

渗透测试 APP流量通用抓包方法

朋与厌 洛米唯熊 2019-11-23



毕老师之前开会的时候提起过微信、支付宝、抖音类的App会检测手机的是否挂代理，就是说不能直接在手机代理的地方做手脚，不然就会被检测到 :)



沉迷学长 日渐消瘦

名米堆

0x01 Proxifier代理介绍

1.1 **首先介绍下Proxifier: **

Proxifier是一款功能非常强大的代理客户端，支持Windows XP/Vista/Win7/Win10 和 MacOS，支持http/https、socks4/5、TCP、UDP等协议，可以指定端口，指定IP，指定域名、指定程序、指定用户名密码授权等运行模式，兼容性非常好，有点类似SOCKSCAP。

有许多网络应用程序不支持通过代理服务器工作，不能用于局域网或防火墙后面。这些会损害公司的隐私和导致很多限制。Proxifier解决了这些问题和所有限制，让您有机会不受任何限制使用你喜爱的软件。此外，它让你获得了额外的网络安全控制，创建代理隧道，并添加使用更多网络功能的权力。

1.2 **Proxifier代理流程**

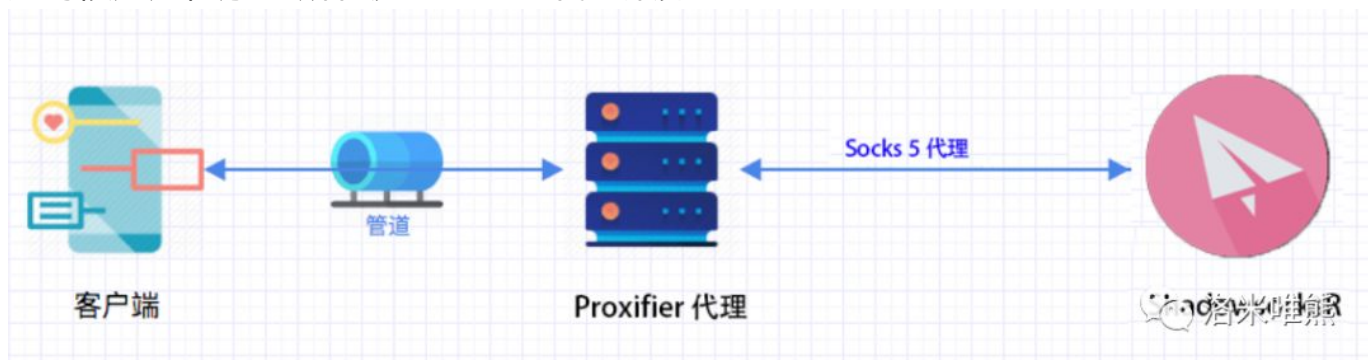
端口转发 | 流量转发

代理流程主要分为两步：

1、添加代理服务器 (Socks5)

2、设置代理规则 (设置需要设置代理 **应用程序**)

这时候应用程序 **所有流量** 经过代理服务器



这样，只要选择需要代理的应用程序，比如chrome.exe，即可实现代理流量转发

0x02 设立猜想

梳理了流程之后，一个很骚的思路就从脑子里蹦了出来：

代理到Socks5 流量就全部走 **小飞机**，也就是说小飞机就是**流量的出口**。



这样就跟浏览器挂代理抓包原理是一样的。

****猜想建立****

1、用代理转发工具将流量出口代理到Burp 8080端口

2、注入流量 (**模拟器有很多进程，其中有个进程是网络的进程**)

安卓模拟器大多是使用virtualbox的虚拟网卡进行的网络通信，那么，如果直接将模拟器的网络进程的所有流量代理到burpsite即可抓取流量包，同时又绕过了关于客户端的相关校验。

