科技导报 2007 年 第 25 卷 第 7 期 (总第 229 期)

攻防对抗环境下的网络安全态势评估技术研究

姚淑萍

北京理工大学计算机网络攻防对抗技术实验室,北京 100081

[摘要] 为了弥补当前网络安全态势评估系统的不足,提出了一种基于攻防对抗环境的网络安全态势量化评估算法。该方法在深入分析影响安全态势各项因素的基础上,将传统的风险评估与网络防护状况、资产安全特性等环境因素相结合,提取出多个量化指标,按照攻击类别进行安全态势的量化评估。实验结果表明,该方法能够为安全管理人员提供更为客观、详实的态势信息,使之更为清晰地把握整个网络的安全状况。

[关键词] 攻防对抗;网络安全;态势评估

[中图分类号] TP393 [文献标识码] A [文章编号] 1000-7857(2007)07-0009-04

Research on Network Security Evaluation Technology Based on Attack-defense Confrontation

YAO Shuping

Laboratory of Computer Network Defense Technology, Beijing Institute of Technology, Beijing 100081, China

Abstract: In order to improve the current network security evaluation systems, a novel evaluation algorithm, called the quantitative network security evaluation based on attack-defense confrontation, is proposed in this paper. In this algorithm, the traditional risk assessment is combined with network environment factors such as the network running status, asset security characteristics and so on, and several quantitative indexes are extracted based on the analysis of factors which can affect the LAN's security situation. Then, evaluations are made based on a classification of attacks. Experiment results show that the novel algorithm can be used to

收稿日期: 2007-03-06

作者简介: 姚淑萍,女,北京市海淀区中关村南大街 5 号北京理工大学计算机网络攻防对抗技术实验室,讲师,研究方向为信息安全;
E-mail: yaosping@163.com

[4] HELMER G, WONG J, HONAVAR V, *et al*. Automated discovery of concise predictive rules for intrusion detection[J]. J Systems and Software, 2002, 60(3): 165-175.

[5] GLASS R L, VESSEY I. Contemporary application-domain taxonomies[J]. IEEE Software, 1995, 12(8): 906-916.

[6] AMOROSO E G. Fundamentals of computer security technology[M]. USA: Prentice-Hall PTR, 1994.

[7] FAN Jang-Jong, SU Keh-Yih. An efficient algorithm for match multiple patterns[J]. IEEE Trans on Knowledge and Data Engineering, 1993, 5(2): 339-351.

[8] 赵 蓓, 胡昌振. 基于有限自动机的躲避攻击快速检测技术[J]. 计算机应用研究, 2006, 23: 973-974.
ZHAO Bei, HU Changzhen. Effcient algorithm for detection evade IDS attack based on finite state automata [J]. Application Research of Computers, 2006, 23: 973-974.

[9] 邢江宁, 张炜, 张铁军, 等. FPW 对缓冲区溢出的实施检测[J]. 小型微型计算机系统, 2004, 25(4): 151-152.
XING Jiangning, ZHANG Wei, ZHANG Tiejun, *et al*. FPW detects buffer overflow in realtime[J]. Mini-Microsystems, 2004, 25(4): 151-152.

[10] LINDQVIST U, JONSSON E. How to systematically classify computer security intrusions [C]//Proceedings of the 1997 IEEE symposium on security and privacy, oakland, USA, May, 1997. IEEE Press, 1997: 154-163.

[11] TEMPLETION S J, LEVITT K. A requires/provides model for computer attacks [C]// Proceedings of the 2000 new security paradigms workshop. Cork, Ireland: ACM Press, 2000: 31-38.

(责任编辑 赵 佳)

extract situation information more objective and detailed so the security administrator may form a clearer picture for the LAN's security situation.

