Tcpdump流量内部式分析

实验概述

使用wireshark直接抓包需要在无线信号中捕获数据包。虽然简单,但是会捕获到很多不相关的数据包。本实验讲解在Android系统中运行抓包软件tcpdump进行抓包。由于在Android系统内部抓包,所以这种方式被称为内部式流量分析。

实验目的

- 1、了解tcpdump的使用方法
- 2、了解wireshark的使用方法

实验原理

Tcpdump是一款非常强大的命令行抓包工具。用户通过使用该工具捕获网络中传输的数据包,可以检查某个服务器以及网络中存在的问题。对于ISO七层模型中的网络层来说,该工具支持的协议、主机、网络或端口的过滤,并且提供and、or、not等逻辑语句可以过滤掉一些无用的信息。

Tcpdump命令的语法格式为:

tcpdump [选项][表达式]

该命令常用的选项和含义:

- -c: 在收到指定的包的数目后, 停止抓包
- -d: 将匹配信息包的代码以人类可读的格式输出
- -dd: 将匹配信息包的代码以C语言程序段的格式输出
- -ddd: 将匹配信息包的代码以十进制输出
- -e: 在输出行打印出数据链路层的头部消息
- -f: 将IPV4的地址以数字形式打印出来
- -i: 指定监听端口。如果不指定端口的话,tcpdump将在系统的接口清单中寻找号码最小,并且已经配置好的接口
- -l: 使标准输出变为缓冲行形式
- -n: 不要把网络地址转换成名字
- -p: 关闭接口的混杂模式
- -r: 从指定文件的文件中读取包
- -v: 输出详细的报文信息
- -w: 指定捕获包的文件名
- -s: 从每个报文中截取snaplen字节的数据,而不是缺省的65535个字节

Tcpdump工具可以使用表达式过滤捕获的数据包。表达式是一个正则表达式,Tcpdump可以利用它作为过滤报文的条件。如果一个报文满足表达式的条件,则该报文将会被捕获。如果没有给出任何条件,则捕获所有的数据包。

1、关于类型的关键字

关键字有: host、net、port等

例如:

host 10.0.0.1:表示只捕获10.0.0.1的数据包

net 10.0.0.0: 只捕获10.0.0.0网段的数据包

2、关于传输方向的关键字

关键字有: src、dst、dst or src等

例如:

src 10.0.0.1: 表示仅捕获源地址为10.0.0.1的数据包

dst 10.0.0.254: 表示仅捕获目的地址为10.0.0.254的数据包

3、协议关键字

关键字有: ip、arp、rarp、tcp、udp等。

实验环境

虚拟机: kali

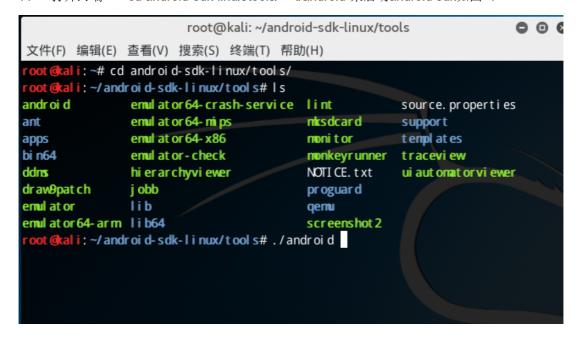
工具: tcpdump、wirshark

模拟器: android 4.0

注意: 需要修改本机网站的权限 (chmod - R 777 /opt/lampp/htdocs/mregister),打开 lampp(/opt/lampp/lampp start),模拟器访问的是本机ip。

