

基于灰色理论的层次化网络安全态势评估方法

李玲娟,孔凡龙

(南京邮电大学 计算机学院,江苏 南京 210003)

摘要:网络安全态势是指某时刻整个系统所处的安全运行状态,网络安全态势评估是安全领域的研究热点之一。文中以能够准确把握一个网络系统的安全态势为目标,设计了一种基于灰色理论的层次化网络安全态势评估方法。该方法利用灰色关联分析法对网络中的攻击要素进行关联,进而在服务、主机、网络等3个层次上综合运用统计技术和专家系统给出的权重来完成相应的态势信息的融合。基于Honeynet数据集的仿真实验结果表明,使用文中设计的方法能够有效而准确地得出网络的总体安全态势。

关键词:网络安全态势;评估;灰色关联分析

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2010)08-0163-04

A Hierarchical Network Security Situation Evaluation Method Based on Grey Theory

LI Ling-juan, KONG Fan-long

(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Network security situation means the safe running-state of the entire network, and the research on network security situation is one of the hot topics in security field. In order to accurately grasp a network system's security situation, designs a hierarchical network security situation evaluation method based on the grey theory. This method relates attack factors in the network by utilizing the grey incidence analysis; obtains the corresponding situation information by using both of the weightiness given by expert system and the statistical technology on the three-layer of services, hosts and networks. The result of simulation experiment based on the Honeynet Data Set illustrates that the whole network security situation can be efficiently and exactly obtained by this method.

Key words: network security situation; evaluation; grey incidence analysis

0 引言

目前,随着Internet的迅速发展,各种网络攻击事件不断发生,使得网络安全问题日益成为人们关注的焦点。为了保证网络安全运行,人们采用了入侵检测、防火墙、病毒检测等技术。然而这些技术每天都会产生海量的告警信息,这使得网络管理员很难了解网络系统的安全状况,不能及时采取合适的应对措施。因此如何真实、准确、客观地对网络安全态势进行评估已经成为当前网络安全领域的一个研究热点。

所谓态势是一种状态,一个趋势,是一个整体和全局的概念。网络安全态势是指某时刻由各种网络设备

运行情况、网络服务状况及用户行为等因素构成的整个网络所处的安全状况^[1]。而网络安全态势感知则指在大规模网络环境中,对能够引起网络安全态势发生变化的安全要素进行提取、理解、显示,并能预测未来发展的趋势,这是网络安全态势评估的关键之一,需要融合海量的网络安全状态数据。

基于此,文中将灰色系统理论引入网络安全态势评估中,把网络攻击行为作为安全要素,通过使用灰色关联分析法来量化某段时间内网络攻击行为对该网络所产生的相对影响,进而建立层次化的网络分析模型,实现对整个网络所处的安全环境的量化评估,帮助管理员更好地了解网络安全状况。

1 层次化网络安全态势评估模型

为了对一个网络的整体安全状况做出判定,分析网络所遭受的各种攻击对网络安全造成的影响,文中综合运用基于层次分析法的网络安全态势评估方法的

收稿日期:2009-12-07;修回日期:2010-03-09

基金项目:国家高技术研究发展计划(863计划)资助项目(2006AA01Z439);江苏省高校自然科学基金研究项目(08KJB620002);南京邮电大学校科研基金(NY207051)

作者简介:李玲娟(1963-),女,辽宁辽阳人,教授,研究方向为数据挖掘、网络安全等。

思想^[2]和灰色系统理论,设计了一个基于灰色关联分析的层次化网络安全态势评估模型。该模型由上至下分为网络系统、主机、服务、关联和攻击共5层,如图1所示。

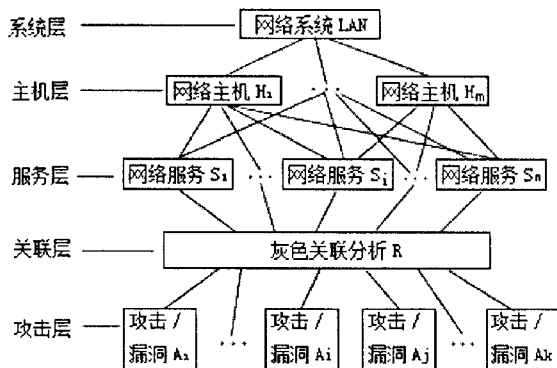


图1 层次化网络安全态势评估模型

图1中,攻击层中的数据来自于常见的入侵检测系统的检测数据、防火墙数据、系统审计日志数据等融合后所形成的具有统一格式的数据。为了简述方便,文中先给出各层涉及的相关概念:

