Kali网络渗透实验一

原创

山野下 于 2020-11-02 22:07:32 发布

分类专栏： Kali网络渗透测试 文章标签： 信息安全 windows

文章目录

前言

通过信息的收集、一些安全工具的使用、搜索引擎的高效运用，完成网络渗透任务。

实验原理

网络扫描与网络侦察的目的
黑客在进行一次完整的攻击之前除了确定攻击目标之外，最主要的工作就是收集尽量多的关于攻击目标的信息。这些信息主要包括目标的操作系统类型及版本、目标提供哪些服务、各服务的类型、版本以及相关的社会信息。
攻击者搜集目标信息一般采用七个基本的步骤：
（1） 找到初始信息，比如一个IP地址或者一个域名；
（2） 找到网络地址范围，或者子网掩码；
（3） 找到活动机器；
（4） 找到开放端口和入口点；
（5） 弄清操作系统；
（6） 弄清每个端口运行的是哪种服务；
（7） 找到目标可能存在的漏洞。

环境搭建

本次实验使用的系统环境为Kali Linux 2、Metasploitnle 2（作为靶机）、Windows10

将在下面给出Metasploitable 2的环境搭建：
（转自：https://www.cnblogs.com/zhangb8042/articles/10623620.html）

先提取Metasploitable2镜像，再使用VM将这个镜像打开，等待靶机打开，然后输入metasploitble login和password的时候一定要注意，password是隐藏的，就是输入的时候不见，但是不要慌，只需要在上面和下面都输入msfadmin就可以进入啦~

实验工具

1.Google Hacking（或baidu）

Google Hacking 是利用谷歌搜索的强大，来在浩瀚的互联网中搜索到我们需要的信息。轻量级的搜索可以搜素出一些遗留后门，不想被发现的后台入口，中量级的搜索出一些用户信息泄露，源代码泄露，未授权访问等等，重量级的则可能是mdb文件下载，CMS 未被锁定install页面，网站配置密码，php远程文件包含漏洞等重要信息。

2.BASE64编码

BASE64是一种编码方式，通常用于把二进制数据编码为可写的字符形式的数据。编码后的数据是一个字符串，其中包含的字符为：A-Z、a-z、0-9、+、/共64个字符。（其实是65个字符，“=”是填充字符）。长度为3个字节(3*8*)*的数据经过Base64编码后就变为4个字节(*4*6)。如果数据的字节数不是3的倍数，则其位数就不是6的倍数，那么就不能精确地划分成6位的块。需在原数据后面添加1个或2个零值字节，使其字节数是3的倍数。字符串“Xue”经过Base64编码后变为“WHVl”。

3.Nmap

Nmap是一个网络侦察和安全扫描程序，系统管理者和个人可以使用这个软件扫描大型的网络，获取哪台主机正在运行以及提供什么服务等信息。Nmap支持很多扫描技术，例如：UDP、TCP connect()、TCP SYN(半开扫描)、ftp代理(bounce攻击)、反向标志、ICMP、FIN、ACK扫描、圣诞树(Xmas Tree)、SYN扫描和null扫描。Nmap还提供了一些高级的特征，例如：通过TCP/IP协议栈特征探测操作系统类型，秘密扫描，动态延时和重传计算，并行扫描，通过并行ping扫描探测关闭的主机，诱饵扫描，避开端口过滤检测，直接RPC扫描(无须端口映射)，碎片扫描，以及灵活的目标和端口设定。
Nmap运行通常会得到被扫描主机端口的列表。Nmap总会给出well known端口的服务名(如果可能)、端口号、状态和协议等信息。每个端口的状态有：open、filtered、unfiltered。open状态意味着目标主机能够在这个端口使用accept()系统调用接受连接。filtered状态表示：防火墙、包过滤和其它的网络安全软件掩盖了这个端口，禁止Nmap探测其是否打开。unfiltered表示：这个端口关闭，并且没有防火墙/包过滤软件来隔离nmap的探测企图。通常情况下，端口的状态基本都是unfiltered状态，只有在大多数被扫描的端口处于filtered状态下，才会显示处于unfiltered状态的端口。
根据使用的功能选项，Nmap也可以报告远程主机的下列特征：使用的操作系统、TCP序列、运行绑定到每个端口上的应用程序的用户名、DNS名、主机地址是否是欺骗地址、以及其它一些东西。

4.WinHex

> WinHex 是一款以通用的 16 进制编辑器为核心，专门用来对付计算机取证、数据恢复、低级数据处理、以及 IT 安全性、各种日常紧急情况的高级工具： 用来检查和修复各种文件、恢复删除文件、硬盘损坏、数码相机卡损坏造成的数据丢失等。

