(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 106295356 A
(43)申请公布日 2017.01.04

(21)申请号 201610712193.2

(22)申请日 2016.08.24

(71)申请人 浪潮电子信息产业股份有限公司
地址 250101 山东省济南市高新区浪潮路1036号

(72)发明人 赵慧

(74)专利代理机构 济南信达专利事务所有限公司 37100
代理人 孟峣

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

权利要求书1页 说明书3页

(54)发明名称

一种基于SSR产品的主机安全级别统计方法

(57)摘要

本发明公开了一种基于SSR产品的主机安全级别统计方法，其实现过程为：首先设置安全系统，该安全系统包括主动防御模块、安全配置模块、完整性检测模块和资源告警模块；根据各个模块对主机安全的影响程度，对各模块设置一个加权系统；将上述各个模块加权后进行相加，得到的和即为安全评分，且该评分根据分值大小分为优良中差四种。该一种基于SSR产品的主机安全级别统计方法与现有技术相比，通过将安全级别最终展示为优、良、中、差四个级别，直观明确；安全级别计算方法以违规日志量作为基础数据，计算出来的结果能真实反应主机安全状态；安全级别计算方法考虑了不同的模块的违规对主机安全的影响不同，计算出来的结果比较客观，实用性强。

CN 106295356 A

1.一种基于SSR产品的主机安全级别统计方法，其特征在于，其实现过程为：

首先设置安全系统，该安全系统包括主动防御模块、安全配置模块、完整性检测模块和资源告警模块，其中主动防御模块用于对主机的主动防御日志进行统计，得到主动防御分数；安全配置模块用于完成安全配置的打分计算得到安全配置分数；完整性检测模块用于对完整性检测评分计算得到完整性检测分数；资源告警模块对主机的资源主动防御日志进行统计得到资源告警分数；

根据各个模块对主机安全的影响程度，对各模块设置一个加权系统；

将上述各个模块加权后进行相加，得到的和即为安全评分，且该评分根据分值大小分为优良中差四种。

2.根据权利要求1所述的一种基于SSR产品的主机安全级别统计方法，其特征在于，主动防御模块在加权前进行统计并计分，其过程为：每小时对主机的主动防御违规日志进行统计，以100分为基准，每条日志减去1分，直到0分，得到的分数即为主动防御分数，所述主机的主动防御违规日志是指通过设置对主机包括文件、进程、注册表的内容进行保护，如果出现违反规则的操作，就会记录一条主动防御违规日志。

3.根据权利要求1所述的一种基于SSR产品的主机安全级别统计方法，其特征在于，安全配置模块在加权前进行统计并计分，其过程为：根据安全配置最近一次扫描结果中基线符合项占总基线条数的比例得到安全配置评分，计算方法为符合项除以安全基线总数再乘以100，满分为100分，得到的分数为安全配置分数。

4.根据权利要求1所述的一种基于SSR产品的主机安全级别统计方法，其特征在于，完整性检测模块在加权前进行统计并计分，其过程为：根据被保护的文件/服务数量和最近一次检测结果，得到完整性检测评分，计算方法是最近一次扫描结果中文件/服务正常数除以被保护文件/服务总数再乘以100，满分为100分，得到的分数即为完整性检测分数。

5.根据权利要求1所述的一种基于SSR产品的主机安全级别统计方法，其特征在于，资源告警模块在加权前进行统计并计分，其过程为：每小时对资源的主动防御日志进行统计，这里的资源包括主机的CPU、内存和硬盘，以100分为基准，每条日志减去1分，直到0分，得到的分数即为资源告警分数。

6.根据权利要求1-5任一所述的一种基于SSR产品的主机安全级别统计方法，其特征在于，主机的安全评分为主动防御分数、安全配置分数、完整性检测分数、资源告警分数的加权和，且主动防御分数、安全配置分数、完整性检测分数、资源告警分数的加权系数为0.5、0.3、0.15、0.05，即安全评分=主动防御分数*0.5+安全配置分数*0.3+完整性检测分数*0.15+资源告警分数*0.05。

