链滴

Frieda 的简单使用

作者：kidcao

原文链接：https://ld246.com/article/1632709665087

来源网站：链滴

Frida 介绍

frida是一款基于python + javascript 的hook框架，可运行在androidioslinuxwinosx等各平台，主使用动态二进制插桩技术。

1. 插桩技术

插桩技术是指将额外的代码注入程序中以收集运行时的信息，**可分为两种**：

- 源代码插桩[Source Code Instrumentation(SCI)]：额外代码注入到程序源代码中。
- 二进制插桩（Binary Instrumentation）：额外代码注入到二进制可执行文件中。

●静态二进制插桩[Static Binary Instrumentation(SBI)]：在程序执行前插入额外的代码和数据，生成个永久改变的可执行文件。

●动态二进制插桩[Dynamic Binary Instrumentation(DBI)]：在程序运行时实时地插入额外代码和数，对可执行文件没有任何永久改变。

2. 你能用DBI做些什么呢

- 访问进程的内存
- 在应用程序运行时覆盖一些功能
- 从导入的类中调用函数
- 在堆上查找对象实例并使用这些对象实例
- Hook，跟踪和拦截函数等等

安装 Frida

frida-server 安装

下载 frida-server

Frida 可以在多个平台中运行(Windows/Android/iOS等)，这里先介绍Android

首先打开下载地址

根据需要下载对应的版本，例如我的设备是Intel平台MacBook Pro的网易mumu安卓模拟器，那么就该下载**frida-server-15.1.2-android-x86_64.xz**

如果是安卓真机，那么就下载**frida-server-15.1.2-android-arm64.xz**。

注意要区分不同环境下的平台，不要下载错了。

安装运行

如果目标设备是真机，那么请提前把设备root。如果是模拟器，先把root权限打开。

打开终端，使用命令 **adb devices** 查看设备是否被adb检查到了

如果没找到，先执行这条命令 **adb kill-server**，再去查找一般都能找到。

双击下载的文件，然后把解压的文件传入到手机指定位置。

```
# 传入文件
adb push 文件存放地址 /data/local/tmp

# 给文件修改权限
chmod 777 文件名

# 执行前确保设备已获得root
./文件名
```

如果报错了有两个可能：

- 下载的文件不对，没有和环境对应上
- 设备没有获得root权限

安装 Frida

直接使用 **pip install frida** 就可以安装了。

简单使用

1. 打开app
2. 获取app在frida中的名字，命令是：frida-ps -U

执行结果：

```
 266  servicemanager
 381  sh
1936  sh
 267  surfaceflinger
 676  system_server
 106  ueventd
 108  ueventd
 269  vinput
 260  virtual_shell
 232  vold
 847  wpa_supplicant
 291  zygote
 290  zygote64
1322  京东
```

代码执行，例如我想获取京东的sign

```
import frida
import json

rpc_sign = """
rpc.exports = {
    getsign: function(function_id, body_string, uuid){
      var sig = "";
      Java.perform(
        function(){
            //拿到context上下文
            var currentApplication = Java.use('android.app.ActivityThread').currentApplication();
            var context = currentApplication.getApplicationContext();
            var BitmapkitUtils = Java.use('com.jingdong.common.utils.BitmapkitUtils');
            sig = BitmapkitUtils.getSignFromJni(context, function_id, body_string, uuid, 'android', '
.2.0');


            //console.log(context, uuid)
        }
      )
       return sig;
    }
};

"""


def get_sign(function_id, body_string, u):
    process = frida.get_remote_device().attach('京东')

    script = process.create_script(rpc_sign)
    script.load()
    sign = script.exports.getsign(function_id, body_string, u)
    return sign


if __name__ == '__main__':
    body_data = {"appId": "jd.mall",
                 "content": "tbV8seY199tCdw6GllmkWyCNNENuGsgwLByA7svt5HbPXvlI9wQhHMk
```

```
dT7f0ldfpq6M0MCiUD+A\nVrY390Yct0FSub03INUml9n1bS9rZSF3XT0q1kQdehKPO4CccMiEA
NQXYiqYn9wLsDDYEIjmkVA\nEbXI88CwO0K7uhwemdhQMZrcIFj6jMmyiDNDxSA1OjFw88hR0
SCF0m8ll9o9iU2MVSHDipF5ZDn\nFR4E+82mwfRYIxamafB+nWG8GuHcKhiQOWGbChTcG3Tx
GT053wfcc6uuMD7+L4PcsNRQjM9syFc\nXR6FBu/sCV/kH/3rT8w/m3zV1c9JpW9lq/7WVzCVvA
j7RNt2zzYFisymCE="}
    body_string = json.dumps(body_data, ensure_ascii=False).replace(" ", "")
    function_id = 'liveauth'
    u = '-a08d16f38776'
    sign = get_sign(function_id, body_string, u)
    print(sign)
```

可能遇到的错误：

1. 提示：frida.ServerNotRunningError: unable to connect to remote frida-server

解决1：没有打开 frida-server，按照上面的教程打开 server

解决2：端口没有转发，执行一下这个命令：adb -s emulator-5554 forward tcp:27042 tcp:27042

2. 提示：frida.ProcessNotFoundError: unable to find process with name 'xxx'

解决：这是因为app的包名填错了，先用：frida-ps -U 找到想操作的包名，然后再填入到这里：frida get_remote_device().attach('京东')