

# 面向 Microsoft Virtual PC 的虚拟机 远程检测方法

韩 玲, 蔡皖东

(西北工业大学 计算机学院, 陕西 西安 710129)

**摘 要:**虚拟机技术的广泛应用给信息安全带来新的问题和挑战,由于现有的安全扫描系统检测不到虚拟机的存在,所以无法扫描虚拟机的安全漏洞。文中提出了一种面向 VPC (Microsoft Virtual PC) 的虚拟机远程检测方法,此方法根据虚拟机 MAC 地址中携带的厂商标识符,能正确地识别网络中存在的 VPC 虚拟机;并利用虚拟机与宿主机的关联性快速寻找到虚拟机的宿主机,为进一步扫描虚拟机的安全漏洞和管理虚拟机网络提供基础。实验结果表明,该方法能准确地检测网络中存在的 VPC 虚拟机。

**关键词:**虚拟机;漏洞扫描;VPC;检测

**中图分类号:**TP301

**文献标识码:**A

**文章编号:**1673-629X(2013)12-0134-05

**doi:**10.3969/j.issn.1673-629X.2013.12.032

## Remote Detection Method Oriented Microsoft Virtual PC

HAN Ling, CAI Wan-dong

(College of Computer, Northwestern Polytechnical University, Xi'an 710129, China)

**Abstract:** The wide application of virtual machine technology brings new problems and challenges to information security. Existing security scanning system can't detect the virtual machine, so can't scan security vulnerabilities. A remote detection method oriented VPC is proposed. This method uses the flag in virtual machine's MAC address to find the running virtual machine, and using the relationship between the virtual machine and the host to position the virtual machine. All this provides a basis for virtual machine scanning and management. Experiment results show that the method can find the running virtual machine effectively.

**Key words:** virtual machine; vulnerability scanning; VPC; detection

## 0 引 言

继互联网之后,虚拟化技术的出现又一次促使信息化产业产生突破性的发展。虚拟机利用虚拟化技术,为具有多操作系统需求的用户提供方便的同时,也节省了大量的资源。目前,比较流行的虚拟机产品有 Microsoft 的 Virtual PC 和 Virtual Server, Vmware 公司的 Vmware Workstation 和 Vmware Server, 以及 Citrix 公司的 XenApp 和 XenServer 等。

然而,虚拟机及其在云服务中的广泛应用,给信息安全系统引入新的安全风险。针对虚拟机的安全漏洞和攻击行为已经出现,如 VMBR<sup>[1]</sup> (Virtual-Machine Based Rootkits),它利用虚拟机使系统控制权限提升并有效地隐藏了 Rootkits 的执行痕迹,使得安全系统

难以察觉和检测。Microsoft Virtual PC (VPC) 作为微软产品的正式成员,对大部分 Windows 家族的完美兼容性是其他虚拟机所无法超越的,但由于 VPC 的广泛应用,给系统带来的安全隐患也越来越明显。也正是由于现有的漏洞扫描系统无法检测到该虚拟机的存在,所以其都不支持虚拟机的安全漏洞扫描,因此,虚拟机漏洞扫描的首要条件是检测虚拟机的存在。同时,这一研究对于局域网的管理、网络终端管理也具有促进作用。

现有的关于虚拟机的安全技术大多是虚拟环境的检测技术,即检测软件的当前运行环境是否是虚拟机环境,如文献[2]中提出了利用内存差异的方法来检测当前环境是否是虚拟机环境。对远程虚拟机的检测

收稿日期:2013-03-11

修回日期:2013-06-18

网络出版时间:2013-09-29

基金项目:2013 年陕西省科学发展计划项目(2013K06-19);西北工业大学基础研究基金(JC201149);西北工业大学研究生创业种子基金(Z2013124)

