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	**实验一 网络扫描与网络侦察**						
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	**24**	日	

辅导教师意见：

成绩　　教师签名：

1. 实验目的和要求

理解网络扫描、网络侦察的作用；通过搭建网络渗透测试平台，了解并熟悉常用搜索引擎、扫描工具的应用，通过信息收集为下一步渗透工作打下基础。

系统环境：Kali Linux 2、Windows

网络环境：交换网络结构

实验工具： Metasploitable2（需自行下载虚拟机镜像）；Nmap（Kali）；WinHex、数据恢复软件等。

实验原理：

1、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；

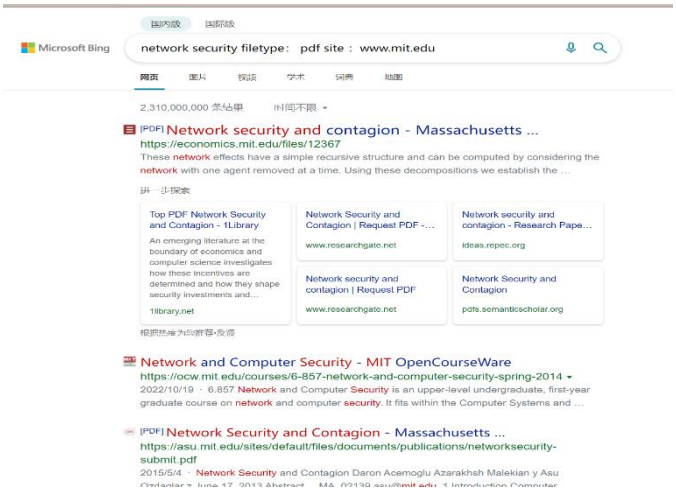
（5） 弄清操作系统；

（6） 弄清每个端口运行的是哪种服务；

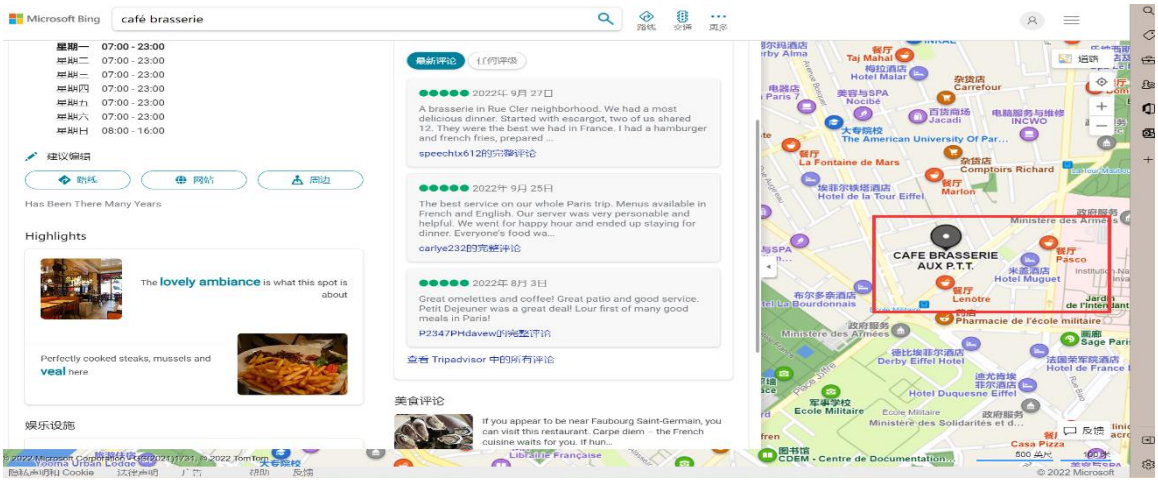
（7） 找到目标可能存在的漏洞。

2. 实验步骤

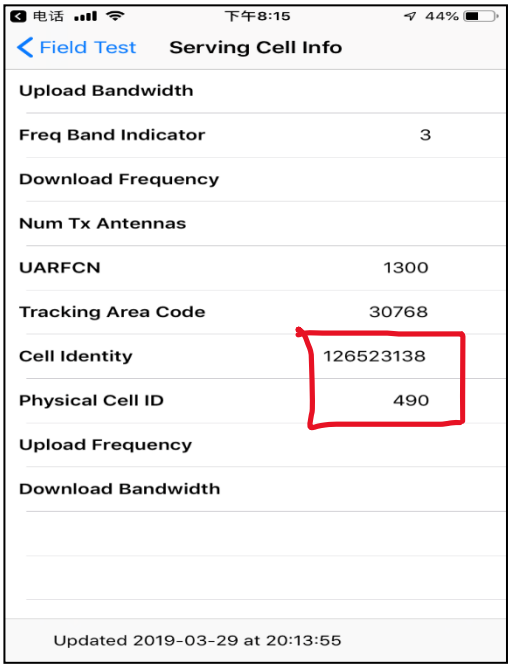
（1） 用搜索引擎 Google 或百度搜索麻省理工学院网站中文件名包含“network security”的 pdf 文档，截图搜索得到的页面。