Key Words: attack-defense confrontation; network security; situation evaluation
CLC Number: TP393 **Document Code:** A **Article ID:** 1000-7857(2007)07-0009-04

0 引言

切实有效的网络安全态势评估可以使安全管理人员准确地把握网络安全状况及趋势，为其决策提供支持。网络安全态势评估是信息安全领域的一个新方向，按照数据源可以分为静态评估和动态评估两大类。静态评估即风险评估，依据一定的标准，基于威胁、脆弱性和资产价值 3 个指标定性或定量地评估网络的安全风险状况。动态评估是真正意义上的态势评估，它将风险与环境紧密结合，动态地把握风险在特定环境下的演化。这里的环境主要指网络运行状况、安全防护状况、用户安全特性等。

目前的研究成果大多集中于风险评估[1-4]。文献[5]提出了网络安全威胁态势的概念，利用 IDS 报警，基于服务、主机的重要性，构建了层次化网络安全威胁态势评估模型和相应的量化计算方法，定量评估了网络所受攻击的状况，使该领域的研究推进了一大步。但其也有不足之处，作者只考虑了单一安全设备报警信息，未将评估与具体的网络环境信息相结合，给出的态势报告仅是一个综合的威胁结果，安全管理员无法从中了解不同种类攻击在态势演化中的作用以便查找安全变化的原因。

本文提出了攻防对抗环境下的网络安全态势评估方法，将传统的风险评估与网络防护状况、资产安全特性等环境因素相结合，构建了基于攻击分类的安全态势评估模型，为安全管理员提供了更为可靠、详实的态势信息。

1 网络安全态势评估拓扑

图 1 为某局域网环境下安全态势评估系统的部署。被评估对象为两个 VLAN 中的所有资产。评估需要的威胁信息来自两个网络入侵检测系统(NIDS)，NIDS1 位于防火墙、VPN 等边界产品之外，它提供的告警信息表征该局域网受到的外部威胁状况，称为威胁检测系统；NIDS2 位于局域网内，它的告警表征来自外部和内部的真正攻击状况，称为攻击检测系统。二者之间外部网络告警的差异体现了局域网的边界防护功效。评估需要的脆弱性信息取自底层的扫描设备，资产价值及其安全特性等环境信息则由安全管理员提供，存储于指定的配置数据库。

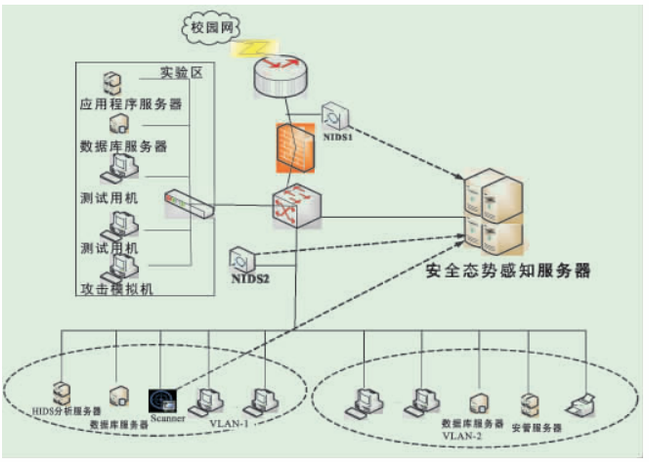

图 1 网络安全态势评估拓扑
Fig. 1 Topology of network security assessment

2 网络安全态势评估体系

图 2 给出了完整的态势评估系统，由信息获取、态势感知和分析报告 3 个层次构成。信息获取层是体系的基础，负责收集所需要的各类原始信息，包括扫描器提供的脆弱性信息，威胁检测系统提供的威胁信息，攻击检测系统的攻击信息以及由配置信息库读取的有关资产信息等；态势感知层是体系的核心，依据特定的评估算法，基于所获取的信息，分层、分类定量评估网络的安全状况；分析报告层则是体系的可视化界面，它以直观、明了的形式将评估结果提供给不同身份的用户。下面先介绍文中所涉及的概念。

