基于蜜罐的主动网络安全系统的研究与实现

孙知信　　杨加园　　施良辉　　王汝传
(南京邮电学院计算机系　南京 210003)

摘　要： 采用自动的大规模扫描，在发现系统漏洞后，能够使对手在短时间内攻破计算机系统。传统的蜜罐系统在处理这些问题时有很多不足，因为其签名是可检测的。针对这些不足，本文从另一个角度构造了一个基于蜜罐的主动网络安全系统 (Active Network Security System, ANSS)的诱骗系统。 ANSS 位于真实的网络环境中，可以自始至终捕获到黑客的行为。仿真实验表明，ANSS 使网络的安全性能达到了一个较高的水平，对入侵行为的监控和预防有着重要的意义。

关键词： 网络安全，诱骗系统，蜜罐
中图分类号： TP393　　**文献标识码：** A　　**文章编号：** 1009-5896(2005)03-0351-04

Research and Implementation of an Active Network Security System Based on Honeypots

Sun Zhi-xin　　Yang Jia-yuan　　Shi Liang-hui　　Wang Ru-chuan
(*Department of Computer Science and Technology, NJUPT, Nanjing* 210003, *China*)

Abstract Exploit automation and massive global scanning for vulnerabilities enable adversaries to compromise computer systems shortly after vulnerabilities become known. Traditional honeypots have shortcomings to deal with these problems because their signatures can be inspected. Aiming at current research state, the paper constructs an Active Network Security System (ANSS) from another point of view, i.e., ANSS situated in a real network circumstance. ANSS is the same as other systems in Internet, and it can capture actions of hacker from beginning to end. The simulation results indicate that ANSS can elevate network's security performance to a higher level and ANSS has important impact on forecast and monitor attack activities.

Key words Network security, Decoy system, Honeypot

1　引言

今天网络正在逐步改变着人们的工作方式和生活方式，成为当今社会发展的一个主题，而与此同时安全隐患亦日益突出。病毒、黑客几乎每天都在困扰着互联网的用户。在银行、证券、电信等行业领域，网络的安全更是关系到整个国家的经济命脉，对于网络安全的研究刻不容缓。

目前，在网络安全方面主要采取被动的防御，比如一些杀毒软件和防火墙。为了主动的研究黑客的行为，并对他们的行为做出防范甚至反攻击，出现了网络诱骗技术，即 Honeypot。它用伪装的漏洞吸引攻击者的注意，所有进出的数据都受到容纳、捕获及控制。诱骗系统改变了传统的防御方式，更具交互性。通过获取、分析捕获到的数据，互联网上的组织将会更好地理解他们所遇到的威胁，并且理解如何防止这些威胁。

近年来国内外在这方面已作了一定的研究，从事这方面研究的有 Honeypot project[1]等研究组织和一些开发网络安全产品的企业。目前提出的 Honeypot 有各种各样的形式和规模，但大体可以分为两种类型：low-interaction honeypots, high-interaction honeypots[2]。

在商业上也出现了一些 Honeypot 产品和解决方案[3-6]，这些解决方案大多数都有一个问题：其签名是可检测的。根据它们所遗留的签名就有可能对其进行识别，这样黑客就会意识到其欺骗性并向安全的目标转移。所有这些解决方案都有着一定的功能，但是只限于某些特定的需求。一些学者也在做这方面的研究工作[7-11]，但大多是一个模型的框架，缺乏细节的描述。

针对当前的研究状况，本文从另一个角度构造了一个诱骗系统 ANSS，即诱骗系统如同在一个真实的网络环境中，

2003-12-9 收到，2004-04-27 改回
863 项目(2002AA776030), 江苏省高校自然科学研究计划(03kjb520090)和中兴基金资助课题

整个诱骗系统与在网络中其他系统是一模一样的，并且 ANSS 能够自始至终地捕获黑客的活动，同时不给网络上任何其他的系统带来危险。

2 ANSS 总体结构

在基于蜜罐的主动网络安全系统中通过成功地构建一个陷阱网络 ANSS，更好地保护真实网络。图 1 是 ANSS 的结构。它主要由防火墙/路由器、陷阱网络（Honeynet）、入侵检测系统（IDS）、数据仓库、数据过滤和监控平台组成。