作者简介:韩 玲(1988-),女,硕士研究生,研究方向为网络信息安全;蔡皖东,教授,博士生导师,研究方向为网络信息安全。

网络出版地址:<http://www.cnki.net/kcms/detail/61.1450.TP.20130929.1544.047.html>

及虚拟机与宿主机的关联性分析技术的研究还很不成熟。文献[3]中提到了通过在 ICMP、TCP 数据中的时间戳上寻找时间异常和检测 IP 包编号异常来探测目标虚拟机,但并未对其进行深入研究,并且该方法的实现建立在远程控制系统的的前提下。文献[4]中提出了一种基于监控器时间开销的虚拟机发现技术,但其并未针对微软旗下几个系列的虚拟机,且该方法受网络情况的影响较大。文献[3-4]中的方法的执行均受制于网络情况,且都需在目标主机中运行包含特殊指令的程序,这一点不符合网络扫描工具不影响检测目标性能的原则<sup>[5]</sup>。

文中针对以上问题,在研究 Virtual PC 虚拟机的基础上,提出并实现了利用虚拟机硬件指纹检测该虚拟机并分析其与宿主机的关联性的方法。该方法克服了现有虚拟机检测技术的不足,能够有效地分析出一个局域网中物理主机上是否运行有 VPC 虚拟机及其详细信息,为进一步扫描虚拟机的漏洞和有效的管理虚拟机提供基础。

## 1 相关概念

### 1.1 虚拟机

从实现层次来分虚拟化技术分为平台虚拟化、资源虚拟化和应用程序虚拟化。虚拟机利用平台虚拟化技术,通过在一台物理计算机上添加一种称为虚拟机监视器(Virtual Machine Monitor, VMM)的中间层软件<sup>[6-7]</sup>,模拟出若干台可以独立运行且互不干扰的多个虚拟计算机,这些计算机可以安装相同或不同的操作系统。每一台虚拟计算机都与真实的计算机相似,拥有自己独立的 CPU、内存和硬盘等硬件设备<sup>[8]</sup>,甚至包括自己的 BIOS。

VMM 用于提供虚拟机的抽象。它与虚拟机和硬件进行通信,允许单一物理主机上模拟多个虚拟机,并提供虚拟机之间的隔离。通常,运行虚拟机的真实主机称为宿主机。虚拟机中运行的操作系统被称为客户机操作系统(Guest OS),运行虚拟机监控器的操作系统则被称为宿主机操作系统(Host OS)。当然某些虚拟机监控器也可以脱离宿主机操作系统直接运行在硬件上。

### 1.2 VPC 工作原理

VPC 安装过程简单、使用操作易学,更重要的是其与 Windows 操作系统有着良好的兼容性,对于 Windows 用户来说是一款首选的虚拟机产品,它采用 NDIS(Network Driver Interface Specification,即网络驱动接口规范)为每个虚拟机自动模拟一个虚拟网络适配器,该适配器同时生成一个默认的 MAC 地址,并在宿主机系统中添加多个服务或驱动—VMNS(Virtual Machine

Network Services),这个服务负责在虚拟网卡和物理网卡之间传递数据。凭借 VMNS,宿主机物理网卡不仅会接收投递到其真实网卡地址的数据包,同样会接收投递到虚拟网卡地址的数据包,然后再依据各个网卡地址分别投送给相应 MAC 的网卡上。虚拟机发送出的数据以同样的方式传送。

VPC 虚拟机为用户提供了四种组网方式:无网络连接方式;仅本地方式;共享网络方式;主机物理网卡,即桥接方式。无网络连接方式无法与外界交互,仅本地方式和共享网络方式下虚拟机可以访问外部网络,却不允许宿主机及外部网络访问虚拟机上的资源,而文中需要采用主动探测的方式从外部与虚拟机交互,所以这三种网络连接方式均不适合。

