基于攻击树和 CVSS 的网络攻击效果评估方法*

潘　刚,米士超,郭荣华,黄丽刚,王金锁,李　凯
(光电对抗测试评估技术重点实验室,河南 洛阳 471003)

摘　要:为有效解决网络攻击效果评估中对指标数据的过度依赖性,提高网络攻击效果评估的准确性,提出了一种基于攻击树和 CVSS 的网络攻击效果评估方法。首先,采用攻击树模型描述系统可能存在的攻击路径,并利用模糊层次分析法对各叶节点的发生概率进行求解;然后,基于 CVSS 漏洞信息建立网络攻击效果量化评估模型;最后,采用实例进行验证分析说明。该方法能够充分利用已有的攻击行为研究成果,评估结果较为客观,且思路清晰,算法简单,具有较强的通用性和工程应用价值。

关键词:攻击树;模糊层次分析法;CVSS 漏洞;网络攻击;效果评估
中图分类号:TP309.2　　**文献标识码**:A　　DOI:10.16157/j.issn.0258-7998.200192

中文引用格式:潘刚,米士超,郭荣华,等. 基于攻击树和 CVSS 的网络攻击效果评估方法[J].电子技术应用,2022,48(4):76-80.
英文引用格式:Pan Gang,Mi Shichao,Guo Ronghua,et al. Evaluation method of network attack effect based on attack tree and CVSS[J]. Application of Electronic Technique,2022,48(4):76-80.

Evaluation method of network attack effect based on attack tree and CVSS

Pan Gang,Mi Shichao,Guo Ronghua,Huang Ligang,Wang Jinsuo,Li Kai
(Key Laboratory of Optoelectronic Countermeasures Measurement and Evaluation Technology,Luoyang 471003,China)

Abstract: In order to solve the over-dependence on index data in network attack effect evaluation and improve the accuracy of network attack effect evaluation, this paper proposed a network attack effect evaluation method based on attack tree and CVSS. Firstly, The attack tree model is used to describe the possible attack paths of the system, and the probability of each leaf node is solved by fuzzy analytic hierarchy process. Then, based on CVSS vulnerability information, a quantitative evaluation model of network attack effect was established. Finally, an example is used for verification analysis. This method can make full use of the existing research results of aggressive behavior, the evaluation results are objective, the thinking is clear, the algorithm is simple, and it has strong universality and engineering application value.

Key words: attack tree; fuzzy analytic hierarchy process; CVSS vulnerability; network attack; effectiveness evaluation

0 引言

网络攻击效果评估就是对处于复杂网络环境下系统的安全性给出定性或定量的评价,并提出针对性的防护建议,促进系统安全性和可靠性的提升。当前研究成果主要通过攻击效果指标量化和相关评估算法构建来开展网络攻击效果评估研究,具体表现为:(1)基于层次分析法的网络攻击效果评估方法[1-2],该方法可通过定性和定量相结合的决策方法实现对复杂目标评估的系统性分析方法,且所需的定量数据信息较少。但分析过程过多依赖于专家的经验,评估结果主观性较强,当指标过多时,数据统计量较大,致使权重难以确定。(2)基于模糊综合评判的网络攻击效果评估方法[3-6],该方法的不足在于模糊综合评价过程本身并不能解决评价指标间相关造成的评价信息重复问题,此外,对各被评价对象的指标信息量考虑不全,有可能影响评价结果的区分度。(3)基于模糊层次分析法的网络攻击效果评估方法[7-8],该方法是对层次分析法的一种改进,可以量化不确定性因素,能够一定程度上弥补层次分析法存在的不足,但是比较适合于定性评估分析。(4)基于粗糙集理论的网络攻击效果评估方法[9-11],该方法的不足之处在于评估选取的样本数据必须具有一定代表性,否则随着样本量的增加,评估结果的偏差可能较大。(5)基于灰色理论的网络攻击效果评估方法[10,12-13],该方法在处理评估数据少、信息不完备等问题上具有一定优势,但是存在聚类系数差异不显著时,无法对评估对象进行准确评估的问题。

