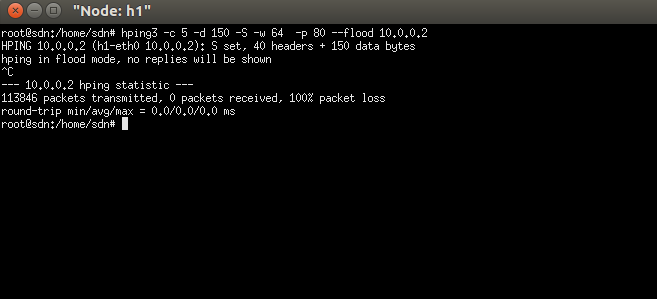
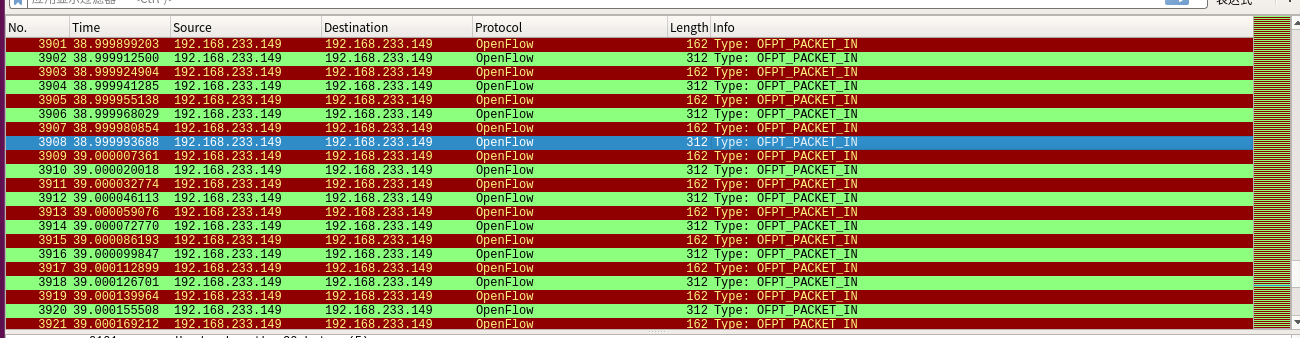
抓openflow包

首先用hping3发动syn攻击，产生大量半连接（没有第三次握手），得到第一次握手和第二次握手的包格式

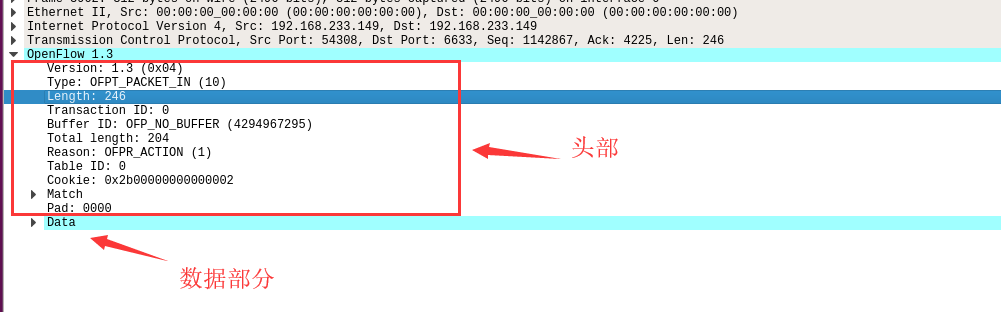
使用hping3工具发动syn攻击：



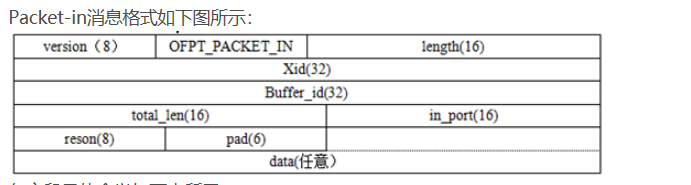
得到半连接：



第一次握手分析：



这里触发packetin的原因是转发到控制器



头部分析：

Version: openflow版本号

Type: 10代表PACKET\_IN的包号

Length：代表openflow包的长度

Transaction ID：packetin对应的事务id，所有的packetin都是一样的

Buffer\_id：表示OpenFlow交换机中保存的数据包的缓存id



数据部分分析：

Destination: fa 7c 4d 7e 24 e9 [108,114) 目的mac

Source: ca 4a b2 54 20 ae [114,120) 源mac

Type:IPv4 08 00 [120,122)

|  |  |  |  |
| --- | --- | --- | --- |
| Ip层 | | | |
| 字段 | 十六进制数据 | 位置 | 含义 |
| Version： 4 |  |  | ip版本号 |
| Header Length：5 这两个是一起的 | 45 | [122,123) | 头部长度 |
| Total Length | 00 28 | [124,126) | 总长度 |
| Identification | 94 09 | [126,128) |  |
| Flags | 40 00 | [128,130) | 标志段 |
| Time to live | 40 | [130,131) | 存活时间 |
| Protocol | 06 | [131,132) | 所采用协议 |
| Header checksum | 92 c4 | [132,134) | 头部校验和 |
| Source | 0a 00 00 02 | [134,138) | 源ip |
| Destination | 0a 00 00 01 | [138,142) |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Transmission Control Protocol 层： | | | |
| 字段 | 十六进制数据 | 位置 | 含义 |
| Source Port | 00 50 | [142,144) | 源端口 |
| Destination Port | 09 d2 | [144,146) | 目的端口 |
| Stream index: |  |  |  |
| TCP Segment Len | 50 | [154,155) |  |
| Sequence number | 00 00 00 00 | [146,150) | 序列号 |
| Acknowledgement number | 11 a7 bd f4 | [150,154) | 确认号 |
| Header Length | 50 | [154,155) |  |
| Flags | 50 14 | [154,156) | 标志 |
| Window size value | 00 00 | [156,158) |  |
| [Calculated window size: 0] | 00 00 | [156,158) |  |
| Window size scaling factor | 00 00 | [156,158) |  |
| Checksum | c2 10 | [158,160) |  |
| Urgent point | 00 00 | [160,162) |  |

