基于 honeyd 对蜜罐技术的应用及分析

黄晟 唐宾徽

四川大学锦城学院 计算机与软件学院 四川 成都 611731

【摘 要】：信息化时代下虽然现代化的计算机以及网络实现了高速普及，计算机网络安全问题成为目前社会各界比较关注的热点。蜜罐技术是当下社会一种常见的网络安全防范手段，计算机与网络用户在生活和工作中，很多私密性的信息被泄露，影响了正常的计算机与网络建设秩序。一些数据中心或者运营商企业会试图设置诸多蜜罐来对攻击者的攻击进行诱导、检测分析、溯源等一系列操作，信息化时代下计算机网络安全所面临的严峻形势不容被忽视。

【关键词】：计算机网络安全；蜜罐技术；信息分析；实现方法

1.蜜罐技术的基本原理解析

蜜罐技术的原理类似于一个诱敌深入的陷阱，常见的网络攻击中，攻击者会在可攻击范围内寻找一台极易被攻击的设备，攻击者通过扫描设备群中漏洞最多的一台设备进行攻击，正是由于这个原因，网管人员利用自身的网络技术搭建一台希望被攻击者进行攻击的一台诱敌机，这台诱敌机可以是服务器也可以是一台简单的物理机，并且这台服务器或者是物理机上存在的漏洞较多，但是这台主机创造一个对攻击的攻击方式进行检测分析的前提，这个是蜜罐技术的基本原理。一旦攻击者入侵后，就可以知道攻击者是如何得逞的，随时了解针对服务器发动的最新的攻击和漏洞．还可以通过分析攻击者所采用的种种工具了解新的攻击方式[1]．网络环境中只要对于各种计算机网络安全漏洞疏于管理，就会为计算机网络危机的产生创造了条件。蜜罐技术有利有弊。在选择蜜罐技术时要从理论和实际等方面同步出发，合理地使用蜜罐技术保障网络的安全。

2.多种常见的蜜罐类型

对于蜜罐的类型来说没有哪个类型的蜜罐来说是最好的，在大型的网络结构中，要根据实际需求选择类型合适的蜜罐，不同的网络环境适合的蜜罐类型也不相同，蜜罐大致上分为几个类型，按蜜罐与攻击者的交互程度分类为高交互、低交互型蜜罐，交互性指的是攻击者在蜜网中的一种自由程度，自由程度越高交互性越高，一般来说，要想对攻击的检测和分析更为具体需要高交互型蜜罐来作为被攻击对象。按蜜罐的结构类型可分为虚拟蜜罐、物理蜜罐，虚拟蜜罐的设计就是利用一个物理的虚拟机软件程序模仿多个真实的主机，伪造成一个大型的网络环境类型。物理蜜罐的概念就是真实的一个物理计算机。这样的一种蜜罐方式不易被攻击者识别出来，但是消耗的资源较多，根据设计的最终目的可以分为产品型、研究型蜜罐，产品型蜜罐，产品型蜜罐的主要作用就是被攻击者攻击，属于低交互型的蜜罐类型，而研究型蜜罐不同，在各种资源较多的时候，有些企业会选择研究型蜜罐，研究型蜜罐采用真实主机来承担蜜罐的角色，主机上运行的服务较多，攻击者可进行的交互程度也更高，这样，企业就会获取攻击者更多攻击的信息。

3.honeyd 针对虚拟网络环境搭建的若干实现

3.1 蜜罐环境的搭建

首先要配置蜜罐环境，配合 libenvent,libdnet,libdcap 三个函数库进行环境的搭建，这三个环境是配置蜜罐的前提，在运行软件之前，还有一个前提是我们自定义的蜜罐能够对分配给它的地址作出 arp 响应。我们可以通过安装运行 arpd 软件来做出 arp 应答。当蜜罐主机的 mac 地址请求时，软件能够做出地址解析。

3.2 配置蜜罐的实现

配置虚拟蜜罐网络拓扑

create windows

set windows personality "Microsoft Windows NT 4.0 SP3"