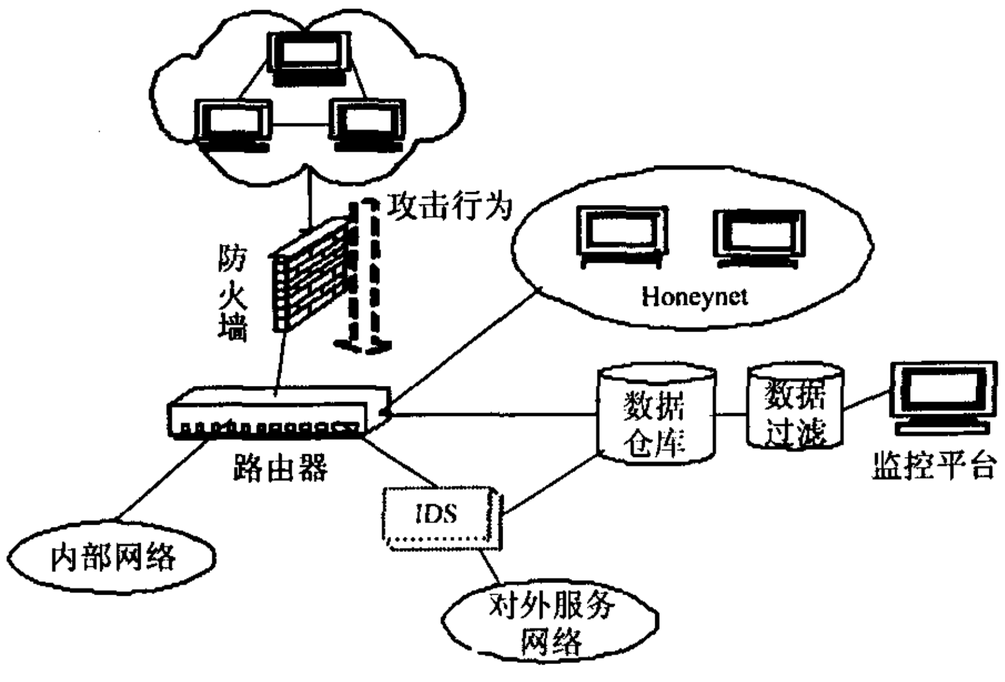

图 1 ANSS 总体结构

防火墙对流量进行控制，限制其对外的连接，但也要给黑客以一定的自由，可以获取工具，测试连接等等。除此以外路由器也对流量进行了控制，而且由于路由器的存在，使得网络更加的真实。另外它也是数据控制的一个备份，所有的流量必须经过路由器，如果防火墙失败了，路由器仍然可以执行防火墙的主要功能。它也方便了网络管理员来通过访问控制列表（ACL）对网络进行更好的管理。

陷阱网络（Honeynet）是整个主动网络安全系统的核心部分，它是一个用来诱骗黑客攻击的网络。在陷阱网络中，所有的操作系统都是真实的，当然也存在着容易引起黑客攻击的漏洞。域名服务器(Domain Name Server, DNS)是必需的，因为黑客经常利用 DNS 解析下载工具或者激活。为了赋予 Honeynet 完整的域名解析功能，所以需要在诱骗网络中增加 DNS 服务器，使 Honeynet 内发出的域名解析限制到某个特定的主机上。NTP（Network Time Protocol）服务器则会确保陷阱网络内所有的时间都是同步的。这一点对于数据的分析而言是非常有用的，这样可以保证从各个系统所捕获到的数据在同一时间。

IDS（入侵检测系统）对数据包进行捕获，并对异常的行为进行分析、发出警报。一方面通知监控平台，让其对入侵行为进行监视和分析；另一方面和路由器通信，对入侵行为进行路由欺骗。本系统的 IDS 系统可以是硬件的，也可以是软件的。

监视平台对网络中的异常流量进行分析和报警，通过对出入 Honeynet 的所有数据进行监控，但是不能与陷阱网络进行通信（我们采用了不给其配 IP 地址的方法），确保所获取的数据不会被黑黑客所破坏。

数据仓库主要是对系统日志、防火墙日志及网络流量记录进行的备份。因为系统本身的日志对我们很重要但又极易被黑客破坏，所以我们设置数据仓库来保存日志文件，以便网络管理员对入侵行为进行详细分析。