### 1.3 桥接(Bridged)

主机物理网卡方式,即桥接方式组网<sup>[9]</sup>,虚拟机直接通过宿主机物理网卡连接到所在的物理网络。虚拟机以真实主机身份出现,相当于一台连接到物理网络的物理主机,允许外部网络访问虚拟机组建的任何服务器和端口。虚拟机 IP 地址直接由路由器分配,且直接和路由器进行通讯,只是借用了物理主机的网卡。此时,虚拟机虚拟出一个网卡并桥接到宿主机网卡,发送到物理网卡的所有数据包就到了虚拟机,反之亦然。在此,宿主机物理网卡相当于一个虚拟的网络交换机,与物理网络组成本地网络,而发给 VPC 的所有数据都必须经过该虚拟交换机,并原封不动地转交给虚拟机。

桥接方式联网,虚拟机相当于一台真实计算机,适用于物理计算机的收发包方式同样适合于该虚拟机。所以,该系统中所发现的虚拟机对象必须是使用该种方式联网的,也就是说,使用其他方式联网的虚拟机,由于未对外部网络开放,不可能通过远程主动探测收集到它的任何身份信息。

### 1.4 MAC 地址解析

MAC(Medium Access Control)地址<sup>[10]</sup>,也称为物理地址,用来定义网络设备的物理位置。在 OSI 模型中,第二层数据链路层负责一种数据包叫 MAC 数据帧,这个数据帧的头部携带有主机的 MAC 地址。

MAC 地址长 48 比特位,在计算机中由 48 位二进制数表示。其中,前 24 位是厂商向 IETF(Internet 工程任务组)等机构申请的代表网络厂商的标识符,后 24 位表示序号,由厂商自行分配且是其制造的所有网卡的一个唯一编号。每个网络厂商会有自己的不同于其他厂商的标识符,而生产出的物理网卡按序号排序,所以,每块网卡都会有一个全球唯一的固定的 MAC 地址。一般采用 12 位十六进制表示一个完整的 MAC 地址,每两个十六进制之间用冒号隔开。比如一个完整的 MAC 地址 00:0e:4c:01:00:85。

无论是局域网还是广域网,数据包在通信节点之间的移动都是由 ARP<sup>[11]</sup> (Address Resolution Protocol, 地址解析协议) 将 IP 地址映射到 MAC 地址上来完成的,数据包在移动过程中会不断询问邻接节点的 MAC 地址,收到的节点填充上自己的物理地址作为应答包返回给发送端,分析应答包,就可以提取出目标的物理地址。ARP 数据包格式如图 1 所示。

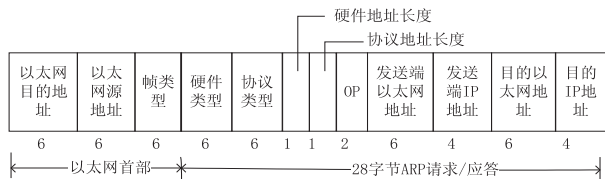


图 1 ARP 数据包格式

在 ARP 应答包中,数据包的 6~12 位以太网源地址即为目标主机的 MAC 地址,只要提取出目标返回的应答数据包的 6~12 位即可得到目标的 MAC 地址。

在开始介绍方法之前,先简单说明一下该方法中涉及到的名词。虚拟硬件指纹,指在建立虚拟机时虚拟出的真实主机中的各种设备,如硬件控制器、网卡、显卡等<sup>[12]</sup>,而这些设备的名称由虚拟机软件指定,它们就像人的指纹一样,相对比较稳定。

## 2 VPC 虚拟机检测方法

文中提出面向 VPC 远程检测方法主要分为 4 步:

(1) 利用地址解析协议和 NetBIOS(网络基础输入输出系统)协议获得目标主机 MAC 地址;

(2) 分析 MAC 地址,提取标识符,匹配 VPC 网卡硬件指纹识别虚拟机;

(3) 如果是虚拟机,分析虚拟机与宿主机的关联性;

