

编号：_____

| | | | | | | | | | | |
|--------|---|---|---|---|---|---|---|---|----|------|
| 实 验 | 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 总评 | 教师签名 |
| 成 绩 | | | | | | | | | | |

武汉大学网络安全学院

课程实验(设计)报告

课程名称：_____计算机病毒_____

实验内容：_____实验四 恶意软件样本行为分析_____

专业(班)：_____网络空间安全 2020 级 3 班_____

学 号：_____2020302181081_____

姓 名：_____陈曦_____

任课教师：_____陈泽茂_____

2023 年 5 月 10 日

目 录

| | |
|-------------------------|---|
| 实验 4 恶意软件样本行为分析 | 3 |
| 4.1 实验名称 | 3 |
| 4.2 实验目的 | 3 |
| 4.3 实验步骤及内容 | 3 |
| 4.4 实验关键过程、数据及其分析 | 4 |
| 4.5 实验体会和拓展思考 | 4 |

实验 4 恶意软件样本行为分析

4.1 实验名称

恶意软件样本行为分析

4.2 实验目的

了解恶意软件，学会使用检测和抓包等工具。配置木马分析环境并分析灰鸽子木马。

4.3 实验步骤及内容

第一阶段：熟悉 Process Monitor 的使用

- 利用 Process Monitor 监视 WinRAR 的解压缩过程。
打开 Procmon.exe 程序。可以看到各种在运行的程序。
- 利用 Process Monitor 分析 WinRAR 的临时文件存放在哪个文件夹中。
- WinRAR 压缩包内文件直接打开后，有两种关闭方式：先关闭打开的文件，再关闭打开的压缩包。
另外一种方式是先关闭打开的压缩包，再关闭打开的文件。利用 Process Monitor 分析上述两种方式的不同点。

第二阶段：熟悉抓包工具 Wireshark 的使用

- 熟练 Wireshark 软件的使用，着重掌握 Wireshark 的过滤器使用。
- 使用 Wireshark 抓取登录武汉大学邮箱或者珞珈山水 BBS 的数据包，并且通过分析数据包获得用户名和密码

第三阶段：VMware 的熟悉和使用

- 着重掌握 VMware 的网络设置方式，主要有 NAT 连接、桥接和 Host-Only 模式。
- 配置自己的木马分析环境

第四阶段：灰鸽子木马的行为分析

- 熟悉灰鸽子木马的使用，利用灰鸽子木马控制虚拟机。
- 利用 Process Monitor 监控感染灰鸽子木马的被控端的文件行为和注册表行为。
- 利用 Wireshark 监控灰鸽子木马与控制端的网络通信。
- 提出灰鸽子木马的清除方案

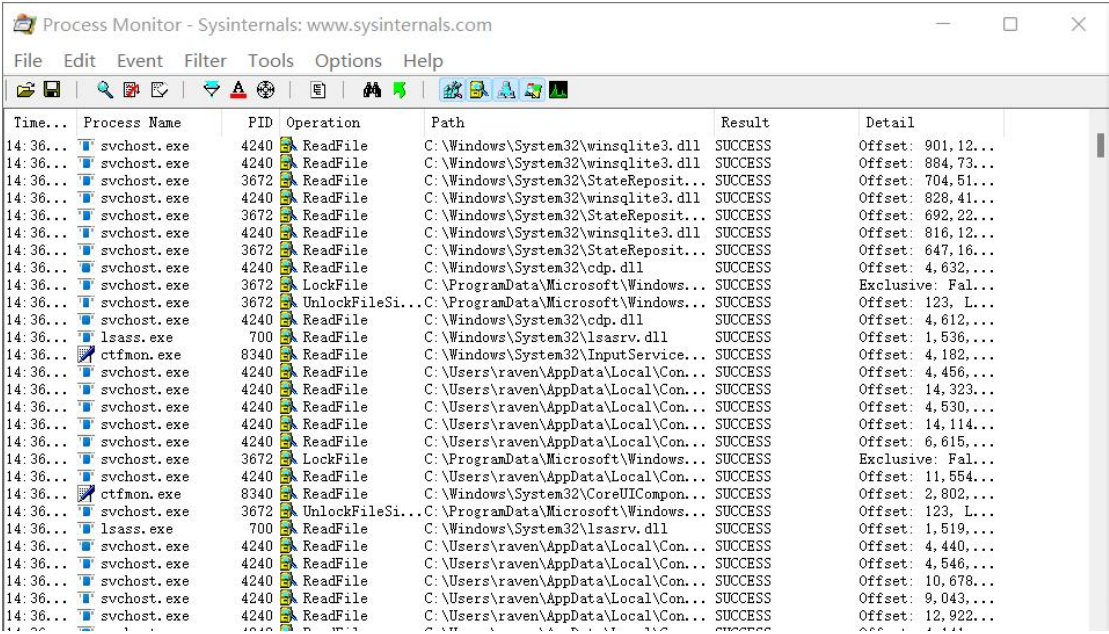
第五阶段：课后习题思考与实践

- 尝试对大白鲨木马或 PCShare 木马进行行为分析。

4.4 实验关键过程、数据及其分析

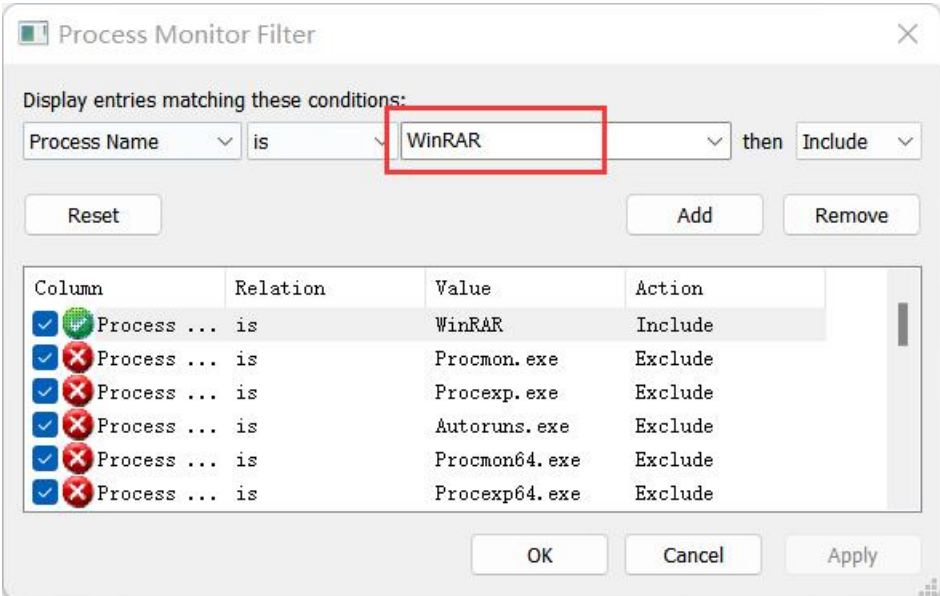
第一阶段：熟悉 Process Monitor 的使用

其利用 Process Monitor 监视 WinRAR 的解压缩过程。



| Time... | Process Name | PID | Operation | Path | Result | Detail |
|----------|--------------|------|-----------------|-------------------------------------|---------|-------------------|
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Windows\System32\winsqlite3.dll | SUCCESS | Offset: 901,12... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Windows\System32\winsqlite3.dll | SUCCESS | Offset: 884,73... |
| 14:36... | svchost.exe | 3672 | ReadFile | C:\Windows\System32\StateReposit... | SUCCESS | Offset: 704,51... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Windows\System32\winsqlite3.dll | SUCCESS | Offset: 828,41... |
| 14:36... | svchost.exe | 3672 | ReadFile | C:\Windows\System32\StateReposit... | SUCCESS | Offset: 692,22... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Windows\System32\winsqlite3.dll | SUCCESS | Offset: 816,12... |
| 14:36... | svchost.exe | 3672 | ReadFile | C:\Windows\System32\StateReposit... | SUCCESS | Offset: 647,16... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Windows\System32\cdp.dll | SUCCESS | Offset: 4,632... |
| 14:36... | svchost.exe | 3672 | LockFile | C:\ProgramData\Microsoft\Windows... | SUCCESS | Exclusive: Fal... |
| 14:36... | svchost.exe | 3672 | UnlockFileSi... | C:\ProgramData\Microsoft\Windows... | SUCCESS | Offset: 123, L... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Windows\System32\cdp.dll | SUCCESS | Offset: 4,612... |
| 14:36... | lsass.exe | 700 | ReadFile | C:\Windows\System32\lsasrv.dll | SUCCESS | Offset: 1,536... |
| 14:36... | ctfmon.exe | 8340 | ReadFile | C:\Windows\System32\InputService... | SUCCESS | Offset: 4,182... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Users\raven\AppData\Local\Con... | SUCCESS | Offset: 4,466... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Users\raven\AppData\Local\Con... | SUCCESS | Offset: 14,323... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Users\raven\AppData\Local\Con... | SUCCESS | Offset: 4,530... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Users\raven\AppData\Local\Con... | SUCCESS | Offset: 14,114... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Users\raven\AppData\Local\Con... | SUCCESS | Offset: 6,615... |
| 14:36... | svchost.exe | 3672 | LockFile | C:\ProgramData\Microsoft\Windows... | SUCCESS | Exclusive: Fal... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Users\raven\AppData\Local\Con... | SUCCESS | Offset: 11,554... |
| 14:36... | ctfmon.exe | 8340 | ReadFile | C:\Windows\System32\CoreUICompon... | SUCCESS | Offset: 2,802... |
| 14:36... | svchost.exe | 3672 | UnlockFileSi... | C:\ProgramData\Microsoft\Windows... | SUCCESS | Offset: 123, L... |
| 14:36... | lsass.exe | 700 | ReadFile | C:\Windows\System32\lsasrv.dll | SUCCESS | Offset: 1,519... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Users\raven\AppData\Local\Con... | SUCCESS | Offset: 4,440... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Users\raven\AppData\Local\Con... | SUCCESS | Offset: 4,546... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Users\raven\AppData\Local\Con... | SUCCESS | Offset: 10,678... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Users\raven\AppData\Local\Con... | SUCCESS | Offset: 9,043... |
| 14:36... | svchost.exe | 4240 | ReadFile | C:\Users\raven\AppData\Local\Con... | SUCCESS | Offset: 12,922... |

