虚拟 Honeynet 在校园网网络安全防御中的实现①

李巧君

(河南工业职业技术学院 计算机工程系, 南阳 473009)

摘 要: 蜜网技术作为一种主动防御机制, 为解决网络安全问题提供一种有效的方法. 通过使用蜜罐技术, 在学院校园网中部署虚拟蜜网, 实现对蜜网中数据的控制、捕获和分析. 通过对蜜网的访问收集攻击者的信息, 研究并分析其攻击战术、攻击动机以及相应的攻击策略, 从而减少校园网被黑客或木马攻击的机率.

关键词: 蜜网; 网络安全; 数据控制; 数据捕获; 数据分析

Realization of Virtual Honeynet on the Network Security in Campus Network

LI Qiao-Jun

(Computer Engineering, Henan Polytechnic Institute, Nanyang 473009, China)

Abstract: The Honeynet is a kind of active defense mechanism, provides an effective method to solve the problem of network security. In this paper, we deploy virtual honeynet in campus network by using the honeypot technology, so that we can control, capture and analysis the honeynet data. We gather information about the attacker much better by accessing the Honeynet. We also study and analyze the attack tactics, attack motivation and the corresponding attack strategy, reducing the probability of attack by hackers or Trojans for the campus network.

Key words: Honeynet; network security; data control; data capture; data analysis

1 引言

随着网络技术的深入发展, 面对层出不穷的网络攻击, 我院校园网网络中安全问题也日益突出, 越来越多的网络病毒攻击校园网络, 网络信息的安全受到极大的威胁. 传统意义上的信息安全, 一般都是防御性质的, 比如防火墙、入侵检测系统、加密等等, 但是, 与其疲于防范, 不如改变防御策略主动出击[1]. 而蜜罐技术作为一种主动防御机制, 希望做到的正是改变传统的信息安全思路, 使其更具交互, 其主要功能是用来学习了解敌人(入侵者)的思路、工具、目的.

2 Honeynet技术

2.1 蜜罐技术概述

蜜罐作为一种主动防御网络安全的技术, 具有高交互性的特点. 通过部署陷阱, 吸引攻击者, 从而降低真实网络被攻击的机率, 同时对捕获攻击者的数据进行深入分析, 掌握攻击者的攻击方法、策略等, 提高防御攻击的能力[2,3]. 主要有以下几方面的特征:

(1) “一种由被探查攻击削弱来体现价值的安全设施”;

(2) 对攻击者具有欺骗性;

(3) 没有业务上的用途, 不存在区分正常流量和攻击的问题;

(4) 所有流入/流出蜜罐的流量都预示着扫描、攻击及攻陷;

(5) 用以监视、检测和分析攻击.

2.2 Honeywall 概况

蜜罐的目的是收集损害或者被攻击的数据以及行为, 因此它们对 Internet 网络构成了潜在的严重威胁, 若要保护受到其他系统进行探测和攻击而损害的高互动蜜罐, 蜜罐被放在一个特殊的实体的后面称为 Honeywall. Honeywall 作为一个连接互联网和陷阱的透明网桥, 其目标是用来捕获网络空间中各种威胁的具体行为, 并能对捕获的数据加以分析.

① 收稿时间:2014-12-04;收到修改稿时间:2015-01-22

2.3 Honeynet 技术

蜜网(Honeynet)技术是由 Honeynet 项目组(The Honeynet Project)提出并倡导的一种对攻击行为进行捕获和分析的新技术，但在本质上来讲仍然是一种蜜罐技术. 要成功地建立一个 Honeynet，需要面临以下三个问题：数据控制、数据捕获和数据分析[4,5].

数据控制代表一种规则，你必须能够确定你的信息包能够发送到什么地方. 数据控制是对攻击者在 Honeynet 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 Honeynet 所带来的安全风险. 数据捕获，即监控和记录攻击者在 Honeynet 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.