7.根据权利要求6所述的一种基于SSR产品的主机安全级别统计方法，其特征在于，根据安全评分的分值大小得到安全级别，具体为：80分以上为优，70-80为良，60-70为中，60分以下为差。

一种基于SSR产品的主机安全级别统计方法

技术领域

[0001] 本发明涉及计算机安全技术领域，具体地说是一种实用性强、基于SSR产品的主机安全级别统计方法。

背景技术

[0002] 在现有技术中，业务升级正在逐步成为IT行业的常态，如何在这种常态下保证系统的安全稳定运行?以邮件系统为例，美国国务院电子邮件系统迫于黑客攻击的压力被关闭，这是2014年11月17日爆出的消息。与之类似，我国政府的电子邮件系统也是黑客攻击的目标。如何保证核心数据的安全?现在提出了一种SSR产品防护系统，实现了防止病毒入侵、防止黑客窃取机密信息的目标。

[0003] SSR产品的安全防护主要是主机安全，其核心内容包括安全应用交付系统、应用监管系统、操作系统安全增强系统和运维安全管控系统。它的具体功能是指保证主机在数据存储和处理的保密性、完整性，可用性，它包括硬件、固件、系统软件的自身安全，以及一系列附加的安全技术和安全管理措施，从而建立一个完整的主机安全保护环境。

[0004] 但是，如果能够根据主机的日志为基础，计算得出不同的安全级别，则能够为SSR产品的安全防护提供一定基础，这是因为每一个模块都有一些规则，一旦主机发生违法规则的安全行为就会记录一条违规日志。如果能够以主机的违规日志为基础，通过计算得到安全评分，从而得到安全级别，就能够进一步提高SSR产品的安全防护能力。基于此，现提供一种基于SSR产品的主机安全级别统计方法。

发明内容

[0005] 本发明的技术任务是针对以上不足之处，提供一种实用性强、基于SSR产品的主机安全级别统计方法。

[0006] 一种基于SSR产品的主机安全级别统计方法，其实现过程为：

首先设置安全系统，该安全系统包括主动防御模块、安全配置模块、完整性检测模块和资源告警模块，其中主动防御模块用于对主机的主动防御日志进行统计，得到主动防御分数；安全配置模块用于完成安全配置的打分计算得到安全配置分数；完整性检测模块用于对完整性检测评分计算得到完整性检测分数；资源告警模块对主机的资源主动防御日志进行统计得到资源告警分数；

根据各个模块对主机安全的影响程度，对各模块设置一个加权系统；

将上述各个模块加权后进行相加，得到的和即为安全评分，且该评分根据分值大小分为优良中差四种。

[0007] 主动防御模块在加权前进行统计并计分，其过程为：每小时对主机的主动防御违规日志进行统计，以100分为基准，每条日志减去1分，直到0分，得到的分数即为主动防御分数，所述主机的主动防御违规日志是指通过设置对主机包括文件、进程、注册表的内容进行保护，如果出现违反规则的操作，就会记录一条主动防御违规日志。

[0008] 安全配置模块在加权前进行统计并计分，其过程为：根据安全配置最近一次扫描结果中基线符合项占总基线条数的比例得到安全配置评分，计算方法为符合项除以安全基线总数再乘以100，满分为100分，得到的分数为安全配置分数。

[0009] 完整性检测模块在加权前进行统计并计分，其过程为：根据被保护的文件/服务数量和最近一次检测结果，得到完整性检测评分，计算方法是最近一次扫描结果中文件/服务正常数除以被保护文件/服务总数再乘以100，满分为100分，得到的分数即为完整性检测分数。

[0010] 资源告警模块在加权前进行统计并计分，其过程为：每小时对资源的主动防御日志进行统计，这里的资源包括主机的CPU、内存和硬盘，以100分为基准，每条日志减去1分，直到0分，得到的分数即为资源告警分数。

[0011] 主机的安全评分为主动防御分数、安全配置分数、完整性检测分数、资源告警分数的加权和，且主动防御分数、安全配置分数、完整性检测分数、资源告警分数的加权系数为0.5、0.3、0.15、0.05，即安全评分=主动防御分数*0.5+安全配置分数*0.3+完整性检测分数*0.15+资源告警分数*0.05。

