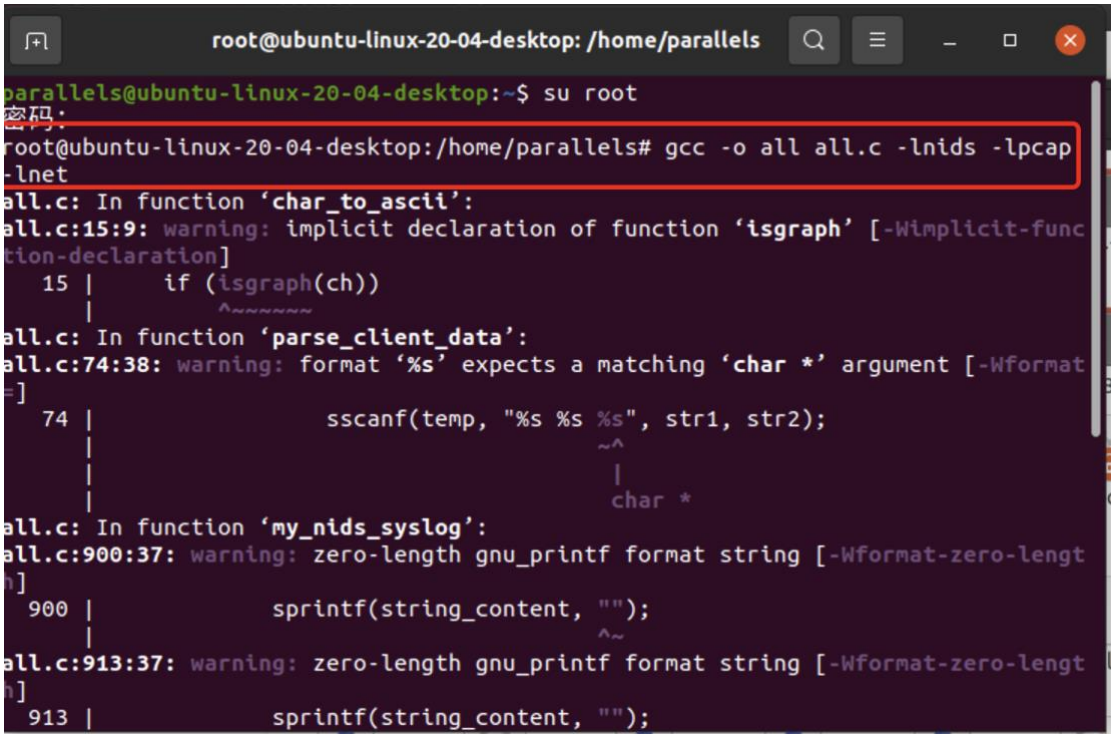
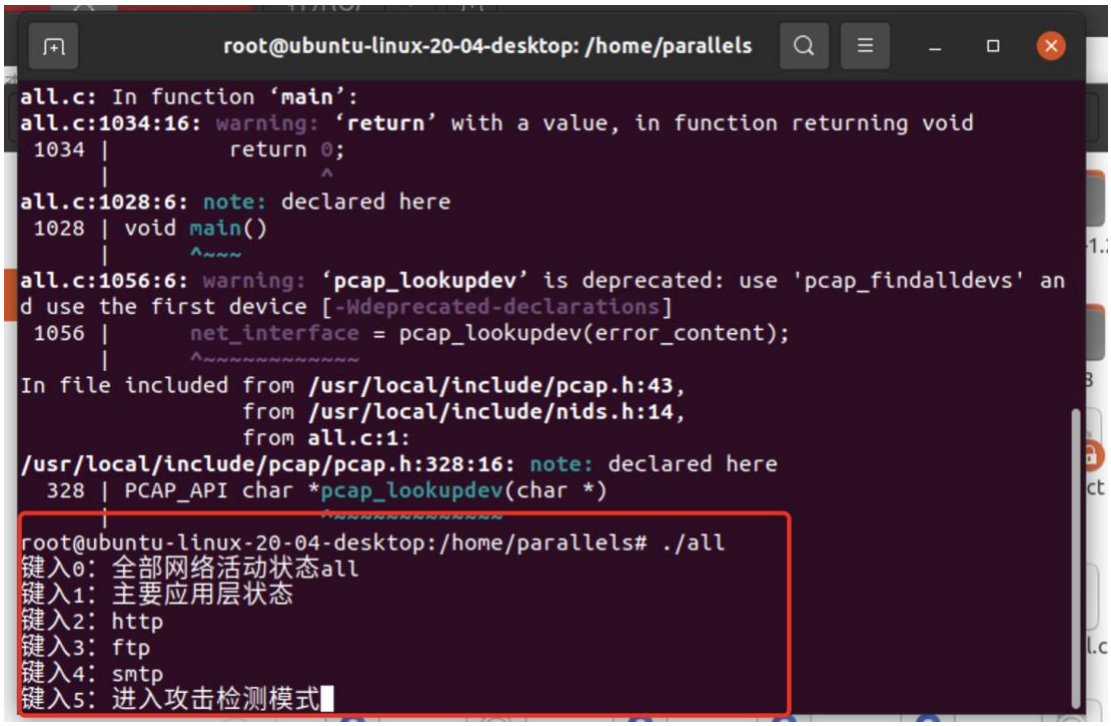
实验名称	**网络空间信息安全审计系统设计与实现**
实验步骤	● *1.实现数据的捕获和内容还原* ● *2.实现内容过滤功能* ● *3.实现安全审计功能*
任务分工	
任务步骤	*1.编写过滤、捕获、内容还原数据的代码* *2.编写检测攻击时将具体内容和时间写入审计日志代码* *3.将上述代码进行整合* *4.运行代码并得出运行结果* *5.分析实验结果并得出结论*
过程记录	*根据任务步骤，在下面单元格中详细记录项目过程中的思路、问题、解决办法、结论、结果，多用图表、截图等展示，代码备查。*

