桂林电子科技大学 2022-2023 学年 第 1 学期

网络渗透测试实验报告

实验名称	**实验二 网络嗅探与身份认证**				
院　　系	**计算机与信息安全学院**	专业	**信息安全**		
学　　号	**2100300124**	姓名	**马驰**		
同 作 者	**马驰**				
实验日期	**2022** 年	**10** 月	**31** 日		

辅导教师意见：

成绩　　教师签名：

1. 实验目的和要求

2. 实验目的：
3. 1、通过使用 Wireshark 软件掌握 Sniffer（嗅探器）工具的使用方法，实现捕捉 HTTP 等协议的数据包，以理解 TCP/IP 协议中多种协议的数据结构、通过实验了解 HTTP 等协议明文传输的特性。
4. 2、研究交换环境下的网络嗅探实现及防范方法，研究并利用 ARP 协议的安全漏洞，通过 Arpspoof 实现 ARP 欺骗以捕获内网其他用户数据。
5. 3、能利用 BrupSuite 实现网站登录暴力破解获得登录密码。
6. 4、能实现 ZIP 密码破解，理解安全密码的概念和设置。
7. 系统环境：Kali Linux 2、Windows
8. 网络环境：交换网络结构
9. 实验工具：Arpspoof、WireShark、BurpSuite、fcrackzip（用于 zip 密码破解）。

