文章编号:1007-5321(2015)01-0082-05　　DOI:10.13190/j.jbupt.2015.01.016

一种基于目标攻击图的态势威胁评估方法

刘威歆[1]，郑康锋[1]，胡　影[2]，武　斌[1]
(1. 北京邮电大学 信息安全中心，北京 100876；2. 武警北京指挥学院，北京 100012)

摘要：针对传统安全威胁评估方法难以理解攻击渗透的相关性，且难以量化相关渗透对于网络环境的影响问题，结合攻击图渗透动作危害性、渗透相关性和主机业务重要性，提出双向威胁评估模型和计算方法，能衡量攻击的深入程度和对目标的威胁程度，最后提出了一个能应用于实时告警分析的攻击序列评估方法，并通过实验验证了所提模型的合理性和有效性.

关　键　词：威胁评估；攻击图；双向威胁评估
中图分类号：TN911.22　　**文献标志码**：A

Approach of Goal-Oriented Attack Graph-Based Threat Evaluation for Network Security

LIU Wei-xin[1]，ZHENG Kang-feng[1]，HU Ying[2]，WU Bin[1]
(1. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Armed Police Beijing Command Academy, Beijing 100012, China)

Abstract: For being not falling in as final targets of attackers, the critical resources in network environments should be protected. It is vital to quantify the threat and impact during the process of multi-stage attacks. Aiming at combine threat quantification of individual attack action and significance value of hosts, as well as large amount of attack dependencies in attack graphs, a methodology for threat evaluation was proposed. The bi-directional threat evaluation presented in this article is able to compute progress attackers already, as well as the threat to goal-resources in attack graph, which can be well applied to real-time attack threat evaluation. The proposed was finally verified in experiment and simulation.

Key words: threat situation; attack graph; bi-directional threat evaluation

目前，安全威胁的研究工作主要是基于多种安全属性的代数叠加计算和基于攻击类型相关性的综合评估. 陈秀真等[1]提出了一个层次化网络安全威胁态势定量评估模型，能直观地给出整个网络系统、主机和服务 3 个层次的安全威胁态势. 刘效武等[2]利用粒子群算法实现 D-S(dempster/shafer)证据融合中的权值寻优，结合对威胁因子和威胁等级函数关系的推演，提出了面向攻击轨迹的层次化态势评估方法. 但以上研究忽略了目标网络中主机和漏洞的相关性和逻辑关系，难以对网络的威胁状态和攻击路径进行预判，而攻击图能在这方面起到很好的补充作用.

目前攻击图的研究集中于整体网络的安全性评估，Pengsu 等[3]提出了一种融合了依赖关系的通用漏洞评分系统(CVSS, common vulnerability scoring system)基础分数的聚合方法，能够评估整体网络的

收稿日期：2014-04-01
基金项目：国家自然科学基金青年科学基金项目(61101108)
作者简介：刘威歆(1987—)，男，博士生，E-mail：jack18jack@gmail.com；郑康锋(1975—)，男，副教授，博士生导师.

安全性. Keramati 等[4]使用路径上的 CVSS 分数的平均值和路径长度的比值来计算攻击发生的可达性. 笔者提出的双向威胁评估模型和计算方法，解决了攻击图中的渗透动作相关性带来的评估难题，能应用于实时的态势威胁评估.

1　攻击图定义

根据常用的攻击图定义和攻击场景分析，可定义攻击图为

$$G=\{S,A,O,E\}$$

1）S 为资源状态节点集合

$S=\{s_i(p,v,h)\mid i\in(1,N),v\in(0,10)\}$ 为资源状态节点集合. 其中，p 为状态节点的状态属性信息；v 为节点的威胁价值，$v=\mathrm{TVL}(s)$，$v\in(0,10)$；h 为状态节点所在的主机. S_{init} 代表的是初始节点.