1. 实验运行结果

（1）编译代码并运行





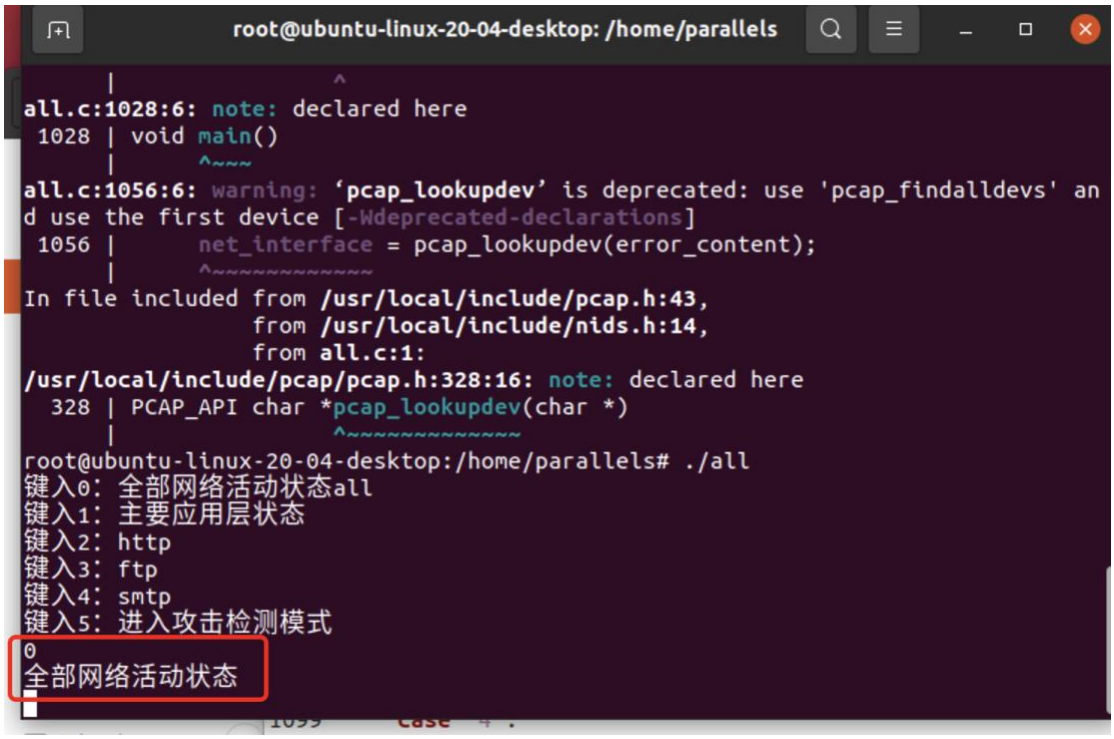
运行后会显示本程序的运行菜单，本程序实现满足了网络空间信息安全审计系统的要求，有以下三种功能：

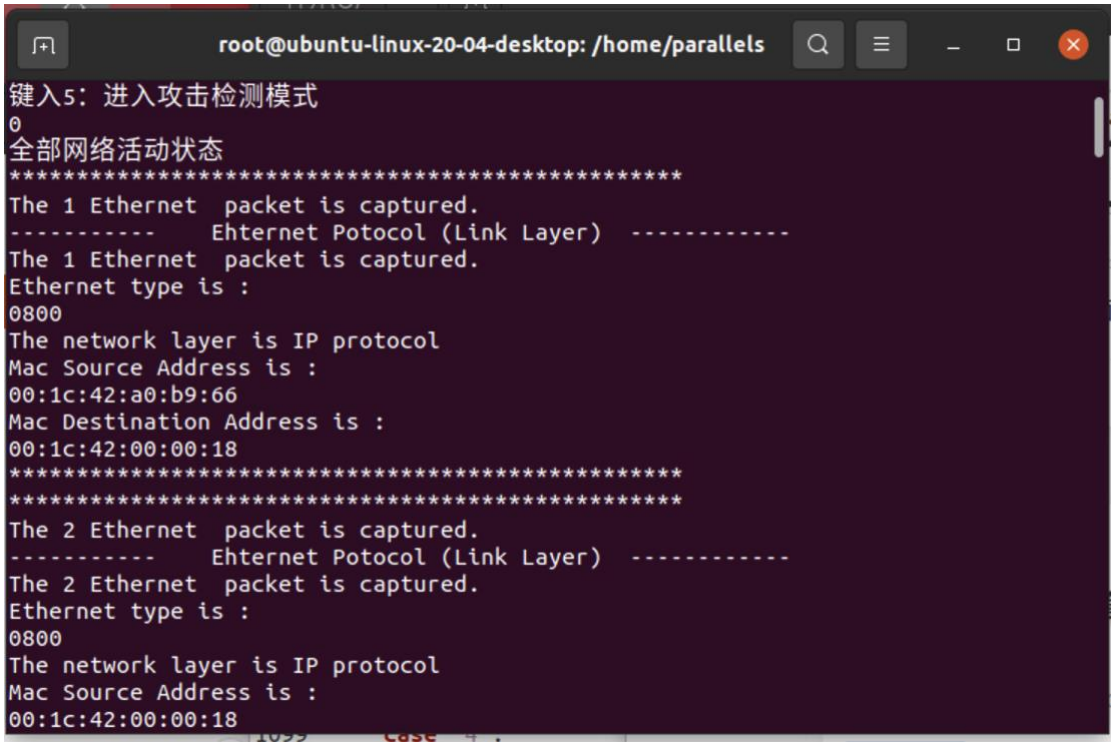
一、根据功能需要的选择，运用 BPF 规则实现对接受数据流的过滤功能，仅捕获我们需要的特定协议的数据。

二、捕获到我们需要的特定协议的数据后，显示协议的连接过程，并对协议传输

的数据进行分析，最后对数据进行还原。
三、通过 Nmap 进行网络攻击，并使用 libnids 检测网络攻击，将 IP 地址、端口号、扫描类型、时间等重要数据记录在审计日志中。