定义1 攻击 A:引发系统安全设备产生报警的黑客攻击行为,该行为通过数据融合后形成统一的表示形式(比如 XML 格式)。

定义2 关联 R:对检测出的安全事件进行关联,确定网络环境中各个要素之间的相对隐含关系。

定义3 服务安全态势指数 FS:具有一定重要程度的服务,在遭受一定数量的外部攻击事件时,其对应的安全策略被违反的程度。

定义4 主机安全态势指数 FH:具有不同重要程度的服务在某时间段内受到的威胁对服务器安全策略的违反程度。

定义5 网络系统安全态势指数 FL:多个遭受不同威胁程度的主机对网络系统安全策略的总体违反程度。

安全态势指数值越高,遭受的威胁越大,安全性越差。

2 灰色关联分析法及安全态势指数的定量计算

2.1 灰色关联分析法

灰色关联分析法的思路^[3]是:在许多客观事物之间、因素之间,相互关系比较复杂,人们在认识、分析、决策时,得不到全面、足够的信息,不容易形成明确的概念。因为这些都是灰色因素、灰色关联性在起作用,所以对灰色系统进行分析和研究时,要解决如何从随机的时间序列中,找到关联性和关联性的度量值,以便

进行因素分析,为系统决策提供依据^[4]。

假设 Y_1, Y_2, \dots, Y_s 为系统特征行为数据序列, $Y_i = (y_i(1), y_i(2), \dots, y_i(n)); i \in (1, 2, \dots, s); X_1, X_2, \dots, X_m$ 为相关因素行为序列, $X_j = (x_j(1), x_j(2), \dots, x_j(n)); j \in (1, 2, \dots, m); Y_i$ 与 X_j 长度相同。

定义 Y_i 对 X_j 的灰色关联度^[5]为:

$$r(Y_i, X_j) = \frac{1}{n} \sum_{k=1}^n R(y_i(k), x_j(k)) \quad (1)$$

$i \in (1, 2, \dots, s), j \in (1, 2, \dots, m)$

其中: $\xi \in (0, 1)$ 为分辨系数, $R(y_i(k), x_j(k))$ 定义为:

$$R(y_i(k), x_j(k)) = \frac{\min_k |y_i(k) - x_j(k)| + \xi \max_k |y_i(k) - x_j(k)|}{|y_i(k) - x_j(k)| + \xi \max_k |y_k(k) - x_j(k)|} \quad (2)$$

计算出所有的 r_{ij} , 即 $r(Y_i, X_j)$ 构成 $s \times m$ 的灰色关联矩阵:

$$(r_{ij}) = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1m} \\ r_{21} & r_{22} & & r_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ r_{s1} & r_{s2} & \dots & r_{sm} \end{bmatrix}$$

此灰色关联矩阵中第 i 行的元素是系统特征数据序列 $Y_i (i \in (1, 2, \dots, s))$ 与相关因素序列 X_1, X_2, \dots, X_m 的灰色关联度;第 j 列的元素是系统特征数据序列 Y_1, Y_2, \dots, Y_s 与 $X_j (j \in (1, 2, \dots, m))$ 的灰色关联度^[6]。

2.2 安全态势指数的定量计算

基于灰色关联分析法,文中设计了安全态势指数的定量计算方法^[7],具体如下:

