

基于蜜罐的主动防御应用研究

杨德全, 刘卫民, 俞宙

(北京理工大学网络信息技术中心, 北京 100081)

摘要: 随着金融信息化的蓬勃发展, 针对金融系统的网络攻击事件也大量增长。主动防御对提高专用网络的防御水平有着重要的作用。如何快速有效的部署和应用蜜罐捕获攻击行为, 分析攻击意图, 提高攻击门槛是保障专网安全的关键所在。本文从主动防御的角度出发, 分析了蜜罐的主动防御优势, 设计了将主动防御和被动防御整合的防御生态链, 并在专网内建立了蜜罐实验环境, 结果表明, 主动防御技术可以有效提高攻击者的攻击门槛, 从而提高整体网络的安全等级。

关键词: 网络安全; 蜜罐; 主动防御; 防御生态链

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018006

Research on active defense application based on honeypot

YANG Dequan, LIU Weimin, YU Zhou

Network Information Technology Center, Beijing Institute of Technology, Beijing 100081, China

Abstract: With the rapid development of financial information technology, cyber security events on the financial system have also increased greatly. Active defense plays an important role in improving the defense level of defined private network. How to quickly and effectively deploy and apply honeypot to capture and attack behavior, analyze the attack intention and raise the threshold of attack is the key to ensure the security of the defined private network. From the perspective of active defense, the advantage of honeypot active defense was analyzed, an active defense and defense filling passive defense integration was designed, and a honeypot within private network experimental environment was set up, the results show that the active defense technology can effectively improve the threshold of the attacker's attack, so as to improve the security level of the whole network.

Key words: cyber security, honeypot, active defense, defensive ecological chain

1 引言

金融信息安全技术是现代化建设的重点问题。没有网络安全就没有国家安全, 网络安全是金融安全的一个重要支撑力量。金融网络和业务系统自诞生以来就有网络安全和病毒的双重威胁, 包括特洛伊木马、恶意代码、蠕虫病毒、勒索病毒、数据泄露、分布式拒绝服务攻击(DDoS, distributed denial of service)、0day 漏洞、APT 攻击等方面。随着网络信息技术和金融业务系统的深层次融合, 安全威胁也面临着日新月异的挑战, 如何有效防御攻击, 构建完整的主动防御生态链, 提高金融信息安全的安全状况是目前的亟需研究的课题。

收稿日期: 2017-12-05; 修回日期: 2018-01-04

通信作者: 杨德全, yanddequan@bit.edu.cn

基金项目: 国家重点研究计划基金资助项目 (No.2017YFF0207400)

Foundation Item: The National Key Research and Development Program of China (No.2017YFF0207400)

2 主动防御生态链构成

2.1 主动防御

现有的防御设备包括防火墙、入侵检测系统 (IDS, intrusion detect system)、入侵保护系统 (IPS, intrusion protection system)、流量控制设备等均处于被动防御状态。攻防双方处于不对等的状态, 防守方在明处, 攻击方在暗处。被保护的信息系统长期处于敌暗我明状态, 不利于开展网络安全防范工作, 不能够有效检测新类型攻击。

主动防御在网络传输的七层理论层级模型中均可实施, 能够在网络层和应用层的层面收集疑似攻击行为数据。主动防御偏重于发现未知威胁, 依托攻击行为对信息系统进行有针对性的渗透测试, 发现漏洞后及时修补, 并调整主动防御产品的规则和策略, 从而可动态提高整体信息系统的安全基线, 主动防御生态链闭环流程如图1所示。

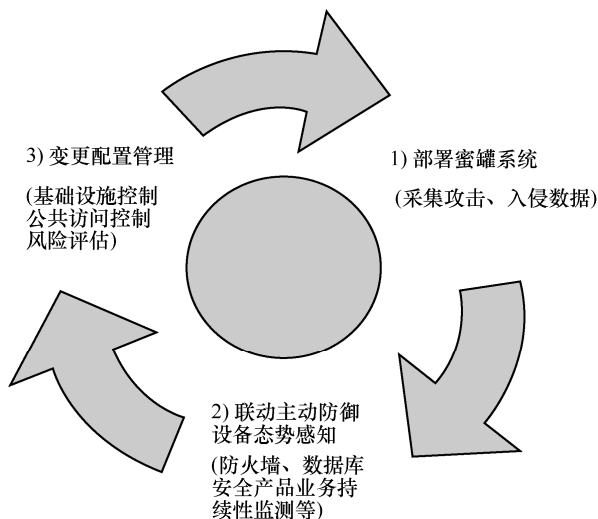


图1 主动防御生态链闭环流程

2.2 蜜罐系统

蜜罐 (honeypot) 是一种安全资源, 它的使命就是成为未经授权访问或攻击的目标, 以此获取攻击者的攻击行为和攻击策略。蜜罐是一种主动防御技术手段^[1], 该技术在网络攻防整个态势中将防御由被动化为主动^[2]。