（2）全部网络活动状态界面及结果



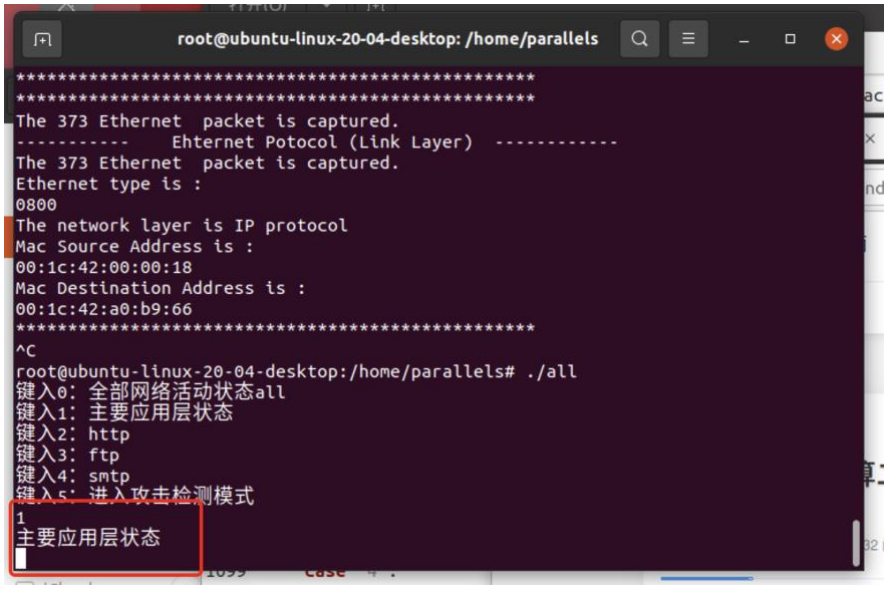


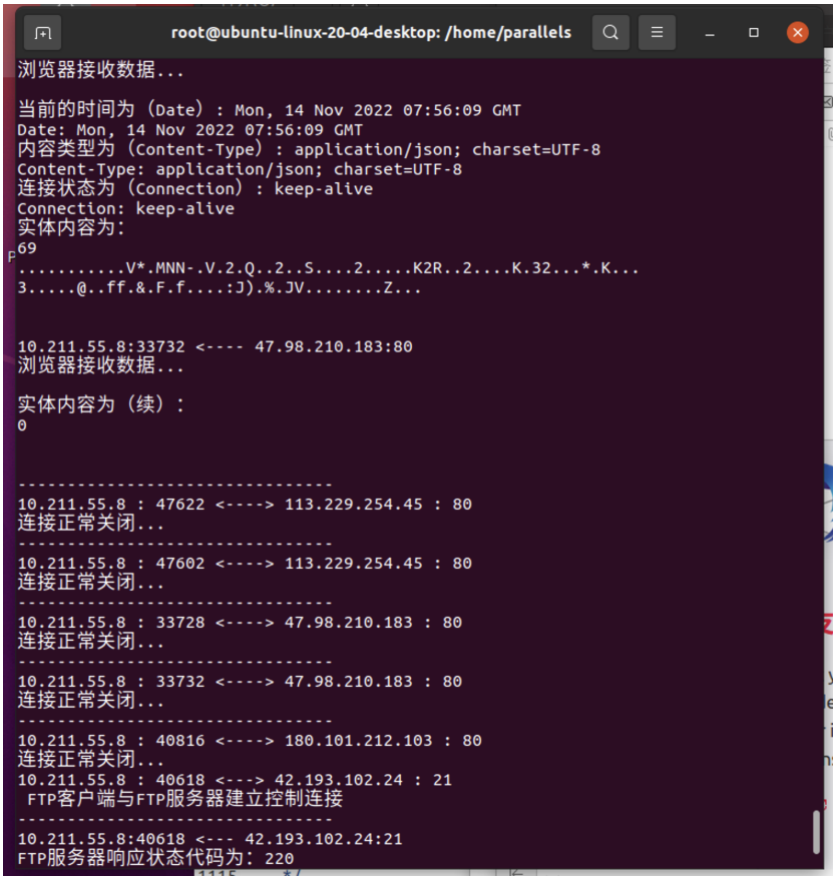
该功能可以通过网卡捕获所有 IP 协议下的互联网活动信息

（3）主要应用层状态界面及捕获结果

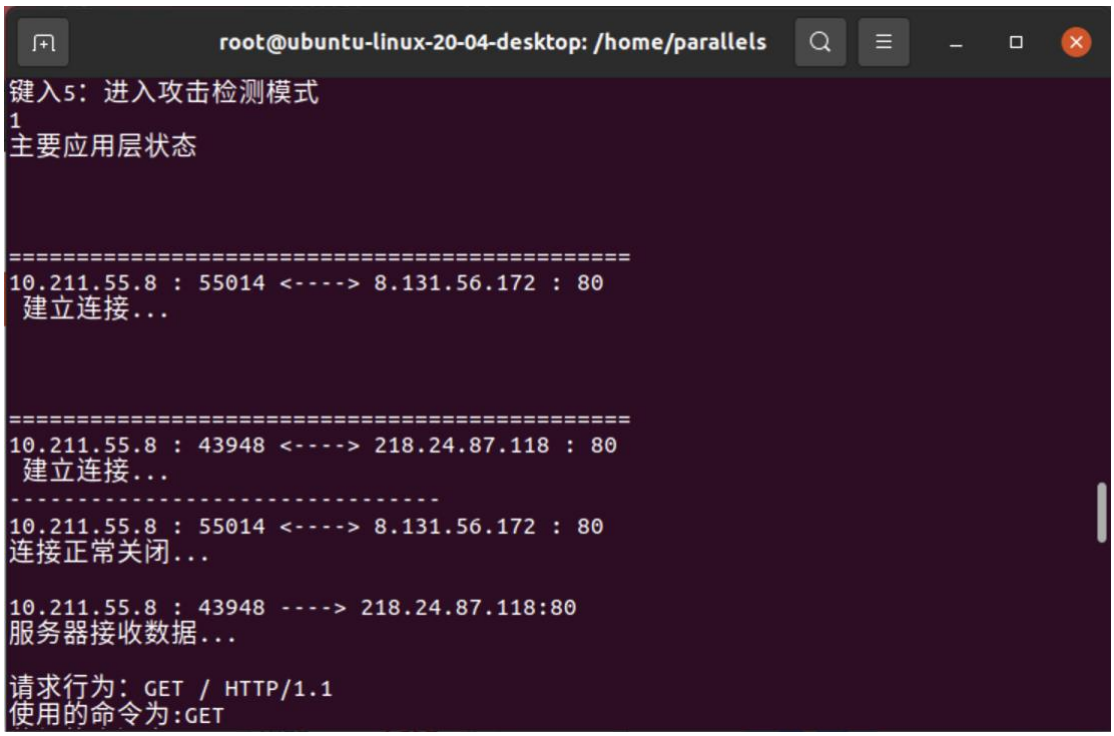
在该功能下，我们可以实现对三种应用层协议的数据的同时捕获并分析，包括 HTTP 协议、FTP 协议、SMTP 协议的数据。在执行该功能的情况下，分别执行能产生三种协议的操作，即可同时捕获到这三种应用层的协议。下面是同时捕获三种不同类型数据的结果。

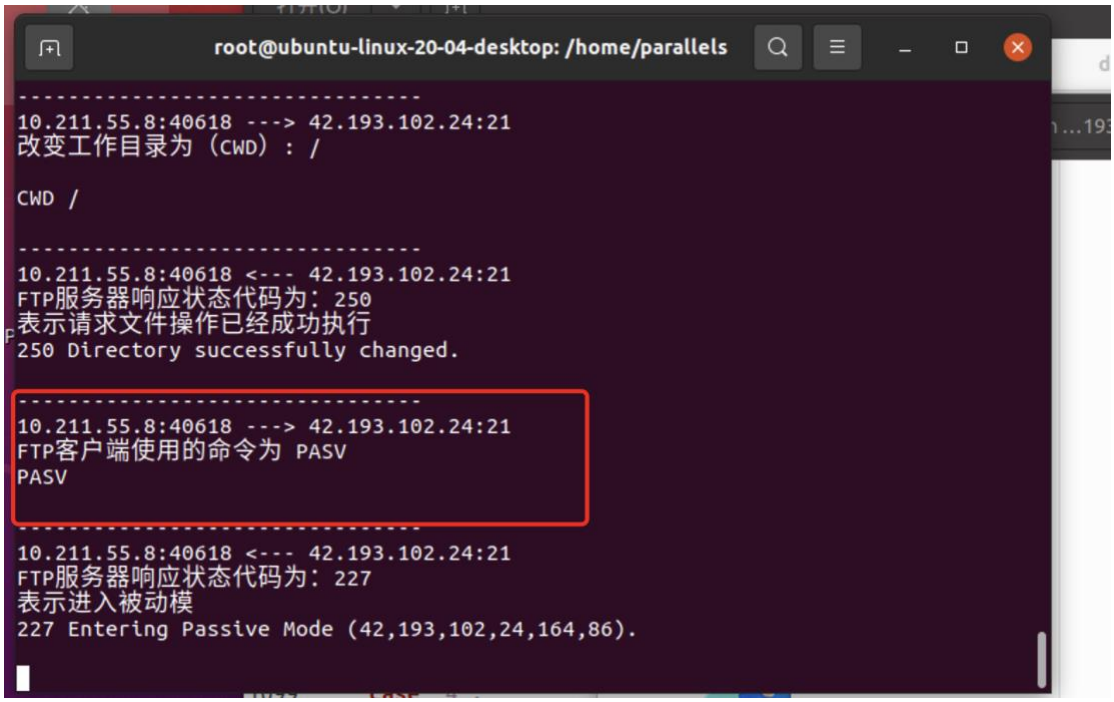
1. 键入 1 进入主要应用层状态的捕获，在该模式下，系统可以捕获网络上全部的 http、ftp 以及 smtp 网络包。





