

基于 CIA 属性的网络安全评估方法研究

刘意先,慕德俊

(西北工业大学 自动化学院,陕西 西安 710072)

摘要:随着网络技术的发展,安全事件不断出现,如何实现整体的安全保护是一项重要的研究问题。安全评估作为一种有效的信息系统的保护手段,与传统的安全保护方法相比,能为信息系统提供全面的安全技术支持。通过分析系统中的资产漏洞对机密性、完整性以及可用性(CIA)的影响程度,采用 CVSS 方式进行相应的评分,结合指标的权重实现了对网络信息系统的评估。实验构建了简单的网络信息系统,使用扫描器对系统中的设备进行扫描发现资产的漏洞信息,从 NVD 漏洞库中获得基本的评分数据,完成了资产风险值的计算,并将相应的风险值进行了转换,实现了定性的评估结果。实验结果验证了该方法的可行性和有效性。

关键词:网络安全;安全评估;漏洞;资产

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2018)04-0141-03

doi:10.3969/j.issn.1673-629X.2018.04.029

Research on Network Security Assessment Method Based on CIA

LIU Yi-xian, MU De-jun

(School of Automation, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: With the development of network technology, security events continually emerge, so how to achieve the overall security protection is an important issue. As an effective protection method to information system, the security assessment can provide the comprehensive support of security technology for information system compared with traditional security protection methods. By analyzing the impacts on the system's asset vulnerability to its confidentiality, integrity and availability, the scores are assigned by CVSS (common vulnerability scoring system), and then the assessment of network information system is achieved with the weight of the attributes. A simple network information system is constructed in the experiment and the scanner is used in the system equipment to find the vulnerability information of assets. The basic score data is obtained from the NVD for the calculation of risk assets value which is transformed for qualitative assessment. The experiment verifies the feasibility and the effectiveness of the proposed method.

Key words: network security; security assessment; vulnerability; asset

0 引言

随着网络技术的发展,网络信息系统也成为了企业和组织日常工作中必不可少的工具和基础设施,各种应用和新业务的不断涌现,产生了巨大的经济效益。与此同时,各种网络安全事件的频发也成为了当前社会的关注焦点。2015年,国家网络应急中心共接收境内外报告的网络安全事件126 916起,较2014年增长了125.9%。其中,境内报告的网络安全事件126 424起,较2014年增长了128.6%^[1]。各种安全事件是黑客利用各种软硬件以及企业组织管理中存在的漏洞实施的攻击。每年各种安全漏洞层出不穷,到2016年底中国国家漏洞库中已有漏洞信息8万多条^[2]。通过安

装各类补丁、杀毒软件、入侵检测系统以及防火墙等,虽然能降低各类安全事件的发生概率,但无法让企业和组织整体把握安全状态和面临安全威胁时进行有目的的安全防护。因此信息安全评估技术成为了处理这类问题的重要手段^[3]。

文中主要是以信息安全保护最重要的三个属性—机密性(confidentiality)、完整性(integrity)和可用性为指标(availability),通过对网络系统的资产进行分析,完成相应的安全评估。

1 信息安全的属性

在不同信息安全的风险评估模型和方法中,对资

收稿日期:2017-03-24

修回日期:2017-07-27

网络出版时间:2017-12-04

基金项目:国家自然科学基金(61672433)

作者简介:刘意先(1980-),男,博士生,研究方向为网络安全、网络安全评估;慕德俊,博士,教授,研究方向为自动控制、信息安全。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20171204.1647.018.html>

产安全性度量以及风险计算上存在一定的差异^[4]。张弢等提出了一种基于风险矩阵的信息安全风险评估模型^[5],通过建立二维矩阵处理专家对各类指标的评分,计算出受评实体的风险要素,再利用 Borda 序值理论和层次分析法(analytical hierarchy process, AHP)得出评估对象的等级值。刘延华等提出了一种基于云模型的多层次可生存性模糊评估方法^[6],用 AHP 方法构建了多层次评估指标体系,并对各级指标权重进行了有效计算,实现了对云环境下网络可用性的评估。杨姗姗等提出了一种基于 TOPSIS 的多属性群决策方法^[7]。Khanmohammadi 等^[8]提出了从业务的目标出发,考虑业务流程的关键性、角色以及重要程度来实现综合的风险评估的方法。这些方法大多数都采用了机密性、完整性以及可用性作为其中的指标。这 3 个属性能体现用户对系统的信息安全的基本要求。机密性指敏感信息不被未授权者获取的程度;完整性指信息的各部分在受到恶意或未授权的攻击下被保护的程
度;可用性指抵抗各种企图降低信息可操作性攻击的程度^[9]。