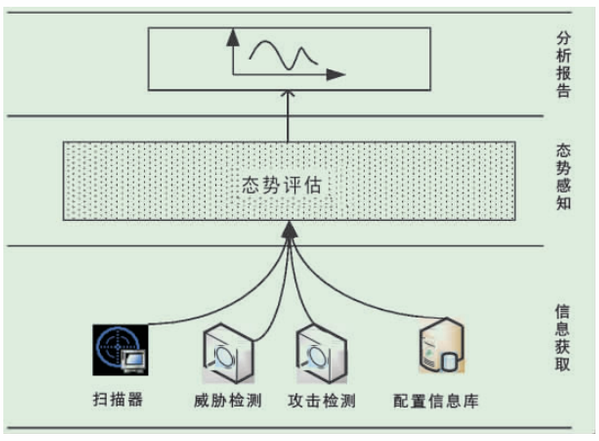

图 2 网络安全态势评估体系
Fig. 2 Assessment system for network security

定义 1 潜在威胁 T。引发威胁检测系统报警但未引发攻击检测系统报警的黑客行为，体现了边界防护产品的效能，预示局域网所受到的潜在的威胁，表示为 $T=\{T_n, T_t, T_c, S_i, S_p, D_i, D_p, T_l, T_v\}$。其中，$T_n$ 表示威胁的名称；T_t 表示威胁发生的时间；T_c 表示威胁类型；S_i 和 S_p 分别表示威胁源 IP 和源端口；D_i 和 D_p 分别表示威胁目标 IP 和目标端口；T_l 表示威胁等级；T_v 表示威胁利用的漏洞，如果威胁不是针对特定漏洞的，则该项的值为 ε。

定义 2 实际攻击 A。引发攻击检测系统报警的黑客行为，体现了局域网真正受到的威胁状况，表示为 $A=\{A_n, A_t, A_c, S_i, S_p, D_i, D_p, A_l, A_v\}$；其中各项含义与定义 1 相同。依据攻击源的不同，A 又可以分为外部攻击 A_o 和内部攻击 A_i。

定义 3 资产安全敏感度 q。指某项资产（普通主机或服务器）对信息的保密性、完整性和可用性 3 个属性的敏感程度，表征了资产的安全特性。

3 态势评估算法

本文将攻击/威胁分为探测、缓冲区溢出、拒绝服务、蠕虫、木马和其他六大类，针对每一类攻击/威胁，分别评估局域网的安全态势，进而获得综合态势。

3.1 基于攻击分类的安全态势评估算法

局域网的安全态势由实际攻击态势和潜在威胁态势两部分构成，给定分析时间窗口 τ，以 τ 为时间单位的第 k（k=1,2,…,6）类攻击对局域网安全的影响态势为

$$S_k(\tau)=f(SA_k(\tau),ST_k(\tau))=SA_k(\tau)+ST_k(\tau) \quad (1)$$

其中，$S_k(\tau)$为某类攻击形成的安全态势，$SA_k(\tau)$和 $ST_k(\tau)$ 分别为第 k 类攻击形成的实际攻击态势和潜在威胁态势。

3.1.1 实际攻击态势评估算法

实际攻击态势由实际发生的属于第 k 类的所有攻击行为形成的态势构成，令 $\boldsymbol{A}_k=\{a_{k1}, a_{k2},\cdots, a_{kn}\}$ 表示时间窗 τ 内第 k 类实际攻击的具体攻击行为，则有

$$SA_k(\tau)=f(S\boldsymbol{A}_k(\tau))=\sum_{i=1}^{n} Sa_{ki}(\tau) \quad (2)$$

其中，$Sa_{ki}(\tau)$为第 k 类的第 i 种（i=1, 2,…, n）真实攻击形成的态势。令 $\boldsymbol{H}=\{h_1, h_2,\cdots, h_l\}$ 表示受到该种攻击的资产集合，则

$$Sa_{ki}(\tau)=f(\boldsymbol{p}(\tau), \boldsymbol{c}(\tau), \boldsymbol{v}(\tau), \boldsymbol{q}(t))=\sum_{j=1}^{l} p_j c_j v_j q_j \quad (3)$$

其中，

1）$\boldsymbol{p}(\tau)=[p_1, p_2,\cdots, p_l]$为时间窗 τ 内该种攻击针对各项资产的发生次数向量，元素 p_j 为第 j 项资产受到该种攻击的次数。

2）$\boldsymbol{c}(\tau)=[c_1, c_2,\cdots, c_l]$为时间窗 τ 内该种攻击针对各项资产的严重程度向量，元素 c_j 为第 j 项资产受到该种攻击的严重度，其评估的方法如下。

首先，参照 Snort 对攻击严重度的划分，根据攻击造成的后果、攻击实施的难易程度以及攻击手段是否易于获取等因素，将攻击分为高、中、低 3 个等级，分别用 3,2,1 表示。

其次，考虑针对具体资产项的攻击是否有效，分别评估各资产项的攻击严重度

$$c_j=\begin{cases}1 & (a_{ki,\text{leak}}\neq\varepsilon)\cap(a_{ki,\text{leak}}\notin \boldsymbol{L}_j)\\ a_{ki,\text{level}} & (a_{ki,\text{leak}}=\varepsilon)\cup(a_{ki,\text{leak}}\in \boldsymbol{L}_j)\end{cases} \quad (4)$$