上图可以看出，同时捕获到了 FTP 协议和 HTTP 协议并进行了分析。





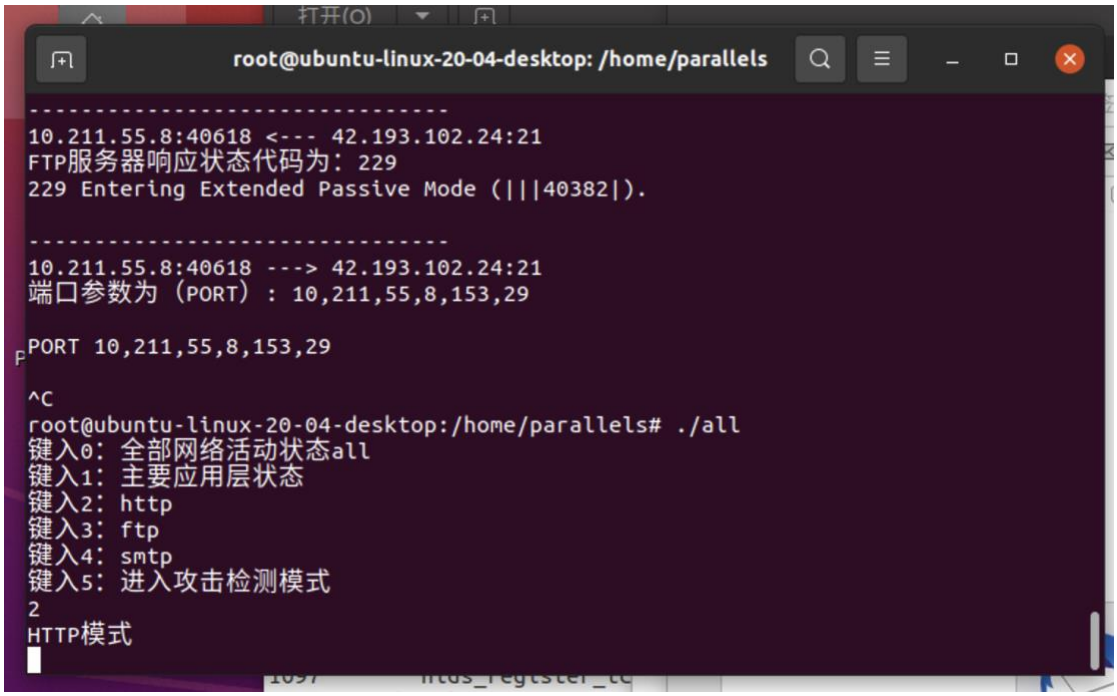
上图可以看出，捕获到了 FTP 协议的数据并进行了分析。

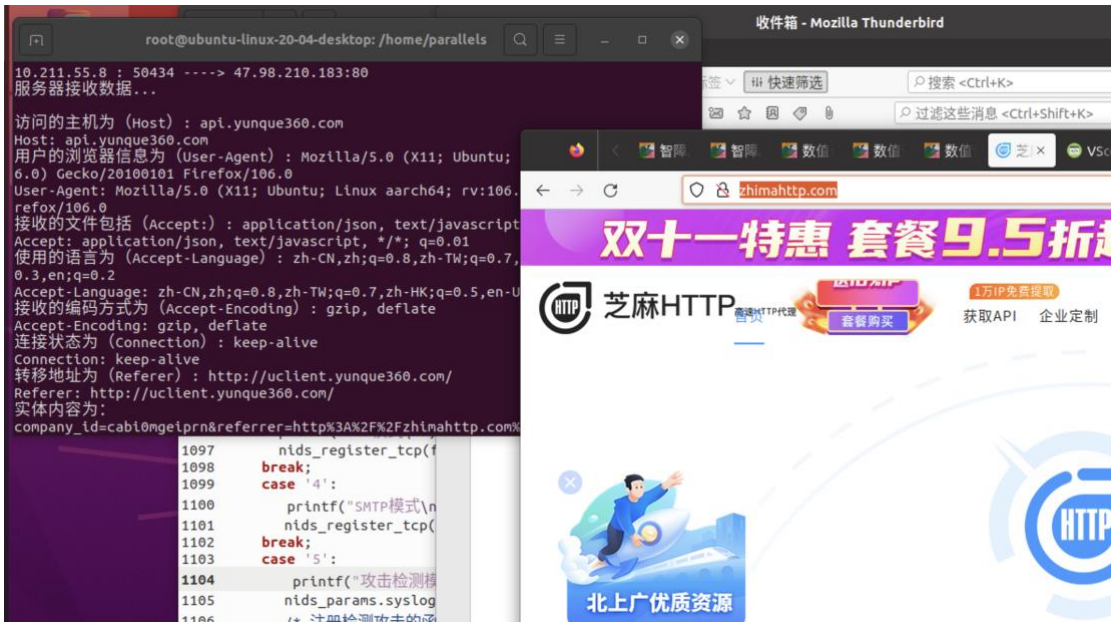
```
访问的主机为（Host）：connectivity-check.ubuntu.com
Host: connectivity-check.ubuntu.com
接收的文件包括（Accept:）：*/*
Accept: */*
连接状态为（Connection）：close
Connection: close
无实体内容

10.211.55.8:50152 <---- 35.232.111.17:80
浏览器接收数据...

当前的时间为（Date）：Mon, 14 Nov 2022 07:58:52 GMT
Date: Mon, 14 Nov 2022 07:58:52 GMT
服务器为（Server）：Apache/2.4.18 (Ubuntu)
Server: Apache/2.4.18 (Ubuntu)
连接状态为（Connection）：close
Connection: close
无实体内容
--------------------------------
10.211.55.8 : 50152 <----> 35.232.111.17 : 80
连接正常关闭...



==========================================
10.211.55.8 : 58374 <----> 202.97.231.111 : 80
 建立连接...

10.211.55.8 : 58374 ----> 202.97.231.111:80
服务器接收数据...

访问的主机为（Host）：ocsp.digicert.cn
Host: ocsp.digicert.cn
用户的浏览器信息为（User-Agent）：Mozilla/5.0 (X11; Linux aarch64; rv:102.0) Gec
ko/20100101 Thunderbird/102.4.2
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:102.0) Gecko/20100101 Thunderbir
d/102.4.2
接收的文件包括（Accept:）：*/*
Accept: */*
使用的语言为（Accept-Language）：zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=
0.3,en;q=0.2
```