实验步骤

1.用搜索引擎Google或百度搜索麻省理工学院网站中文件名包含“network security”的pdf文档，截图搜索得到的页面。

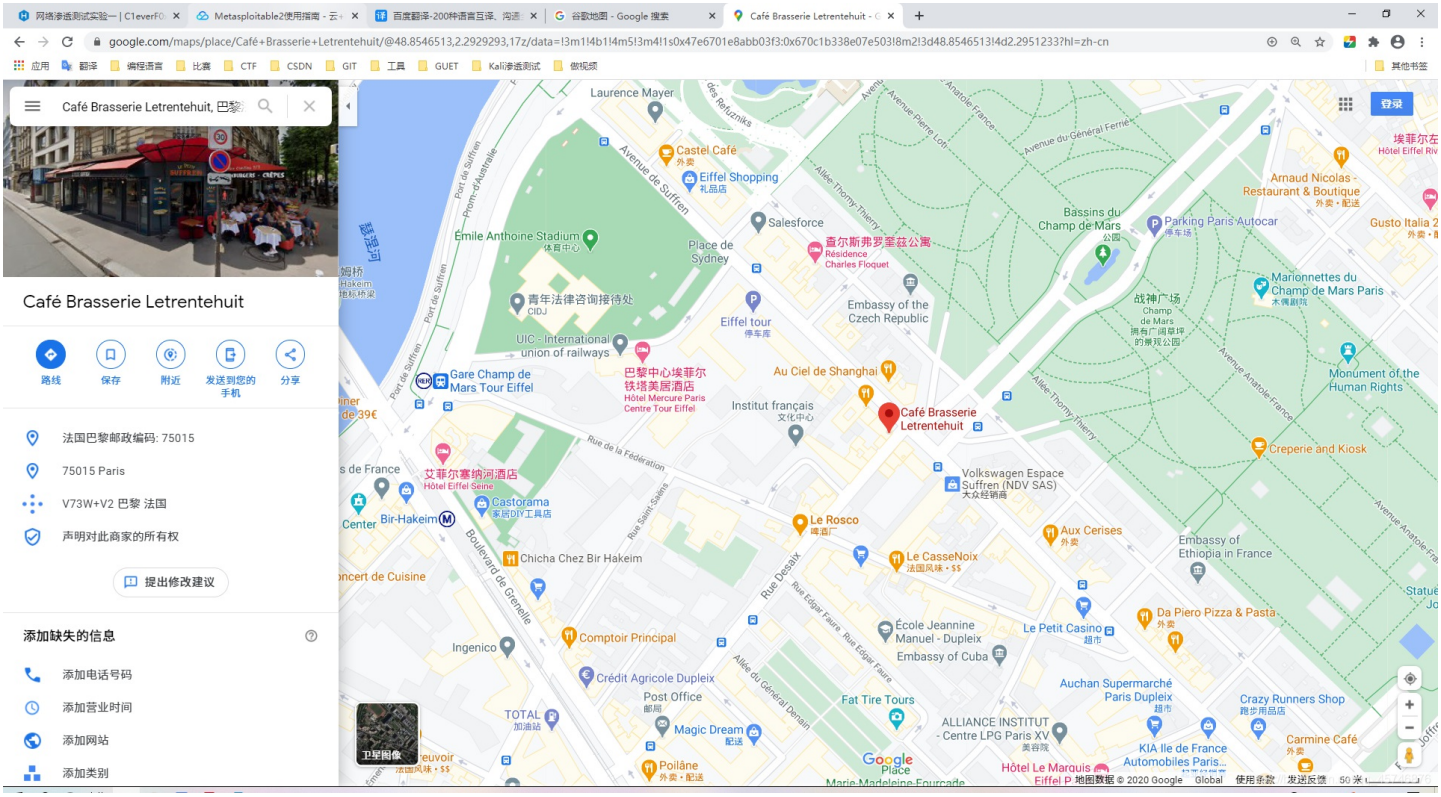
先百度/Google到麻省理工学院的官方网站 https://www.mit.edu/，再使用搜索引擎的常用语法，限制搜索结果就可以啦~

> google基本语法
> Index of/　　使用它可以直接进入网站首页下的所有文件和文件夹中。
> intext:　　将返回所有在网页正文部分包含关键词的网页。
> intitle:　　将返回所有网页标题中包含关键词的网页。
> cache:　　搜索google里关于某些内容的缓存。
> define:　　搜索某个词语的定义。
> filetype:　　搜索指定的文件类型，如：.bak，.mdb，.inc等。
> info:　　查找指定站点的一些基本信息。
> inurl:　　搜索我们指定的字符是否存在于URL中。
> Link:link :thief.one可以返回所有和thief.one做了链接的URL。
> site:site:thief.one将返回所有和这个站有关的URL。
> +　　把google可能忽略的字列如查询范围。
> -　　把某个字忽略，例子：新加 -坡。
> ~　　同意词。
> .　　单一的通配符。
> *　　通配符，可代表多个字母。
> “”　　精确查询。

2、照片中的女生在哪里旅行？截图搜索到的地址信息。

图片:

看题目就知道是一道社工题啦，只不过这张照片不是原图，无法通过照片经纬度来找到这家店，那么只能从图中寻找信息了，看到上面的一串英文，还是很容易看出来是一家咖啡店的，那就打开给谷歌地图，开整，就可以找到这家店啦。



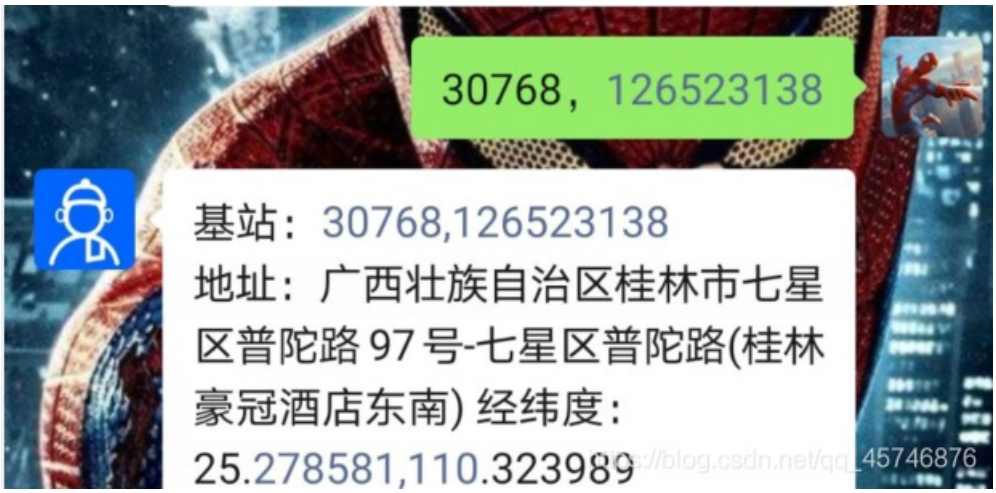
3、手机位置定位。通过LAC（Location Area Code，位置区域码）和CID（Cell Identity，基站编号，是个16位的数据（范围是0到65535）可以查询手机接入的基站的位置，从而初步确定手机用户的位置。