添加“进程名称包含 WinRAR”这一规则，并应用。



运行 WinRAR.exe 程序之后，可以看到检测系统显示关于 WinRAR 的进程。

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time... | Process Name | PID | Operation | Path | Result | Detail |
|----------|--------------|-------|-----------------|-------------------------------------|----------------|-------------------|
| 14:38... | WinRAR.exe | 21636 | Process Start | | SUCCESS | Parent PID: 32... |
| 14:38... | WinRAR.exe | 21636 | Thread Create | | SUCCESS | Thread ID: 18536 |
| 14:38... | WinRAR.exe | 21636 | Load Image | D:\Winrar\WinRAR.exe | SUCCESS | Image Base: 0x... |
| 14:38... | WinRAR.exe | 21636 | Load Image | C:\Windows\System32\ntdll.dll | SUCCESS | Image Base: 0x... |
| 14:38... | WinRAR.exe | 21636 | CreateFile | C:\Windows\Prefetch\WINRAR.EXE-E... | SUCCESS | Desired Access... |
| 14:38... | WinRAR.exe | 21636 | QueryStandar... | C:\Windows\Prefetch\WINRAR.EXE-E... | SUCCESS | AllocationSize... |
| 14:38... | WinRAR.exe | 21636 | ReadFile | C:\Windows\Prefetch\WINRAR.EXE-E... | SUCCESS | Offset: 0, Len... |
| 14:38... | WinRAR.exe | 21636 | CloseFile | C:\Windows\Prefetch\WINRAR.EXE-E... | SUCCESS | |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\System\CurrentControlSet\Co... | REPARSE | Desired Access... |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\System\CurrentControlSet\Co... | SUCCESS | Desired Access... |
| 14:38... | WinRAR.exe | 21636 | RegQueryValue | HKLM\System\CurrentControlSet\Co... | SUCCESS | Type: REG_SZ, ... |
| 14:38... | WinRAR.exe | 21636 | RegQueryValue | HKLM\System\CurrentControlSet\Co... | SUCCESS | Type: REG_SZ, ... |
| 14:38... | WinRAR.exe | 21636 | RegCloseKey | HKLM\System\CurrentControlSet\Co... | SUCCESS | |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\System\CurrentControlSet\Co... | REPARSE | Desired Access... |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\System\CurrentControlSet\Co... | SUCCESS | Desired Access... |
| 14:38... | WinRAR.exe | 21636 | RegQueryValue | HKLM\System\CurrentControlSet\Co... | NAME NOT FOUND | Length: 80 |
| 14:38... | WinRAR.exe | 21636 | RegCloseKey | HKLM\System\CurrentControlSet\Co... | SUCCESS | |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Co... | REPARSE | Desired Access... |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Co... | NAME NOT FOUND | Desired Access... |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Co... | REPARSE | Desired Access... |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Co... | SUCCESS | Desired Access... |
| 14:38... | WinRAR.exe | 21636 | RegQueryValue | HKLM\System\CurrentControlSet\Co... | NAME NOT FOUND | Length: 24 |
| 14:38... | WinRAR.exe | 21636 | RegCloseKey | HKLM\System\CurrentControlSet\Co... | SUCCESS | |

使用 Jump to.. 可以跳转到文件所在位置。

| | | | | | | |
|----------|------------|-------|---------------|-------------------------------------|----------------|--|
| 14:38... | WinRAR.exe | 21636 | RegQueryValue | HKLM\System\CurrentControlSet\Co... | NAME NOT FOUND | |
| 14:38... | WinRAR.exe | 21636 | RegCloseKey | HKLM\System\CurrentControlSet\Co... | SUCCESS | |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\System\CurrentControlSet\Co... | REPARSE | |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\System\CurrentControlSet\Co... | REPARSE | |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\System\CurrentControlSet\Co... | REPARSE | |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\System\CurrentControlSet\Co... | REPARSE | |
| 14:38... | WinRAR.exe | 21636 | RegQueryValue | HKLM\System\CurrentControlSet\Co... | NAME NOT FOUND | |
| 14:38... | WinRAR.exe | 21636 | RegCloseKey | HKLM\System\CurrentControlSet\Co... | SUCCESS | |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Co... | REPARSE | |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Co... | NAME NOT FOUND | |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Co... | REPARSE | |
| 14:38... | WinRAR.exe | 21636 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Co... | SUCCESS | |
| 14:38... | WinRAR.exe | 21636 | RegQueryValue | HKLM\System\CurrentControlSet\Co... | NAME NOT FOUND | |
| 14:38... | WinRAR.exe | 21636 | RegCloseKey | HKLM\System\CurrentControlSet\Co... | SUCCESS | |

Properties... Ctrl+P

Stack... Ctrl+K

Toggle Bookmark Ctrl+B

Jump To... Ctrl+J

Search Online...

跳转到对应注册表。

注册表编辑器

文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)

计算机\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager

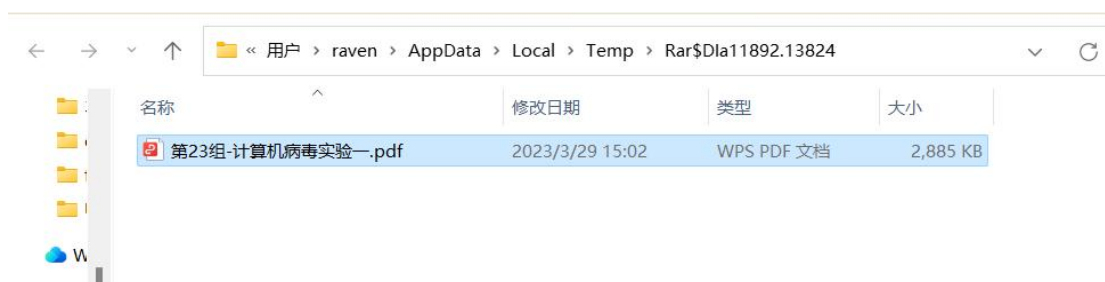
| 名称 | 类型 | 数据 |
|--------------------|---------------|--|
| (默认) | REG_SZ | (数值未设置) |
| AutoChkSkipS... | REG_DWORD | 0x00000000 (0) |
| AutoChkTimeo... | REG_DWORD | 0x00000005 (5) |
| BootExecute | REG_MULTI_SZ | autocheck autochk * |
| BootShell | REG_EXPAND_SZ | %SystemRoot%\system32\bootim.exe |
| CriticalSection... | REG_DWORD | 0x00278d00 (2592000) |
| ExcludeFromK... | REG_MULTI_SZ | |
| GlobalFlag | REG_DWORD | 0x00000000 (0) |
| GlobalFlag2 | REG_DWORD | 0x00000000 (0) |
| HeapDeComm... | REG_DWORD | 0x00000000 (0) |
| HeapDeComm... | REG_DWORD | 0x00000000 (0) |
| HeapSegment... | REG_DWORD | 0x00000000 (0) |
| HeapSegment... | REG_DWORD | 0x00000000 (0) |
| InitConsoleFlags | REG_DWORD | 0x00000000 (0) |
| NumberOfIni... | REG_DWORD | 0x00000002 (2) |
| ObjectDirector... | REG_MULTI_SZ | \Windows\RPC Control |
| PendingFileRe... | REG_MULTI_SZ | \\?\C:\WINDOWS\system32\spool\DRIVERS\W... |
| ProcessorCont... | REG_DWORD | 0x00000002 (2) |
| ProtectionMode | REG_DWORD | 0x00000001 (1) |
| ResourceTime... | REG_DWORD | 0x00000096 (150) |
| RunLevelExecu... | REG_MULTI_SZ | WinInit ServiceControlManager |
| RunLevelValida... | REG_MULTI_SZ | ServiceControlManager |
| SETUPEXECUTE | REG_MULTI_SZ | |

利用 Process Monitor 分析 WinRAR 的临时文件存放在哪个文件夹中。

选中一个文件，右键点击 Jump to...

| | | | | | |
|------------|-------|-----------------|-----------------------------------|-----------------|--------|
| WinRAR.exe | 11892 | SetBasicInfo... | C:\Users\raven\AppData\Local\T... | Properties... | Ctrl+P |
| WinRAR.exe | 11892 | QueryAttribu... | C:\Users\raven\AppData\Local\T... | Stack... | Ctrl+K |
| WinRAR.exe | 11892 | QueryStandar... | C:\Users\raven\AppData\Local\T... | Toggle Bookmark | Ctrl+B |
| WinRAR.exe | 11892 | CreateFile | C:\Users\raven\AppData\Local\T... | Jump To... | Ctrl+J |
| WinRAR.exe | 11892 | SetBasicInfo... | C:\Users\raven\AppData\Local\T... | | |
| WinRAR.exe | 11892 | CloseFile | C:\Users\raven\AppData\Local\T... | | |

打开后发现文件不在原本的路径，而是在一个临时文件夹中。



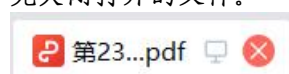
该文件夹路径为：C:\Users\raven\AppData\Local\Temp。

WinRAR 压缩包内文件直接打开后，有两种关闭方式：先关闭打开的文件，再关闭打开的压缩包。另外一种方式是先关闭打开的压缩包，再关闭打开的文件。利用 Process Monitor 分析上述两种方式的不同点。