(1) 服务级。

定义 t 时间段内,服务 FS_j 的安全态势指数为:

$$FS_j(t) = \sum_{i=1}^n 10^{P_{ij}} FA_i(t) \quad (3)$$

其中, FA_i 为 t 时间段某类攻击对服务 S_j 产生的攻击态势指数,该态势指数是基于灰色关联分析法的攻击要素关联而得到的, i 为某段时间内该服务所遭受攻击的种类数, P_{ij} 为 A_i 对服务 S_j 的危害程度,其值由攻击所属类型来决定。文中参照 Snort^[8,9] 手册用 3、2、1 来表示高、中、低 3 个等级的危害程度,表 1 是从 Snort 手册上摘录的部分攻击类别及其对应的危害程度。

(2) 主机级。

在 t 时间段内,主机 FH_k 的安全态势指数为:

$$FH_k(t) = \sum_{j=1}^m V_j FS_j(t) \quad (4)$$

式中, $FS_j(t)$ 为 t 时间段主机 H_k 的服务 S_j 的安全态势指数, j 为主机 H_k 中开通的服务数, V_j 为服务 S_j

在主机 H_k 的各种服务中所占的重要性权值,该值通过专家系统获得。

表 1 攻击类别与危害程度

攻击类别	攻击描述	危害程度
Attempted admin	企图获得管理员权限	高(3)
Shell code detect	检测到可执行代码	高(3)
Http_uri decode	企图修改 IE 内核信息	高(3)
Attempted dos	企图拒绝服务	中(2)
RPC-port map decode	远程过程调用查询解码	中(2)
Mapping modified	企图修改映射信息	中(2)
Network scan	检测到网络扫描	低(1)
Misc-antivity	其他活动	低(1)

(3) 网络系统级。

在 t 时间段内,网络系统的安全态势指数为:

$$FL(t) = \sum_{l=1}^n W_l FH_l(t)$$
 (5)

其中, l 为局域网 L 中主机的数量。 W_l 为主机 l 在局域网 L 中所占重要性权值,该值通过专家系统获得。

3 仿真实验及结果分析

3.1 实验数据选择及所用网络拓扑结构

“Honeynet Project”(蜜网项目组)是一个非赢利性的研究组织,其目标是学习黑客社团所使用的工具、技术和动机,并将学习到的信息共享给安全防护人员。该组织维护着 8 个高度控制和完全监视的网络,收集和归档了 2000 年 4 月到 2001 年 2 月这段时期中网络的每一个攻击。Honeynet DATA 有价值的地方是减少了主动错误信息和被动错误信息所产生的问题。

基于上述 Honeynet 及其数据的特点,文中选用 Honeynet 数据集^[10,11]为实验数据来模拟黑客的入侵行为,并进行安全态势分析。

下面以 Honeynet 2000 年 9 月份的数据为例,分析这一个月服务、主机及网络系统的安全状态演化。由于 Honeynet 组织并没有给出网络拓扑结构,所以文中根据其数据集进行分析时,建立了以下网络拓扑结构,如图 2 所示。

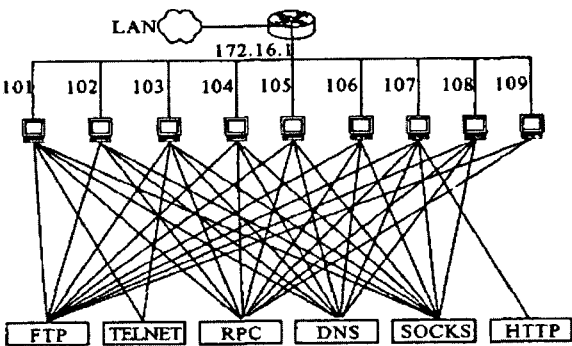


图 2 网络拓扑结构

该拓扑结构中有 9 台主机,提供 6 项服务。

3.2 实验结果分析

通过对 Honeynet 数据集进行分析,参照表 1 所示的 Snort 手册给出的各攻击类别的危害程度,文中统计了在 t 时间内(可根据系统性能,来调整时间段 t 的大小)网络所遭受的攻击情况,包括受攻击的总次数和受影响的主机数。如表 2 所示。其中: A_1 是 Ping 攻击, A_2 是 RPC 攻击, A_3 是 DOS 攻击, A_4 是 Shellcode 攻击, A_5 是 DNS 欺骗, A_6 是 http 攻击。