> 获取自己手机的LAC和CID：
> Android 获取方法：Android： 拨号*##4636##*进入手机信息工程模式后查看
> *iphone获取方法：iPhone：拨号*3001#12345#*进入FieldTest
> Serving Cell info–>LAC=Tracking Area Code -->cellid = Cell identity
> 若不能获取，用右图信息。
> 截图你查询到的位置信息。

刚开始是想使用自己手机的LAC和CID的，但是发现自己的华为手机拨号进去的工程模式好像不太一样：
华为手机进入工程模式：（拨号：*#*#2846579#*#*，语法问题，请忽视其中的空格）

所以只能只用文档上面的截图啦：

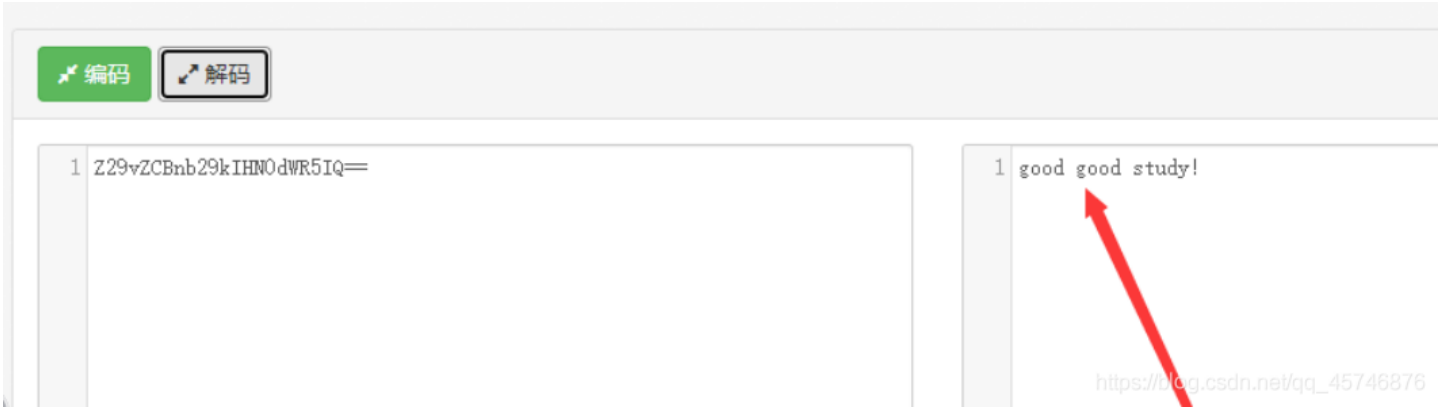
使用微信公众号查找一波：



补充一下自己的手机无法通过拨号获取LAC和CID的原因：是因为华为EMUI10.1版本没有信息工程模式，所以拨号进不去嗷

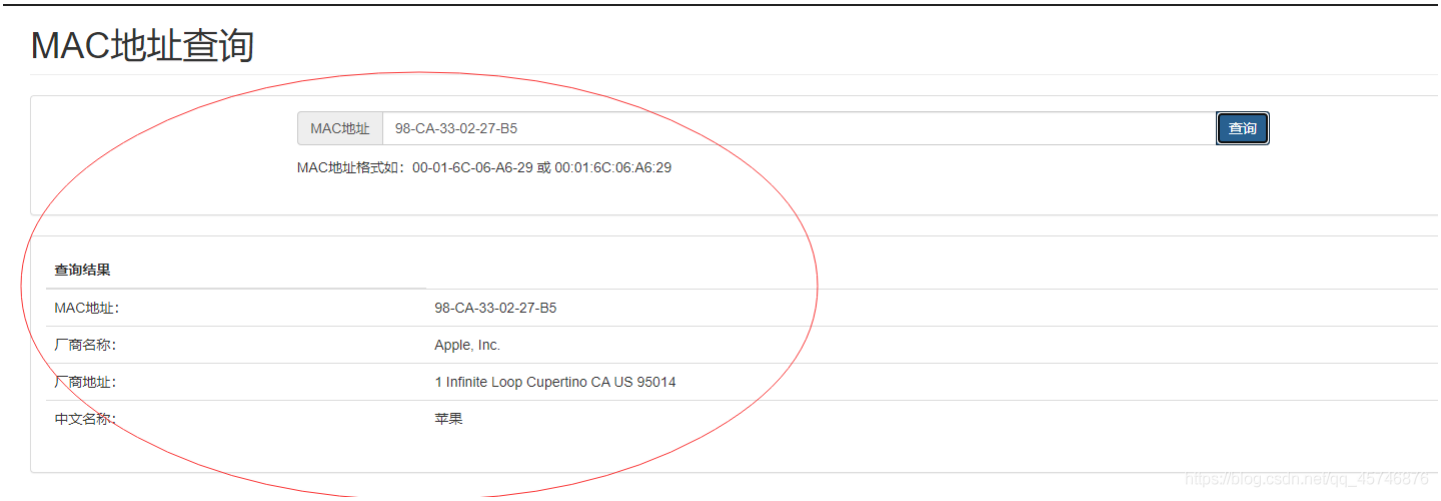
4.编码解码：将Z29vZCBnb29klHN0dWR5lQ==解码。截图。

直接使用base64在线解码工具进行解码就好啦：



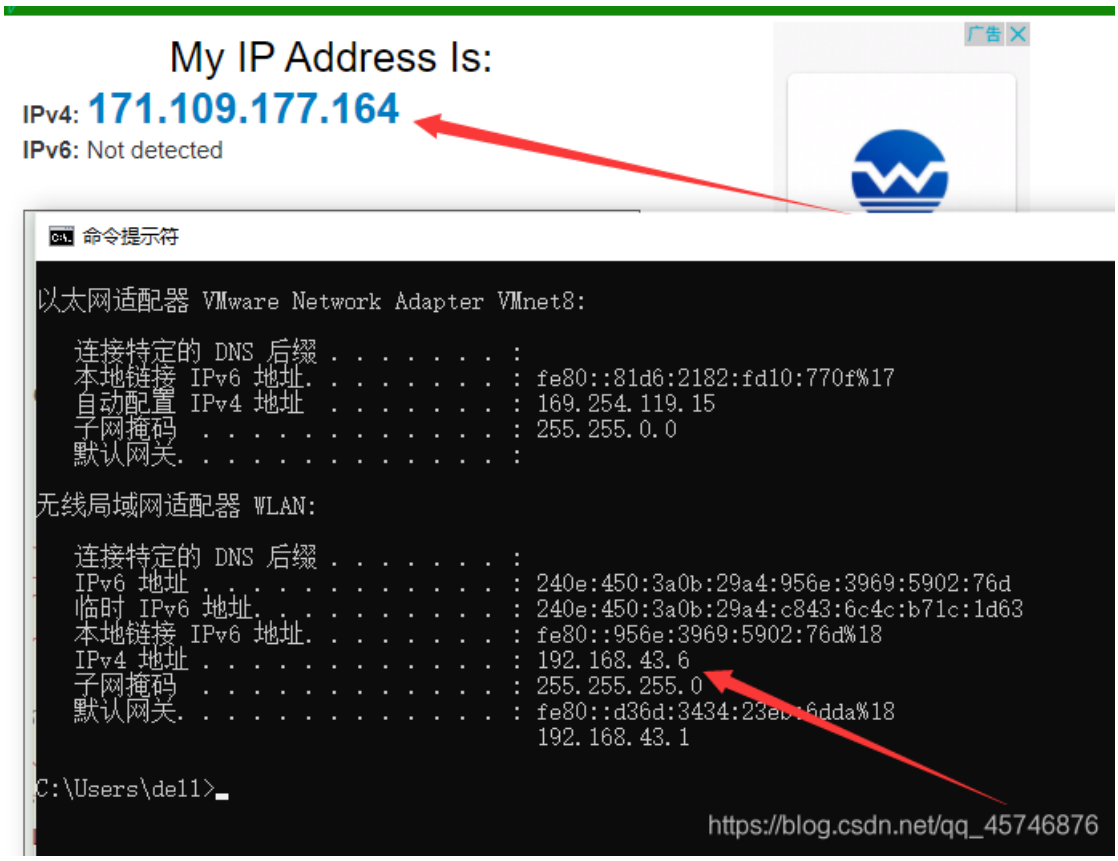
5.地址信息

5.1内网中捕获到一个以太帧，源MAC地址为：98-CA-33-02-27-B5；目的IP地址为：202.193.64.34，回答问题：该用户使用的什么品牌的设备，访问的是什么网站？并附截图。



估计是姚总的苹果访问桂电个官网了吧，嘿嘿~

5.2 访问https://whatismyipaddress.com得到MyIP信息，利用ipconfig(Windows)或ifconfig(Linux)查看本机IP地址，两者值相同吗？如果不相同的话，说明原因。