2）A 为动作节点集合

$A=\{a_i(r,l)\mid i\in(1,M)\}$. 其中，$r$ 为该动作节点所表示的漏洞利用信息，包括源和目标主机以及相应的公共漏洞和暴露 CVE 编号；v 为该动作节点的威胁价值，$v\in(0,10)$；$l=\mathrm{VL}(a_i)$.

3）O 为目标节点集合

$O=\{o_i\mid O_i\in S\}$，O 为一系列需要针对分析的状态节点.

4）E 为边集合

$E=\{e_i\mid e_i\in((A\times S)\cup(S\times A))\}$，$E_{\mathrm{f}}$ 为攻击图资源状态节点和动作节点间的前向指针，$E_{\mathrm{b}}=E_{\mathrm{f}}^{-1}$ 为后向指针，表示节点间的逆向关系. 其中，状态节点到动作节点的前向指针存在 AND、OR 和直接推理的逻辑关系；动作节点到状态节点的指针不存在逻辑关系，都是直接推理.

2　基于攻击图双向威胁评估方法

2.1　单节点威胁值计算

对于攻击图中的动作节点，采用 CVSS 评价系统中的当前度量标准 temporal metrics 作为评分参考，该评分能定量地描述攻击者利用该漏洞后造成的影响程度和难易程度.

动作节点 a 的威胁值：

$$\mathrm{TVL}(a)=\mathrm{Temporal\ Score}(r_a)$$

对于攻击图中的状态节点，都会有 1 个与主机威胁相关的价值衡量 Score，和 CVSS 的 Temporal Score 一样，可以设置为 0 ~ 10 区间的分数.

状态节点 s 的威胁值：

$$\mathrm{TVL}(s)=\mathrm{Average}(\mathrm{Score}(h_{\mathrm{src}}),\mathrm{Score}(h_{\mathrm{dst}}))$$

其中：h_{src} 为源主机，h_{dst} 为目标主机.

2.2　双向威胁距离计算

双向威胁距离包括初始威胁距离，即与初始节点的逻辑距离；目标威胁距离，即与目标节点之间的逻辑距离. 这两个逻辑距离就能定量地判断该节点的攻击深入程度和对目标的潜在威胁程度，进而判断网络态势.

2.2.1　逻辑距离的计算

在初始威胁距离的计算中，给定目标攻击 $G_A=(S,A,O,E)$. 在初始威胁距离的计算中，$Q_{\mathrm{and}}(v)$ 表示节点 v 的前序节点所经过的前件关系为 AND 的节点所组成的队列，$\mathrm{times}(k,Q_{\mathrm{and}}(v))$ 表示节点 k 在 $Q_{\mathrm{and}}(v)$ 出现的次数，$\mathrm{dtimes}(k,Q_{\mathrm{and}}(v))$ 表示节点 k 在 $Q_{\mathrm{and}}(v)$ 被处理过的次数，$\mathrm{RD}_{\mathrm{in}}(Q_{\mathrm{and}}(v))$ 和 $\mathrm{RD}_{\mathrm{gl}}(Q_{\mathrm{and}}(v))$ 分别表示初始威胁距离和目标威胁距离中需要处理的重复加权路径.

重复加权距离 $\mathrm{RD}(Q_{\mathrm{and}}(v))$ 的计算如下：

1）遍历 $Q_{\mathrm{and}}(v)$，找出所有 $\mathrm{times}(k,Q_{\mathrm{and}}(v))-\mathrm{dtimes}(k,Q_{\mathrm{and}}(v))>1$ 的节点 k；

2）对于第 1）步中的节点 k，$\mathrm{dtimes}(k,Q_{\mathrm{and}}(v))=\mathrm{times}(k,Q_{\mathrm{and}}(v))-\mathrm{dtimes}(k,Q_{\mathrm{and}}(v))-1$；

3）最后，计算重复加权路径 $\mathrm{RD}(Q_{\mathrm{and}}(v),W)=\sum_k(\mathrm{times}(k,Q_{\mathrm{and}}(v))-\mathrm{dtimes}(k,Q_{\mathrm{and}}(v))-1)\times W(k)$，$\mathrm{times}(k,Q_{\mathrm{and}}(v))-\mathrm{dtimes}(k,Q_{\mathrm{and}}(v))>1$. W 为单点重复值.

