ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/bilgi-guvenliginde-sizma-testleri/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Bilgi%20G%C3%BCvenli%C4%9Fi%20A%C3%A7%C4%B1s%C4%B1ndan%20S%C4%B1zma%20Testleri.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Vulnerability assessment çalışmaları sızma testleri kadar tecrübe zaman gerektirmeyen çalışmalardır

(page 4)

2)

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

3)

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

(Page 6-7)

4)

Sızma Testi Metadolojisi

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

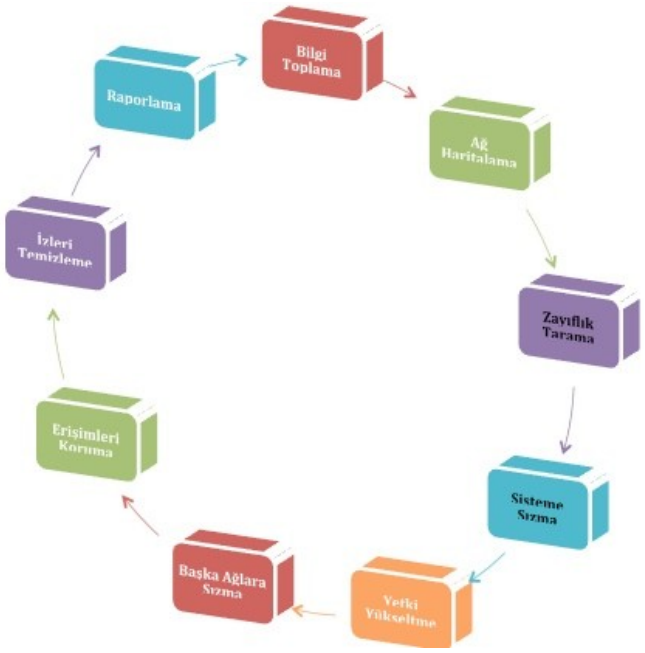
Metodoloji hazırlanmasında dikkat edilmesi gereken en önemli hususlardan biri sızma test metodolojisinin araç tabanlı (X adımı icin Y aracı kullanılmalı gibi) olmamasına dikkat edilmesidir**.**

(Page 8-9)

5)

BGA Sızma Test Metodolojisi

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



1. **Bilgi Toplama**

   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

2. **Ağ Haritalama**

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

3. Zafiyet Tarama Süreci

Bu aşamada hedef sisteme zarar vermeyecek taramalar gerçekleştirilir. Zayıflık tarama sonuçları mutlaka uzman gözler tarafından tekrar tekrar incelenmeli, olduğu gibi rapora yazılmamalıdır. Çünkü otomatize zafiyet tarama araçları ön tanımlı ayarlarıyla farklı portlarda çalışan servisleri tam olarak belirleyememektedir.

Zafiyet Tarama Araçları

- Nessus
- Nexpose
- Netsparker

4. Sızma Süreci

Açıklıktan sızmak için uygun araç yoksa ve imkan varsa ve test için yeteri kadar zaman verilmişse sıfırdan araç yazılır. Genellikle bu tip araçların yazımı için Python, Ruby gibi betik diller tercih edilir. Bu adımda dikkat edilmesi gereken en önemli husus çalıştırılacak exploit'lerden 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

5. Erişimi Elde Etme ve Hak Yükseltme

Sızma sürecinde amaç sisteme bir şekilde giriş hakkı elde etmektir.

6. Hak Yükseltme

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. Amaç edinilen herhangi bir sistem hesabı ile tam

yetkili bir kullanıcı moduna geçiştir.(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.

7. **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 /

8. **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.

9. **İzlerin Silinmesi**

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

10. **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.

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.

(Page 10-12)

6)

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

(Page 12)

7)

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 adımdaki başarılarıdır.

Exploit çalıştırma denemelerinde mutlaka müşteri tarafı ile koordinasyon içinde olunmalı. Aksi halde hedef sistemi ele geçirmek amacıyla çalıştırılan bir exploit hedef sistemin bir daha açılmamasına, yeniden başlamamasına ya da veri kaybına sebep olabilir. BGA olarak genellikle test yapılacak firmalara ait bilişim sistemlerinin bir kopyaları kendi lab ortamımızda kuruludur ve exploit öncesi denemeler gerçekleştirilir.
(Page 12)

8)

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 sızılabilirlik gösterilmelidir.

(Page 13)

9)

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.

(Page 13)

10)

Pentest konusunda kendinizi geliştirmek için öncelikle bu alana meraklı bir yapınızın olması 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 doğrusunu 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.

(Page 15)