虚拟机技术在计算机网络安全中的有效应用

何 方[1] 黄坚裕[1] 李炎强[2] 吴靖欣[2]
（1. 中国移动通信集团广东有限公司广州分公司，广东 广州 510000
2. 中国移动通信集团广东有限公司佛山分公司，广东 佛山 528000）

摘要：随着信息技术的飞速发展，计算机网络安全面临日益严峻的挑战。当然，虚拟机技术的出现，无疑给计算机网络安全管理找到了新的发展思路，以新技术、新理念与新模式的应用，或许能够维护计算机网络安全环境。事实也是如此，以虚拟机技术的漏洞检测与动态分析，能够有效解决大多问题。因此，本文探讨虚拟机技术概念，并从网络安全防护、恶意软件分析等角度呈现虚拟机技术的应用价值，希望能够为相关从业者提供更多借鉴与参考。

关键词：虚拟机技术；计算机；网络安全；有效应用

引言

如今是信息化、数字化与智慧化时代，计算机网络更是人们生活与工作的重要部分。但计算机应用的普及也带来安全威胁和数据风险，每个用户、每个企业也都面临如此风险。诸如黑客攻击、恶意入侵、数据泄露等事件频发，也让我们认识到维护计算机网络安全环境刻不容缓。通过对虚拟机技术的挖掘应用，在一台物理计算机上就可以创建多个相互隔离的虚拟环境，也算是提供了一种合理的解决思路，形成有效方案设计，以下展开讨论：

一、虚拟机技术概述

（一）什么是虚拟机?

虚拟机是一种通过软件模拟的、具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。通过此可以在一台物理计算机中运行多个甚至是不同操作系统的虚拟机实例，也因此可以实现相互隔离，避免计算机受到攻击和威胁。其中，每个虚拟机都有独立的 CPU、内存、硬盘、网络等资源，就像一台真实的计算机一样，既能够独立完成运行工作，也能够避免网络安全风险，切实营造出优良的计算机网络安全环境。

（二）虚拟机技术的分类

根据实现方式的不同，虚拟机技术主要分为系统虚拟机和程序虚拟机。前者显然拥有独立完整的计算机系统，支持多个操作系统同时运行，包括 VMware Workstation、VirtualBox 等等。而后者是程序上的独立，主要用于执行特定的程序代码，Java 虚拟机（JVM）就是一个很好的例子。

（三）虚拟机技术的工作原理

虚拟机技术的核心是虚拟化技术，通过在物理硬件和操作系统之间引入一个虚拟化层（Hypervisor），实现对硬件资源的抽象和管理。Hypervisor 负责创建、管理和监控虚拟机，为每个虚拟机分配独立的硬件资源，并在虚拟机之间进行资源调度和隔离。当虚拟机需要访问硬件资源时，Hypervisor 会将其请求转换为对物理硬件的实际操作，实现虚拟机与物理硬件的交互。

二、当前计算机网络安全现状

当今时代下，对计算机网络安全采取防范措施十分必要。所谓计算机网络安全与规范，主要指管理和保障信息的完整性、保密性与可用性。计算机网络安全可以分为两个具体层面，即物理安全与逻辑安全。前者是计算机硬件设施受到保护，防止信息的丢失和破坏；后者是直接对数据的保护，保护信息具完整性、保密性与可用性。伴随现代社会不断进步与发展，海量数据安全问题受到了广泛关注，其与人类活动间的关系也愈发密切。而分析计算机网络安全现状，还是可以总结出网络瘫痪、账号密码窃取等不良现象，使得计算机网络安全矛盾不断升级，严重威胁到了社会群众的个人隐私，更威胁到了社会经济的稳定发展。可见，不论个人、企业，还是社会组织，都有必要做好计算机网络安全与规范工作，维护计算机网络安全的同时发挥其社会功能，促进社会稳定和经济繁荣发展。

