

基于两级重定向机制的蜜网研究和设计

许显月, 张凤斌

(哈尔滨理工大学 计算机学院, 黑龙江 哈尔滨 150080)

摘 要:针对当前蜜网部署中存在两个不足之处:一是如果黑客知道蜜网的存在,从而绕开它去攻击非蜜网主机,这样蜜网存在就没有价值;二是如果黑客利用攻陷的蜜罐去攻击外网主机,现在流行的办法采取蜜网网关来简单限制外出连接数,这存在两个致命的弱点:(1)少量的外出连接有可能造成危害,蜜罐被人误认为攻击者;(2)黑客知道自己被限制向外连接,那么蜜网就可能被暴露,更有可能利用错误消息迷惑蜜网部署者。文中提出两级重定向机制来弥补这两个不足之处。第一级重定向机制在非蜜网主机设置使对其攻击流定向到蜜网,第二级重定向机制把从蜜罐出去的攻击流定向到其它蜜罐。通过文中建立的模拟蜜网很好地实现了这两种机制,实验证明基于两级重定向机制的蜜网可以起到保护非蜜网主机的作用,限制对外入侵,同时能让黑客感觉不到它的存在。

关键词:蜜罐;重定向;蜜网;两级

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2009)05-0158-04

Research and Design about Honeynet Based on Two-level Redirect Mechanism

XU Xian-yue, ZHANG Feng-bin

(Computer College, Harbin Univ. of Sci. and Tech., Harbin 150080, China)

Abstract: There are two defects in the current honeynet deployment. Firstly, if the hackers know of the existence of honeynet, thus bypassing it to attack non-honeynet host, so there will be no value; secondly, if hackers use compromised honeypot to attack the non-honeynet host, now popular way is taking network gateway simply to restrict connect on the number, there are two fatal weaknesses: (1) outside connections probably cause harm and honeypot maybe be mistaken for attackers; (2) hackers know that they were restricted from outside connections, then the honeynet could be exposed, are more likely to use error messages to confuse honeynet deployer. Therefore recommend two-level redirect mechanisms can make up for deficiencies. First-layer redirect mechanism by setting up non-honeynet host to redirect attack stream to honeynet, the second-layer mechanism redirect attack stream from a honeypot to another honeypot.

Key words: honeypot; redirect; honeynet; two-level

1 相关工作

为了对抗网络犯罪,多种网络安全防护技术如防火墙、入侵检测、身份认证、访问控制、密码技术等应运而生,传统的这些网络安全技术大多是被动的,如防火墙,它有一些难以克服的缺陷:无法防御通过防火墙以外的其他途径进入的攻击;无法防御带病毒的数据进入网络;不能抵抗未知的漏洞攻击;无法防御内部攻击等。入侵检测系统虽然一定程度动态地检测外部攻击和内部攻击,但它会产生大量的错误报警信息,产生的漏报将导致对真正的恶意行为“无动于衷”。而且这些

技术越来越为黑客们所熟悉,如何绕开这些防护手段已经是黑客们经常研究的课题。要避免攻击,就要了解自己面临的威胁和攻击者的情况。蜜罐就是为研究攻击者而发展起来的一项新技术,蜜罐系统主要有几种技术:网络欺骗技术、数据控制技术、数据收集技术、报警技术、入侵行为重定向技术等^[1],反蜜罐技术也取得了实质性的进展,并有商业反蜜罐软件 Honeypot Hunter 的出现^[2]。蜜罐是一种信息系统资源,其价值在于被扫描、攻击和攻陷^[3]。这个定义表明蜜罐并不提供具备信息价值的服务,因此所有流入/流出蜜罐的网络流量都可能预示了扫描、攻击和攻陷。而蜜罐的核心价值就在于对这些攻击活动进行监视、检测和分析。由该定义可以看出,蜜罐与大部分安全工具的不同之处在于:它们可以具有不同的表现形式,但其主要作用都是提供了一条获取黑客信息的途径。可以通过

收稿日期:2008-08-17

基金项目:国家自然科学基金(60671049)

