(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109101818 A
(43)申请公布日 2018.12.28

(21)申请号 201810919259.4

(22)申请日 2018.08.14

(71)申请人 齐鲁工业大学
地址 250353 山东省济南市长清区大学路3501号

(72)发明人 亓蓓 王国栋

(74)专利代理机构 西安铭泽知识产权代理事务所(普通合伙) 61223
代理人 李振瑞

(51)Int.Cl.
G06F 21/56(2013.01)
G06F 21/57(2013.01)

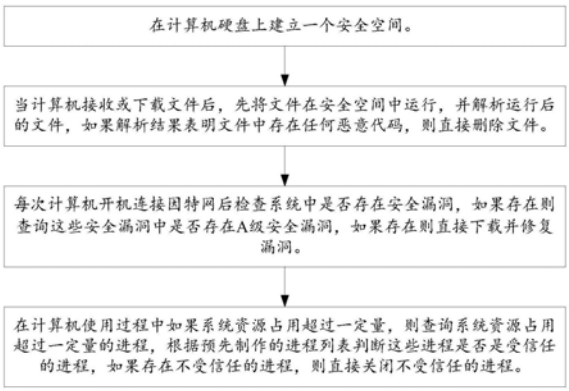
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种计算机网络安全检测方法

(57)摘要

本发明公开了一种计算机网络安全检测方法,涉及计算机网络技术领域,首先在计算机硬盘上建立一个安全空间,在计算机下载或接收文件后先在这个安全空间中运行,如果文件中存在恶意代码则直接将文件删除,在计算机使用中还查询是否存在安全漏洞,如果存在威胁程度很大的A级安全漏洞则直接下载并修复,同时还实时监测系统资源的占用量,当占用量超过一定值时判断占用量高的进程是否为受信任的,如果不受信任则直接结束进程。本发明的方法从计算机本身出发对接入的网络进行分析,在安全漏洞、下载安全和资源占用等多个方面进行检测管理,对计算机进行实时检测和保护。



CN 109101818 A

1.一种计算机网络安全检测方法,其特征在于,该方法包括以下步骤:

步骤1,在计算机硬盘上建立一个安全空间;

步骤2,当计算机接收或下载文件后,先将文件在安全空间中运行,并解析运行后的文件,如果解析结果表明文件中存在恶意代码,则直接删除文件;

步骤3,每次计算机开机连接因特网后,检查系统中是否存在安全漏洞,如果存在则查询这些安全漏洞中是否存在A级安全漏洞,如果存在则直接下载并修复漏洞;

步骤4,在计算机使用过程中实时监测系统资源的使用情况,如果系统资源占用超过一定量,则查询系统资源占用超过一定量的进程,根据进程列表判断这些进程是否是受信任的进程,如果这些进程中存在不受信任的进程,则直接关闭不受信任的进程。

2.如权利要求1所述的计算机网络安全检测方法,其特征在于,步骤1中在建立所述安全空间后在显示屏上弹出通知对话框。

3.如权利要求1所述的计算机网络安全检测方法,其特征在于,步骤1中如果计算机上安装有两个或以上的独立硬盘,则在建立安全空间时询问使用者,随后在选择的硬盘中建立安全空间。

4.如权利要求1所述的计算机网络安全检测方法,其特征在于,步骤2中文件删除后在显示屏上弹出提示对话框,提醒使用者文件被删除。

5.如权利要求1所述的计算机网络安全检测方法,其特征在于,步骤3中如果不存在A级安全漏洞则提醒使用者存在安全漏洞,使用者选择修复后开始下载并修复这些安全漏洞。

6.如权利要求1所述的计算机网络安全检测方法,其特征在于,步骤4中如果系统资源占用超过一定量的进程都是受信任的进程,则忽略本次系统资源占用超过一定量的事件。

一种计算机网络安全检测方法

技术领域

[0001] 本发明涉及计算机网络技术领域，特别是涉及一种计算机网络安全检测方法。

背景技术

[0002] 随着Internet在全球的普及和发展，越来越多的计算机用户可以通过网络足不出户地享受丰富的信息资源，方便快捷地收发信息。计算机网络已经和人们的学习、工作紧密的联系在一起，成为许多人生活中不可获取的重要部分。但是，在人们享受网络带来的巨大便利时，计算机网络的安全性也日益受到关注。一方面随着网络结构的日趋复杂和应用的多元化，使得系统存在漏洞的可能性大大增加；另一方面黑客攻击手段日新月异，加之内部工作人员有意或者无意的非法越权操作，对于网络的正常运行构成了极大的威胁。

[0003] 目前很多网络安全检测方法主要是集中在对网络本身的分析，这种分析适用于大量计算机处在同一网络中的情况，这种方法可以很大程度上节省成本且效果较好。而对于单个计算机的分析较少，计算机本身的情况对网络安全的影响也是举足轻重的，因此有必要提供一种从计算机本身出发对网络安全进行检测并保证使用安全的方法。