[0012] 根据安全评分的分值大小得到安全级别，具体为：80分以上为优，70-80为良，60-70为中，60分以下为差。

[0013] 本发明的一种基于SSR产品的主机安全级别统计方法，具有以下优点：

本发明的一种基于SSR产品的主机安全级别统计方法，安全级别的最终展示为优、良、中、差四个级别，直观明确；安全级别计算方法以违规日志量作为基础数据，计算出来的结果能真实反应主机安全状态；安全级别计算方法考虑了不同的模块的违规对主机安全的影响不同，计算出来的结果比较客观，实用性强，适用范围广泛，易于推广。

具体实施方式

[0014] 下面结合具体实施例对本发明作进一步说明。

[0015] 本发明提出一种基于SSR产品的主机安全级别统计方法，其实现过程为：

首先设置安全系统，该安全系统包括主动防御模块、安全配置模块、完整性检测模块和资源告警模块，其中主动防御模块用于对主机的主动防御日志进行统计，得到主动防御分数；安全配置模块用于完成安全配置的打分计算得到安全配置分数；完整性检测模块用于对完整性检测评分计算得到完整性检测分数；资源告警模块对主机的资源主动防御日志进行统计得到资源告警分数；

根据各个模块对主机安全的影响程度，对各模块设置一个加权系统；

将上述各个模块加权后进行相加，得到的和即为安全评分，且该评分根据分值大小分为优良中差四种。

[0016] 主动防御模块在加权前进行统计并计分，其过程为：每小时对主机的主动防御违规日志进行统计，以100分为基准，每条日志减去1分，直到0分，得到的分数即为主动防御分数，所述主机的主动防御违规日志是指通过设置对主机包括文件、进程、注册表的内容进行保护，如果出现违反规则的操作，就会记录一条主动防御违规日志。

[0017] 安全配置模块在加权前进行统计并计分，其过程为：根据安全配置最近一次扫描结果中基线符合项占总基线条数的比例得到安全配置评分，计算方法为符合项除以安全基

线总数再乘以100，满分为100分，得到的分数为安全配置分数。

[0018] 完整性检测模块在加权前进行统计并计分，其过程为：根据被保护的文件/服务数量和最近一次检测结果，得到完整性检测评分，计算方法是最近一次扫描结果中文件/服务正常数除以被保护文件/服务总数再乘以100，满分为100分，得到的分数即为完整性检测分数。

[0019] 资源告警模块在加权前进行统计并计分，其过程为：每小时对资源的主动防御日志进行统计，这里的资源包括主机的CPU、内存和硬盘，以100分为基准，每条日志减去1分，直到0分，得到的分数即为资源告警分数。

[0020] 主机的安全评分为主动防御分数、安全配置分数、完整性检测分数、资源告警分数的加权和，且主动防御分数、安全配置分数、完整性检测分数、资源告警分数的加权系数为0.5、0.3、0.15、0.05，即安全评分=主动防御分数*0.5+安全配置分数*0.3+完整性检测分数*0.15+资源告警分数*0.05。

[0021] 根据安全评分的分值大小得到安全级别，具体为：80分以上为优，70-80为良，60-70为中，60分以下为差。

[0022] 以下举例描述主机安全级别计算方法：

主机防御模块：最近一小时内主机的主动防御违规日志数量为30条；

安全配置模块：最近一次安全配置扫描分数为78分；

完整性检测模块：最近一次扫描结果中文件服务正常数为150，被保护的文件服务总数为200；

资源告警模块：最近一小时内主机的主动防御违规日志数量为18条；

则，主机安全评分 = 70*0.5+78*0.3+(150/200)*100*0.15+82*0.05=73.75，根据“70--80为良”，得到主机安全级别为良。

[0023] 上述具体实施方式仅是本发明的具体个案，本发明的专利保护范围包括但不限于上述具体实施方式，任何符合本发明的一种基于SSR产品的主机安全级别统计方法的权利要求书的且任何所述技术领域的普通技术人员对其所做的适当变化或替换，皆应落入本发明的专利保护范围。