（一）操作系统的安全问题

实际上，保障计算机网络安全的前提是计算机设备具有安全操作系统，但随着大数据技术普及和推广，更多的计算机网络安全操作系统已经发展至网络操作。那么，就容易出现各种各样的安全漏洞，具体包含 RDP 漏洞、VM 漏洞、UPNP 漏洞等。如果这些漏洞被攻击者利用，就很可能突破计算机操作系统的安全防线，进而对网络用户造成威胁。

（二）计算机病毒感染风险

计算机病毒指的是一类编制程序，而计算机运行过程中这一程序能够自动拷贝或有修改地进入到其他程序中，进而造成计算机故障乃至瘫痪。计算机病毒传播途径多样、感染风险程度不同，常见的就有收发邮件、插入不安全移动硬盘或 u 盘等。目前，广为传播的活性病毒有一万四千多种，大数据时代背景下这一数字还在不断增长，已经成为了威胁计算机网络安全的重要因素之一。

三、虚拟机技术在计算机网络安全中的应用

（一）隔离网络环境

虚拟机技术的一大核心优势就是有效隔离，在计算机网络安全中发挥积极作用。传统网络架构中，不同网络应用服务往往设置在同一服务器下统一管理，如果一个系统出现问题，其他系统就可能受到波及，进而可能导致整个系统瘫痪。这显然是不够乐

观的，如遭遇恶意攻击还可能造成漏洞在不同系统发挥作用，最终扩大损失和风险。基于虚拟机技术的应用，覆盖整个恶意攻击威胁范围，在一台物理计算机上就可以独立出多个虚拟机，假使其中一个遭到攻击，其他也能够独立运行而避免安全风险。以企业网络为例，企业通常需要对外提供多种服务，同时还拥有内部办公网络。如果将这些对外服务的服务器和内部办公网络部署在同一网络环境中，一旦外部服务器遭受攻击，内部网络也将面临巨大风险。而利用虚拟机技术，完全可以将 Web 服务器、邮件服务器等部署在独立的虚拟机中，与内部办公网络隔离开来。以虚拟机技术支持，配置独立的网络地址和安全策略，与内部网络之间通过防火墙等安全设备进行通信。即使外部服务器遭受攻击，由于其与内部网络的隔离，攻击者也很难直接入侵到内部网络，从而保障了内部网络的安全。这也方便了不同部门之间的独立工作，如果有安全需求还可以设置网络访问权限，也是相对的独立系统，避免了潜在的安全风险。

（二）建立蜜罐系统

顾名思义，蜜罐是一种诱捕攻击者的安全技术，在当前信息安全、计算机与网络安全维护中扮演重要角色。该系统能够在一些看似有价值但实际上是陷阱的系统中吸引攻击者注意力，使其认为找到了有价值的目标，而对其进行攻击。那么，安全管理员就可以获取攻击者的行为信息与手段，为后续安全防护提供依据和参考。虚拟机技术的应用无疑为蜜罐系统的部署规划提供了极大地便利。当前，虚拟机技术广泛应用，使得管理员能够在一台物理计算机上快速创建多个蜜罐虚拟机，提供相应的网络服务。例如，在虚拟机中部署一个看似正常的 Web 应用程序，还包含一些虚假的用户数据和敏感信息。进一步设置监控工具，实时监测攻击者对 Web 应用的访问行为，包括 URL 请求、表单提交等等。当攻击者入侵蜜罐时，监控工具会记录下攻击者的 IP 地址、攻击时间、攻击方式等信息。管理员可以通过分析这些信息，了解攻击者的攻击思路和手段，及时调整企业的安全防护策略。此外，管理员可以随时创建、删除或修改蜜罐虚拟机，根据实际情况调整蜜罐的配置和陷阱设置。由于蜜罐虚拟机是在物理计算机上虚拟出来的，不会对真实的业务系统造成影响，即使蜜罐被攻击者攻破，也不会导致实际的业务损失。