初始威胁距离：

1）当与前件关系为 AND 时，有

$$\mathrm{IND}(v)=\mathrm{TVL}(v)-\mathrm{RD}_{\mathrm{in}}(Q_{\mathrm{and}}(v))+\sum\mathrm{IND}(\mathrm{Pre}(v))$$

2）当与前件关系为 OR 时，有

$$\mathrm{IND}(v)=\mathrm{TVL}(v)+\mathrm{MIN}(\mathrm{IND}(\mathrm{Pre}(v)))$$

3）初始威胁距离中的重复路径为

$$\mathrm{RD}_{\mathrm{in}}(Q_{\mathrm{and}}(v))=\mathrm{RD}(Q_{\mathrm{and}}(v,W)),W(k)=\mathrm{IND}(k)$$

目标威胁距离：若 $\exists\,\mathrm{times}(k,Q_{\mathrm{and}}(v))>1$，$\mathrm{GLD}(v)=-\mathrm{RD}_{\mathrm{gl}}(Q_{\mathrm{and}}(v))+\sum\mathrm{GLD}(\mathrm{Post}(v))$；否则，$\mathrm{GLD}(v)=\mathrm{TVL}(\mathrm{Post}(v))+\mathrm{MIN}(\mathrm{GLD}(\mathrm{Post}(v)))$. 目标威胁距离中的重复路径 $\mathrm{RD}_{\mathrm{gl}}(Q_{\mathrm{and}}(v))=\mathrm{RD}(Q_{\mathrm{and}}(v,W))$，$W(k)=\mathrm{GLD}(k)+\mathrm{TVL}(k)$.

在目标威胁距离的计算中，衡量的是每个节点到目标节点的逻辑距离，$Q_{\mathrm{and}}(v)$ 表示节点 v 的后序节点所经过的前件关系为 AND 的节点. 若 times

$(k, Q_{and}(v)) - dtimes(k, Q_{and}(v)) > 1$，说明后件序列含有未处理的重复路径. $RD_{gl}(Q_{and}(v))$表示目标威胁距离中需要处理的重复加权路径.

2.2.2 算法复杂度分析

若攻击图中的状态节点数量为 s，动作节点的数量为 a，有向边的数量为 e，AND 节点的最大 Q_{and} 队列的长度为 c，所有节点的最大前件数量是 P. 由于 Q_{and} 的长度是随着搜索的深入依次增长的，所以根据平均情况，逻辑距离计算的时间复杂度为 $O\left(\frac{(a+s)c}{2}+e\right)$. 在大规模网络产生的攻击图中，前件关系为 AND 的节点的数量 V_{and} 是小于状态节点和动作节点的数量的，而 Q_{and} 队列的长度也必定小于 V_{and}，即 $l < V_{and} < \min(s, a)$. 所以提出的算法是较有效率的，但是比在不涉及循环路径时，叶等[7]的 $O(s+a+e)$ 和陈锋[8]的 $O(P(s+a))$ 差，这是由于需要进行 Q_{and} 间的比对，Q_{and} 的长度会在一定程度上影响算法的运行时间.

2.3 攻击序列威胁评估

在基于攻击图的告警关联中，攻击告警首先会根据告警的漏洞属性和目标 IP 网络地址映射到相应的攻击图节点上[5-6]，形成告警序列后就可以做威胁评估.

