BGA

BİLGİ GÜVENLİĞİ
AKADEMİSİ
www.bga.com.tr

Bilgi Güvenliği Açısından Sızma Testleri

Proaktif Güvenlik Yaklaşımı Olarak Penetrasyon Testleri

Huzeyfe ÖNAL

11/21/2012

[Bu yazı bilgi güvenliğinde sızma testlerinin yeri ve önemine ait teknik olmayan bilgiler içermektedir.]

Bilgi Güvenliğinde Sızma Testleri

Giriş

Günümüz bilgi güvenliğini sağlamak için iki yaklaşım tercih edilmektedi. . Bunlardan ilki savunmacı yaklaşım(defensive) diğeri de proaktif yaklaşım (offensive)olarak bilinir. Bunlardan günümüzde kabul göreni proaktif yaklaşımdır. Pentest –*sızma testleri*– ve vulnerability assessment –*zayıflık tarama*- konusu proaktif güvenliğin en önemli bileşenlerinden biridir.

Son yıllarda gerek çeşitli standartlara uyumluluktan gerekse güvenliğe verilen önemin artmasından dolayı sızma testleri ve bu konuda çalışanlara önem ve talep artmıştır. Bu yazıda sızma testleri ile ilgili merak edilen sorulara sektörün gözünden cevap verilmeye çalışılacaktır. Yazı, sızma testleri konusunda **teknik detaylar** içermemektedir. Sızma testleri konusunda teknik bilgiler için http://blog.bga.com.tr adresi takip edilebilir.

Sızma Testleri Lüks mü İhtiyaç mı?

Sahip olduğunuz bilişim sistemlerindeki güvenlik zaafiyetlerinin üçüncü bir göz tarafından kontrol edilmesi ve raporlanması proaktif güvenliğin ilk adımlarındandır. Siz ne kadar güvenliğe dikkat ederseniz birşeylerin gözünüzden kaçma ihtimali vardır ve internette hackerlarin sayısı ve bilgi becerisi her zaman sizden iyidir. Hackerlara yem olmadan kendi güvenliğinizi bu konudaki uzmanlara (beyaz şapkalı hacker, ethical hacker, sızma test uzmanı vs)test ettirmek firmanın yararına olacaktır.

Sağlam bir ekibe yaptırılacak sızma testleri internet üzerinden gelebilecek tehditlerin büyük bir kısmını ortaya çıkarıp kapatılmasını sağlayacaktır. Bununla birlikte bilişim güvenliğinin zamana bağımsız dinamik bir alan olduğu gözönünde bulundurulursa sızma testlerinin tek başına yeterli olmayacağı aşikardır.

Sızma testlerinini bitimini takip eden günlerde ortaya çıkabilecek kritik bir güvenlik zafiyeti kurumları zor durumda bırakmak için yeterlidir. Dolayısıyla sızma testleri ile yetinmeyerek mutlaka katmanlı güvenlik mimarisinin kurum güvenlik politikalarında yerini alması önerilmektedir.

Güvenlik açısından olduğu kadar çoğu kurum ve kuruluş için sızma testleri ISO 27001, PCI, HIPAA gibi standartlarla zorunlu hale getirilmiştir.
Sızma testleri maliyetli bir iştir ve genellikle yöneticiler tarafındans ROI(Return of investment)si hesaplanamayan ya da hatalı hesaplanan bir projedir. Burada iş bilgi güvenliği uzmanlarına düşmektedir. Gerçekleştirilen sızma testlerinin sonuçları

yöneticilerin anlayacağı uygun bir biçimde üst yönetime anlatılmalı ve yapılan işin şirkete uzun vadeli kazandırdıkları gösterilmelidir.
Kısaca sızma testleri konusunda uzman ekiplere sahip firmalara yaptırılırsa değerli bir iştir, bunun haricinde sadece vicdani rahatlık sağlar ve standartlara uyumluluk kontrol listelerinden bir madde daha tamamlanmış olur.

Sızma Testlerinde Genel Kavramlar

Pentest, Vulnerability Assessment ve Risk Asssessment Kavramları

Sızma Testleri (Pentest): Belirlenen bilişim sistemlerine mümkün olabilecek ve müşteri tarafından onayı verilmiş her yolun denenerek sızılmaya çalışma işlemine pentest denir.

Pentest de amaç güvenlik açıklığını bulmaktan öte bulunan açıklığı değerlendirip sistemlere yetkili erişimler elde etmek ve elde edilen erişimler kullanılarak tüm zafiyetlerin ortaya çıkarılmasıdır.