发明内容

[0004] 本发明实施例提供了一种计算机网络安全检测方法，可以解决现有技术中存在的问题。

[0005] 本发明提供了一种计算机网络安全检测方法，该方法包括以下步骤：

[0006] 步骤1，在计算机硬盘上建立一个安全空间；

[0007] 步骤2，当计算机接收或下载文件后，先将文件在安全空间中运行，并解析运行后的文件，如果解析结果表明文件中存在恶意代码，则直接删除文件；

[0008] 步骤3，每次计算机开机连接因特网后，检查系统中是否存在安全漏洞，如果存在则查询这些安全漏洞中是否存在A级安全漏洞，如果存在则直接下载并修复漏洞；

[0009] 步骤4，在计算机使用过程中实时监测系统资源的使用情况，如果系统资源占用超过一定量，则查询系统资源占用超过一定量的进程，根据进程列表判断这些进程是否是受信任的进程，如果这些进程中存在不受信任的进程，则直接关闭不受信任的进程。

[0010] 优选地，步骤1中在建立所述安全空间后在显示屏上弹出通知对话框。

[0011] 优选地，步骤1中如果计算机上安装有两个或以上的独立硬盘，则在建立安全空间时询问使用者，随后在选择的硬盘中建立安全空间。

[0012] 优选地，步骤2中文件删除后在显示屏上弹出提示对话框，提醒使用者文件被删除。

[0013] 优选地，步骤3中如果不存在A级安全漏洞则提醒使用者存在安全漏洞，使用者选择修复后开始下载并修复这些安全漏洞。

[0014] 优选地，步骤4中如果系统资源占用超过一定量的进程都是受信任的进程，则忽略本次系统资源占用超过一定量的事件。

[0015] 本发明实施例中的一种计算机网络安全检测方法，首先在计算机硬盘上建立一个安全空间，在计算机下载或接收文件后先在这个安全空间中运行，如果文件中存在恶意代码则直接将文件删除，在计算机使用中还查询是否存在安全漏洞，如果存在威胁程度很大的A级安全漏洞则直接下载并修复，同时还实时监测系统资源的占用量，当占用量超过一定值时判断占用量高的进程是否为受信任的，如果不受信任则直接结束进程。本发明的方法从计算机本身出发对接入的网络进行分析，在安全漏洞、下载安全和资源占用等多个方面进行检测管理，对计算机进行实时检测和保护，适用于家庭计算机使用。

附图说明

[0016] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0017] 图1是本发明实施例中一种计算机网络安全检测方法的流程图。

具体实施方式

[0018] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0019] 参照图1，本发明实施例提供了一种计算机网络安全检测方法，该方法包括以下步骤：

[0020] 步骤1，在计算机硬盘上建立一个安全空间，该安全空间对使用者不可见，且不能被使用者删除或修改。该安全空间的大小一般在10G以内为宜，避免占用计算机硬盘的过大空间，对日常使用造成影响。当然，为了避免使用者在不知情的情况下误认为计算机出现故障，在建立所述安全空间后需要在显示屏上弹出通知对话框，以使使用者了解。

[0021] 在本实施例中，由于计算机硬盘一般都会分区，而计算机操作系统都安装在C盘中，则安全空间也以建立在C盘上为宜。如果计算机上安装有两个或以上的独立硬盘，则在建立安全空间时可以询问使用者，使用者选择后即在选择的硬盘中建立安全空间。

[0022] 步骤2，当计算机接收或下载文件后，先将文件在安全空间中运行，并解析运行后的文件，如果解析结果表明文件中存在任何恶意代码，则直接删除文件，并在文件删除后在显示屏上弹出提示对话框，提醒文件被删除。

[0023] 步骤3，每次计算机开机连接因特网后，检查系统中是否存在安全漏洞，如果存在则查询这些安全漏洞中是否存在A级安全漏洞，如果存在则直接下载并修复漏洞，并在修复完成后提醒使用者；如果不存在A级安全漏洞则提醒使用者存在安全漏洞，使用者选择修复后开始下载并修复这些安全漏洞。

[0024] 漏洞按其对目标主机的危险程度一般分为三级：

[0025] (1)A级漏洞

[0026] 它是允许恶意入侵者访问并可能会破坏整个目标系统的漏洞，如，允许远程用户

未经授权访问的漏洞。A级漏洞是威胁最大的一种漏洞，大多数A级漏洞是由于较差的系统管理或配置有误造成的。同时，几乎可以在不同的地方，在任意类型的远程访问软件中都可以找到这样的漏洞。如:FTP，GOPHER，TELNET，SENDMAIL，FINGER等一些网络程序常存在一些严重的A级漏洞。