在一般的评估方法中,对相关指标的评价大多采用专家打分的方式来完成^[10-11],分值可以用语言型的数据进行定性的表达,而在数据处理计算中,对这种以定性形式表达的数据将以具体的数量值来表达。如对 CIA 属性语言型数据,按照风险程度表达为很低、低、中、较高和高这样的五级制表达方式,对应的分值可用 1~5 进行对应的评分。

企业和组织在评估自身机构内部的资产时,会有不同的侧重点,如涉密单位对机密性的要求更高,而文教单位更看重资产的可用性,因此对 CIA 属性设置不同的权重。单个资产的漏洞风险值可由式(1)表达。

$$\text{Risk}_{\text{asset}} = W_c \cdot L_c + W_i \cdot L_i + W_a \cdot L_a \quad (1)$$

其中, $\text{Risk}_{\text{asset}}$ 为资产的风险值; W_c 、 W_i 、 W_a 分别对应机密性、完整性以及可用性的权重; L_c 、 L_i 、 L_a 分别对应资产 CIA 属性的风险等级的量化值。

2 评估的整体流程

系统的风险评估是对系统在发生安全事件后产生的损失进行度量。这个过程需要分析系统的价值或相关的生产收益,而系统的价值一般体现在系统所包含的资产的价值或是资产承载的业务所产生的价值。因此,在评估中首先要明确系统所包含的各种资产,资产可以是实体设备也可以是组织内部的人员或文件规范等。因此评估开始后要对待评估系统的构成进行分解,分解的过程要将系统划分为不可分的部件,每个部件可以看作是一个待评估的资产。资产本身的漏洞是产生风险的来源,如操作系统没有安装合适的补丁,前

端 Web 程序的输入检测不完善,设备的操作手册过程不明确等都是相应的安全漏洞。对资产的漏洞可以通过手工方式发现也可以通过工具进行扫描。一般而言漏洞所产生的风险对系统的影响是多方面的,信息安全的风险评估中常用作安全考量的属性众多,如机密性、完整性、可用性、不可抵赖性、可审计性等,选择合适的属性影响指标是评估其中的一个重要问题,经常取决于管理者对安全考虑的侧重点。对安全属性的影响程度可以采用定量或定性的方式表达。最后结合安全属性的影响程度,可以综合计算出相应的风险程度。

3 评估方法分析

首先对系统进行相应的资产分解,分解后的系统资产可以用集合 A 来表示:

$$A = \{a_1, a_2, \dots, a_n\} \quad (2)$$

其中, a_i 为系统中第 i 个资产, n 为系统中资产的数量。

构成复杂的系统会得到更大的资产集合,评估的过程也会更长,因此在资产分解时有必要考虑是否对某些资产采用合并的处理方式,这样可以加快评估的过程。

网络信息设备的漏洞通常可以通过漏洞扫描器进行发现,通过漏洞扫描器对资产进行扫描可以快速地发现漏洞并能够从许多统一的安全漏洞库中得到漏洞信息^[12]。一般单个资产的漏洞扫描可能会得到不止一个漏洞,为了方便处理,这里将选择资产上最严重的漏洞,因为最严重漏洞面临的风险造成的损失是最大的,也包含了其他漏洞所造成的损失。经过扫描器扫描后得到对应的集合 V 来表示风险集合:

$$V = \{v_1, v_2, \dots, v_n\} \quad (3)$$

其中, v_i 表示资产 a_i 对应的最严重漏洞。

接下来要进行的处理是安全属性的评分,开始评分前要选择合适的属性。如前所述, CIA 属性作为信息安全评估中最重要也是最常见的属性,能基本体现用户对系统的安全需求。因此采用 CIA 属性作为评分的指标。通常评分过程采用专家打分的方式进行处理,为了保证处理方法的通用性,采用 CVSS 系统^[13]中的评分方式。该评分方法对 CIA 属性只有三个等级的评分,但是能和大多数的扫描器和漏洞库的分析结果自动对接,形成评分结果。该评分方式的三个等级分别为无、低和高,对应的量化值为 0、1、2。

根据式(1)的计算方法,输入预先设定的权重值和 CIA 属性值,可以得到对应资产的风险值,该值是一个数值型的数据。对于大多数系统使用者,总是希望用最直观的表达方式来查看最后的评估结果,这时可以将该值进行类型转换,最终得出资产安全风险的

定性表达方式。转换过程如表 1 所示。

表 1 风险值从定量到定性的转换

风险值 R	风险等级
$0 \leq R \leq 0.5$	低
$0.5 < R \leq 1$	中等
$1 < R \leq 1.5$	较高
$1.5 < R \leq 2$	很高