蜜罐通过部署没有实际业务的安全资源, 诱使攻击者进入内部破坏, 防御方即可对攻击行为进行分析和研究判断, 获取攻击策略和攻击动机,

构成完整的防御生态链从而在实际的生产系统提高对应的攻击防范水平。此外, 采用蜜罐获取的数据可以协助金融信息犯罪进行电子取证。

蜜罐在主动防御方面的部分特点如下。

1) 蜜罐能够迷惑攻击方, 使其攻击行为和轨迹暴露, 入侵过程的全部数据均可被捕获, 这也是支撑金融网络犯罪取证的一个有效手段。

2) 正常的使用者一般不会进入到蜜罐系统, 故其误报率很低, 能够对外部和内部的攻击行为进行报警和关联分析。蜜罐并不作为系统提供业务功能, 因此只要有与之相关的通信即可能是攻击行为。

3) 低交互类型的蜜罐后期维护的成本较低。而高交互仿业务型的蜜罐可以协助安全研究人员研究攻击者的攻击轨迹和特性。

4) 同时在业务端口部署若干蜜罐系统可以增加攻击者的成本, 提高攻击复杂度以及不确定性, 消耗攻击者资源。

当然蜜罐也有自身的缺点, 比如若蜜罐系统被攻破后, 作为跳板机, 攻击者更容易入侵业务系统。

2.3 研究进展

蜜罐属于高级主动防御技术, 当攻击者进入高交互行为的蜜罐系统, 其对文件的修改、删除、传输等行为均会被记录并上传至后台的取证机, 从而固化证据。文献[3]研究了网络取证方法和工具, 并对蜜罐在网络取证中的价值进行了分析。文献[4]通过低交互蜜罐收集包括被攻击目标和攻击方的地址等信息, 用来发现新的僵尸网络, 实验表明, 部分僵尸网络存活时间长达700天。文献[5]在蜜罐部署后的4个月时间内收集到来自130个国家的大约10000名不同的攻击者, 大约有60000个TCP不同的连接已经登录。

文献[6]提出了利用虚拟化技术和蜜罐系统动态采集攻击信息, 并通过实验验证方法的有效性。文献[7]采用 Spampot 搭建了一个基于分布式的交互蜜罐的垃圾邮件捕获系统, 捕获了大量的攻击行为和垃圾邮件样本以及发送垃圾邮件的僵尸网络。文献[8]通过“灰盒”预测统计蜜罐网络中的参数特性, 捕获网络攻击行为, 并为防御者提供足够的预警时间来调整他们的防御配置或资源分配。文献[9]在智能电网业务系统中引入了蜜

罐作为诱饵系统检测和收集攻击信息，并制定了一个防御的最佳策略。文献[10]在物联网中部署蜜罐，采用贝叶斯的理论提出用攻防两方的博弈模型来解决防御攻击的思路，降低攻击者的成功率。文献[11]开发了基于蜜罐的监控系统用于监测 URL 重定向行为，提出了针对恶意 URL 重定向的实际对策，防范 Web 攻击。文献[12]采用蜜罐方法检测和隔离 MANET 网络中 Black Hole 攻击，应用该方法可以降低网络开销、平衡路由负载和降低分组丢失率。文献[13]利用虚拟漫游蜜罐和多层安全架构收集网络中不同级别的入侵者信息，在不产生任何流量开销的情况下对分布式拒绝服务(DDoS)进行多级防御。文献[14]提出了一种基于蜜罐检测和数据挖掘技术的入侵检测机制，预测和阻断攻击发生前的可疑行为。文献[15]基于虚拟机架设了虚拟蜜罐网络，轻量级的蜜罐系统可对动态资源灵活分配，利于数据控制、数据采集、数据显示和分析。文献[16]搭建另一个 Web 服务的蜜罐，采用自动化技术分析蜜罐收集的数据，自动捕获攻击并能够检测拒绝服务和新的攻击。文献[17]设计了一种混合蜜罐，部署在 Webserver 上，用以提高入侵欺骗系统的暴露程度，提升攻击次数，增加发现新威胁的可能性。