2、照片中的女生在哪里旅行？截图搜索到的地址信息。



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。

4、编码解码

将 Z29vZCBnb29kIHN0dWR5IQ==解码。截图

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。

请输入IP或网站域名： 202.193.64.34 查询

IP 地址:	202.193.64.34
IP Long:	3401662498
归属地(纯真数据):	广西桂林市 桂林电子科技大学
归属地(ipip):	中国 广西 桂林 -
归属地(淘宝数据):	
归属地(IP2REGION):	中国 广西 桂林市 教育网
归属地(GeoLite2):	China -

MAC地址查询

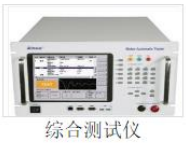
MAC地址 98:CA:33:02:27:B5 查询


大学生实习网


下载用友


日程管理系统


学生兼职网

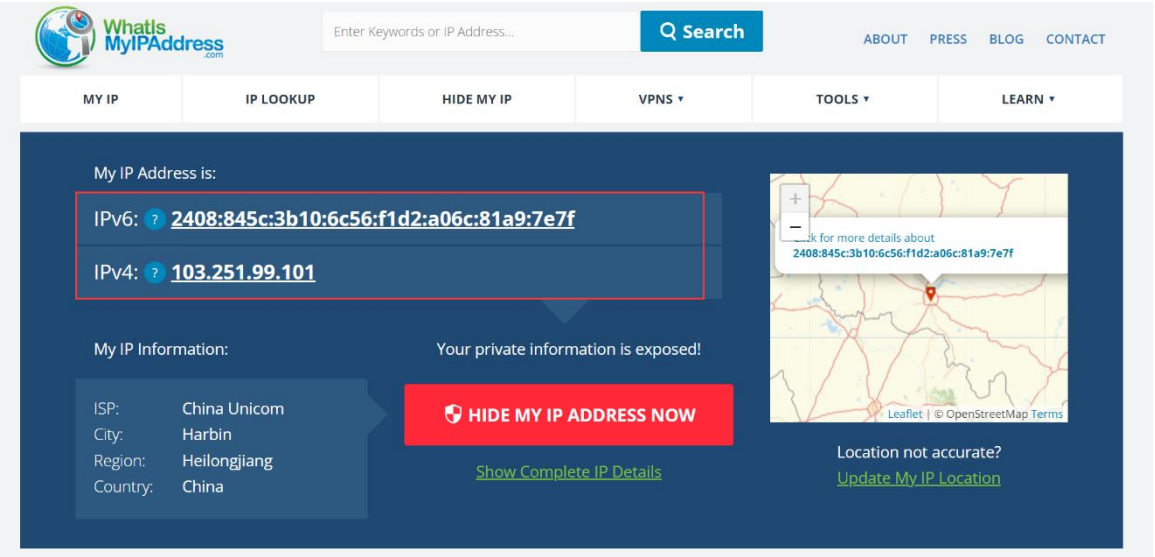

综合测试仪


mt4软件下载

MAC地址	98:CA:33:02:27:B5
组织名称	Apple, Inc.（苹果公司）
国家/地区	US
地址	1 Infinite Loop Cupertino CA 95014

