文章编号: 1001- 2486(2008) 03- 0065- 05

基于欺骗的网络主动防御技术研究*

姚 兰, 王新梅
(西安电子科技大学 ISN 国家重点实验室, 陕西 西安 710071)

摘 要: 针对网络对抗和计算机网络安全防护的现实需求, 提出了一种在分布式欺骗空间中实施多重欺骗的网络主动防御技术, 通过仿真常用的网络服务程序以及伪造安全漏洞来诱骗入侵者, 利用内核级操作控制、文件系统镜像和信息欺骗, 构建基于 Windows 和 Linux 平台的欺骗性操作环境, 实现了对网络入侵全过程的欺骗、监视与控制。该技术突破了普通蜜罐技术单一欺骗层次的局限性, 使得欺骗性、交互性和安全性同时得到明显提高。

关键词: 网络欺骗; 主动防御; 蜜罐; 网络服务仿真; 操作行为控制
中图分类号: TP393. 08 文献标识码: A

A Study on the Network Active Defense Technology Based on Deception

YAO Lan, WANG Xin-mei
(ISN Key National Laboratory, Xidian Univ., Xi' an 710071, China)

Abstract: A network active defense technology based on multi-layers deception in the distributed deception space is proposed to meet the needs of network countermeasure and network security. This technology simulates usual network service programs and forges vulnerabilities to lure the intruder. With operation control at kernel level, file system mirror and information deception, it creates the deceiving operating environment on the platform of Windows and Linux. Thus the process of intrusion is fully deceived, monitored and controlled. This technology breaks the limitation of a single layer deception used by other general honeypots, and obviously promotes the level of deception, interaction and ensures security.

Key words: network deception; active defense; honeypot; network service simulation; operation control

由防火墙、入侵检测、防病毒等常规技术手段构建的信息安全防御体系是处于被动防御状态的, 不适应网络安全面临的新形势和网络对抗的需要。近几年, 一种新的信息安全防护理念正逐渐成为国内外研究的热点, 这就是网络欺骗安全防护技术[1-2]。常规的网络安全防护技术主要是从正面抵御网络攻击, 网络欺骗则是旁路引导。它通过吸引网络入侵、消耗攻击者的资源来减少网络入侵对真实系统的威胁, 从而赢得时间与信息去增强安全防护策略与措施, 因此能够弥补传统网络防御体系的不足, 与其他多种网络安全防护技术相结合, 互为补充, 共同构建多层次的信息安全保障体系。

在目前的网络欺骗技术中, 欺骗性与安全性不能两全, 成为核心问题之一[3]。传统的蜜罐主要采用守护程序调用配置文件的方式, 模拟网络服务和安全漏洞来吸引入侵者, 例如 Honeyd[4-5] 和 Specter[6]。该技术安全风险小, 但是伪装初级, 易于识别。高交互型蜜罐如 Mantrap[7], 则通过修改操作系统内核, 建立"牢笼"环境, 能提供真实的网络服务, 欺骗性好, 但实现难度大, 所以只支持特定的操作系统。蜜网项目组提出的蜜网技术[8], 直接利用真实的网络系统来实现欺骗, 同时辅助以安全措施。由于其维护困难, 安全风险高, 因此主要用于研究目的。据此, 本文提出了一种基于欺骗的网络主动防御技术, 它基于深度欺骗策略, 对入侵行为实施层层深入的欺骗与控制, 突破了普通蜜罐技术欺骗层次单一的局限性, 使欺骗性、交互性和安全性得到明显提高。

* 收稿日期: 2007- 12- 20
基金项目: 国家 863 计划重大专项资助项目(2003AA146010)
作者简介: 姚兰(1973—), 女, 博士生。

1 多重欺骗与控制架构

根据入侵行为与被攻击对象的交互过程, 可以将网络欺骗分成 4 个纵深层次, 如图 1 所示, 依次为网络服务欺骗、安全漏洞欺骗、操作系统级欺骗和文件系统欺骗。

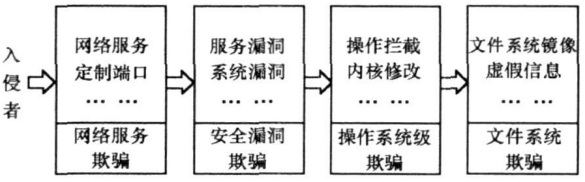


图 1 欺骗控制的纵深层次

Fig. 1 Layers of deception and control

网络服务欺骗通过对外提供网络服务(例如 Web、FTP、Telnet 等)来吸引入侵者。所提供的网络服务可以是默认安装的真实服务, 也可以是模拟服务, 甚至是虚假服务。网络服务欺骗还可以通过定制网络端口来实现, 通常是模拟某个木马程序, 以造成被木马植入的假象。