[0027] (2)B级漏洞

[0028] 它是允许本地用户提高访问权限，并可能允许其获得系统控制的漏洞。例如，允许本地用户(本地用户是在目标机器或网络上拥有账号的所有用户，并无地理位置上的含义)非法访问的漏洞。网络上大多数B级漏洞是由应用程序中的一些缺陷或代码错误引起的。

[0029] SENDMAIL和TELNET都是典型的例子。因编程缺陷或程序设计语言的问题造成的缓冲区溢出问题是一个典型的B级安全漏洞。据统计，利用缓冲区溢出进行攻击占所有系统攻击的80％以上。

[0030] (3)C级漏洞

[0031] 它是任何允许用户中断、降低或阻碍系统操作的漏洞。如，拒绝服务漏洞。拒绝服务攻击没有对目标主机进行破坏的危险，攻击只是为了达到某种目的，对目标主机进行故意捣乱。最典型的一种拒绝服务攻击是SYN-Flooder，即入侵者将大量的连接请求发往目标服务器，目标主机不得不处理这些“半开”的SYN，然而并不能得到ACK回答，很快服务器将用完所有的内存而挂起，任何用户都不能再从服务器上获得服务。

[0032] 步骤4，在计算机使用过程中实时监测系统资源的使用情况，如果系统资源占用超过一定量，例如超过90％，则查询系统资源占用超过一定量的进程，根据预先制作的进程列表判断这些进程是否是受信任的进程，如果是则忽略本次事件；如果这些进程中存在不受信任的进程，则直接关闭不受信任的进程，避免这些不受信任的进程影响计算机正常使用。

[0033] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0034] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

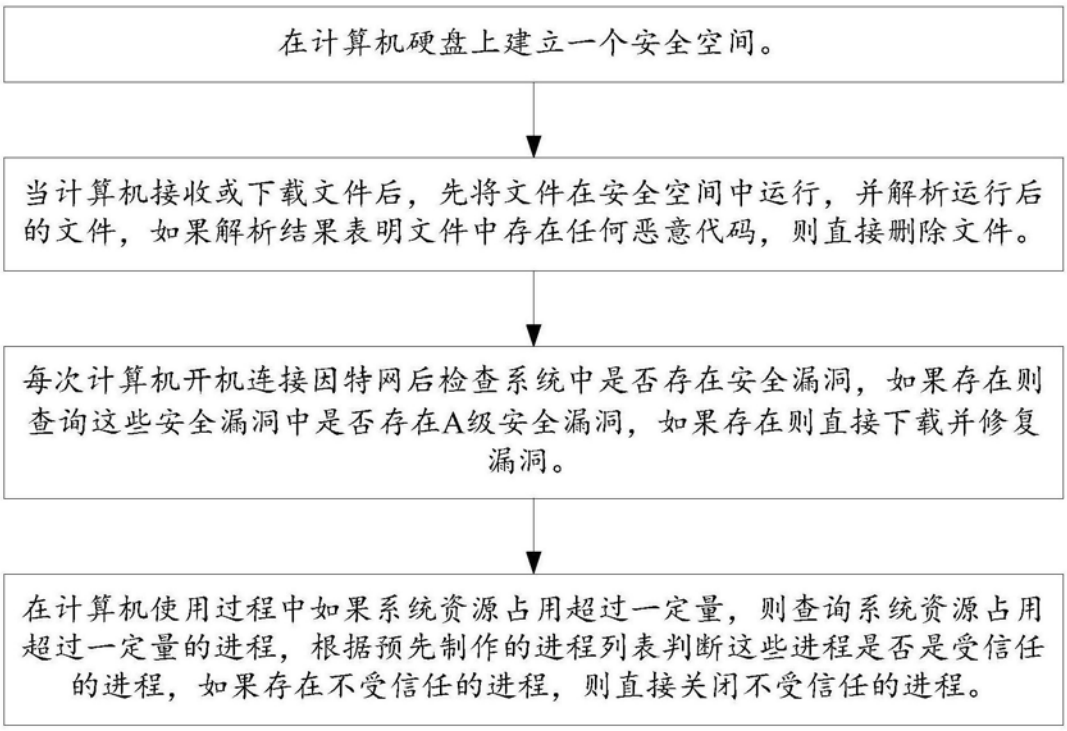

在计算机硬盘上建立一个安全空间。
当计算机接收或下载文件后，先将文件在安全空间中运行，并解析运行后的文件，如果解析结果表明文件中存在任何恶意代码，则直接删除文件。
每次计算机开机连接因特网后检查系统中是否存在安全漏洞，如果存在则查询这些安全漏洞中是否存在A级安全漏洞，如果存在则直接下载并修复漏洞。
在计算机使用过程中如果系统资源占用超过一定量，则查询系统资源占用超过一定量的进程，根据预先制作的进程列表判断这些进程是否是受信任的进程，如果存在不受信任的进程，则直接关闭不受信任的进程。

图1