动态防御模型在军用网络上的应用①

康松林　孙永新　胡赐元 (中南大学 信息科学与工程学院 湖南 长沙 410083)

摘　要： 当前军用网络安全体系还没有形成统一的安全策略，难以保障军用网络上重要信息的安全。提出一种利用蜜罐技术改进 P2DR 模型的防御模型。该模型通过对蜜罐部署的优化和对入侵行为的重定向等方法，有效提高了针对网络入侵的事前检测能力，改善了 P2DR 的效能，并初步实现了在军用网络上的应用，增加了军用网络的防御纵向深度。

关键词： 军用网络；动态防御模型；蜜罐；入侵行为；重定向

Application of Dynamic Defense Model to Military Networks

KANG Song-Lin, SUN Yong-Xin, HU Ci-Yuan

(School of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: Currently, there is not a unified security strategy in military networks' security system. So, the security of important information in military networks is not yet guaranteed. In this paper, a defense system is put forward, which is an advanced P2DR model with honeypot technology. By optimizing honeypot deployments and redirecting the intrusive actions, this system has effectively improved the pre-detection ability on network intrusion, and the P2DR performance. It is also used in elementary applications of the military networks, which has boosted the defense capability of military networks.

Keywords: military network; P2DR; honeypot; intrusive action; redirect

1　引言

军队计算机网络的安全性是各国军队信息化建设中非常重要的一个环节，如军用指挥自动化网络、C4ISR 系统等网上信息的安全和保密尤为重要。因此，要提高军队计算机网络的防御能力，加强网络的安全措施，否则该网络将是个无用、甚至会危及国家军队安全的网络。目前，大多数军用网络都采用尽可能多的禁止策略来进行防御，常用防御手段主要有防火墙、加密、身份认证、访问控制、安全路由器等[1,2]，这些方法对防止系统非法入侵都能够起到一定的防御作用，但是从系统安全管理角度来说，仅有这些静态的防御是不够的，还应采取动态防御的策略。为此，本文提出了在军用网络上利用蜜罐技术对动态防御模型进行改进，以增强其防御能力。

2　相关概念

2.1 动态防御模型(P2DR)

P2DR 模型包含四个主要部分:Policy (安全策略) 、Protection(防护) 、Detection(检测)、Response(响应)[3-5]。Policy 是模型的核心，负责制定一系列的控制策略、通信策略和整体安全策略，Protection 负责采用一些传统的静态安全技术和方法(防火墙、加密、认证等)来实现安全策略，Detection 负责采取有效的手段对网络的运行进行监测，Response 负责在检测到安全漏洞和安全事件之后及时做出正确的响应，从而把系统调整到安全状态。Protection、Detection 和 Response 组成了一个较完整的、动态的安全循环(如图 1)。

① 基金项目:国家自然科学基金(60773013)
收稿时间:2009-06-10

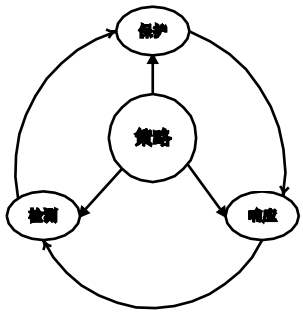

图 1 P²DR 安全模型

2.2 蜜罐技术

所谓蜜罐，是指一个专门让黑客攻击的系统，主要作用是提供了一条获取黑客信息的途径[6]。蜜罐的复杂性可以用交互程度(Level of Involvement，蜜罐系统与攻击者交互的能力)来衡量。可以将蜜罐分为三类：(1)低交互程度蜜罐，只提供对待定服务的虚拟，在虚拟待定服务的实现形式上只是对待定端口的监听和记录；(2)中交互程度蜜罐，提供了更多的可交互信息，但是仍然没有为攻击者提供一个可使用的 OS,同时诱骗进程变得更加复杂，对待定服务的模拟变得更加完善，风险性也更大了；(3)高交互程度蜜罐，提供了一个支撑 OS,收集信息的能力和吸引攻击的能力显著提高，风险性也随之大大增加。蜜罐交互程度的比较见表 1：

表 1 三种不同交互程度蜜罐比较

	低交互程度蜜罐	中交互程度蜜罐	高交互程度蜜罐
复杂程度	低	中	高
风险性	低	中	高
信息收集程度	连接	请求	全部
被攻破可能性	无	无	有

3 利用蜜罐技术对动态防御模型改进

3.1 蜜罐部署

将蜜罐部署在军用网络的内部，是目前大多数军网中蜜罐部署的常用位置，目标是检测或响应来自网络内部的攻击或者未授权活动，由于大部分军用网络都是与 Internet 物理隔绝的，为探测内网攻击行为，这样布置是很有必要的。如图 2 所示，这种部署模式是通过重定向模块主动将攻击导向蜜罐环境，使攻击者的时间和精力都花费在攻击蜜罐系统，而不是真正的服务器上[7]。同时，还可以通过蜜罐记录攻击者的攻击手法，这样不仅能够帮助保护在攻击期间使用的网络，还能防范未来同样类型的攻击。这种部署模式还可以将防火墙和路由器过滤掉的流量引入给蜜罐，具有很高的实用价值。

