关于droidbox的实例drops文章: http://drops.wooyun.org/tips/1314

把droidbox封装进Docker后可以更轻松的使用droidbox,毕竟动不动就实机去装模拟器是很费神的一件事情

我把docker hub上的docker-droidbox重新在国内的时速云上build了一遍(因为网速快,拖800多M的镜像会快几个小时……)

然后放进了Woobuntu软件中心,然而使用起来还是有些难度的,在这里说明一下

安装:点鼠标就行,woobuntu软件中心docker目录下面

使用示例:

root@alkaid-VirtualBox:/home/alkaid# docker run -it --rm -v ~/samples:/samples -v ~/sample
s/out:/samples/out index.tenxcloud.com/lxj616/droidbox /samples/ganjihaoche.apk 360

其中samples是你自己建的文件夹,用来放apk还有生成的报告,最后的数字是运行的时间,当然你也可以 在运行时手动停止

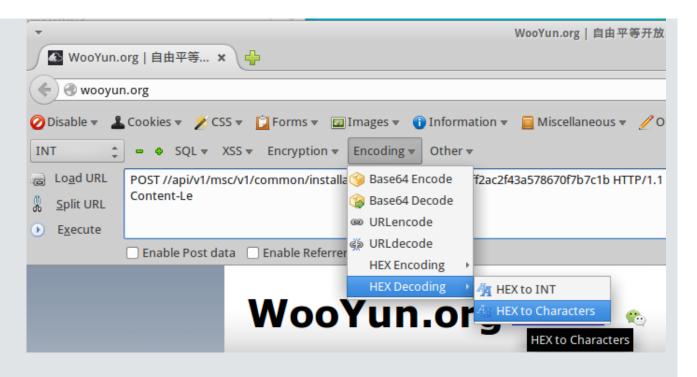
这里随便用一个apk演示

```
oot@alkaid-VirtualBox:/home/alkaid# docker run -it --rm -v ~/samples:/samples
v ~/samples/out:/samples/out index.tenxcloud.com/lxj616/droidbox /samples/ganjih
aoche.apk 360
Droidbox Docker starting
Waiting for the emulator to startup...
* Starting OpenBSD Secure Shell server sshd
                                                                           [ OK ]
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
Waiting for the device...
Installing the application /samples/ganjihaoche.apk...
Running the component com.ganji.android.haoche_c/com.ganji.android.splash.Splash
Activity...
  \ \_
Starting the activity com.ganji.android.splash.SplashActivity...
Application started
Analyzing the application during 360 seconds...
{"apkName": "/samples/ganjihaoche.apk", "enfperm": ["com.ganji.android.haoche_c.
permission.MIPUSH_RECEIVE"], "recvnet": {"1.6123430728912354": {"data": "4854545
.
02f312e3120323030204f4b0d0a5365727665723a2054656e67696e650d0a446174653a204d6f6e2
c203235204a616e20323031362030383a34313a323020474d540d0a436f6e74656e742d547970653
a206170706c69636174696f6e2f6a736f", "host": "124.250.6.151", "type": "net read",
"port": "80"}, "1.6193361282348633": {"data": "222c226e616d65223a225c7534653064
5c7539363530227d2c7b226964223a2232363238222c226e616d65223a2241344c222c2276616c75
65223a22617564692d61346c227d2c7b226964223a2232363237222c226e616d65223a2241364c22
2c227661", "host": "124.250.6.151", "type": "net read", "port": "80"}, "2.124541
997909546": {"data": "485454502f312e3120323030204f4b0d0a5365727665723a206e67696e
780d0a446174653a204d6f6e2c203235204a616e20323031362030383a34313a323020474d540d0a
436f6e74656e742d547970653a206170706c69636174696f6e2f6a736f6e0d", "host": "124.25
1.6.107", "type": "net read", "port": "80"}, "1.922523021697998": {"data": "6c75
65223a2269383030227d2c7b226964223a22313036313130222c226e616d65223a22536174656c6c
697465222c2276616c7565223a22736174656c6c697465227d5d7d2c7b226964223a223133303822
```

说简单也简单,说不简单肯定有人不会

接下来就可以看各种ison格式的日志了,比如网络连接之类的

取出的数据都是hex编码后的,这时可以用wooyun-firefox集成的hackbar来解码



最后给出一些可能有用的信息:

国外原始docker hub的droidbox地址 (800多M镜像,小水管要有心理准备)
https://hub.docker.com/r/honeynet/droidbox/
docker pull honeynet/droidbox

