中国科技资源导刊 ISSN 1674-1544 CHINA SCIENCE & TECHNOLOGY RESOURCES REVIEW
2008年7月 第40卷第4期 45-48 ISSN1674-1544 Vol.40 No.4 45-48,Jul. 2008

基于 Honeypot 技术的数字图书馆网络安全系统设计与实现

唐海萍
(浙江海洋学院,浙江舟山 316000)

摘 要:本文从数字图书馆网络安全现状入手,针对性地提出了网络环境下为保护数字资源的安全,引入 Honeypot 技术的必要性及 Honeypot 技术如何与数字图书馆网络安全系统相结合,并对此种网络安全架构进行模拟测试与分析。

关键词:Honeypot;数字图书馆;网络安全
中图分类号: G250.76 **文献标识码**: A DOI: 10.3772/j.issn.1674-1544.2008.03.009

Design and Realization of the Digital Library's Network Security System Basede on Honeypot

Tang Haiping
(Zhejiang Ocean University, Zhoushan 316000)

Abstract: This paper analyzes the current status of digital library's network security, brings forward the necessary of introducing Honeypot and how to combine it with digital library's network security system for protecting the security of digital resources in Internet environment. Then tests and analyzes this kind of network security structure in simulation.

Keywords: Honeypot, digital library, network security

Honeypot 是一种资源,它的价值就在于其可以被未授权或非法用户使用[1]。Honeypot 是一个真实系统的映射,即在 Internet 中能找到其他与之一模一样的真实系统[2],它能够牵制入侵者,耗费他们的时间和资源。同时还能够防止病毒的蔓延,对付来自内部网络的攻击,发现并报告网络或系统中存在的可疑迹象。

1 基于 Honeypot 技术的数字图书馆网络安全系统的总体设计

1.1 设计目标

结合图书馆网络安全现状及现有安全防护手段普遍缺乏网络防御的主动性和时效性的特

第一作者简介:唐海萍(1979-),女,工程师,硕士,主要研究方向是数字图书馆。

收稿日期:2008年3月21日。

点，在系统设计时应着重加强以下几个方面：

(1) 数据捕获：数据捕获是指获取入侵者的所有活动，并能够根据日志分析结果对现有的安全策略做出调整，以提高系统的安全性。其难点是如何获取尽可能多的数据而不被发觉。它包含3个层面：防火墙日志、入侵检测系统捕获的数据和主机的系统日志[3]。

(2) 数据控制：由于Honeypot是专门用于被攻占的系统，但不允许入侵者将它作为跳板去攻击其他系统，因此，数据控制的难点在于控制系统数据流量的同时又不会引起黑客的怀疑[4]。

(3) 网络欺骗能力：根据网络系统中存在的安全弱点，采取适当技术，通过伪造的敏感信息和有意暴露的系统漏洞来引诱入侵者，其主要目的是收集和分析入侵者的行为，保护真正重要的系统。

1.2 体系结构

根据设计目标，本文构建了一种将Honeypot技术、IDS与防火墙紧密结合的防护体系（图1），使得三者在实际部署中构成一个有机整体。

系统采用两层防火墙设计，外防火墙的特点是“严进宽出”，外防火墙的主要作用是限制黑客的攻击行为，将大部分外部的入侵行为隔离。内防火墙采用“宽进严出”的设置策略，“宽进”是为了迷惑入侵者，以收集更多数据，“严出”则是为了防止入侵者利用该系统作为跳板，对其他信息系统进行进一步的攻击。IDS放在防火墙之后，实时检测，用于监视系统的异常。若访问事件确定为入侵行为，则远程控制台的入侵行为重定向子系统截断入侵者同实际系统的连接，把所有的攻击数据导向Honeypot，并将系统的所有活动严格、详细地记录到报警、日志服务器，以对可疑行为及入侵行为做进一步的分析。若访问事件被引入蜜罐主机后，经检测与入侵特征库的数据不匹配，则判断为不正常记录。不正常记录按入侵事件处理，同时更新入侵检测系统的知识库。正常记录转入正常访问，同时更新合法访问特征库。