作者简介:许显月(1983-),男,湖南永州人,硕士研究生,研究方向为信息安全技术;张凤斌,博士生导师,研究方向为信息安全技术。

NDS 跟 Honeypot 相互合作,共同保护工作网络^[4]。现在蜜罐技术发展到了蜜网阶段,蜜网蕴含两个概念:一个概念是它代表一种蜜罐类型即一种高交互的蜜罐,提供真实的系统、应用服务来和黑客进行交互,另一种蜜罐类型是低交互蜜罐,它通过部署 Honeyd 和 Nephentes 模拟真实服务和操作系统,简单地诱惑黑客来转移注意力,而蜜网用来捕获攻击信息并分析出对安全潜在威胁的攻击技术和工具。第二个概念是它是一种网络结构,这种结构是高度可控制的,你可以观察里面发生的任何活动,网内的不同蜜罐可以配置不同的系统和应用,达到最大程度地吸引黑客目光,并和他进行交互,这样,他的攻击动机和攻击手段全部展现在我们的面前。当前官方公布的蜜网结构基本如图 1^[5]所示。

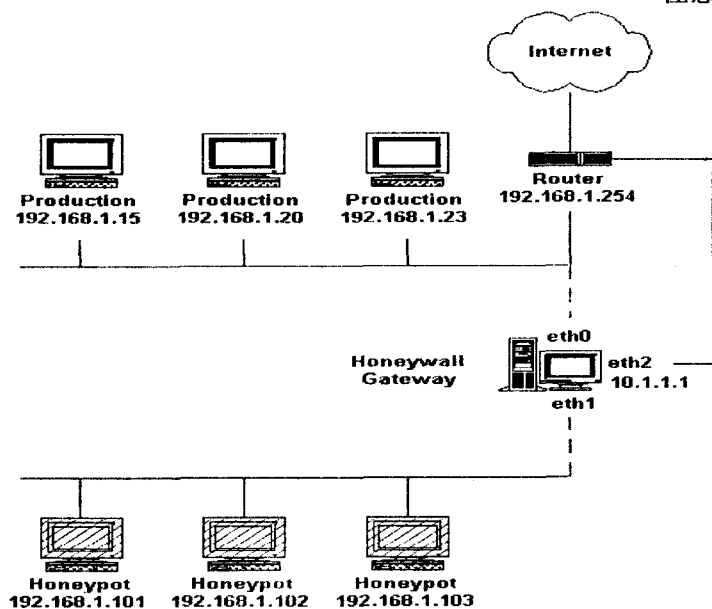


图1 蜜网基本结构

Honeywall Gateway 起到网桥的作用,文中用的 Linux 的版本是 2.4,缺省支持网桥功能,网关外部接口 eth0,内部接口 eth1 将工作网络跟蜜罐网络连在一起,在攻击者看来它们在一个网络中。工作网络和蜜网中的主机提供类似的应用服务,它们的区别在于:工作网络的主机打上系统和相应服务漏洞补丁,而蜜网的主机提供有缺陷的系统和相应服务,扫描这两个网络其实是同一个网络,发现有缺陷的主机并攻陷它,获得系统管理员用户的权限,工作网络的主机因为打上系统和相应服务补丁,攻击者对其攻击暂时不能成功,从而将注意力转移到蜜网上。在蜜网中的蜜罐部署 Sebek 客户端,攻击者的任何活动都被 Sebek 记录并将记录传送到 Honeywall Gateway 的 Sebek 服务端。在 Honeywall Gateway 中分析这些记录,重构出攻击者的行为,进一步知道攻击的策略,所使用的工具,及攻击动机。

2 两级重定向机制原理

一个系统或应用服务不存在缺陷几乎不可能,它只是在一段时间内没有被发现而已,例如微软 Windows 系统每隔一段时间就会发布更新包,这些包其实是对自身打补丁,减轻安全威胁,其他的应用软件存在同样的情况^[6]。既然这样,工作网络中的主机就会存在未被发现的系统和应用服务漏洞,对于技术高超的黑客,这样的主机会被轻而易举地攻破,而蜜网对此一无所知,更不用提检测出攻击手段,同时,如果黑客利用这台攻陷的主机去试探攻击同一个网的其他主机更容易,因为同一个网中主机相互信任,黑客利用信任关系欺骗其他主机获取重要的资源信息。蜜罐其实只是利用开放有漏洞的服务去吸引黑客,让黑客只是暂时把注意力集中到有漏洞的蜜罐上,但如果非蜜罐主机存