基于上述文献可知,对基于指标量化的网络攻击效果评估方法主要存在以下方面不足:(1)对指标体系的

* 基金项目:国家自然科学基金项目(61372039)

建立通常会存在一些主观因素的影响；(2)对于一些攻击效果数据很难直接测量的情况则难以适用。为此，文献[14]提出了一种基于攻击树的无线局域网攻击效果评估方法。受该文献研究成果的启发，本文首先根据系统特征采用 FAHP 计算各叶节点的属性权值，通过定量分析的方法确定叶节点的发生概率，而后基于 CVSS 漏洞信息和模糊层次分析法，提出了一种新的攻击效果量化评估模型，并以某典型工控系统进行实例验证，可为后续安全防护策略的制定提供技术支撑。

1 攻击树模型

攻击树是多层树型结构，树的根节点表示攻击者的最终攻击目标；叶节点表示具体的攻击事件，即攻击者有可能采取的各种攻击手段；子节点表示要达到最终目标所必须完成的一些中间步骤[15-16]。节点之间的关系包括(与)AND、或(OR)和顺序与(Sequence AND，SAND)3 种[17]。

基于攻击树和 CVSS 的网络攻击效果量化评估的主要思路如图 1 所示。

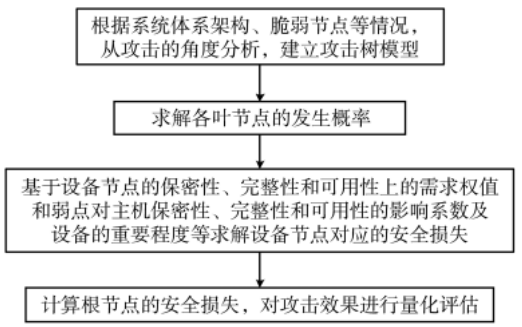

图 1 基于攻击树和 CVSS 的网络攻击效果量化评估思路

2 基于 FAHP 的叶节点发生概率求解

2.1 叶节点的指标量化

本文从攻击者角度出发，建立攻击分析模型，通过属性的概念给每个叶节点赋予攻击成本、攻击难度和被发现的可能性 3 个安全属性，并采用多属性效用理论，将上述属性转换为实现目标的效用值。计算叶节点发生概率的公式为[18]：

$$P\_E_i=W_{\text{cost}}\times U_{\text{cost\_}E_i}+W_{\text{diff}}\times U_{\text{diff\_}E_i}+W_{\text{det}}\times U_{\text{det\_}E_i} \tag{1}$$

其中，E_i 表示第 i 个叶节点，即攻击事件；$U_{\text{cost\_}E_i}$、$U_{\text{diff\_}E_i}$、$U_{\text{det\_}E_i}$ 分别表示攻击成本、难度及被发现可能性的效用值；$\text{cost\_}E_i$、$\text{diff\_}E_i$、$\text{det\_}E_i$ 分别表示实现该叶节点所代表事件的攻击成本、难易程度及被发现的可能性；W_{cost}、W_{diff}、W_{det} 分别表示攻击成本参数、难度参数及被发现可能性参数的权重，且三者之和为 1。在实际应用中，叶子节点的属性值通常通过专家评估的方法给出，其中攻击成本由专家大概给出具体值，而攻击难度和被发现的可能性由专家作出判断。在对叶节点的指标量化过程存在诸多主观因素的影响，为尽可能降低各主观因素的影响，本文引用文献[19]中方法对有关叶节点的指标进行量化。

2.2 叶节点发生概率求解

模糊层次分析法是将模糊数学与层次分析法相结合，充分考虑人思考的模糊性的一种理论方法[20]，是一种典型的主观权值确定方法。为此，本文采用模糊层次分析法对主观权值进行求解。通过两两比较各属性对攻击事件发生概率的影响程度，确定攻击难度、攻击被发现的可能性和攻击成本的权重。