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。

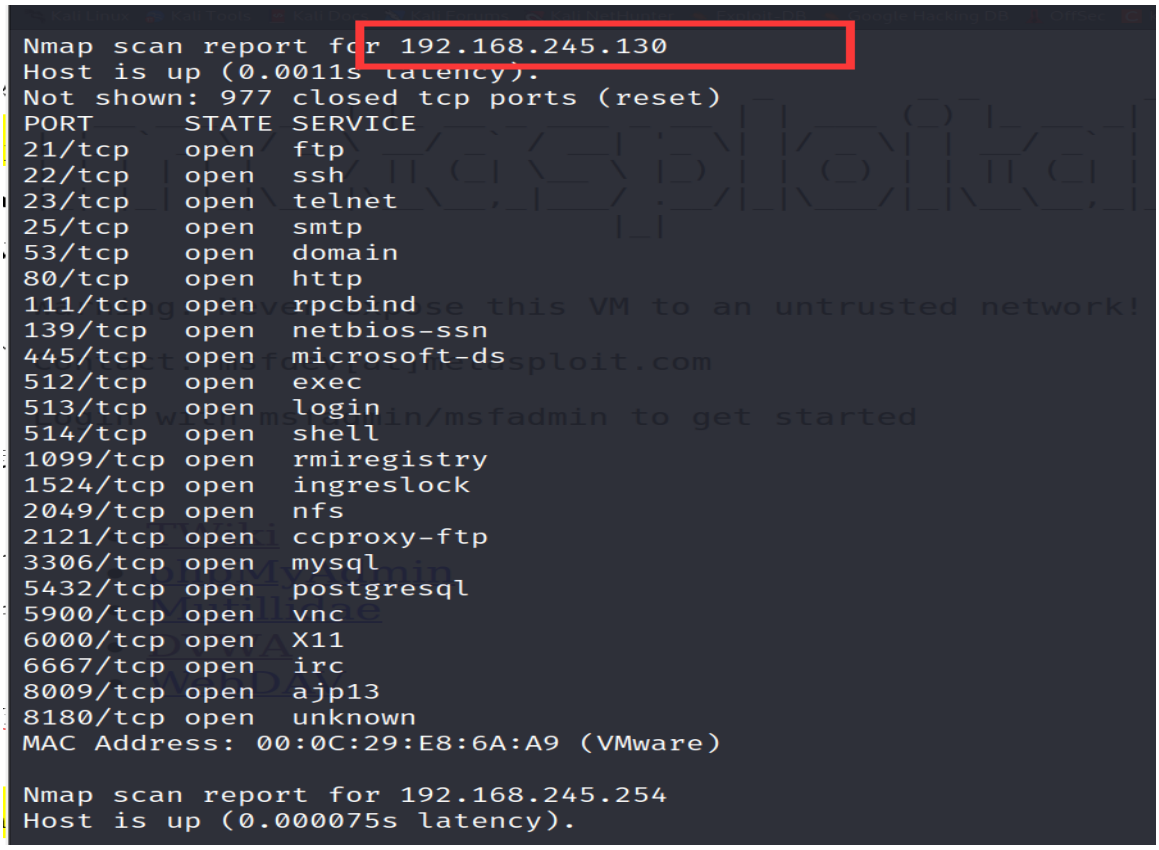
原因：两者值是不相同的。原因：myIPadress 搜索到的是公网 IP，而使用命令 ipconfig 获得的是内网 IP。