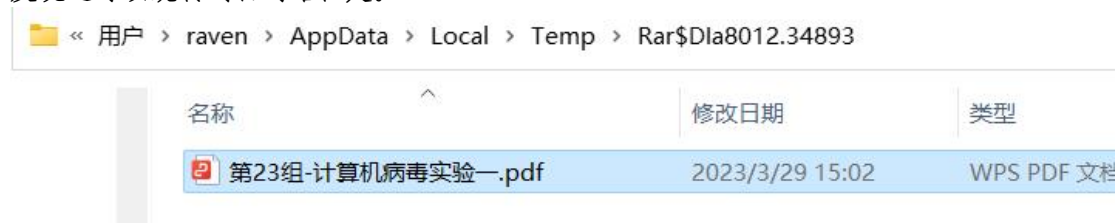
从 WinRAR 中打开一个文件。



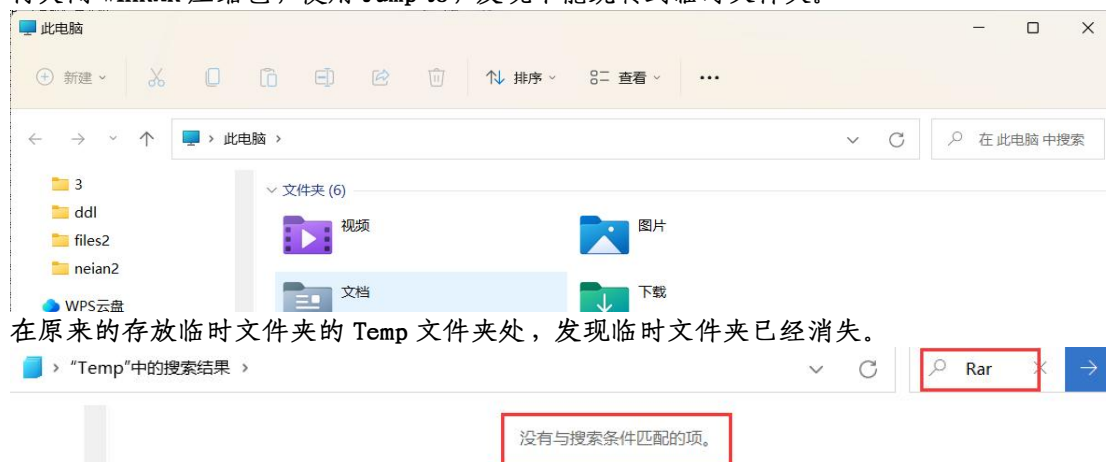
先关闭打开的文件。



发现还可以跳转到目的路径处。

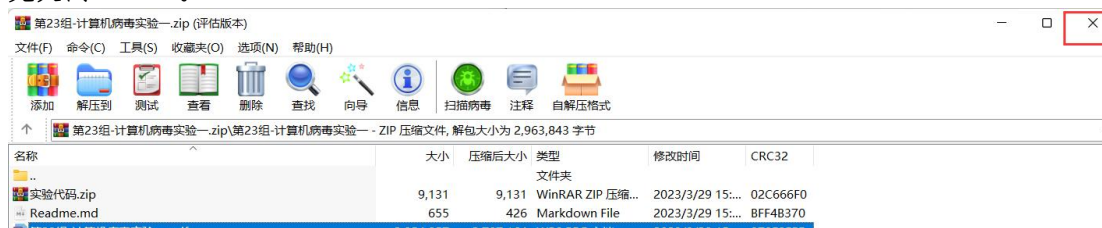


再关闭 WinRAR 压缩包，使用 Jump to，发现不能跳转到临时文件夹。

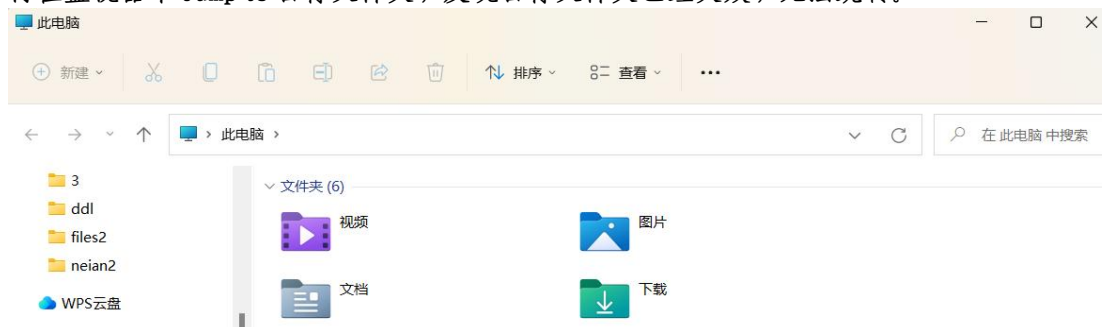


再次从 WinRAR 打开之前的文件，这次先关闭 WinRAR 程序再关闭文件。

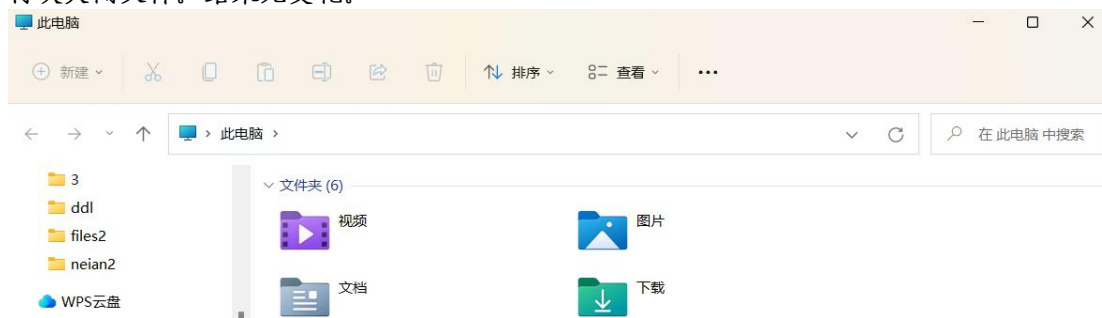
先关闭 WinRAR。



再在监视器中 Jump to 目标文件夹，发现目标文件夹已经失效，无法跳转。



再次关闭文件。结果无变化。

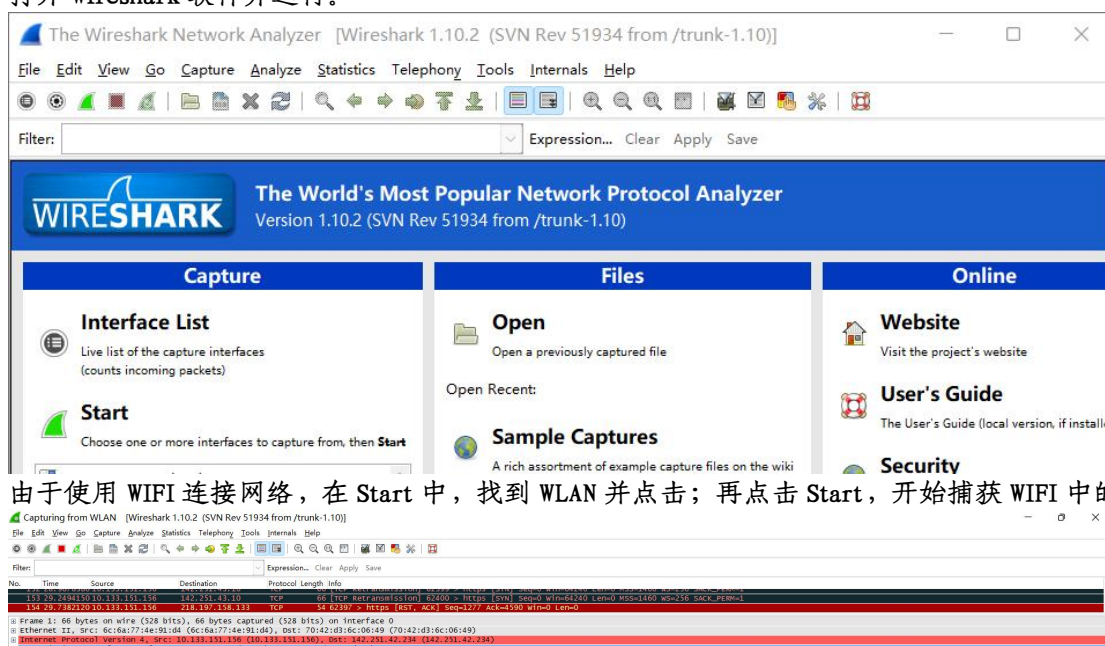


可见，临时文件夹随 WinRAR 压缩包의 打开而创建，关闭而消除。

第二阶段：熟悉抓包工具 Wireshark 的使用

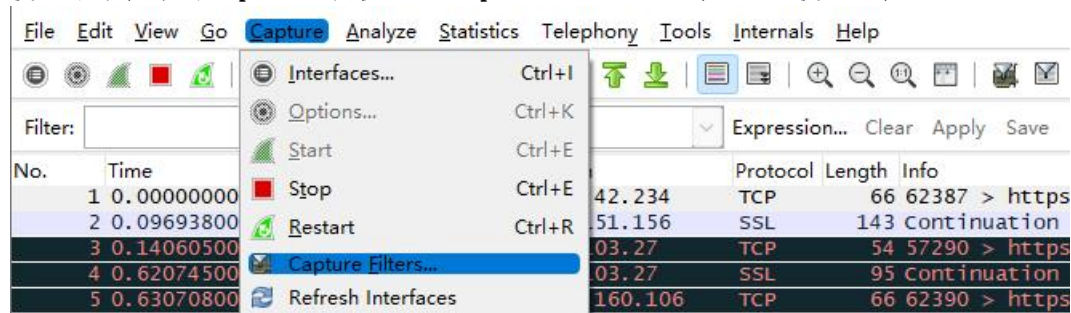
其 熟练 Wireshark 软件的使用，着重掌握 Wireshark 的过滤器使用。

打开 Wireshark 软件并运行。

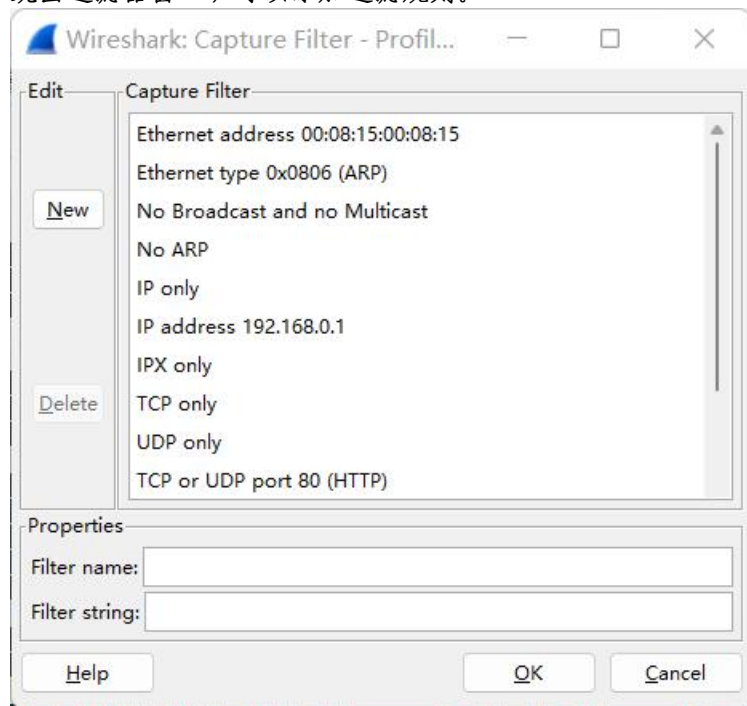


由于使用 WIFI 连接网络，在 Start 中，找到 WLAN 并点击；再点击 Start，开始捕获 WIFI 中的数据包。

使用菜单栏中的 Capture（捕获）—>Capture Filters...（过滤器），使用过滤器。



跳出过滤器窗口，可以添加过滤规则。



其 使用 Wireshark 抓取登录武汉大学邮箱或者珞珈山水 BBS 的数据包，并且通过分析数据包获得用户名和密码

登录珞珈山水的网站：bbs.whu.edu.cn。



先注册账号。

珞珈山水 -- 新用户注册

欢迎加入珞珈山水 (有“*”号的必须填写, 一个汉字作为两个字符计算)

本站注册流程为:
(1) 如实填写以下注册信息, 点击“申请”后跳转到下一页面;
(2) 在校生或已毕业校友, 请在下一页面中上传身份证和校园卡 (校友上传毕业证或学位证) 照片进行实名认证审核认证;
(3) 教职工用户可上传身份证和校园卡 (工作证) 照片在线办理实名认证, 或将本人身份证和校园卡 (工作证) 至本科生院楼南楼503办公室办理认证。
我们为什么要这样做? 点击[帮助](#)查看相关信息。

*用户名: (2-12字符, 可用英文字母或数字, 首字符必须是字母)
*密码: (4-39字符)
*确认密码: (4-39字符, 必须和密码一致)
昵称: (2-39字符, 中英文不混)
*真实姓名: (请用中文, 至少2个汉字)
*学号/工号/毕业证或学位证编号:
(在校生填写学号; 在职教职工填写工号; 已毕业校友填写毕业证编号或学位证编号, 如填写错误将影响实名认证)
*身份证号: (请填写真实的身份证号, 否则将不予通过人工审核)
性别: ☐ 男 ☐ 女
出生年月日: 年 月 日
*Email: (如填写错误将收不到实名认证通过的邮件)
*您的联系电话:

注册成功之后登录, 登录的过程中不能关闭 WireShark。



Copyright © 2011 BBS 珞珈山水站 武汉大学. All rights reserved.
建议使用Cterm或Fterm登陆本站, 有关 Web 首页设计请去 WebArt 讨论. 实名注册请见教程.

