Win7靶机安装问题说明

1. Win7靶机的软件与资料从哪里获取？

答：部分在QQ群，完整的各种ISO在百度网盘。链接：https://pan.baidu.com/s/1DCazz69XEeYHTCVvss2riQ 提取码：n9b6

由于百度网盘可能存在下载限制，如果失效，提醒老师更新共享链接。可以在QQ群@5146279提醒。此次实验不需要提交完整版实验报告，在微助教提交实验截图与实验小结。

几个比较大的软件与ISO注意提前下载：

VC6.rar  
vs6sp5\_en.exe  
vcpp5.exe  
cn\_visual\_studio\_2010\_ultimate\_x86\_dvd\_532347.iso  
VS2010SP1dvd1.iso  
cn\_windows\_7\_ultimate\_with\_sp1\_x64\_dvd\_u\_677408原版!.iso  
尤其是Win7的ISO，比较大，需要大家提前下载。

1. 能否使用Windows8 Windows 10作为靶机环境？

答：可以。

1. 能否安装VS2013,VS2019代替VS2010?

答：可以。

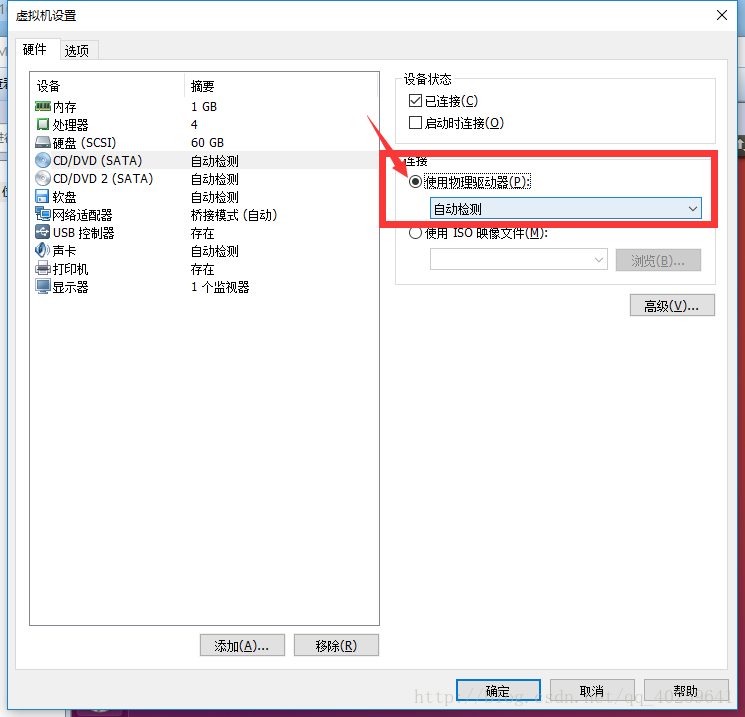
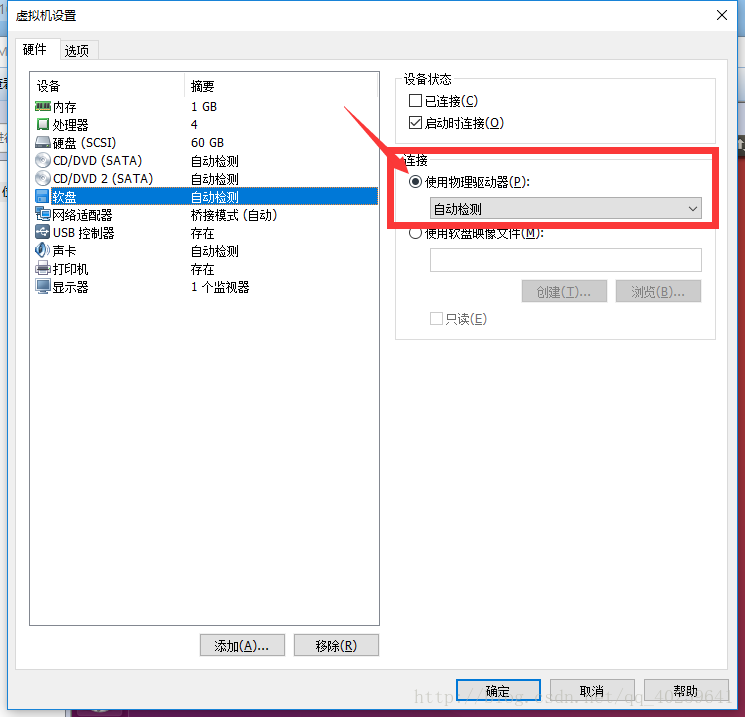
1. 病毒压缩口令到底是多少？

答：最外层的压缩口令是hust5146279,里面有好几个病毒样本的压缩包，请参照压缩包的文件名里面的提示，比如wannacry压缩包的口令为147147.