6.NMAP 的使用

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。



1. 21 端口：file transfer protocol（文件传输协议）一台主机作为 ftp 客户端，一台主机作为 Ftp 服务器，实现两台计算机之间文件的上传和下载。
2. 53 端口；domain name sever(域名服务器)，能将域名解析成 ip，从而访问网站
3. 22 端口： **Secure Shell** ：提供安全性的网络传输协议，具有三层：传输，用户认证，连接。相比于 ftp,传输速度快，保密性高。
4. 23 端口：Telnet 协议，它是 TCP/IP 协议中的一员

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

```
└─# nmap -O 192.168.245.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 05:23 EDT
Nmap scan report for 192.168.245.130
Host is up (0.00066s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:E8:6A:A9 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

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

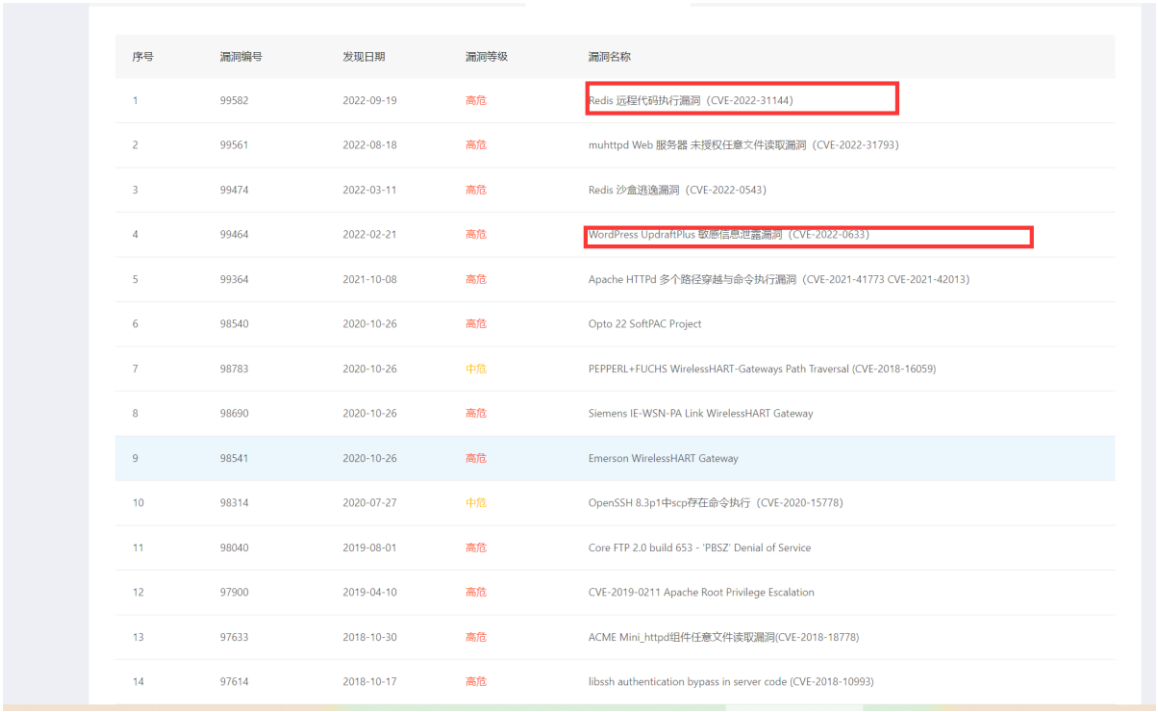
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 80 -script=http-form-brute -script-args=http-form-brute.path=/dvwa/login.php 192.168.245.130

Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 05:37 EDT
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 192.168.245.130
Host is up (0.00030s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-form-brute:
|   Accounts:
|     admin:password - Valid credentials
|_  Statistics: Performed 18385 guesses in 6205 seconds, average tps: 51.5
MAC Address: 00:0C:29:E8:6A:A9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6205.35 seconds
```

