**西安邮电大学**

**网络空间安全学院**

**实验报告**

**（2020/ 2021学年第2学期）**

实验名称： 网络空间安全基础实践

学生姓名： 王璐 \_\_\_\_\_\_\_

专 业： 网安2101班 \_\_

学 号： 26213035（35）\_\_\_\_\_

指导教师： 冯景瑜

**西安邮电大学网络空间安全学院网络空间安全基础实践课程**

**考核表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **学生姓名** | **王璐** | **班级/学号** | | **网安2101/26213035** | |
| **承担任务实验室（单位）** | **网络空间安全实验室** | **所在部门** | | **网络空间安全系** | |
| **实施时间** | **2022年 4月 25日 — 2021年 4月 30日** | | | | |
| **实验内容** | **（一）经典网络空间攻防案例中的法律分析**  **（二）漏洞扫描器的使用**  **（三）网络嗅探熟悉** | | | | |
| **指导教师（师傅）姓名** | **冯景瑜** | **职务或职称** | | **副教授** | |
| **指导教师（师傅）**  **对学生的评价** | **评价点** | **评价内容** | | | **评价得分** |
| **平时成绩**  **（20分）** | **投入学习时间、课堂纪律及学习态度、遵守实验室的规章制度等情况** | | |  |
| **实验能力**  **（30分）** | **法律意识能力、漏洞扫描能力、嗅探分析能力** | | |  |
| **实验验收**  **（20分）** | **实验要求达成情况**  **实验演示与答辩情况** | | |  |
| **实验报告**  **（30分）** | **语言及文字表达能力**  **实验报告工作量及撰写规范性** | | |  |
| **总评成绩** |  | | **五级制** |  | |
| **指导教师（师傅）评语** | **指导教师（师傅）签字**  **2022年 4月 30 日** | | | | |

**实验三：网络嗅探熟悉**

**1实验目的和要求**

**1.1实验目的**

掌握嗅探工具的使用方法，实现捕捉HTTP、FTP、SMTP、TELNET 等协议的数据包，初步了解 TCP/IP 主要协议的数据结构、会话连接建立和终止的过程、TCP 序列号应答号的变化规律。

**1.2基本要求：**

1.2.1选择一款常用的嗅探工具，比如Wireshark；

1.2.2描述嗅探工具的安装过程，给出截图；

1.2.3用嗅探工具监听局域网或个人电脑通信过程，比如进行网页登陆邮箱或FTP登录，分析捕获数据包，描述整个嗅探过程；

1.2.4为了减少分析的数据量，必须有效地设置过滤规则；

1.2.5完成嗅探工作之后，撰写实验报告，并分析如何对局域网嗅探器进行防范。

**2实验原理**

**2.1**网络嗅探

**2.2**使用嗅探工具

**2.3** Wireshark是一个网络封包分析软件，网络封包分析软件的功能是抓取网络封包，并尽可能显示出最为详细的网络封包资料，Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。

2.4安装时需要安装WinPcap和USBPcap

2.5实验背景

嗅探器知识原理

嗅探技术是网络安全攻防技术中很重要的一种，通过他可以获取网络中的大量信息。与主动扫描相比，嗅探更难以被察觉，能够对网络中的活动进行实时监控。

网络嗅探器实际上就是网络中的窃听器，其用途就是捕获分析网络中的数据包，帮助网络管理员发现入侵、分析网络问题等等，它是能够进行嗅探的软件或硬件设备。通过嗅探得到二进制的数据包后，对这些数据包进行解析和理解，获得协议字段与传输的数据的过程就是网络协议分析。所以说，网络嗅探与网络协议分析联系紧密。

对于攻击者来说，通过网络嗅探，进行协议分析，能够窃取内部机密，搜集信息。而对于管理员来说，网络嗅探可以实现网络流量情况的监听，定位网络故障，并且能够为网络入侵检测提供底层的数据来源。

网络嗅探的关键在于以太网的通信机制和网卡的工作模式。迄今为止，以太网仍然是最普遍的组网方法之一，而以太网的共享特性决定了嗅探能够成功。由于以太网是基于广播方式传送数据，因此网络中所有的数据信号都会被传送到每一个主机节点，这样每一台机器实际上都能接受到数据帧。由于在正常情况下，一个网络接口应该只响应目MAC的地址为本机一件地址的数据帧、向所有设备发送的广播数据帧。一个网络接口使用网卡的接收模式有以下几种：

