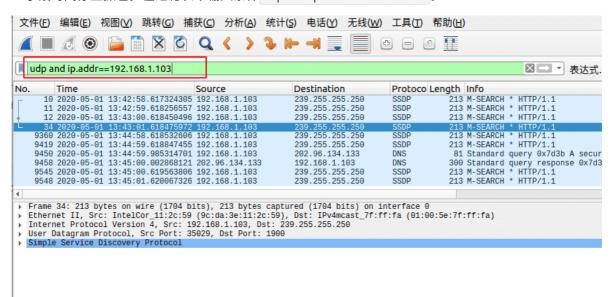
实验目的

了解UDP报文格式

实验内容

ifconfig 找到自己的地址是 192.168.1.103 ,然后打开Wireshark开始嗅探,随便浏览器点点什么然后隔一小段时间停止抓包。在过滤表中输入条件 udp and ip.addr==192.168.103 。



回答问题

1.从跟踪中选择一个UDP数据包,从此数据包中,确定UDP标头中有多少字段,并为这些字段命名。

```
Wireshark·分组 9458·wlp2s0
    Frame 9458: 300 bytes on wire (2400 bits), 300 bytes captured (2400 bits) on interface 0

    Ethernet II, Src:
    Internet Protocol Version 4, Src: 202.96.134.133, Dst: 192.168.1.103
    User Datagram Protocol, Src Port: 53, Dst Port: 59399

        Source Port: 53
         Length: 266
        Checksum: 0x32a5 [unverified]
          Checkson
                        Status
         [Stream index: 4]
Domain Name System (response)
        01 1e d1 10 40 00 30 11 5f c9 ca 60 86 85 c0 a8 01 67 00 35 68 07 01 0a 32 a5 7d 3b 81 80 00 01 00 08 00 0 00 03 08 73 65 63 75 72 69 74 79 02 69 65 05 73 61 67 6f 75 03 63 6f 6d 00 00 01 00
                                                                                                 0.6
                                                                                            s ecurity
                                                                                           ie·sogou ·com·
         01 c0 0c 00 05 00 01 00
63 75 72 69 74 79 c0 18
                                                 00 02 58 00 0b 08 73 65
                                                 c0 33 00 01 00 01 00 00
                                                                                           curity...
                                                                                                          .3.
         02 58 00 04 24 6e aa 20
02 58 00 04 24 6e aa 3a
02 58 00 04 31 07 15 33
02 58 00 04 31 07 15 39
                                                                                           · X · $n · : 
 · X · 1 · 3 
 · X · 1 · 9
                                                 c0 33 00 01 00 01 00 00
                                                                                                           3.
                                                 c0 33 00 01 00 01 00 00
                                                                                                           3....
0090
00a0
                                                c0 33 00 01 00 01 00 00
c0 33 00 01 00 01 00 00
                                                                                                          .3.
                                                                                            ·X··1··.
·X··1··-
·X··$n·!
         02 58 00 04 31 07 14 2e
02 58 00 04 31 07 15 2d
                                                 c0 33 00 01 00 01 00 00
c0 33 00 01 00 01 00 00
                                                                                                          . 3 . . . . .
         02 58 00 04 24 6e aa 21
00 4c 00 06 03 6e 73 32
00 00 00 4c 00 06 03 6e
                                                 c0 18 00 02 00 01 00 00
                                                 c0 18 c0 18 00 02
                                                                                           ·L···ns2 ····
                                                 73 31 c0 18 c0 cc 00 01
         00 01 00 00 00 d5 00 04
00 01 00 00 00 05 00 04
                                                 b4 95 9c 0c c0 ba 00 01
76 bf d8 3d c0 ba 00 01
         00 01 00 00 00 05 00 04 7b 7e 33 0c
```

这是我随便选择的一个报文,可以看到UDP标头中有源端口src port,目的端口号dst port,长度length,校验和checksum。都是占2个字节。(图中圈出来的是目的端口号十六进制的表示形式,刚好是两个字节)

2.通过查询Wireshark的数据包内容字段中显示的信息,确定每个UDP报头字段的长度(以字节为单位)。

从上个回答就可以知道头字段的长度2*4=8个字节。

3.长度字段中的值是指的是什么?使用捕获的UDP数据包验证您的声明。

Internet Protocol Version 4, Src: 202.96.134.133, Dst: 192.168.1.103

**User Datagram Protocol, Src Port: 53, Dst Port: 59399 Source Port: 53 Destination Port: 59399 Length: 266 Checksum: 0x32a5 [unverified] [Checksum Status: Unverified] [Stream index: 4] 01 1e d1 10 40 00 36 11 5f c9 ca 01 67 00 35 e8 07 01 0a 32 a5 <mark>70</mark> 5f c9 ca 60 86 85 c0 a8 <u>2</u>. 0020 g · 5 · · · · 0030 08 00 02 00 03 08 73 65 05 73 6f 67 6f 75 c0 0c 00 05 00 01 00 75 72 69 74 79 c0 18 58 00 04 24 6e aa 20 58 00 04 31 07 15 39 58 00 04 31 07 15 39 58 00 04 31 07 15 20 58 00 04 31 07 15 20 58 00 04 31 07 15 20 58 00 04 31 07 15 20 58 00 04 31 07 15 20 58 00 04 31 07 15 20 58 00 04 31 07 15 20 58 00 04 31 07 15 20 58 00 04 24 6e aa 21 4c 00 06 03 6e 73 32 03 63 67 6d 00 00 01 00 00 02 58 00 0b 08 73 65 c0 33 00 01 00 01 00 00 c0 33 00 01 00 01 00 00 c0 33 00 01 00 01 00 00 0040 ie∙soaou ∙com 0050 0060 curity… X · · \$n · · · X · · \$n · : 0070 0080 c0 33 00 01 00 01 00 33 00 01 00 01 00 0090 00a0 14 2e 15 2d aa 21 73 32 c0 33 00 01 00 01 c0 33 00 01 00 01 c0 33 00 01 00 01 c0 18 00 02 00 01 00b0 00c0 00d0 4c 00 06 03 6e 73 32 00 00 4c 00 06 03 6e 01 00 00 00 d5 00 04 01 00 00 00 05 00 04 c0 73 b4 00e0 18 c0 00f0 31 c0 18 c0 cc 00 01 95 9c 0c c0 ba 00 bf d8 3d c0 ba 00 0100 0110 0120

UDP中的length值为266个字节,刚好DNS的消息内容长度为258个byte,所以加上UDP的头部消息就是266个byte。

DNS: (0110-0030) = 16*14 + 16*14+12+6=258byte

4.UDP有效负载中可包含的最大字节数是多少?

UDP头部的length是2个byte,所以可以包含的最大字节数是(2¹⁶-1=65535)-8=65527byte。(UDP头部的length是以byte为单位的)

5.最大可能的源端口号是多少?

其实跟上道题同样的道理,最大的端口号是65535。

6.UDP的协议号是什么?以十六进制和十进制表示法给出答案。

参考资料

TCP支持的应用协议主要有: Telnet、FTP、SMTP等;

UDP支持的应用层协议主要有: NFS(网络文件系统)、SNMP(简单网络管理协议)、DNS(主域名称系统)、TFTP(通用文件传输协议)等。