如何在windows系统中构建蜜罐 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/454/2021_2022__E5_A6_82_E4_BD_95_E5_9C_A8w_c100_454467.htm 搭建一个基于Unix系统的蜜罐网络相对说来需要比较多系统维护和网络安全知识的基础，但是做一个windows系统的蜜罐的门槛就比较低，今天我们就一起尝试搭建一个windows下的蜜罐系统。 由于win和Unix系统不一样，我们很难使用有效的工具来完整的追踪入侵者的行为，因为win下有各式各样的远程管理软件（VNC，remote-anything），而对于这些软件，大部分杀毒软件是不查杀他们的，而我们也没有象LIDS那样强大的工具来控制Administrator的权限，相对而言，蜜罐的风险稍微大了点，而且需要花更加多的时间和精力。 先介绍一下我们需要的软件 vpc Virtual pc，他是一个虚拟操作系统的软件，当然你也可以选择vmware. ActivePerl-5.8.0.805-MSWin32-x86.msi windows下的perl解析器 evtsys_exe.zip 一个把系统日志发送到log服务器的程序 comlog101.zip 一个用perl写的偷偷记录cmd.exe的程序，不会在进程列表中显示， 因为入侵者运行的的确是cmd.exe :) Kiwi_Syslog_Daemon_7 一个很专业的日志服务器软件 norton antivirus enterprise client 我最喜欢的杀毒软件，支持win2k server。 当然，如果你觉得其他的更加适合你，你有权选择 ethereal-setup-0.9.8.exe Ethereal的windows版本，Ethereal是*nix下一个 很出名的sniffer，当然，如果你已经在你的honeynet中布置好了 sniffer,这个大可不必了，但是本文主要还是针对Dvldr 蠕虫的，而且ethereal的 decode功能很强，用他来获取irc MSG很不错的 WinPcap_3_0_beta.exe ethereal需要

他的支持。 md5sum.exe windows下用来进行md5sum校验的工具 windows 2000 professional的ISO镜象 用vpc虚拟操作系统的时候需要用到他 Dvldr蠕虫简介 他是一个利用windows 2000/NT弱口令的蠕虫。该蠕虫用所带的字典暴力破解随机生成的ip的机器，如果成功，则感染机器，并植入VNC修改版本，并向一个irc列表汇报已经感染主机的信息，同时继续向其他机器感染。可以访问郑州大学网络安全园或者关于他更详细的信息。 一：安装一个win2k pro，具体的安装方法本文就省略了，打上所有的补丁，只留一个漏洞，就是dvldr蠕虫需要的administrator的空密码。 二：安装norton antivirus enterprise client，升级到最新的病毒库，并启动实时监控 三：用cmdlog替换cmd.exe程序，把comlog101.zip解压缩后有五个文件cmd.exe，cmd101.pl，COMLOG.txt，MD5.txt，README.txt，其中cmdlog.txt和readme.txt都是说明文件，md5.txt包含这五个文件的md5校验和的值，我们可以使用md5sum.exe工具来检测一下他们是否遭受修改D:comlog101>md5sum.exe * md5sum.exe: .: Permission denied md5sum.exe: ..: Permission denied f86ba5ffaa8800a2efa9093d2f11ae6f *cmd.exe 484c4708c17b5a120cb08e40498fea5f *com101.pl 001a6f9ca5f6cf01a23076bad9c6261a *comlog.txt 121bf60bc53999c90c6405440567064b *md5.txt eb574b236133e60c989c6f472f07827b *md5sum.exe 42605ecfa6fe0f446c915a41396a7266 *README.TXT 把这些数字和md5.txt的数字对比，如果出现不一致，就证明程序遭受修改，请勿使用。 在校验无误之后，我们开始覆盖系统

的cmd.exe.先打开资源管理器>工具>文件夹选项>查看，把"隐藏受保护的操作系统文件"的钩去掉，并选择"显示所有文件和文件夹">确定，然后去到C：WINNTsystem32dllcache目录，并找到cmd.exe，并把他改名成cm_.exe，再把comlog101下的cmd.exe和com101.pl复制到这里，并把C：WINNTsystem32下的cmd.exe也改成cm_.exe，同样把comlog101目录下的cmd.exe和com101.pl复制到这里。在这段时间，系统会提醒你系统文件遭到修改，问你是否修复，选择取消就可以了。然后在C：WINNTHelp目录下建一个叫"Tutor"的目录，这里是用来放cmd.exe的命令记录的地方，当然你同样可以修改com101.pl来选择日志的存放位置。 现在我们运行cmd.exe，你会发现窗口一闪而过，这是因为我们还没装perl解析器。运行ActivePerl-5.8.0.805-MSWin32-x86.msi，一路next就OK了。 现在我们运行cmd.exe，这回我们可爱的cmd窗口就跳出来了，随便敲几个东西进去，然后去到C：WINNTHelpTutor目录下，你就可以看到记录了。为了避免记录自己在cmd.exe的操作，我们可以把原来的cmd.exe改成另外一个名字来执行。 四：安装日志服务器，我们选择Kiwi的Syslog Daemon 7是因为他够专业并且有很多统计信息和支持产品，一路next并启动服务即可。 netstat -an我们可以看到514端口 UDP 0.0.0.0：514 *：* 五：安装evtsys_exe，解压缩之后有两个程序evtsys.exe和evtsys.dll，同样需要检测文件是否被修改D:evtsys_exe>md5sum.exe * md5sum.exe: .: Permission denied md5sum.exe: ..: Permission denied f5ba9453e12dc030b5e19f75c079fec2 *evtsys.dll dcc02e429fbb769ea5d94a2ff0a14067 *evtsys.exe

eb574b236133e60c989c6f472f07827b *md5sum.exe 如果一切正常的话，执行evtsys.exe /？D:evtsys_exe>evtsys.exe /? Usage: evtsys.exe -i|-u|-d [-h host] [-p port] [-q char] -i Install service (安装服务) -u Uninstall service (卸载服务) -d Debug: run as console program (以debug模式运行) -h host Name of log host (日志服务器IP地址) -p port Port number of syslogd (日志服务器端口，默认是514) -q char Quote messages with character Default port: 514 我们运行D：evtsys_exe>evtsys.exe -h 日志服务器IP -i来安装服这样你系统的应用程序日志，系统日志，安全日志都会发到日志服务器去了，这样我们就可以更加真实的了解到系统的运行情况。 六：安装WinPcap_3_0_beta.exe 和ethereal-setup-0.9.8.exe 下面针对本案例大概的说说ethereal的使用 先启动ethereal capture->start capture packets in promiscuous mode 不选这个，因为我们只需要得到本机的信息，不需要以混杂模式运行 filter filter name：irc string：ip host urip and tcp port 6667 只能有一条规则，但是可以使用逻辑符号 否定（`！ or `not） 交集（`amp. or `and） 并集（`|| or `or） 还有=，>=，，&amp.等等 更加详细的设置请查看ethereal的manual 先自己测试一下sniffer是否工作 连接上IRC，并发言，我们可以看到一些结果 然后选择一个记录，并且按“ follow tcp stream ”就可以查看IRC的聊天内容了 七：安装设置绿色警戒防火墙 关闭“ 进入请求通知 ”，开放共享，把所有的入侵检测对策的“ 拦截 ”都改成“ 警告 ”，警告级别都改成“ 记录 ”，我们主要是想了解一下大概的攻击情况 接着打扫战场，把你下载的软件，临时文件，历史记录，文档的记录全部删除，但是别忘记用regsnap做个镜象哦，最后再次开启ethereal 现在剩下

的就是等蠕虫感染来了……