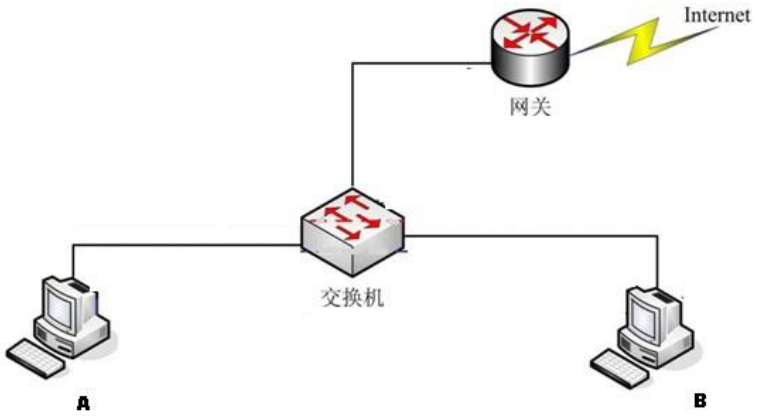
2. 实验步骤

网络嗅探部分：

网络嗅探：Wireshark 监听网络流量，抓包。

ARP 欺骗： ArpSpoof，实施 ARP 欺骗。

防范： 防范 arp 欺骗。

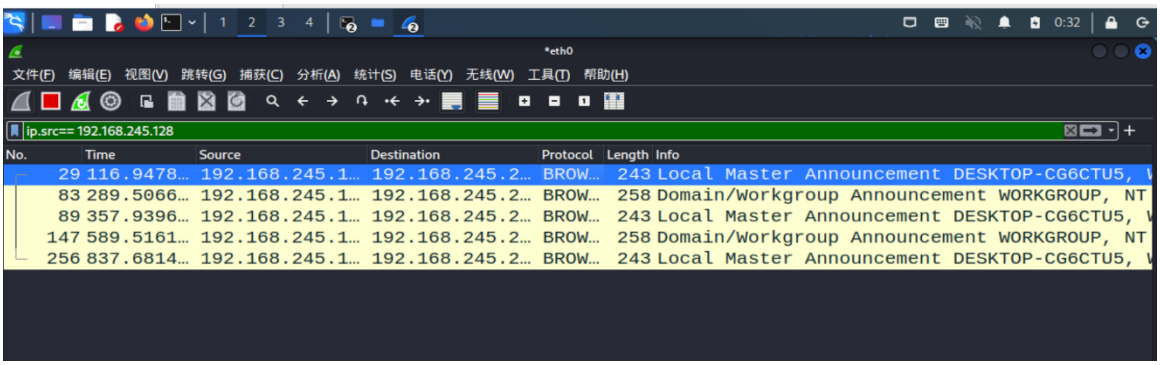


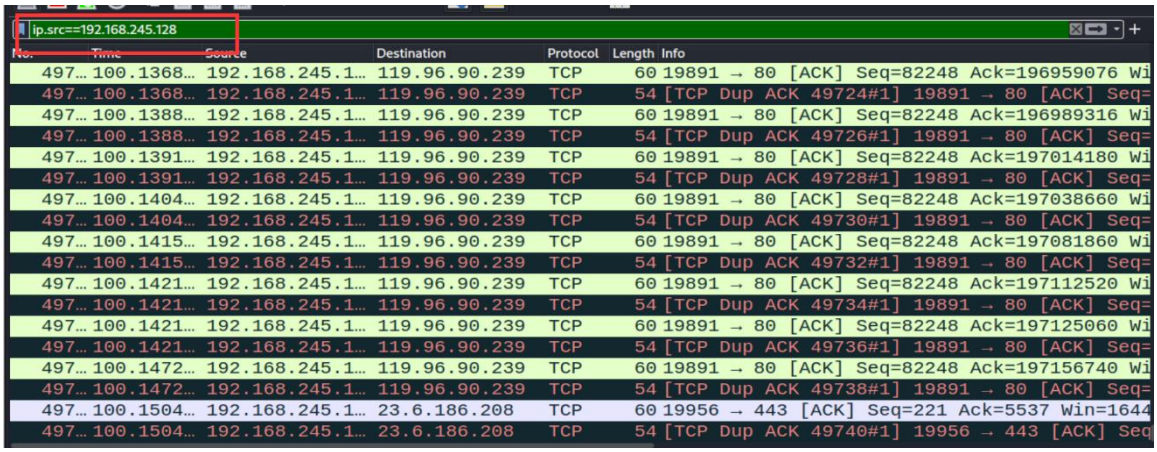
实验网络拓扑

1、A 主机上外网，B 运行 sinffer(Wireshark)选定只抓源为 A 的数据)。

1.1 写出以上过滤语句。

【ip.src==192.168.245.128】





1.2 在互联网上找到任意一个以明文方式传递用户帐号、密码的网站，B 是否能看到 A 和外网（该网站）的通信（A 刚输入的帐户和口令）？为什么？

B 不能看到 A 和外网的通信，A 的数据包会直接发送给网关，不经过 B，无法嗅探到。

2.1 为了捕获 A 到外网的数据，B 实施 ARP 欺骗攻击，B 将冒充该子网的什么实体？

