iOS Jailbreaking - 10.3.3 & 12.4

Prepared By:
Sahad

iOS Jailbreaking

iOS jailbreaking is the process of gaining root access to iOS devices. It removes the software restrictions implemented by Apple. It is similar to the rooting process of Android devices. The jailbreaking method differ based upon the version of iOS.

Why Mobile Pentesters Care about Jailbreaking?
1. Jailbreaking allows pentesters to install security tools from third-party repo like Cydia, Sileo, etc.
2. Root access to the filesystem
3.Unrestricted debugging and dynamic analysis

Here I'm going to explain the Jailbreaking process of version **10.3.3** and **12.4**.

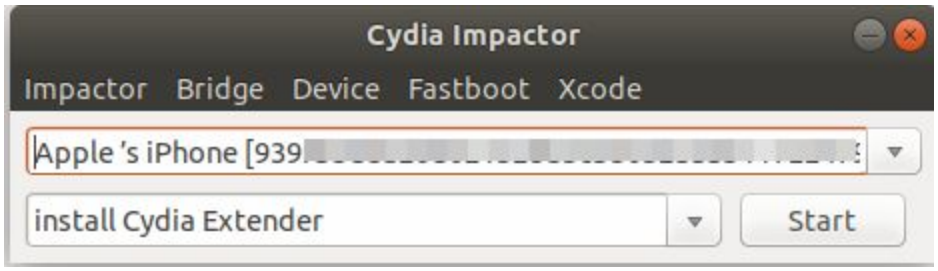
1. Jailbreaking iOS 10.3.3(Goblin with Cydia)

Follow the given below steps for Jailbreaking:
Part 1:
Sideload the Goblin package on your iOS device

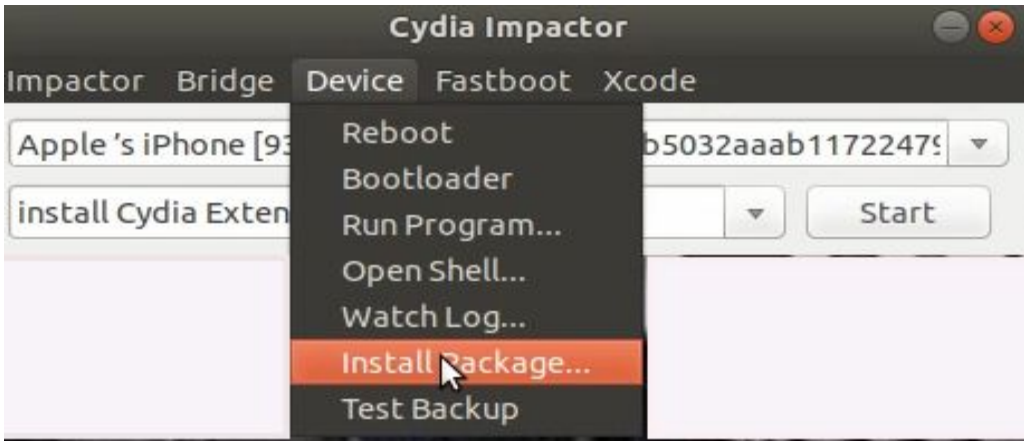
1. Download Cydia Impactor and Goblin Packages

    a.Cydia Impactor
    b.g0blin

2. Run **Cydia impactor** binary in your PC and connect your iOS device.



3. Choose Install Package option from Device Menu and select the **Goblin IPA** file.



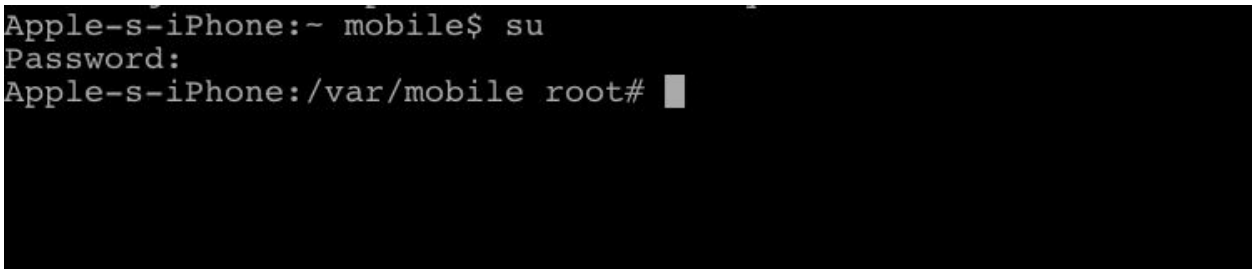
4. After Entering your Apple account credentials, Cydia impactor starts the Goblin package installation on your device.

Part 2:
Run the goblin and start the Jailbreaking on your device.

1.Verify the Goblin app by Trust the installed developer profile.
go to “Settings -> General -> Device Management-> trust (installed developer profile)

2. Now open the Goblin app and click the 'Jailbreak' button.

The Jailbreak process will start and finish within few seconds and device reboots.



*Now you will have a Jailbroken device with package manager **Cydia**.*

Fix Error:

Revoke the certificates if you get the following error(**provision.cpp ;line 81**).