上图可以看出，同时捕获到了 HTTP 协议和 SMAT 协议的数据并进行了分析。

2. 仅捕获 HTTP 协议数据并进行分析

在选择捕获 HTTP 协议的功能的情况下，通过浏览器浏览 HTTP 网页，即可产生 HTTP 协议数据并进行捕获分析。

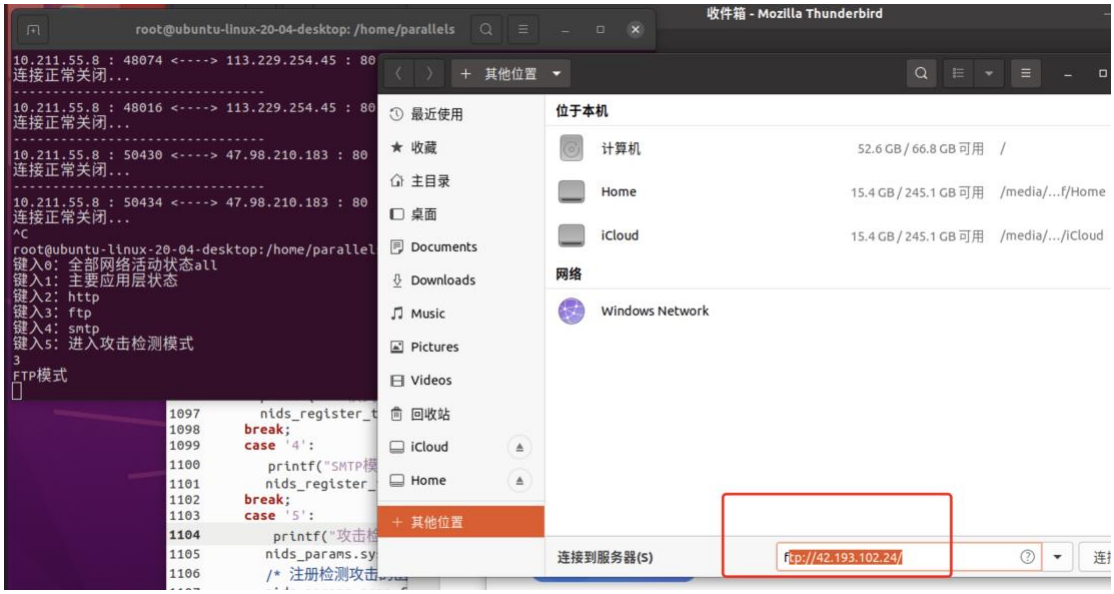




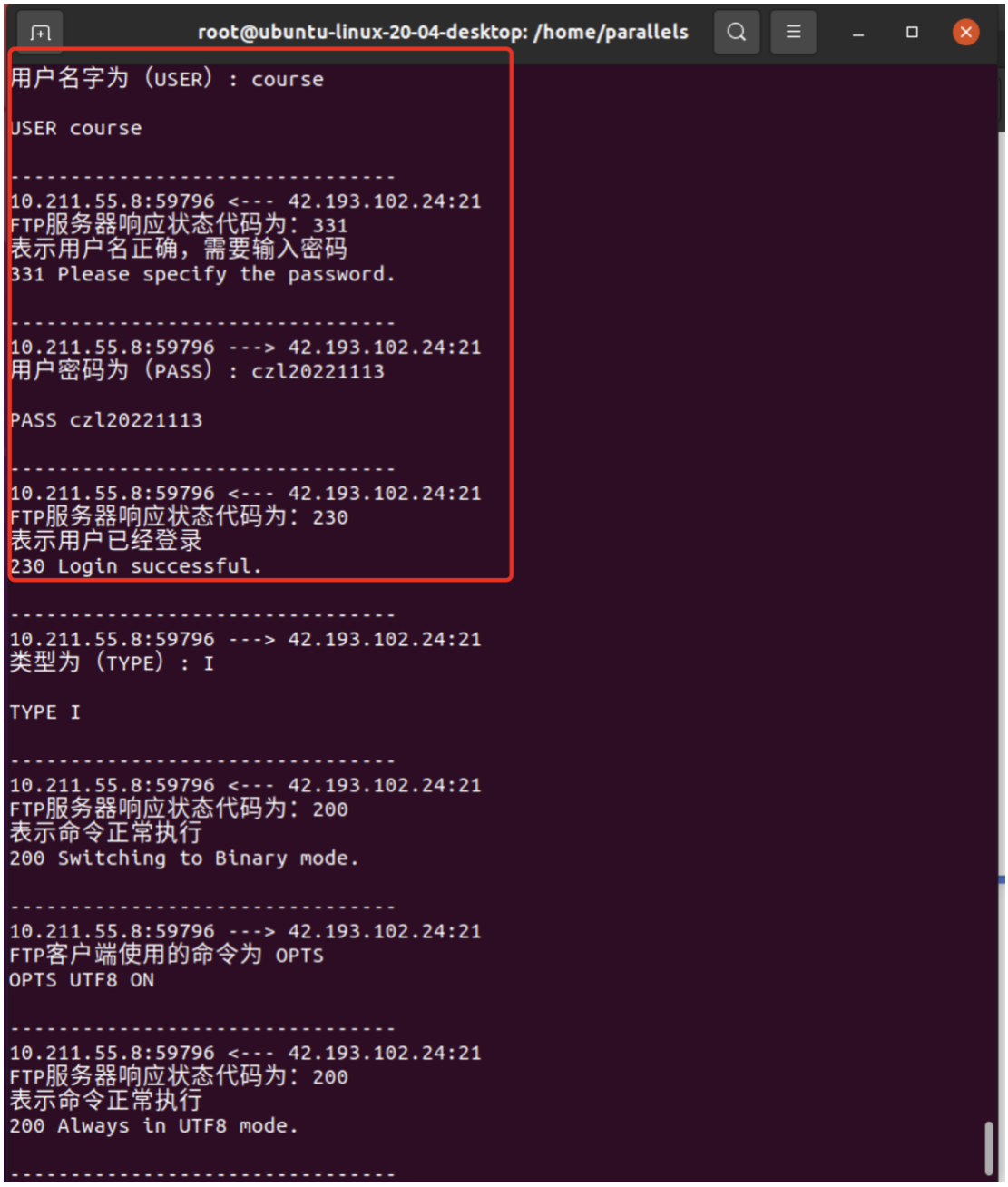
上图可以看出，通过浏览器浏览了一个 HTTP 协议的网址，产生了 HTTP 数据，并进行了捕获和分析。HTTP 协议数据包的产生是由于我们打开了