在不可预知的漏洞,就会同样被利用,最后被攻陷,再次,如果蜜罐开启有漏洞的服务,被有经验和技巧高深的黑客识破,他就不会去攻击,蜜罐价值就没有了,因此文中提出的第一级重定向机制用来解决这个问题,其原理是这样:在每台工作主机端口划分出开启的端口和关闭的端口,开启的端口又分为使用重定向的端口和不使用重定向的端口,不使用重定向的端口分配给用来提供比较重要的服务,如 WEB 服务,FTP 服务,SMTP 服务;使用重定向的端口提供敏感服务如 TELNET, FINGER, NETBOIS, 配置只用来只允许特定的 IP 区间进行访问,任何其它 IP 区间针对该主机重定向端口的扫描流和攻击流都会被重定向到相应的蜜罐,黑客其实真正在跟蜜罐进行交互,工作主机起到中转攻击流和响应流的作用,黑客得到信息其实都是蜜罐的,黑客攻陷了蜜罐,但给他的假象是他已经攻破了工作主机。

攻击者攻陷了蜜罐以后,他的下一步就可能利用该蜜罐对外网别的主机进行攻击,平常对付此行为的方法就是严格限制从内网到外网的连接数,这虽然能有效地阻止向外入侵,但这没有给攻击者活动的自由,他们很可能怀疑自己的行为处于别人的监控之下,从而更加小心,可能他会想出办法揪出“监控设备”,利用技术如把攻击信息隐藏于大量的垃圾信息之中来欺骗监控者,让监控者疲于奔命。文中提出的第二级重定向机制来解决这个问题。原理如图 2 所示。

首先攻击者 a 攻陷蜜罐 b,如果对主机 e 扫描攻击是不允许的,但是对主机 f 就可以,其实它的攻击流被重定向到蜜罐 c,这样,攻击者认为已经攻陷了主机 f,

然后它还要利用 f 去攻击主机 g, 结果被重定向到了蜜罐 d, 一般只要两级重定向就足以迷惑攻击者, 我们要做到, 如果攻击者通过蜜罐 b 去攻击 g, 确保它也要被重定向到蜜罐 d, 否则, 攻击者发现: 通过 a → b → f → g 跟 a → b → g 这两条攻击路径得到信息不一样, 它们就会怀疑, 从而追踪, 进而找出监控它们的原因或者就会不再进行任何活动。

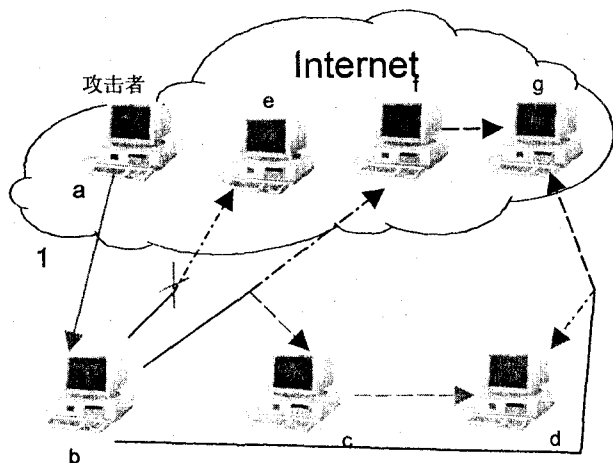


图 2 第二级重定向机制原理图

3 两级重定向机制的实现

文中要用到的是建立 netfilter 防火墙的 iptables 防火墙管理程序, netfilter 是用来实现 Linux 内核中防火墙的 Linux 内核空间程序代码段, 它要么被直接编译进内核, 要么被包含在模块集中, 而 iptables 是用于管理 netfilter 防火墙的用户程序, iptables 主要有三个模块: filter 表, nat 表, mangle 表, 分别实现不同的功能。filter 表是默认的表, 他真正实现防火墙过滤规则, 有 INPUT, OUTPUT, FORWARD 三条规则链; nat 表实现源和目的地址和端口转换, 有 PREROUTING, OUTPUT, POSTROUTING 三条规则链; mangle 表用于设置特殊的数据包路由标志的规则, 这些标志随后被 filter 表中的规则检查, 有 PREROUTING, OUTPUT, POSTROUTING, INPUT, FORWARD 等 5 条规则链^[7]。这 3 个数据处理模块都是 netfilter 的钩子函数和 IP 表^[8]。

