利用虚拟机搭建安全的木马及病毒测试系统

秦　光

(西昌学院　信息技术系，四川　西昌　615013)

【摘　要】网络安全十分重要，对网络中的木马及病毒进行安全测试，搭建一个安全的测试系统十分重要，本文探讨一种采用虚拟机技术来构建安全的木马及病毒测试系统的方法。

【关键词】网络安全；虚拟机；木马；病毒

【中图分类号】TP393.08　　【文献标识码】B　　【文章编号】1673-1891(2007)01-0054-03

1 引言

由于防毒软件有相对的滞后性，在网络中下载一个共享软件或木马及病毒样木，如何判断它是不是木马及病毒呢？因为网络安全的原因，一般单位的局域网禁止用于木马及病毒测试，普遍采用的方法是利用几台服务器与 PC 来搭建局域网，组成一个测试系统。由于需要评测木马及病毒对不同操作系统的影响程度，所以需要的设备较多，搭建这样的系统成本较高；另外由于是对木马、病毒进行测试，多种原因常常造成系统崩溃而无法运行，需要不断重新安装操作系统等软件，这对于木马及病毒测试工作人员而言，工作量大，甚至影响正常测试。

如何建立一个价格便宜，操作方便，使用安全的木马及病毒测试系统呢？这是一个值得探讨的问题，由于虚拟机技术越来越成熟，利用虚拟机技术，可以搭建一个安全的木马及病毒测试系统。

2 木马及病毒分析者的测试方法[1]

木马及病毒分析者拿到一个测试样本时，并不敢直接运行它，因为它可能是带毒的，而且极可能是未知的，谁也无法查杀的新病毒。要分析它，必须做的是跟踪它的执行，查看它是否有传染模块，是否有破坏模块。如果一个样本中有用于传染的模块，就认定它是病毒，如果它还有破坏模块，将它归入恶性病毒，有些病毒是戏剧性的、学术性的，不会破坏系统，归入普通病毒。

这里涉及到一个重要问题，判定样本是否是病毒的重要问题：传染性。如果能让程序判定一个‘样本’是否有传染性，也就解决了反病毒领域中的一个重要难题‘预警’。传统的程序员分析病毒会使用 DOS 的 DEBUG 程序，现在更多的人选择 SOFT-ICE 一类功能更强大的软件。但终归一点，这类动态调试软件的核心就是单步跟踪执行被调程序的每一个语句。事实上，更为具体的做法可以是这样：用程序代码虚拟一个 CPU 来，同样也虚拟 CPU 的各个寄存器，甚至将硬件端口也虚拟出来，用调试程序调入被调的‘样本’，将每一个语句放到虚拟环境中执行，这样我们就可以通过内存和寄存器以及端口的变化来了解程序的执行。这样的一个虚拟环境就是一个虚拟机。

既然虚拟机中可以反映程序的任何动态，那么，将病毒放到虚拟机中执行，则病毒的传染动作一定会被反映出来。虚拟机用来侦测已知病毒速度更为惊人，误报率很低！这项技术被认为是国际反病毒领域的前沿技术，至今仍有许多人在研究和完善它。

3 用虚拟机软件构建木马及病毒测试系统

3.1 虚拟机软件

虚拟机软件可以在一台电脑上模拟出来若干台 PC，每台 PC 可以运行单独的操作系统而互不干扰，可以实现一台电脑‘同时’运行几个操作系统，还可

收稿日期：2006-12-15

作者简介：秦光(1973-　)，男，讲师，软件工程硕士，主要从事计算机课程的教学及网络管理工作。

以将这几个操作系统连成一个网络。

使用虚拟机构建木马及病毒测试系统，因为是采用软件来实现，有以下几个好处：

() 可同时在同一台电脑上运行多个操作系统。不用虚拟机的话，有两个办法：一是装多个硬盘，每个硬盘装一个操作系统，这个方法比较昂贵。二是在一个硬盘上装多个操作系统，这个方法不够安全，因为硬盘 MBR 是操作系统的必争之地，搞不好会几个操作系统同归于尽。而使用虚拟机来构建木马病毒测试系统既省钱又安全。

() 在虚拟机中测试运行，可设置还原点，将所做的任何操作都即时保存，如果需要，可以还原至任意的还原点，不必繁琐的重新安装操作系统。例如中马后可还原至中马前的状态。

() 可作为任何软件的测试环境，在虚拟机内运行木马与病毒样本，可以做到完全不影响实体电脑，十分安全。

3.2 常用的虚拟机软件[2] VMWare 与 Virtual PC

常用的虚拟机软件较多，有 Windows 平台的，也有 Linux 平台的，较为著名的有 VMWare 与 Virtual PC，二者的主要区别有：

() VMWare 没有模拟显卡，要通过 VMWare – tools 才能用上高分辨率和真彩色，否则只能用 VGA。而 Virtual PC 模拟了一个比较通用的显卡 S3 Trio 32/64(4M)。

() 因为 Virtual PC 模拟了显卡，所以通用性很强。connectix. com 网站声称，目前新版的 Virtual PC 5 支持所有基于 x86 的操作系统。