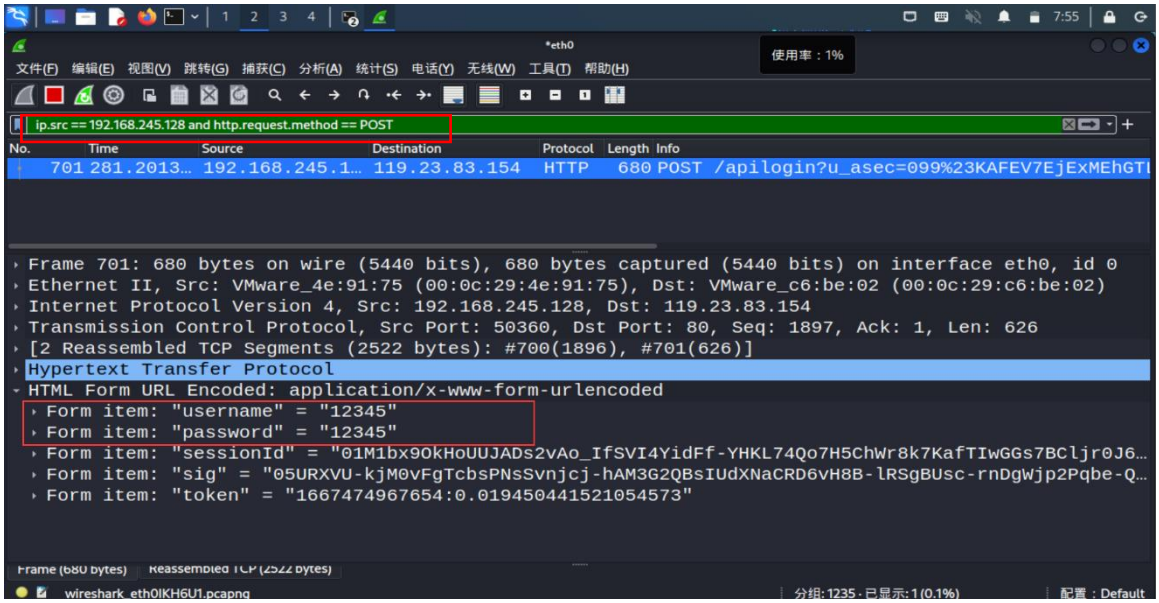
交换机

2.2 写出 arpspoof 命令格式。

arpspoof -i 【网卡】-t 【目标 ip】【目标网关】

含义：把自己伪装成目标主机的网关

2.3 B 是否能看到 A 和外网的通信（A 输入的帐户和口令）？截图 Wireshark 中显示的明文信息。

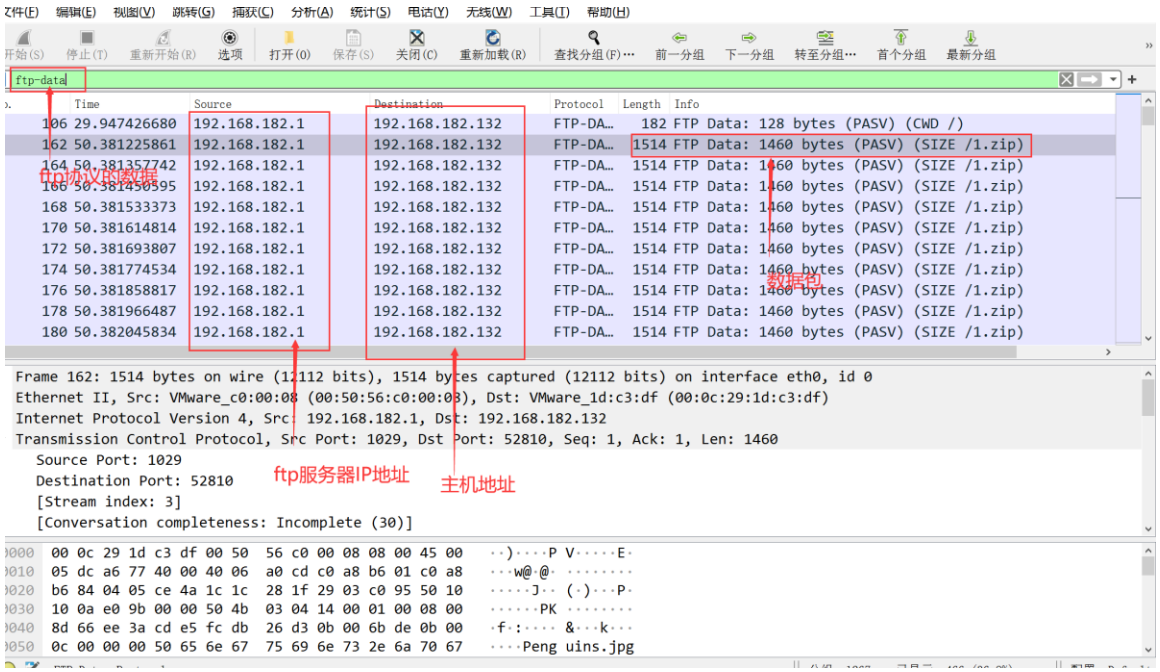


3. FTP 数据还原部分：利用 WireShark 打开实验实验数据 data.pcapng。

3.1 FTP 服务器的 IP 地址是多少？你是如何发现其为 FTP 服务器的？

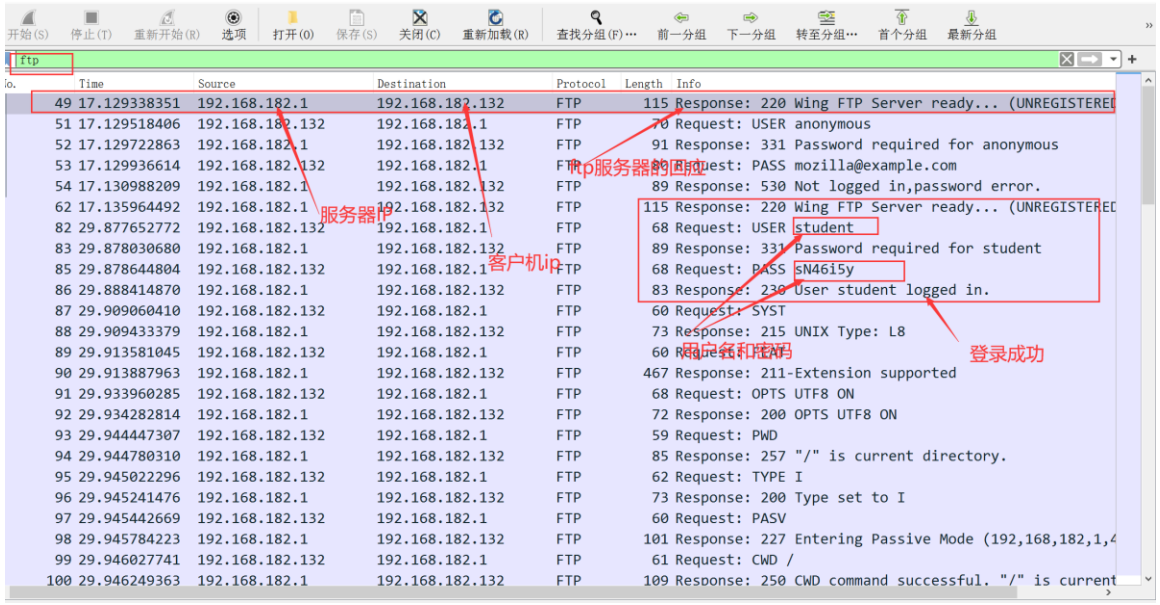
FTP 服务器（File Transfer Protocol Server）是在互联网上提供文件存储和访问服务的计算机，它们依照 FTP 协议提供服务。 FTP 是 File Transfer Protocol(文件传输协议)。顾名思义，就是专门