安全漏洞欺骗通过故意暴露安全弱点作为诱饵, 漏洞可来源于操作系统、应用服务和通信协议等方面。真实的安全漏洞不易控制, 必须建立全方位的安全措施; 虚假的安全漏洞易于控制, 安全性高。

操作系统级欺骗是指通过对操作系统内核进行必要的修改或拦截系统调用, 以监视和控制入侵行为, 这是建立中高交互的安全的欺骗环境的前提。

文件系统欺骗是欺骗控制的最深层次。通过建立虚拟文件系统, 来保护主机的文件系统不被入侵者破坏, 同时又不阻止入侵者的文件访问操作。进一步地, 产生有针对性的假信息, 来欺骗入侵者。

本文采用多层次的欺骗与控制的设计思路, 通过仿真常用的网络服务程序以及伪造安全漏洞来诱骗入侵者, 利用内核级操作控制、文件系统镜像和信息欺骗, 构建基于 Windows 和 Linux 平台的可控操作环境, 实现对网络入侵全过程的欺骗、监视与控制。这种层层递进的欺骗与控制体现了深度欺骗的思想, 引导入侵者按照设定的路线一步步地进入欺骗环境, 尽量延长入侵者在系统中停留的时间。

2 网络服务仿真与安全漏洞伪造

通过仿真常用的网络服务程序, 结合伪造的安全漏洞, 作为实施欺骗的诱饵。与目前普遍采用的守护程序调用特征配置文件的欺骗技术不同, 仿真服务能够实现正常的网络服务, 能产生与真实服务和漏洞完全一致的访问、扫描与攻击过程, 提高了交互性和欺骗性。相比利用真实服务和漏洞的欺骗技术, 其优点在于仿真程序完全可控, 能够有效地全程监视和控制攻击行为, 使得网络入侵按照可控的、预定义的轨道进行, 从而大幅度降低了欺骗系统的安全风险。

2.1 网络服务仿真

网络服务仿真是对真实网络服务程序的模拟, 例如模拟微软公司的 Internet Information Server(简称 IIS)服务程序, 任何人通过浏览器就能够访问该服务。仿真程序实现了与真实服务程序相同的功能与指令, 进一步添加了欺骗与控制措施, 包括伪造旗标版本信息, 伪造本地日志并且异地保存真实日志, 提供安全漏洞伪造扩展接口以及嵌入网络服务级的入侵检测扩展接口等。

2.2 安全漏洞伪造

安全漏洞伪造, 包括欺骗网络扫描器和欺骗攻击工具两部分内容。一方面, 要使伪造安全漏洞的表现信息与真实漏洞无异; 另一方面, 还要能控制入侵行为, 将其重定向至可控操作环境, 确保系统安全性。网络扫描器通常以请求/应答的方式获取信息, 并基于特征匹配技术来判断目标是否存在安全漏洞。为了欺骗扫描器, 首先需要建一个漏洞特征表, 以建立接收特征码与发送特征码的对应关系。考虑到不同的网络扫描器提取的特征信息有所差异, 需要为不同的网络扫描器定制相应的应答信息。当服务器接收到请求信息时, 会将其与漏洞特征表进行比较。如果请求信息不是漏洞扫描探测, 则执行正常的网络访问操作, 如果属于漏洞扫描探测, 则返回相应的漏洞特征码, 从而达到欺骗扫描器的结果。以“远程. printer 缓冲区溢出漏洞”为例, 建立漏洞特征列表, 如图 2 所示。

对攻击工具的欺骗基于类似的原理。通过截获攻击信息加以分析, 建立数据列表, 维护不同攻击工

ID	code_receive
10	GET /.printer HTTP/1.0
11	HEAD /NULL.printer HTTP/1.0
12	GET /NULL.printer HTTP/1.0
13	HEAD /.printer HTTP/1.0
18	GET /.printer HTTP/1.1
19	HEAD /NULL.printer HTTP/1.1
20	GET /NULL.printer HTTP/1.1
21	HEAD /.printer HTTP/1.1