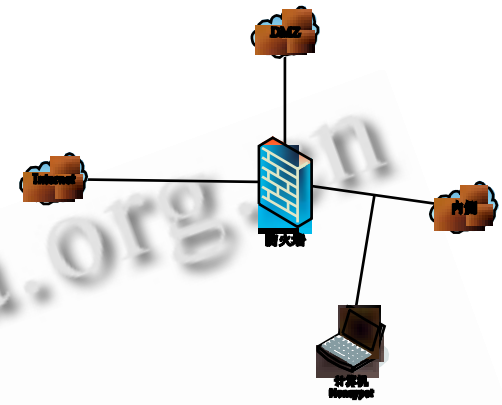

图 2 蜜罐系统在网络中的部署

3.2 加入蜜罐后的动态防御模型

网络动态防御模型的主要思想是以管理控制模块为中心，并结合现有的入侵检测机制，主动对网络可能遭受的攻击进行预先评估[8]。其体系结构如图 3 所示：

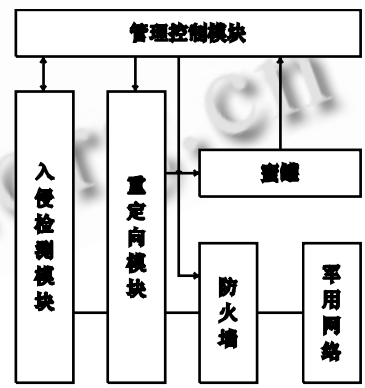

图 3 动态防御模型体系结构

动态防御模型在未加入蜜罐前，当入侵检测模块发现攻击时，只能进行简单的阻断和隔绝[9]。加入蜜罐后，当检测到可疑连接或攻击时，检测模块能够自动提取入侵规则，及时通过重定向模块将其转移到蜜罐中，并进一步分析、学习攻击者使用的技术和他们的动机，一旦确认为攻击，就提取入侵者的入侵行为特征，并将其添加到规则库中，并通知管理控制中心，更改防火墙的规则库，使入侵检测、防火墙和蜜罐之

间实现联动，并做出响应，这样使网络防护始终处于一个主动的地位，从而保护了军用网络的安全。

4　军网安全模型的设计

根据军用网络中的操作系统数据库等软件的应用具体情况，本设计中选用了 WINNT2000, Linux, VMWARE, SNORT, SQLSERVER 数据库等软件，进行加入 Honeypot 的 P²DR 模型网络安全系统设计。

4.1 系统结构的设计

军用网络系统结构主要包括，防火墙、IDS、蜜罐系统和 P²DR 策略库等，具体设计如图 4 所示。

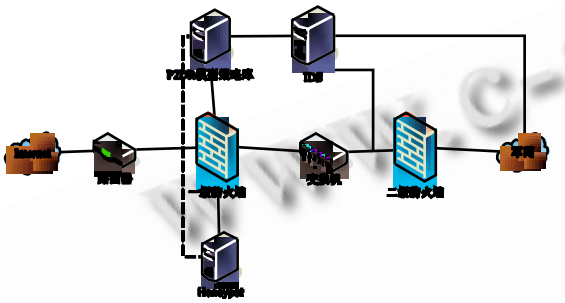

图 4　军网基于 P²DR 模型系统结构

P²DR 模型策略库主要包括攻击事件表、攻击行为表、规则表，基本结构如表 2–表 4 所示。同时，以前由防火墙担当的记录连接企图、分析流量异常等功能和 IDS 模块的功能，也在策略库的统一指导下完成。

表 2　攻击事件表结构

包序列号	协议类型	源IP	目标IP	源MAC	目标MAC	源PORT	目标PORT	URG	ACK	PSH	RST	SYN	FIN

表 3　攻击行为库

序号	探测端口号	服务类型

表 4　规则表

包序列号	协议类型	允许/拒绝	源IP	目标IP	源PORT	目标PORT	URG	ACK	PSH	RST	SYN	FIN

4.2 构建蜜罐及工作流程设计

蜜罐构建主要有两种方法：一是使用已有的蜜罐软件构建蜜罐系统：如 MANTRAP 等著名软件等。二是采用弱化系统构建蜜罐，主要是将真实系统的一些防护功能弱化，如开放一些重要端口，模拟系统漏洞的方法构成蜜罐[10]。本文采用弱化系统的方法及低交互方式设计蜜罐，其系统工作流程如图 5 所示。

