Açık kaynak istihbaratı |
| OSVDB | Open sourced vulnerability database | Açık kaynak açıklık veri tabanı |
| OTS | Open text summarizer | Açık metin özetleyici |
| PCI | Peripheral component interconnect | Çevre birimleri bağlantı veri yolu |
| PGP | Pretty good privacy | |
| PHP | Hypertext preprocessor | Üstün metin ön işlemcisi |
| PING | Packet InterNet Groper | |
| PKI | Public-key infrastructure | Açık anahtar altyapısı |
| PSRT | Public Safety Response Team | kamu güvenliği müdahale ekibi |
| RDP | Remote desktop protocol | Uzak masaüstü protokolü |
| SFTP | Secure file transfer protocol | Güvenli dosya aktarım protokolü |
| S/MIME | Secure/Multipurpose Internet Mail Extension | Güvenli/çok maksatlı İnternet ileti uzantısı |
| SMTP | Simple mail transfer protocol | Basit posta iletim protokolü |
| SNMP | Simple network management protocol | Basit ağ yönetim protokolü |
| SNA | Systems network architecture | Sistem ağ mimarisi |
| SOME | Siber olaylara müdahale ekibi | |
| SSH | Secure Shell | Güvenli kabuk |
| SWOT | Strengths/Weaknesses/Opportunities/Threats | Güçlü yönler/zayıf yönler/fırsatlar/tehditler |
| TCP | Transmission control protocol | Aktarma kontrol protokolü |
| TDL | Top level domain | Üst düzey etki alanı |
| TOR | The onion router | Anonim ağ |
| UDP | User datagram protocol | Kullanıcı veri bloğu iletişim kuralları |
| USB | Universal serial bus | Evrensel seri veriyolu |
| VLAN | Virtual local area network | Sanal yerel alan şebekesi |
| VoIP | Voice over IP technologies | IP üzerinden ses verisi gönderme teknolojisi |
| VPN | Virtual private network | Sanal özel ağ |
| WAFP | Web application Fingerprinter | Web uygulaması ayırt edici özelliklerini bulma |