3. 仅捕获 FTP 协议数据并进行分析

在选择捕获 FTP 协议的功能的情况下，通过登陆 FTP 服务器，即可产生 FTP 协议数据并进行捕获分析。



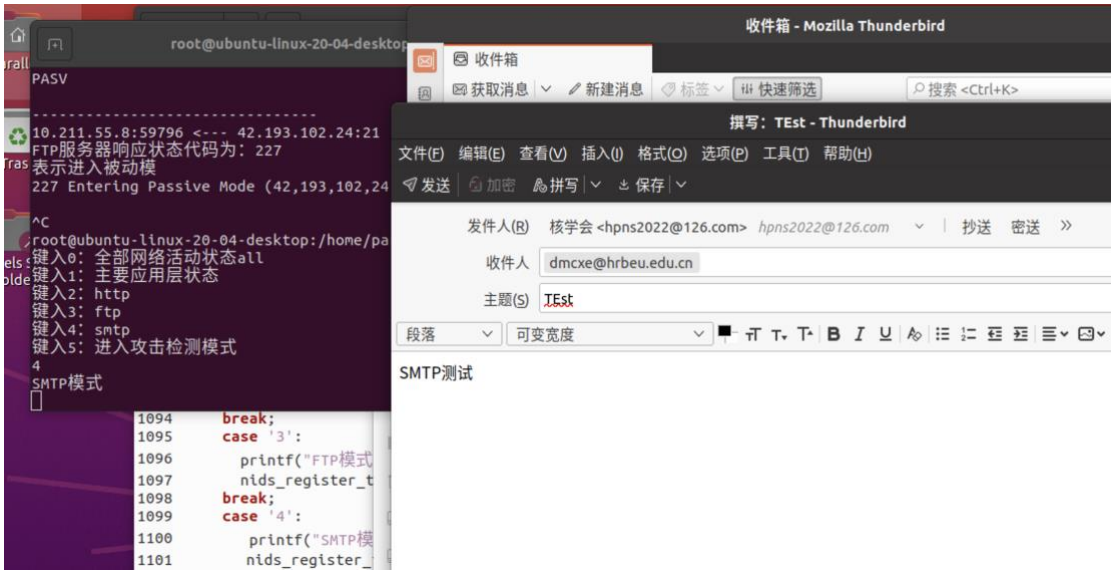
上图是连接 FTP 服务器的操作，通过该操作即可产生 FTP 协议的数据，方便我们进行捕获。FTP 服务器依赖于腾讯云轻量应用服务器上搭建的 FTP 服务。当我配置开放端口 21 后，在 linux 环境下对服务器进行访问，由于未设置安全协议，因此过程中全部的账号、密码均通过明文传播。



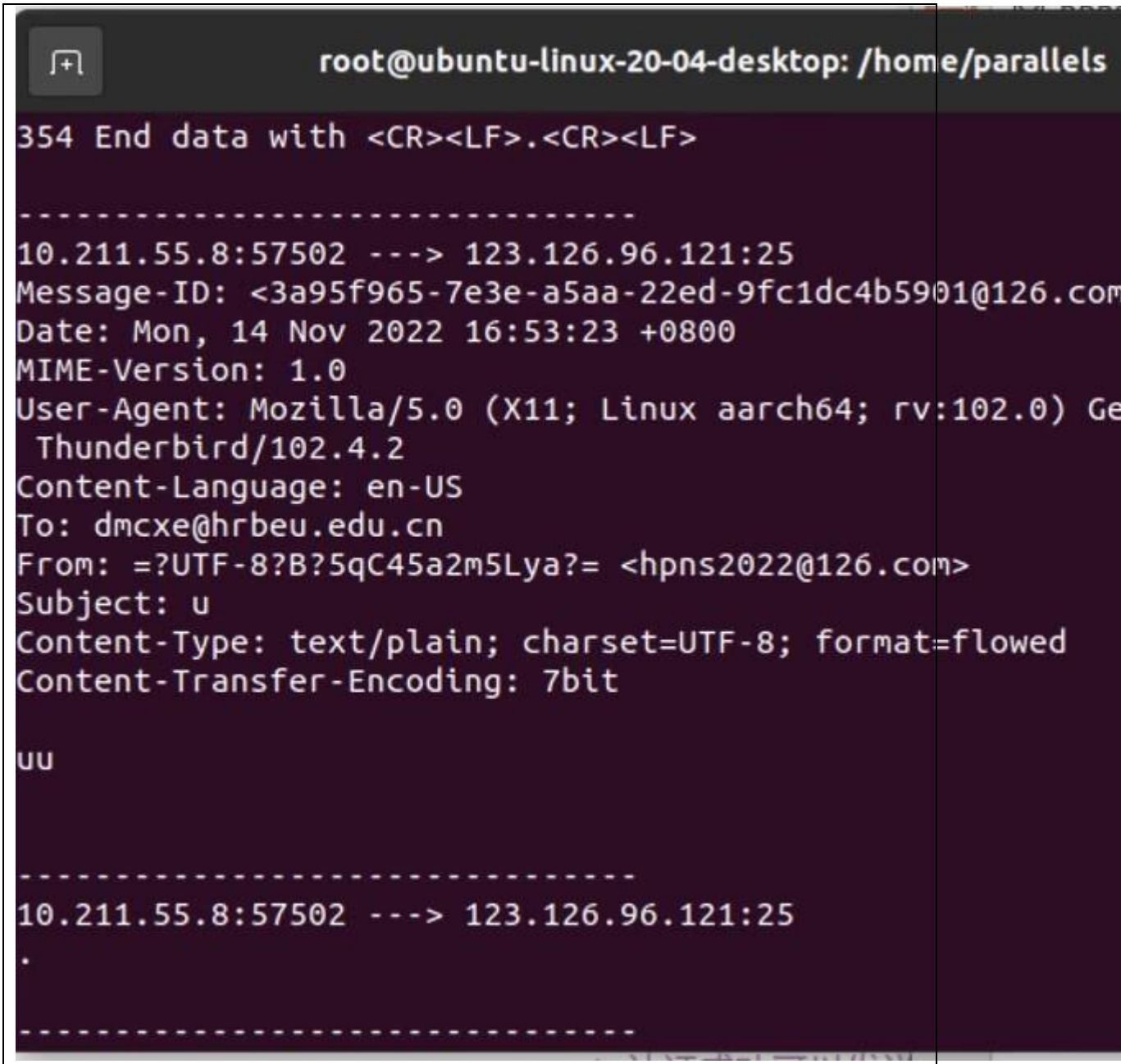
上图是我们捕获到的 FTP 协议的数据并进行分析的结果。它包含了我们明文传送的账号与密码，以及 FTP 服务器的活动状态。