3 Honeynet 的构建

要成功地构建一个 Honeynet，就必须处理好两个问题，一个是流量的控制，另一个就是数据的捕获。

流量控制就是对进出数据的控制。何种数据能够到达何种目的地是由网络管理员来决定和控制的，这是相当重要的。数据控制的关键在于访问控制设备，例如防火墙，可用它将 Honeynet 和 Internet 的其他部分隔离开。所有进出 Honeynet 的数据首先都会经过防火墙。这里使用透明防火墙，这样黑客就不会觉察到自己正在通过一个防火墙系统了。对于访问控制设备一定要具备下面几条规则：(1) 任何人都可以发起从 Internet 到 Honeynet 的连接。这样就可以允许黑客扫描、探测并最终攻入 Honeynet 中的系统。(2) 访问控制设备控制着 Honeynet 能够发起与 Internet 连接的方式。因为它可以阻止黑客利用 Honeynet 来攻击或者摧毁 Internet 中的其他系统。一旦某个 Honeypot 被攻破了，就必须要容纳黑客的活动。这里所说的活动，指的是允许从 Honeynet 发出的对外连接。如果禁止所有发往 Internet 的连接，虽然这样可以消除绝大部分风险，但是这种做法基本上是行不通的。一旦某个 Honeypot 被攻入了，如果黑客不能发起通往 Internet 的连接，他们就会迅速对此产生怀疑。他们就会离开这个系统甚至可能在离开之前销毁整个系统，这样 Honeynet 的设置就没有任何价值。当然，访问控制设备也不能允许过多的对外连接，否则被攻入的系统就有可能被用于探测或者攻击 Internet 上的其他系统。

数据捕获记录了黑客在 Honeynet 中所做的一切活动，这也正是 Honeynet 的价值所在，只有捕获到数据才能进行分析和学习。因此对数据进行恰当正确的捕获是整个诱骗系统成功的关键。在数据捕获地点的选择方面一定要是可信的，而且要多方位的。捕获到的数据也要存放在可信的网络或主机上。例如黑客的击键存放在 Honeynet 内部，黑客就很有可能会检测到这部分数据并对其修改或销毁。在这一部分对于日志文件的备份也是很重要的，可以保存到一个远端受保护的服务器上，便于日后的分析。为了保证数据的完整性，在日志数据的传输过程中要采取加密和认证技术。

4　ANSS 中的路由欺骗

为了使欺骗网络能更好地保护真实网络，我们提出了路由欺骗算法。它的核心部分是路由转换和端口重定向，这是一个运行在内部网络中的路由协议。路由转换协议对易受攻击的端口和服务器未开放的端口进行保护，当 IDS 系统检测到攻击行为时，路由器会对攻击数据包转发，欺骗网络或蜜罐会对其作出响应，图 2 是路由欺骗算法在网络上的应用示意图。

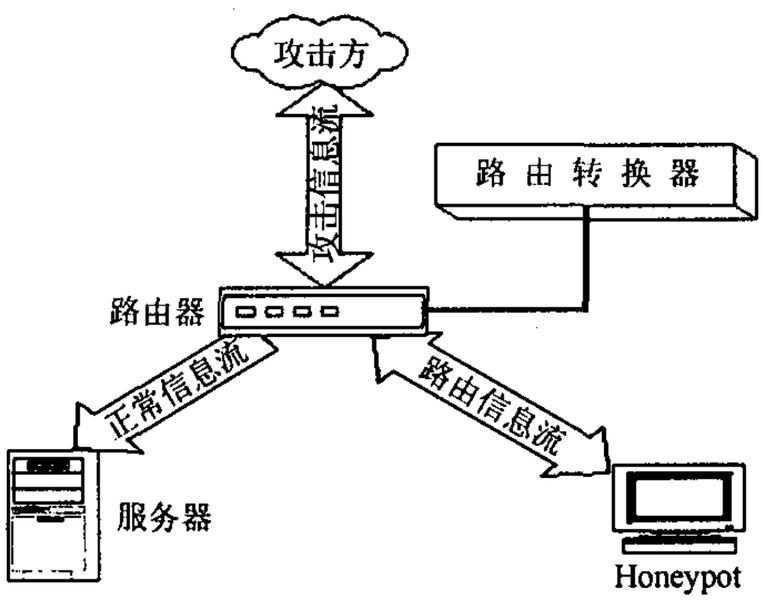

图 2　ANSS 中的路由欺骗算法示意图

转换机制主要在路由器上实现，其主要是一张类似于路由表的路由转换和端口重定向表，见表 1，路由转换表决定攻击数据包的去向。另一张 Honeypot 管理表是动态的分配 Honeypot 的连接和服务端口，见表 2。