登录成功。

尊敬的signorino, 您好! 欢迎来到珞珈山水

本站对用户进行实名管理, 只有通过实名认证的用户才有发帖权限, 未实名认证的用户只能浏览。实名方法如下:

1. 请点击[这里](#)上传相关证件, 审核通过后即开通相关权限; (如您已上传, 请等候审核。我们会在1~3个工作日内完成审核。)
2. 在校生请上传校园卡、身份证的照片;
3. 已毕业的校友请上传武汉大学毕业证 (或学位证)、身份证的照片;
4. 教职工用户可上传身份证和校园卡 (工作证) 照片, 或直接持本人身份证和校园卡 (工作证) 至本科生院楼南楼503办公室办理审核。

我们为什么要这样做? 点击[帮助](#)查看相关信息。 (此处帮助内容即“关于珞珈山水 BBS 实施人工审核注册用户证件的说明”)
如果您需要更多帮助, 请进入[BBS使用求助讨论区](#)。

使用 WireShark 过滤器。

输入命令 `http and ip.addr==218.197.148.129`。218.197.148.129 是珞珈山水的 IP 地址。

以及命令 `http.request.method=="POST"`, 表示过滤出 POST 表单的信息。

应用该过滤信息。

| Filter | Expression... | Clear | Apply | Save |
|--------|---|-------|-------|-----------------------------|
| No. | http and ip.addr==218.197.148.129 and http.request.method=="POST" | | | |
| 420 | http and ip.addr==218.197.148.129 | HTTP | 868 | POST /bbsreg.php HTTP/1.1 |
| 483 | http and ip.addr==218.197.148.129 | HTTP | 934 | POST /bbsreg.php HTTP/1.1 |
| 500 | http and ip.addr==218.197.148.129 | HTTP | 937 | POST /bbsreg.php HTTP/1.1 |
| 6917 | 886.121604 10.133.151.156 218.197.148.129 | HTTP | 769 | POST /bbslogin.php HTTP/1.1 |

下方详情栏中可以看到输入的用户名和密码。

| |
|---|
| Frame 12665: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface 0 |
| Ethernet II, Src: 6c:6a:77:4e:91:d4 (6c:6a:77:4e:91:d4), Dst: 70:42:d3:6c:06:49 (70:42:d3:6c:06:49) |
| Internet Protocol Version 4, Src: 10.133.151.156 (10.133.151.156), Dst: 218.197.148.129 (218.197.148.129) |
| Transmission Control Protocol, Src Port: 63292 (63292), Dst Port: http (80), Seq: 6125, Ack: 2489, Len: 834 |
| Hypertext Transfer Protocol |
| Line-based text data: application/x-www-form-urlencoded |
| id=signorino&passwd=CXwds189%21&webtype=wforum |

第三阶段: VMware 的熟悉和使用

其 着重掌握 VMware 的网络设置方式, 主要有 NAT 连接、桥接和 Host-Only 模式。

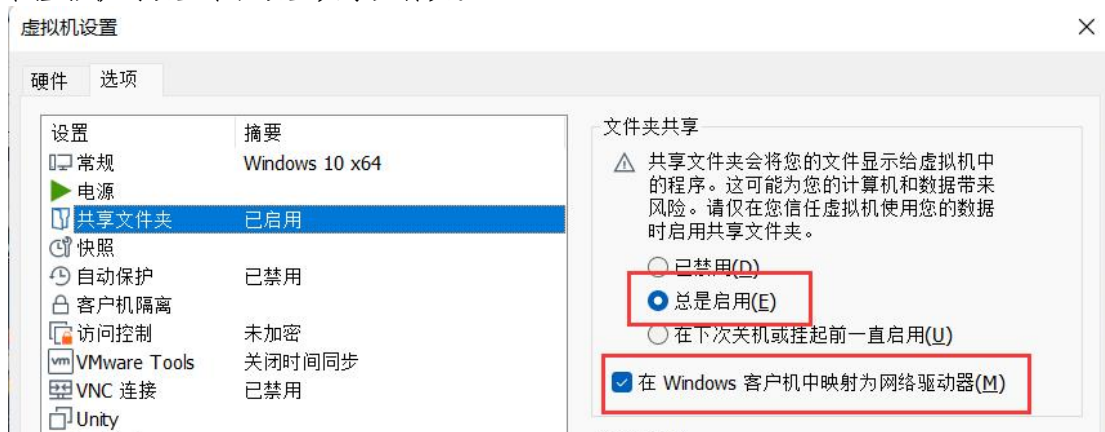
使用 VMware 打开 Windows 7 系统。

安装成功。

将实验所需要用到的工具都放在本地的 share 文件夹中, 准备用作共享文件夹的文件夹。

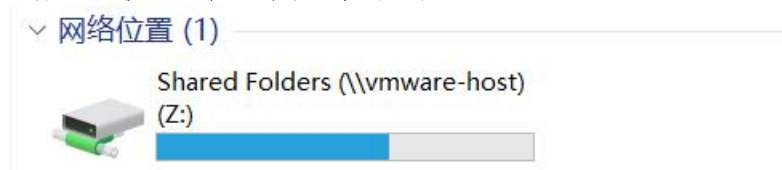


在虚拟机的设置中，设置共享文件夹。

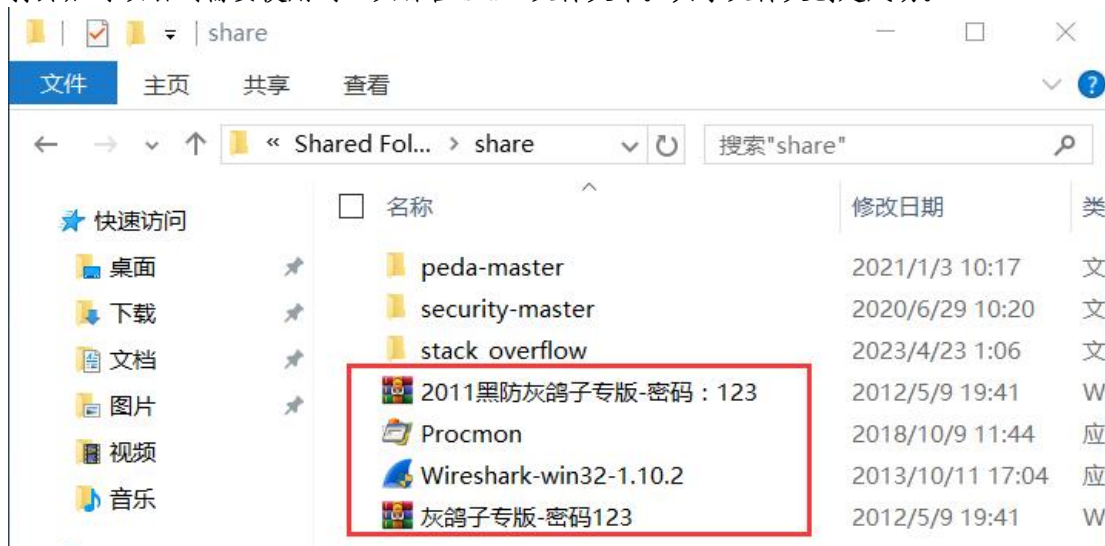


安装 VMware tools。

重启虚拟机后，在网络位置处找到 Shared Folders。



打开后可以看到需要使用的工具都在 share 文件夹中。共享文件夹创建成功。



配置网络。VMware 有四种网络配置选项。

Host-Only

虚拟机与宿主机具有不同的 IP 地址，与宿主机位于不同网段。从网络技术上相当于为宿主主机增添了一个虚拟网卡，让宿主机变成一台双网卡主机。这种方式只能进行虚拟机和宿主机之间的网络通信，网络内其他机器不能访问虚拟机，虚拟机也不能访问其他机器。

Bridge（桥接方式）

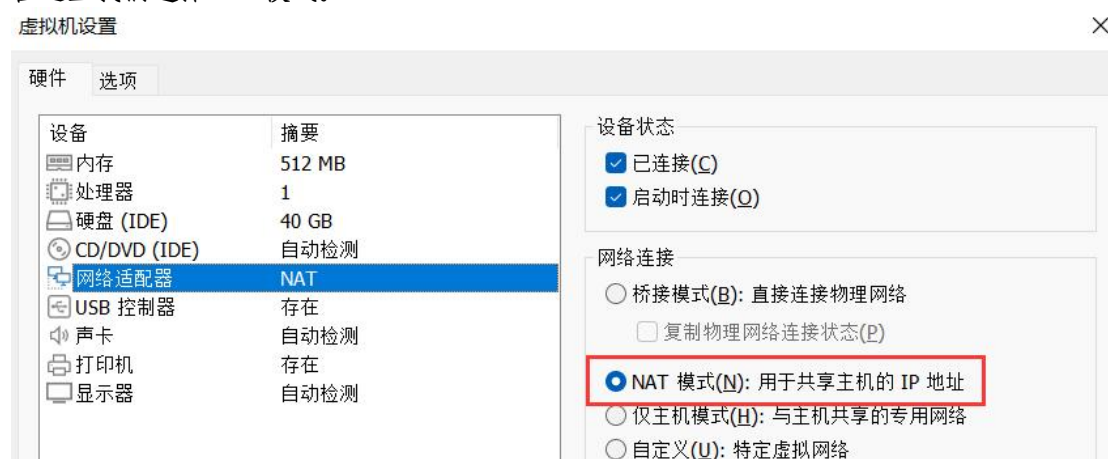
虚拟机与宿主机具有不同的 IP 地址，与宿主机保持在同一网段。宿主机局域网内其他主机可以访问虚拟机，虚拟机也可以访问网络内其他机器。

NAT 连接

与 Host-only 一样，宿主主机成为双网卡主机，同时参与现有的宿主局域网和新建的虚拟局域网，但由于加设了一个虚拟的 NAT 服务器，使得虚拟局域网内的虚拟机在对外访问时，完全“冒用”宿主主机的 IP 地址。这种方式可以实现本机系统与虚拟系统的双向访问，但网络内其他机器不能访问虚拟系统，虚拟系统可以通过本机系统用 NAT 协议访问网络内其他机器。