广播模式（Broadcast Mode）：该模式下的网卡能够接收网络中所有类型为广播报文的数据帧。

组播模式（Multicast Mode）：该模式下的网卡能够接受特定的组播数据。

直接模式（Unicast Mode）：该模式下的网卡在工作时只接收目的地址匹配本机MAC地址的数据帧。

混杂模式（Promiscuous Mode）：在这种模式下，网卡对数据帧中的目的MAC地址不加任何检查，全部接收。

因此只要将网卡的工作模式设置为“混杂模式”，网卡将会接受所有传递给他的数据包，从而实现嗅探。嗅探得到结果后，再进行网络协议分析，根据网络协议分析的粒度可以分为三种：针对原始数据包进行分析，层次最低、最细粒度；对网络流（会话）进分析，通过5元组进行流（会话）；以及网络流高层统计。针对网络报文分析的工具，常用的有集成工具WireShark，网络流重组工具Nstreams、Snort，进行高层统计和摘要分析的Netflow、RRDTools等等。

Wireshark简介

Wireshark（前称Ethereal）是一个网络封包分析软件。网络封包分析软件的功能是截取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark使用WinPcap作为接口，直接与网卡进行数据报文交换。

网络封包分析软件的功能可想象成“电工技师使用电表来量测电流、电压、电阻”的工作——只是将场景移植到网络上，并将电线替换成网络线。在过去，网络封包分析软件是非常昂贵的，或是专门属于盈利用的软件。Wireshark的出现改变了这一切。在GNUGPL通用许可证的保障范围底下，使用者可以免费取得软件与其源代码，并拥有针对其源代码修改及客制化的权利。Wireshark是目前全世界最广泛的网络封包分析软件之一，它可以帮助网络管理员解决网络问题，帮助网络安全工程师检测安全隐患，开发人员可以用它来测试协议执行情况、学习网络协议等。

