实验二：中间人攻击

【实验目标】

通过本次实验，理解局域网中的安全风险，深入理解 ARP 欺骗和中间人攻击的工作原理、技术和风险，掌握协议包数据的构造与发送方法。

【实验环境】

处于同一局域网的三台主机（可以使用虚拟机），其中一台主机为攻击机，攻击机使用装有 Scapy 软件包的 Linux 操作系统。

目前，为实验环境准备两个虚拟机镜像：Ubuntu 和 kali，百度云网盘链接: https://pan.baidu.com/s/1mhJgubm 密码: yhpb。推荐从清华镜像源下载 ubuntu 镜像安装，https://mirrors.tuna.tsinghua.edu.cn/#，从 https://www.kali.org/downloads/ 下载最新版的 kali 机安装使用，页面有完整版的安装教程可以学习。

Kali 为攻击者，Ubuntu 作为靶机，并选择如 www.baidu.com 进行 http 访问，或公开 ftp 站点进行 ftp 实验；也可以利用 Ubuntu 做两个虚拟机，其中一个虚拟机内自行安装 http.ftp server，Kali 作为中间人对两个 Ubuntu 靶机进行实验。

Kali 系统： root:hack

Ubuntu 系统：root:victim victim:victim

【实验过程】

在攻击机上利用 Scapy 伪造数据包，对另外两台靶机进行 ARP 欺骗，实现窃听靶机之间的会话，在实现 ARP 欺骗的基础上，进一步实现中间人攻击。利用 iptables 修改流量的转发端口，使用 mitmproxy 进行拦截请求，可以获取到请求的参数，从中提取出重要的信息，比如用户名和密码，也能够修改响应，改变返回的内容。mitmproxy 提供了 inline script 方法，能够使用脚本来操作流量，使得 mitmproxy 的功能更加强大，当然也可以尝试拦截 https 的流量，mitmproxy 也具有这样的能力。

【实验要求】

要求 1：使用 Scapy 实现窃听另外两台靶机的会话。例如窃听并提取另外两台靶机之间 FTP 或者 HTTP 会话的登录账号。

要求 2：对另外两台靶机进行中间人攻击，实现对会话进行篡改。例如对靶机间的 HTTP 会话进行注入，修改 HTTP 响应。

探索（不做要求）：在实验要求 2 的基础上，有兴趣的同学可以尝试对 HTTPS 会话进行窃听。

【实验相关材料】

1. 利用 Netwox 进行 ARP 攻击实验视频过程：视频地址 http://pan.baidu.com/s/1EDCp3
2. 中间人攻击框架 mitmproxy
   下载地址：https://github.com/mitmproxy/mitmproxy
   主页及文档: http://mitmproxy.org (需翻墙)
3. scapy 文档
   文档地址：http://www.secdev.org/projects/scapy/doc/
   中文版教程：https://github.com/Larryxi/Scapy_zh-cn