一种基于蜜网的网络安全联动模型①

赵会锋[1]，李丽娟[2]

[1](湖南大学 软件学院，长沙 410082)
[2](湖南大学 计算机与通信学院，长沙 410082)

摘　要：传统安全防御技术，如加密、认证、防火墙等，具有静态和滞后的缺点，以及蜜网存在容易被攻陷的不足。针对这个问题，提出了一种基于蜜网的安全联动模型，并对该模型进行了形式化分析，引入了重定向概念，设计并实现了该模型的联动机制。通过仿真实验，初步验证了该系统防御的有效性。最后，给出了下一步的主要研究任务。

关键词：网络安全；蜜网；联动模型；形式化分析；重定向

Honeynet-Based Linkage Model for Network Security

ZHAO Hui-Feng[1], LI Li-Juan[2]

[1](School of Software, Hunan University, Changsha 410082, China)
[2](School of Computer and Communication, Hunan University, Changsha 410082, China)

Abstract: Traditional security defense technologies, such as encryption, authentication, firewall, etc., were static and lagging behind, and honeynet was easily compromised. To solve this problem, a honeynet-based linkage model for network security is proposed. Then, its formal analysis is made. The concept of redirection is introduced, and its linkage mechanism is designed and implemented. Also, the simulation results validate the initial effectiveness of the system defense. Finally, the main task of the next step is pointed out.

Key words: network security; honeynet; linkage model; formal analysis; redirection

传统的网络安全技术，如加密、认证、防火墙和入侵检测系统(IDS)等，在保护信息的机密性、完整性和鉴别、控制访问方面虽有成效[1]，但基本上都是从自身出发而进行的一系列检测和保护，对入侵者很难有效防御甚至反击，其实质不外乎闭门造车，亡羊补牢，很难避免相对静态、滞后和孤立的防御所造成的损失。因此，需要对入侵者进行真实，及时甚至是实时的研究，以提高防御的针对性、及时性和有效性。

蜜网则是一种较新的技术。该技术基于主动防御，采用诱骗思想。通过该技术，可以对入侵的目的、技术、策略和攻击工具进行研究，更加具有针对性、真实性和有效性。但是，蜜网也同样存在一定的缺陷。比如，蜜网一旦被攻陷，会被攻击者所利用，成为攻击其它系统的跳板[2]。

总之，当前还未形成一套有效的安全系统。面对各种威胁，尤其是分布式、协作式攻击，任何单一安全组件的防御能力都是有限的，只有各安全组件实现有效联动，取长补短，才能进行充分而有效的防护。

1　PPDSRC模型

针对上面的问题，根据闭环理论，本文提出了一种新安全模型——PPDSRC 模型。该模型用一个六元组来描述，即 PPDSRC=(Policy,Protection,Detection, Study,Recovery,Counterattack)。

(1) Policy 为该模型的核心。负责生成一系列的控制策略、通信策略和整体安全策略，以及对生成这些策略的分发。在制定安全策略时，要根据蜜网学习的结果进行及时完善。

① 收稿时间:2011-03-14;收到修改稿时间:2011-05-03

(2) Protection 根据蜜网学习的结果，通过对传统安全技术进行动态更新、及时加固来实现。

(3) Detection 根据蜜网学习的成果，通过更新、完善相关数据库，来不断提高监测的效能。

(4) Study 为该模型的关键，包括特征抽取和数据融合等机制。其成果包括攻击特征、工具、技术、目的和解决方案等。

(5) Recovery 指将受损的系统复原到安全事故以前的状态。这是系统生存能力的重要体现。

(6) Counterattack 是指当破坏行为发生时，网络安全系统能及时取证，并主动封杀甚至反击。

1.1 模型架构

该模型采用五层纵深防御体系，具有开放性，针对性，整体联动的特性。其架构如图 1 所示。第 1 层由认证、加密和防火墙组成，为典型的静态防御技术，能抵抗多数黑客攻击，大大提高了入侵成功的技术门槛。第 2 层由 IDS、病毒检测和漏洞扫描与加固组成，其主要任务是对入侵行为进行检测，同时主动检测系统漏洞并加固。历史数据表明，大部分入侵都是利用已有的漏洞，该层能有效降低入侵成功的概率。第 3 层由对抗、反击组成，其主要任务是根据收到的警报，对攻击者进行反击。第 4 层由系统备份和灾难恢复组成，其主要任务是对系统的关键信息做备份，灾难发生时，则根据备份信息对损害进行恢复。第 5 层为安全策略，根据对入侵行为的研究结果，负责生成与分发安全策略。

