Hacking Mobile Apps with Frida

Hacking Mobile Apps with Frida and the other tools that are based on Frida which don't always show it.

ABOUT ME

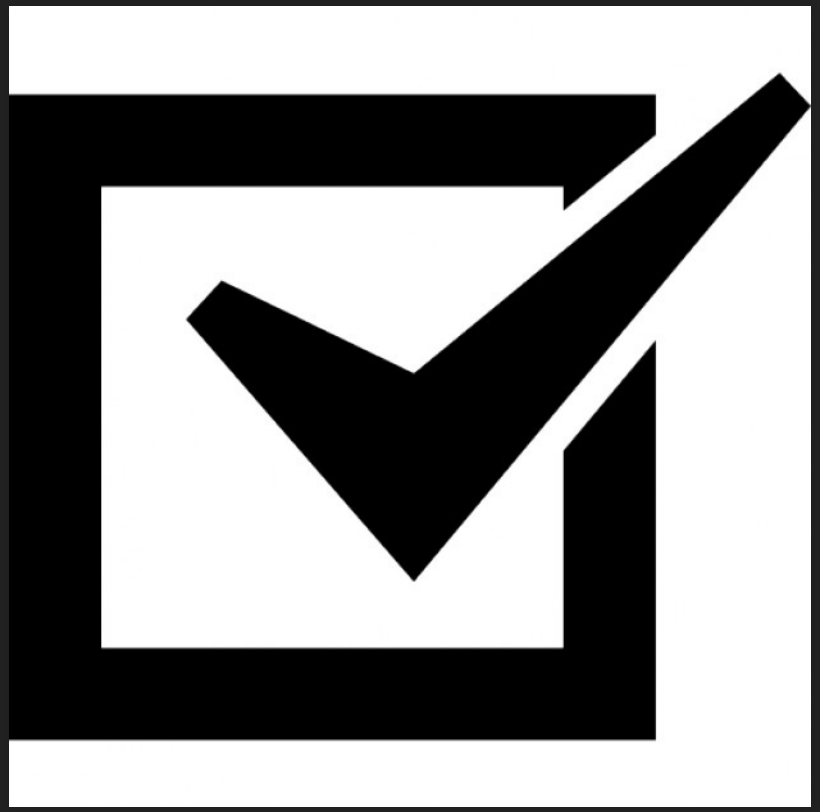
Jobs Before Pentesting (in order):

- US Army
- Throwing Newspapers
- Home Depot
- Web Developer
- Construction
- Programmer
- Systems Eengineer
- Network Engineer
- DoD InfoSec Blue Team

That's great. WTF are we doing here?

TRAFFIC ANALYSIS

CONFIG ANALYSIS



STATIC ANALYSIS

DUNZO

What is Frida?

What can we do with it?

How does it work?