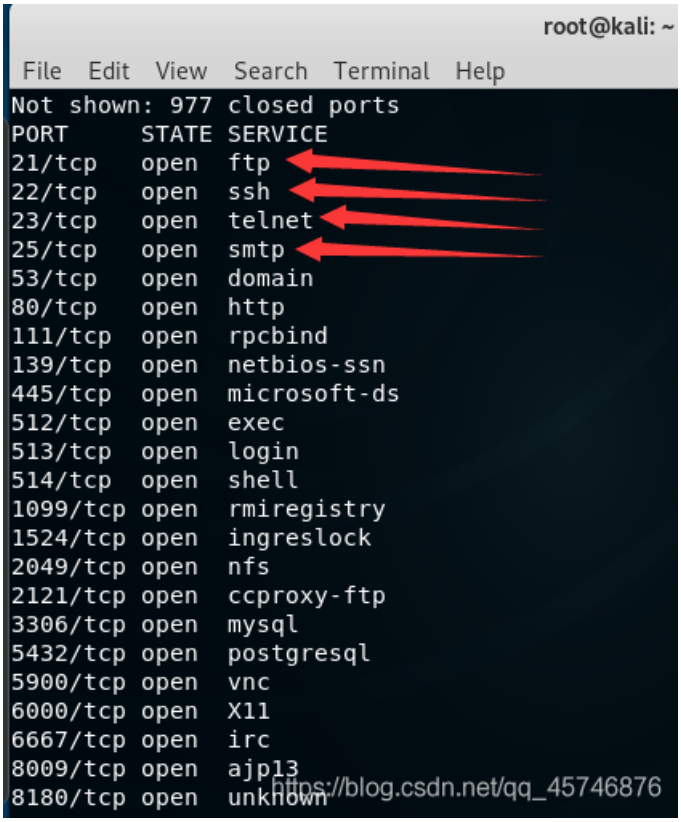


> 还是不一样的，在咨询了大佬结合姚总之前所讲，两个IP不一样的原因是：在网站上查询到的是公网IP，而ipconfig获取到的是内网IP

6.NMAP使用

6.1利用NMAP扫描Metasploitable2（需下载虚拟机镜像）的端口开放情况。并附截图。说明其中

四个端口的提供的服务，查阅资料，简要说明该服务的功能。



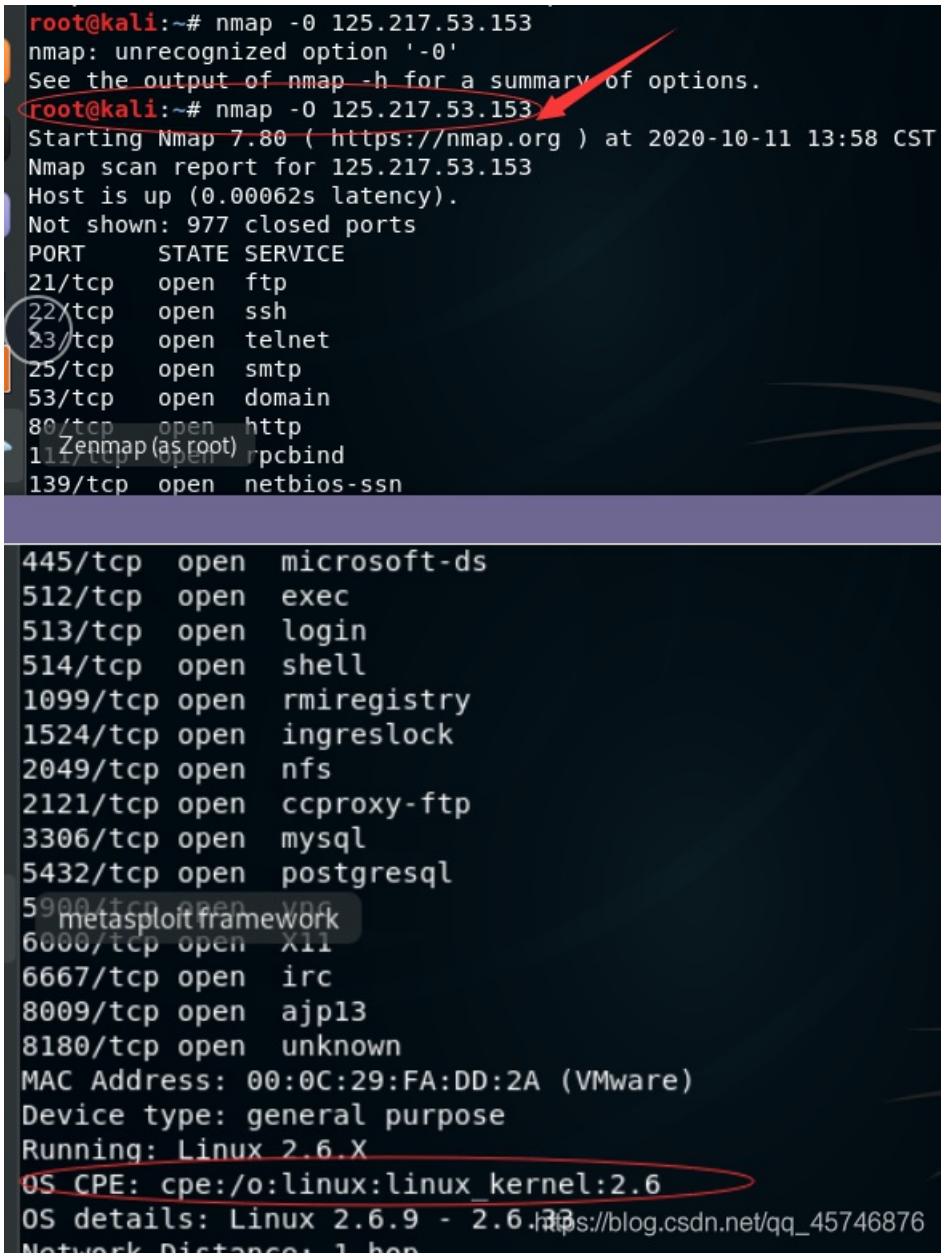
> 21/tcp:21端口主要用于FTP（File Transfer Protocol，文件传输协议）服务，FTP服务主要是为了在两台计算机之间实现文件的上传与下载，一台计算机作为FTP客户端，另一台计算机作为FTP服务器，可以采用匿名（anonymous）登录和授权用户名与密码登录两种方式登录FTP服务器。

> 22/tcp:安全外bai壳（duSSH）用来加密网管会话，该加zhi密基于RSA，基于TCP端口号dao22

> 23/tcp:23端口是telnet的端口。Telnet协议是TCP/IP协议族中的一员，是Internet远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的电脑上使用telnet程序，用它连接到服务器。终端使用者可以在telnet程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样。可以在本地就能控制服务器。要开始一个telnet会话，必须输入用户名和密码来登录服务器。Telnet是常用的远程控制Web服务器的方法。

> 25/tcp:25端口为SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）服务器所开放，主要用于发送邮件。

6.2利用NMAP扫描Metasploitable2的操作系统类型，并附截图。



6.3利用NMAP穷举 Metasploitable2上dvwa的登录账号和密码。

利用kali自带的nmap对dvwa的密码进行暴力破解，构造破解脚本：

```
nmap -p 80 -script=http-form-brute -script-args=http-form-brute.path=/dvwa/login.php 125.217.53.153
```

但是下图还是翻车了，推测原因可能是安装了VMtwareools之后没有重启，重启可以解决99%的问题嘛，所以在重启之后就成功啦~

```
root@kali:~# nmap -p 80 -script=http-form-brute-script-args=http-form-brute.path
=/dvwa/login.php 125.217.53.153
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-02 21:48 CST
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:818: 'http-form-brute-script-args=http-form-
brute.path=/dvwa/login.php' did not match a category, filename, or directory
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:818: in local 'get_chosen_scripts'
        /usr/bin/../share/nmap/nse_main.lua:1310: in main chunk
        [C]: in ?

QUITTING!
root@kali:~#
```