表 2 网络遭受攻击数统计

攻击要素 攻击数, 主机数 时间片	攻击要素 (危害 程度) $A_1(1)$	$A_2(2)$	$A_3(2)$	$A_4(3)$	$A_5(2)$	$A_6(3)$
t_1	40,1	0,0	0,0	2,1	3,1	2,1
t_2	0,0	6,3	16,5	4,2	9,3	0,0
t_3	1,1	1,1	1,1	0,0	6,1	28,1
t_4	0,0	0,0	0,0	0,0	24,6	0,0
t_5	8,1	0,0	20,8	1,1	14,2	0,0
t_6	50,1	10,5	20,6	3,3	35,8	15,1
t_7	45,1	5,5	10,5	1,1	24,3	15,1
t_8	0,0	3,2	5,3	0,0	10,4	14,1

将表 2 中的数据进行无量纲化和标准化处理,并根据公式(1)、公式(2)求取其灰色关联矩阵,得到其相关因素的灰色关联度值,如表 3 所示,其中攻击要素的含义同表 2。

表 3 灰色关联度值

攻击要素 关联度值 (威胁 程度) 时间片	$A_1(1)$	$A_2(2)$	$A_3(2)$	$A_4(3)$	$A_5(2)$	$A_6(3)$
t_1	0.6699	0	0	0.5704	0	0.1647
t_2	0	0.4979	0.4787	0.6004	0.6667	0
t_3	0.0352	0.4253	0.0684	0	0.1134	0.6667
t_4	0	0	0	0.0000	0.6665	0
t_5	0.8024	0	0.6699	0.3990	0.3932	0
t_6	0.6345	0.6667	0.5814	0.5769	0.5633	0.5034
t_7	0.4727	0.3062	0.1626	0	0.2408	0.3114
t_8	0	0.2568	0.6667	0	0.1397	0.3527

然后,根据公式(3)、公式(4)、公式(5)可计算出相应的服务、主机、网络系统的安全态势指数,其中服务、主机的重要性权值采用参考文献[2]中得出的权值。6 项服务对应的 $V' = \{0.25, 0.083, 0.25, 0.25, 0.167, 0.083\}$, 9 台主机对应的 $W' = \{0.105, 0.105, 0.158, 0.105, 0.105, 0.105, 0.158, 0.105, 0.054\}$ 。最终的计算结果(即网络系统安全态势指数值 FL)如表 4 所示。

表 4 网络系统安全态势指数值

时间	t_1	t_2	t_3	t_4
安全态势指数值	0.1932	0.2143	0.4234	0.0758
时间	t_5	t_6	t_7	t_8
安全态势指数值	0.7633	0.8724	0.8253	0.5651

通过表 4 的数据分析可以看出,该网络在时间段 t_1 、 t_2 、 t_4 内的安全态势指数值比较小,表明此阶段网络的安全态势比较安全、稳定;在时间段 t_3 、 t_5 、 t_8 内虽然遭受到一定的威胁,但还可以维持其运行状态。在 t_6 、 t_7 时刻,网络安全态势指数值很高,表明此时间段内网络遭受到较大的威胁,应该引起网络管理员的重视,采取必要的措施。

对照表 2,可以看出用文中设计的基于灰色理论的层次化网络安全态势评估方法得出的评估结果比较符合客观情况。

需要指出的是,以上的分析中,默认安全态势指数值与网络安全状态的对应关系为:

FL 在 $[0, 0.3]$ 之间,网络是安全的;

FL 在 $[0.31, 0.8]$ 之间,网络可正常运行;