(1) 扫描器的请求特征信息

code_send
HTTP/1.1 500 13$Server: Microsoft-IIS/5.0$Date: #$内容类型: text/html$$Web 打印机安装出错。$
HTTP/1.1 500 13$Server: Microsoft-IIS/5.0$Date: #$内容类型: text/html$$Web 打印机安装出错。$
HTTP/1.1 500 13$Server: Microsoft-IIS/5.0$Date: #$内容类型: text/html$$Web 打印机安装出错。$
HTTP/1.1 500 13$Server: Microsoft-IIS/5.0$Date: #$内容类型: text/html$$Web 打印机安装出错。$
HTTP/1.1 500 13$Server: Microsoft-IIS/5.0$Date: #$内容类型: text/html$$Web 打印机安装出错。$
HTTP/1.1 500 13$Server: Microsoft-IIS/5.0$Date: #$内容类型: text/html$$Web 打印机安装出错。$
HTTP/1.1 500 13$Server: Microsoft-IIS/5.0$Date: #$内容类型: text/html$$Web 打印机安装出错。$
HTTP/1.1 500 13$Server: Microsoft-IIS/5.0$Date: #$内容类型: text/html$$Web 打印机安装出错。$

(2) 服务器的应答特征信息

图 2　漏洞特征列表

Fig. 2　Vulnerability signature list

具针对不同安全漏洞的攻击特征、服务器应答信息和攻击结果。当服务器接收到请求信息时,会将其与攻击特征列表进行比较。如果请求信息不是漏洞攻击,则执行正常的网络访问操作; 如果属于漏洞攻击,则执行进一步的欺骗操作: 返回攻击失败的结果或者返回攻击成功的结果,进而将攻击重定向至可控操作环境。

3　建立可控操作环境

系统必须在提供欺骗的同时对入侵行为进行控制,确保其不会损害真实主机或网络的安全。内核级的操作控制是其中的关键,它通过拦截到内核的系统调用,或替换相应的系统调用,将入侵行为导入一个特定的逻辑区域中,从而建立中高交互的安全的欺骗环境。

3.1　内核级操作控制

与操作系统内核交互的行为都发生在用户空间,例如进程启动或指令执行。几乎所有的网络应用,包括 WWW、DNS 和 FTP,均在用户空间操作。因此,可从用户空间实现指令或应用对内核交互行为的拦截,从而达到控制对入侵行为的目的。

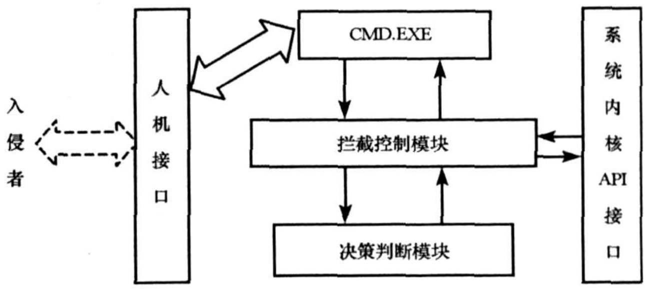


图 3　CMD 至内核的系统调用拦截

Fig. 3　System calls interception from CMD to kernel

对于 Windows 操作系统,最基本的需要是拦截 CMD 到内核的系统调用。这是因为成功地攻击了某些 Windows 安全漏洞,例如“.printer 缓冲区溢出漏洞”,入侵者就会得到一个远程 SHELL。通过增加可策略配置的控制模块,拦截 CMD 至内核的系统调用,就能够控制远程 SHELL 上的所有入侵行为,包括重定向、信息捕获、会话重放等,该过程如图 3 所示。实现中采用 Detours 工具库,对 Win32 函数调用实施拦截。在 Linux 平台上,则通过以 LKM 和 Chroot 相结合的行为控制技术来隐藏敏感的系统信息和系统进程,构建安全可控的欺骗环境。

3.2　文件系统镜像

文件系统镜像是利用真实主机文件系统的一个目录实现对整个文件系统的模拟,镜像的文件系统拥有独立完整的文件结构、设备文件、库文件和系统文件等,使得入侵者与镜像文件系统的交互和与真实文件系统的交互相一致。这样,入侵者所看到的整个文件系统其实只是真实文件系统的一个目录而已。