（三）安全补丁测试

安装安全补丁也是可行的办法，对于此类防护要做好充分前置准备工作，也就是进行兼容性和有效性测试。例如，测试一个操作系统的安全补丁，测试人员需要在虚拟机中安装补丁后，运行各种常用的应用程序，检查应用程序是否能够正常启动和运行，是否存在与补丁不兼容的情况。还可以使用性能测试工具，监测系统在安装补丁后的 CPU 使用率、内存使用率等性能指标，判断补丁是否对系统性能产生负面影响。如果在测试过程中发现补丁存在问题，测试人员可以及时调整或回滚补丁。这一操作便捷、简单，只需要将虚拟机恢复到安装补丁之前的备份状态即可。以此有效地避免在生产环境中安装有问题的补丁，确保生产环境的安全稳定。对于此类安全防护操作的模拟、演练，使得在遇到安全威胁之后，有更多支持性的处理办法和方案，对于个人和企业来说都是可操作的。今后的计算机网络安全管理中也应当推广虚拟机技术，以安全补丁测试发挥防护作用，提高计算机网络安全与信息安全水平，需要我们深层次探索与实践。

（四）恶意软件分析

虚拟机中运行恶意软件，对于运行系统进行动态监测与分析，就能够获取信息并拦截，或是做好后续处理工作，维护计算机网络安全。其主要是通过软件植入来完成的，又在后续的防护处理上做出精巧设置，使得虚拟机技术支持恶意软件传播途径与感染机制分析。例如，将恶意软件分别在 Windows XP、Windows 7、Windows 10 等不同版本的操作系统中运行，观察其在不同系统中的表现。有些恶意软件可能只针对特定版本的操作系统进行攻击，那么，我们能够发现恶意软件的攻击目标和适用范围。例如，观察恶意软件是否通过网络共享、电子邮件附件、移动存储设备等方式进行传播，以及它是如何感染其他计算机系统的。了解这些传播途径和感染机制后，企业可以采取相应的防范措施，如加强网络访问控制、对电子邮件附件进行安全扫描、对移动存储设备进行加密和杀毒等。检测恶意软件是否存在后门程序也是动态行为分析的重要内容。后门程序是恶意软件在感染计算机系统后留下的一种隐藏通道，攻击者可以通过后门程序远程控制计算机。虚拟机中运行恶意软件时，使用端口扫描工具、进程监控工具等，检测恶意软件是否在系统中打开了异常的端口，是否创建了隐藏的进程。如果发现恶意软件存在后门程序，企业可以及时采取措施，关闭后门程序，防止攻击者远程控制计算机。

结束语

总而言之，虚拟机技术是一种先进技术手段，在当今产业发展与计算机网络安全维护方面具有积极意义。合理规划并应用虚拟机技术，隔离网络环境、建立蜜罐系统、模拟漏洞环境并进行补丁测试等等，都使得潜在的网络安全威胁被发现或祛除。随着该门技术与时俱进，相信我国计算机网络安全水平能够不断提升，也在其他技术手段的支持下焕然一新。以此共同应对日益复杂、多变的网络安全威胁，也为广大群众与企业上好一堂计算机课程。

参考文献：

[1] 姜晓武 .VMware 虚拟机技术在实训教学中的应用与实践——以 Windows Server 操作系统安全配置课程为例 [J]. 中国新通信 ,2024,26(02):113-115+136.

[2] 潘晓梅 . 虚拟机技术在高职计算机网络安全教学中的作用及应用 [J]. 网络安全技术与应用 ,2024,(01):96-98.

[3] 郝彬 , 李薇 . 基于虚拟机技术的大型仪器公共平台远程数据处理系统建设 [J]. 实验室研究与探索 ,2022,41(02):278-281.

[4] 张智龙 . 虚拟机技术在高职计算机网络安全教学中的应用分析 [J]. 电脑知识与技术 ,2021,17(34):209-210+222.