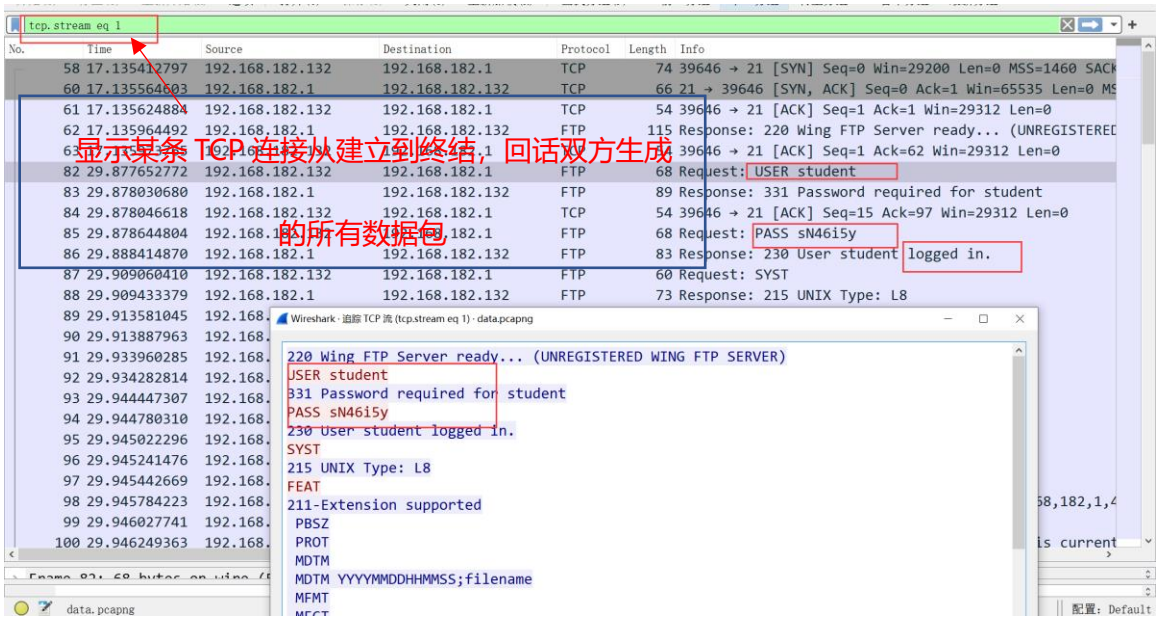
用来传输文件的协议。简单地说，支持 FTP 协议的服务器就是 FTP 服务器。



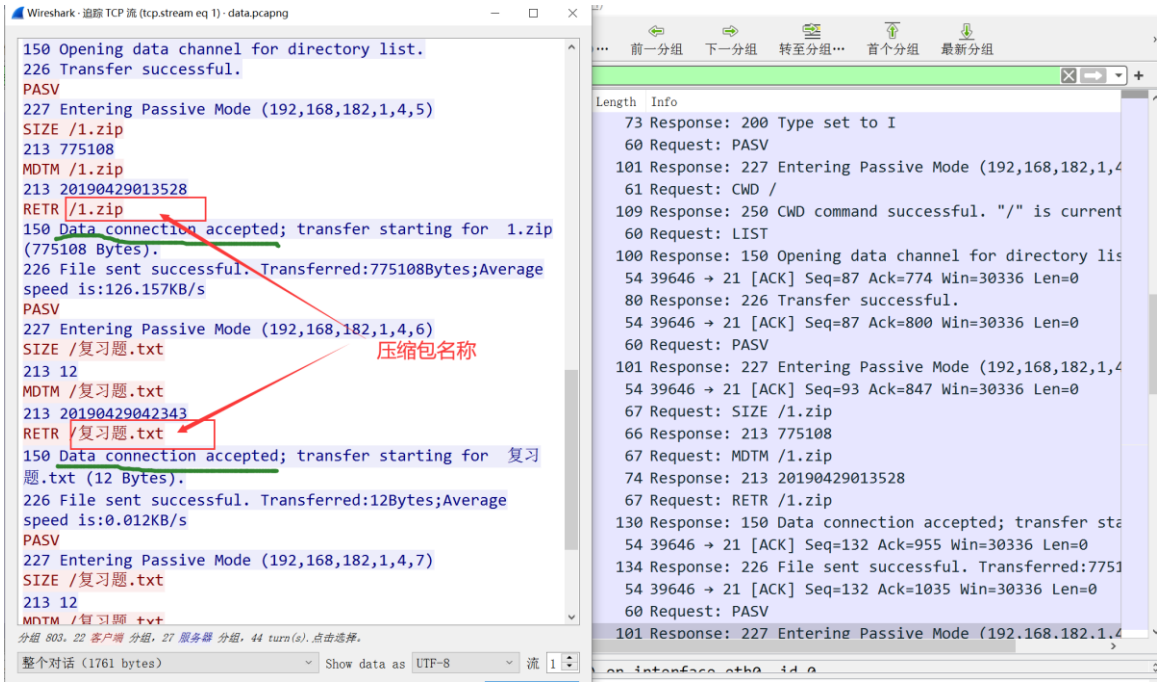
3.2 客户端登录 FTP 服务器的账号和密码分别是什么?