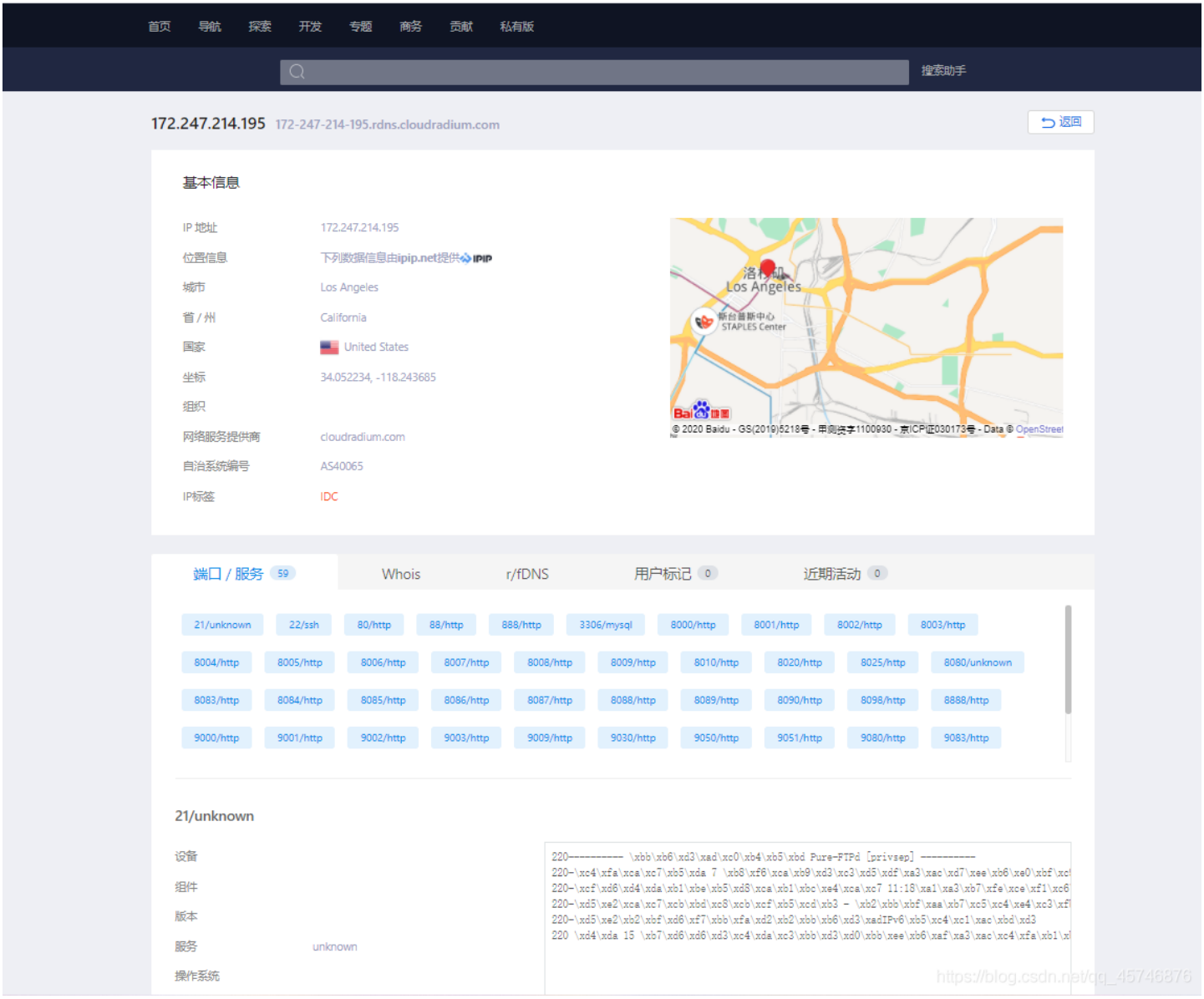

成功破解：

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Stats: 0:02:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 33.33% done; ETC: 22:04 (0:04:58 remaining)