FL 在 $[0.81, 1]$ 之间,网络遭受到的威胁严重,网络处于不安全的状态。

在实际运用中,管理人员可以根据安全防范需求,动态设置安全态势指数的阈值^[12]。

4 结束语

文中设计了一种基于灰色理论的层次化网络安全态势评估方法,给出了层次化网络安全态势评估模型和安全态势指数的定量计算方法,并采用 Honeynet 数据集,利用所设计的方法,对网络中发生的网络安全事件和基于这些事件的网络安全态势评估过程进行了仿

真和分析,给出了整个网络系统在实验所处环境下的安全状况。通过实验可以看出,文中设计的这种方法能比较有效而准确地评估网络的安全态势,这有助于网络管理员及时根据反馈信息进行安全措施调整,从而提高网络安全管理效率。

参考文献:

- [1] 陈秀真,郑庆宏,管晓宏,等.网络化系统安全态势评估的研究[J].西安交通大学学报,2004,38(4):503-507.
- [2] 王廷博,徐世超.基于层次分析法的网络安全态势评估方法研究[J].电脑知识与技术,2008,5(4):56-58.
- [3] 刘思峰,党耀国,张岐山.灰色系统理论及其应用[M].第3版.北京:科学出版社,2004.
- [4] 肖新平,宋中民,李峰.灰技术基础及其应用[M].北京:科学出版社,2005.
- [5] 熊和金,陈绵云.灰色关联度公式的几种推广[J].系统工程与电子技术,2000,22(11):8-11.
- [6] 唐志刚,赵建国,张超.灰色关联度分析法评判目标威胁度[J].火力与指挥控制,2004,29(6):79-80.
- [7] 朱振国,鄢羽,张闽,等.一种量化的网络安全态势评估方法[J].微计算机信息,2007,23(3):62-65.
- [8] Feng D G, Zhang Y, Zhang Y Q. Survey of information security risk assessment[J]. Journal of China Institute of Communications, 2004, 25(7): 10-18.
- [9] Martin R, Chris G. Snort users manual, Snort release 2.0.0 [EB/OL]. 2002-07-06. <http://www.snort.org/docs/SnortUsersManual.pdf>.
- [10] Honeynet Project. Know your enemy: statistics [EB/OL]. 2001-07-22. <http://www.HoneyNet.org/papers/stats/>.
- [11] Honeynet Project. Scan 17 [EB/OL]. 2002. <http://www.honeynet.org/scans/scan17>.
- [12] 柯敏毅,肖俊林.网络安全评估的量化研究[J].网络安全技术与应用,2006(9):18-21.

(上接第 162 页)

- [3] 范萍,李罕伟.基于 ACL 的网络层访问权限控制技术[J].华东交通大学学报,2004(4):89-92.
- [4] 洪新建,洪新华,谢庆华.反射访问控制列表在网络安全中的应用[J].计算机安全,2007(3):40-41.
- [5] 曾旷怡,杨家海.访问控制列表的优化问题[J].软件学报,2007,18(4):978-986.
- [6] Lammle T. CCNA 学习指南[M].北京:电子工业出版社,2004.
- [7] Vatsavai R R, Chakravarthy S, Mohania M. Access Control Inference and Feedback for Policy Managers: A Fine-Grained Analysis[C]//IEEE International Workshop on Policies for Distributed Systems and Networks. London: [s. n.], 2006.
- [8] 刘军,王彩萍.ACL 在 IP 网络中的应用[J].计算机与数字工程,2009,37(1):178-181.
- [9] Hariri S, Qu Guangzhi, Dharmagadda T, et al. Impact analysis of faults and attacks in large-scale networks[J]. Security Private Magazine, IEEE, 2003, 11(1): 49-54.
- [10] 诸晔.用 ACL 实现系统的安全访问控制[J].计算机应用与软件,2005,22(3):111-114.
- [11] 方贤进,李敬兆,姚亚锋,等.一种校园网的网络安全策略[J].计算机技术与发展,2006,16(5):121-124.
- [12] Verma D C, Calo S, Amiri K. Policy-based management of content distribution networks[J]. Network, IEEE, 2002, 16(2): 34-39.