Sızma Test Çeşitleri
Gerçekleştirilme yöntemlerine göre sızma testleri üçe ayrılmaktadır. Bunlar aşağıdaki gibi listelenmektedir.

- Whitebox
- Blackbox
- Graybox

Black box Pentest – Kapalı Kutu Sızma Testleri
Bunlardan blackbox bizim genelde bildiğimiz ve yaptırdığımız pentest yöntemidir. Bu yöntemde testleri gerçekleştiren firmayla herhangi bir bilgi paylaşılmaz. Firma ismi ve firmanın sahip olduğu domainler üzerinden firmaya ait sistemler belirlenerek çalışma yapılır.

White box Pentest – Açık Kutu Sızma Testleri
Bu sızma test yönteminde firma tüm bilgileri paylaşır ve olabildiğince sızma testi yapanlara bilgi verme konusunda yardımcı olur.

Zafiyet Değerlendirme Testleri (Vulnerability Assessment): Belirlenen sistemlerde güvenlik zaafiyetine sebep olabilecek açıklıkların araştırılması. Bu yöntem için genellikle

otomatize araçlar kullanılır(Nmap, Nessus, Qualys vs)gibi. Vulnerability assessment çalışmaları sızma testleri kadar tecrübe zaman gerektirmeyen çalışmalardır.

Risk assessment tamamen farklı bir kavram olup pentest ve vuln. assessmenti kapsar. Zaman zaman technical risk assessment tanımı kullanılarak Vulnerability assessment kastedilir.

Sızma Testlerinde Proje Yönetimi

Gerçekleştirilecek sızma testlerinden en yüksek verimi alabilmek için her işte olduğu gibi burada da plan yapmak gerekir. Pentest planı oluşturmaya başlamak için aşağıdaki temel sorular yeterli olacaktır:

- Pentest'in kapsamı ne olacak?
- Sadece iç ağ sistemlerimimi, uygulamalarımı mı yoksa tüm altyapıyı mı test ettirmek istiyorum
- Testleri kime yaptıracağım
- Ne kadar sıklıkla yaptırmalıyım
- Riskli sistem ve servisler kapsam dışı olmalı mı yoksa riski kabul edip sonucunu görmelimiyim.
- DDOS denemesi yapılacak mı
- Pentest sonuç raporundaki zafiyetleri kapatmak icin idari gücüm var mı?

Müşteri İçin Pentest Proje Zaman Çizelgesi

1. Pentest yapmak için karar verilir
2. Temel kapsam belirlenir . Hangi bileşenlerin test edileceği konusunda Kapsam Belirleme kısmı yardımcı olacaktır.
3. Firma araştırması [Firma seçimi konusunda dikkat edilmesi gereken maddeler incelenmeli]
4. Firmalardan teklif toplama
5. Firmalardan kapsam önerilerini isteme
6. Firmalardan örnek sızma test raporu isteme

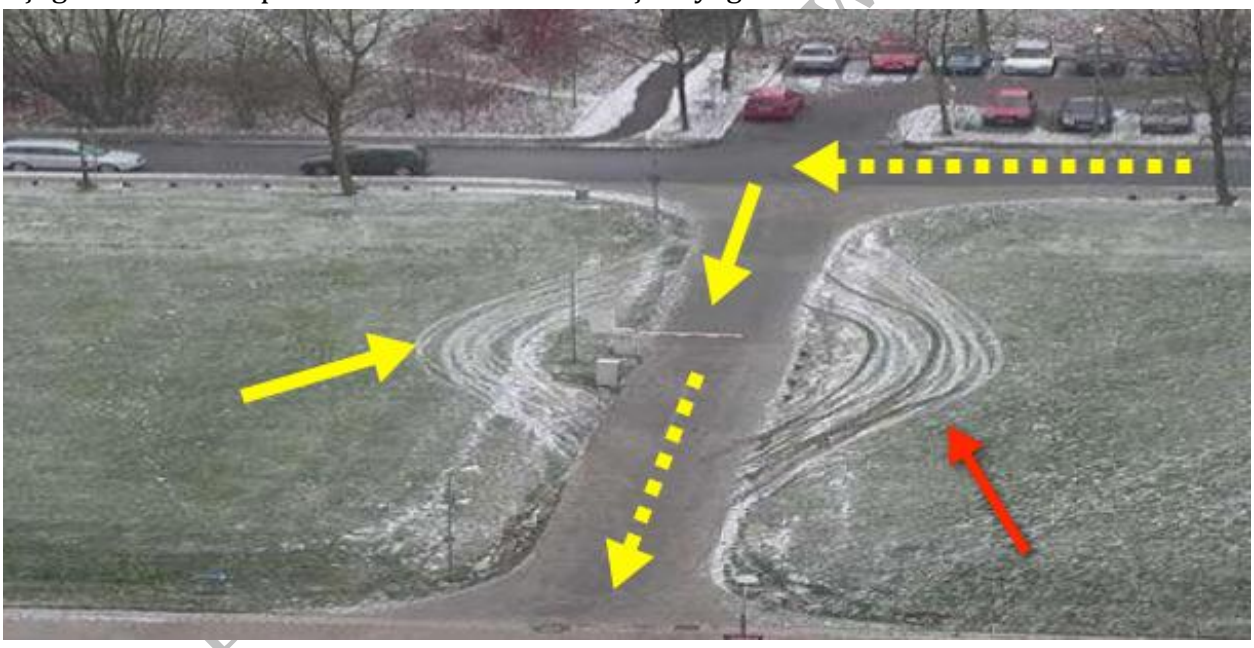
7. Gerekli durumda kapsam belirleme için firmayla ek toplantılar
8. Firmaya karar verme ve sızma testlerine başlama