首先设置每台工作主机的 iptables 防火墙的 shell 脚本, 脚本里面为经常使用的名字或地址定义了符号常量, 因此防火墙的脚本就极易读懂和维护:

```
# ! /bin/sh
IPT="/sbin/iptables" # 系统中 iptables 的路径
INTERNET="eth0" # 因特网所连接的网卡
IPADDR="my.ip.address" # 本机 ip 地址
PRIVPORT="0:1023" # 定义授权接口范围
UNPRIVPORTS="1024:65535" # 定义非授权接口范围[7]
```

下面开启必须提供的服务, 例如开启 WEB 服务:

```
# 允许外网建立连接
if[ "$CONNECTION_TRACKING" = "1" ]; then
    $IPT -A INPUT -i $INTERNET -p tcp \
    sport $UNPRIVPORTS \
    -d $IPADDR --dport 80 -m state NEW -j ACCEPT
# 允许外网数据传输
Fi
$IPT -A INPUT -i $INTERNET -p tcp -sport $UNPRIVPORTS \
    -d $IPADDR --dport 80 -j ACCEPT
```

```
# 允许本机服务应答
$IPT -A OUTPUT -o $INTERNET -p tcp ! --syn \
    -s $IPADDR --sports 80 \
    --dport $UNPRIVPORTS -j ACCEPT
```

其他服务如 FTP, SMTP 等服务开启类似于上面。对于像 TELNET, FINGER, NETBOIS 等服务, 只提供给特定的 IP 区间范围如: 192.168.1.0/24 开启 TELNET 服务, 类似于 WEB 服务开启。

```
# 允许外网建立连接
if[ "$CONNECTION_TRACKING" = "1" ]; then
    $IPT -A INPUT -i $INTERNET -p tcp -s 192.168.1.0/24 \
    --sport $UNPRIVPORTS \
    -d $IPADDR --dport 23 -m state NEW -j ACCEPT
# 允许外网数据传输
Fi
$IPT -A INPUT -i $INTERNET -p tcp -s 192.168.1.0/24 \
    --sport $UNPRIVPORTS \
    -d $IPADDR --dport 23 -j ACCEPT
# 允许本机服务应答
$IPT -A OUTPUT -o $INTERNET -p tcp ! --syn \
    -s $IPADDR --sports 23 \
    -d 192.168.1.0/24 --dport $UNPRIVPORTS -j ACCEPT
```

对于不属于上述网段的数据流进行重定向到蜜罐, 假设蜜罐 ip 为 192.168.0.32。

```
# 路由决定前首先要改变数据包的目的 ip 地址和端口
iptables -t nat -A PREROUTING -p tcp -i $INTERNET \
    -s ! 192.168.1.0/24 --sport $UNPRIVPORTS -d $IPADDR \
    --dport 23 -j DNAT --to-destination 192.168.0.32
# 路由决定后要改变数据包的源 ip 地址和端口
iptables -t nat -A POSTROUTING -p tcp -o $INTERNET \
    -s ! 192.168.1.0/24 --sport $UNPRIVPORTS \
    -d 192.168.0.32 --dport 23 -j SNAT --to-source $IPADDR
```

假设每台工作主机要对应一个蜜罐,在工作主机维持一个从若干个攻击者 IP 和端口,当从相应蜜罐的数据包到达该工作主机,将其包的目的地址和端口修改为 IP 池的 IP 和端口,一对多,然后将源 IP 和端口改为本机的主机和端口,例如:

#路由决定前首先要改变数据包的目的 ip 地址和端口

```
iptables -t nat -A PREROUTING -p tcp -i $INTERNET \
-s 192.168.0.32 --sport 23 -d $IPADDR \
--dport $UNPRIVPORTS -j DNAT \
--to --destination IP池IP
```