Wireshark的特性

Wireshark拥有以下特色功能：

支持UNIX、Windows、MacOS、Solaris等多个平台；

在接口实时捕捉包；

能详细显示包的详细协议信息；

可以打开/保存捕捉的包；

可以导入导出其他捕捉程序支持的包数据格式；

可以通过多种方式过滤包；

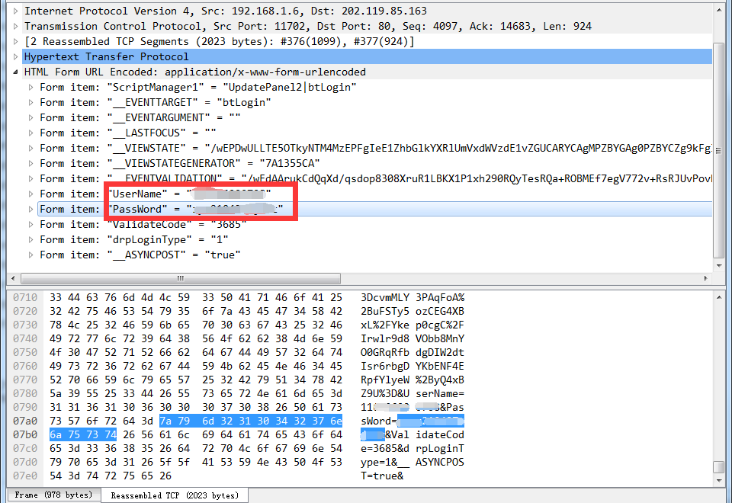
多种方式查找包；

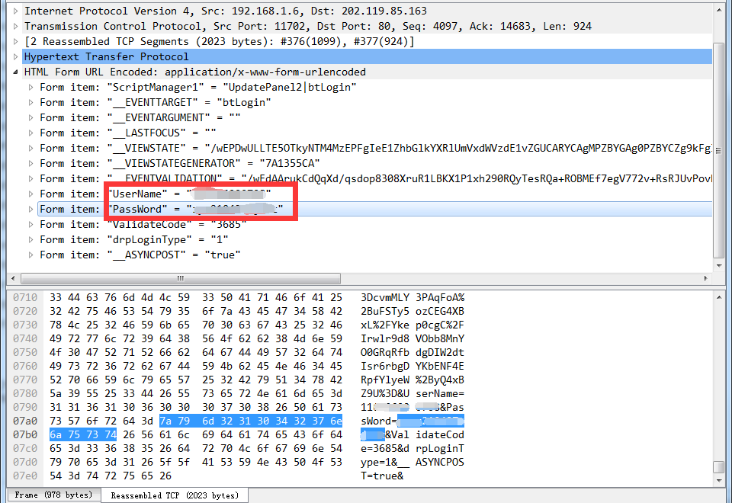
通过过滤以多种色彩显示包；

创建多种统计分析。

Wireshark的使用

Wireshark的使用界面如图3.1所示，它能够实时捕获包，并且能够显示获取的数据包的内容。





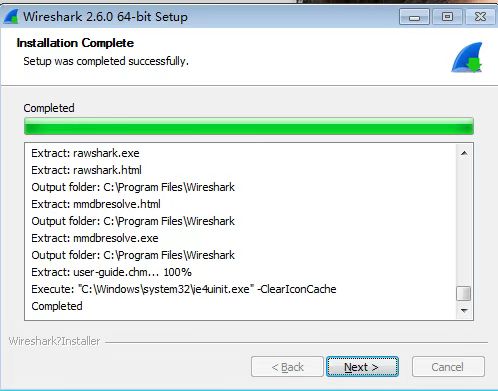
**3实验内容及步骤**

**3.1**具备网络嗅探的基本知识。

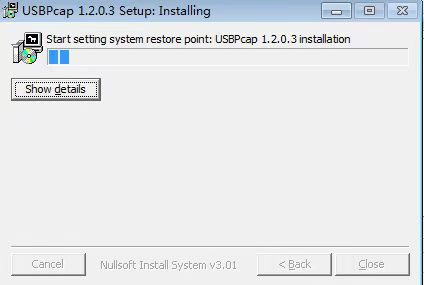
**3.2**到 Wireshark 官方网站（www.wireshark.org/download.html）下载