检测完成度(PM，process metric)表示作为告警输入的 IDS 对目标网络的检测的完整情况. 威胁度(TM，threat metric)表示现有攻击序列对于目标节点的威胁情况. x_{eq} 代表攻击序列.

$$PM(x_{eq}) = [MAX(IND(v)) - MIN(IND(v))]/[MAX(IND(v)) + MIN(GLD(v))], v \in x_{eq}$$

$$TM(x_{eq}) = MAX(IND(v))/[MAX(IND(v)) + MIN(GLD(v))], v \in x_{eq}$$

3 实验分析

以图 1 中的真实网络和 3 个规模不同、复杂性也不同的网络为例，验证所提方法的合理性和有效性. 实验环境是 Intel i5-2430M@2.40 GHz 处理器、2 GB 内存、Windows 7，算法在 Microsoft Visual Studio 用 C#实现. Host0 是运行在 Windows NT4.0 上的 IIS Web Server，Host1 的系统平台是 Windows 2000 sp2，上面运行了 FTP 和 SSH 服务；Host2 的系统是 Windows XP，上面运行了 Netbios-ssn 服务；Host3 是 Redhat Linux 7.0 系统，上面运行的服务有 LICQ、Squid、Mysql Database. Host3 是作为攻击者的目标主机，其上的 Mysql 数据库中的数据是重要资源，也是攻击者的目标.

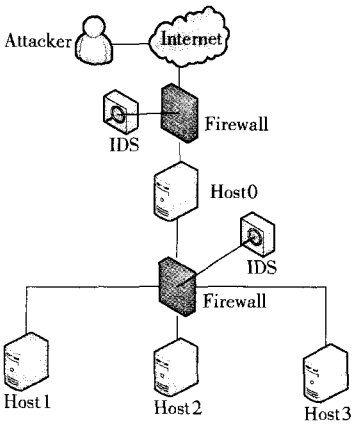

图 1 实验环境

使用 Nessus 对图 1 中的 4 台主机进行漏洞扫描，能得到各主机上的脆弱性信息，根据其 CVE 编号查询美国国家数据库即可得出表 1 中主机漏洞的得分情况. 结合表 2 和表 3 中的防火墙规则、主机连通性情况和主机漏洞情况，可以构建出图 2 所示的攻击图；同时，根据相应的漏洞评分和主机评分表，可以得出每个动作节点和状态节点的威胁值，最后利用 2.2 节中的双向威胁计算方法即可得出每个节点的初始威胁距离和目标威胁距离，均标记在图 2 中节点旁的括号中. 从表 4 中可以看出，随着攻击路径的增长，威胁度持续上升.

为了测试提出的算法，建立了 3 个不同复杂度和规模的网络模型，测试的结果如表 5 所示. 从测试结果可以看出，随着目标网络中的主机的增长，产生的攻击图中的节点数目和有向边的数目也在急剧上升，同时从算法的运行时间可以看出，提出的算法由于需要重复比对 AND 关系的节点队列，在算法性能上略差于叶等[7]的算法和陈[8]的算法.

表 1 主机评分表

主机	H0	H1	H2	H3
分数	5	8	8	10

表 2 防火墙规则表

Host	Att	H0	H1	H2	H3
Att	localhost	IIS	None	None	None
H0	All	localhost	ssh	All	Squid LICQ
H1	All	IIS	localhost	None	Squid LICQ
H2	All	IIS	ftp	localhost	Squid LICQ
H3	All	IIS	ssh	All	localhost

表 3　主机漏洞分布表

Host	Services	CVEIDs	TS
H0	IIS,Web,Service	CVE-2002-0364	5.872 5
H1	ftp	CVE-2008-1396	3.472 3
	ssh	CVE-1999-1455	6.375 0
	rsh	CVE-1999-0180	7.500 0
H2	Netbios-ssn	CVE-2003-0661	4.286 8
	rsh	CVE-1999-0180	7.500 0
H3	LICQ	CVE-2001-0439	7.125 0
	Squid Proxy	CVE-2001-1030	5.888 9
	Mysql DB	CVE-2006-3368	4.750 0