3 蜜罐技术在校园网网络安全防御的实现

在本文研究中，根据我院校园网络环境的实际要求，通过使用虚拟软件(VMWare)和物理计算机建立一个混合虚拟 Honeynet，从而减少了物理计算机的需要. VMWare 宿主主机(物理计算机)配置 Honeywall 网关和控制机，在主机中的虚拟机中配置二台基于 Linux 和 Windows 的蜜罐，并使用一台物理计算机部署为 Windows 的蜜罐. 部署的虚拟 Honeynet 如图 1 所示.

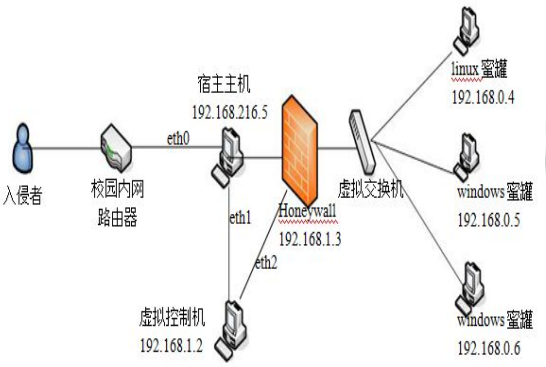

图 1　虚拟 Honeynet 网络结构图

3.1 数据控制的实现

数据控制的策略主要是对流经系统的数据进行控制. 首先，让攻击者顺利进入并攻击系统是部署虚拟 Honeynet 的目的之一，因此对流入的虚拟 Honeynet 的数据不作任何限制；然而，为了降低虚拟 Honeynet 的风险，防止攻击者将虚拟 Honeynet 作为跳板攻击其他正常系统，应对虚拟 Honeynet 外出的连接做流量限制，并且还要分析数据包抑制攻击数据包的传播.

在部署的 Honeynet 中，数据控制的第一个策略是将所有流向 192.168.x.0/24 的数据都导向 Honeywall 宿主主机上. 虚拟 Honeynet 中的两个蜜罐对于攻击者是隐蔽的，攻击者在攻击是不知道哪是真实的系统. 在防火墙中，所有主机访问校园内网路由器中 192.168.0.x/24 字段的数据均通过 eth0 导向 Honeywall 宿主主机(192.168.216.5)上，通过设置 Iptables 模块完成数据流量导向，设置如下：

[root@hn root]# Iptables –P INPUT DROP

[root@hn root]# Iptables –P FORWARD DROP

[root@hn root]# Iptables –P OUTPUT ACCEPT

[root@hn root]# Iptables –A FORWARD –I eth0 –d 192.168.0.2/24 –j ACCEPT

数据控制的第二个策略是在部署的虚拟 Honeynet 中对流出的数据流量进行了限制，每分钟流出的 TCP, UDP, ICMP 和其他协议数据包不超过 20 个，同时防火墙是否将包发给 snort_inline，snort_inline 对已知攻击包设置方式为 Replace. 若流出数据流量超过每分钟 20 个或发现已知攻击时，系统将通过 Swatch 产生 Email 报警发送给宿主主机(管理机). 具体实现如图 2 数据控制机制所示.

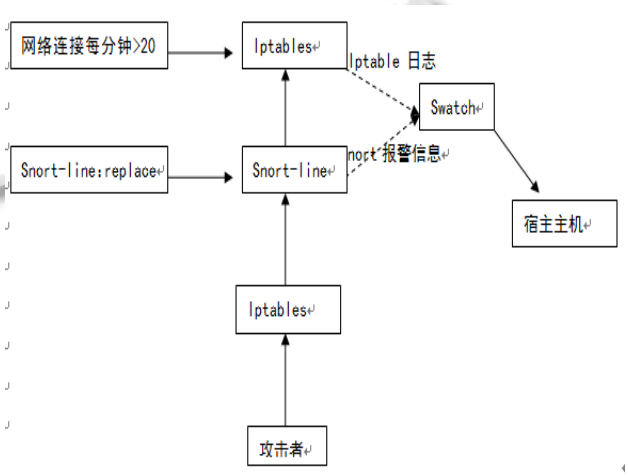

图 2　数据控制机制

3.2 数据捕获的实现

数据捕获是蜜网的一个重要目的，如果没有捕获到数据，那蜜网只能是一堆浪费网络带宽、金钱的废铁而已. 蜜网通过三个层次来捕获数据，一是 Honeywall 的日志记录；二是 snort 记录的网络流；三

是 Sebek 捕获的系统活动. 具体实现如 3 数据控制实例所示.