其中，$\boldsymbol{L}_j$ 为扫描器发现的第 j 项资产项的漏洞集合，若攻击 i 需要利用特定漏洞且扫描器没有发现该项资产存在相应漏洞，攻击无效，将其攻击严重度降为低；若攻击 i 与漏洞无关或该项资产存在相应漏洞，攻击严重度保持原值。

3）$\boldsymbol{v}(\tau)=[v_1, v_2,\cdots, v_l]$为时间窗 τ 内该种攻击针对的各项资产的价值向量，元素 v_j 为第 j 项资产的价值。本文资产价值由安全管理员评估后录入，分为非常重要、重要、一般 3 个等级，分别用 3,2,1 表示。

4）$\boldsymbol{q}(\tau)=[q_1, q_2,\cdots, q_l]$为时间窗 τ 内不同资产项对某种安全属性的敏感程度向量。每一类攻击威胁信息安全的角度不同，如 DOS、蠕虫攻击主要危害信息的可用性，通过缓冲区溢出提升了用户权限，则可以破坏信息的机密性和完整性。另一方面，不同资产项的安全需求也不一样，WWW 服务器看重的主要是可用性和完整性，而数据库服务器则重视信息的机密性和完整性。资产安全敏感度的引入可以使安全管理员在面对同等程度风险的状况下优先处理敏感度高的主机。其评估方法如下。

首先，根据资产项的信息特性，分别针对机密性、完整性和可用性 3 个属性按照高、中、低 3 种程度计分，例如对一台数据库服务器的计分方法为：完整性 3 分，机密性 2 分，可用性 1 分，表示为 sc_1=3，sc_2=2 和 sc_3=1。

其次，确定第 k 类攻击主要破坏的信息安全属性 r，每一资产项的敏感度为

$$q_j=\frac{sc_{jr}}{\sum_{u=1}^{l} sc_{ur}} \quad (5)$$

其中，q_j 为第 j 项资产的安全敏感度，sc_{ur} 为第 u 项资产的第 r 个安全属性的分值。

3.1.2 潜在威胁态势评估算法

潜在威胁态势由属于第 k 类的所有潜在威胁行为形成的态势构成，令 $\boldsymbol{T}_k=\{t_{k1}, t_{k2},\cdots, t_{km}\}$ 表示时间窗 τ 内第 k 类潜在威胁的具体威胁行为，则

$$ST_k(\tau)=f(S\boldsymbol{T}_k(\tau))=\sum_{i=1}^{m} St_{ki}(\tau) \quad (6)$$

其中，$St_{ki}(\tau)$为第 k 类的第 $i(i=1, 2, \cdots, m)$种潜在威胁形成的态势，令 $\boldsymbol{H}'=\{h_1, h_2, \cdots, h_w\}$为受到该种攻击的资产集合，则有

$$St_{ki}(\tau)=f(\boldsymbol{p}(\tau), \boldsymbol{c}(\tau), \boldsymbol{v}(\tau), \boldsymbol{q}(t))=\sum_{j=1}^{w} p_j c_j v_j q_j \qquad (7)$$

其中，除攻击严重度的评估外，其他各项的评估方法与 3.1.1 节相同。

考虑到潜在威胁毕竟是未成功的攻击行为，其严重度应适当降低，具体为

$$c_j=\begin{cases}1 & (t_{ki,\text{leak}}\neq\varepsilon)\cap(t_{ki,\text{leak}}\notin \boldsymbol{L}_j)\\ t_{ki,\text{level}}-1 & (t_{ki,\text{leak}}=\varepsilon)\cup(t_{ki,\text{leak}}\in \boldsymbol{L}_j)\end{cases} \qquad (8)$$

其中，$\boldsymbol{L}_j$ 为扫描器发现的第 j 项资产项的漏洞集合，若威胁 i 需要利用特定漏洞且扫描器没有发现该项资产存在相应漏洞，威胁无效，将其攻击的严重度降为零，不计入威胁评估中；若威胁 i 与漏洞无关或该项资产存在相应漏洞，威胁严重度比实际严重度降低一级。