根据文献[8]有关模糊层次分析法的效果评估方法，通过两两比较攻击难度、攻击被发现的可能性和攻击成本对攻击事件发生概率的影响程度，得到以下判断矩阵 $\boldsymbol{\Omega}_{\text{leaf}}$：

$$\boldsymbol{\Omega}_{\text{leaf}}=\begin{bmatrix}0.5 & 0.6 & 0.7\\ 0.4 & 0.5 & 0.6\\ 0.3 & 0.4 & 0.5\end{bmatrix} \tag{2}$$

并求得 $U_{\text{diff\_}E_i}=0.383\ 4$，$U_{\text{det\_}E_i}=0.333\ 3$，$U_{\text{cost\_}E_i}=0.283\ 3$；将上述参数代入式(1)即可求得叶节点的发生概率。

3 攻击序列的安全损失求解

3.1 设备节点的安全损失算法

假定叶节点 $E_{i,l}$ 对应设备节点 $\textbf{Host}_i$ 的第 l 个漏洞的攻击事件，其中，$\textbf{Host}_i$ 用三元组 $(\text{type}_i,\text{imp}_i,\vec{A}_i)i=1,2,\cdots,n$ 表示。其中，type_i 为设备类型，工控系统的设备类型包括交换机、工程师站、操作员站、PLC、服务器及现场设备等；imp_i 为设备的重要程度；$\vec{A}_i=(a_{i,s},a_{i,I},a_{i,A})$ 表示设备的保密性、完整性和可用性上的需求权值，可通过模糊层次分析法进行具体求解。表 1 给出了控制系统网络环境中各设备类型重要度的量化标准。

表 1 控制系统各设备重要度量化标准

等级	设备类型	重要度
L1	交换机	5
L2	重要服务器 PLC 工程师站 无线 AP	4
L3	操作员站	3
L4	一般服务器	2
L5	办公主机或终端	1

实现叶节点 $E_{i,l}$ 对应所需利用的弱点信息为 $\textbf{Vul}_{i,l}$，其中，$\textbf{Vul}_{i,l}$ 用三元组 $(\text{Vid}_{i,l},v\_\text{type}_{i,l},\vec{w}_{i,l})$ 表示，$\text{Vid}_{i,l}$ 为第 i 个设备的第 l 个弱点在 CVE 漏洞库中的编号 $(i=1,2,\cdots,n;l=1,2,\cdots,L)$；$v\_\text{type}_{i,l}$ 为第 i 个设备的第 l 个弱点的类型；$\vec{w}_{i,l}=(w_{i,l,s},w_{i,l,I},w_{i,l,A})$ 表示第 i 个设备的第 l 个弱点对主机保密性、完整性和可用性的影响系数，可通过 CVSS 查询赋值。

第 i 个设备的第 l 个弱点对应叶节点 $E_{i,l}$ 发生后对

应的安全损失 Lost_$E_{i,l}$。依据叶节点 $E_{i,l}$ 发生对相应设备节点 Host_i 的重要度及安全需求计算安全损失Lost_$E_{i,l}$。

$$\text{Lost\_}E_{i,l}=\text{imp}_i\cdot P\_E_{i,l}\cdot(\vec{A}_{i,l}\cdot\vec{w}'_{i,l}) \tag{3}$$

其中，$P\_E_{i,l}$ 表示叶节点 $E_{i,l}$ 的发生概率，imp_i 表示设备节点 Host_i 的重要度，$\vec{A}_{i,l}$ 表示设备的保密性、完整性和可用性上的需求权值，$\vec{w}_{i,l}$ 表示第 i 个设备的第 l 个弱点对设备节点 Host_i 保密性、完整性和可用性的影响系数。

如果利用同一设备节点的多个($l=1,2,\cdots,L$)漏洞进行攻击，则该设备节点的产生的损失为：

$$\text{Lost\_}H_i=\text{imp}_i\cdot\prod_{l=1}^{L}P_{i,l}\cdot(\vec{A}_{i,l}\cdot\vec{w}'_{i,l}) \tag{4}$$

