iPhone Notlar

a)

.APK vs. .IPA

Mobil akıllı telefonlarda uygulama mağazalarından indirdiğimiz uygulamalar android cihazlara .apk şeklinde, iOS cihazlara .ipa şeklinde inerler ve kurulurlar.

APK android cihazların bir dosya uzantısıdır. IPA iOS cihazların bir dosya uzantısıdır.

Kaynak:

https://geekflare.com/mobile-app-security-scanner/
https://medium.com/productmafia/nedi%CC%87r-1-apk-ve-ipa-nedir-14c3e8620153
https://en.wikipedia.org/wiki/.ipa
https://thebigbrains.com/full-form-of-apk-and-ipa/

b)

Mobsf Tool'u ile iOS Uygulamaları Tarama Hakkında

Mobsf OWASP tarafından tavsiye edilen bir Mobil Güvenlik Testi aracıdır. Mobsf ile mobil uygulamalara binary analiz, kaynak kod analiz ve dinamik analiz yapılabilir. MobSF hem Android hem de iOS uygulamalar için kullanılabilir. Fakat MobSF dinamik analizde sadece Android'lere destek sunar. iOS uygulamalara dinamik analiz desteği sunmaz. Ayrıca kaynak kod analizinde sadece Objective-C programlama dili ile yazılmış iOS uygulamalar desteklenmektedir. Dolayısıyla MobSF ile iOS uygulamalara dinamik zafiyet tarama yapılamaz ve kaynak kod analizinde iOS uygulamaları tarama sadece Object-C dili desteği ile sınırlıdır.

Kaynak:

https://www.netguru.com/blog/ios-security-analysis-with-mobsf

c)

Harici Kaynaklardan İnen IPA Dosyalar Nasıl iOS Mobil Cihazlara Atılır?

Android'lere göre iOS platformu çok daha güvenliklidir. Bu nedenle Android cihazlarda olduğu gibi harici bir uygulama bilgisayardan indirip mobil cihaza iOS'larda atılamaz. Eğer bilgisayardan harici bir kaynak aracılığıyla iOS uygulama indirip iOS mobil cihaza atmak istiyorsak iOS mobil cihaz jailbreak'li olmalıdır.

Kaynak:

https://thebigbrains.com/full-form-of-apk-and-ipa/

d)

iOS Cihazlarda Jailbreak ile Gelen Cydia Bağımsız Uygulama Mağazası

iOS cihazlara Jailbreak uygulanması cihazın temel özelliklerini değiştirmez ve jailbreak uygulanmış bir iPhone veya iPad'e Apple App Store'dan uygulama satın alınıp indirilmeye devam edilebilir. Fakat bunun yanısıra Jailbreak uygulanmış bir iPhone veya iPad'e Apple'ın reddettiği uygulamaları indirmek veya jailbreak'in sağladığı ek özelliklerden faydalanmak için bağımsız uygulama mağazaları da kullanılabilir. Bunların en popüleri genelde jailbreak işlemi sırasında yüklenen ve jailbreak uygulanan iOS cihazlar için sanal vitrin niteliğinde olan "Cydia" mağaza uygulamasıdır.

Kaynak:

https://www.kaspersky.com.tr/resource-center/definitions/what-is-jailbreaking
https://medium.com/productmafia/nedi%CC%87r-1-apk-ve-ipa-nedir-14c3e8620153

e)

plist Nedir ve Güvenliğe Dokunan Yanı

MacOS ve iOS programlama framework'lerinde "property list" şeklinde dosyalar vardır. Bu dosyalar sıklıkla kullanıcı ayarlarını depolamak için kullanılırlar. Ayrıca uygulama hakkında bilgi depolamak için de kullanılırlar. Property list dosyaları .plist uzantısını alırlar. Bu nedenle sıklıkla p-list dosyalar olarak adlandırılırlar.

Plist dosyalar key-value şeklinde veri içerirler ve bir XML dosyasıdırlar. Kalıcı bir şekilde veri depolama yöntemidirler. Bu nedenle bazen bu dosyalarda hassas bilgi bulunabilir. Plist dosyalarının uygulama yüklendikten sonra ve ayrıca plist dosyasına yeni bir veri yazılıp yazılmadığını anlamak adına uygulamayı yoğun bir şekilde kullandıktan sonra kontrol edilmesi tavsiye edilir.

```
> find ./ -name "*.plist"
```

Benim Not:

info.plist dosyasında güvensiz ATS konfigurasyonu hakkında Coverity kaynak kod analizinin bir testte raporladığı bulgunun hazırladığım şablon dosyası için bkz. /home/hefese/Desktop/Yaz Tatili - 2014/Tubitak/Pentest Raporları/Kaynak Kod Analizi Raporlarım/Şablon (Güvensiz ATS Yapılandırması) - 2022.txt

Kaynak:

https://book.hacktricks.xyz/mobile-apps-pentesting/ios-pentesting
https://en.wikipedia.org/wiki/Property_list

f)

Bundle Nedir?

Çalıştırılabilir kodları ve bu çalıştırılabilir kodlarla ilgili kaynakları (örn; resimleri, sesleri) tek bir yerde bir arada gruplayan dosya sistemindeki bir klasöre Bundle adı verilir. iOS'ta tam bir

yüklemeye hazır uygulama paketlerine genellikle Bundle denmektedir. Bundle'ın Türkçe kelime karşılığı Bohça demektir.