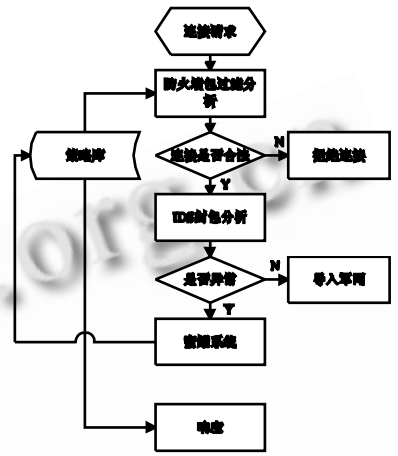

图 5　系统工作流程

(1) 首先防火墙对来自 Internet 的连接流量进行判别。如果信息流量异常，防火墙将在 P2DR 模型库中查找是否有相应的规则，如果有相应的规则，则按照规定好的策略进行响应，如：丢包、阻断连接、通知管理员等；如果没有相应的规则，则通过地址转换模块将连接转入 Honeypot，对黑客的行为进行监视、控制，并形成规则后加入 P2DR 模型的规则库、攻击行为库、策略库。

(2) 如果信息流量正常，通过地址转换模块将连接转入军用网络。

(3) IDS 模块负责对进入军用网络或网络内部的攻击行为进行监视、控制。如果发现异常行为通过 P2DR 模型的统一策略进行响应。

5　系统应用分析

通过加入蜜罐系统的 P2DR 模型的设计，在军用网络上初步实现了网络安全的四道防线，如图 6 所示。

A 未经许可或未开放的通讯协议(服务)可直接由防火墙切断。

B 当 Network-Based IDS 确认攻击行为发生后，除做成日志备查外，并指示防火墙将该连接中断。

C 攻击嫌疑者被 Network-Based IDS 导入蜜罐系统进行严密监视。

D 当 Host-Based IDS 以 misuse 入侵检测技术发现系统有不正常纪录时，便将其导入蜜罐系统进行严密监视。

E 正常的联机状况。

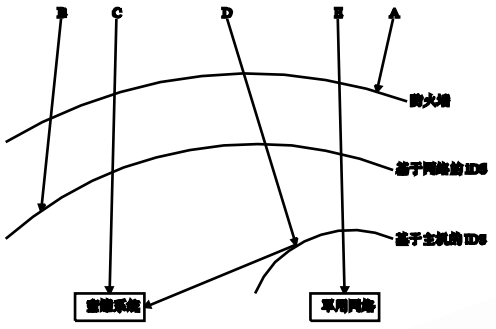

图 6 军用网络安全的四道防线

各防御层次的功能包括：

第一道防线由防火墙负责，防火墙可阻挡大多数攻击，另外网络地址转译(NAT)功能，可以隐藏内部网址，降低被攻击几率。

第二道防线由基于网络的 IDS 负责，检测网络异常现象，并负责将异常行为导入蜜罐系统，紧急或必要时立即物理断开，以降低危害。

第三道防线由基于主机的 IDS 负责，安装在受保护的服务器(或应用系统)上，检测异常行为，并负责将异常行为导入蜜罐系统，紧急或必要时可立即物理断开，以降低危害。

第四道防线由蜜罐系统负责，对被导入的嫌疑者进行行为观察，确认为异常行为者(如非法读取密码文件、企图植入后门程序等)，予以切断联机，若观察一段时间仍无异常行为者，会被自动导回军用网络系统。

6 小结

使用蜜罐系统改进 P2DR 模型具有以下优点：Honeypot 收集数据量小，减少误报率，捕获漏报，资源最小化，检测、捕获、记录所有的 IP 层行为。通过在军用网络上部署加入蜜罐的 P2DR 模型，有效地整合了军用网络现有的网络安全技术，提高了军网的安全水平，在一定程度上保证了军用网络的安全。

参考文献

1 Qu ZY, Jia Y. The Design of the Network Security Model of Active Defense. Wireless Communications, 2008,6(2):1－4.

2 Krawetz N. Anti-honeypot technology. Security & Privacy, 2004,7(3):76－79.

3 孟学军,石岗.基于 P2DR 的网络安全体系结构.计算机工程, 2004, 30(4):99－101.

4 张云鹏,胡飞.基于 P2DR 模型的分布式入侵检测系统设计与实现.计算机工程与应用, 2005,35(6):141－144.

5 Hu HP, Liang X, Zhang BL, Guo WX. An adaptive security end-system model based on active defense. Communications Systems, 2004,7(3):331－335.

6 程杰仁,殷建平,刘运等.蜜罐及蜜网技术研究进展.计算机研究与发展, 2008,45(6):375－378.

7 马莉波,段海新,李星.蜜罐部署分析.大连理工大学学报, 2005,45(4):150－156.

8 霍成义,吴振强,见晓春等.网络安全动态防御模型研究.通信安全与通信保密, 2006,12(3):105－107.

9 宋富强,将外文,刘涛.蜜罐技术在入侵检测系统中的应用研究.现代计算机, 2008,3(2):10－12.

10 李之堂,徐晓丹.动态蜜罐技术分析与设计.华中科技大学学报, 2005,33(2):86－88.