自定义接口

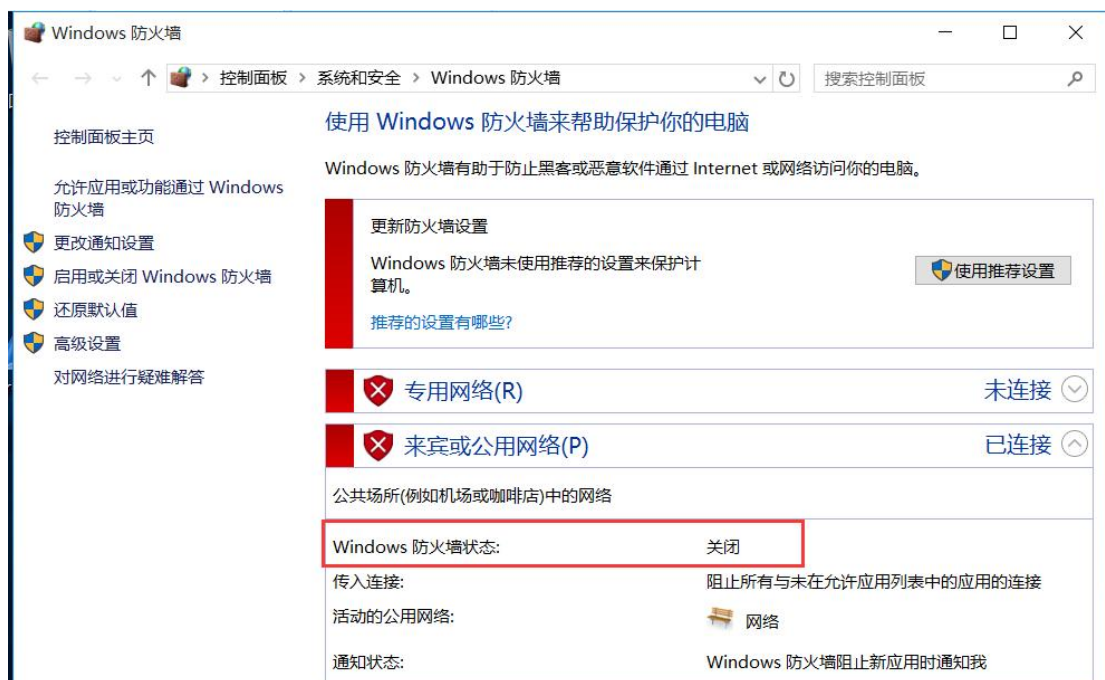
在这里我们选择 NAT 模式。



在虚拟机中打开百度网址，发现成功连接网络。



先关闭防火墙。



查看虚拟机 IP 地址为 10.133.255.128。

```
C:\Users\raven>ipconfig

Windows IP 配置

以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . : localdomain
    本地链接 IPv6 地址. . . . . : fe80::acea:9778:e16d:24c3%4
    IPv4 地址 . . . . . : 10.133.255.128
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 10.133.255.2

以太网适配器 蓝牙网络连接:
```

在本机 ping 虚拟机。发现可以 ping 通。

```
C:\Users\raven>ping 10.133.255.128

正在 Ping 10.133.255.128 具有 32 字节的数据:
来自 10.133.255.128 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.255.128 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.255.128 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.255.128 的回复: 字节=32 时间<1ms TTL=128

10.133.255.128 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

在本机查看 IP 地址。查看无线局域网适配器的 IPv4 地址。

```
无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . : 
    本地链接 IPv6 地址. . . . . : fe80::108d:f705:f6c5:16dc%11
    IPv4 地址 . . . . . : 10.133.151.156
    子网掩码 . . . . . : 255.255.128.0
    默认网关. . . . . : 10.133.255.254
```

在虚拟机 ping 本机。发现可以 ping 通。

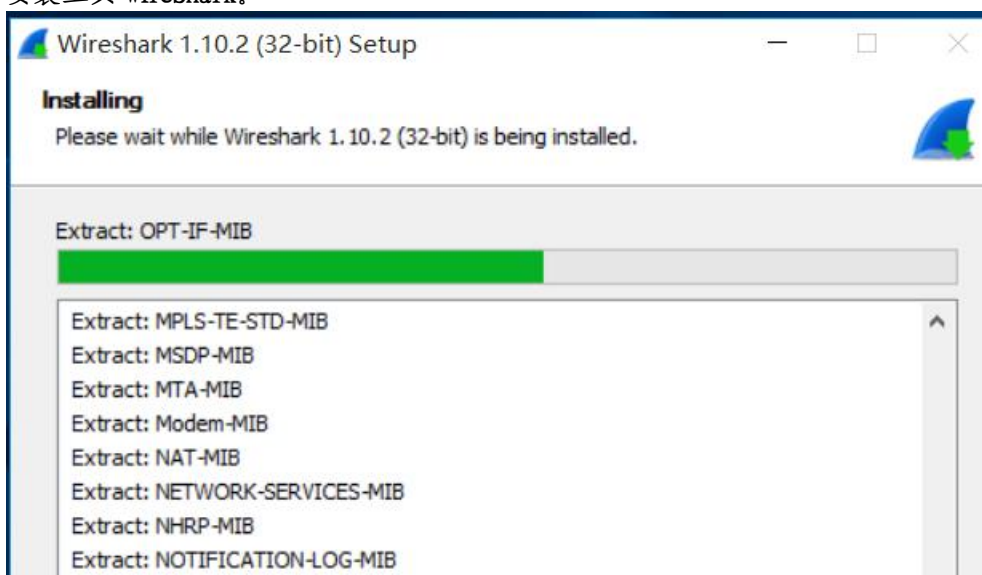
```
C:\Users\raven>ping 10.133.151.156

正在 Ping 10.133.151.156 具有 32 字节的数据:
来自 10.133.151.156 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.151.156 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.151.156 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.151.156 的回复: 字节=32 时间<1ms TTL=128

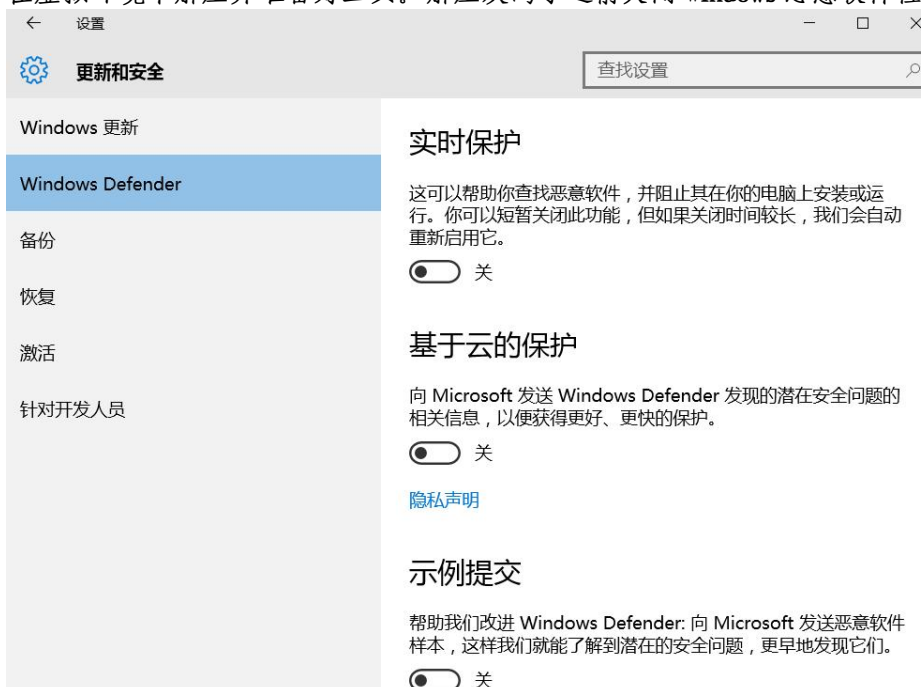
10.133.151.156 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

其 配置自己的木马分析环境

安装工具 WireShark。



在虚拟环境中解压并准备好工具。解压灰鸽子之前关闭 Windows 恶意软件检测程序。



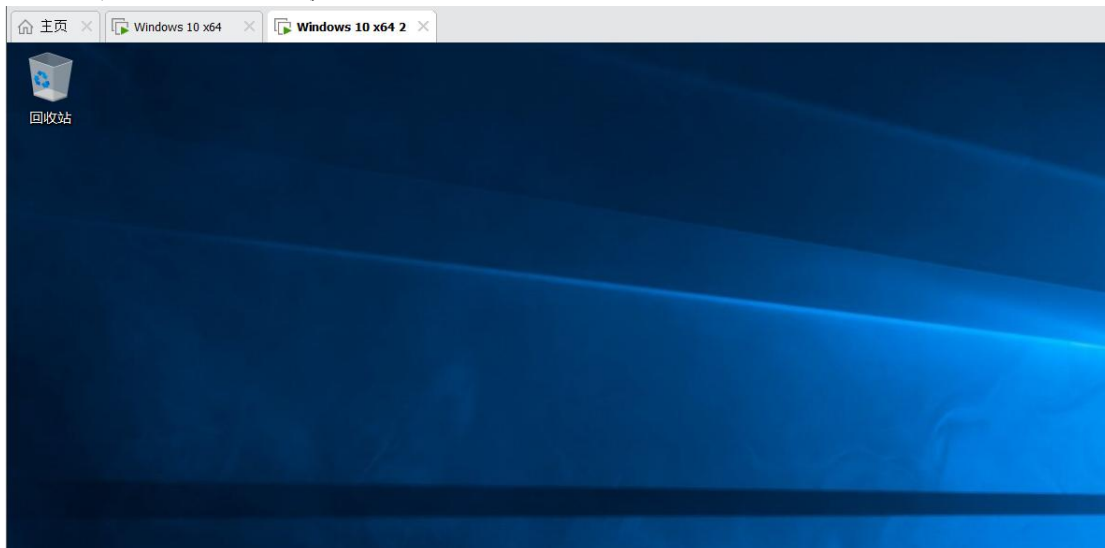
并将存放目标程序的文件存为排除项；包括共享文件夹。



最后解压工具。



添加一个 Windows10 虚拟机，Windows 10 x64 2。



关闭防火墙。



查看虚拟机 2 的 IP 地址。

```
C:\Users\raven>ipconfig
```

Windows IP 配置

以太网适配器 Ethernet0:

```
连接特定的 DNS 后缀 . . . . . : localdomain
本地链接 IPv6 地址. . . . . : fe80::4861:e109:c4cc:d22b%5
IPv4 地址 . . . . . : 10.133.255.129
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 10.133.255.2
```