Two Modes: Interceptor & Stalker

INTERCEPTOR

STALKER

Setup

WORKSTATION

virtualenv -p python3 ~/.venv/frida

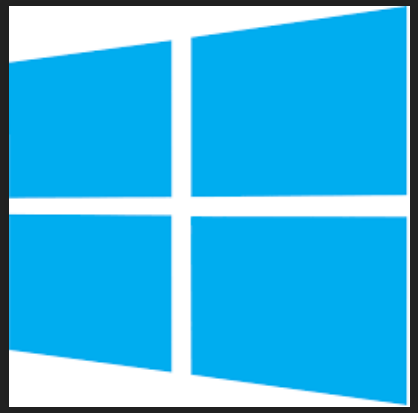
pip install -U frida

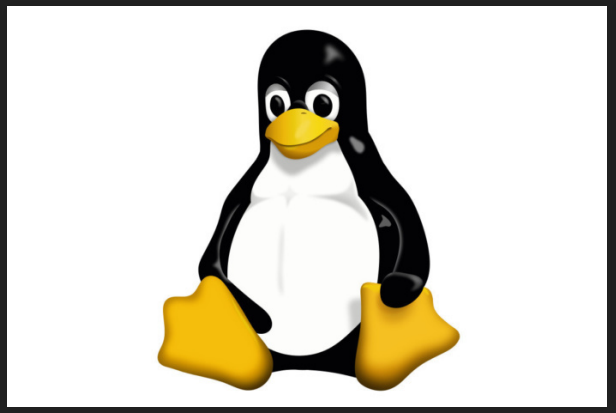
pip install -U frida-tools

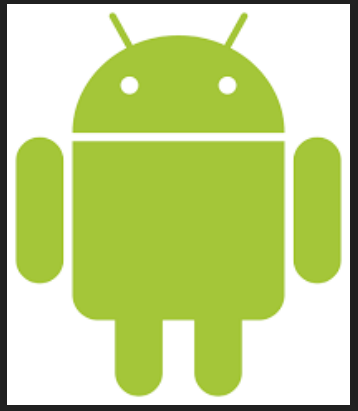
Android Studio

XCode + CLI Tools*

TARGET DEVICE







ANDROID

github.com/frida/frida/releases

(find frida-server for your arch)

adb push ./frida-server /data/local/tmp/frida-server

adb shell chmod +x /data/local/tmp/frida-server

adb shell "/data/local/tmp/frida-server &"

IOS - JAILBROKEN

cydia add source

apt?

Install latest

IOS - NOT JAILBROKEN

Recompile App

Deploy Gadget

Doing Stuff

BASIC OPERATIONS

frida-ls-devices

frida-ps -Ua

frida-trace -i "*" -U -f com.target.app

open / send / recv

How to draw an owl

1.

1. Draw some circles

2.

2. Draw the rest of the fucking owl

NOT SO BASIC OPERATIONS

frida -U --no-pause -f com.target.app

Process.enumerateModulesSync()

Module.findBaseAddress('name')

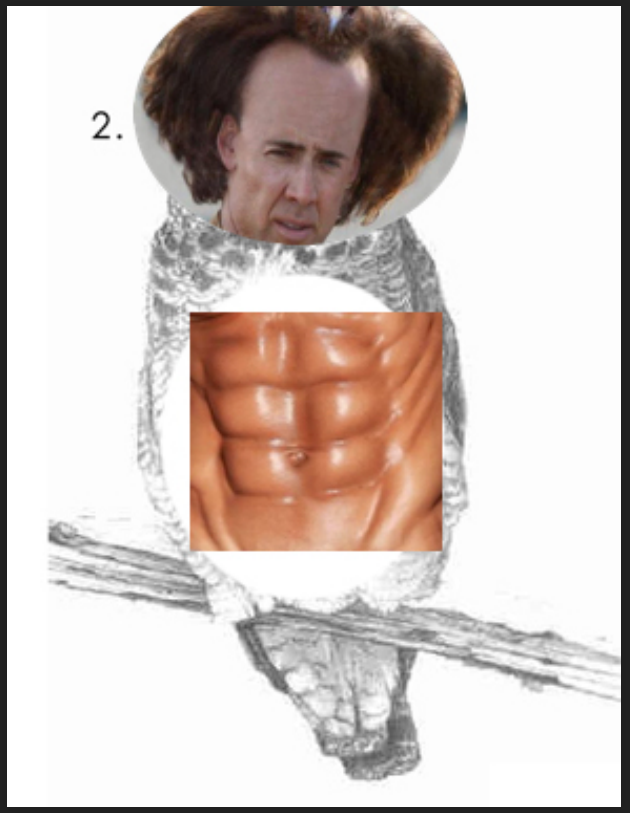
SCRIPTING

frida -U --no-pause -f com.target.app -l wizardscript.js

```
from __future__ import print_function
import frida
import sys

session = frida.attach("hello")
script = session.create_script("send(1337);")
def on_message(message, data):
        print(message)
script.on('message', on_message)
script.load()
sys.stdin.read()
```

```
frida -U --codeshare someotherwizard -f com.target.app
```


2.