打开模拟器分析网络进程，会发现模拟器使用的网络进程有：

`virtualbox headless fronrend`和`NoxVMHandle Frontend`。

名称	状态	CPU	内存	磁盘	网络	GPU	GPU 显存
Google Chrome (14)		0%	491.1 MB	0.1 MB/秒	0 Mbps	0%	
NoxVMHandle Frontend		26.8%	462.1 MB	4.1 MB/秒	43.7 Mbps	0.9%	GPU 1
Adobe Photoshop CC 2019 (3)		0%	441.1 MB	0 MB/秒	0 Mbps	0%	
Java(TM) Platform SE binary (32...		0%	238.1 MB	0 MB/秒	0 Mbps	0%	
Google Chrome		0%	225.0 MB	0 MB/秒	0 Mbps	0%	
Antimalware Service Executable		0%	99.1 MB	0 MB/秒	0 Mbps	0%	
WeChat (32 位)		0%	94.0 MB	0 MB/秒	0 Mbps	0%	
Typora (2)		0%	79.7 MB	0 MB/秒	0 Mbps	0%	
腾讯QQ (32 位)		0%	76.8 MB	0 MB/秒	0 Mbps	0%	
Google Chrome		0%	71.5 MB	0 MB/秒	0 Mbps	0%	
桌面窗口管理器		2.1%	68.4 MB	0 MB/秒	0 Mbps	0.8%	GPU C
Typora		0%	42.7 MB	0 MB/秒	0 Mbps	0%	
Google Chrome		0%	42.5 MB	0 MB/秒	0 Mbps	0%	
Google Chrome		0%	38.1 MB	0 MB/秒	0 Mbps	0%	
Windows 资源管理器		0.4%	37.2 MB	0 MB/秒	0 Mbps	0%	