1. 我的VMWare无法安装VMWare Tools，菜单项为灰色。

答：原因是该VMware没有输入注册号或者没有输入正确的注册号，导致部分功能没法使用。可以按照课程提供的破解补丁或者序列号重新输入试试，百度网盘提供了VMware 12注册机，如果是VMWare15,请自己百度序列号。另外就是直接到VMWare网站下载VMWare Tools通过U盘拷贝到虚拟机进行安装。

如果已经注册，也输入了正确序列号，可能是虚拟的配置原因。先关闭虚拟机；.在虚拟机设置分别设置CD/DVD、CD/DVD2和软盘为自动检测三个步骤。再重启虚拟机试试。



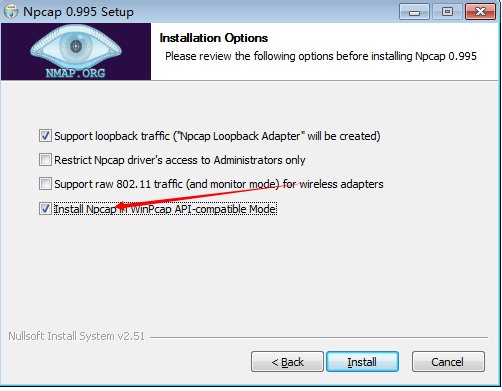
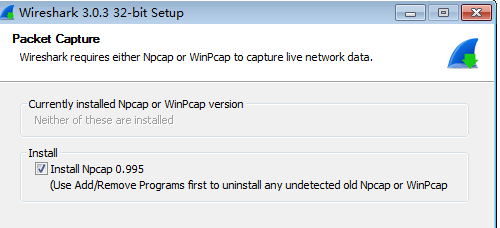
1. “5) 进入系统与安全，打开防火墙，尝试关闭某个应用程序通信，测试是什么效果。”具体如何认定？

答：可以在防火墙中增加一个出站规则，禁止浏览器访问外网，测试浏览器的禁止访问效果。



1. Wireshark无法找到监听接口？

答：原因是报文截获驱动没有正确安装。按照以下勾选：

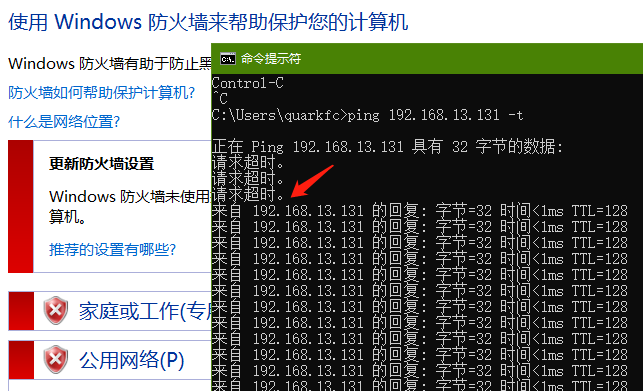


或者到<https://www.winpcap.org/install/default.htm下载winpcap>安装也可以。

注意，打开Wireshark以系统管理员身份打开。

1. “打开或者关闭Windows 7防火墙，同样监听，查看监听数据不同效果；”具体如何操作？

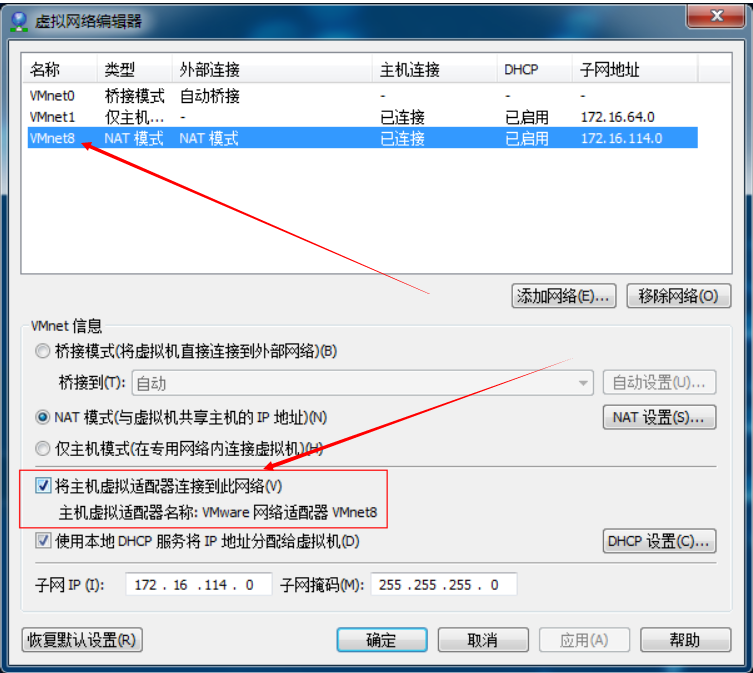
答：可以在虚拟机中，先获取其IP地址，比如：192.168.13.131,然后在外面的真实操作系统中，ping 192.168.13.131 -t，如果初始防火墙打开状态，然后关闭，可以观察到从超时到ping通的变化过程。如下图：