#命令配置一个叫做 Windows NT 4.0 SP3 的模板，对应设备的类型。

bind 1.1.1.1 windows

bind 1.1.1.2 windows

bind 1.1.1.3 windows

#命令绑定了三个蜜罐机的地址，并且着三个地址为同一网段，通过三个虚拟地址模拟一个简单的网络环境。

route entry 1.1.1.9 network 1.1.0.0/16

route 1.1.1.9 link 1.1.1.0/24

bind 1.1.1.9 router

#命令绑定一个虚拟路由器的地址，配置路由输入网络和链路连通问题，也可通过路由增加网段配置路由表里面的数据，让多个路由器相互连接的多路由结构的连通性，蜜罐软件让蜜罐读取配置文件时，蜜罐就可以模拟真机，当一个客户端试图用 NMap 或者 XProbe 等探测工具探测蜜罐的指纹时就能伪装成真实系统。并且虚拟网络的入口路由为虚拟路由器的地址。

add windows tcp port 80 open

add windows tcp port 21 open

#在蜜罐上打开两个端口，分别对应文件传输协议和超文本传输协议，模仿真实运行的实机，这样更不易被攻击者发现攻击的是蜜罐。

3.3 运行 honeyd 的实现

切换到创建的蜜罐配置文件的目录下，配置的虚拟蜜罐网络要使用 honeyd 命令来读取刚刚配置的虚拟蜜罐配置文件。并且要将防火墙暂时或者永久关闭防火墙，使得攻击者能够嗅探到网络环境。

3.4 模拟仿真服务的实现方法

add windows tcp port 80 shweb.sh

#运行脚本库中的 web.sh 配置脚本

add windows tcp port 21 sh ftp.sh

#运行脚本库中的 ftp.sh 配置脚本

利用蜜罐软件提供仿真服务脚本模拟虚拟的仿真服务，在提高交互性的同时模拟真实的服务，诱骗攻击者。安装蜜罐软件后可以在源代码包中的目录下的文件里找到软件提供的脚本 web.sh。蜜罐软件提供的脚本的语法并不复杂，基本的规则就是当攻击者登陆后，输入命令，脚本会做出相应的输出回应，配置一台虚拟主机为网页服务器。使用的端口运行配置脚本，网页服务脚本的作用是在攻击者登录仿真的虚拟网页服务器时，配置脚本能够监听攻击者对网页服务器的按键记录，网管人员可以按照自己的需求编写自己的虚拟网页服务。通过自己的诱导方式提取这段交互过程中对自己有利的信息。

3.5 信息分析的实现方法

根据编写的网页代码，通常包括用户名和密码等重要信息内容。待攻击者完成交互动作之后，浏览记录可通过脚本的监听记录保存在特定的文件里面，之后通过 tshark 命令带上服务器地址可以对数据包进行分析等一系列操作。数据的分析属于蜜罐技术中当前需要突破的难题，将手机获取的相关讯息，实行关联分析。利用数据，了解入侵人员于蜜罐系统中的所有活动以及键盘命令和使用工具、攻击目的等，进而构建入侵人员行为数据的统计模型[2]。

4.总结蜜罐技术需要改进的技术问题

4.1 交互程度的调整

高交互蜜罐在提升黑客活动自由度的同时，自然地加大了部署和维护的复杂度及风险的扩大。

4.2 作用范有限、成功率不是百分百

蜜罐不同于其他的安全设备，它是网络环境中的一个陷阱，只能对进入蜜网的攻击进行分析，即将蜜网中的蜜罐安全漏洞较多，但还是不能完全保证攻击者能够进入蜜网当中进行攻击，

并不是所有的蜜罐都能够骗到攻击者，计算机网络的发展是在攻击者与被攻击者相互成长发展起来的，所以有些有经验的攻击者会识别出蜜罐，他可能会绕开密网进行攻击或者伪造攻击信息进入密网，诱导网管人员进行一些错误的操作。世上没有绝对安全的说法，蜜罐服务器容易被攻击者攻破，也容易被攻击者利用成跳板，从而连接进行更加深层的渗透。