6.4 查阅资料，永恒之蓝-WannaCry 蠕虫利用漏洞的相关信息。

WannaCry（又叫 Wanna Decryptor），一种“蠕虫式”的勒索病毒软件。蠕虫病毒是一种常见的计算机病毒，是无须计算机使用者干预即可运行的独立程序，它通过不停的获得网络中存在漏洞的计算机上的部 分或全部控制权来进行传播。此病毒通过远程高

危漏洞进行自我传播复制,并且加密文件采用了高强度的 双 RSA+AES 加密,至少目前来说破解秘钥是不可能的,只能通过预防的方式来防御,勤打补丁,关闭 445、139 等端口,及时安装安全软件。

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



序号	漏洞编号	发现日期	漏洞等级	漏洞名称
1	99582	2022-09-19	高危	Redis 远程代码执行漏洞（CVE-2022-31144）
2	99561	2022-08-18	高危	muhttpd Web 服务器 未授权任意文件读取漏洞（CVE-2022-31793）
3	99474	2022-03-11	高危	Redis 沙盒逃逸漏洞（CVE-2022-0543）
4	99464	2022-02-21	高危	WordPress UpdraftPlus 敏感信息泄露漏洞（CVE-2022-0633）
5	99364	2021-10-08	高危	Apache HTTPd 多个路径穿越与命令执行漏洞（CVE-2021-41773 CVE-2021-42013）
6	98540	2020-10-26	高危	Opto 22 SoftPAC Project
7	98783	2020-10-26	中危	PEPPERL+FUCHS WirelessHART-Gateways Path Traversal (CVE-2018-16059)
8	98690	2020-10-26	高危	Siemens IE-WSN-PA Link WirelessHART Gateway
9	98541	2020-10-26	高危	Emerson WirelessHART Gateway
10	98314	2020-07-27	中危	OpenSSH 8.3p1中scp存在命令执行（CVE-2020-15778）
11	98040	2019-08-01	高危	Core FTP 2.0 build 653 - 'PBSZ' Denial of Service
12	97900	2019-04-10	高危	CVE-2019-0211 Apache Root Privilege Escalation
13	97633	2018-10-30	高危	ACME Mini_httpd组件任意文件读取漏洞(CVE-2018-18778)
14	97614	2018-10-17	高危	libssh authentication bypass in server code (CVE-2018-10993)