表 1　路由转换和端口重定向表

攻击 IP	服务器 IP	服务端口	Honeypot IP	重定向端口	转包数
攻击 IP1	服务器 1	80	Honeypot 1	80	300
攻击 IP2	服务器 2	21	Honeypot 2	21	300
攻击 IP3	服务器 3	23	Hoenypot 3	23	300

表 2　Honeypot 管理表

Honeypot IP	服务端口	空闲端口	连接数
Honeypot 1	80	21，23，…	1
Honeypot 2	21	80，23，…	1
Hoenypot 3	23	21，80，…	1

诱骗网络中的某个 Honeypot 启动时它会向路由器发送一个数据包，通知路由器 Honeypot 的上线信息，路由器更新其 Honeypot 管理表。转换表中的转包数是为了减少网络的消耗和防止产生网络瓶颈，因为对网络上每一个数据包检查要消耗大量的网络资源和带宽。当 IDS 检测到某个数据包为攻击包，在路由器转换表上设置一个转包的初值 N，在这以后来自这个 IP 相同端口的 N 个数据包认为其为攻击数据包。这样的设法是非常巧妙的，根据实际情况黑客的攻击行为往往是一连串的攻击包，本系统能很快地做出诱骗的反应，又减轻了 IDS 的网络负荷。转包数是一个变化的值，网络管理员要根据其网络环境和黑客攻击的一般统计规律进行设置。转包数要定期置为 0，以适应不断变化的网络环境和提供正常的服务。

例如网络上某黑客（攻击 IP1）试图对服务器 1 开放端口 80（web 服务）进行攻击，但路由器不能对其检测（因为其转换表中没有改 IP 地址），路由器让其通过。经过 IDS 系统检测后确定其为恶意包，通知路由器。路由器根据 Honeypot 管理表的连接数和空闲端口决定转换的 Honeypot 主机。路由器根据表的内容决定重定向主机为 Honeypot 1，端口号为 80，设定转包数的初值为 300，以后一定的时间内有来自这个 IP 相同端口的数据，路由器对其转发和诱骗，相应的转发数据包数减一。然后路由器根据 Honepot1 的 IP 地址查出 MAC 地址，封装成帧发给 Honeypot 1。如果转发数据包数值减为 0，路由器让其正常通过，IDS 再对其进行检测。如果在一定的时间内没有来自该 IP 和端口的数据包，路由器要将路由转换表包含此 IP 和端口号的行撤销，并更新 Honeypot 管理表。通过这样的转换和端口的重定向，诱骗网络很好地保护了服务网络。

端口重定向主要是为了节省主机(Honeypot) 资源，有效的利用 Honeypot 的不同端口对不同的攻击行为进行诱骗。例如当我们的服务网络中还有一台服务器被攻击时，诱骗网络中没有连接数为 0 的主机，我们仍然可以利用 Honeypot 的其他端口提供服务。即使网络中只有一台主机时，也可利用不同端口进行诱骗。

路由器、IDS 和诱骗网络上的日志和报警信息要定期的发往分析主机，以便网络管理员对网络进行监控和管理。通过运用路由欺骗技术，我们可以跟踪黑客行为、分析黑客的攻击技术和心理，构建更加安全的网络系统。

5　实验与仿真

我们在一个实际的校园网络中进行了仿真实验。在诱骗网络中布置了 Sun 的 Solaris ftp 服务器。这些操作系统我们都采用了缺省安装，因此它们都具有一些常见的系统漏洞。在分析平台上安装 IDS，为了安全起见我们不给其配置 IP 地址。

我们对黑客的攻击行为进行了相应的研究，并开发了扫描攻击软件，扫描是黑客发起攻击的第一步，我们对诱骗网络中的某台 Honeypot 主机进行扫描，图 3 是扫描模块进行扫描的图示。