RAPID TESTING

FiOS

appmon

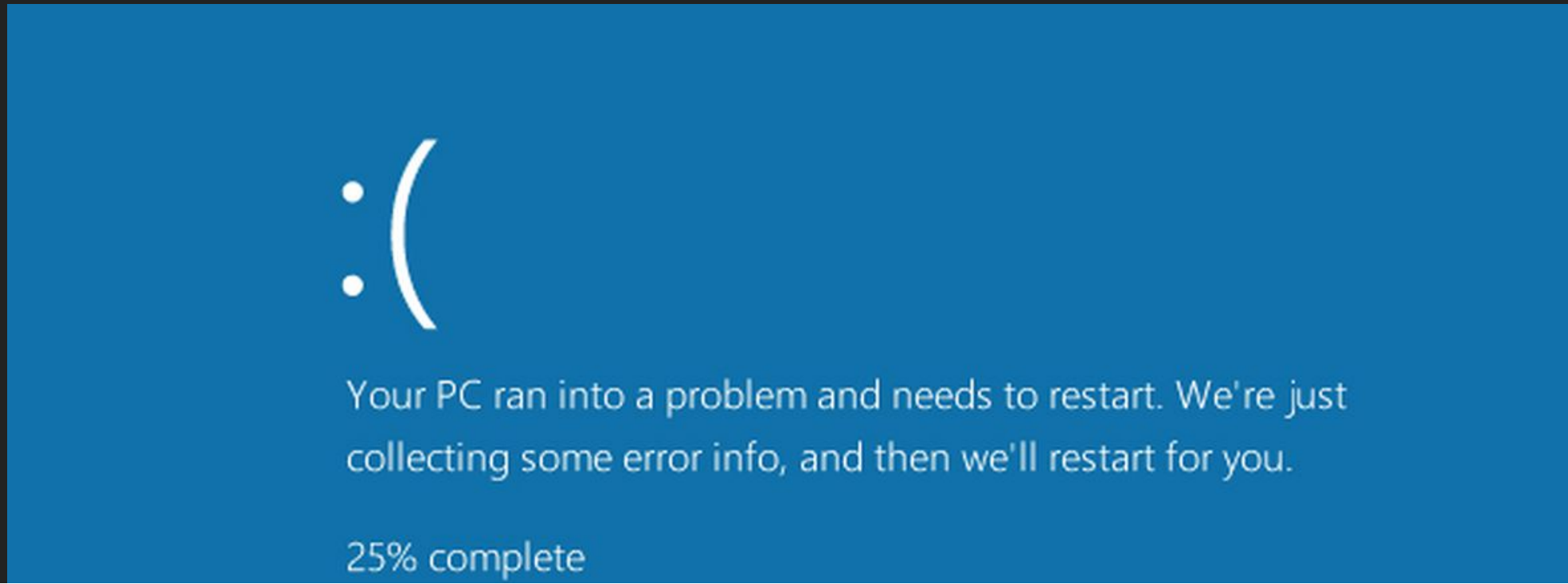
passion fruit

frick

r2frida

objection

SOME DEMO STUFF?


:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.
25% complete

[Trolling Intensifies]

Resources

CREATOR

Ole André Vadla Ravnås (@oleavr)

PEOPLE

Frida on Telegram

#frida Freenode

secRet Slack (secret.re for invite)

iDevicePwn Slack

QUESTIONS?

@dacoursey

No unibrows were harmed in the making of these slides.

INTERESTING LINKS

https://developer.apple.com/download/more/
https://github.com/skylot/jadx
https://support.ssl.com/Knowledgebase/Article/View/19/0/der-vs-crt-vs-cer-vs-pem-certificates-and-how-to-convert-them
https://nvisium.com/resources/blog/2017/07/12/advantages-and-disadvantages-of-android-n-network-security-configuration.html
https://github.com/maltek/swift-frida
https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2016/october/ios-instrumentation-without-jailbreak/
https://codewithchris.com/deploy-your-app-on-an-iphone/
https://github.com/dweinstein/awesome-frida
https://codeshare.frida.re
https://github.com/frida/frida/releases
https://codeshare.frida.re/@dki/ios10-ssl-bypass/
https://github.com/strazzere/android-unpacker/tree/master/native-unpacker
https://github.com/lasting-yang/FridaAutoHook
https://github.com/lojikil/dotfiles