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27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

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

**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

利用ARP协议的无认证机制，通过伪造虚假的ARP响应，向工控试验箱的PLC发送错误的MAC地址信息。PLC会更新其ARP缓存，导致后续的数据包无法正确到达目标设备，从而实现拒绝服务（DoS）攻击的效果。这种攻击可以干扰PLC的正常通信，导致工控网络功能异常。

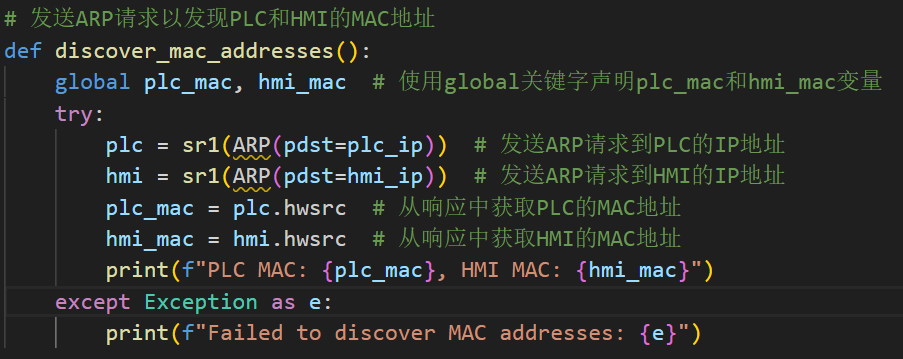
### 3、实验目标和实验步骤

#### 目标：

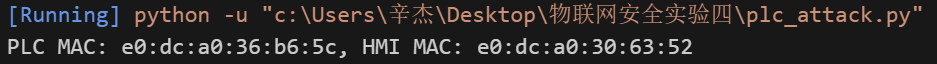
使用Python Scapy对工控试验箱PLC进行ARP攻击实验，达到拒绝服务攻击效果。

#### 实验步骤：

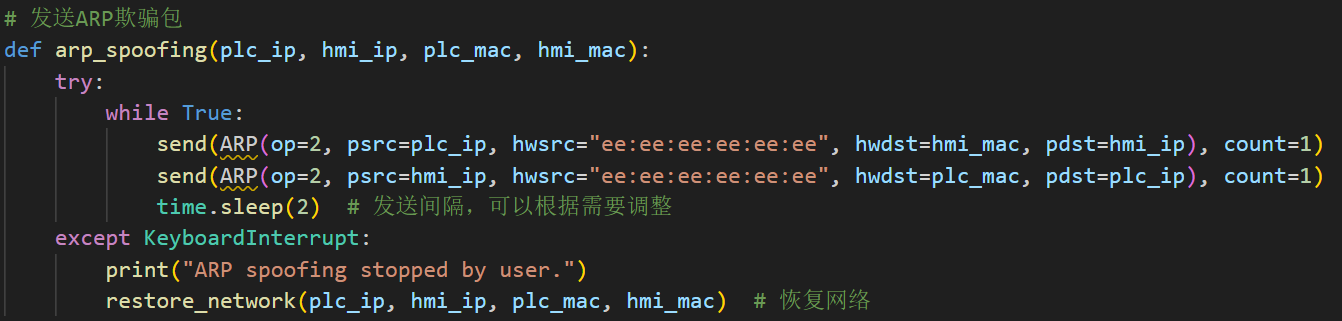
##### 发送ARP请求包确认并记录PLC和HMI的MAC地址与IP地址

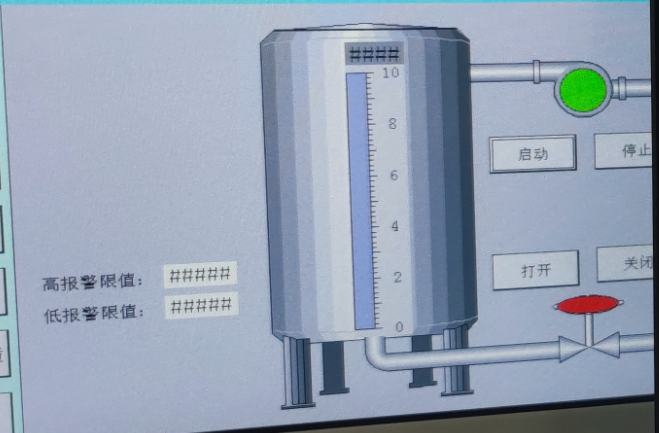
发送方检查ARP缓存表，如果没有目标IP地址对应的MAC地址，则构造一个ARP请求包并广播到局域网中；PLC和HMI接收到请求后，如果IP地址匹配，它们会发送ARP响应包，包含自己的MAC地址；发送方接收到响应后，更新ARP缓存表并记录下PLC和HMI的MAC地址与IP地址的对应关系。