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

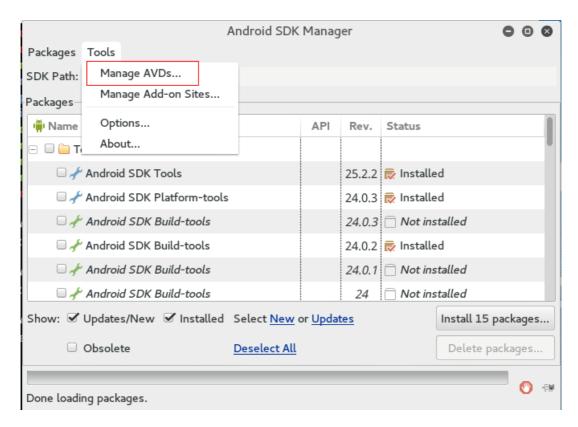


图 2开启模拟器控制台

3、选择创建好的Android虚拟机单击start来开启虚拟机,如图 3

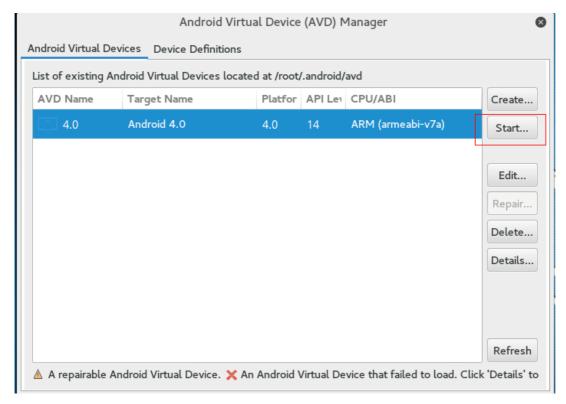


图 3开启4.0模拟器

4、此处可设置屏幕的尺寸,使用默认值,单击launch,如图 4

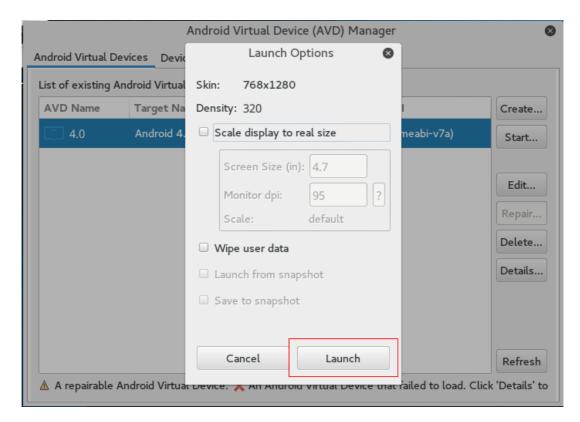


图 4开启模拟器

5、成功开启android虚拟机,桌面如图 5

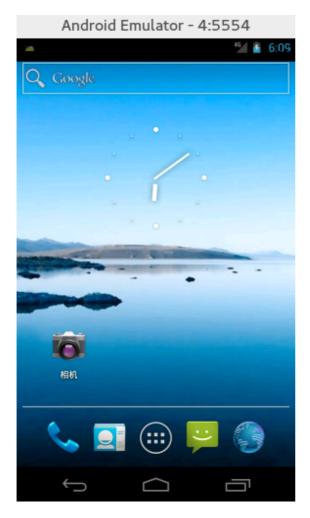


图 5模拟器界面

6、确认tcpdump工具是否为ARM的可执行文件

使用命令"打开新的终端">"cd tools">"ls">"file tcpdump"如图 6

```
<mark>ot@kali:</mark>~# cd tools/
     kali:~/tools# ls
bluedon.png qianming tcpdump
root@kali: /tools# file tcpdump
tcpdump: ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically link
ed, for GNU/Linux 2.6.14, not stripped
root@kali:~/tools#
```

图 6查看tcpdump

7、把工具上传到android模拟器的tmp目录,并且确定是否上传成功

用命令 "adb tcpdump /data/local/tmp/tcpdump">"adb shell">"cd push /data/local/tmp">"ls"如图 7

```
ot@kali:~/tools# adb push tcpdump /data/local/tmp/tcpdump
[100%] /data/local/tmp/tcpdump
root@kali:~/tools# adb shell
# cd /data/local/tmp/
# ls
drozer-agent-2.3.4.apk
tcpdump
```