Sızma Testlerinde Kapsam Belirleme Çalışması

Sızma testinde ana amaçlardan biri tüm zafiyetlerin degerlendirilerek sisteme sızılmaya çalışılmasıdır. Bu amaç doğrultusunda gerçekleştirilecek sızma testlerinde kapsam pentest çalışmasının en önemli adımını oluşturmaktadır.

Sistem/ağ yöneticileri ile hackerların bakış açısı farklıdır ve sitem/ağ yöneticisi tarafından riskli görülmeyen bir sunucu/sistem hacker için sisteme sızmanın ilk adımı olabilir. Bu nedenle kapsam çalışmalarında mutlaka pentest yaptırılacak kişi/firma ile ortaklaşa hareket edilmelidir.

Aşağıdaki resim kapsam konusunun önemimi çok iyi göstermektedir.



Kapsam belirlemek için standart bir formül yoktur. Her firma ve ortam için farklı olabilmektedir. Genellikle sızma testleri aşağıdaki gibi alt bileşenlere ayrılmaktadır.

- Web uygulama sızma testleri
- Son kullanıcı ve sosyal mühendislik testleri
- DDoS ve performans testleri
- Ağ altyapısı sızma testleri
- Yerel ağ sızma testleri
- Mobil uygulama güvenlik testleri

- Sanallaştırma sistemleri sızma testleri

Kapsam belirleme konusunda sızma testini gerçekleştirecek firma ve hizmeti alacak firma birlikte karar vermelidir. Genellikle hizmet alan firma maliyetleri düşürmek için kapsamı olabildiğince daraltmaya çalışmakta ve kapsam olarak güvenli olduğu düşünülen sistemlerin ip adresleri verilmekte ya da örnekleme yapılmaya çalışılmaktadır. Oysa sızma testlerinde ana amaçlardan birisi en zayıf noktayı kullanarak sisteme sızmak, sızılabildiğini göstermektir.

Kapsam konusunda sadece ip adresi alarak sızma testi yapılmaz. Bir web uygulamasını test etmek ile DNS sunucuyu, güvenlik duvarını test etmek çok farklıdır. Yine statik içerik barındıran bir web sitesi ile dinamik içerik barındıran web sayfasını test etmek de içerik ve üzerine harcanan emek açısından oldukça farklıdır.

Firma Seçimi

Sızma testleri sonuçları somut olmayan hizmetler kapsamındadır. Firmalar kendilerinin uzman olduklarını farklı şekilde ortaya koyabilirler. Bunlardan en önemlisi firmanın referansları ve bu konuda çalıştırdığı kişilerin yetkinliği ve firmanın sızma testlerine olan ilgisidir. Güvenlik ürün çözümleri sunup yanında sızma testleri yapan firmalar genellikle halihazırda sundukları ürünleri satabilmek için sızma testleri gerçekleştirir ve sonuçları daha çok ürün satmaya yönelik olur.

Tek işi sızma testleri ve benzeri hizmetler vermek olan firmalar bu konuda daha öncelikli olarak değerlendirilmelidir.

Firma seçimi konusunda yardımcı olabilecek bazı maddeler aşağıdaki gibi sıralanabilir.