方法：**抓取客户端到 ftp 服务器的数据**

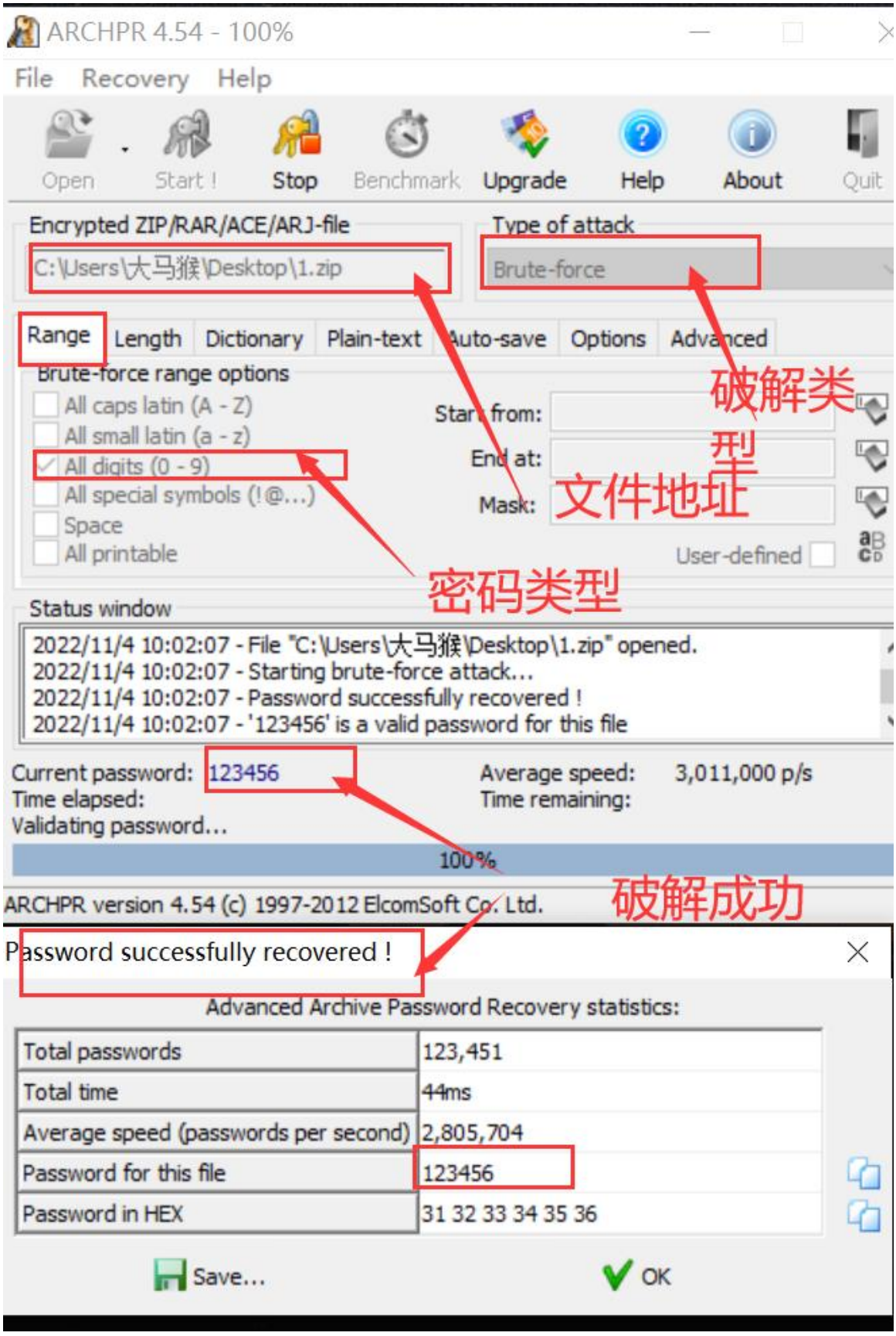


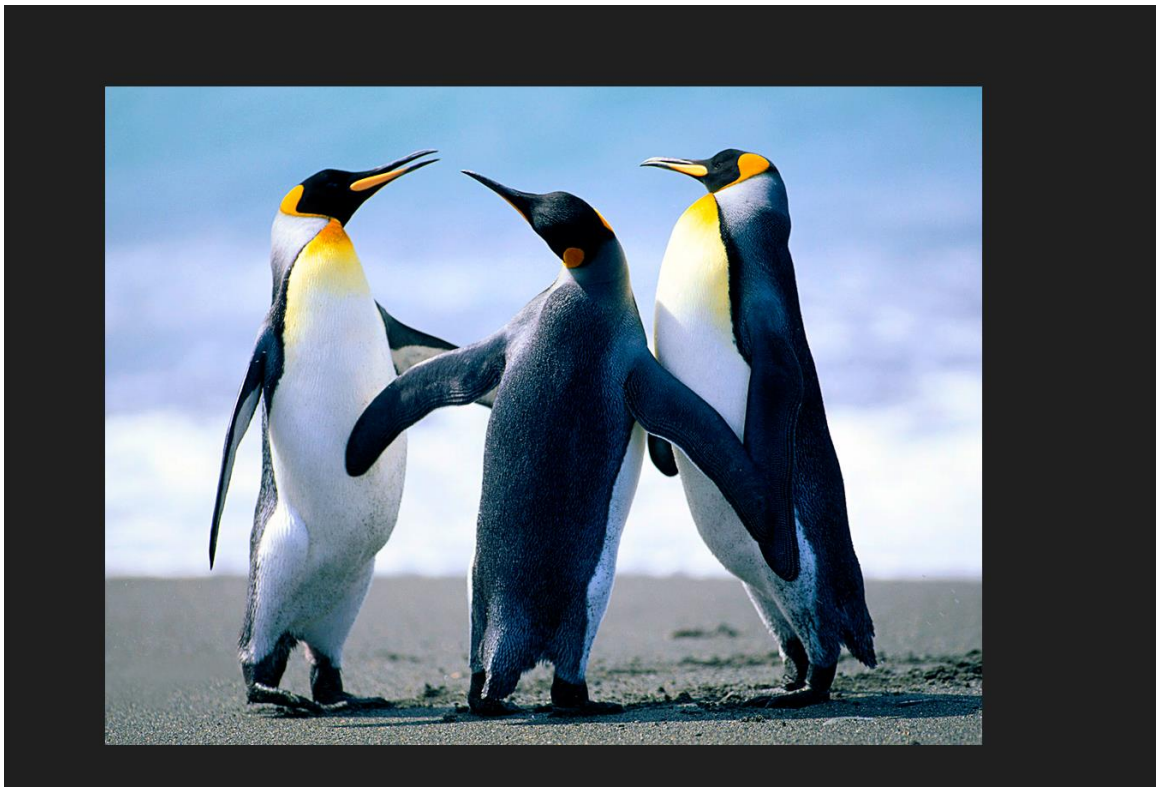


3.3 客户端从 FTP 下载或查看了 2 个文件，一个为 ZIP 文件，一个为 TXT 文件，文件名分别是什么？**提示：文件名有可能是中文。**



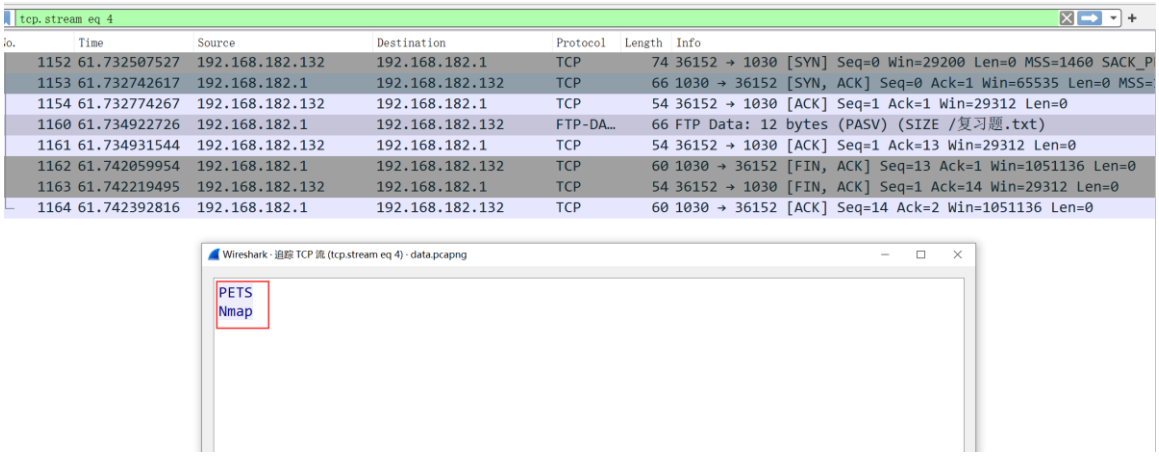
3.4 还原 ZIP 文件并打开（ZIP 有解压密码，试图破解，提示：密码全为数字，并为 6 位）。截图破解过程。


ARCHPR 4.54 - 100%
File Recovery Help
Open Start ! Stop Benchmark Upgrade Help About Quit
Encrypted ZIP/RAR/ACE/ARJ-file
C:\Users\大马猴\Desktop\1.zip
Type of attack
Brute-force
Range Length Dictionary Plain-text Auto-save Options Advanced
Brute-force range options
All caps latin (A - Z)
All small latin (a - z)
All digits (0 - 9)
All special symbols (!@...)
Space
All printable
Start from:
End at:
Mask:
User-defined
破解类型
文件地址
密码类型
Status window
2022/11/4 10:02:07 - File "C:\Users\大马猴\Desktop\1.zip" opened.
2022/11/4 10:02:07 - Starting brute-force attack...
2022/11/4 10:02:07 - Password successfully recovered !
2022/11/4 10:02:07 - '123456' is a valid password for this file
Current password: 123456
Time elapsed:
Validating password...
Average speed: 3,011,000 p/s
Time remaining:
100%
ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.
破解成功
Password successfully recovered !
Advanced Archive Password Recovery statistics:
Total passwords 123,451
Total time 44ms
Average speed (passwords per second) 2,805,704
Password for this file 123456
Password in HEX 31 32 33 34 35 36
Save...
OK