主机 ping 虚拟机 2，可以 ping 通。

```
C:\Users\raven>ping 10.133.255.129
```

```
正在 Ping 10.133.255.129 具有 32 字节的数据:
来自 10.133.255.129 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.255.129 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.255.129 的回复: 字节=32 时间=1ms TTL=128
来自 10.133.255.129 的回复: 字节=32 时间<1ms TTL=128
```

```
10.133.255.129 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

虚拟机 2 ping 主机，可以 ping 通。

```
C:\Users\raven>ping 10.133.151.156
```

```
正在 Ping 10.133.151.156 具有 32 字节的数据:
来自 10.133.151.156 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.151.156 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.151.156 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.151.156 的回复: 字节=32 时间<1ms TTL=128
```

```
10.133.151.156 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

虚拟机 1 ping 虚拟机 2。

```
C:\Users\raven>ping 10.133.255.129
```

```
正在 Ping 10.133.255.129 具有 32 字节的数据:
来自 10.133.255.129 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.255.129 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.255.129 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.255.129 的回复: 字节=32 时间<1ms TTL=128
```

```
10.133.255.129 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

虚拟机 2 ping 虚拟机 1。

```
C:\Users\raven>ping 10.133.255.128

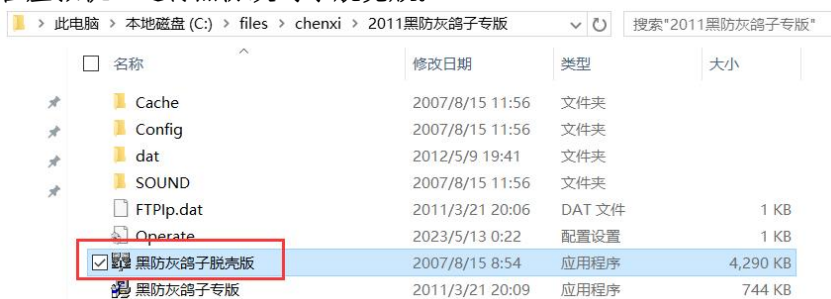
正在 Ping 10.133.255.128 具有 32 字节的数据:
来自 10.133.255.128 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.255.128 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.255.128 的回复: 字节=32 时间<1ms TTL=128
来自 10.133.255.128 的回复: 字节=32 时间<1ms TTL=128