4.3 功能性健壮

因为在一个完整的网络体系中，有漏洞就有一定的危险因素，所以蜜罐技术需要解决的问题是这类存在漏洞的服务器或物理机会不会对内网的服务器、物理机或者网络设备的安全产生影响，对于大型的运营商或者是数据中心来说，如果内部网络资源中的某些漏洞被攻击者利用或者一些蜜罐被作为跳板机将会对整个数据中心的安全性产生影响，所以说蜜罐技术是存在一定的风险的，所以引入了蜜网的概念，蜜网阶段是在蜜罐技术之上逐渐发展起来的，它本身就是一个网络体系架构，在网络体系内运用多种工具收集入侵者信息，同时也提高了网络的可控性。虚拟蜜网是利用虚拟计算机技术组建而成的一套网络系统。这样可有效实现降低蜜网设计成本的目的，并可实行维护、管理[2]。密网的意义在于蜜罐搭配了其他的网络安全设备，对网络安全设备更加灵活的一个组合，通过建立反向防火墙、入侵检测设备与蜜罐于一个整体这样的一个集合被称为蜜网，它的作用相对于蜜罐来说更加健壮，防火墙起到一个控制蜜网与业务网络之间安全的作用，入侵检测设备对攻击的数据进行检测出来进行分析。虽然蜜罐技术作为一种主动防御的网络安全技术在国外

已得到大力发展，但在国内对蜜罐技术的研究尚处于发展阶段，还没有形成自己的理论体系和流派，也没有成熟的产品[3]，因此未来发展中，蜜罐技术产品可能需要一定的企业来进行发展和创新，不断地完善蜜罐技术的结构体系。在很多计算机软硬件以及网络系统当中存在一定的技术漏洞，这使得在网络正常运行时各方面都会受到一定的影响，导致运行效率的降低。计算机以及网络功能的完善是为了更好地服务于用户主体，用户的体验也是计算机网络改进设计的重要依据。其实，研究型蜜罐能提供给一个保护对象的直接安全保护是非常有限的，但是研究型蜜罐所提供的信息对于保护对象来说却是非常有价值的，通过这些信息，保护对象可以改进攻击防御、攻击检测甚至可以产生欺骗性的攻击响应。研究型蜜罐常被架设在高校、政府、军队或其他对学习黑客攻击有兴趣的大型组织中[4]。在我们当代社会，社会集体和国家应该加快对现代化计算机以及网络技术人才的培养和吸收，提升计算机网络安全风险的应对和处置能力。除此之外，相关的网络企业对于计算机以及网络软硬件设备的研发，要充分保证系统运行的稳定和高效，完善软硬件设施的基础配置。在信息化以及网络化的高速发展背景下，我国的网民数量逐年提升，用户对于计算机以及网络也产生了较强的依赖性，计算机以及网络已经成为目前我国现代化建设的重要基础设施，虽然计算机以及网络技术每年都在升级和换代，但是在使用过程中仍然存在诸多不确定性，强化信息化时代下计算机网络安全建设，不仅可以充分保障网络用户的个人隐私信息，同时也能避免网络用户在消费过程中受到欺诈和损失。

5 总结

本文主要讲述了蜜罐技术的原理、分类和一些需要改进的问题，并通过模拟一个虚拟网络蜜罐来进行演示简单的蜜罐防范流程，其中有一些重要的配置文件的配置和网络环境的规划。通过一系列实验，充分了解目前计算机网络安全构建体系中蜜罐技术的作用以及实践价值，也希望网络发展过程中，通过不断改进蜜罐技术，使得蜜罐在保障计算机网络环境正常运行问题的同时，提升各种类型的网络环境的安全性。蜜罐技术在网络安全中的发展要时刻关注当下网络安全技术的发展，不同的网络背景适合的网络安全防范措施会有所区别。不断完善蜜罐技术才能在网络安全防护中起到关键性的作用。

参考文献：

[1] 胡山泉,于芳,龚德良.基于主被动结合防御的网络安全体系[J].湖南城市学院学报(自然科学版),2005(04):74-76.

[2] 付强,刘青华.蜜罐技术在网络安全领域中的应用[J].中国高新技术企业,2016(30):60-62.

[3] 姚东铌.蜜罐技术的原理及现状研究[J].企业导报,2010(06):288-289.

[4] 朱思奇. 基于 Honeyd 的蜜罐系统的设计与实现[D].上海交通大学,2010.