- Firmada test yapacak çalışanların CVlerini isteyin . Varsa testi yapacak çalışanların konu ile ilgili sertifikasyonlara sahip olmasını ercih edin.
- Testi yapacak çalışanların ilgili firmanın elemanı olmasına dikkat edin.
- Firmaya daha önceki referanslarını sorun ve bunlardan birkaçına memnuniyetlerini sorun.
- Mümkünse firma seçimi öncesinde teknik kapasiteyi belirlemek için tuzak sistemler kurarak firmaların bu sistemlere saldırması ve sizin de bildiğiniz açıklığı bulmalarını isteyin.
- Firmadan daha önce yaptığı testlerle ilgili örnek raporlar isteyin.

- Testlerin belirli ip adreslerinden yapılmasını ve bu ip adreslerinin size bildirilmesini talep edin.
- Firmaya test için kullandıkları standartları sorun.
- Firmanın test raporunda kullandığı tüm araçları da yazmasını isteyin.
- Pentest teklifinin diğerlerine göre çok düşük olmaması

En önemli maddelerden biri Penetration test firmanın özel işi mi yoksa oylesine yaptığı bir iş mi? Bu sorgu size firmanın konu hakkında yetkinliğine dair ipuçları verecektir.

Ücretiz sızma testi hizmeti veren firmalar genellikle sızma testi konusunu yan iş olarak yapmaktadır ve bu konuda alınacak hizmetin kalitesi sıfıra yakın olacaktır. Sızma testleri tamamen uzmanlık alanı bu olan kişi/firmalara bırakılmalıdır.

Genellikle ürün satmak için ücretsiz sızma testleri gerçekleştiren firmaların yapacağı sızma testleri otomatik araçlarla taramanın ötesine geçememektedir.

Sızma Test Metodolojisi Kullanımı

İşinin ehli bir hacker kendisine hedef olarak belirlediği sisteme sızmak için daha önce edindiği tecrübeler ışığında düzenli bir yol izler. Benzeri şekilde sızma testlerini gerçekleştiren uzmanlar da çalışmalarının doğrulanabilir, yorumlanabilir ve tekrar edilebilir olmasını sağlamak için metodoloji geliştirirler veya daha önce geliştirililen bir metodolojiyi takip ederler.

Metodoloji kullanımı bir kişilik olmayan sızma test ekipleri için hayati önem taşımaktadır ve sızma testlerinde daha önce denenmiş ve standart haline getirilmiş kurallar izlenirse daha başarılı sonuçlar elde edilir

Internet üzerinde ücretsiz olarak edinilebilecek çeşitli güvenlik testi kılavuzları bulunmaktadır.

Bunların başında ;

- OWASP(Open Web Application Security Project)
- OSSTMM(The Open Source Security Testing Methodology Manual)
- ISSAF(Information Systems Security Assessment Framework)
- NIST SP800-115

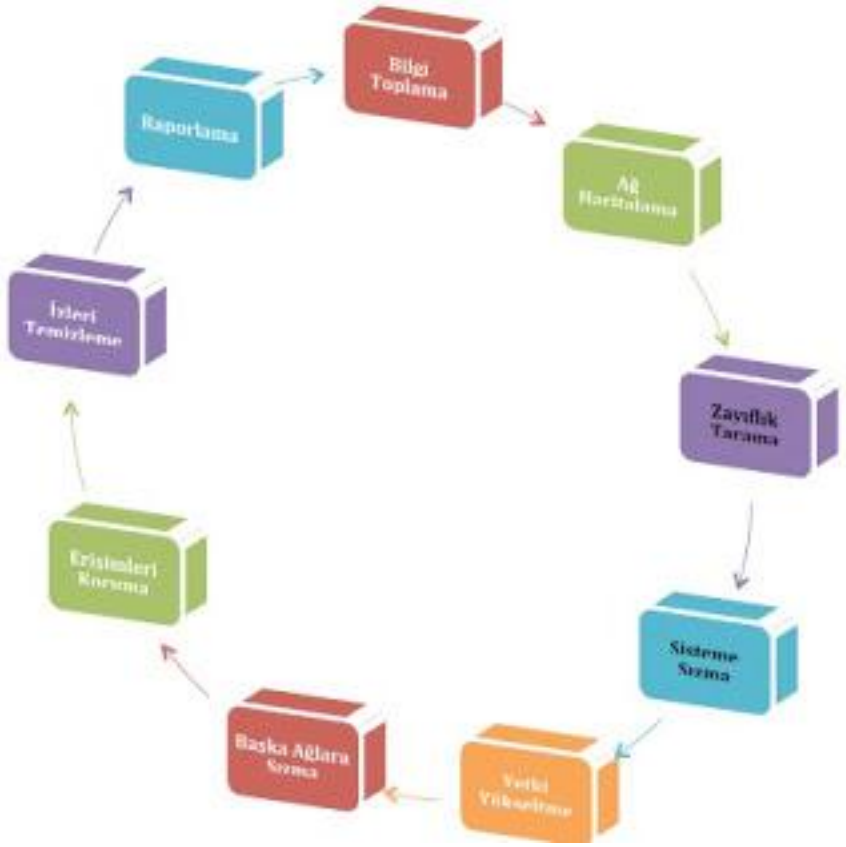
gelmektedir. Internetten ücretsiz edinilebilecek bu test metodojileri incelenerek yapılacak güvenlik denetim testlerinin daha sağlıklı ve tekrar edilebilir sonuçlar

üretmesi sağlanabilir.