3.5 TXT 文件的内容是什么？

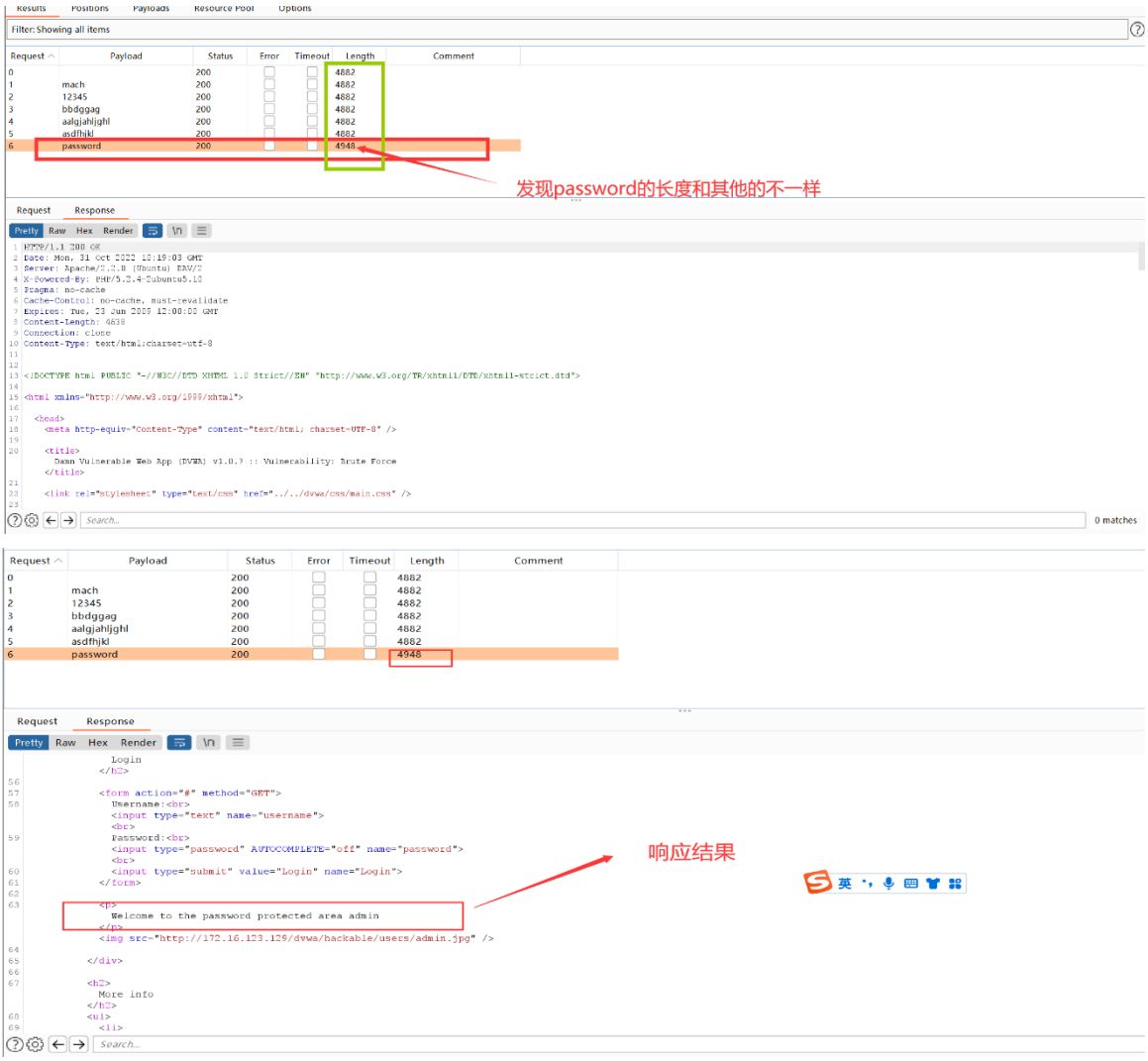
用 ftp-data 筛选出文件数据，找到 txt 文件数据，选择 tcp 流打开，



网站密码破解部分：

利用人们平时常用的词、句破译，如果说暴力破解是一个一个的尝试那么字典破译就是利用人们习惯用人名、地名或者常见的词语设置成密码的习惯进行破译。字典破译速度比暴力破译更快但是有时候密码设置中包含了没有字典库中的词句就无法破解出来了，因此有好的字典是关键。

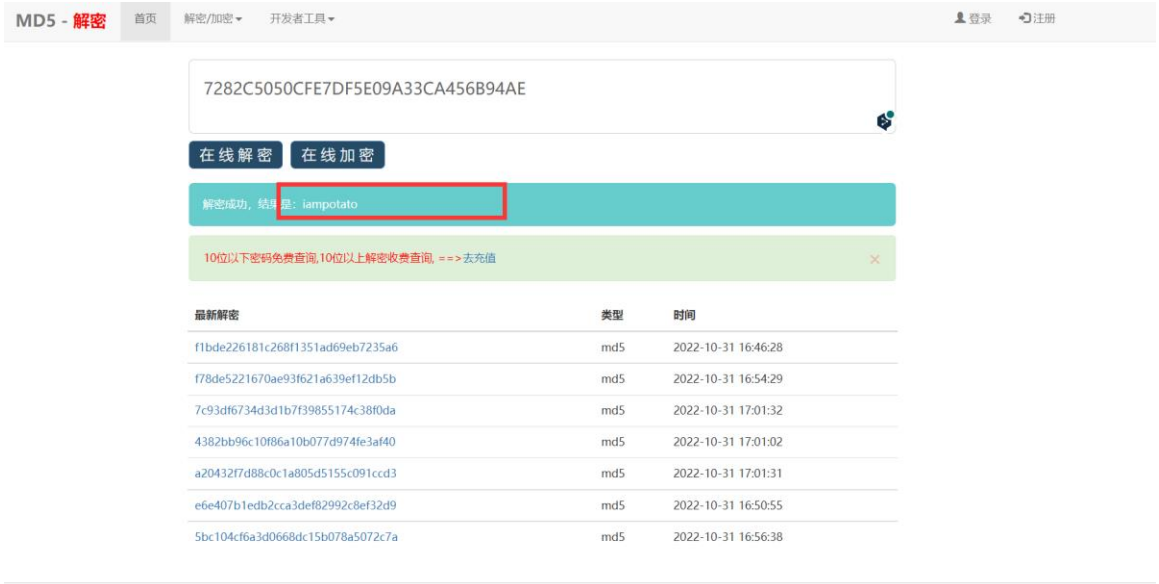
以*****为目标网站，构造字典（wordlist），其中包含你的正确密码，利用 burpsuite 进行字典攻击，实施字典攻击，你是如何判断某个密码为破解得到的正确密码，截图。



4、MD5 破解

SqlMap得到某数据库用户表信息，用户口令的MD5值为 7282C5050CFE7DF5E09A33CA456B94AE

那么，口令的明文是什么？（提示：MD5 值破解）



5、John the Ripper 的作用是什么？

John the Ripper 是一个快速的密码破解工具，用于在已知密文的情况下尝试破解出明文，支持目前大多数的加密算法，如 DES、MD4、MD5 等。它支持多种不同类型的系统架构，包括 Unix、Linux、Windows、DOS 模式、BeOS 和 OpenVMS，主要目的是破解不够牢固的 Unix/Linux 系统密码。除了在各种 Unix 系统上最常见的几种密码哈希类型之外，它还支持 Windows LM 散列，以及社区增强版本中的许多其他哈希和密码。它是一款开源软件。Kali 中自带 John。