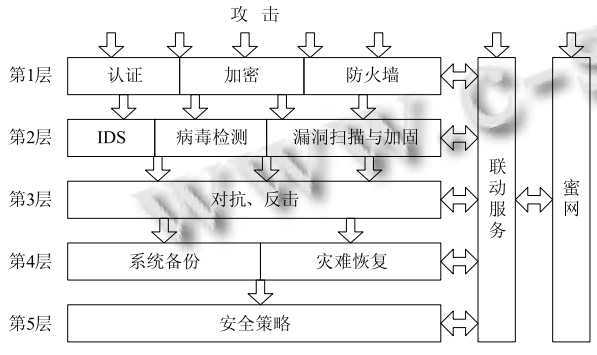

图 1 PPDSRC 模型架构

1.2 模型分析

该模型 M 采用一个六元组进行描述，即 M=(P,D,I,V,R,C)。其中，P 为该模型设置的所有保护的集合。D 为该模型配置的有关监测系统的集合。I 为入侵行为的集合。V 是蜜网环境,即所有应用服务协议的集合。R 是目标网络攻陷后，相关恢复机制的集合。C 为系统配置的相关控制机制（比如系统控制、入侵行为重定向（R1 是由 I →V 的映射）、特征提取和数据融合等机制）的集合。

① P1(T(P)≥T(D) + T(R1) +T(R)) →1，P1：概率函数，T：时间函数。

② 目标系统裸露时间 T(E)=T(D)+T(R1)+T(R)-T(P)，If T(P)< (T(D)+T(R)+T(R1)) 。

③ ∀i∈I , P1(R1(i) ∈V) →1 ,P1 为概率函数。

④ ∀i∈I , T(R1(i) ∈V) →0 ,T 是时间函数。

⑤ ∀i∈I,∀v∈V, T(i ， v) →∞,T 是时间函数

⑥ ∀i∈I,∀v∈V, T(S(i ，v)) →0 ,T 是时间函数，S：学习更新机制（包括特征抽取和数据融合等机制，其成果包括攻击工具、技术、特征和解决方案等）。

其中, T(P)为系统防护时间,即黑客用于攻击所花的时间;T(D)为从开始攻击到被系统检测到所花的时间;T(R1)为重定向时间，即从监测到入侵行为，至被重定向到蜜网的时间（此时 T(R)=0），或者，从监测到入侵行为至目标网络被攻陷即重定向失败所用时间。T(R)为目标被攻陷到恢复至安全态的恢复时间。满足①，系统具有理论上的安全性。现实中的安全性可以用②来描述。其中，T(E)越小系统越安全。满足③和④说明，将监测到的攻击行为重定向到蜜网的成功概率越高、时间代价越小，系统性能越好。满足⑤，则说明黑客攻击蜜网的时间越长越好。也说明，蜜网系统比较完善，既成功的诱导黑客改变了攻击方向，降低了目标系统被攻陷的概率，又为对其研究获得了充分的时间和宝贵的第一手资料。满足⑥则说明，对攻击行为有效性的学习、及时更新所花的时间，要尽可能的短，以满足整体的联动协作，提高防御的及时性、针对性和有效性，以做到有的放矢。

1.3 联动机制的研究与实现

首先，通过外部防火墙，可以对熟知的没有价值的入侵行为进行过滤，从而可以获取高质量的研究数据。再通过重定向机制，将流向内网的可疑数据重新定向到蜜网中。对数据研究后，可以实时地对策略等进行更新。其联动机制如图 2 所示。

该机制的实现具有以下几个特点：

（1）采用两层防火墙模式。外层防火墙可以过滤掉已知的攻击，内部防火墙采用严进宽出的原则进行

处理。这样能更好的实现防护和研究的针对性和有效性。

（2）结合入侵检测系统（IDS）引入重定向机制。通过 IDS 的检测，可以将流向内网的可疑行为，通过重定向功能将其诱导向蜜网系统.这样不但保护了内网而且还为进一步研究或取证提供了有力的保障。