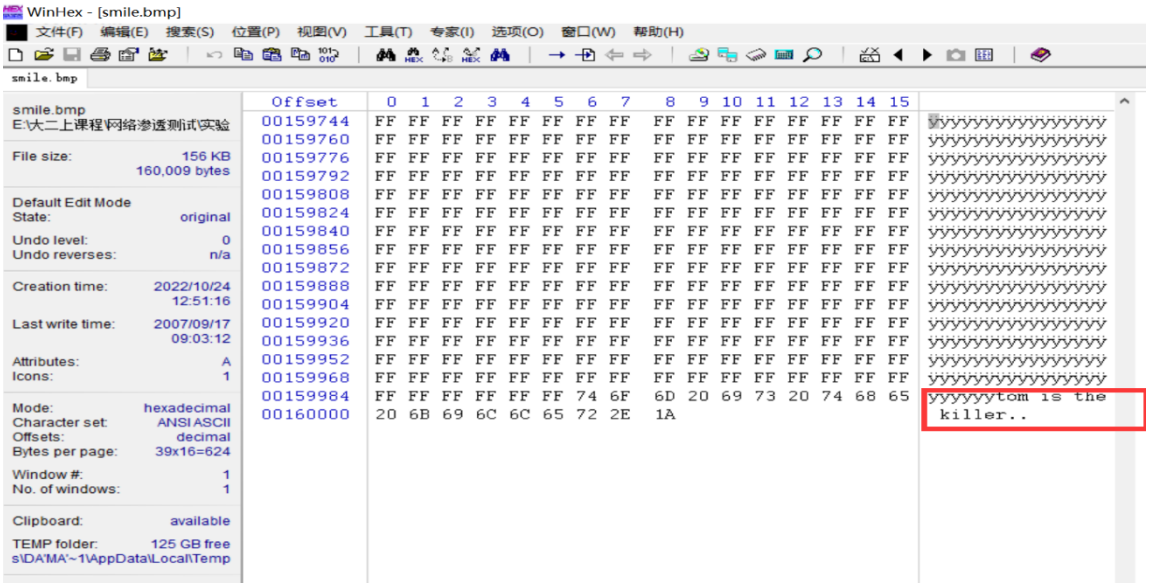
8、Winhex 简单数据恢复与取证

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

使用 winhex 打开后，发现 JPG 格式的文件头存在问题，记得 JPG 格式的文件头是 FF D8 FF，剪切多余的文件头，保存即可。

8.2 笑脸背后的阴霾：图片 smile 有什么隐藏信息。

信息：tom is the killer

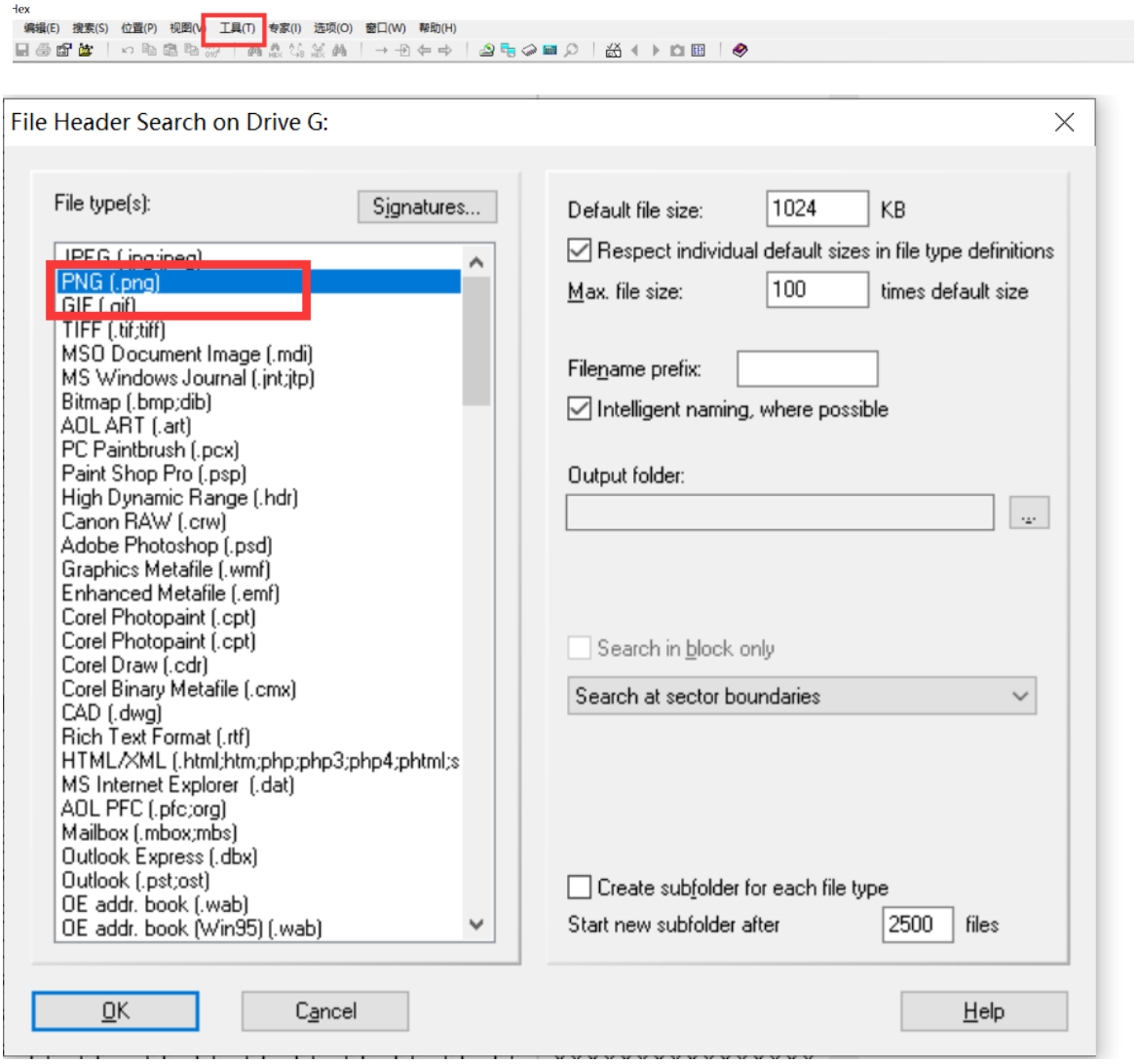