在系统运作的同时，收集防火墙日志、IDS日志和Honeypot主机的系统日志，形成“三重捕获”，通过对这些有价值的入侵信息、攻击记录的分析，可以更好地理解图书馆网络所遇到的威胁，进而获悉如何防止这些威胁，以期及时调整网络防护规则与手段，从而提高图书馆的网络安全性能。

2 基于Honeypot技术的图书馆络安全系统的实现

依据总体设计，在图书馆网络系统中安装应用软件：蜜罐系统Honeyd[4]、入侵检测系统Snort[5]和防火墙Netfilter/iptable，并进行必要的配置。本

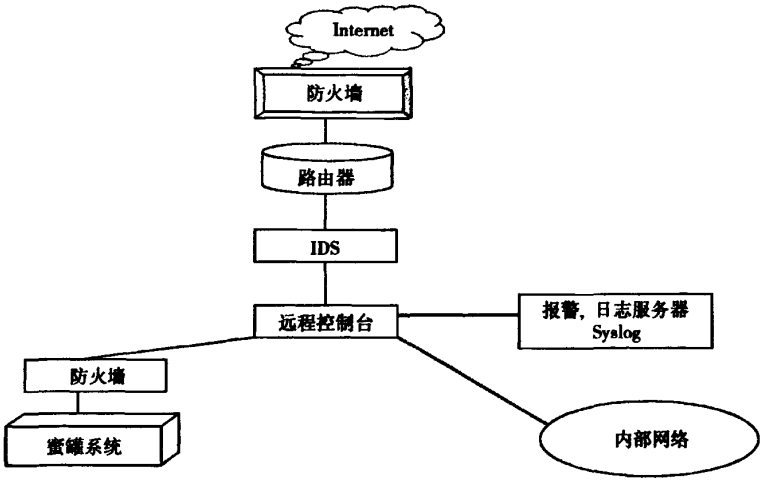

图1 基于Honeypot技术的数字图书馆网络安全系统

文以图书馆的数字资源服务器 Windows Server 2003 SP2 受攻击为例，在 Honeyd 的 honeyd.conf 文件中，配置出需保护服务器的脚本：

#创建一个 WINDOWS SERVER 2003 模版，该模版开放 80、21 等端口的对应服务，另外还开设 135、137、139 等端口。

```
create windows
set windows personality" WINDOWS SERVER 2003 SP2"
add windows tcp port 80 "scripts/web.sh"
add windows tcp port 137 open
add windows tcp port 21 "scripts/ftp.sh"
add windows tcp port 139 open
add windows udp port 137 open
add windows udp port 135 open
add windows udp port 1433 open
set windows uptime 3284460
set windows default tcp action reset
set windows default udp action reset
```

用 nmap 命令测试 honeyd 模拟的服务器：

```
#nmap -PO -O -sS 172.16.1.15
Starting nmap V.3.00(www.insecure.org/nmap/)
Interesting ports on (172.16.1.15)
(The 1599 ports scanned but not shown below are in state: closed)
Port        State       Service
110/tcp     open        pop3
21/tcp      open        ftp
Remote operating system guess: windows server 2003 sp2.
```

从指令运行的结果可以看出，目标使用 Windows Server 2003 操作系统，与虚拟的系统相符。

同时，在真实的数字资源服务器上设置一个账号 sa 来做一个蜂蜜信标。这个账号是伪造的无效账号，系统中的操作人员不会使用它，而任何使用该账号的访问都被认为是非法的。由于 sa 是 SQL SERVER 数据库的一个缺省账号，在某种意义上，该账号具有比 administrator 还要大的权限，而且许多 SQL SERVER 的实际应用者，对 sa 账户的安全性不够重视，不少黑客利用此账号缺省密码为空的漏洞攻击服务器，因此，sa 对黑客具有较大的吸引力。

如果有人使用该账号，就有可能发生了入侵行为，可在入侵检测系统系统 Snort 中设置一条规则：Alert ip any any -> any any(msg:"Honeytoken Access - Potential Unauthorized Activity"; content:"sa")，当蜂蜜信标被触发就发出警告信息。这样该服务器就成为了一个含有蜂蜜信标的系统，能有效地监测和定位攻击者，特别是位于内网的攻击者，通过日志的相关记录，如时间、IP、MAC、协议、访问对象等信息有效地进行追踪。