Metodoloji hazırlanmasında dikkat edilmesi gereken en önemli hususlardan biri sızma test metodolojisinin araç tabanlı (X adımı icin Y aracı kullanılmalı gibi) olmamasına dikkat edilmesidir.

BGA Sızma Test Metodolojisi

Sızma testlerinde ISSAF tarafından geliştirilen metodoloji temel alınmıştır. Metodolojimiz üç ana bölümde dokuz alt bölümden oluşmaktadır.



1.1 [Bilgi Toplama]

Amaç, hedef sistem hakkında olabildiğince detaylı bilgi toplamaktır. Bu bilgiler firma hakkında olabileceği gibi firma çalışanları hakkında da olabilir. Bunun için internet siteleri haber gruplari e-posta listeleri , gazete haberleri vb., hedef sisteme gönderilecek çeşitli paketlerin analizi yardımcı olacaktır.

Bilgi toplama ilk ve en önemli adımlardan biridir. Zira yapılacak test bir zaman işidir ve ne kadar sağlıklı bilgi olursa o kadar kısa sürede sistemle ilgili detay çalışmalara geçilebilir.

Bilgi toplamada aktif ve pasif olmak üzere ikiye ayrılır. Google, pipl, Shodan, LinkedIn, facebook gibi genele açık kaynaklar taranabileceği gibi hedefe özel çeşitli yazılımlar kullanılarak DNS, WEB, MAIL sistemlerine yönelik detaylı araştırmalar gerçekleştirilir.

Bu konuda en iyi örneklerden biri hedef firmada çalışanlarından birine ait e-posta ve parolasının internete sızmış parola veritabanlarından birinden bulunması ve buradan VPN yapılarak tüm ağın ele geçirilmesi senaryosudur.

Sızma testlerinde bilgi toplama adımı için kullanılabilecek temel araçlar:

- FOCA
- theharvester
- dns
- Google arama motoru
- Shodan arama motoru
- E-posta listeleri, LinkedIn, Twitter ve Facebook

1.2 [Ağ Haritalama]

Amaç hedef sistemin ağ yapısının detaylı belirlenmesidir. Açık sistemler ve üzerindeki açık portlar, servisler ve servislerin hangi yazılımın hangi sürümü olduğu bilgileri, ağ girişlerinde bulunan VPN, Firewall, IPS cihazlarının belirlenmesi, sunucu sistemler çalışan işletim sistemlerinin ve versiyonlarının belirlenmesi ve tüm bu bileşenler belirlendikten sonra hedef sisteme ait ağ haritasının çıkartılması Ağ haritalama adımlarında yapılmaktadır.

Ağ haritalama bir aktif bilgi toplama yöntemidir. Ağ haritalama esnasında hedef sistemde IPS, WAF ve benzeri savunma sistemlerinin olup olmadığı da belirlenmeli ve gerçekleştirilecek sızma testleri buna göre güncellenmelidir.

Ağ Haritalama Amaçlı Kullanılan Temel Araçlar

- Nmap,
- unicornscan

1.3 [Zafiyet/Zayıflık Tarama Süreci]

Bu sürecin amacı belirlenen hedef sistemlerdeki açıklıkların ortaya çıkarılmasıdır. Bunun için sunucu servislerdeki bannerler ilk aşamada kullanılabilir. Ek olarak birden fazla zayıflık tarama aracı ile bu sistemler ayrı ayrı taranarak oluşabilecek false positive oranı düşürülmeye çalışılır.

Bu aşamada hedef sisteme zarar vermeycek taramalar gerçekleştirilir. Zayıflık tarama sonuçları mutlaka uzman gözler tarafından tekrar tekrar incelenmeli, olduğu gibi rapora yazılmamalıdır. Otomatize zafiyet tarama araçlar ön tanımlı ayarlarıyla farklı portlarda çalışan servisleri tam olarak belirleyememktedir.