运行结果

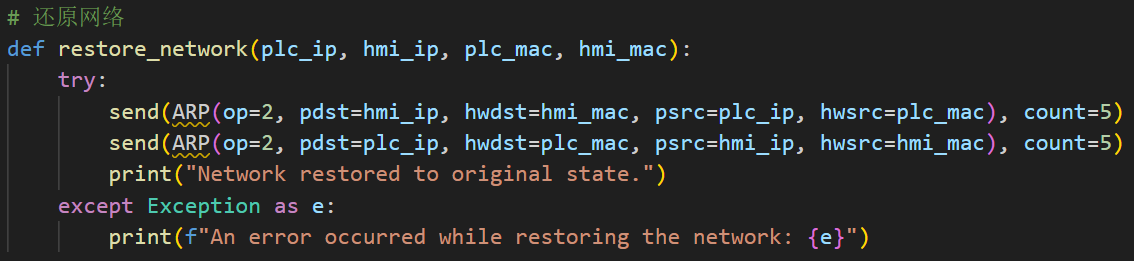


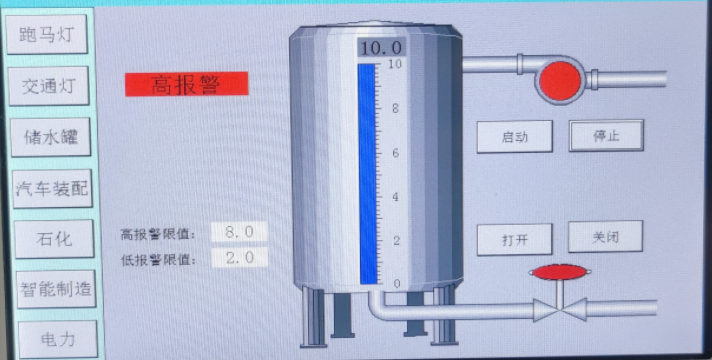
##### 利用ARP欺骗攻击，使得HMI无法控制PLC

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。



##### 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。



## 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. **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
5. **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
6. **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
7. **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、实验遇到的问题及解决办法

### 问题一：在实验的过程中，某些实验箱的HMI无法连接上

在某周实验过程中正常连接工程箱子，可以ping通PLC但是无法ping 通HMI，导致无法发送arp包获得HMI的硬件地址，又换了一个实验箱子发现还是不能ping通HMI，下周上箱子才可以正常连接HMI

**原因分析**：玄学，没搞懂为啥，可能是上次实验同学忘记恢复HMI的arp了

**解决办法**：换台机器，或者等一段时间PLC工程箱自动恢复arp映射

### 问题二：循环发送arp请求包，导致恢复和攻击同时存在

一开始我的代码是先进行arp欺骗攻击，循环发送欺骗包，然后停止发送欺骗包循环发送正常的arp包，两端代码在一起，会导致PLC一会正常一会异常

**原因分析：**问题的根本原因在于ARP缓存的动态更新机制。攻击阶段发送的ARP欺骗包和恢复阶段发送的正常ARP包相互竞争，导致PLC的ARP缓存在错误和正确的MAC地址之间不断切换，造成通信状态一会正常一会异常

**解决办法：**严格分离攻击与恢复阶段，停止攻击包发送后再发送恢复包，使用.ipynb文件来实现实验的代码编写和执行。

## 六、收获感悟

通过本实验，可以深入理解ARP协议的工作机制及其安全性漏洞，同时认识到网络协议中缺乏认证机制可能带来的严重威胁。实验也提醒我们，在工业控制系统中，强化网络安全措施（如启用静态ARP表或使用网络隔离）至关重要，以防止类似攻击对关键设备和生产过程造成破坏。