3.2 综合态势评估算法

综合态势是各类安全态势的总和，给定分析时间窗口 τ，以 τ 为时间单位的局域网安全态势为

$$S(\tau)=f(S_k(\tau))=\sum_{i=1}^{6} S_k(\tau) \qquad (9)$$

4 实验仿真

4.1 实验环境

测试环境为本实验室的百兆局域网，拓扑结构如图 1 所示，评估 VLAN_1，主机的 IP 范围为 10.1.113.100~10.1.113.115，其中 10.1.113.101 为数据库服务器，10.1.113.107 为 mail 服务器，10.1.113.110 为 WWW 服务器，10.1.113.111 为 FTP 服务器，其余均为普通主机。攻击模拟机不定期发起扫描攻击、缓冲区溢出攻击及 Syn flooding 攻击。

4.2 实验结果

令 τ=1 min，则 2006 年 12 月 5 日 9:00–10:00 的扫描类攻击安全态势评估情况如图 3 所示，整体安全态势评估结果如图 4 所示。

图 3 表明，局域网分别在 9:17–9:19 之间，9:32 和 10:00 受到不同程度的扫描类攻击。查阅原始报警发现，共有 10 台机器在不同时间点分别受到 SCAN–SYN FIN 攻击，形成了图 3 所示态势。图 4 则是各类攻击和威胁态势的综合，既表现出一定的波动性，又表现出一定的连续性。

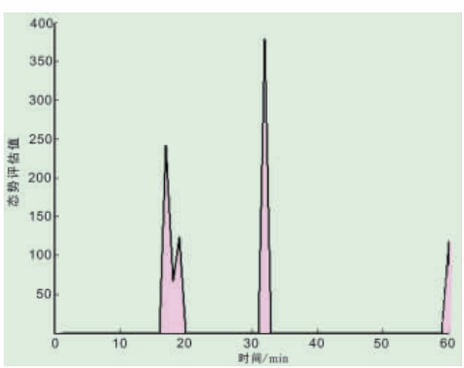

图 3 扫描类攻击评估结果

Fig. 3 Assessment result of scan attack

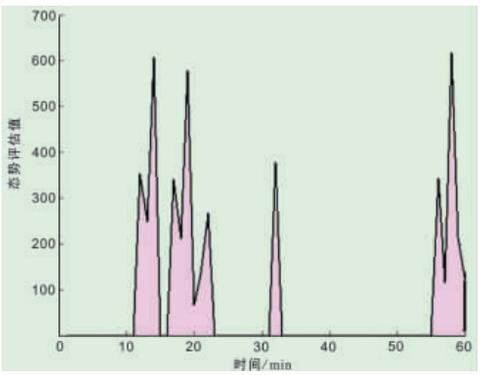

图 4 整体态势评估结果

Fig. 4 Assessment result of LAN

5 结论

本文探讨了攻防对抗环境下的网络安全态势评估，构建了基于攻击分类的网络安全态势评估算法，并得出以下结论。

1）在攻防对抗环境下评估网络安全态势，评估结果更为可信。

2）基于攻击分类评估态势，使安全管理员视野更为集中，对威胁程度的把握更为准确。

参考文献(References)

[1] HARIRI S, QU G Z, DHARMAGADDA T, *et al*. Impact analysis of faults and attacks in large-scale networks[J]. IEEE Sec Priv, 2003, 1(5): 49–54.

[2] BASS T. Intrusion systems and multisensor data fusion: cyberspace situational awareness [J]. Comm ACM, 2000, 43(4): 99–105.

[3] 冯登国，张阳，张玉清. 信息安全风险评估综述[J]. 通信学报, 2004, 25(7): 10–18.
FENG Dengguo, ZHANG Yang, ZHANG Yuqing. Survey of information security risk assessment[J]. J Comm, 2004, 25(7):10–18.

[4] 肖道举，杨素娟，周开峰，等. 网络安全评估模型研究[J]. 华中科技大学学报(自然科学版), 2002, 30(4): 37–39.
XIAO Daoju, YANG Sujuan, ZHOU Kaifeng, *et al*. A study of evaluation model for network security [J]. J Huazhong Univ Sci Tech (Nat Sci ed), 2002, 30(4): 37–39.

[5] 陈秀真，郑庆华，管晓宏，等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4): 885–897.
CHEN Xiaozhen, ZHENG Qinghua, GUAN Xiaohong, *et al*. Quantitative hierarchical threat evaluation model for network security[J]. J Software, 2006, 17(4): 885–897.

(责任编辑 朱宇)