图 7传送工具到模拟器内

8、查看tcpdump权限,如果权限不是777,则需要执行命令"chmod 777 tcpdump"来改变权限,如图 8

```
# ls
drozer-agent-2.3.4.apk
tcpdump
# ls -l
                               633110 2016-10-20 08:53 drozer-agent-2.3.4.apk
-rwxrwxrwx root
                   root
                              1801155 2016-08-08 09:31 tcpdump
                    root
-rwxrwxrwx root
```

图 8赋予执行权限

9、使用tcpdump工具开始捕获数据包

使用命令 "./tcpdump host 172.16.9.119 (虚拟机本地IP) -v -s 0 -w output.pcap",返回如图 9的内容说明抓包开始。

```
# ./tcpdump host 172.16.9.119 -v -s 0 -w output.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byt
es
Got 0
```

图 9开始捕获数据包

10、在android中模拟上网行为

操作: "在手机上方搜索框输入172.16.9.119 (虚拟机本地IP) /mregister/login.html"进入到登录界面,如图 10



图 10模拟器访问网站

11、随便输入任意的手机号码和密码,如图 11



图 11输入任意帐号密码注册

12、手机返回个注册成功的界面



图 12注册成功

13、停止抓包

操作: "按ctrl+c停止抓包">"ls"如图 13所示抓包成功

```
./tcpdump host 172.16.9.119 -v -s 0 -w output.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byt
es
^C26 packets captured
26 packets received by filter
0 packets dropped by kernel
#
 ls
drozer-agent-2.3.4.apk
output.pcap
tcpdump
```

图 13停止抓包

14、把获取的数据包传到kali上分析

操作: "ctrl+c退出手机shell">"adb_pull /data/local/tmp/output.pcap /root/output.pcap">"cd /root">"Is"查看是否存在output.pcap如图 14

```
root@kali:~/tools# adb pull /data/local/tmp/output.pcap /root/output.pcap
[100%] /data/local/tmp/output.pcap
root@kali:~/tools# cd /root
root@kali:~# ls
android-sdk-linux jd-gui_1.4.0-0_all.deb tools
                                                    图片
apk
                                             公共
                                                          音乐
                   output.pcap
                                             模板
bluedon.png
                    test
                                                    文档
                                                          桌面
```