(4) 建立数据库,将提取到的虚拟机及关联宿主主机信息存入数据库,并生成结果报告。

### 2.1 获取 MAC

获得 MAC 算法思想:向目标主机的某个开放端口发送 ARP 请求包来获得对方的 MAC 地址,然后将 IP 和得到的网卡 MAC 地址输入到 MAC 数据库中进行存储。由于 ARP 有不能跨网段的局限性,又追加了利用 NetBIOS 协议向目标主机的 137 端口发送“UDP-NetBIOS-NS”询问包询问对方的 NetBIOS Name 信息来获得跨网段主机 MAC 地址的方法。如图 2 所示,具体算法如下:

算法名称:MAC 地址获取算法。

算法输入:目标主机 IP 地址队列 IPList;

算法输出:目标主机 MAC 地址。

算法步骤:

(1) 如果 IPList 队列非空,取出一个目标 IP;如果

为空,算法结束,MAC 地址获得完成;

(2) 扫描目标主机端口,如果找到打开端口 X,进入步骤 3,否则返回步骤 1;

(3) 找到打开端口 X,向目标 IP 的端口 X 发送构造的 ARP 请求包;否则返回步骤 1;

(4) ARP 到达目标主机后,目标填写自己的 MAC 地址,将应答包返回给发送端。如果等待应答失败,进入步骤 6;否则进入步骤 5;

(5) 从网卡中解析出应答包,提取应答包的 6~12 位,进入步骤 7;

(6) 向目标 IP 的 137 端口发送“UDP-NetBIOS-NS”询问包,如果成功,提取 MAC 地址(MAC 地址起始位为应答包的第  $(56 + \text{Name 个数} \times 18)$  位,长度为 6 字节),否则返回步骤 1;

(7) 将取得的 MAC 地址与 IP 地址组成 IP-MAC 信息对存入 MAC 数据库,返回步骤 1。

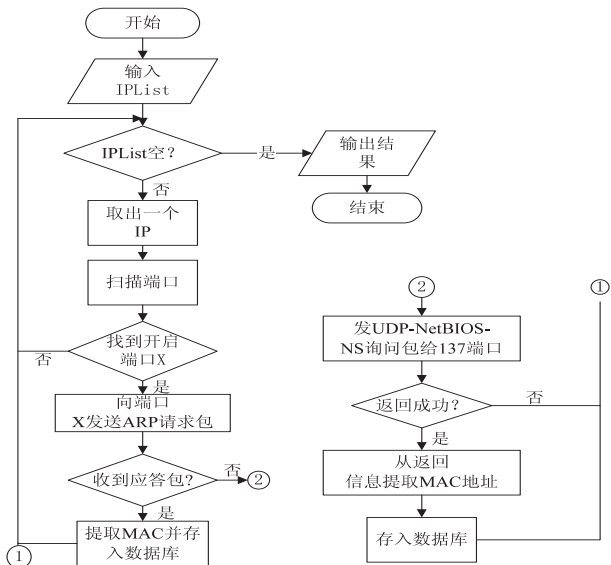


图 2 MAC 地址获取算法流程图

### 2.2 识别 VPC 虚拟机

经过大量的实验表明,微软的 VPC 虚拟机软件在安装时会自动创建一个默认的虚拟网卡,该虚拟网卡的 MAC 地址都是以 00-03-FF 开头,且固定不变。VPC 为其虚拟机分配的 MAC 地址前 24 比特位厂商标识符即可暴露其的身份信息,比如安装有 Windows XP 操作系统的 VPC 2007 虚拟机,其 MAC 地址为 00:03:ff:5e:a3:f9,前 6 位 00:03:ff(二进制的前 24 比特位)即为 VPC 的厂商标识符。所以,只要能准确地得到目标主机的 MAC 地址,提取出它的厂商标识符(MAC 地址前 6 位)并与虚拟机的 MAC 地址硬件指纹即 6 位微软 VPC 虚拟机厂商标识符“00:03:ff”匹配,即可判断出它是否是微软虚拟机 VPC。