root@kali:~# nmap -p 80 -script=http-form-brute -script-args=http-form-brute.path=/dvwa/login.php 125.217.5
3.153
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-02 21:59 CST
NSE: [http-form-brute] usernames: Time limit 10m00s exceeded.
NSE: [http-form-brute] usernames: Time limit 10m00s exceeded.
NSE: [http-form-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 125.217.53.153
Host is up (0.00030s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-form-brute:
|   Accounts:
|     admin:password - Valid credentials
|_  Statistics: Performed 24898 guesses in 600 seconds, average tps: 41.1
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 599.95 seconds
root@kali:~#
```


6.4 查阅资料，永恒之蓝-WannaCry蠕虫利用漏洞的相关信息。

> 永恒之蓝（Eternal Blue）爆发于2017年4月14日晚，是一种利用Windows系统的SMB协议漏洞来获取系统的最高权限，以此来控制被入侵的计算机。甚至于2017年5月12日， 不法分子通过改造“永恒之蓝”制作了wannacry勒索病毒，使全世界大范围内遭受了该勒索病毒，甚至波及到学校、大型企业、政府等机构，只能通过支付高额的赎金才能恢复出文件。不过在该病毒出来不久就被微软通过打补丁修复。

7.利用ZoomEye搜索一个西门子公司工控设备，并描述其可能存在的安全问题。

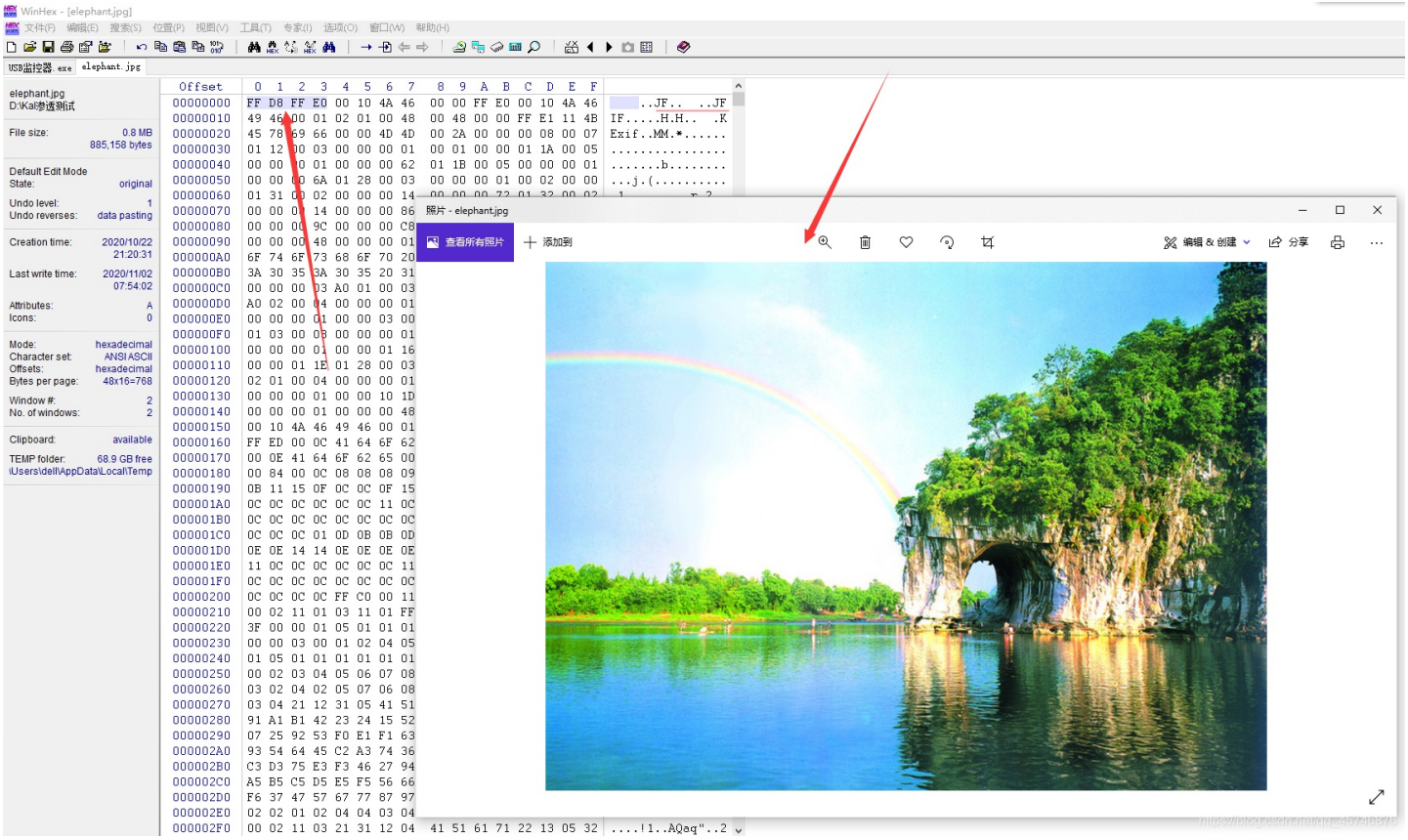


存在的问题：该设备开启的http服务和ssh服务都有可能被攻击。

8.Winhex简单数据恢复与取证

8.1 elephant.jpg不能打开了，利用WinHex修复，说明修复过程。

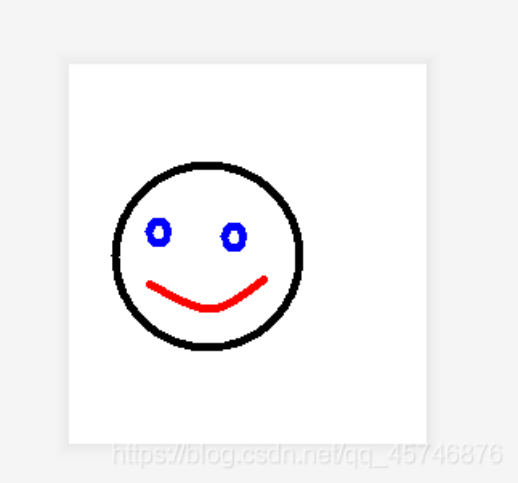
一开始打开elephant.jpg是一张空白图片，用winhex打开elephant.jpg后，发现这张照片没有jps文件的文件头(左边第一个箭头所指处)，加上文件头之后保存就可以看到美丽的象鼻山啦~



常用文件头：
JPEG (jpg)，文件头：FFD8FFE1
PNG (png)，文件头：89504E47 (0D0A1A0A)
GIF (gif)，文件头：47494638
ZIP Archive (zip)，文件头：504B0304
RAR Archive (rar)，文件头：52617221
XML (xml)，文件头：3C3F786D6C
MPEG (mpg)，文件头：000001BA
MPEG (mpg)，文件头：000001B3
AVI (avi)，文件头：41564920

8.2 笑脸背后的阴霾：图片smile有什么隐藏信息。

首先将文件打开，可以看到这张照片也没有什么可用信息，再查看文件详细信息后也没有啥收获，那就丢到winhex里面吧，终于在其尾部找到了隐藏信息，嘿嘿

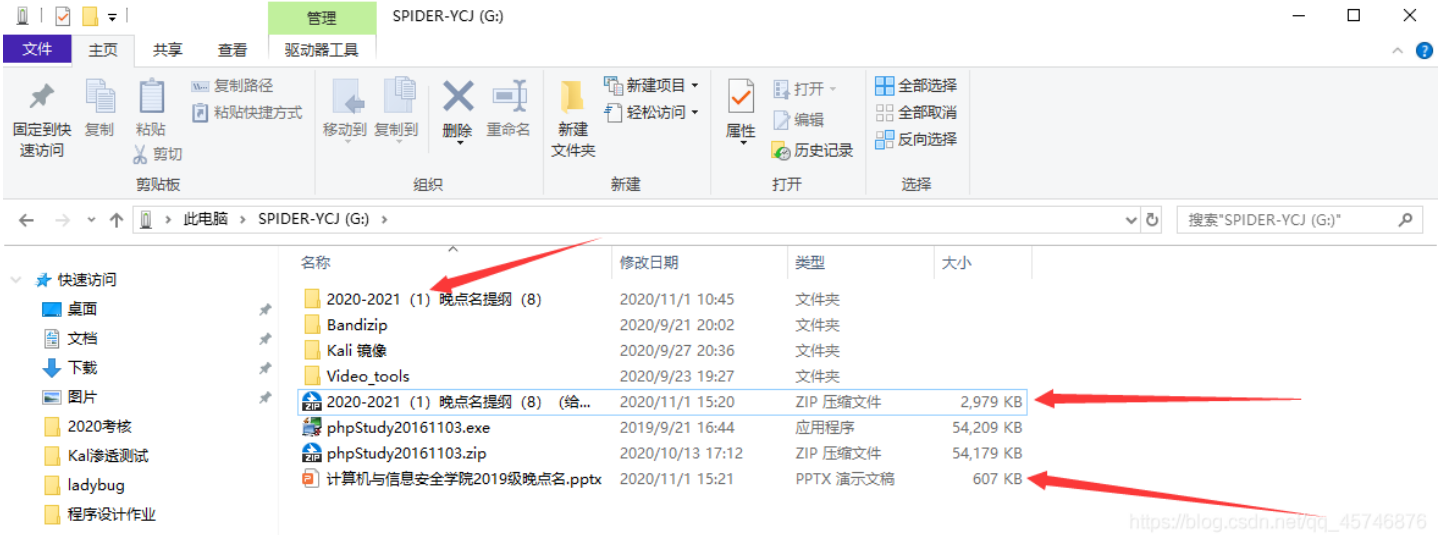