#路由决定后要改变数据包的源 ip 地址和端口

```
iptables -t nat -A POSTROUTING -p tcp -o $INTERNET \
-s 192.168.0.32 --sport 23 -d IP池IP \
--dport $UNPRIVPORTS -j SNAT --to --source $IPADDR
```

以上都是以 TELNET 为例设置规则,其他如 FINGER, NETBOIS 服务类似。

至此,第一级重定向机制已经完成,下面设置第二级重定向机制假设攻击者已经攻陷了蜜罐 A, IP 为 192.168.0.32,他要利用向外 1 台主机或 n 台主机进行攻击,如攻击目标 IP 为 202.125.32.54,可以在网路上这样设置:

#路由决定前改变数据包的目的 ip 地址和端口

```
iptables -t nat -A PREROUTING -p tcp \
-s 192.168.0.32 --sport 0:65535 -d 202.125.0.0/16 \
-dport 0:65535 \
-j DNAT --to --destination 192.168.0.31(另一个蜜罐)
```

#路由决定后要改变数据包的源 ip 地址和端口

```
iptables -t nat -A POSTROUTING -p tcp -o $INTERNET \
-s 192.168.0.31 --sport 0:65535 -d 192.168.0.32 \
--dport 0:65535 -j SNAT --to --source 192.168.0.32
```

对于向不同的网段攻击应该重定向不同的蜜罐如攻击目标为 61.202.36.45,就应该把所有的数据包重定向蜜罐 192.168.0.33,要不然攻击者很可能因为得到都是相同的信息,就会产生怀疑,增加规则为:

#路由决定前改变数据包的目的 ip 地址和端口

```
iptables -t nat -A PREROUTING -p tcp \
-s 192.168.0.32 --sport 0:65535 -d 202.125.0.0/16 \
-dport 0:65535 \
-j DNAT --to --destination 192.168.0.31(另一个蜜罐)
```

4 实验结果分析

利用各种攻击手段对工作网络的主机进行扫描,入侵,例如:

```
telnet xxx.xxx.xxx.13 23
```

就算攻击者拥有了用户名和密码,如果不在某个 IP 区域内,同样被重定向到蜜罐上,得到只是蜜罐的信息。像这样的扫描:显式扫描和隐蔽扫描都很容易被发现进行重定向,但是对 finger 进行扫描,返回信息却出现了蜜罐的 IP 地址信息,因为蜜罐对于此类响应,会把自己的 IP 地址封装在响应包中,发给工作主机,这是本实验今后改进的地方。

对于攻击者通过蜜罐向外攻击,结果跟前面的类似,这里不做解释。

5 结束语

通过两级重定向机制可以加强对工作网络的保护,而且,从工作网络被重定向过来的攻击流进入蜜罐,这样,蜜罐就更能发挥自己诱惑敌人的作用,很容易监控对于工作网络的威胁程度,起到双重的效果,今后的工作是要完善机制的功能,在更大规模的环境进行测试。

参考文献:

- [1] 孙印杰,王敏,陈智芳.解析蜜罐技术在网络安全方面的应用[J].计算机技术与发展,2008,18(7):130-131.
- [2] 郭文举.反蜜罐技术的研究和实践[D/DB].中国优秀硕士学位论文全文数据库,2005.
- [3] Spitzner L. Honeypot - Definition and value of honeypots [EB/OL]. 2003. <http://www.tracking-hackers.com/papers/honeypots.html>.
- [4] 刘小杨.用 Honeypot 改善 NDS 性能[J].吉林大学学报:理学版,2006,44(1):68-69.
- [5] www.honeynet.org.. know your enemy [EB/OL]. 2006. <http://www.honeynet.org/papers/honeynet/index.html>.
- [6] Spitzner L. Honeypots: Tracking Hackers [M]. America: Addison-Wesley Readings, 2004.
- [7] Suehring S. Linux Firewalls: linux 防火墙 [M]. 何泾沙译.北京:机械工业出版社,2004:41-46,50-51.
- [8] 周华平.防火墙中规则的翻译及检测方法的研究[J].计算机技术与发展,2007,17(11):135-136.