上一步中,MAC 地址数据库已经建立完毕,将 MAC 数据库中每条数据的 MAC 地址前 6 位提出



(MAC 地址存入的是十六进制,如果是二进制则为前 24 位),与指纹库进行虚拟硬件指纹匹配(匹配网卡地址前 24 比特位厂商标识符),如果匹配成功说明是 VPC 虚拟机,将其存入虚拟机数据库。否则,说明是非 VPC 虚拟机,将主机信息存入到物理主机库。

算法中使用虚拟指纹库的目的是为了以后的扩展方便,当需要新加入一种虚拟机的检测功能时,只需将该虚拟机的指纹加入指纹库即可。

### 2.3 VPC 虚拟机与宿主机关联性分析

通过以上两步,已经可以成功检测到网络中开启的所有 VPC 虚拟机。但是,这些虚拟机可能以两种情况存在:

(1)检测到的所有虚拟机都是由同一台宿主机开启的,它们同归于一台物理主机管理。

(2)检测到的虚拟机是由多台宿主机开启的,它们归于不同的物理主机管理。

成功地定位一个已被检测到的虚拟机在网络中的准确位置,即找到它的宿主机,判断其所在宿主机是否同时运行其他虚拟机,这些信息对于有效地管理该网络有重要的意义。

由于 VPC 的虚拟网卡非真实的网卡产品,其 MAC 地址后 24 比特序号无法按出厂序号排列。通过大量数据分析发现 VPC 虚拟机软件在自动生成虚拟 MAC 地址时,前 24 比特取自厂商标识符,后 16 比特则取自虚拟机所在宿主机物理网卡的后 16 比特,其他 25 ~ 32 比特按序生成。比如,实验中所用到的一台 MAC 地址为 48:5b:39:cb:6c:d 的物理主机,其上运行了三台微软虚拟机,如表 1 所示。

表 1 一个真实的虚拟机环境

	操作系统	网卡地址
宿主机	WIN XP	48:5b:39:cb:6c:d1
虚拟机 1	WIN XP	00:03:ff:ca:6c:d1
虚拟机 2	Ubuntu 8.04.1	00:03:ff:cf:6c:d1
虚拟机 3	WIN XP	00:03:ff:c9:6c:d1

从表 1 中的实例可以观察到,同一宿主机下的 VPC 虚拟机 MAC 地址的后 16 位(十六进制后 4 位 6c:d1)是相同的,且与宿主机物理网卡的后 16 位序号相同。这些并不是巧合,通过验证,其他实验环境中的微软虚拟机网卡 MAC 地址也遵从了同样的规律。因此,通过比对目标网络主机的物理地址,可以寻找到虚拟机的宿主机物理位置。

详细算法步骤如下:

(1)如果虚拟机数据库非空,取出一条虚拟机信息;如果数据库为空,算法结束;

(2)取出该条信息中 MAC 地址后 4 位(十六进

制);

(3)将该 4 位作为标记遍历物理主机库,与每个物理主机的 MAC 地址后 4 位进行比较;

(4)如果物理主机库已经查找完,返回步骤 1;否则,如果当前信息匹配,则为虚拟机宿主机,保存虚拟机—宿主机信息对到结果数据库,返回步骤 1,若不匹配,后移一步到下条物理主机,重复步骤 4。

### 2.4 数据处理

建立结果数据库,将提取到的虚拟机及其宿主机的详细信息存入该数据库,为虚拟机的漏洞扫描和虚拟机网络管理提供基础。

结果数据库的处理,即统计每台物理主机开启的虚拟机数量及其详情,并向用户输出报告。结果数据库储存的是虚拟机—宿主机信息对,统计算法以宿主机为标记,遍历结果数据库,如果找到匹配信息对,将该条信息中的虚拟机添加到宿主机下,最后统计每台宿主机所开启的虚拟机台数。

## 3 实验结果及分析

该实验根据前面阐述的虚拟机检测方法,在 Windows XP/Microsoft Visual Studio 2008 环境下,使用 C# 语言实现了 VPC 虚拟机远程检测系统,并连入互联网进行测试。