3 系统设计和实现

3.1 主动防御平台架构

业界认为攻击的要素包括：攻击方、攻击载体、

攻击过程。其中攻击过程包括 8 个步骤：踩点、扫描、查点、获取访问权、权限提升、窃取、清理现场、创建后门。针对金融系统的攻击往往具有结构化的，采用的技术多、隐秘性强的特点，而受保护的金融系统的防御规则应随着攻击形势的变化而做出相应的调整。在金融系统内网搭建蜜罐系统能够显著地增加攻击者的攻击时间，同时防御方可以跟踪入侵者的行为，在入侵真实的业务服务器之前修补存在的安全漏洞。对进入系统中的操作和行为进行记录和分析是蜜罐的主要目标。蜜罐部署如图 2 所示。

3.2 蜜罐云环境部署

实验环境搭建在服务器区中，所在的网络安全域属于核心业务区域。实验采用 T-Pot 平台部署，该平台采用 docker 容器技术，融合多个蜜罐平台，包括的运行实例如图 3 所示。

T-pot 平台提供的蜜罐实例按照交互程度的不同分为 3 类，高交互式蜜罐、中交互式蜜罐和低交互式蜜罐。交互性反映了攻击者和蜜罐系统之间的交互程度。蜜罐的交互级别越高，提供给攻击者的陷阱越多，蜜罐获取的攻击信息越多。实验蜜罐环境采用 VMware 虚拟云主机的方式部署。按官方指导手册，虚拟机的硬件配置如下：CPU 双核，内存 8 G，硬盘 100 G。网络和业务服务器同处于核心联动防御区域，便于捕获攻击行为。本次实验主要开启的蜜罐包括：基于 kippo 更改的中交互 ssh 蜜罐 Cowrie 和开放 Internet 常见服务的默认端口的

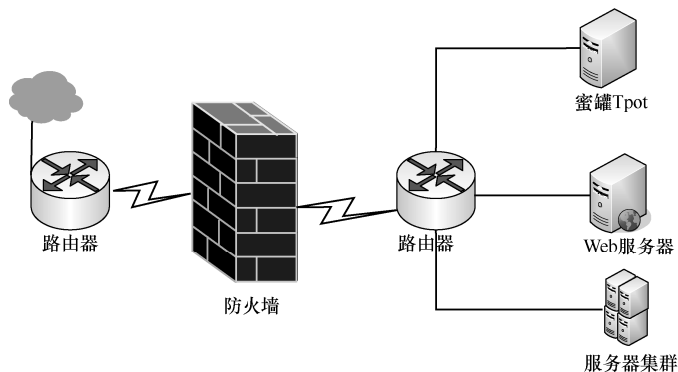


图 2 蜜罐部署网络



图 3 多蜜罐运行实例

Dionaea。蜜罐平台具有的部分漏洞分布如表 1 所示。

表 1	蜜罐模拟部分漏洞	
	服务名称	漏洞数量
	CheckPoint	1
	SSH	2
	MySQL	80
	JRun	1
	VNC	1
	PHP	1
	iPlanet	1
	MS SQL Server	2
	Apache	64
	Oracle	1
	OpenSSH	2
	其他	41

3.3 捕获数据和攻击行为分析

在核心服务器区域同时开启 2 个类型的蜜罐用以捕获不同层级的攻击数据，Cowrie 用于收集暴力破解的信息，Dionaea 用于收集对模拟开放 Internet 常见服务的攻击信息。

3.3.1 Cowrie

Cowrie 是 ssh 交互类型的蜜罐，能够捕获暴力攻击账号密码等记录，并通过欺骗环境记录入侵者的操作行为，包括输入命令、上传或下载恶意文件。实验部署捕获攻击者使用的用户名和攻击者尝试使用的密码如图 4 和图 5 所示（彩图见插页 2）。入侵者进入系统的部分执行命令如表 2 所示，入侵者的 IP 地址如表 3 所示。考虑到 IP 地址等数据较为敏感，本文对此做了去敏感化操作。



图 4 捕获攻击者使用的用户名



图 5 攻击者尝试使用的密码

表 2	入侵者进入系统的部分执行命令	
	命令行输入	执行次数
	uname	30
	uname	30
	cat/etc/bclinux-release	6
	cat/etc/klinux-release	4
	rpm-ql centos-release grep-i bclinux	4
	unset PROMPT_COMMAND	4
	PS1='[PEXPECT]\\$'	2
	cat/etc/deepin-version	2
	cat/etc/lsb-release	2
	cat/etc/neokylin-release	2