```
00027042  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00027051  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00027060  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
0002706F  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
0002707E  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
0002708D  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
0002709C  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000270AB  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000270BA  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000270C9  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000270D8  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000270E7  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000270F6  74 6F 6D 20 69 73 20 74  68 65 20 6B 69 6C 6C  tom is the kill
00027105  65 72 2E 1A                                    er..
```

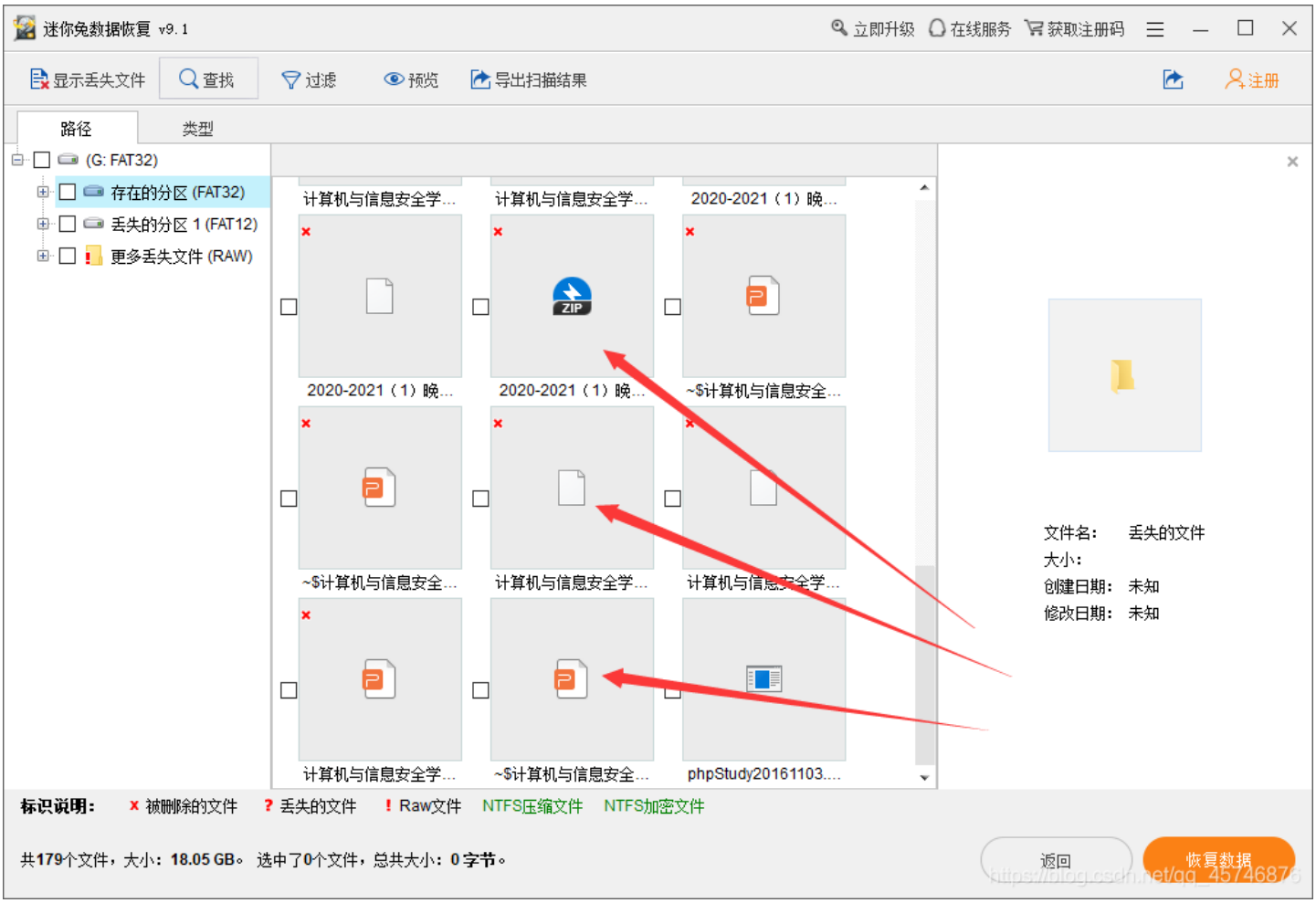

8.3 尝试使用数据恢复软件恢复你的U盘中曾经删除的文件。

根据姚总所说，U盘中有文件被删除，其中的数据域是不会改变的（每次删除和添加都修改的话代价太大），所以我们是可以将U盘中被删除的文件恢复的。既然如此，那就测试一波，冲冲冲！

首先拿出自己的U盘（没敢拿舍友的hhh），删除其中的一些文件：



然后打开一个数据恢复软件（本次实验中使用的是 迷你兔数据恢复），开始扫描U盘，然后就可以看到被咱们删除的文件啦：



点击之后就可以完成文件的恢复啦~

9.实验小结

本次实验的大多数内容都是认证性的，但是即便如此自己还是踩到了一些坑，但是也学会了一些之前不知道的，越菜就越不能松懈呀。安全之路，道阻且长，愿各位也能通过自己不断的学习，取得自己想要的进步，做一名光荣的白帽子~