表 4　攻击路径和威胁度计算

攻击路径	TM
IIS_BOF(0,0)	0.32
IIS_BOF(0,0)→netbios_ssn_nullsession(0,2)	0.47
IIS_BOF(0,0)→netbios_ssn_nullsession(0,2)→ftp_rhost(2,1)	0.56
IIS_BOF(0,0)→netbios_ssn_nullsession(0,2)→ftp_rhost(2,1)→rsh_login(2,1)	0.62
IIS_BOF(0,0)→netbios_ssn_nullsession(0,2)→ftp_rhost(2,1)→rsh_login(2,1)→squid_port_scan(1,3)	0.73
IIS_BOF(0,0)→netbios_ssn_nullsession(0,2)→ftp_rhost(2,1)→rsh_login(2,1)→squid_port_scan(1,3)→LICQ-remote-to-user(1,3)	0.86
IIS_BOF(0,0)→netbios_ssn_nullsession(0,2)→ftp_rhost(2,1)→rsh_login(2,1)→squid_port_scan(1,3)→LICQ-remote-to-user(1,3)→local_setuid_bof(3,3)	1.00

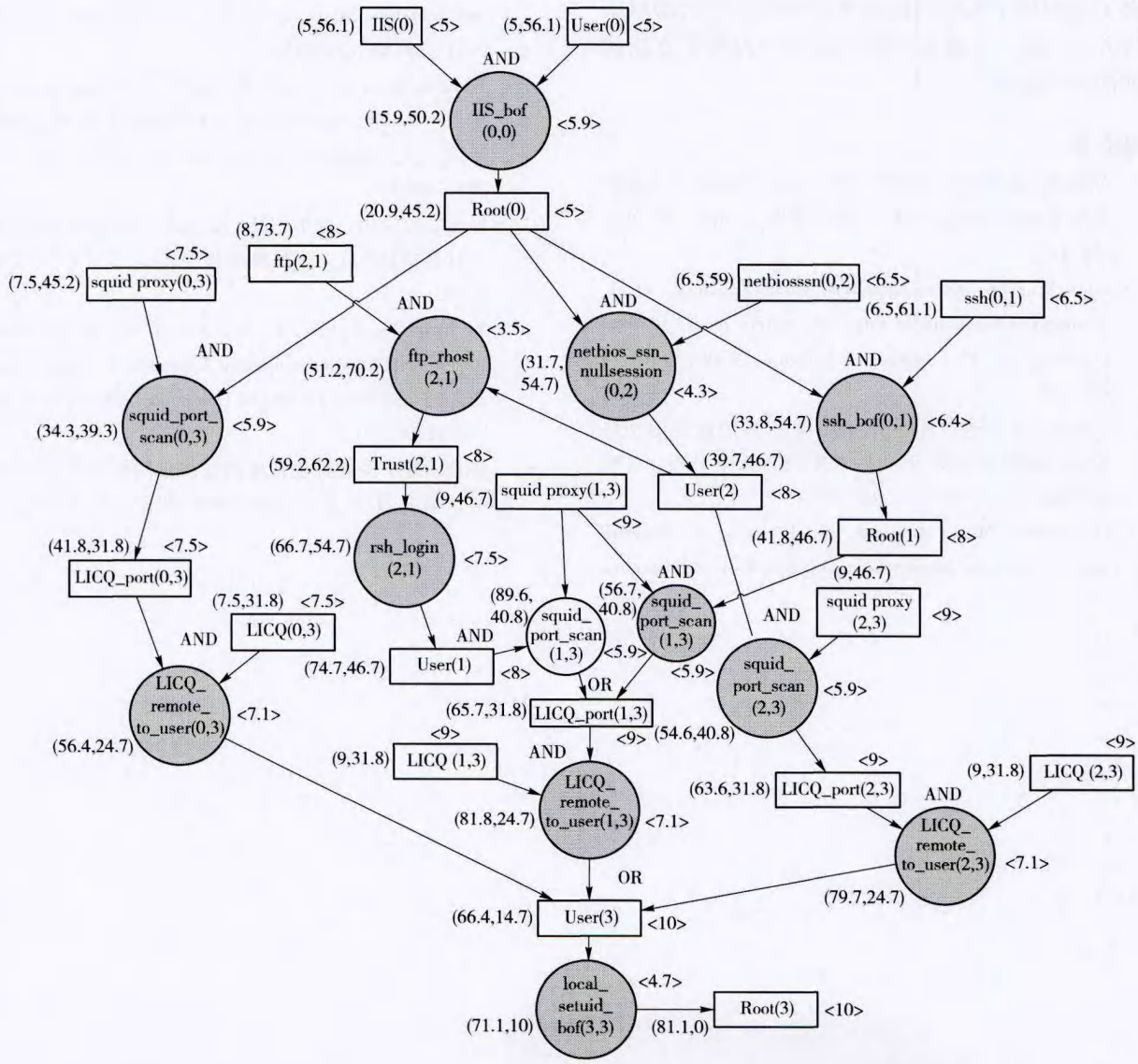

图 2　实验攻击图

表5 不同规模和复杂度的网络的算法运算结果对比

测试模型	主机数	状态节点数	动作节点数	AND节点数	初始距离计算/ms	目标距离计算/ms	叶等[7]的算法/ms	陈[8]的算法/ms
A	4	21	13	8	4	4	3	5
B	8	45	30	17	18	19	14	20
C	16	94	63	35	71	73	54	66

4 结束语

讨论了攻击图中的威胁评估问题,结合漏洞和状态之间的因果关系和逻辑关系,提出双向威胁距离计算的方法,能利用攻击图中的因果关联和与或条件关系,计算出初始威胁距离和目标威胁距离,并提出了能应用于实时网络检测中的攻击序列的威胁评估方法. 最后在真实环境的实验中表明了方法的合理性和有效性.

参考文献:

[1] 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 Xiuzhen, Zheng Qinghua, Guan Xiaohong, et al. Quantitative hierarchical threat evaluation model for network security[J]. Journal of Software, 2006, 17(4): 885-897.

[2] 刘效武, 王慧强, 禹继国, 等. 基于多源融合的网络安全态势感知模型[J]. 解放军理工大学学报: 自然科学版, 2012, 13(4): 403-407.