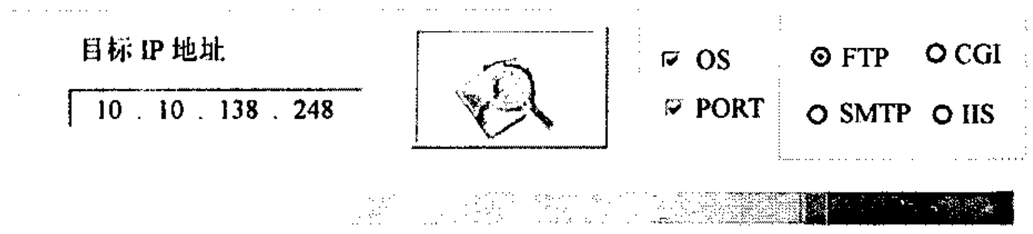

图 3 扫描模块进行扫描的图示

IDS 系统很快检测到本次扫描，经过数据的过滤，在分析平台上看到的报警数据如图 4 所示。

```
[1:620:3] SCAN Proxy (8080) attempt
[Classification: Attempted Information Leak] [Priority:2]
0./31-09:47:53 . 024386 10.10.138.242:1177 -> 10.10.138.248: 8080
TCP TTL:128 TOS:0x0 ID:49263 IpLen:20 DgmLen:48 DF
Seq:0x6F7A842F ACK:0x0 Win:0x4000 TcpLen:28
TCP Options(4)
```

图 4 报警数据

从图 4 的数据可以看出本次进行的攻击是一次扫描，并且来自内部，网络管理员要对其行为进行限制。实践证明我们的 ANSS 能检测到黑客的攻击行为，并对其进行监控，更重要的是这样我们可以学习到黑客的攻击手段和方法。

6 结束语

诱骗系统是用来获取黑客团体的智慧、使用的工具、方法策略及他们的动机。我们构建的诱骗系统的特点在于它是一个包含多系统、复杂的网络环境,它没有对任何东西进行模拟，而由一些真实的操作系统和应用程序组成。我们设计的全新的路由算法能对真实网络进行更好的保护，它的核心部分是路由转换协议，这是一个运行在内部网络中的路由协议。路由转换协议对易受攻击的端口进行保护，当黑客尝试攻击受保护的端口或服务器未开放的端口时，由于路由转换协议的存在，欺骗网络会对其做出响应。路由转换协议分为服务器与服务器，服务器与 Honeypot 之间的通信。服务器上主要维护路由转换表、计数表和服务器 IP 表，在 Honeypot 上主要维护转发表和服务器 IP 表。在数据分析方面我们采用了审计数据统计的数据挖掘技术，能更高效的对数据进行分析。一旦被攻入，ANSS 就不仅能够告知我们黑客的操作方式，而且还能识别出该环境所存在着的风险和薄弱环节，此诱骗系统已用于我们承担的 863 项目：分布式入侵检测与预警系统中。

参 考 文 献

[1] The honeynet project. http://project.honeynet.org.

[2] Lance Spitzner. Definitions and value of honeypots. http: //www.tracking-hackers.com/papers/honeypots.html, 2003, 5.

[3] Deception Toolkit. 2001. http://www.all.net/dtk/index.html.

[4] Intrusion battleground evolves. http://www. nwfusion. com/reviews/ 2001/1008bg.html.

[5] Review: Intrusion-detection products grow up. http://www.nwfusion.com/reviews/2001/1008rev.html.

[6] The honeynet project: Know your enemy. 2002,12, http://www.linuxsecurity.com/feature_stories/honeynet-review-kye.html.

[7] Klug D. Honeypots and intrusion detection. 2000.9.13, www.san.org/infosecfaq/honeypots.

[8] 夏春和，吴震，赵勇，王海泉. 入侵诱骗模型的研究与建立. 计算机应用研究, 2002, (4): 76 – 79.

[9] 杨书凡，李方敏，朱剑丘，刘新峰. 架构主动方式的网络安全系统. 通信学报，2003，24(7): 170 – 175.

[10] Levine J, LaBella R, Owen H, Contis D, Culver B. The use of honeynets to detect exploited systems across large enterprise networks. Proc. of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY, June 2003, www.tracking-hackers.com/papers/gatech-honeynet.pdf

[11] Nathalie Weiler. Honeypots for distribute denial of service attacks. 2002, 10, http://www.tik.ee.ethz.ch/~weiler/papers/wetice02.pdf.

孙知信： 男，1964 年生，副教授，研究方向为计算机网络、软件工程.

扬家园： 男，1982 年生，硕士生，研究方向为网络安全.

施良辉： 男，1982 年生，硕士生，研究方向为网络安全.

王汝传： 男，1942 年生，教授，研究方向为计算机网络和分布式计算.