3.2 攻击效果量化评估算法

不失一般性，假定攻击序列 $S_j=\{E_{1,l},\cdots,E_{i,l},\cdots,E_{m,l}\}$，$j=\{1,2,\cdots,J\}$，$i\in\{1,2,\cdots,m\}$，$m\in\{1,2,\cdots,n\}$，$l=1,2,\cdots,L$。

$$\text{AssResult\_}S_j=\prod_{i\in\{1,2,\cdots,m\}}\text{Lost\_}H_i \tag{5}$$

4 实例分析

为便于对比验证分析本文方法的有效性，采用文献[21]中实例进行分析说明，系统架构如图 2 所示。为对目标系统的攻击效果进行分析，在分析了系统的脆弱性和攻击面的基础上，给出如图 3 所示攻击树模型，其中各节点含义在文献[21]已详细说明，本文不再赘述，各设备与弱点漏洞对应关系及各设备的重要度对应关系如表 2、表 3 所示。

根据文献[19]中属性评分标准对该攻击树中各个叶节点的安全属性值进行打分，同时采用本文给出的叶节点发生概率求解方法可得各叶节点的安全属性得分及发生概率，具体如表 4 所示。

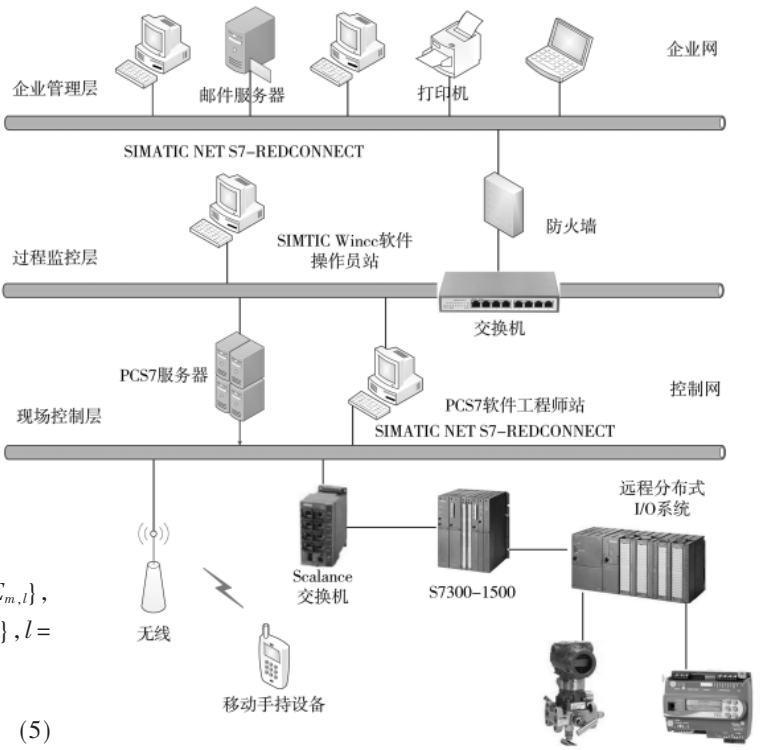

图 2 某工控系统架构

表 4 中各叶节点的得分为得分区间值的中值，X 的取值为评分等级最大值时，$\overline{X}=X$，其他情况 $\overline{X}=X_{\text{mid}}+\alpha X_{\text{mid}}$，$\underline{X}=X_{\text{mid}}-\alpha X_{\text{mid}}$，不失一般性，取置信水平 $\alpha=0.05$。