10.133.255.128 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

第四阶段：灰鸽子木马的行为分析

其 熟悉灰鸽子木马的使用，利用灰鸽子木马控制虚拟机。

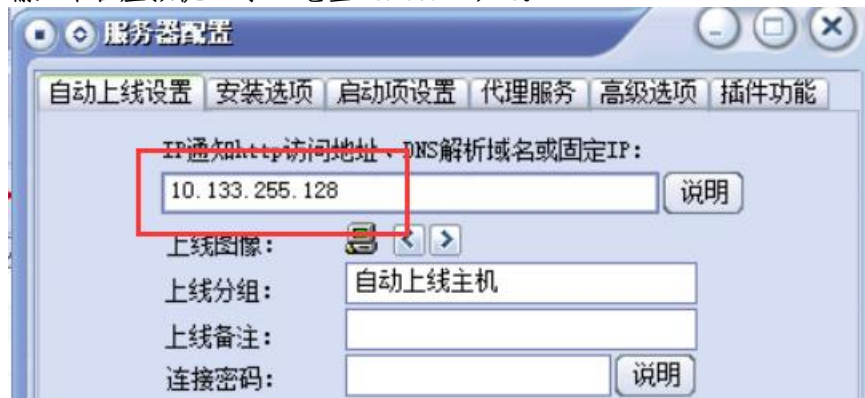
在虚拟机 1 运行黑防灰鸽子脱壳版。



点击“配置服务程序”。



输入本台虚拟机 1 的 IP 地址 10.133.255.128。



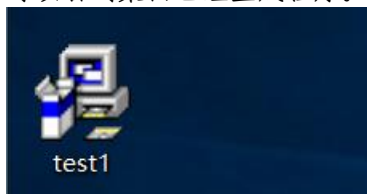
设置启动项设置。



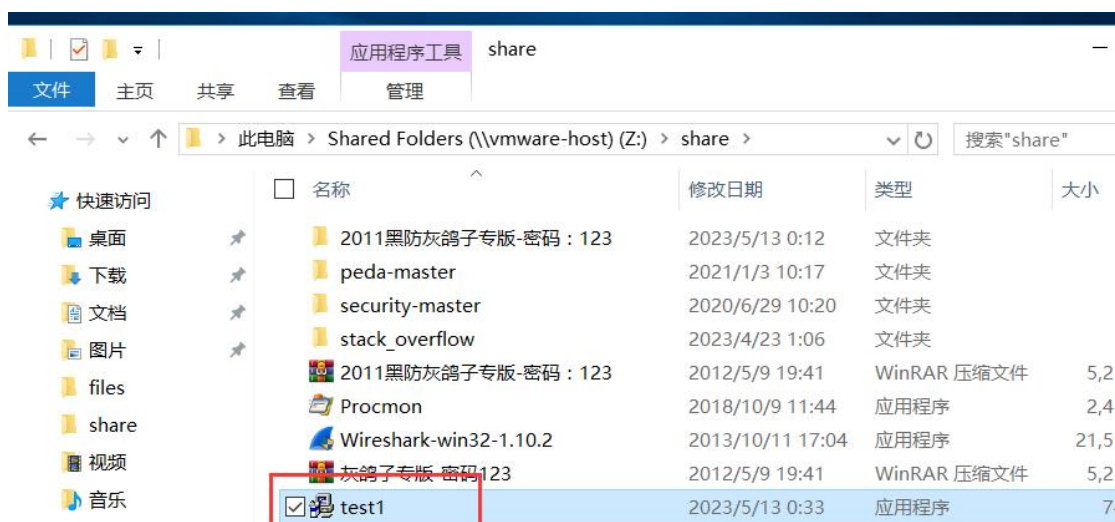
设置保存路径为桌面，再点击生成服务器。



可以看到桌面已经生成程序。



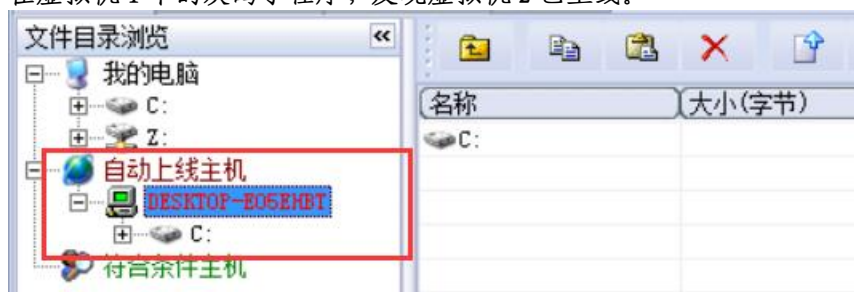
将该程序放在虚拟机 1 的共享文件夹中。



打开虚拟机 2 的共享文件夹，将木马程序放在桌面上并执行。



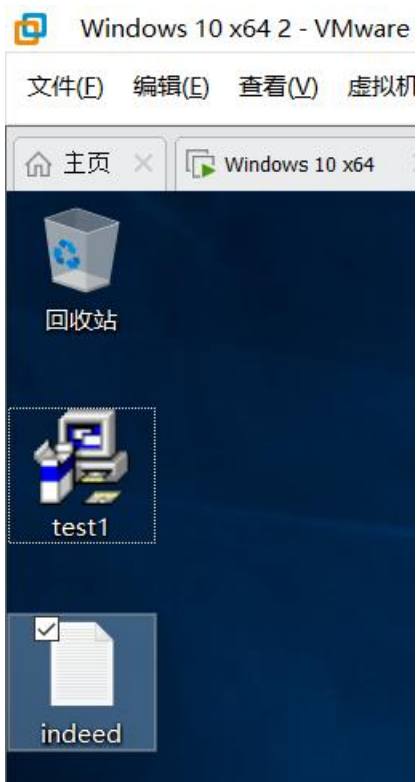
在虚拟机 1 中的灰鸽子程序，发现虚拟机 2 已上线。



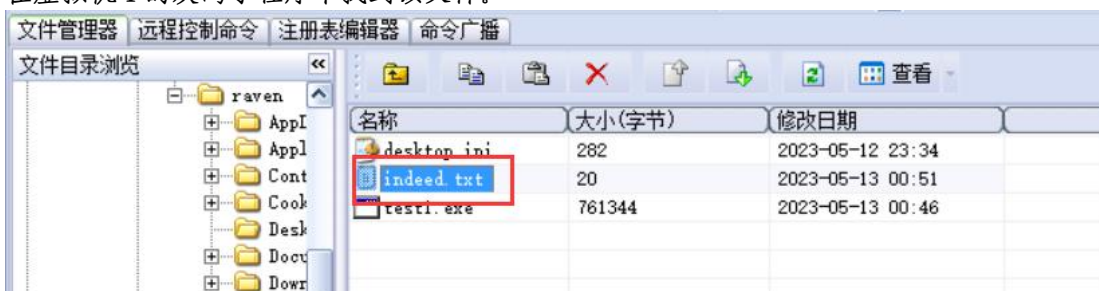
可以看到虚拟机 2 的磁盘内容。



在虚拟机 2 中添加一个 txt 文档。



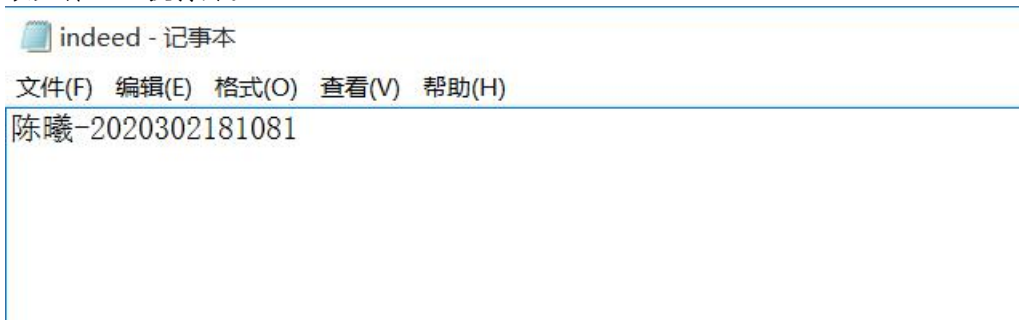
在虚拟机 1 中可以查看该文档内容。
在虚拟机 1 的灰鸽子程序中找到该文件。



选择本地打开。



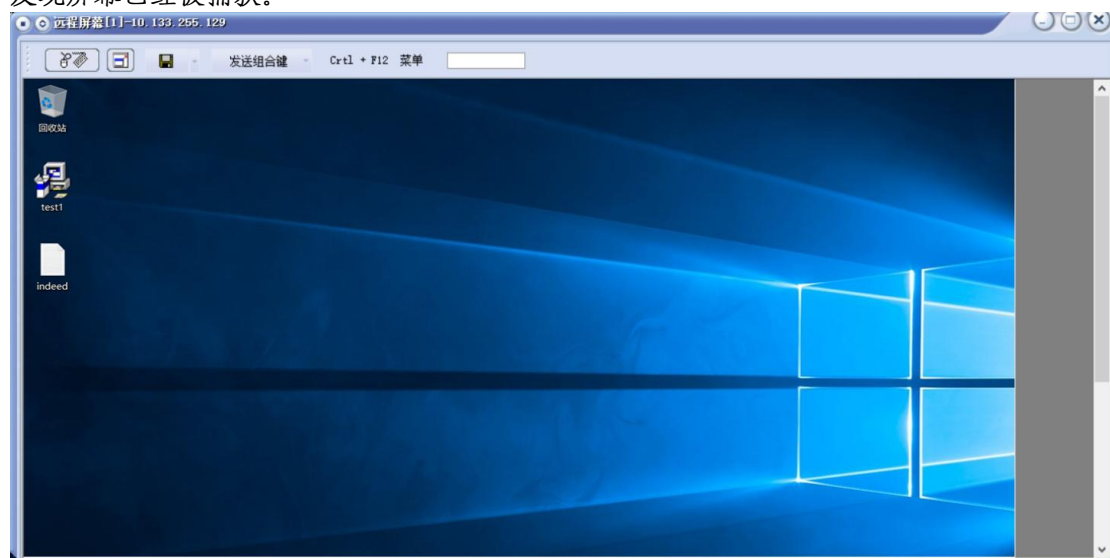
该文件已经被打开。



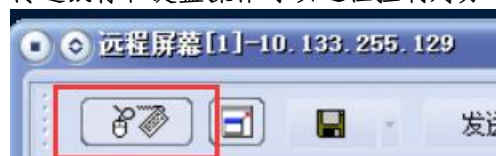
除此之外，还可以使用远程屏幕。
点击捕获屏幕。



发现屏幕已经被捕获。



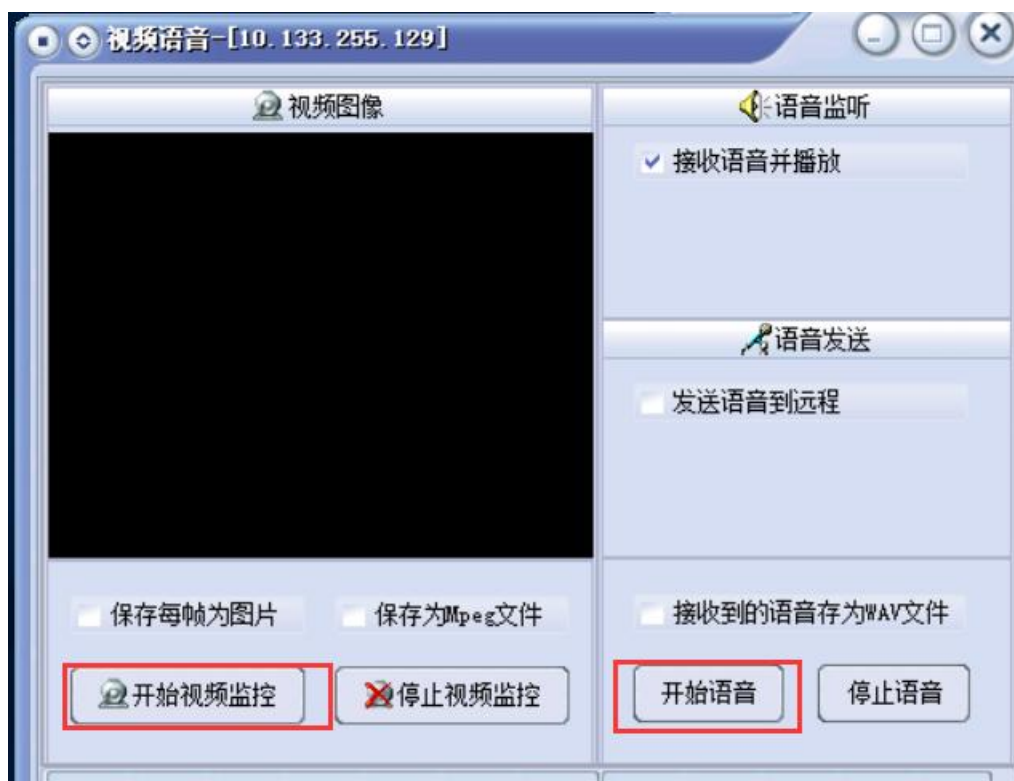
传送鼠标和键盘操作可以远程控制对方电脑。



点击视频语音可以打开对方的摄像头或者麦克风。



可以开始视频监控和语音。



使用 Telnet 可以使用目标主机的命令行工具。



输入 dir 可以看到对面的文件目录。

```
C:\>dir
dir
驱动器 C 中的卷没有标签。
卷的序列号是 D064-E9AC

C:\ 的目录
2015/07/10 19:04 <DIR> PerfLogs
2023/05/13 00:02 <DIR> Program Files
2015/07/10 19:04 <DIR> Program Files (x86)
2023/05/12 23:34 <DIR> Users
2023/05/13 00:48 <DIR> Windows
0 个文件 0 字节
5 个目录 50,031,271,936 可用字节

C:\>
```

也可以在桌面文件夹中看到虚拟机 2 中创建的 txt 文件。

```
C:\Users\raven\Desktop 的目录
2023/05/13 00:52 <DIR> .
2023/05/13 00:52 <DIR> ..
2023/05/13 00:51 20 indeed.txt
2023/05/13 00:46 761,344 test1.exe
2 个文件 761,364 字节
2 个目录 50,031,271,936 可用字节
```

也可以在目录下新建一个文件夹。

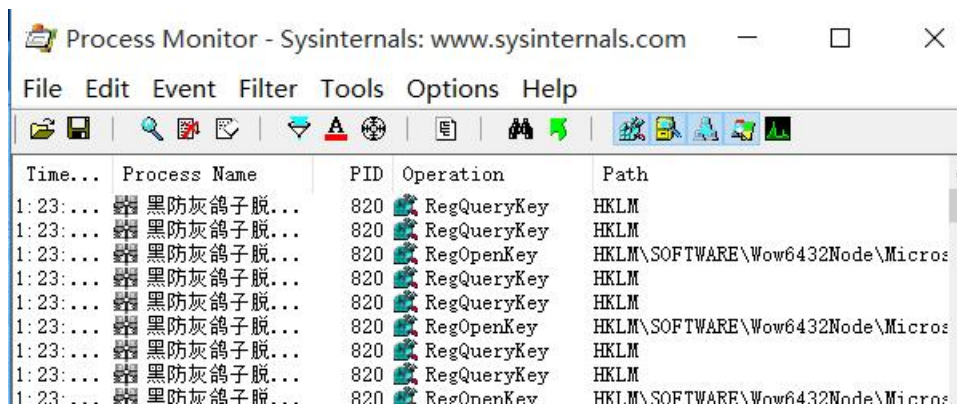
命令为 md cx。

```
C:\Users\raven\Desktop>md cx
md cx
```

在虚拟机 2 中查看桌面。发现 cx 文件夹已经被建立。



利用 Process Monitor 监控感染灰鸽子木马的被控端的文件行为和注册表行为。打开 Process Monitor 程序，在过滤器中过滤程序名包含灰鸽子的进程。

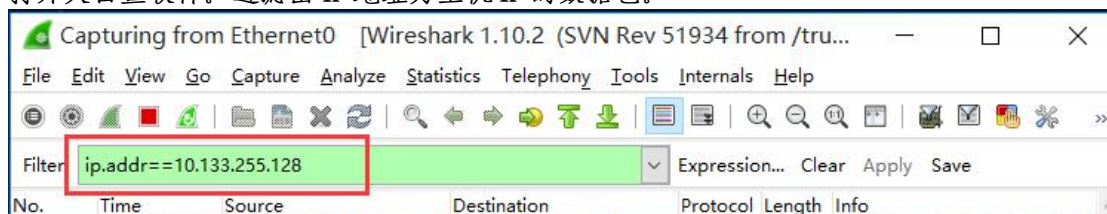


再过滤出口包包含 Server 的，观察注册表行为。

| | | | |
|------------|------|---------|---|
| server.exe | 2420 | 注册表-设置值 | HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed |
| server.exe | 2420 | 注册表-设置值 | HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed |
| server.exe | 2420 | 注册表-设置值 | HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed |
| server.exe | 2420 | 注册表-设置值 | HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed |
| server.exe | 2420 | 注册表-设置值 | HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed |
| server.exe | 2420 | 注册表-设置值 | HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed |
| server.exe | 2420 | 注册表-设置值 | HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed |
| server.exe | 4048 | 注册表-设置值 | HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed |

利用 Wireshark 监控灰鸽子木马与控制端的网络通信。

打开大白鲨软件。过滤出 IP 地址为主机 IP 的数据包。



查看数据包。这说明灰鸽子木马采用的是 TCP 协议进行的通信。

| | | | | | | |
|----|------------|----------------|----------------|------|-----|------------------------|
| 2 | 0.28163000 | 10.133.255.129 | 10.133.255.128 | TCP | 60 | 50063 > irdmi [ACK] Se |
| 3 | 0.28165600 | 10.133.255.128 | 10.133.255.129 | TCP | 66 | irdmi > 50063 [ACK] Se |
| 4 | 0.36318400 | 10.133.255.128 | 10.133.255.2 | NBNS | 110 | Refresh NB WORKGROUP<1 |
| 8 | 0.98438100 | 10.133.255.129 | 10.133.255.128 | TCP | 60 | 50086 > irdmi [ACK] Se |
| 9 | 0.98441500 | 10.133.255.128 | 10.133.255.129 | TCP | 66 | irdmi > 50086 [ACK] Se |
| 10 | 1.30026200 | 10.133.255.128 | 104.26.11.240 | TCP | 62 | 50404 > https [SYN] Se |
| 11 | 1.86325700 | 10.133.255.128 | 10.133.255.2 | NBNS | 110 | Refresh NB WORKGROUP<1 |
| 13 | 3.37923000 | 10.133.255.128 | 10.133.255.2 | NBNS | 110 | Refresh NB WORKGROUP<1 |
| 15 | 3.98474000 | 10.133.255.129 | 10.133.255.128 | TCP | 60 | [TCP Keep-Alive] 50086 |
| 16 | 3.98476700 | 10.133.255.128 | 10.133.255.129 | TCP | 66 | [TCP Keep-Alive ACK] i |
| 22 | 4.89435500 | 10.133.255.128 | 10.133.255.2 | NBNS | 110 | Refresh NB WORKGROUP<0 |
| 23 | 6.41042300 | 10.133.255.128 | 10.133.255.2 | NBNS | 110 | Refresh NB WORKGROUP<0 |
| 24 | 7.00059500 | 10.133.255.129 | 10.133.255.128 | TCP | 60 | [TCP Keep-Alive] 50086 |

