iPhone 5S’e Pentest Yapılacak Bir IPA Uygulaması Atma

Mobil uygulama pentest’lerinde müşteriden alınabilecek iOS uygulama kurulum dosyasını (.ipa uzantılı dosyayı) iphone mobil cihazda kurmak için şu adımlar takip edilmelidir:

a) iOS Uygulama Kurulum Dosyasını (.IPA’yı) Safari Web Tarayıcısı ile İndirme

iPhone cihazın safari web tarayıcısından uygulama ipa dosyası indirilir. Örneğin kasıtlı zafiyetler içeren iOS uygulaması Damn Vulnerable iOS App (DVIA) gibi.

DVIA.ipa İndirme:

https://damnvulnerableiosapp.com/

https://github.com/prateek147/DVIA-v2/releases/download/v2.0/DVIA-v2-swift.ipa

b) iOS Uygulama Kurulum Dosyasını (.IPA’yı) iOS Cihazda Kurma

1. iPhone cihaz jailbreak’lendikten sonra gelen Cydia mağazası açılır.

2. Cydia mağazasında ipa kurulumu yapan uygulamayı indirebilmek için repository eklenir. Bunun için;

Cydia Uygulaması -> Sources -> Edit -> Add -> https://cydia.akemi.ai/ -> Add Source

adımları takip edilir.

3. Ardından Cydia Uygulaması -> Search sekmesinden ipa kurulumu yapan şu iki birbirini tamamlayan uygulama indirilir:

- AppSync Unified

- Filza File Manager

Not:

iPhone 5S’e jailbreak sürecine başlarken unc0ver jailbreak ipa uygulamasını AltStore Client uygulaması ile kurduğumuz gibi (bkz. iPhone 5S JailBreak Yapma.docx) AltStore Client ile yeni ipa uygulamalar da kurabiliriz. AltStore Client ile DVIA uygulamasını ipa’sı kurulmaya çalışıldığında başarılı şekilde kurabilmiştir. Fakat AltStore’un jailbreak’li mağaza Cydia’dan indirilen ipa kurucu uygulamaya göre dezavantajları vardır. Örneğin iphone cihazdaki AltStore Client ile en fazla 3 adet ipa kurulumu yapılabilmektedir. Daha fazla ipa kurulumu yapılamamaktadır. Çünkü AltStore Client’ta resmi apple id geliştirici hesabı premium olanlar sadece sınırsız yetkilere sahiptir. Bizim gibi resmi apple id geliştirici hesabı free olan hesaplarda ipa kurulumu yapma

kısıtı vardır. İkinci olarak AltStore Client uygulaması ipa kurulumu için bilgisayara (bilgisayardaki AltStore Server'a) ihtiyaç duyar. AltStore Client ile ipa kurulumu yapabilmek için iPhone 5S cihazı usb kablo ile bilgisayara bağlı olmalıdır, bilgisayarda iTunes, iCloud ve AltStore Server açık olmalıdır, ve iTunes'da iPhone mobil cihazın "Wifi Sync" ayarı tick işaretli olmalıdır. Ancak bu gereksinimler sayesinde iPhone mobil cihaza safari web tarayıcıdan inen ipa kurulum dosyası mobil cihazdaki AltStore client uygulaması ile kurulabilmektedir. Mobil cihazdaki AltStore Client'ta ipa kurulumu bilgisayarsız yapılamamaktadır. Üçüncü dezavantaj ise AltStore Client uygulamasında kurulan ipa uygulamalar 7 günlük süreye sahiptir. 7 gün sonunda kurulumların yeniden tekrarlanması gerekmektedir. Bu dezavantajlar dolayısıyla jailbreak'lenmiş iphone cihazda jailbreak Cydia mağazasından ipa kurucu uygulama indirmek ve bu ipa kurucu uygulama aracılığıyla iphone cihaza sınırsız bir şekilde ipa uygulaması kurmak daha pratiktir. AltStore Client'ı jailbreak yokken jailbreak uygulamasını atmak için kullanmıştık. Artık jailbreak var olduğundan jailbreak cydia mağazasındaki sınırsız ipa kurmayı sağlayan uygulamalardan yararlanabiliriz.

4. Daha sonra iPhone cihazda indirilmiş ipa kurulumunun yer aldığı klasöre gidilir.

    Files -> iCloud Drive -> DVIA.ipa

5. İnmiş IPA dosyasının üzerine basılı tutulur ve

    Share -> Copy to Filza

denir.

6. Ardından iPhone cihazda ana ekrana dönülür, Filza Uygulamasına girilip açılan ekrandaki ipa dosyasına tıklanır ve Install denir.

7. Bu adımlar neticesinde iPhone cihazda IPA kurulumu tamamlanır.

c) iOS Uygulama Kurulum Dosyasını (.IPA'yı) iOS Cihazda Çalıştırma

1. DVIA uygulaması cihazın ana ekranında uygulamalar arasında yer alır.

2. Kurulan uygulamaya tıklanır ve başlatılır.

Sonuç

Mobil uygulama pentest'lerinde müşteriden alınabilecek iOS uygulama kurulum dosyasını (.ipa uzantılı dosyayı) iphone mobil cihazda kurmak özetle şu adımlardan oluşur:

a) iOS uygulama kurulum dosyası (.ipa uzantılı dosya) mobil cihaza Safari web tarayıcısı ile indirilir.

b) iOS uygulama kurulum dosyası (.ipa uzantılı dosya) mobil cihazdaki jailbreak mağazası Cydia ile yüklenmiş ipa kurulumu yapan AppSync ve Filza uygulaması ile kurulur.
c) iOS uygulama kurulum dosyası (.ipa uzantılı dosya) mobil cihazda çalıştırılır.

Bu adımlar neticesinde ipa kurulum dosyası iphone cihazda kurulur ve çalıştırılarak mobil penteste hazır hale gelir.

Kaynaklar:

https://www.reddit.com/r/jailbreak/comments/dtdhra/question_how_to_install_ipa_files/

https://www.youtube.com/watch?v=QOeyrLo7bQM