Liu Xiaowu, Wang Huiqiang, Yu Jiguo, et al. Network security situation awareness model based on multi-source fusion[J]. Journal of PLA University of Science and Technology(Natural Science Edition), 2012, 13(4): 403-407.

[3] Cheng Pengsu, Wang Lingyu, Jajodia S, et al. Aggregating CVSS base scores for semantics-rich network security metrics[C]// Reliable Distributed Systems (SRDS), 2012 IEEE 31st Symposium on. Irvine, CA: IEEE, 2012: 31-40.

[4] Keramati M, Akbari A, Keramati M. CVSS-based security metrics for quantitative analysis of attack graphs[C]// Computer and Knowledge Engineering (ICCKE), 2013 3th International Conference on. Mashhad: IEEE, 2013: 178-183.

[5] Ahmadinejad S H, Jalili S, Abadi M. A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs[J]. Computer Networks, 2011, 55(9): 2221-2240.

[6] Wang Lingyu, Liu Anyi, Jajodia S. Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts[J]. Computer Communications, 2006, 29(15): 2917-2933.

[7] 叶云, 徐锡山, 贾焰, 等. 基于攻击图的网络安全概率计算方法[J]. 计算机学报, 2010, 33(10): 1987-1996.
Ye Yun, Xu Xishan, Jia Yan, et al. An Attack Graph-Based Probabilistic Computing Approach of Network Security[J]. Chinese Journal of Computers, 2010, 33(10): 1987-1996.

[8] 陈锋. 基于多目标攻击图的层次化网络安全风险评估方法研究[D]. 长沙: 国防科学技术大学, 2009.