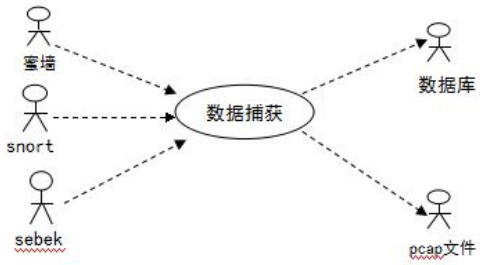

图 3 数据捕获实例

把蜜墙、snort 及 sebek 上的收集到的数据捕获, 经过处理后放到数据库和 pcap 文件中, 为后续进行的数据分析提高资料.

(1) Honeywall 的日志记录

Honeywall 的日志可以轻松捕获经过 Honeywall 的数据, 通过配置 rc.honeywall 脚本就可以实现, 在 Honeywall 日志记录中的所有进入和外出的连接均被记录到/var/log/messages, 这样可以从整体的角度来看系统干了些什么.

(2) 网络原始数据流

Snort 进程捕获所有的网络活动和内部网络接口(eth1)的数据包的数据流量信息, 包括所有用 UDP 包来发送的 Sebek 活动. 当 snort 运行在数据包记录器模式下时, 它会把所有抓取的数据包按 IP 分类地存放到 log_directory 中. 可用-h 指定本地网络, 以使 snort 记录与本地网络相关的数据包[6,7]. 命令如下: snort -vde -l log_directory -h 192.168.1.0/24

在部署的 Honeywall 中, 通过配置 snort_pacp.sh 脚本, 启动基于数据包记录器模式下的 snort, 编辑 /etc/snort/snort.conf 文件, 找到“var HOME_NET any”行, 把 any 换为宿主主机所在子网地址(192.168.1.2), 将该行改为“var HOME_NET 192.168.1.2”; 另外, 找到“var EXTERNAL_NET …”行, 将该行改为“var EXTERNAL_NET !2192.168.1.2”(注意感叹号和后面的地址之间没有空格), 其它的环境变量一般使用默认值即可. 接着找到 output log_tcpdump 一行, 日志格式的配置为 mysql 数据库方式, 将这行改为:

output database: log, mysql, dbname=snortdb user=snort host=localhost

(3) Sebek 捕获的系统活动

虽然蜜罐对于攻击者是不可见的, 但是产生在蜜罐上的大量数据应被捕获, Sebek 就是一个在数据加密情况下进行数据捕获的工具. Sebek 有两个组成部分: 客户端和服务端, 客户端安装在虚拟 Honeynet 的蜜罐上, 蜜罐里攻击者行为被捕获后发送到网络(对攻击者是不可见的)并且由 Honeywall 网关被动的收集[8].

在本次研究中, 在 Honeywall 网关上自动配置了 Sebek 的服务端, 在蜜罐 192.168.0.4、蜜罐 192.168.0.5 和蜜罐 192.168.0.6 中配置了 Sebek 客户端.

① 在 windows 蜜罐(192.168.0.6)下配置 Sebek 客户端: 指定 eth2 为网络接口; 目的 MAC: 00:0C:29:12:86:6D, 这是 Honeywall 的 MAC 地址, 是配置中的一个重要参数; 目标 IP: 0.0.0.0; 目的端口: 1101; MAGIC_VALUE: XXXXX.