Zafiyet Tarama Amaçlı Kullanılan Temel Araçlar

- Nessus
- Nexpose
- Netsparker

2.1 [Penetrasyon(Sızma) Süreci]

Belirlenen açıklıklar için POC kodları/araçları belirlenerek denelemeler başlatılır. Açıklık için uygun araç yoksa ve imkan varsa ve test için yeteri kadar zaman verilmişse sıfırdan yazılır. Genellikle bu tip araçların yazımı için Python, Ruby gibi betik dilleri tercih edilir.

Bu adımda dikkat edilmesi gereken en önemli husus çalıştırılacak exploitlerden önce mutlaka yazılı onay alınması ve mümkünse lab ortamlarında önceden denenmesidir.

Sızma Sürecinde Kullanılan Temel Araçlar

- Metasploit, Metasploit Pro
- Core Impact, Immunity Canvas
- Sqlmap
- Fimap

2.2 [Erişim Elde Etme ve Hak Yükseltme]

Sızma sürecinde amaç sisteme bir şekilde giriş hakkı elde etmektir. Bu süreçten sonra sistemdeki kullanıcının haklarının arttırılması hedeflenmelidir. Linux sistemlerde çekirdek (kernel) versiyonunun incelenerek priv. escelation zafiyetlerinin belirlenmesi ve varsa kullanılarak root haklarına erişilmesi en klasik hak yükseltme adımlarından biridir.

Sistemdeki kullanıcıların ve haklarının belirlenmesi, parolasız kullanıcı hesaplarının belirlenmesi, parolaya sahip hesapların uygun araçlarla parolalarının bulunması bu adımın önemli bileşenlerindendir.

Hak Yükseltme

Amaç edinilen herhangi bir sistem hesabı ile tam yetkili bir kullanıcı moduna geçişttir.(root, administrator, system vs)

Bunun için çeşitli exploitler denenebilir.

Bu sürecin bir sonraki adıma katkısı da vardır. Bazı sistemlere sadece bazı yetkili makinelerden ulaşılabiliyor olabilir. Bunun için rhost, ssh dosyaları ve mümkünse history'den eski komutlara bakılarak nerelere ulaşılabiliyor detaylı belirlemek gerekir.

2.3 [Detaylı Araştırma]

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

Linux sistemlerde en temel örnek olarak grep komutu kullanılabilir.
grep parola|password|sifre|onemli_kelime -R /

3.1 [Erişimlerin Korunması]
Sisteme girildiğinin başkaları tarafından belirlenmemesi için bazı önlemlerin alınmasında fayda vardır. Bunlar giriş loglarının silinmesi, çalıştırılan ek proseslerin saklı olması , dışarıya erişim açılacaksa gizli kanalların kullanılması(covert channel), backdoor, rootkit yerleştirilmesi vs.

3.2 [İzlerin silinmesi]

Hedef sistemlere bırakılmış arka kapılar, test amaçlı scriptler, sızma testleri için eklenmiş tüm veriler not alınmalı ve test bitiminde silinmelidir.

3.3 [Raporlama]
Raporlar bir testin müşteri açısından en önemli kısmıdır. Raporlar ne kadar açık ve detaylı/bilgilendirici olursa müşterinin riski değerlendirmesi ve açıklıkları gidermesi de o kadar kolay olur.

Testler esnasında çıkan kritik güvenlik açıklıklarının belgelenerek sözlü olarak anında bildirilmesi test yapan takımın görevlerindendir. Bildirimin ardından açıklığın hızlıca giderilmei için çözüm önerilerinin de birlikte sunulması gerekir.

Ayrıca raporların teknik, yönetim ve özet olmak üzere üç farklı şekilde hazırlanmasında fayda vardır.
Teknik raporda hangi uygulama/araçların kullanıldığı, testin yapıldığı tarihler ve çalışma

zamanı, bulunan açıklıkların detayları ve açıklıkların en hızlı ve kolay yoldan giderilmesini amaçlayan tavsiyeler bulunmalıdır.

Zamanlama

Hedef sistemlerin kritiklik durumlarına göre sızma testlerinin zamanlaması ayarlanmalıdır. DDoS testlerinin genellikle hafta sonu ve gece yarısı gerçekleştirilmesi önerilmektedir.

Bunun haricinde diğer testlerin gün içinde veya mesai saatleri sonrası yapılması tamamen müşterinin talebine bağlı değişkenlik göstermektedir. Fakat hedef sistemi performans açısından zorlayabilecek taramalar mesai saatleri dışında yapılması tercih edilmelidir.