4 仅捕获 SMTP 协议数据并进行分析

在选择捕获 SMTP 协议的功能的情况下，通过邮件客户端发送邮件，即可产生 SMTP 协议数据并进行捕获分析。

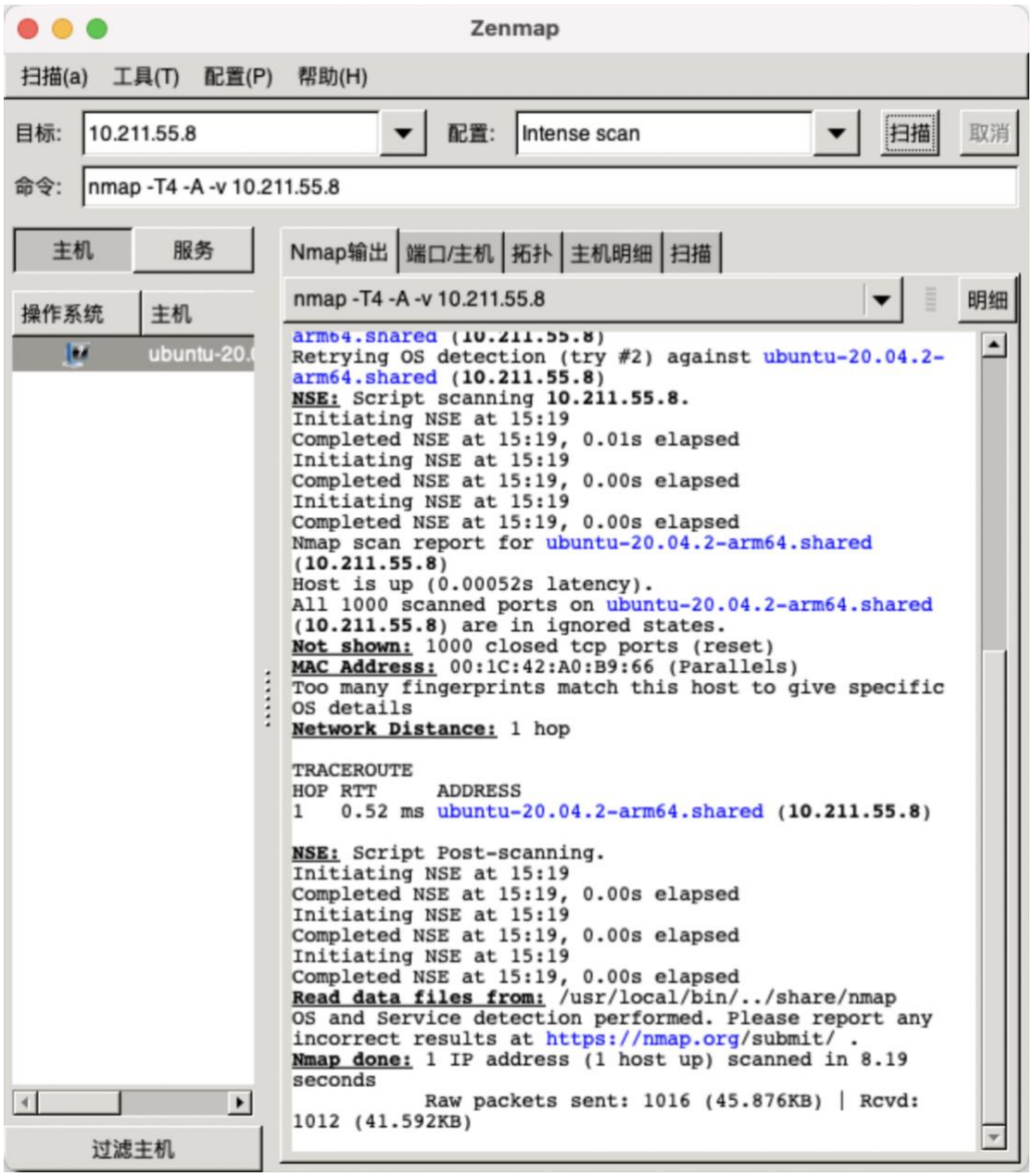


SMTP 数据包的产生与 POP3 数据包的产生类似，需要通过邮件客户端联系 smtp 服务器并关闭 SSL 安全协议选定合适的端口才能够正常运行并抓到网络中的 smtp 数据包。数据包的形式与 POP3 数据包类似。

