网络安全实验报告

实验目的

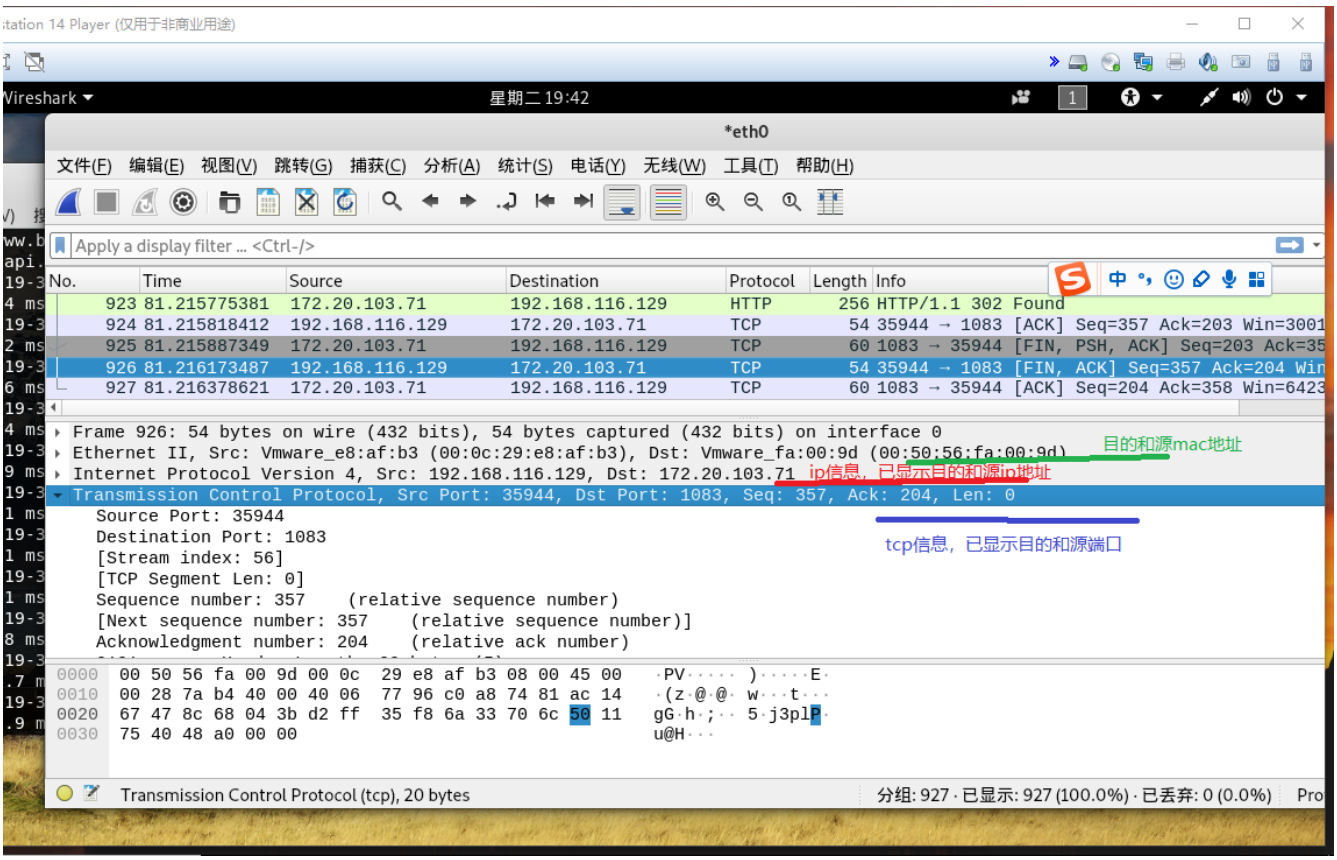
捕包软件的使用和实现

实验内容

1. 熟练使用sniffer或wireshark软件，对协议进行还原（能找到访问网页的四元组）
2. 利用libpcap或winpcap进行编程，能够对本机的数据包进行捕获分析（比如将本机所有数据包的四元组写到指定文件），按照自己的设想撰写需求分析和详细设计。

实验结果

1. 使用wireshark找到四元组



2. 利用libpcap,捕获本机数据包，并找到四元组。实验的toy code将捕获十个数据包，并将每个数据包的目的和源的mac地址，ip地址和端口写入`capture.txt`，下面是示例内容：

```
Ether Destination host:ff:ff:ff:ff:ff:ff
```

```
Ether Source host: 0:50:56:c0: 0: 8
Not IP proto


Ether Destination host: 0:50:56:fa: 0:9d
Ether Source host: 0: c:29:e8:af:b3
ip destination host:192.168.116.2
ip source host:192.168.116.129
tcp/udp destination port:53
tcp/udp source port:44193


Ether Destination host: 0:50:56:fa: 0:9d
Ether Source host: 0: c:29:e8:af:b3
ip destination host:192.168.116.2
ip source host:192.168.116.129
tcp/udp destination port:53
tcp/udp source port:44193


Ether Destination host: 0: c:29:e8:af:b3
Ether Source host: 0:50:56:fa: 0:9d
ip destination host:192.168.116.129
ip source host:192.168.116.2
tcp/udp destination port:44193
tcp/udp source port:53


Ether Destination host: 0: c:29:e8:af:b3
Ether Source host: 0:50:56:fa: 0:9d
ip destination host:192.168.116.129
ip source host:192.168.116.2
tcp/udp destination port:44193
tcp/udp source port:53


Ether Destination host: 0:50:56:fa: 0:9d
Ether Source host: 0: c:29:e8:af:b3
ip destination host:119.75.217.26
ip source host:192.168.116.129
Not TCP or UDP proto


Ether Destination host: 0: c:29:e8:af:b3
Ether Source host: 0:50:56:fa: 0:9d
ip destination host:192.168.116.129
ip source host:119.75.217.26
Not TCP or UDP proto


Ether Destination host: 0:50:56:fa: 0:9d
Ether Source host: 0: c:29:e8:af:b3
ip destination host:192.168.116.2
```

```
ip source host:192.168.116.129
tcp/udp destination port:53
tcp/udp source port:51543


Ether Destination host: 0: c:29:e8:af:b3
Ether Source host: 0:50:56:fa: 0:9d
ip destination host:192.168.116.129
ip source host:192.168.116.2
tcp/udp destination port:51543
tcp/udp source port:53


Ether Destination host: 0:50:56:fa: 0:9d
Ether Source host: 0: c:29:e8:af:b3
ip destination host:119.75.217.26
ip source host:192.168.116.129
Not TCP or UDP proto
```

实验总结

了解了捕包软件的基本使用方法和利用现有库编写捕包程序的基本方法。