大家可以在Wireshark中查看ICMP ping报文的变化情况。

1. **我的虚拟机即使关闭防火墙，也无法从外部ping通啊!**

答：打开VMWare的虚拟网络编辑器，注意勾选以下配置。



1. “在win7防火墙打开或者关闭某个应用，同样监听，查看监听数据不同效果”具体如何操作？

答：可以在防火墙中增加一个出站规则，禁止浏览器或者其他网络应用访问外网，测试浏览器的禁止之前与禁止之后，截获的报文类型数量的差别。

1. 几个开发环境安装包到底什么关系？

答：VC6.rar是VC6的安装包，在Win7下面提示有兼容性问题，不用理会，只需要继续运行与安装，序列号填全1即可。如果安装完成后，可以新建工程编译，则不需要安装补丁包。如果有问题，则可以安装补丁包试试。补丁包有vs6sp5\_en.exe与vcpp5.exe

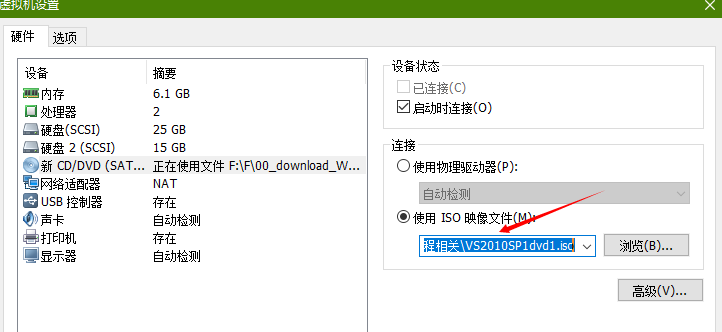
如果补丁安装还是无法编译生成exe，则需要安装VS2010，cn\_visual\_studio\_2010\_ultimate\_x86\_dvd\_532347.iso，如果装完可以正确编译，则不需要安装补丁包VS2010SP1dvd1.iso，否则建议把VS2010SP1dvd1.iso也安装好。

注意，安装VS2013,2016,2019都可以用。

1. ISO文件需要拷贝到虚拟机里面安装吗？

答：不需要，可以在虚拟机配置里面增加光驱，选择该ISO文件作为虚拟光驱，启动虚拟机，就可以打开该光驱安装文件。Setup.exe或者install.exe

注意：有些VMware版本对ISO文件名的长度有限制，无法打开，可以把ISO文件名改短，再装载为虚拟光驱即可。



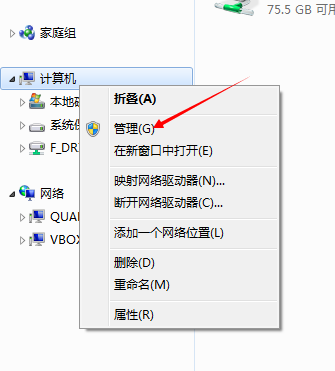
1. “以自己提出的数据恢复方案，测试数据恢复的有效性。” 到底如何恢复？

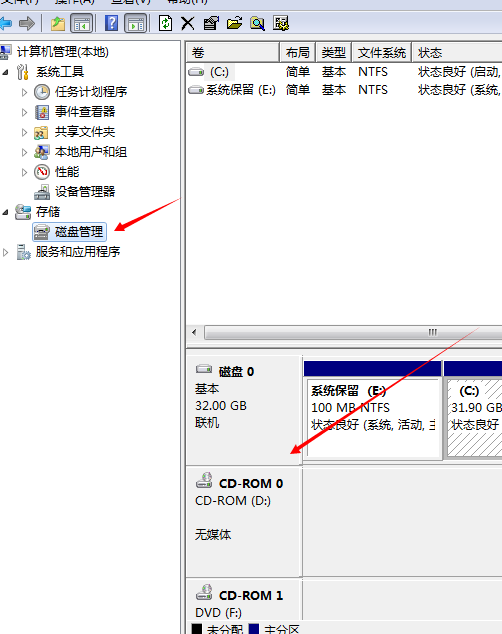
答：该项为选做任务，根据自己的情况决定是否实验，不作为考核要求。

1. “其它，比如是否对注册表做了修改等。”到底怎么做？

答：该操作没有约定具体步骤，一方面大家可以检查比如注册表的自启动位置是否增加了启动项，文件关联是否发生了变化等，另外一方面建议大家尝试网络资源搜索，比如以“WannaCry的深度分析”为关键字百度，会找到大量的相关资料。

1. “增加一个虚拟磁盘或者物理磁盘，查看虚拟机的状态变化；”，到底如何看？

答：在虚拟机配置里面增加磁盘，然后启动虚拟机，在虚拟机里面找到我的电脑，右键，进入到“管理”，点击磁盘管理，就看到新建的磁盘，截图。只有初始化 并新建分区后，才能到资源管理器看到该新建的磁盘。



1. VS2010中的对话框编辑器找不到啊？