表 3	入侵者的 IP 地址	
	攻击源地址	攻击次数
	202.204.*.*	1 382
	172.25.*.*	7

应对此类攻击，防御方可以改变密码策略，将密码强度设置为 13 位以上包括字母、数字、特殊字符，并定期更改，提升安全基线。若捕获到入侵者的上传文件，可将该文件放置在沙箱中检测，分析文件的属性是否为恶意代码等。对关联的防火墙设备配置白名单，以及最小开放服务等策略，动态提升安全防范能力。

3.3.2 Dionaea

Dionaea 是模拟开放 Internet 常见服务的默认端口。包括网站服务 http 80、微软数据库服务 mssql 1433、文件传输服务 ftp 21、数据库服务 mysql 3306、基于分布式文件存储的开源数据库系统 mongodb 27017 等。当有入侵者尝试连接时，

模拟正常服务给予交互操作,并记录分析网络数据流。Dionaea 系统流量分析得到的服务流量和端口分布如图 6 所示(彩图见插页 2)。攻击者使用的用户名、尝试使用的密码如图 7 所示(彩图见插页 2)。攻击者的源 IP 如表 4 所示,其中次数较多的 IP 地址是漏洞扫描设备,其他的 IP 地址为真实的入侵者。

表 4 攻击者的源 IP 地址

攻击源 IP	次数
202.204.*.*	1 029
10.0.*.*	14
10.0.*.*	6
172.28.*.*	3
10.51.*.*	1

应对此类攻击，防御方对攻击 IP 进行排查，查看该 IP 地址是否有中木马的状况或者口令泄露导致的恶意代码执行等问题。对入侵行为日志进行分析，在防火墙将设置黑名单机制，确保业务的正常运行。针对不同业务的攻击信息对防守方发出提示，及时升级各个系统的应用系统并按

需求进行补丁管理。依据每个子系统在整体系统中重要性的不同, 设置相应的权重系数, 可以估算出整个系统的安全健康指数, 使主动防御生态链的防御更加具有针对性。

统计结果表明,实验环境上线部署后平均每周可收到 6 000 例攻击事件。在蜜罐环境中,防御者可以在入侵者不知情的情况下有条不紊地收集、分析和整理全部数字证据。分析基于蜜罐的日志文件能够帮助防御方确定攻击来源和攻击意图,对收集到的攻击信息加工梳理可指导防御设备策略的配置。防御方可协同蜜罐系统实施联动工作,在网络边界区域、核心路由器以及防火墙上设置严格的访问控制策略,组成主动防御生态链,提高网络安全防范等级。

4 结束语

在基于蜜罐系统的主动防御体系的帮助下可随着攻击者的攻击手段变化而动态调整安全策略从而提高整体网络的安全。下一步的工作展望分为 2 个方向：1) 进行分布式的主动防御设施部署，期望发现规模化的 APT（高级持续攻击）入

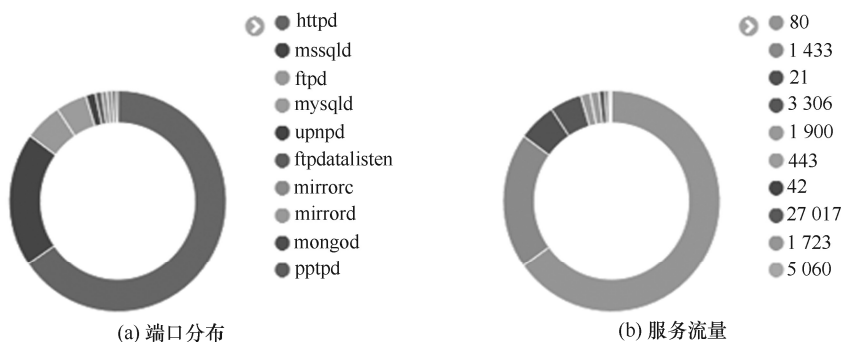


图 6 Dionaea 系统流量分析到的端口分布和服务流量



图7 攻击者使用的用户名、尝试使用的密码

侵权行为; 2) 部署与真实业务系统功能高度近似的高交互仿业务性的主动防御设施, 发现高水平的入侵者, 保障各类信息系统安全, 扩大主动防御生态链的保护范围。并可采用 COBIT 的评估方法, 拓展定制控制风险基线。将信息系统关联的数据、应用系统、设备、人员等方面纳入主动防御生态链管理当中。