Go to the **Xcode -> Revoke Certificate**. Then enter your Apple credentials. Reinstall the Goblin package after completion of the revocation process.

Success Message After Certificate Revocation:

2. Jailbreaking iOS 12.4 (Chimera with Sileo)

Follow the given below steps for Jailbreaking:

Part 1:
Sideload the Chimera package on your iOS device

1.Download Cydia Impactor and Chimera Packages

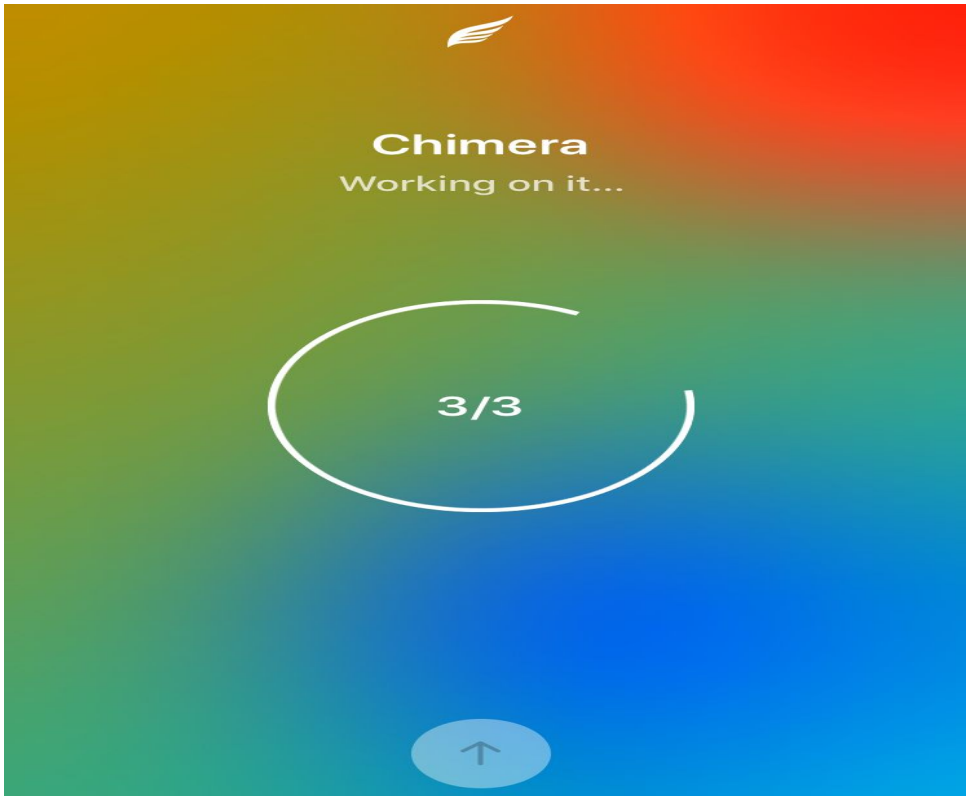
a.Cydia Impactor
b.Chimera

Follow the same steps that explained in **Part 1** of Jailbreaking iOS 10.3.3

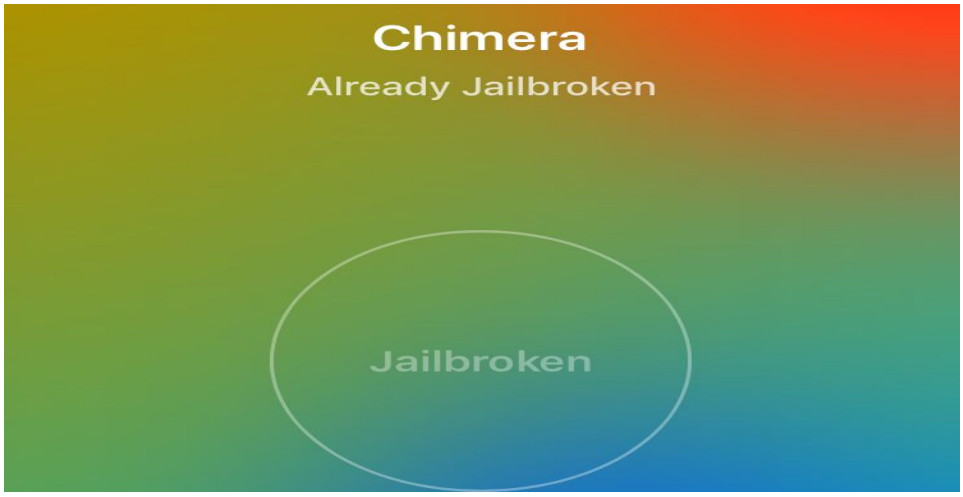
Part 2:
Run the Chimera and start the Jailbreaking on your device.

1.Verify the Chimera app by Trust the installed developer profile.
go to “Settings -> General -> Device Management-> trust (installed developer profile)

2. Now open the Chimera app and click the 'Jailbreak' button



The Jailbreak process will start and finish within few seconds



*Now you will have a Jailbroken device with package manager **Sileo**.*

Fix Error:

If you are stuck at any point of the jailbreak process, do the rootFS Restore in chimera and retry the Jailbreak process.