图 14把数据包导入到kali

15、打开wireshark分析数据包

操作: "单击左上角的应用程序">"选择嗅探/欺骗">"wireshark"。如图 15



图 15开启wireshark

16、打开output.pcap

操作: "单击左上角文件">"打开">"选择output.pcap文件所在路径">"打开"如图 16

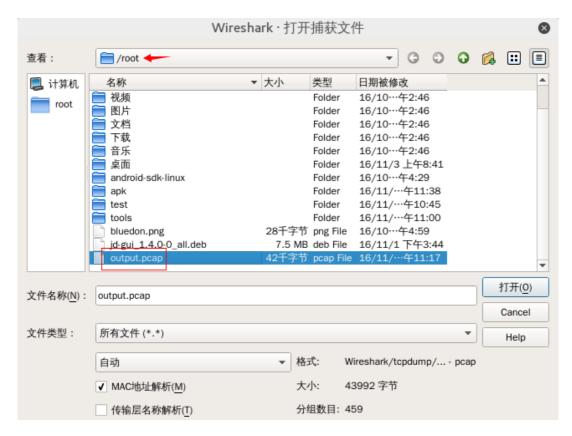


图 16打开文件

17、成功后可以查看到刚刚在手机端抓取的数据包,如图 17

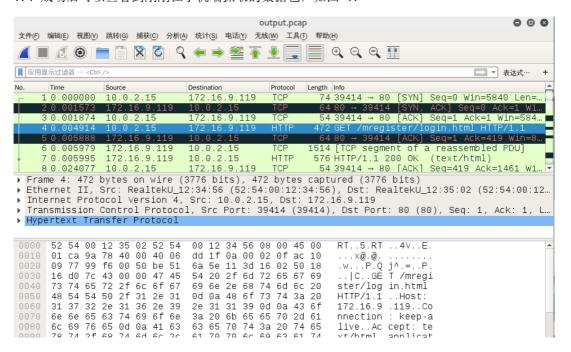


图 17数据包

18、过滤http包,在过滤栏输入http,只显示http包。如图 18

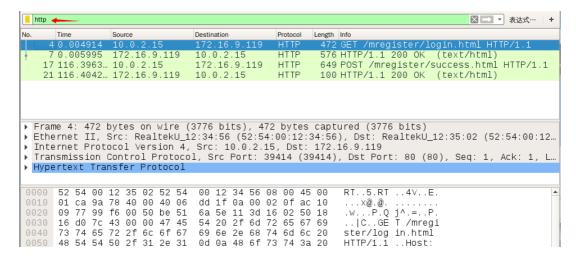


图 18 http包

19、此数据包是手机端向服务器请求页面的数据包。如图 19

```
7 0.005995 172.16.9.119 10.0.2.15
17 116.3993... 10.0.2.15 172.16.9.1
21 116.4042... 172.16.9.119 10.0.2.15
android模拟器严地址
                                                                                                                               576 HTTP/1.1 200 OK
                                                                                                                                                                                  (text/html
                                                                                                                               649 POST /mregister/success.html HTTP/1.1
100 HTTP/1.1 200 OK (text/html)
                                                                          172.16.9.119
                                                                                                             HTTP
Frame 4: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits)
Fthernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Dst: RealtekU_12:35:02 (52:54:00:12...
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.16.9.119
Transmission Control Protocol, Src Port: 39414 (39414), Dst Port: 80 (80), Seq: 1, Ack: 1, L...
   Hypertext Transfer Protocol

→ GET /mregister/login.html HTTP/1.1\r\n → 请求页面请求

Host: 172.16.9.119\r\n → BEX 英校in.html
                                                                               -服务器的ip地址
         Connection: keep-alive\r\n
         Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
User-Agent: Mozilla/5.0 (Linux; U; Android 4.0.2; zh-cn; sdk Build/ICS_MR0) AppleWebKit/53...
Accept-Encoding: gzip,deflate\r\n
Accept-Language: zh-CN, en-US\r\n
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
          [Full request URI: http://172.16.9.119/mregister/login.html]
[HTTP request 1/1]
[Response in frame: 7]
```

图 19请求包

20、此数据包是服务器向手机端发送html页面的数据包。如图 20

```
4 0.004914 10.0.2.15
                                       172.16.9.119
                                                          HTTP
                                                                    472 GET /mregister/login.html HTTP/1.1
    17 116.3963... 10.0.2.15 172.16.9.1
21 116.4042... 172.16.9.119 10.0.2.15
                                                                    649 POST /mregister/success.html HTTP/1.1
100 HTTP/1.1 200 OK (text/html)
                                       172.16.9.119
                                                          HTTP
▶ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 39414 (39414), Seq: 1461, Ack:...
▶ [2 Reassembled TCP Segments (1982 bytes): #6(1460), #7(522)]
 Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n
    Date: Fri, 04 Nov 2016 02:42:15 GMT\r\n
    Server: Apache/2.4.17 (Unix) OpenSSL/1.0.1q PHP/5.5.30 mod_perl/2.0.8-dev Perl/v5.16.3\r... Accept-Ranges: bytes\r\n
  ▶ Content-Length: 1713\r\n
    Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
                                                                                    服务器的相关配置
    Content-Type: text/html\r\n
     [HTTP response 1/1]
     [Time since request: 0.001081000 seconds]
[Request in frame: 4]
                                                                                      服务器返回的html代码,需要浏览器来解析
▼ Line-based text data: text/html
     <!DOCTYPE html>\r\n
    <html>\r\n
          <head>\r\n
               <title>\347\231\273\351\231\206\351\241\265\351\235\242</title>\r\n
               <meta charset="utf-8">\r\n
<meta name="format-detection" content="telephone=no">\r\n
               <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-sc.</pre>
```