Exploit Denemeleri

Sızma testlerinin en önemli adımlarıdan biri exploiting aşamasıdır. Bu adımla hedef sistem üzerinde bulunan güvenlik zafiyetleri istismar edilir ve sisteme sızılacak yollar belirlenebilir. Test yapan firmanın kalitesinin göstergelerinden biri de bu adımıdaki başarılarıdır.

Exploit çalıştırma denemelerinde mutlaka müşteri tarafı ile koordinasyon içinde olunmalı. Aksi hale hedef sistemi ele geçirmek amacıyla çalıştırılan bir exploit hedef sistemin bir daha açılmamasına, yeniden başlamasına ya da veri kaybına sebep olabilir.

BGA olarak genellikle test yapılacak firmalara ait bilişim sistemlerinin bir kopyaları kendi lab ortamımızda kurulu ve exploit öncesi denemeler gerçekleştirilir.

Pentest Çalışmasının Kayıt Altına Alınması

Bazı durumlarda hedef sistemde istenmeyen, beklenmeyen sonuçlar yaşanabilir. Testler esnasında hedef sistemden verilerin silinmesi, test yapılan ağın çökmesi, veya müşteri bilgilerinin internet ortamına sızması gibi. Bu gibi durumlarda sızma testlerini gerçekleştiren firmanın kendini sağlama alması açısından tüm sızma test adımlarının raw paket olarak kayıt altına alması önemlidir. Yaşanabilecek herhangi bir olumsuz durumda kayıt altına alınan paketlerden problem çözümü kolaylıkla sağlanabilir.

Pentest yapacak firma ne kadar güvenili olsa da-aranizda muhakkak imzalı ve maddeleri açık bir NDA olmalı- siz yine de kendinizi sağlama alma açısından firmanın yapacağı tüm işlemleri loglamaya çalışın.

Bunu nasıl yaparsınız? Firmanın pentest yapacağı ip adres bilgilerini isteyerek bu ip adreslerinden gelecek tum trafiği Snort veya benzeri bir yazılım kullanarak loglayabilirsiniz.

- Özellikle web trafiği -ki en kirik bilgiler burada çıkacaktır- Snort ile cok rahatlıkla sonradan incelendiğinde anlaşılacak şekilde kaydettirilebilir.

Bunun için Snort gibi açık kaynak kodlu araçlar kullanılabilir. BGA olarak gerçekleştirdiğimiz sızma testlerinde müşteri talep ederse bu tip bir altyapıyı sağlamaktayız.

Sızma Test Kalitesinin Ölçümü

Dikkat edilmesi gereken en önemli husus, firmanın yaklaşımıdır. Genellikle firmalar sızma testi yerine zayıflık tarama ile yetinmek istemektedir ki günümüzde zayıflık tarama işlemlerinin %90'ı Nessus, Netsparker, Nmap gibi yazılımlar kullanılarak gerçekleştirilebilmektedir. Önemli olan sızma testlerinde otomatize araçların ortaya çıkardığı bulguların teker teker incelenerek aralarında ilişki kurulabilmesi ve hedef sisteme sızmaya çalışmaktır.

Açıklığı bulup bunu raporlamak çoğu firma için yeterli olsa da gerçek bir sızma testi raporunda bulunan açıklık tüm yönleriyle incelenmeli ve hedef sisteme sızılabilirliğin gösterilmesidir.

Buna örnek olarak http://www.bga.com.tr/ornek_pentest_raporu.pdf adresindeki BGA sızma test sonuç raporu incelebilir.

Raporlama

Sızma testlerinin en önemli bileşenlerinden biri raporlamadır. Ticari açıdan yaklaşıldığında pentest yaptıran müşteri rapora para vermektedir. Dolayısıyla pentest raporunun olabildiğince detaylı ve müşteriyi doğru yönlendirecek nitelikte olması gerekir. Doğrudan otomatik analiz ve tarama araçlarının çıktılarını rapora eklemek müşterinin karşılaşmak istemediği durumların başında gelmektedir.

Raporun İletimi

Raporun mutlaka şifreli bir şekilde müşteriye ulaştırılması gerekir. Raporu açmak için gerekli olan parolanın e-posta harici başka bir yöntemle müşteriye ulaştırılabilir. Sık tercih edilen yöntem SMS kullanımıdır.

Bulguların Saklanması

Sızma teslerini yapan ekiplerin kullandıkları bilişim sistemleri ve sızma test sonçlarının saklandığı online, fiziksel ortamların koruma altında olması gerekmektedir. Aksi halde hedef sistemlere ait çok hassas bilgiler başkalarının eline geçebilir.
Bulguları saklamak için Truecrypt gibi disk şifreleme yazılımları kullanılabilir.

