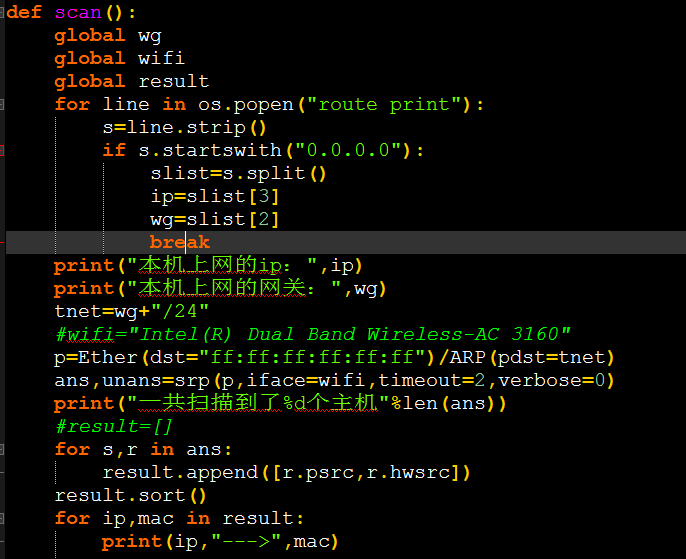
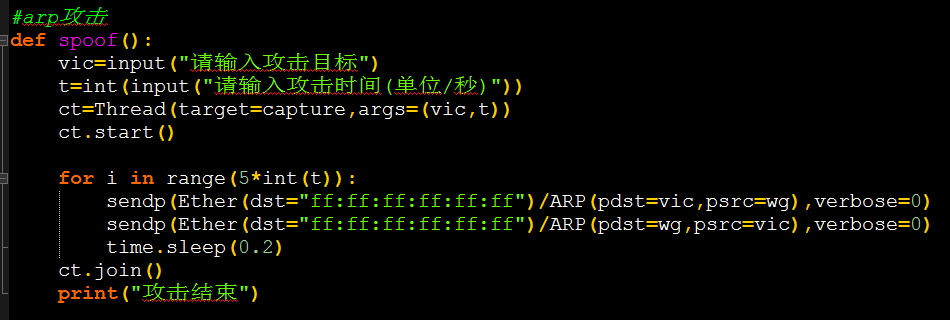
# 局域网攻击项目

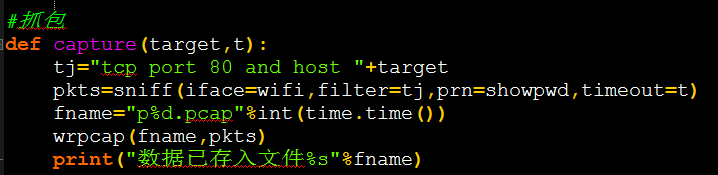
前提：攻击者与被攻击者位于同一个局域网内：

1.攻击者扫描局域网，选择攻击对象，进行Arp扫描



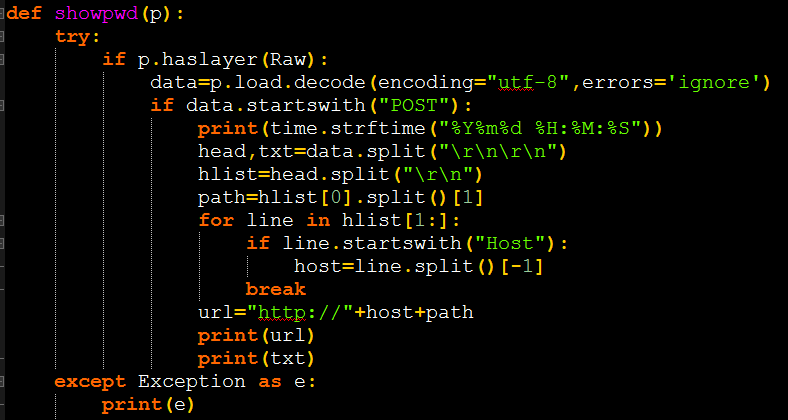
2.进行ARP劫持（从被攻击者看，攻击者是网关，从网关看，攻击者是被攻击者，从网关看，攻击者是被攻击者，开启路由转发功能）





3.抓包及分析

设定过滤条件，进行抓包，将抓包数据解析为刻度字符，获取敏感信息

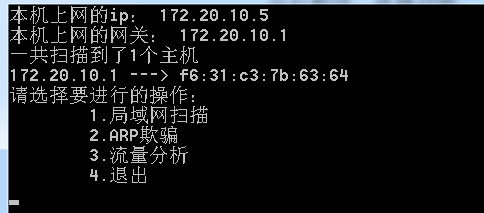


4.运行结果

运行程序，选择功能



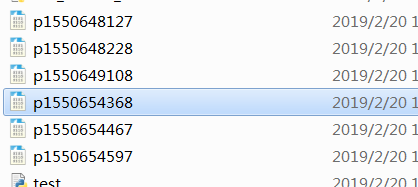
（1）局域网扫描扫 描出局域网内所有主机，

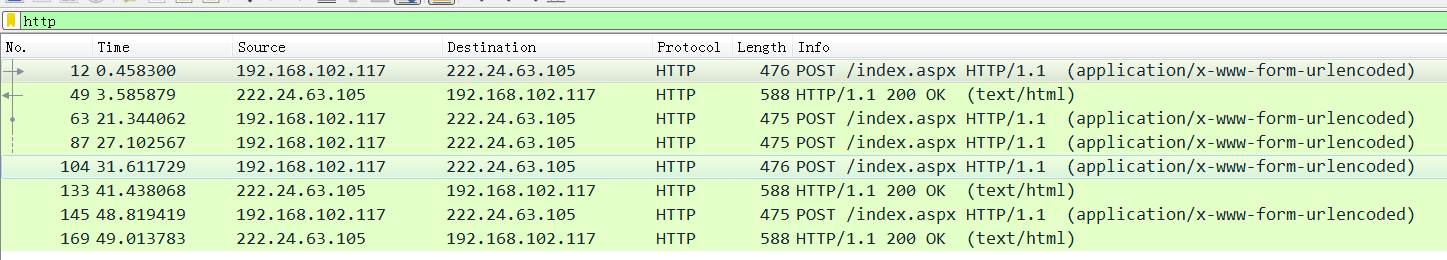


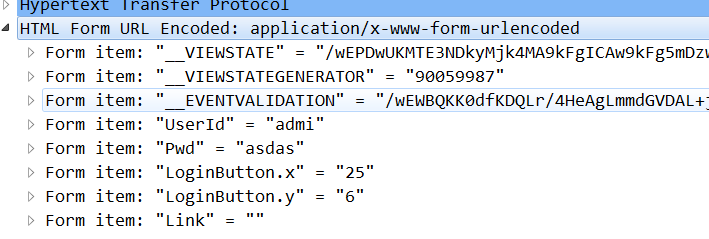
（2）arp欺骗，输入目标主机及攻击时间



（3）查看pcap文件







成功抓到用户名和密码