(1)算法功能测试。

这部分将由实验结果来证明方法的有效性。实验中,使用 4 台物理主机,10 台虚拟机对该方法中的三个算法进行了串行测试。包括对 MAC 地址的正确获得、VPC 虚拟机的正确识别及对宿主机的准确查找。

在网络中经过多次测试,手动检查其准确性,结果表明文中设计的方法可以准确地识别远程 VPC 虚拟机,也能够有效地查找到该虚拟机所属的宿主机,并且准确率达到了 1。而虚拟机的虚拟网卡默认由虚拟机监控器(VMM)自动生成,不易改动,这也极大地保证了该方法的高准确率。在实验结果总结报告中,对每台物理主机所开启的虚拟机信息进行了总结。图 3 为实验结果报告图。

结果报告表明,宿主机 10.13.32.14 开启了三台 VPC 虚拟机,分别为 10.13.32.135、10.13.32.208 和 10.13.32.222。主机 10.13.32.197 和 10.13.32.213 也分别开启了 2 台和 1 台虚拟机,虚拟机类型为 VPC 虚拟机。结果中专门列出虚拟机类型这一项是为了以后将该方法扩展到其他类型虚拟机的检测中。

(2)算法开销及性能分析。

实验中,对著名系统漏洞扫描与分析软件 Nessus 进行了扫描测试,将其用于 VPC 虚拟机的扫描时,并未检测到目标是虚拟机。另外也未见到其他面向 VPC

虚拟机的安全漏洞扫描工具,所以无法做相应的对比实验。

结果报告

```
宿主机IP: 10.13.32.14  MAC: 48:5b:39:cb:6c:d1
开启虚拟机3台:
[1]IP: 10.13.32.135  MAC: 00:03:ff:cf:6c:d1
虚拟机类型: Virtual PC
[2]IP: 10.13.32.208  MAC: 00:03:ff:c9:6c:d1
虚拟机类型: Virtual PC
[3]IP: 10.13.32.222  MAC: 00:03:ff:ca:6c:d1
虚拟机类型: Virtual PC

宿主机IP: 10.13.32.197  MAC: 00:1d:72:5f:a3:f9
开启虚拟机2台:
[1]IP: 10.13.32.23  MAC: 00:03:ff:cb:a3:f9
虚拟机类型: Virtual PC
[2]IP: 10.13.32.186  MAC: 00:03:ff:cf:a3:f9
虚拟机类型: Virtual PC

宿主机IP: 10.13.32.213  MAC: 00:01:6c:54:90:d8
开启虚拟机1台:
[1]IP: 10.13.32.25  MAC: 00:03:ff:cb:90:d8
虚拟机类型: Virtual PC
```

图 3 实验结果报告图

但是,文中提出的检测方法所用算法简单,检测速率高,实验中对 100 个目标主机的检测只用了约 4 分钟时间。而且,文中实现的虚拟机与宿主机关联性分析及虚拟环境拓扑总结功能是前所未有的。

4 结束语

由于虚拟机是云计算的核心技术,其安全漏洞的扫描必将成为接下来的研究热点,因此,有效的检测远程虚拟机是做好虚拟机安全扫描的重中之重。文中提出的基于虚拟硬件指纹检测 VPC 虚拟机的方法在实验中达到了很好的效果,通过扩充虚拟机硬件指纹库还可以将该方法应用到其他的虚拟机产品中,从而提高该方法的适用度。

下一步的工作,将把该检测方法集成到一个自主

研发的远程漏洞扫描系统,使该系统可以有效地支持面向虚拟机的安全扫描。

参考文献:

[1] King S T,Chen P M,Virt S. Implementing malware with virtual machines[C]//Proceedings of the 2006 IEEE symposium on security and privacy. Washington,DC,USA;IEEE Computer Society,2006:314-327.

[2] 王宝林,杨 明,张永辉. 虚拟机检测技术研究[J]. 计算机安全,2009(12):1-3.