Anlık Acil Zafiyet Bildirimi

Bazı durumlarda hedef sisteme sızılacak bir yol, giriş kapısı bulunduğunda vakit geçirmeden müşteri detaylı olarak bilgilendirilmeli ve geçmişe yönelik adli bilişim analizi yapması önerilmelidir. Aksi halde pentest çalışması öncesi birilerinin sızdığı sistemden pentest sürecinde bir zarar gelirse pentest çalışmasını yapan firma zor durumda kalabilir.

Doğrulama Testleri

Doğrulama testleri yeni bir pentest çalışması gibi değildir ve ana pentest çalışmasının ayrılmaz bir parçasıdır. Doğrulama testleri için ek bir ücret talep edilmez.
Doğrulama testlerinde çalışmayı gerçeklştiren firmadan raporda yazılan tüm açıklıkların kontrol etmesi istenir. Bu esnada yeni açıklıklar incelenmez.

Sızma Test Çalışması Sonrası Yapılması Gerekenler

Pentest yaptırmak ne kadar önemliyse sonuçlarını değerlendirip aksiyon almak çok daha önemlidir.Malesef ki yaygın olarak yapılan yanlış sadece pentest yapıp raporu incelemek oluyor.
Pentest sonrası açıklıkların kapatılmaması ve bir sonraki pentestde aynı açıklıkların tekrar çıkması sık karşılaşılan bir durumdur.

- Pentest raporlarının üst yönetimle paylaşılıp yönetim desteğinin alınması
- Sonuçlarının basit açıklıklar olarak değil, bir risk haritası kapsamında yönetime sunulması(bu açıklık hackerlar tarafından değerlendirilirse şu kadar kaybımız olur gibisinden)
- Raporu detaylıca inceleyip her bir açıklığın kimin ilgi alanına girdiğinin belirlenmesi

- Sistem yöneticileri/yazılımcılarla toplantı yapıp sonuçların paylaşılması
- Açıklıkların kapatılmasının takibi
- Bir sonraki pentestin tarihinin belirlenmesi

Sızma Testlerinde Kullanılan Araçlar:

Öncelikle sızma test kavramının araç bağımsız olduğunu belirtmek gerekir. Bu konudaki yazılımlar

Açık kodlu bilinen çoğu pentest yazılımı Backtrack güvenlik CDsi ile birlikte gelir. Bu araçları uygulamalı olarak öğrenmek isterseniz Backtrack ile Penetrasyon testleri eğitimine kayıt olabilirsiniz.

Ticari Pentest Yazılımları: Immunity Canvas, Core Impact, HP Webinspect, Saint Ssecurity Scanner

Sızma Testleri Konusunda Uzmanlık Kazanma

Pentest konusunda kendinizi geliştirmek için öncelikle bu alana meraklı bir yapınızın olmasın gerekir. İçinizde bilişim konularına karşı ciddi merak hissi , sistemleri bozmaktan korkmadan kurcalayan bir düşünce yapınız yoksa işiniz biraz zor demektir.
Zira pentester olmak demek başkalarının düşünemediğini düşünmek, yapamadığını yapmak ve farklı olmak demektir.
Bu işin en kolay öğrenimi bireysel çalışmalardır, kendi kendinize deneyerek öğrenmeye çalışmak, yanılmak sonra tekrar yanılmak ve doğrsunu öğrenmek. Eğitimler bu konuda destekci olabilir. Sizin 5-6 ayda katedeceğiniz yolu bir iki haftada size aktarabilir ama hiçbir zaman sizi tam manasıyla yetiştirmez, yol gösterici olur.

Pentest konularının konuşulduğu güvenlik listelerine üyelik de sizi hazır bilgi kaynaklarına doğrudan ulaştıracak bir yöntemdir.
Linux öğrenmek, pentest konusunda mutlaka elinizi kuvvetlendirecek, rakiplerinize fark attıracak bir bileziktir. Bu işi ciddi düşünüyorsanız mutlaka Linux bilgisine ihtiyaç duyacaksınız.

Sızma Testleri Konusunda Verilen Eğitimler

- Bilgi Güvenliği AKADEMİSİ Pentest Eğitimleri
- Ec-Council Pentest Eğitimleri
- SANS Pentest Eğitimleri
- Offensive Security Pentest Eğitimleri

BGA Sızma Test Hizmetleri hakkında detay bilgi almak için bilgi@bga.com.tr adresine e-posta gönderebilirsiniz.

Huzeyfe ÖNAL <huzeyfe.onal@bga.com.tr>