其它渠道游戏

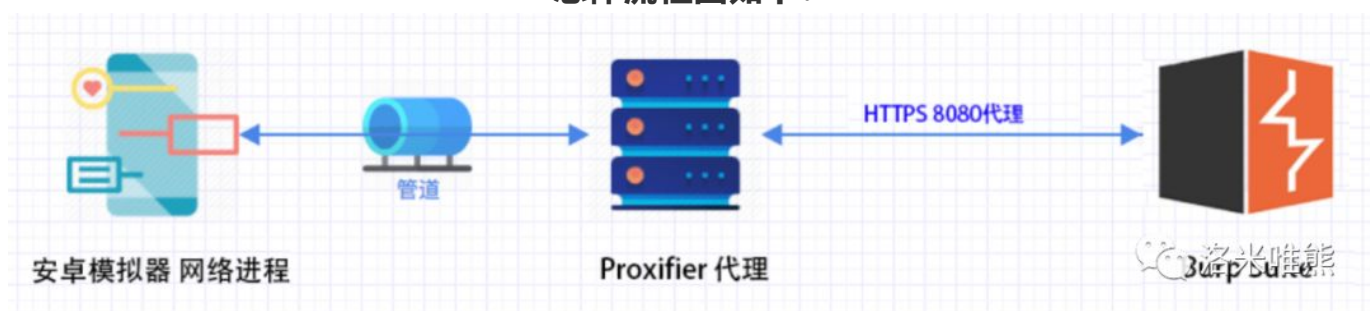


扫描到手机

28%

洛米唯熊

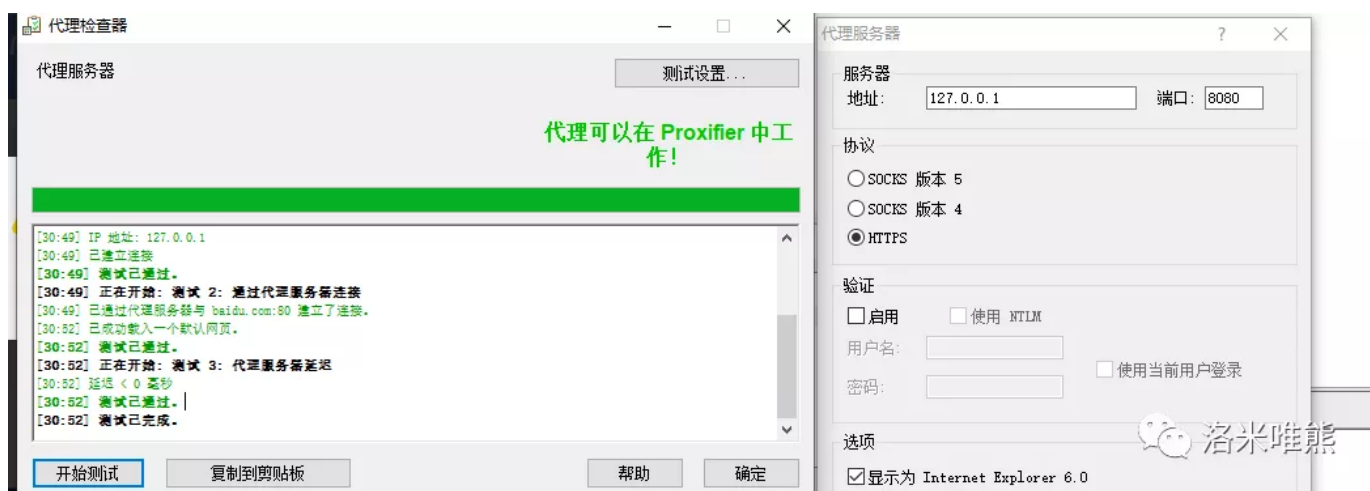
总体流程图如下：



验证猜想

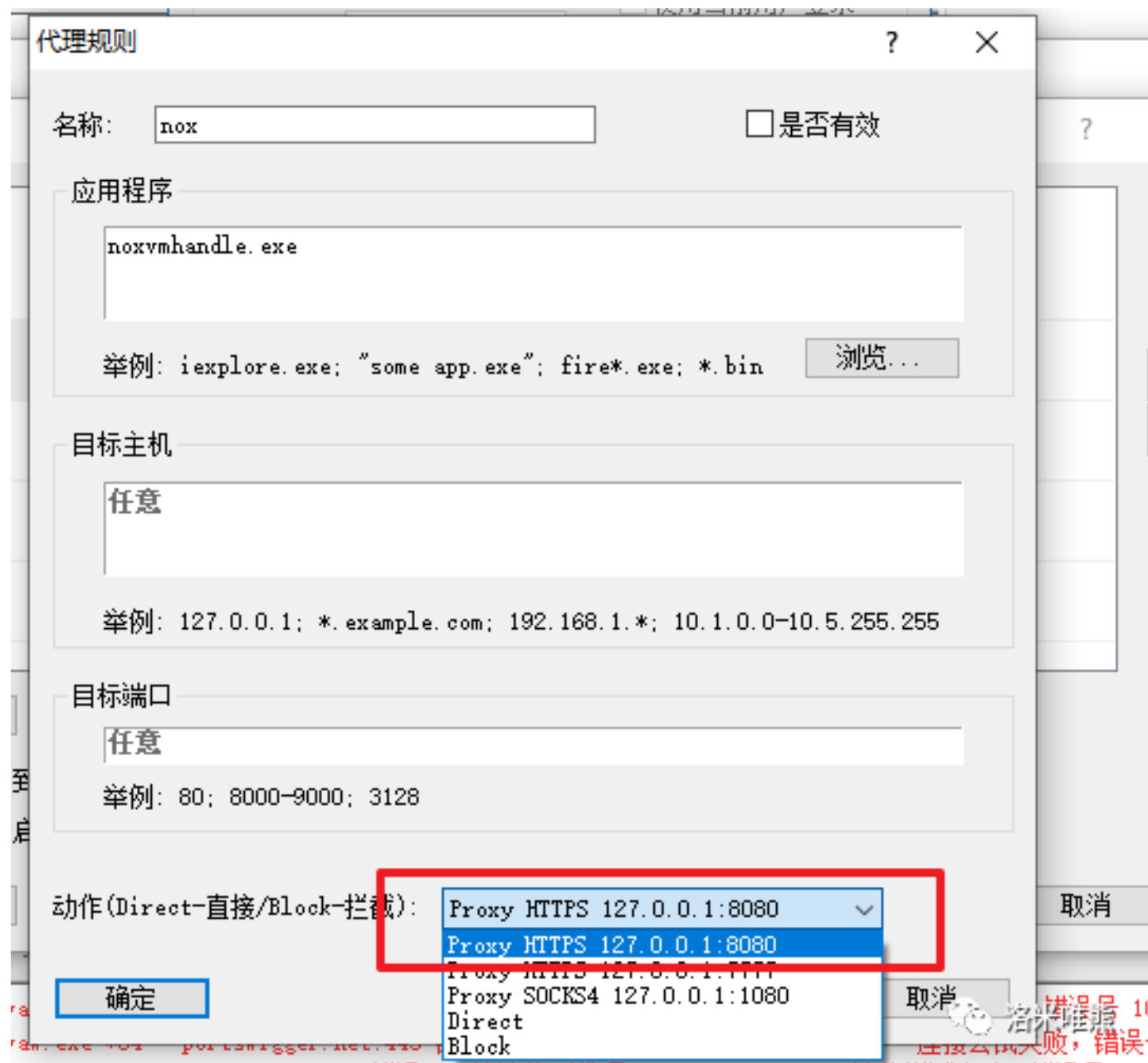
2.1 设置Proxifier代理服务器

代理服务器设置为burp监听端口。



2.2 设置代理规则

将`NoxVMHandle Frontend`进程对应的应用程序文件加入代理规则。



2.3 安装证书

这里不再详细讲。

虚拟机都是用的虚拟网卡 不能直接访问到宿主机


```
NOX 夜神模拟器 6.3.0.6 Android 5
$ ifconfig
eth1 Link encap:Ethernet HWaddr 08:00:27:64:1E:C7
    inet addr:172.17.100.15 Bcast:172.17.100.255 Mask:255.255.255.0
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:207063 errors:0 dropped:0 overruns:0 frame:0
    TX packets:91887 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:275318206 (262.5 MiB) TX bytes:6243565 (5.9 MiB)

lo Link encap:Local Loopback
    inet addr:127.0.0.1 Mask:255.0.0.0
    UP LOOPBACK RUNNING MTU:65536 Metric:1
    RX packets:84725 errors:0 dropped:0 overruns:0 frame:0
    TX packets:84725 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:7052974 (6.7 MiB) TX bytes:7052974 (6.7 MiB)

wlan0 Link encap:Ethernet HWaddr 08:00:27:9E:10:16
    inet addr:172.17.99.15 Bcast:172.17.99.255 Mask:255.255.255.0
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:4232 errors:0 dropped:0 overruns:0 frame:0
    TX packets:572 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:253366 (247.4 KiB) TX bytes:37806 (36.9 KiB)

$
```