参考文献:

- [1] 石乐义, 姜蓝蓝, 贾春福, 等. 蜜罐诱骗防御机理的博弈理论分析[J]. 电子与信息学报. 2012, 34(6): 1420-1424.
SHI L Y, JIANG L L, JIA C F, et al. A game theoretic analysis for the honeypot deceptive mechanism[J]. Journal of Electronics & Information Technology. 2012, 34(6): 1420-1424.
- [2] 诸葛建伟, 唐勇, 韩心慧, 等. 蜜罐技术研究与应用进展[J]. 软件学报. 2013, 24(4): 825-842.
ZHUGE J W, TANG Y, HAN X H, et al. Honeypot technology research and application[J]. Journal of Software, 2013, 24(4): 825-842.
- [3] NASIR Q, AL-MOUSA Z A. Honeypots aiding network forensics: challenges and notions[J]. Journal of Communications, 2013, 8(11): 53-84.
- [4] PHAM V H, DACIER M. Honeypot trace forensics: The observation viewpoint matters[J]. Future Generation Computer Systems-The International Journal Of Escience, 2011, 27(5): 539-546.
- [5] MARCHESE M, SURLINELLI R, ZAPPATORE S. Monitoring unauthorized internet accesses through a 'honeypot' system[J]. International Journal Of Communication Systems, 2011, 24(1): 75-93.
- [6] YANG H S. A study on attack information collection using virtualization technology[J]. Multimedia Tools and Applications, 2015, 74(20): 8791-8799.
- [7] 郭军权, 诸葛建伟, 孙东红, 等. Spampot: 基于分布式蜜罐的垃圾邮件捕获系统[J]. 计算机研究与发展, 2014, 51(5): 1071-1080.
GUO J Q, ZHUGE J W, SUN D H, et al. Spampot: A spam capture systems based on distributed honeypot[J]. Journal of Computer Research and Development, 2014, 51(5): 1071-1080.
- [8] ZHAN Z X, XU M C, XU S H. Characterizing honeypot-captured cyber attacks: statistical framework and case study[J]. Transactions on Information Forensics and Security, 2013, 8(11): 1775-1789.
- [9] WANG K, DU M, MAHARJAN S, et al. Strategic honeypot game model for distributed denial of service attacks in the smart grid[J]. Transactions on Smart Grid, 2017, 8(5): 2474-2482.
- [10] LA Q D, QUEK T, LEE J, et al. Deceptive attack and defense game in honeypot-enabled networks for the internet of things[J]. Internet of Things Journal, 2016, 3(6): 1025-1035.
- [11] AKIYAMA M, YAGI T, YADA T, et al. Analyzing the ecosystem of malicious URL redirection through longitudinal observation from honeypots[J]. Computers & Security, 2017, 69: 155-173.
- [12] BABU M R, USHA G. A novel honeypot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in manet[J]. Wireless Personal Communications, 2016, 90(2SI): 831-845.
- [13] SELVARAJ R, KUTHADI V M, MARWALA T. Ant-based distributed denial of service detection technique using roaming virtual honeypots[J]. IET Communications, 2016, 10(8): 929-935.
- [14] JIANG C B, LIU I H, CHUNG Y N, et al. Novel intrusion prediction mechanism based on honeypot log similarity[J]. International Journal Of Network Management. 2016, 26(3): 156-175.
- [15] ZHANG W Z, HE H, KIM T H. Xen-based virtual honeypot system for smart device[J]. Multimedia Tools and Applications, 2015, 74(19): 8541-8558.
- [16] GHOURABI A, ABBES T, BOUHOULA A. Characterization of attacks collected from the deployment of Web service honeypot[J]. Security And Communication Networks, 2014, 7(2): 338-351.
- [17] KIM H G, KIM D, CHO S J, et al. Efficient detection of malicious web pages using high-interaction client honeypots[J]. Journal of Information Science and Engineering, 2012, 28(5): 911-924.

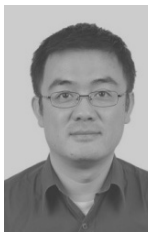
[作者简介]



杨德全 (1980-), 男, 山西应县人, 博士, 北京理工大学助理研究员, 主要研究方向为网络应用安全、安全审计。



刘卫民 (1976-), 男, 山西太原人, 北京理工大学工程师, 主要研究方向为计算机网络和无线网络。



俞宙 (1969-), 男, 浙江兰溪人, 北京理工大学副研究员, 主要研究方向为网络与信息安全。