提出灰鸽子木马的清除方案

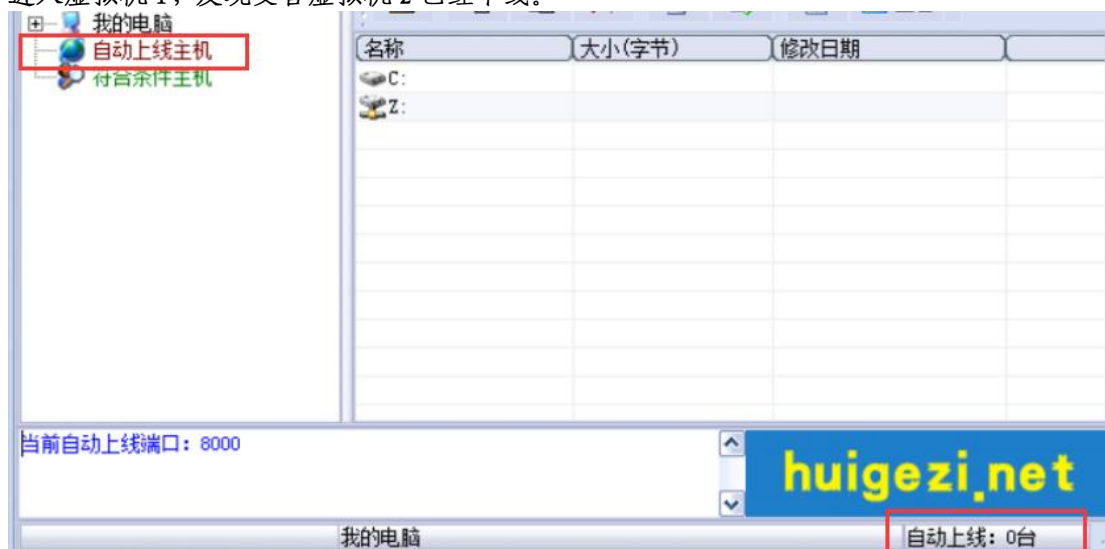
灰鸽子使用 Explorer 作为自己的隐藏进程。打开虚拟机 2 的任务管理器，终止该进程。

| | | | |
|---------------|-----------------|----|----------|
| vmtoolsd.exe | Administrator | 00 | 17,308 K |
| explorer.exe | Administrator | 00 | 9,572 K |
| wmiiprvse.exe | NETWORK SERVICE | 00 | 8,192 K |
| spoolsv.exe | SYSTEM | 00 | 6,728 K |
| wsentfy.exe | Administrator | 00 | 2,516 K |
| alg.exe | LOCAL SERVICE | 00 | 3,688 K |
| svchost.exe | LOCAL SERVICE | 00 | 4,544 K |
| svchost.exe | NETWORK SERVICE | 00 | 3,684 K |
| IEXPLORE.EXE | SYSTEM | 00 | 20,656 K |
| svchost.exe | SYSTEM | 00 | 18,572 K |
| svchost.exe | NETWORK SERVICE | 00 | 4,388 K |
| svchost.exe | SYSTEM | 00 | 4,948 K |

进入系统 C 盘目录，搜索服务端程序。

再将服务端程序删除。

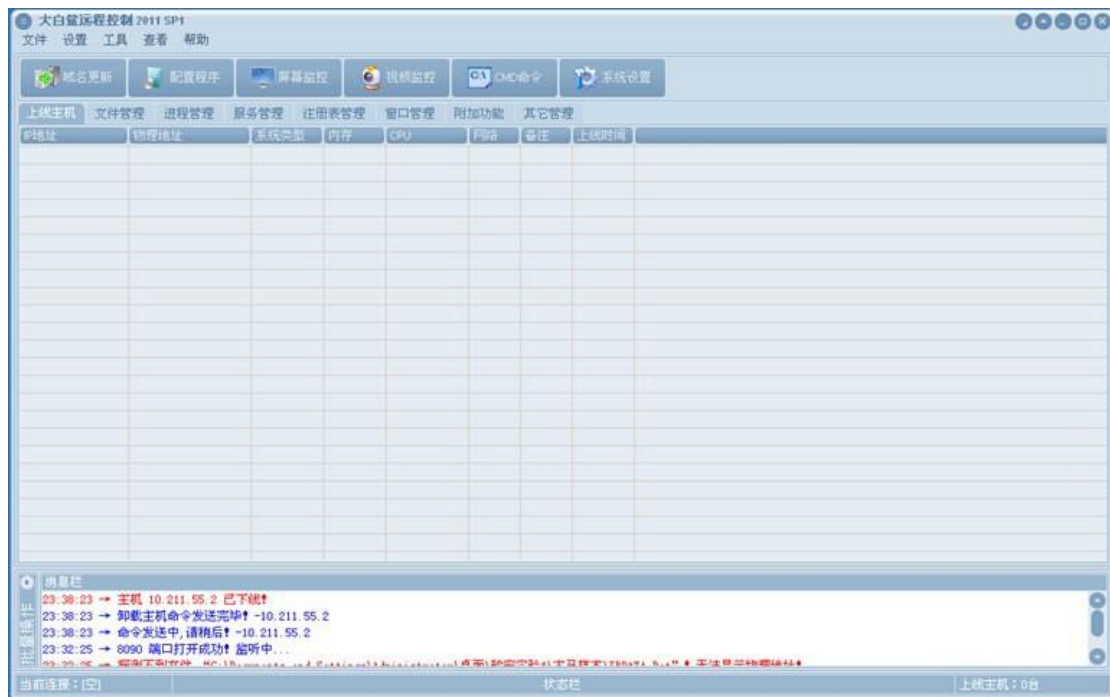
进入虚拟机 1，发现受害虚拟机 2 已经下线。



第五阶段：课后习题思考与实践

尝试对大白鲨木马或 PCShare 木马进行行为分析。

打开大白鲨木马主界面



木马配置方式与灰鸽子类似



配置完成后在受害机中安装，打开主机客户端，发现受害机上线。



使用 Process Monitor 监控木马进程，信息如下。

| | | | | | |
|------------|------|--|--|----|--|
| server.exe | 2252 | 关闭文件 | C:\WINDOWS\luiside.EXE | 成功 | |
| server.exe | 2252 | 注册表-创建项 | HKLM\SOFTWARE\Microsoft\DBS | 成功 | 访问期望: 允许的最大值 |
| server.exe | 2252 | 设置文件末尾信息-文件C:\WINDOWS\system32\config\software.LOG | | 成功 | 文件末尾: 20,480 |
| server.exe | 2252 | 设置文件末尾信息-文件C:\WINDOWS\system32\config\software.LOG | | 成功 | 文件末尾: 24,576 |
| server.exe | 2252 | 设置文件末尾信息-文件C:\WINDOWS\system32\config\software.LOG | | 成功 | 文件末尾: 28,672 |
| server.exe | 2252 | 设置文件末尾信息-文件C:\WINDOWS\system32\config\software.LOG | | 成功 | 文件末尾: 32,768 |
| server.exe | 2252 | 注册表-关闭项 | HKLM\SOFTWARE\Microsoft\DBS | 成功 | |
| server.exe | 2252 | 注册表-打开项 | HKLM\SOFTWARE\Microsoft\DBS | 成功 | 访问期望: 设置值 |
| server.exe | 2252 | 注册表-设置值 | HKLM\SOFTWARE\Microsoft\DBS\InstallTime | 成功 | Type: REG_SZ, 长度: 38, 数据: 2017-5-30 23:40:27 |
| server.exe | 2252 | 注册表-关闭项 | HKLM\SOFTWARE\Microsoft\DBS | 成功 | |
| server.exe | 2252 | 注册表-打开项 | HKLM\System\CurrentControlSet\Control\Session... | 成功 | 访问期望: 查询值 |
| server.exe | 2252 | 注册表-查询值 | HKLM\System\CurrentControlSet\Control\Session... | 成功 | 名称未找到, 长度: 16 |
| server.exe | 2252 | 注册表-关闭项 | HKLM\System\CurrentControlSet\Control\Session... | 成功 | |
| server.exe | 2252 | 查询-打开 | C:\WINDOWS\luiside.EXE | 成功 | 创建时间: 2017-5-30 23:40:27, 最后 |
| server.exe | 2252 | 查询-打开 | C:\WINDOWS\luiside.EXE | 成功 | 创建时间: 2017-5-30 23:40:27, 最后 |
| server.exe | 2252 | 创建文件 | C:\WINDOWS\luiside.EXE | 成功 | 访问期望: 读取数据/列出目录, 执行/写 |
| server.exe | 2252 | 查询标准信息-文件 | C:\WINDOWS\luiside.EXE | 成功 | 分配的大小: 118,784, 文件末尾: 118,784 |
| server.exe | 2252 | 注册表-打开项 | HKLM\System\CurrentControlSet\Control\Session... | 成功 | 访问期望: 查询值 |
| server.exe | 2252 | 注册表-打开项 | HKLM\System\CurrentControlSet\Control\Session... | 成功 | 访问期望: 查询值 |
| server.exe | 2252 | 注册表-查询值 | HKLM\System\CurrentControlSet\Control\Session... | 成功 | 名称未找到, 长度: 20 |
| server.exe | 2252 | 注册表-关闭项 | HKLM\System\CurrentControlSet\Control\Session... | 成功 | |

与灰鸽子类似，大白鲨也在系统盘复制了客户端程序。

使用 Wireshark 对大白鲨木马进行抓包，同样发现其采用的也是 TCP 协议。



清除大白鲨木马与灰鸽子无法删除不同，大白鲨可以直接删除客户端程序。但是进入主机客户端发现仍然能够控制受害机。打开进程管理器。发现存在一个名叫 userinit 的进程。

将其结束，回到主机服务端发现受害机已经自动下线。

4.5 实验体会和拓展思考

通过本次实验,我受益匪浅。我熟悉了虚拟机的操作,并学习了解了工具 Peocess Monitor, 大白鲨抓包工具, 灰鸽子木马程序的应用。并使用一个虚拟机 1 制作了木马, 安装在虚拟机 2 上, 并用虚拟机 1 实时检测虚拟机 2 的文件管理器。并且还可以使用键鼠控制虚拟机 2 的屏幕, 控制虚拟机 2 的摄像头和麦克风, 还可以使用命令行工具操作受害机虚拟机 2。

除此之外, 我也学习了作为受害机如何消除该木马的控制, 同时也学习了另一种木马软件大白鲨远程控制软件, 也学习了如何消除大白鲨木马的控制。我对计算机病毒的理解又更深了一层。