4 工作原理

欺骗主机部署在所保护的网络信息系统中时,通过提供仿真的网络服务而充当一台服务器。入侵者和欺骗主机之间的交互过程如图 4 所示。

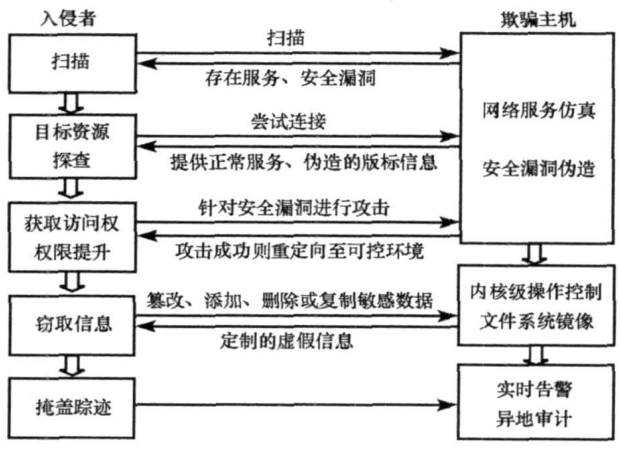


图 4 交互过程
Fig. 4 Interaction process

一个完整的入侵过程通常包括扫描、目标资源探察、获取普通用户的访问权限,进而提升权限、窃取信息、掩盖踪迹等步骤。当入侵者扫描受保护的网络系统时,欺骗主机会立即做出反应,返回存在网络服务和安全漏洞的特征信息来吸引入侵者。如果入侵者尝试连接,欺骗主机则会提供正常的网络服务来迷惑对方。一旦入侵者针对安全漏洞发起攻击,欺骗主机经过判断后返回相应的结果。在入侵者看来,攻击成功的结果是他获得了远程 SHELL 或者根权限,而事实上入侵行为已经被重定向至一个可控的虚拟操作环境中。其后,入侵者的操作指令会被拦截和控制,所访问的文件系统只是主机文件系统的镜像而已。入侵者最终获取的敏感信息,是欺骗主机为其定制的虚假信息。至此,对网络入侵行为,欺骗主机实施了完整有效的吸引、欺骗与控制,同时,将告警和日志信息实时发送至审计服务器,监控和记录网络入侵行为的整个过程。

5 实验结果

欺骗主机伪装成一台 Web 服务器,提供仿真的"Microsoft IIS v5.0 WWW 服务"和". printer 缓冲区溢出漏洞"作为欺骗吸引入侵者。入侵者用扫描器对网络进行扫描,结果如图 5 所示,Nessus 扫描器发现欺骗主机上开放的 WWW 服务及其存在的高风险远程缓冲区溢出漏洞". printer"。扫描到该漏洞后,利用黑客程序 iis5hack. exe 进行攻击,可成功远程登录欺骗主机,然后进行文件的拷贝、浏览、删除等操作后退出。与此同时,审计服务器记录了入侵行为的全过程,见图 6。记录表明,黑客在欺骗主机上的所有操作被控制在一个虚拟环境中,所访问的根目录"C:\"其实是真实文件系统的子目录"E:\Ev\C\"。实验表明,该系统能够对网络入侵进行全程深度欺骗与控制。欺骗主机通过开放特定的通道,让入侵者只能通过仿真的网络服务和伪造的安全漏洞进入虚拟环境,使得入侵者的攻击探测、主机操作和信息获取均处于受监控状态而无法察觉。

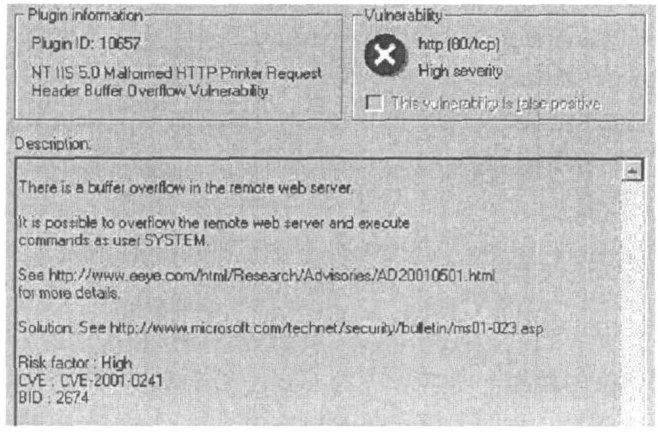
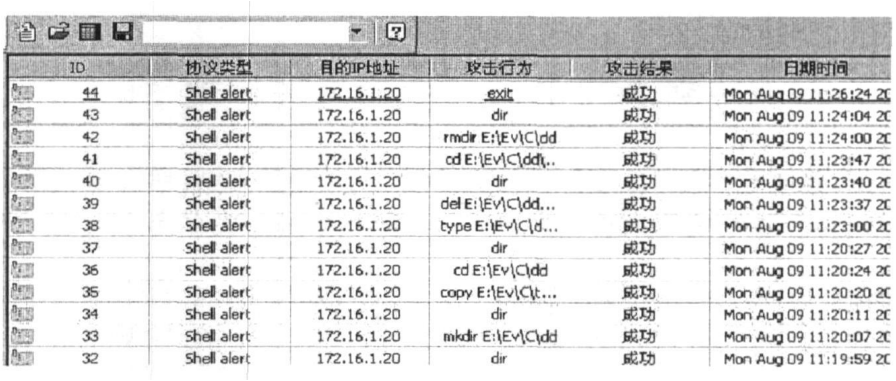