Kaynak:

https://book.hacktricks.xyz/mobile-apps-pentesting/ios-pentesting

https://developer.apple.com/library/archive/documentation/General/Conceptual/DevPedia-CocoaCore/Bundle.html

g)

iOS .ipa Uygulama Dosyalarının İçerik Yapısı

iOS işletim sisteminde uygulama dosya uzantısı olan .ipa dosyaları zip paketleridirler. Dolayısıyla .ipa dosyasının uzantısını .zip şeklinde değiştirip zip arşiv dosyasını açarak içeriğine erişmek mümkündür. Zip arşivi içerisinde <NAME>.app şeklinde bir klasör olacaktır. Bu klasörün içerisinde ise uygulamaya dair her bir bileşen yer alacaktır.

.ipa dosyalarının içerisinde şu dosyalar ve klasörler yer alır:

> Benim Not:
>
> Aşağıda bahsedilen dosyalar ve dizinler .ipa uygulama dosyalarında gerçekten var mı diye
>
> https://iosninja.io/ipa-library
>
> adresinden rastgele bir ipa dosyası indirilmiştir ve zip ile açılarak bu dosyaların ve klasörlerin her birinin var olduğu görülmüştür (Not: Sadece Core Data/ dizini görülememiştir). İlaveten uygulamaya has dosya ve klasörlerin de var olduğu görülmüştür.

Info.plist Dosyası	: Uygulamaya özel konfigurasyonların bazılarını içerik olarak tutar.
_CodeSignature/ Dizini	: Uygulamanın bundle'ındaki tüm dosyalar üzerinde bir imzası olan plist dosyası tutar.
Assets.car Dosyası	: Uygulamaya ait icon'ları içerik olarak tutar.
Frameworks/ Dizini	: Uygulamaya ait kütüphaneleri .dylib uzantılı dosya halinde veya .framework uzantılı klasör halinde tutar.
Plugins/ Dizini	: .appex uzantılı uygulamaları içerik olarak tutar.
Core Data/ Dizini	: Bu klasör uygulamanın offline kullanımı için depolanacak uygulama kalıcı verilerilerini tutar. Örneğin tek bir cihaz üzerinde geçici verilerin cache'lenmesi gibi, veya geri al (undo) seçeneğinin uygulanabilmesi adına verilerin kaydedilmesi gibi bu türden veriler tutulur. iCloud hesabı ile birden fazla cihaza senkronizasyon kurmak için senkronizasyon açıldığında Core Data otomatik olarak CloudKit

container’ına depoladığı verileri kopyalar ve böylece birden fazla cihazda uygulamaya dair geçmiş verileri senkronize olur.

PkgInfo Dosyası : Bundle’ın türünü ve yaratıcı kodlarını belirten bilgiler tutar. PkgInfo dosyası bu bilgileri belirtmenin alternatif bir yoludur.

en.lproj, fr.proj Dosyaları : Belirli diller için uygulama dil paketi bilgilerini içerir.

Kaynak:

https://book.hacktricks.xyz/mobile-apps-pentesting/ios-pentesting#ipa-structure

h)

iOS Pentesting Checklist Sitesi

https://book.hacktricks.xyz/mobile-apps-pentesting/ios-pentesting-checklist

i)

Jailbreak alma işlemi basittir ve yaklaşık 2 ile 5 dakika arasında bir vakit alır. Belirli iOS versiyonlarını jailbreak’lemek için ilgili araçlar şu şekildedir:

iOS Version	Jailbreak provider/tool
11.0 → 14.3	uncOver
10.0 → 10.3.4	doubleH3lix
9.3.5 → 9.3.6	Phoenix
9.1 → 9.3.4	Home Depot

Kaynak:

https://cobalt.io/blog/ios-pentesting-101

j)

iPhone cihazlara sürümden sürüme değişen jailbreak uygulamaları indirmek için şu adresten yararlanılabilir:

https://iosninja.io/ipa-library#jailbreak

k)

Objective-C ve Swift

Objective-C genel amaçlı kullanılan “nesne yönelimli bir C programlama dili”dir. Apple macOS ve iOS platformlarına uygulamalar geliştirmek için Objective-C nesne yönelimli c programlama dilini 2014 yılına kadar standart bir programlama dili olarak kullanmıştır. 2014 yılına gelindiğinde ise Apple firması geliştirdiği Swift adlı nesne yönelimli yeni bir programlama dilini duyurmuştur. Apple artık bu geliştirdiği Swift programlama dili ile macOS ve iOS platformlarına uygulama geliştirmektedir.

Kaynaklar:

https://en.wikipedia.org/wiki/Objective-C
https://tr.wikipedia.org/wiki/Swift_(programlama_dili)

l)

Sideloading

Sideloading AltStore, Cydia Impactor, Xcode gibi bir iphone uygulaması kullanarak bilgisayardan iphone cihaza .ipa dosyaları yüklemeye denir. Yani bilgisayardan iPhone cihaza uygulama aktarmaya / yüklemeye sideloading adı verilmektedir. Bu sayede iPhone cihaza iPhone cihazdaki Apple Store dışında bir uygulama yüklenir. Apple bu işleme resmi olarak izin vermemektedir ya da onaylamamaktadır.

Kaynak:

https://tweak-box.com/tr/altstore-indir/