② 在 windows 蜜罐(192.168.0.5)下配置 Sebek 客户端: 指定 eth2 为网络接口; 目的 MAC: 00:0C:29:12:86:6D, 这是 Honeywall 的 MAC 地址, 是配置中的一个重要参数; 目标 IP: 0.0.0.0; 目的端口: 1101; MAGIC_VALUE: XXXXX.

③ 在 linux 蜜罐(192.168.0.4)下配置 Sebek 客户端, 在 skb_install.sh 脚本中修改配置文件.

④ 在 Honeywall 网关配置 Sebek 服务端, 在 Honeywall 建立接收捕获数据的数据库 sebek 后, 使用命令: sbk_extract –i eth0 –p 1101 | sbk_upload.pl -u roo –p honey – d Sebek, 将 sbk_extract 监听 eth0 上 UDP 端口是 1101 的 Sebek 数据包, 提取出来的数据发送给 sbk_upload.pl, 它把这些数据插入到用户名是”roo”、口令是”honey”、数据库名字叫”Sebek”的本地主机数据库. 通过在 Honeywall 网关中使用命令: sbk_extract –i eth0 –p 1101 | sbk_ks_log.pl 实现捕获数据, 其中 sbk_extract 监听 eth0, 收集 UDP 端口 1101 上的数据, 然后把这些记录传递给 sbk_ks_log.pl 来提取击键活动.

3.3 数据分析的实现

当数据捕获后, 若不对其进行分析, 则捕获的数据没有任何意义, 在本文部署的 Honeynet 中, 采用自动报警机制与辅助分析机制两种机制. Swatch 工具为蜜网中的 Snort 日志文件与 IPTables 提供了视功能, 同时在被攻击时能够发出自动的报警. 在蜜网中, 主机被攻击者攻陷然后它会向外部发起连接, Swatch 工具根据指定特征的配置文件进行匹配并自动向安全管理人员发出报警邮件[9].

辅助分析采用了强大的基于浏览器的数据分析工具 Walleye，该工具安装在蜜网网关上，较多的显示对进程视图与网络连接视图，而且结合被捕获数据的多种类型在单一视图中，从而使安全管理人员能够迅速了解对蜜网中所发生的所有攻击事件[10]. 如图 4 所示.

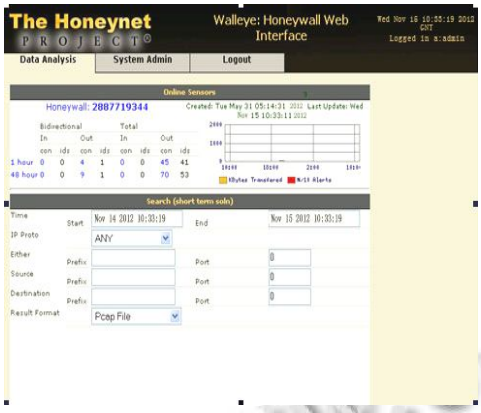

图 4 Walleye 视图

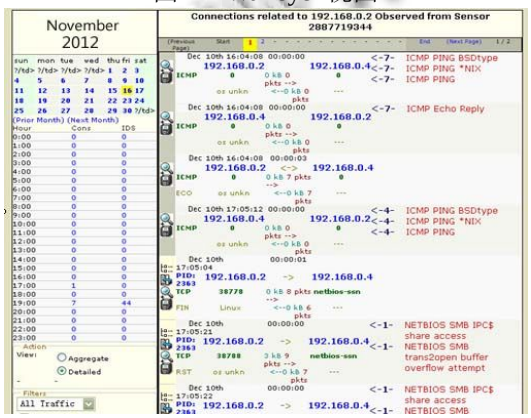

图 5 Walleye 网络流视图

在蜜网中，辅助分析机制与自动警报机制的结合，提供了非常方便的攻击数据分析流程，如图 5，如果蜜罐主机被入侵者攻击，同时发动外部连接，它将会启动自动警报机制并通过报警邮件发送给安全管理人员，并提供重要数据连接信息，如外部连接目标 IP、发起时间和端口等. 安全管理人员收到警报后，就可以将所给出的连接信息进行参考，对发生的攻击事件通过 Walleye 辅助分析接口来仔细分析，从而掌握攻击者攻击的动机与方法.