图 5 Nessus 扫描结果
Fig. 5 Scanning results of Nessus



ID	协议类型	目的IP地址	攻击行为	攻击结果	日期时间
44	Shell alert	172.16.1.20	exit	成功	Mon Aug 09 11:26:24 20
43	Shell alert	172.16.1.20	dir	成功	Mon Aug 09 11:24:04 20
42	Shell alert	172.16.1.20	rmdir E:\Ev\C\dd	成功	Mon Aug 09 11:24:00 20
41	Shell alert	172.16.1.20	cd E:\Ev\C\dd\..	成功	Mon Aug 09 11:23:47 20
40	Shell alert	172.16.1.20	dir	成功	Mon Aug 09 11:23:40 20
39	Shell alert	172.16.1.20	del E:\Ev\C\dd...	成功	Mon Aug 09 11:23:37 20
38	Shell alert	172.16.1.20	type E:\Ev\C\d...	成功	Mon Aug 09 11:23:00 20
37	Shell alert	172.16.1.20	dir	成功	Mon Aug 09 11:20:27 20
36	Shell alert	172.16.1.20	cd E:\Ev\C\dd	成功	Mon Aug 09 11:20:24 20
35	Shell alert	172.16.1.20	copy E:\Ev\C\t...	成功	Mon Aug 09 11:20:20 20
34	Shell alert	172.16.1.20	dir	成功	Mon Aug 09 11:20:11 20
33	Shell alert	172.16.1.20	mkdir E:\Ev\C\dd	成功	Mon Aug 09 11:20:07 20
32	Shell alert	172.16.1.20	dir	成功	Mon Aug 09 11:19:59 20

图 6　文件操作的数据库记录
Fig. 6　Database records of file operations

6　结 论

为了弥补传统网络防御体系的不足,变被动防御为主动防御,本文提出了一种基于欺骗的网络主动防御技术。它基于深度欺骗策略,建立了由网络服务仿真、安全漏洞伪造、操作行为控制和文件系统镜像组成的四层欺骗与控制架构,在入侵行为的每一个阶段实施欺骗与控制。实验表明,该技术突破了普通蜜罐技术单一欺骗层次的局限性,使得欺骗性、交互性和安全性同时得到明显提高。网络欺骗系统由于提供了一个让入侵者扫描、探测、攻击和攻破的平台,较之防火墙、IDS 等安全技术而言,面临着更大的安全风险。因此必须不断提高欺骗水平,更逼真的安全漏洞模拟、更全面的操作系统级入侵者行为控制技术是下一步的努力方向。

参 考 文 献:

[1] Spitzner L. Honeypots: Tracking Hackers[M]. Boston: Addison-Wesley, 2003: 73- 86.

[2] Spitzner L. Honeypots: Catching the Insider Threat[C]// Proceedings of the 19th Annual Computer Security Applications Conference, 2003: 170-179.

[3] Spitzner L. Problems and Challenges with Honeypots[EB/OL]. http://www.security focus.com/infocus/1757, 2004.

[4] Provos N. A Virtual Honeypot Framework[EB/OL]. http://www.usenix.org/event/sec04/tech/full_papers/provos/provos_html, 2004.

[5] Spitzner L. Open Source Honeypots: Learning with Honeyd[EB/OL]. http://www.security focus.com/infocus/1659, 2003.

[6] Netsec. Specter Intrusion Detection System[EB/OL]. http://www.specter.com, 2004.

[7] Recourse Technologies Inc. Mantrap: A Secure Deception System[EB/OL]. http://www.recourse.com, 2001.

[8] The Honeynet Project. Know Your Enemy: Learning about Security Threats(2nd Edition)[M]. Boston: Addison-wesley, 2004.