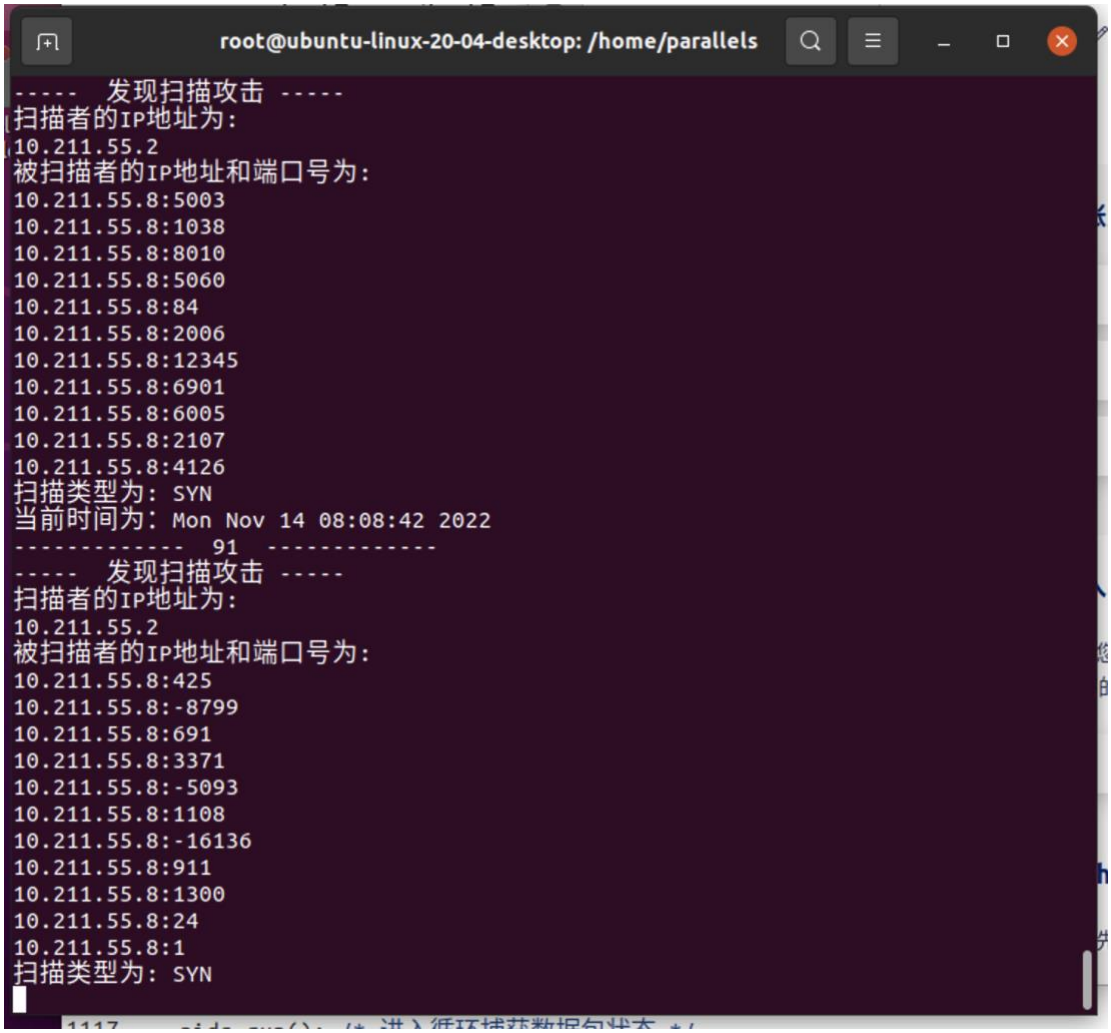


上图是我们通过邮件客户端发送邮件后产生的 SMTP 协议并捕获和分析的结果。

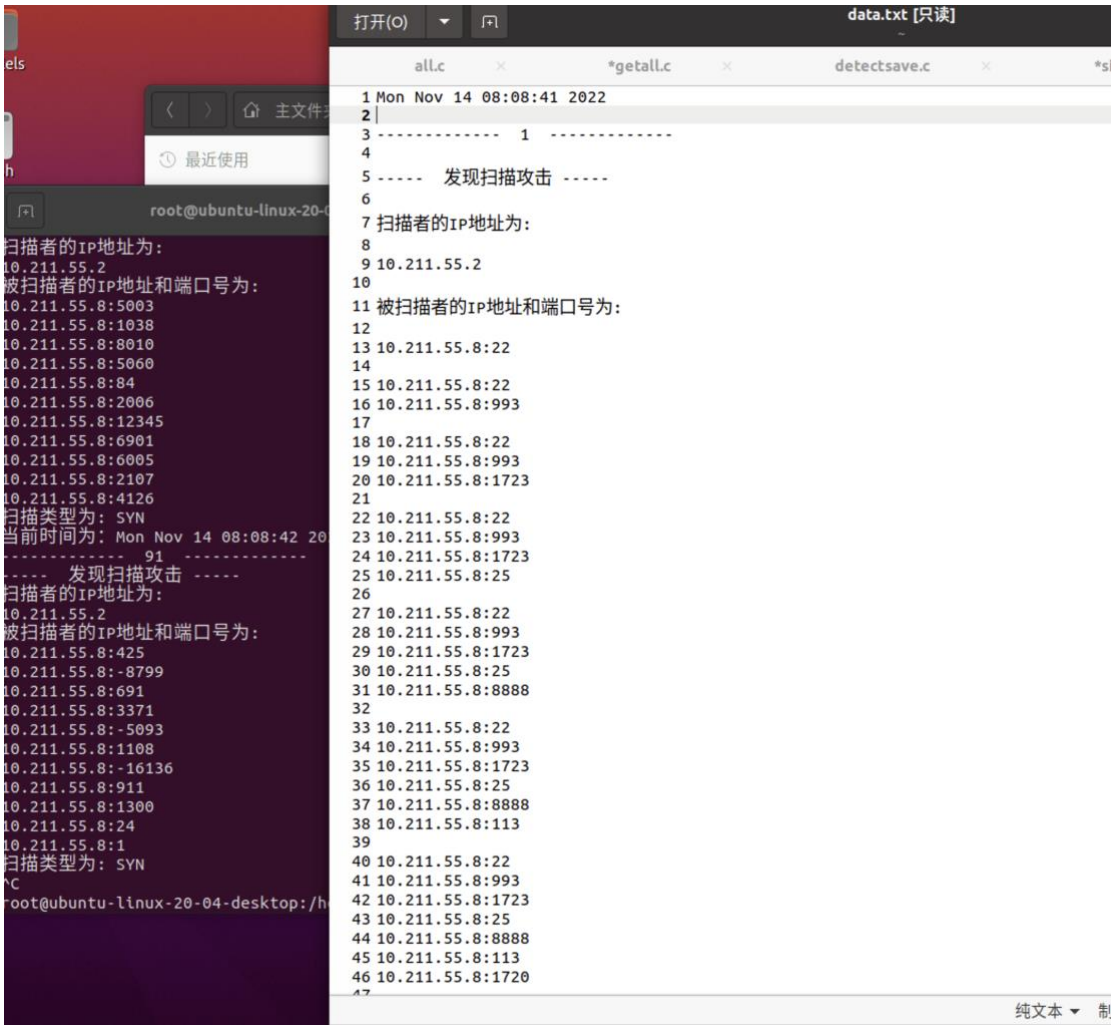
（3）攻击检测模式：利用 Nmap 软件在主机上攻击虚拟机，并使用 libnids 检测网络攻击，将 IP 地址、端口号、扫描类型、时间等重要数据记录在审计日志中。



在虚拟机中查找到虚拟机 IP，并在主机中执行命令 nmap -PS IP 协议即可产生对虚拟机的攻击



上图是捕获到的攻击的重要信息，IP 地址、端口号、扫描类型。



上图是我们实现的将重要信息和时间记录在审计日志中的功能的结果。

2. 分析实验结果，得出实验结论

通过对网络安全开发包详解书籍的学习以及对网络上一些相关资料的查找与学习，我们通过小组合作交流讨论编写了本代码，实现满足了网络空间信息安全审计系统的要求，实现了以下三种功能：

一、根据功能需要的选择，运用 BPF 规则实现对接受数据流的过滤功能，仅捕获我们需要的特定协议的数据。

二、捕获到我们需要的特定协议的数据后，显示协议的连接过程，并对协议传输的数据进行分析，最后对数据进行还原。

三、通过 Nmap 进行网络攻击，并使用 libnids 检测网络攻击，将 IP 地址、端口号、扫描类型、时间等重要数据记录在审计日志中。

编译并运行代码后，我们执行了三种产生所需应用层协议的数据的操作，通过浏览器浏览 http 网页产生 HTTP 协议的数据，通过邮件客户端发送邮件产生 SMTP 协议的数据，通过连接 FTP 服务器产生 FTP 协议的数据。

通过运行结果截图可以看出，我们很好地满足了我们所设计的功能，既能同时捕获 HTTP 协议、FTP 协议、SMTP 协议的数据，又能在 BPF 过滤规则下实现对单独一种我们需要的协议的捕获，且两种模式下，我们均实现了对捕获到的数据的分析。并且在用 Nmap 软件在主机上攻击虚拟机的情况下，在虚拟机中我们实现了对攻击信息的记录，将重要信息和时间记录在审计日志中，满足了实验要求。

过程记录	*根据任务步骤，在下面单元格中详细记录项目过程中的思路、问题、解决办法、结论、结果，多用图表、截图等展示，代码备查。*
过程记录	*根据任务步骤，在下面单元格中详细记录项目过程中的思路、问题、解决办法、结论、结果，多用图表、截图等展示，代码备查。*