4 应用实例

以上简述了根据 CIA 属性对网络信息系统的评估过程。为了验证该评估方法,文中进行的工作之一就是搭建一个待评估的应用环境。该实验网络内有 2 台计算机、1 台 FTP 服务器、1 台 Web 服务器,并通过 1 台路由器连接到外部校园网。网络拓扑结构如图 1 所示。

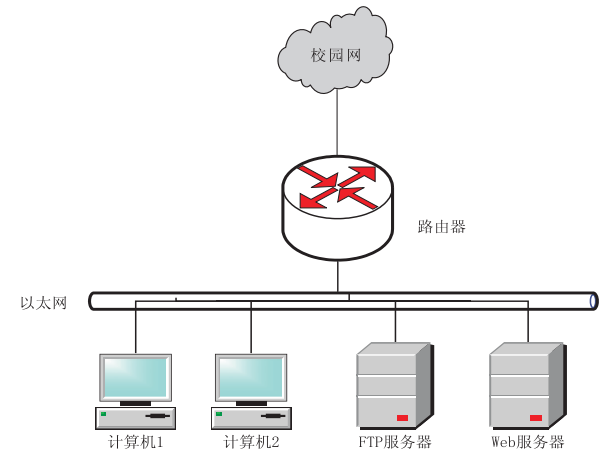


图 1 实验环境拓扑

在不考虑单个设备的软硬件组成以及操作人员的情况下,可以对该环境的组成进行相应的资产分解,得到的资产信息如表 2 所示。

表 2 资产信息

资产 ID	资产名称
1	计算机 1
2	计算机 2
3	FTP 服务器
4	Web 服务器
5	路由器

然后采用扫描工具 Nessus^[14]对资产信息进行扫描,可得到资产对应的最严重漏洞,见表 3。

表 3 资产对应的漏洞信息

资产 ID	漏洞编号
1	CVE-2014-0301
2	CVE-2012-2317
3	CVE-2000-1033
4	CVE-2006-6578
万方数据	CVE-2013-2645

资产对应的漏洞信息对应 CIA 影响的属性值可自动从漏洞库 NVD^[15]上取得,由此可得到所对应的结果,见表 4。

表 4 资产漏洞对应的 CIA 属性影响等级

资产 ID	机密性	完整性	可用性
1	高	高	高
2	无	低	无
3	低	低	低
4	低	低	低
5	高	高	高

该实例中设置的机密性、完整性和可用性的权重向量 $W = \{0.5, 0.25, 0.25\}$,并按照表 1 的量化方法进行转换,结合权重进行计算,得到最后的风险等级的计算结果,具体的数据和评估结果见表 5。风险等级列将风险进行了定性的表达。

表 5 系统的评估数据及结果

资产名称	机密性	完整性	可用性	风险值	风险等级
计算机 1	2	2	2	2	很高
计算机 2	0	1	0	0.25	低
FTP 服务器	1	1	1	1	中等
Web 服务器	1	1	1	1	中等
路由器	2	2	2	2	很高

5 结束语

主要论述了通过分析信息系统资产的 CIA 属性实现安全评估的方法。该方法首先对资产进行分析,然后通过扫描发现资产漏洞相应的漏洞,结合 CVSS 评分系统和 NVD 漏洞库,实现对系统的风险等级的评估。该方法进一步的改进工作包括资产的价值评估和权重分析,可以凸显出核心资产在安全风险评估中的地位,实现更准确的评估效果。

参考文献:

[1] 国家计算机网络应急技术处理协调中心. 2015 年中国互联网络网络安全报告[M]. 北京:人民邮电出版社,2016.

[2] 中国信息安全测评中心. 2016 年国内外信息安全漏洞态势报告[J]. 中国信息安全,2017(1):110-116.

[3] SHAMELI-SENDI A, AGHABABAEI-BARZEGAR R, CHERIET M. Taxonomy of information security risk assessment (ISRA)[J]. Computers & Security,2016,57:14-30.

[4] IONITA D, HARTEL P, PIETERS W, et al. Current established risk assessment methodologies and tools[R]. [s. l.]: [s. n.],2014.

[5] 张 弢,慕德俊,任 帅,等. 一种基于风险矩阵法的信息安全风险评估模型[J]. 计算机工程与应用,2010,46(5):93-95.