图 20响应包

21、此数据包是手机端输入帐号密码提交给服务器的数据包。如图 21

```
4 0 . 004914 10 . 0 . 2 . 15
                                                           172.16.9.119
                                                                                       HTTP
                                                                                                     472 GET /mregister/login.html HTTP/1.1
                                                                                                     576 HTTP/1.1 200 OK (text/html)
         7 0.005995 172.16.9.119
                                                           10.0.2.15
                                                                                       HTTP
       21 116 . 4042 ... 172 . 16 . 9 . 119
                                                           10.0.2.15
                                                                                       HTTP
                                                                                                     100 HTTP/1.1 200 OK (text/html)
Frame 17: 649 bytes on wire (5192 bits), 649 bytes captured (5192 bits)

Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Dst: RealtekU_12:35:02 (52:54:00:12...)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.16.9.119

Transmission Control Protocol, Src Port: 39415 (39415), Dst Port: 80 (80), Seq: 1, Ack: 1, L...

Hypertext Transfer Protocol
    POST /mregister/success.html HTTP/1.1\r\n
HOST: 172.16.9.119\r\n
Connection: keep-alive\r\n
       Content-Length: 0\r\n
       Cache-Control: max-age=0\r\n
Origin: http://172.16.9.119\r\n
       Origin: http://lo.s.is/s.is/s/in/Content-Type: application/x-www-form-urlencoded\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
User-Agent: Mozilla/5.0 (Linux; U; Android 4.0.2; zh-cn; sdk Build/ICS_MR0) AppleWebKit/53...
Accept-Encoding: gzip,deflate\r\n
Accept-Language: zh-CN, en-US\r\n
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
        \r\n
        [Full request URI: http://172.16.9.119/mregister/success.html]
        [HTTP request 1/1]
[Response in frame: 21]
```

图 21请求包

22、此数据包是服务器接收到手机端提交的数据后,服务器返还给手机的数据包如图 22

```
4 0.004914 10.0.2.15
7 0.005995 172.16.9.119
17 116.3963... 10.0.2.15
                                            172.16.9.119
10.0.2.15
172.16.9.119
                                                                              472 GET /mregister/login.html HTTP/1.1
576 HTTP/1.1 200 OK (text/html)
649 POST /mregister/success.html HTTP/1.1
                                                                   HTTP
                                                                   HTTP
➤ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 39415 (39415), Seq: 1461, Ack:...

► [2 Reassembled TCP Segments (1506 bytes): #19(1460), #21(46)]

► Hypertext Transfer Protocol

► HTTP/1.1 200 OK\r\n

Date: Fri, 04 Nov 2016 02:44:11 GMT\r\n
     Server: Apache/2.4.17 (Unix) OpenSSL/1.0.1q PHP/5.5.30 mod_perl/2.0.8-dev Perl/v5.16.3\r... Accept-Ranges: bytes\r\n
  **Content-Length: 1237\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n
     Content-Type: text/html\r\n
      [HTTP response 1/1]
      [Time since request: 0.007933000 seconds]
[Request in frame: 17]
▼ Line-based text data: text/html
                                                                                        服务器返回的页面代码
      <!DOCTYPE html>\r\n
     <html>\r\n
           <head>\r\n
                 <title>\346\263\250\345\206\214\351\241\265\351\235\242</title>\r\n
                 <meta charset="utf-8">\r
```

图 22响应包

整个分析下来,抓取的数据包和上述android系统模拟上网的行为一致。

思考总结

本实验通过使用tcpdump对模拟器的上网行为进行抓包,然后使用wireshark对包进行分析查看是否和上网行为一致来演示tcpdump工具的使用。

- 1、还有什么方法可以抓取android内部的数据包?
- 2、除了wireshark,还有什么可以分析数据包的工具?