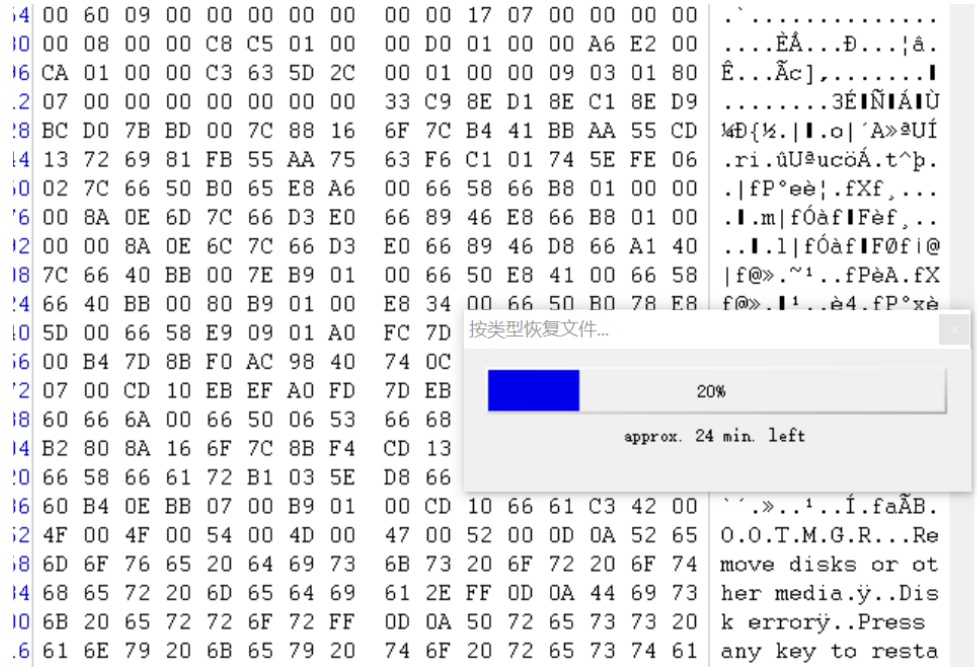
8.3 尝试使用数据恢复软件恢复你的 U 盘中曾经删除的文件。

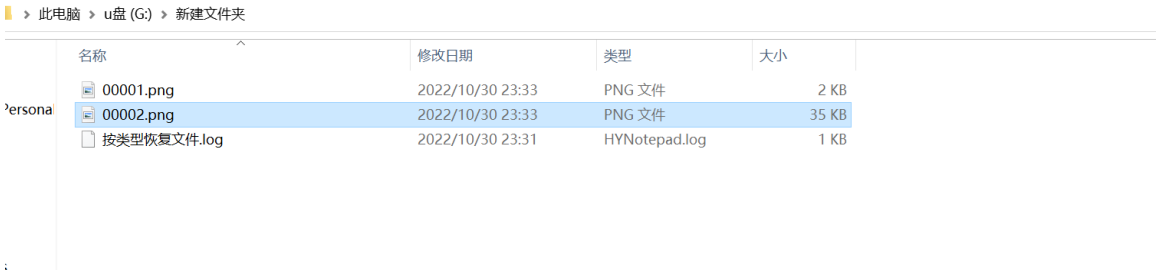
（1）使用工具:winhex

（2）步骤：

找一块 U 盘->打开 winhex->点击【工具】->【打开磁盘】，在此我们选择 U 盘->再点击【工具】->【磁盘工具】->【文件恢复工具】->选择文件类型：png,点击 OK->选择保存路径：在此我们选择 U 盘新建的文件夹，点击 OK