系统运行两个多月后，在远程日志主机上的 var/log/honeyd 发现黑客登陆的信息和一些攻击的方法。

攻击者通过一个 SQL SERVER 数据库用户名密码嗅探工具，扫描出蜂蜜信标——sa 账号，并利用此账号建立一个操作系统账号。入侵检测系统 Snort 发现此行为后，就在入侵者没察觉的状态下，向中央控制台发报警信息。由中央控制台发指令给 Honeyd 系统，并在数据包回送网络之前，特征引擎对其进行修改，使机器模拟受攻击的数字资源服务器的指纹，以欺骗攻击者。通过此种方式，将攻击者的入侵行为转入诱骗系统，同时记录入侵者的下一步动作。

进一步查阅日志记录，发现入侵者安装了代理服务器软件 CCProxy，欲将数据资源服务器作为一个免费上网的代理服务器。通过 CCProxy 的日志分析，查得入侵者的 IP 为 172.15.23.45，MAC 地址为：00-17-31-1E-E7-8A。这是一个校园网上的主机信息，且来源于学生寝室网络。通过获得的 IP 和 MAC 地址追踪到账号和连接交换机的端口，进而查到该攻击者。

这样蜜罐系统 Honeyd 与入侵检测系统 Snort 联动起来，当 Snort 发现可疑行为或入侵行为时，立刻将检测结果通知中央控制台的入侵行为重定向子系统。入侵行为重定向子系统根据检测结果，通知受可疑攻击的服务器系统向 Honeypot 进行必要的数据反馈，使 Honeypot 模拟受可疑攻击的服务器的状态，将入侵者攻击行为重定向到 Honeypot，有效地保护了真实的数字资源服务器（数据处理流程如图 2 所示）。

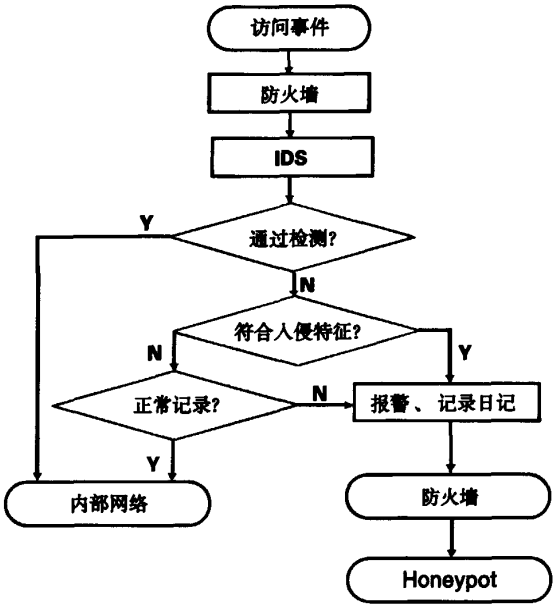

图2 数据处理流程

由此可见，基于Honeypot技术的图书馆网络安全防护系统，使得网络安全防御体系由静态转为动态，从新的角度去解决图书馆网络安全问题，能够牵制、转移入侵者的注意力并防止病毒的蔓延，发现并报告网络或系统中存在的可疑迹象，为图书馆网络安全管理人员及时采取对策提供有价值的信息。

参考文献

[1] Spitzner L. The honeynet project: Trapping the hackers[J]. IEEE Security and Privacy, 2003, 1(2): 15 - 23.

[2] 王伟平，李更生，崔锦法．一种基于蜜罐技术的入侵诱骗模型的研究与建立 [J]．云南大学学报（自然科学版），2006, 28(S1): 117 - 120.

[3] 王旅．新一代蜜网技术剖析 [J]．航空计算技术，2004 (12): 121 - 123, 127.

[4] 周莲英，曹登元，年秩．虚拟蜜罐系统框 Honeyd 的分析与研究[J]. 计算机工程与应用，2005(27)：137 - 140.

[5] 齐建东，陶兰，孙总参．入侵检测工具——Snort 剖析[J]. 计算机工程与设计，2004(1): 36 - 38, 47.