3.4 对 Honeypot 的渗透攻击

Metasploit 作为来检测系统的安全性. 在 linux 平台上版本比较老的 samba 服务的 smbd 守护进程由于对外部输入缺少正确的边界缓冲区检查，远程攻击者可以利用这个漏洞以 root 用户权限在系统上执行任意指令，本系统利用这个漏洞来进行渗透攻击. 安全漏洞检测工具选择开源免费的 Metasploit[11,12].

(1) 在宿主主机上安装 Metasploit.

(2) Metasploit 渗透攻击测试.

将宿主主机的防火墙打开，使得能够接收 4444 端口的连入. 在 Honeypot 上开放 samba 服务，然后运行 MSFConsole，输入渗透攻击命令，获得反向 shell. 攻击过程为:

```
use samba_trans2open
set PAYLOAD linux_ia32_reverse
set RHOST 192.168.0.4        // Honeypot 的 IP
set LHOST 192.168.0.2        //攻击机的 IP
show targets
set TARGET linux
check
exploit
```

通过 exploit 命令运行该漏洞利用，并且把有效负载传送到了目标系统中，

Got connection from 192.168.0.2:4321 <-> 192.168.0.4:1027 表示已经与主机建立了连接，取得了一个 root 权限的 Shell 命令行，攻击成功.

```
msf samba_trans2open(linux_ia32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Starting bruteforce mode for target Linux x86
[*] Trying return address 0xbffffdfc...
[*] Trying return address 0xbffffbfc...
[*] Trying return address 0xbffff9fc...
[*] Trying return address 0xbffff7fc...
[*] Trying return address 0xbffff5fc...
[*] Got connection from 192.168.0.2:4321 <-> 192.168.0.4:1027
```

图 6 渗透攻击过程

(3) 对攻击数据进行分析，验证蜜网数据捕获和分析功能.

漏洞渗透攻击成功，我们通过 Walleye 分析工具来查看蜜网网关捕获的数据和分析结果，发现数据记录. 如图 7.

从抓到的数据包，可以看到攻击主机发包的操作系统是 linux, IP 地址是 192.168.0.2，如图 8.

我们再看一下对攻击数据包的解码结果(见图 9)，可以看到有很长一段数据是重复的“A”或“0”，这是典型的缓冲区溢出的包的特征，可以判断这是一次缓冲区溢出的攻击.