印算法中的编解码问题,实现 H. 264 的视频解码功能,包括 ts、mp4 等视频格式。提出了 FFMPEG 转码图形用户界面的具体实现方法,介绍了 FFMPEG 转码加密模块的流程、函数调用关系、具体加密算法的实现和视频播放模块的具体实现。利用模块化思想,为不同编码格式的视频水印算法提供一个通用平台,对视频的版权保护起到了积极作用,具有一定的现实意义和参考价值。

参考文献:

[1] CHANG X, WANG W, ZHAO J, et al. A survey of digital video watermarking [C]//Seventh international conference on natural computation. [s. l.]:[s. n.], 2011:61-65.

[2] 任 严,韩 臻,刘 丽.基于 FFMPEG 的视频转换与发布系统[J]. 计算机工程与设计,2007,28(20):4962-4963.

[3] 王 彤.基于 FFmpeg 的 H. 264 解码器实现[D]. 大连:大连理工大学,2011.

[4] CHENG Yun, LIU Qingtang, ZHAO Chengling, et al. Design and implementation of mediaplayer based on FFmpeg [J]. Software Engineering and Knowledge Engineering, 2012, 2: 867-874.

[5] ZENG Hao, FANG Yuan. Implementation of video transcoding client based on FFMPEG [J]. Advanced Materials Research, 2013, 756-759:1748-1752.

(上接第 143 页)

[6] 刘延华,陈国龙,吴瑞芬.基于云模型和 AHP 的网络信息系统可生存性评估[J]. 通信学报,2014,35(8):107-115.

[7] 杨姗媛,朱建明.基于 TOPSIS 的信息安全风险评估应用研究[J]. 现代管理科学,2014(2):24-26.

[8] KHANMOHAMMADI K, HOUMB S H. Business process-based information security risk assessment [C]//Fourth international conference on network and system security. Washington, DC, USA: IEEE Computer Society, 2010:199-206.

[9] FIRESMITH D G. Common concepts underlying safety, security, and survivability engineering [R]. [s. l.]:[s. n.], 2003.

[10] KARABACAK B, SOGUKPINAR I. ISRA M; information security risk analysis method [J]. Computers & Security, 2005, 24(2):147-159.

[6] 辛长春,姜小平,吕乃光.基于 FFmpeg 的远程视频监控系统编解码[J]. 电子技术,2013(1):3-5.

[7] 张国庆.基于 FFmpeg 的视频转码与保护系统的设计与实现[D]. 武汉:华中师范大学,2011.

[8] 李芳芳,苏凯雄.基于 FFmpeg 的 H. 264 格式转换器的设计与实现[J]. 电视技术,2016,40(7):32-35.

[9] 胡 聪,周 甜,唐璐丹.基于 FFMPEG 的跨平台视频编解码研究[J]. 武汉理工大学学报. 2011, 33(11):139-142.

[10] 吴 岳,施惠娟.基于 FFMPEG 的视频水印系统[J]. 电子设计工程,2013,21(23):185-187.

[11] 胡 成,任平安,李文莉.基于 Android 系统的 FFmpeg 多媒体同步传输算法研究[J]. 计算机技术与发展,2011,21(10):85-87.

[12] LI Chengbo, JIANG Hong, WILFORD P, et al. Video coding using compressive sensing for wireless communications [C]//WCNC 2011. [s. l.]:IEEE, 2011:2077-2082.

[13] 李 科,李 璐,兰时勇.基于 FFmpeg 和 SDL 实现多路实时流变换及播放[J]. 计算机技术与发展,2014,24(4):65-68.

[14] 汪俊杰,王志明.基于 SDL 的 H. 264 流媒体播放系统[J]. 计算机系统应用,2013,22(12):51-54.

[15] DUAN H, NG B P, CHONG M S S, et al. Applications of the SRV constraint in broadband pattern synthesis [J]. Signal Processing, 2008, 88(4):1035-1045.

[11] SENDI A S, JABBARIFAR M, SHAJARI M, et al. FEMRA: fuzzy expert model for risk assessment [C]//Fifth international conference on internet monitoring and protection. Washington, DC, USA: IEEE Computer Society, 2010:48-53.

[12] RHINOW F, CLEAR M. Scargos: towards automatic vulnerability distribution [C]//International conference on security and cryptography. [s. l.]:IEEE, 2015:369-376.

[13] Forum of Incident Response and Security Teams (first.org). Common vulnerability scoring system CVSS v3.0 specification [S/OL]. 2015. <https://www.first.org/cvss/cvss-v30-specificationv1.7.pdf>.

[14] 肖 晖,张玉清. Nessus 插件开发及实例[J]. 计算机工程, 2007, 33(2):241-243.

[15] 温 涛.安全漏洞危害评估研究暨标准漏洞库的设计与实现[D]. 西安:西安电子科技大学,2016.