File Header Search on Drive G:
File type(s):
Signatures...
PNG (.png)
GIF (.gif)
TIFF (.tif;tiff)
MSO Document Image (.mdi)
MS Windows Journal (.jnt;jtp)
Bitmap (.bmp;dib)
AOL ART (.art)
PC Paintbrush (.pcx)
Paint Shop Pro (.psp)
High Dynamic Range (.hdr)
Canon RAW (.crw)
Adobe Photoshop (.psd)
Graphics Metafile (.wmf)
Enhanced Metafile (.emf)
Corel Photopaint (.cpt)
Corel Photopaint (.cpt)
Corel Draw (.cdr)
Corel Binary Metafile (.cmx)
CAD (.dwg)
Rich Text Format (.rtf)
HTML/XML (.html;htm;php;php3;php4;phtml;s
MS Internet Explorer (.dat)
AOL PFC (.pfc;org)
Mailbox (.mbox;mbs)
Outlook Express (.dbx)
Outlook (.pst;ost)
OE addr. book (.wab)
OE addr. book (Win95) (.wab)
Default file size:
1024
KB
Respect individual default sizes in file type definitions
Max. file size:
100
times default size
Filename prefix:
Intelligent naming, where possible
Output folder:
Search in block only
Search at sector boundaries
Create subfolder for each file type
Start new subfolder after
2500
files
OK
Cancel
Help


按类型恢复文件...
20%
approx. 24 min. left



9、讨论学校热点 GUET-WiFi 的安全问题，以截图说明。

（1）校园网是一个开放式的网络，包括教学局域网、图书馆局域网和办公自动化局域网等等，由于教学教务对于网络的依赖性越来越重，网络管理日趋复杂。 由于缺乏统一的管理软件和监控、日志系统，这些机房的管理基本处在各自为政的状态。绝大多数的机房登记管理制度存在漏洞，导致上网用户的身份无法唯一识别。有些计算机甚至服务器系统建设完毕之后无人管理，甚至被攻击者攻破作为攻击的跳板、变成攻击试验床也无人觉察。

（2）校园网用户活跃，校园网的主要用户是学生，用户安全意思薄弱，没有防范网络攻击的经验；有些人崇拜黑客，一心想着如何进行网络攻击，甚至因此走上网络犯罪的道路。

（3）学校网络建设经费不足，而且经费主要投在网络设备上，对于网络安全建设没有比较系统的投入。在校园网中，通常只有网络中心的少数工作人员，他们只能维护网络正常运行，无暇顾及、也没有条件管理和维护数万台计算机的安全。学校的机房实验室，只有简单的系统恢复，再无其他的维护，系统漏洞百出，而杀毒软件和防火墙往往得不到有效的更新。

3. 实验小结

（1）通过本次实验，我了解并且学习到一些搜索引擎语法和一些搜集信息的网站，以及渗透工具NMAP 的一些简单使用方法。

（2）本次实验比较有特色的是 winhex 的使用，在图片查看和恢复具有可观的效果，当然，最实用的便是它恢复数据的功能。

（3）Ethical Hacking：翻译为道德黑客，作为信息安全的学习者，学习道路上应该时刻具有严格的法律和道德意识，将自身所学用在正确的、符合法律的、切合道德的方面，做一名有道德的“黑客”。

（4）本次实验积累了一些简单的经验，为之后实验的进行增强了信心。