（3）蜜墙采用两层桥接模式。该模式有三个接口，eth0：外网接口，eth1：蜜网接口，eth2：为秘密通道，用于远程监控。蜜墙处在链路层，对数据包不进行网络路由和 TTL 递减, 不会提供本身的 MAC 地址, 所以蜜网对入侵者来说是透明的，其身份很难被识破。而且，eth0 与 eth1 无 IP 地址，内网和蜜网属于同一网段，因此，蜜网也可以捕获来自内部的入侵。蜜墙采用宽进严出的策略，由于所有进出蜜网的数据都必经蜜墙，并受其控制和审计，这样不仅能为充分研究可疑行为提供了有力保障，还能避免蜜网被彻底攻陷后，作为跳板用来攻击第三方。

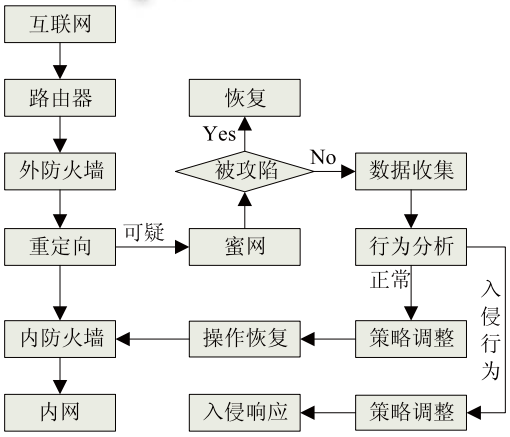

图 2　联动机制图

2　仿真实验

本模型采用 VMware，Honeywall 建立蜜网，Swatch 为监视工具，用 IPtables, Snort-inline 作为防护系统并实现将可疑数据或者连接重新定向到蜜网中。试验结果表明，目前绝大多数攻击采用 TCP 协议，而 IIS 则是攻击的重点，如表 1，表 2 所示。

表 3 为蜜网捕获的入侵行为。因为蜜网用于研究入侵行为，所以其安全性也受到了威胁。要保证其正常工作，系统必须具有动态更新安全策略的能力。如在表 3 中，当黑客执行命令 vi host.deny 后，系统迅速可以依据该行为的危害级别将其切断，避免了蜜网被用作攻击第三方的工具，从而也确保整个系统的安全。

表 1　入侵所用协议统计

统计内容	协议	所占比例(%)
入侵所用协议统计	TCP	98.53
	ICMP	0.80
	UDP	0.67

表 2　入侵行为统计

统计内容	入侵名称	所占比例（%）
入侵行为统计	WEB-IIS cmd.exe access	37.28
	WEB-IIS ISAPI.ida attempt	26.67
	FTP USER overflow attemp	15.89
	FTP PASS overflow attempt	13.75
	WEB-IIS Unicode directory	6.38
	其它	0.03

表 3　入侵行为跟踪示例

入侵步骤	入侵行为	入侵命令	危害级别
第1步	建立shell	//bin/sh	4
第2步	用户信息	id	1
第3步	系统信息	uname -a	2
第4步	修改密码	vi passwd	4
第5步	修改host.deny	vi host.deny	5

3　结语

试验结果表明，本模型不但具有一定的鲁棒性，而且可以捕获入侵行为并进行初步的统计分析，其不足在于，数据处理方面还需要大量的人工参与。为了更好的保护目标系统的安全，下一步的任务是对入侵特征提取与数据融合进行研究，希望在数据的自动化处理方面有所突破。这也是整个模型有效协作的关键。

参考文献

1 傅狮,王娟,秦志光,等.宏观网络安全预警与应急响应系统.电子科技大学学报,2006,35(4):702−705.

2 Spitzner L. Definitions and Value of Honeypots. http://www.spitzner.net.2008

3 The Honeynet Project. http ://www.honeynet.org.2009.

4 侯小梅,毛宗源,张波.基于 P2DR 模型的 Internet 安全技术.计算机工程与应用,2000,36(12):1−2.