[3] 程微微,张 琦,谢亿鑫. 虚拟机检测与反检测技术研究[J]. 网络安全技术与应用,2011(2):28-32.

[4] 余 冲,王振兴,郭浩然,等. 基于监控器时间开销的虚拟机发现方法[J]. 计算机工程,2009,35(22):47-49.

[5] 丁 顺,李明禄,翁楚良,等. 一种基于虚拟机的安全监测方法[J]. 计算机应用与软件,2012,29(6):51-56.

[6] 董耀祖,周郑伟. 基于 X86 架构的系统虚拟机技术与应用[J]. 计算机工程,2006,32(13):71-73.

[7] Popek G J. Survey of virtual machine research[J]. Computer, 1974,7(6):34-45.

[8] 尹湘舟,赵国光,谢深泉. 虚拟机中的通信机制的安全问题研究[J]. 信息安全,2010,26(4-3):97-99.

[9] 谷 丰. 虚拟机组网技术在网络实验教学中的应用[J]. 中国科技信息,2011(13):133-133.

[10] 蔡晓东. 计算机网络[M]. 西安:西安电子科技大学出版社,2007.

[11] 何 欣,王晓凤. ARP 协议及其安全隐患[J]. 河南大学学报(自然科学版),2004,34(2):90-92.

[12] Liston T,Skoudis E. On the cutting edge:Thwarting virtual machine detection[EB/OL]. 2006-07-15. [http://handlers.sans.org/tliston/ThwartingVMDetection\\_Liston\\_Skoudis.pdf](http://handlers.sans.org/tliston/ThwartingVMDetection_Liston_Skoudis.pdf).

+++++ (上接第 127 页)

中理工大学学报,1999,27(7):92-94.

[7] 刘剑锋,牟丽君,万 宇. 基于逼近理想解排序法的导弹保障性评价研究[J]. 现代防御技术,2012,40(4):167-170.

[8] 罗明灿,李晓宝,马焕成. 逼近于理想解的排序方法及其在林业经营决策中的应用[J]. 新疆农业大学学报,1996,19(2):71-74.

[9] 胡劲松,陈怡宁. 多目标问题的逼近于理想解的排序方法研究[J]. 青岛大学学报(自然科学版),2000,13(1):72-76.

[10] Behzadian M,Otaghsara S K,Yazdani M,et al. TA state-of the-art survey of TOPSIS applications[J]. Expert Systems with applications,2012,39(17):13051-13069.

[11] Rouhani S,Ghazanfari M,Jafari M. Evaluation model of business intelligence for enterprise systems using fuzzy TOPSIS[J]. Expert systems with applications,2012,39(3):3764-3771.

[12] 百度文库. 理想解及其应用[EB/OL]. 2013-01-21. <http://wenku.baidu.com/view/7de628b069dc5022aaea0019.html>.

[13] Can Han,Lu Ma,Gan Luying. The research on application of information technology in sports stadiums[J]. Physics procedia,2011,22(1):604-609.

[14] 人人小站. 对逼近理想解排序法(TOPSIS)的理解[EB/OL]. 2013-01-21. <http://zhan.renren.com/wuweizc?gid=3602888498029569820&from=post&checked=true>.

[15] Vahdani B,Mousavi S M,Tavakkoli-Moghaddam R. Group decision making based on novel fuzzy modified TOPSIS method[J]. Applied mathematical modeling,2011,35(9):4257-4269.

# 面向Microsoft Virtual PC的虚拟机远程检测方法

作者：[韩玲](#)，[蔡皖东](#)，[HAN Ling](#)，[CAI Wan-dong](#)  
作者单位：[西北工业大学 计算机学院, 陕西 西安, 710129](#)  
刊名：[计算机技术与发展](#)

ISTIC

英文刊名：[Computer Technology and Development](#)

年，卷(期)：2013(12)

本文链接：[http://d.wanfangdata.com.cn/Periodical\\_wjfz201312032.aspx](http://d.wanfangdata.com.cn/Periodical_wjfz201312032.aspx)