Wireshark软件。

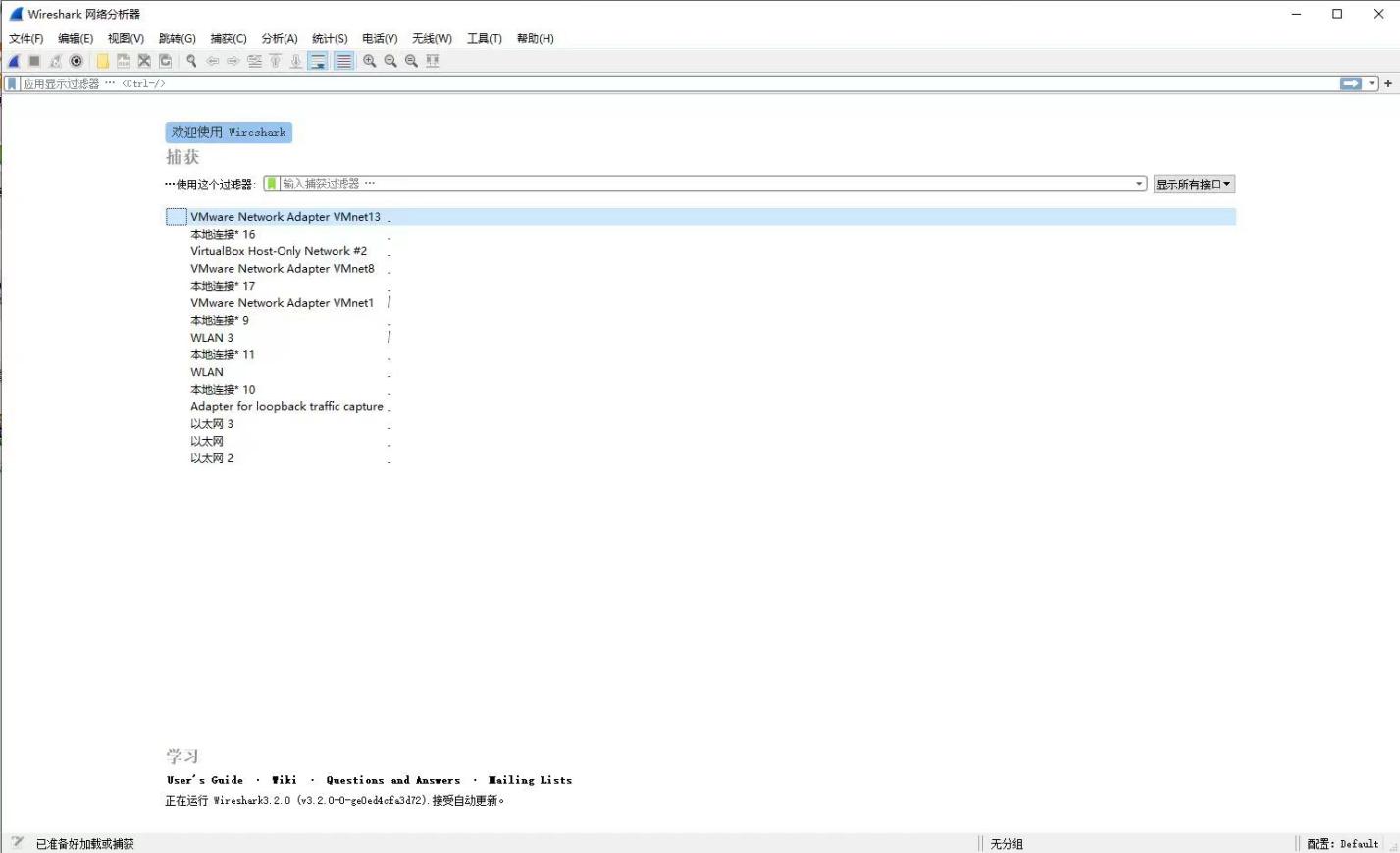
**3.3**阅读 Wireshark 官方安装文档和使用文档。

****

****

****

**4实验结果分析**

****

通过安装wireshark，了解了网络嗅探。安装并运行wireshark后，开始抓包。

## 4.1实施抓包

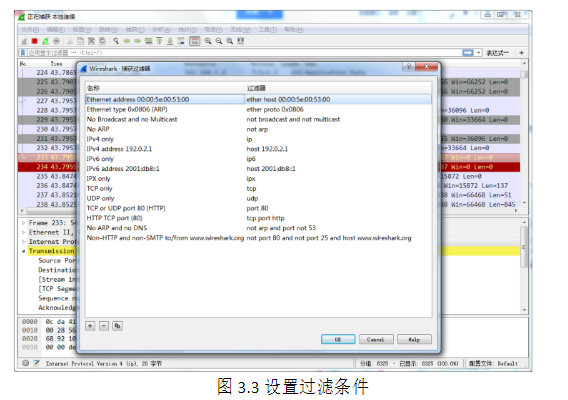
4.1.1在 Windows 的“开始”菜单中，单击 Wireshark 菜单，启动 Wireshark， Wireshark 的主界面，界面中显示了当前可使用的接口，例如，本地连接 5、本地连接 10 等。要想捕获数据包，必须选择一个接口，表示捕获该接口上的数据包。  
4.1.2选择捕获“本地连接”接口上的数据包。选择“本地连接”选项，然后单击左上角的“开始捕获分组”按钮，将进行捕获网络数据，  
图中没有任何信息，表示没有捕获到任何数据包。这是因为目前“本地连接”上没有任何数据。只有在本地计算机上进行一些操作后才会产生一些数据，如浏览网站。

4.1.3当本地计算机浏览网站时，“本地连接”接口的数据将会被 Wireshark 捕获到。捕获的数据包如图所示。图中方框中显示了成功捕获到“本地连接”接口上的数据包。

4.1.4Wireshark 将一直捕获“本地连接”上的数据。如果不需要再捕获，可以单击左上角的“停止捕获分组”按钮，停止捕获。

## 4.2使用显示过滤器

默认情况下，Wireshark 会捕获指定接口上的所有数据，并全部显示，这样会导致在分析这些数据包时，很难找到想要分析的那部分数据包。这时可以借助显示过滤器快速查找数据包。  
显示过滤器是基于协议、应用程序、字段名或特有值的过滤器，可以帮助用户在众多的数据包中快速地查找数据包，可以大大减少查找数据包时所需的时间。  
使用显示过滤器，需要在 Wireshark 的数据包界面中输入显示过滤器并执行。



## 4.3分析数据包层次结构

任何捕获的数据包都有它自己的层次结构，Wireshark 会自动解析这些数据包，将数据包的层次结构显示出来，供用户进行分析。这些数据包及数据包对应的层次结构分布在 Wireshark 界面中的不同面板中。  
下面介绍如何查看指定数据包的层次结构。  
4.2.1 使用 Wireshark 捕获数据包，界面如图所示。

4.2.2以 HTTP 协议数据包为例，了解该数据包的层次结构。在 Packet List 面板中找到一个 HTTP 协议数据包

**5实验总结及心得体会**

5.1通过本次实验，学习到了Wireshark的安装及使用方法，捕获过滤器表达式作用在wireshark开始作用捕获数据包之前，只捕获符合条件的数据包，不记录不符合条件的数据包。

5.2在wireshark2.x版本，启动后欢迎界面既有捕获过滤器，在其中输入过滤表达式开始捕获数据包时即生效。

