 随着Internet的高速发展，个人、企业以及政府部门越来越多地依靠网络传递信息，然而网络的开放性与共享性使它正遭受着来自黑客、脚本编辑者所带来的巨大的安全威胁，分布式拒绝服务攻击、被控主机敏感信息的窃取，严重地影响了网路的正常工作，一个安全可靠的防御网络成为现在安全领域的一个热点。究其根源，是攻击者与防御者之间在进行着一场不对称的博弈，特别是信息上的不对称，攻击者可以利用扫描、探测等一系列技术手段全面获取攻击目标的信息，而防御者对他所受到的安全威胁一无所知，即使在被攻陷后还很难了解攻击者的来源、攻击方法和攻击目标，蜜网技术就是为了扭转这种不对称局面而提出的。 1 蜜网技术原理 蜜网技术实质上仍是一种蜜罐技术，是一种对攻击者进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务以及信息诱使攻击者对他们进行攻击，减少对实际系统所造成的安全威胁。但蜜网有其自身特点：首先，蜜网是由多个蜜罐以及防火墙、入侵防御系统、系统行为记录、自动报警、辅助分析等一系列系统和工具所组成的一整套体系结构，这种体系结构创建了一个高度可控的网络，使得安全研究人员可以控制和监视其中的所有攻击活动，从而去了解攻击者的攻击工具、方法和动机。其次，蜜网是一种高交互型的用来获取广泛的安全信息的蜜罐，高交互意味着蜜网是用真实的系统，应用程序以及服务来与攻击者进行交互。 蜜网体系结构具有三大关键需求:即数据控制、

数据捕获和数据分析。数据控制是对攻击者在蜜网中对第三方发起的攻击行为进行限制的机制，用以降低部署蜜网所带来的安全风险。最大的挑战在于对攻击数据流进行控制而不能让攻击者怀疑:我们必须要给攻击者一定的自由度，允许他们做大部分“ 合法 ”的事情，比如从网络上下载入侵工具包等，这样才能获取信息，学习他们的攻击方法，但是要拒绝所有攻击其它机器的行为，这就需要一个自由度和安全性的权衡。数据捕获，即监控和记录攻击者在蜜网内的所有行为，最大的挑战在于要搜集尽可能多的数据，而又不被攻击者所察觉。数据分析则是对捕获到的攻击数据进行整理和融合，以辅助安全专家从中分析出这些数据背后蕴涵的攻击工具、方法、技术和动机，在分布式部署的蜜网体系中，还存在着将多个蜜网中捕获数据进行安全地传输到一台中央服务器，并进行集中化分析的分布式数据收集需求。 2 基于LINUX蜜网的防御系统的实现 本系统中使用IP分布如下: Name |Type |IPorGroupitems |DescriptionFirewall |Workstation |10.10.14.11 |honeynetadministratorRoxen |Workstation |10.10.14.20 |runningtheRoxenwebserverDNS |Workstation |10.10.14.23 |DNSserverApache |Workstation |10.10.14.30 |webserver，vulnerabiliable Honeynet |Group |Roxen DNS Apache |Theseareourhoneypots本honeynet没有故意留下了漏洞，但可以通过Apache能够给用户一个nobodyshell，再使用EOE防止普通用户成为root，这样限制了攻击者所能做的事。在此基础上增加策略： (1)有主机都可以通过ssh或MYSQL连通/firewall； (2)有主机都可以连接到honeynet这个组； (3)honeynet允许连接到任意主机； (4)除了以上之外，所有的

通信都被拦截；(5)所有防火墙允许通过的数据都记录。 因此策略可以有下面四条： Num Source Destination Service ActionLog00 Firewall sshorMySQL AcceptLog01 honeynet any acceptlog02 honeynet any anyacceptlog 03 other any 0droplog进行日志服务器配置 日志服务器数据库采用MYSQL，首先在MYSQL中建立snort和ssyslog的用户并分别给他们对各自数据库的INSERT，DELETE，USAGE，SELECT权限方法如下： Echo CREATE DATABASE snort；| mysql u root - pmypass mysql> grant INSERT，SELECT on snort.* to root@* ；入侵检测系统配置 作为一个Honeynet，有大量的数据需要手工分析，IDS在这里可以起到很大的帮助。主机型入侵检测系统往往以系统日志、应用程序日志等作为数据源，它保护的一般是所在的系统。网络型入侵检测系统的数据源则是网络上的数据包。往往将一台主机的网卡设于混杂模式(promiscmode)，监听所有本网段内的数据包并进行判断。一般网络型入侵检测系统担负着保护整个网段的任务。作为Honeynet，从目的考虑，我们需要捕获网络及主机上的所有信息。这时主机IDS的必要性不是非常明显，所以主机只要能够阻止用户执行shell或者成为超级用户就可以了。网络层使用snort作为入侵检测的记录工具。 主机IDS：EyeonExec如我们上面所说的，EyeonExec就是一个阻止用户执行shell或者成为超级用户的微型HIDS，它可以在发现这样的企图后报警，并且发送mail给系统管理员。更多资料请访问：100testLinux认证栏目[1] [2] 下一页 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com