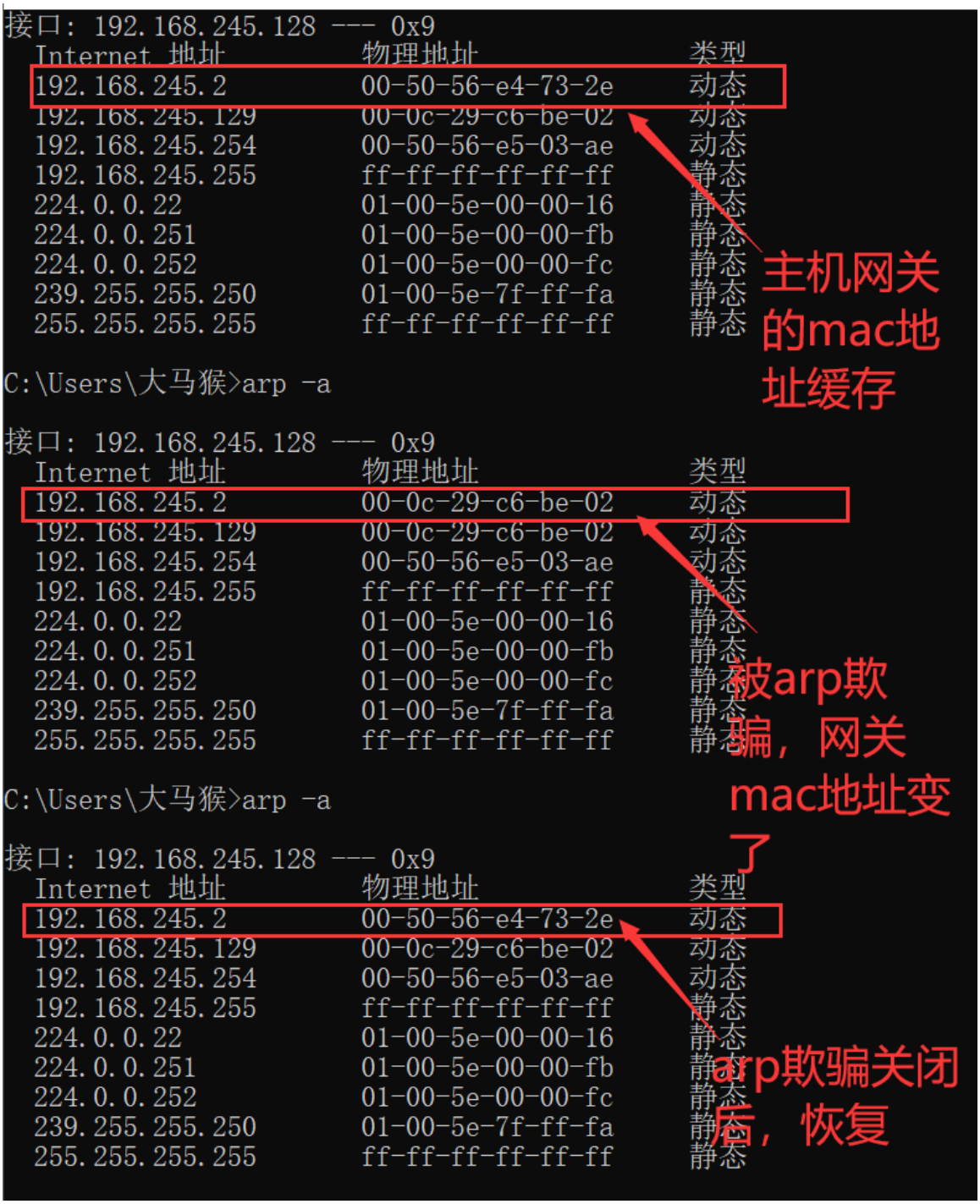
思考问题：

1、谈谈如何防止 ARP 攻击。

（1） 添加静态的 ARP 映射表，不让主机刷新设定好的映射表

（2） 停止使用 ARP，将 ARP 作为永久桃木保存在映射表中。

（3） 使用防火请连续监听网络



（4）

2、安全的密码（口令）应遵循的原则。

（1） 不要选择弱口令密码；

（2） 不要用一些容易被收集到的信息构成的密码，例如家人的生日

（3） 不要在所有的平台都使用一样的密码

（4） 使用中强口令密码，例如存在字母大小写，特殊字符等

（5） 根据安全级别的判断选择不同强度的密码

（6） 选择适合自己的密码长度，吻合自身的记忆力，不至于创建后就忘记。

3、谈谈字典攻击中字典的重要性。

（1）对一些弱口令进行快速的爆破

（2）在对目标进行信息收集之后，构建字典可以增加爆破成功的机率，快速拿到信息。

3. 实验小结

本次实验围绕 ftp 协议，arp 欺骗，密码的爆破展开，通过具体的操作，对 ftp 协议、kali 欺骗操作和密码爆破工具有了进一步的认识。对网络嗅探、数据还原、网站密码破解有了一定的了解。