ESC CTRL ALT

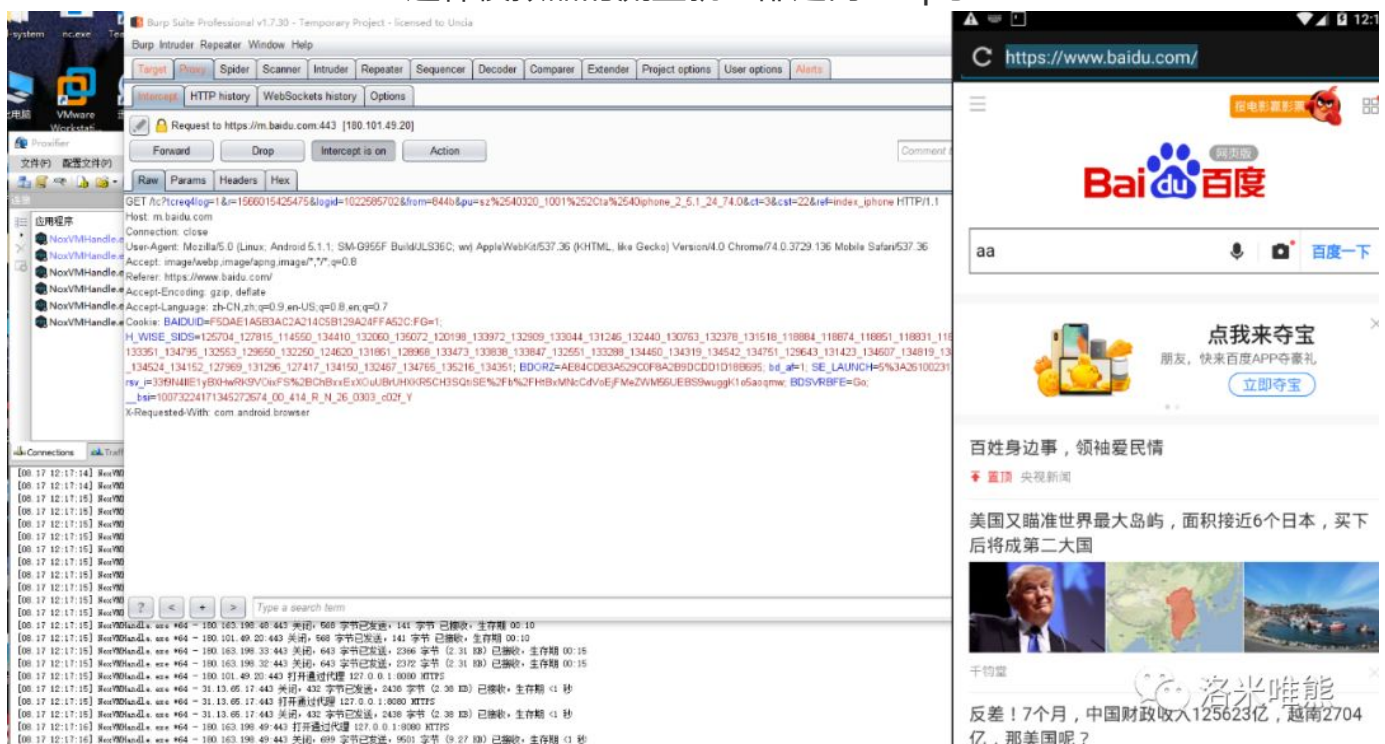
洛米唯熊

将Burp的CA证书文件复制到模拟器安装就可以了

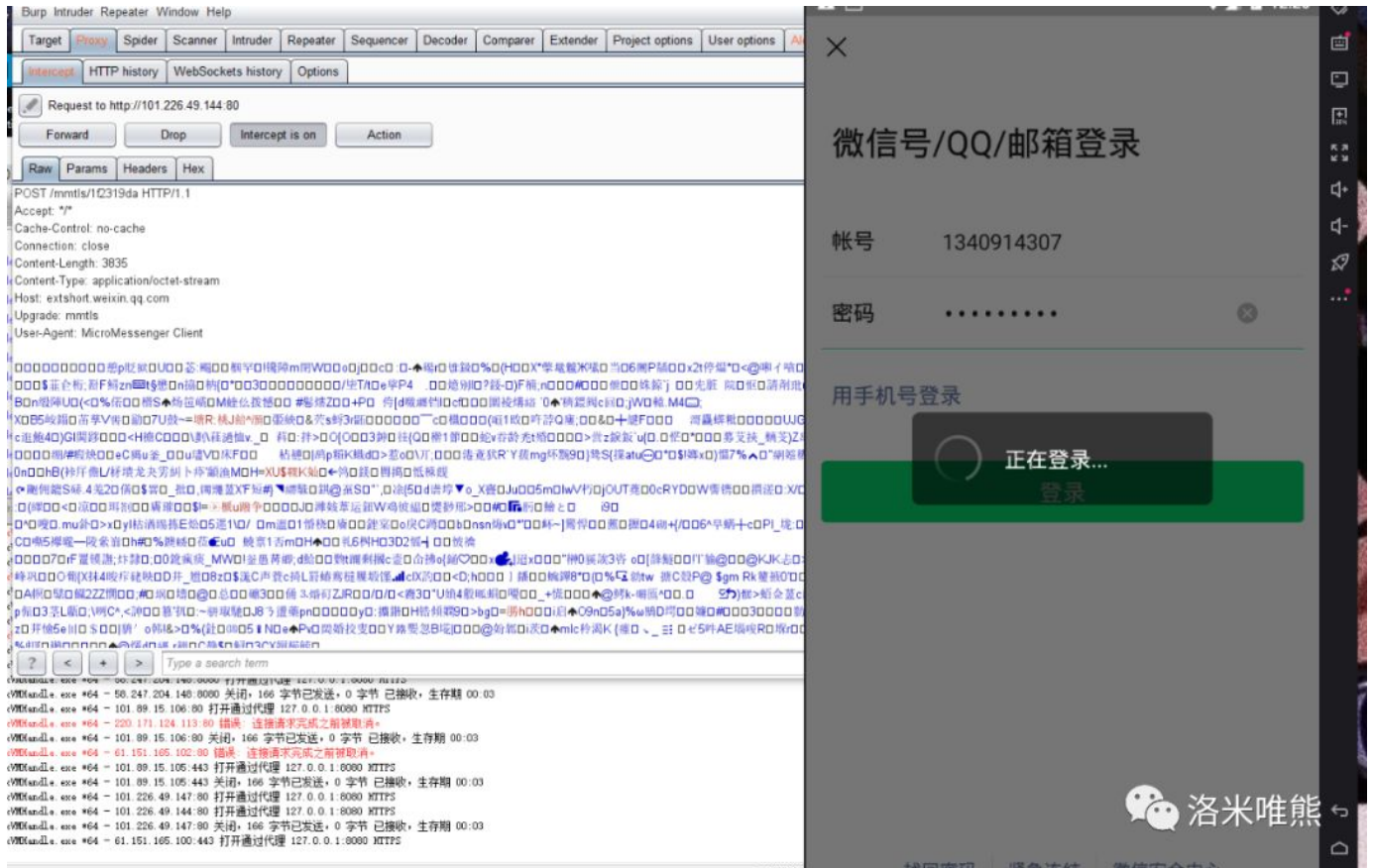
2.4 抓取流量包

配置之后，即可在proxifier中获取到模拟器内对应app的流量

这样模拟器的流量就全部走向Burp了



实现 微信登录数据包



完毕收工

这有一个
很可爱的公众号

关注它吧



洛米唯熊