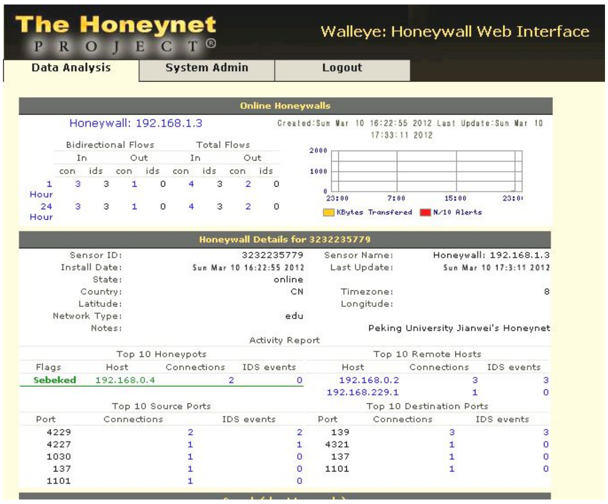

图 7　渗透攻击测试的摘要视图

图 8　被抓的数据包

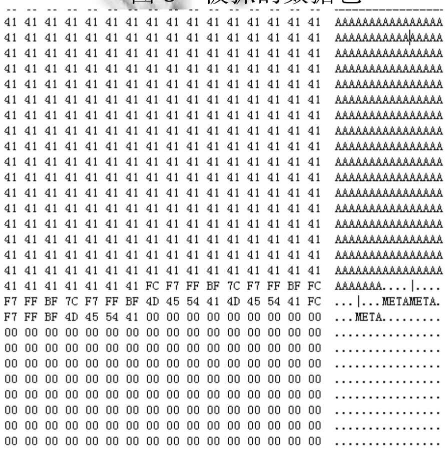

图 9　攻击数据包的解码结果

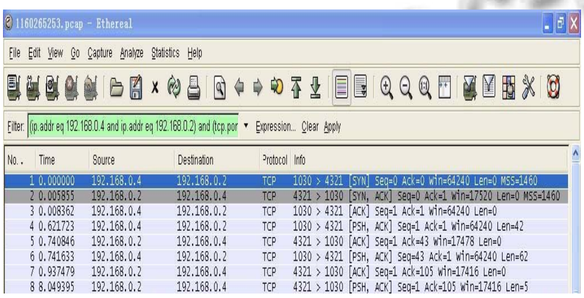

图 10　测试结果

攻击结果是得到了一个反向的 Shell，在这里我输入了 ls 和 cd 命令仅作为测试，可以看到有相应的结果输出，如图 10.

本节详细介绍蜜罐技术的三大核心机制(数据控制、数据捕获及数据分析)的实现，通过在校园内网中的实际攻击测试，验证所部署的蜜网对这些攻击测试的数据捕获和分析能力，说明本次部署各功能均达到预期效果，只要进行简单设置调整，可以广泛应用与实际互联网中，从而降低网络被攻击的概率.

4　结语

蜜网技术的提出为解决网络安全问题提供了一种有效的方法，它作为一种主动防御机制，通过部署“陷阱”使攻击者对其进行攻击，从而保护真实的网络，降低真实网络被攻击的概率，并且使用数据捕获机制将攻击者访问蜜网的数据流量和信息捕获，并通过限制数据流量等措施有效防止攻击者将蜜网作为跳板而攻击其他主机.

通过使用蜜罐技术，在校园网中部署虚拟 Honeynet 系统，解决了我院校园网内部对攻击数据信息的捕获问题，从而达到了能够更好地收集攻击者的工具数据、研究并分析其攻击战术、攻击动机以及相应的攻击策略等的效果，减少校园网被黑客或木马攻击的机率.

参考文献

1 蔡立军.网络安全技术.北京:清华大学出版社,2006.

2 李雪峰,段海新,诸葛建伟,吴建平.识别蜜罐网络的 P2P 僵尸网络构建机制.清华大学学报(自然科学版),2012,3(5):

3 刘冬梅,张志忠.防火墙中主动防御机制的研究.武汉科技学院学报,2005,18(6):9–12.

4 The Honeynet Project. Know Your Enemy: GenII Honeynets. 2005. http://www.honeynet.org/papers/gen2/index.html.

5 陈颢.蜜罐技术在网络安全中的设计与应用[学位论文].成都:电子科技大学,2012.

6 彭文波.利用 TCPDump 检测网络数据.计算机安全,2006,7:78–80.

7 赵会锋,李丽娟.一种基于蜜网的网络安全联动模型.计算机系统应用,2011,(11):128–130.

8 王乐乐.基于蜜罐技术的电子政务安全系统研究与设计[学位论文].郑州:解放军信息工程大学,2012.

9 章英,向宏,田庆宜.基于蜜网的网络攻防平台的设计与实现.微计算机信息,2007,21():45–46.

10 岳洋.基于 Snort 的蜜罐系统的设计与实现[硕士学位论文].哈尔滨:哈尔滨理工大学,2009.

11 孟江桥,李爱平.基于 Metasploit 加载 Nessus 的漏洞扫描技术实现.信息网络安全,2012,9:34–37.

12 吴文洁,葛昕,胡德敏.基于虚拟化技术的分布式蜜网.计算机系统应用,2013,(3):69–72.