() Virtual PC 的网络共享方式与 VMWare 不同。VMWare 是通过模拟网卡实现网络共享的，而 Virtual PC 是通过在现有网卡上绑定 Virtual PC emulated switch 服务实现网络共享的。对于 win2000/xp 等操作系统，如果网线没插或没有网卡的时候，要安装 Microsoft 的 loopback 软网卡，才能实现网络共享。在 Virtual PC 的 global setting 里，当有网卡并插好网线的时候，将 Virtual switch 设成现实的网卡；当没有网卡或网线没插的时候，将 Virtual switch 设成 ms loopback 软网卡，即可实现网络共享。

3.3 采用虚拟机软件搭建测试平台

首先在测试者的主机中安装虚拟机软件，虚拟机软件安装十分简单，下面以 VMWare 为例进行介绍。安装时直接点击 “Next ”即可完成安装，安装完成后，计算机中多了两块虚拟网卡，如图 1 所示，在 VMWare 下用户可使用虚拟网卡进行联网测试。

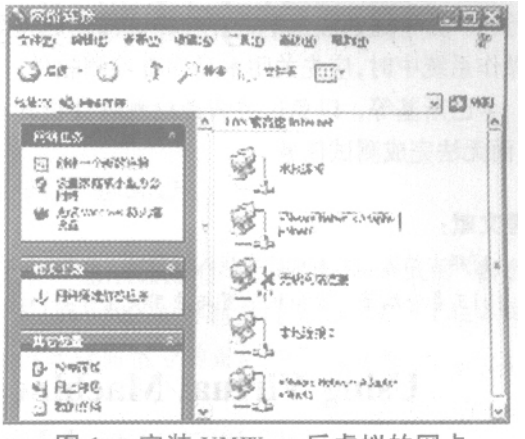

图 1　安装 VMWare 后虚拟的网卡

接下来再安装测试样本的操作系统，如安装 Windows 2003，然后将测试样本放入操作系统中，用测试软件进行分析测试。下面用在虚拟机中模拟 ARP 攻击为例进行介绍，在测试主机中安装一个防止 ARP 攻击的软件，如 ArpFix_Beta_1.6，在虚拟机中通过网络下载软件 ‘网络执法官 ”，安装后运行，然后对测试主机进行 ARP 攻击——禁止与所有主机相连，如图 2 所示。

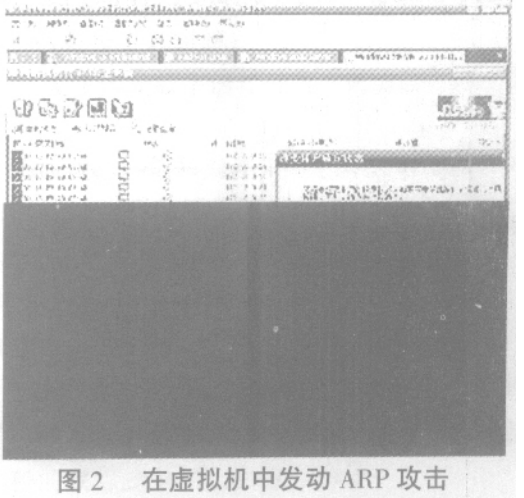

图 2　在虚拟机中发动 ARP 攻击

在测试主机用 Arpfix 软件检测到虚拟机对它的 ARP 攻击，如图 3 所示。

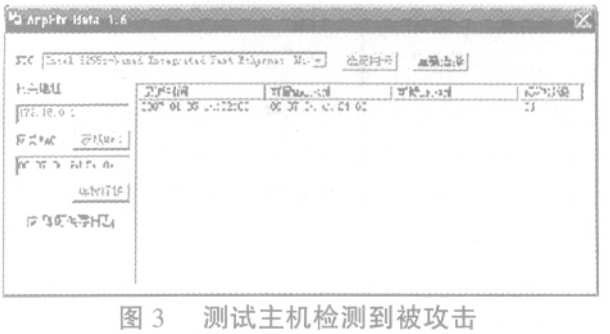

图 3　测试主机检测到被攻击

在木马与病毒的测试过程中，需要随时注意先

建立快照，即创建还原点，以便在测试过程中随时进行还原。另外还需注意的是在将测试样本放入虚拟机操作系统中时，应先关闭木马病毒检测软件，如瑞星、卡巴斯基等，以免这类病毒检测软件将样本清除，而无法完成测试任务。

4 总结

采用虚拟机技术来构建木马及病毒测试系统的方法具有安全，操作方便，系统搭建价格便宜。在实际的木马及病毒测试中，使用效果良好。

参考文献：

[1]邓吉编著．黑客攻防实战入门[M]．北京：电子工业出版社，2004.

[2]王春海编著．虚拟机配置与应用完全手册[M]．人民邮电出版社，2003.

Using Virtual Machine to Build Security Trojan Horse and Virus Test System

QIN Guang

(Engineering and Technology Department of Xichang College, Xichang, Sichuan 615013)

Abstract: The network security is extremely important. Carrying out the security testing to the network's Trojan horse and the virus, building a safe test system is also extremely important. This paper discusses how to use the virtual machine technology to construct the security the Trojan horse and the virus test system.

Key words: Network security; Virtual machine; Trojan horse; Virus

(责任编辑：张荣萍)

(上接53页)

Abstract: The Serial softwares of FLASH are the popular flat – animation softwares all over the world. Based on the analysis of FLASH Classical examples, the paper dicusses how to finish malcing Flash animation by using existing elements in FLASH softwares and creative techniques.

Key words: FLASH; Creative techniques；Vector；Increase

(责任编辑：张荣萍)