通过模糊层次分析法对表 3 中各设备的保密性、完整性和可用性上的需求权值进行求解，具体步骤如下：

(1)首先确定各设备在保密性、完整性和可用性上的判断矩阵 $\boldsymbol{\Omega}$：

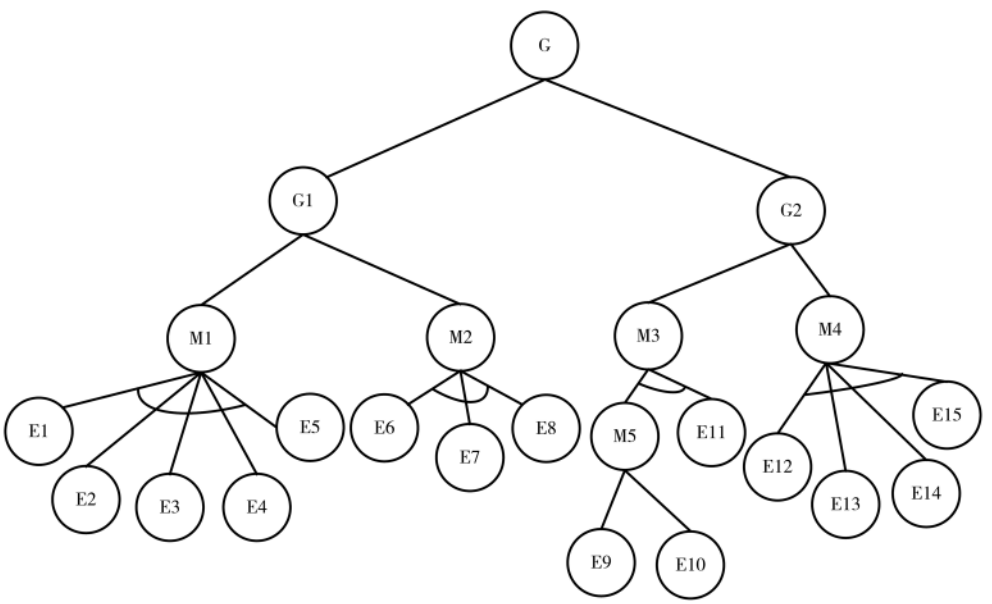

图 3 某工控系统攻击树建模

表 2 各设备与弱点漏洞对应关系

节点符号	漏洞(CVSS 评价字符串)	设备名称
E1	CVE-2011-3190 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	邮件服务器
E2	CVE-2008-4932 (AV:N/AC:L/Au:S/C:C/I:C/A:C)	办公主机
E3	CVE-2015-2509 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	办公主机
E4	CVE-2014-8552 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	操作员站
E5	CVE-2015-1358 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	操作员站
E6	CVE-2013-3958 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	PCS7 服务器
E7	CVE-2014-8551 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	PCS7 服务器
E8	CVE-2014-4686 (AV:N/AC:M/Au:N/C:P/I:P/A:P)	工程师站
E9	CVE-2008-5230 (AV:N/AC:M/Au:N/C:P/I:P/A:P)	无线 AP
E10	CVE-2012-3040 (AV:N/AC:M/Au:N/C:N/I:P/A:N)	工程师站
E11	CVE-2014-5410 (AV:N/AC:M/Au:N/C:N/I:N/A:C)	工程师站
E12	CVE-2010-2568 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	办公电脑
E13	CVE-2014-4682 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	工程师站
E14	CVE-2008-4250 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	工程师站
E15	CVE-2014-9209 (AV:L/AC:M/Au:N/C:C/I:C/A:C)	工程师站

表 3 各设备的重要度对应关系

序号	设备名称	重要度
1	邮件服务器	2
2	办公主机	1
3	PCS7 服务器	4
4	工程师站	4
5	操作员站	3
6	无线 AP	4

$$\boldsymbol{\Omega}\_\text{Mail\_server}=\begin{bmatrix}0.5 & 0.7 & 0.6\\ 0.3 & 0.5 & 0.4\\ 0.4 & 0.6 & 0.5\end{bmatrix} \tag{6}$$

$$\boldsymbol{\Omega}\_\text{Office\_host}=\begin{bmatrix}0.5 & 0.4 & 0.3\\ 0.6 & 0.5 & 0.4\\ 0.7 & 0.6 & 0.5\end{bmatrix} \tag{7}$$

$$\boldsymbol{\Omega}\_\text{PCS7\_server}=\begin{bmatrix}0.5 & 0.4 & 0.3\\ 0.6 & 0.5 & 0.4\\ 0.7 & 0.6 & 0.5\end{bmatrix} \tag{8}$$

表 4 各叶节点的安全属性得分及发生概率

叶节点	攻击成本	攻击难度	被发现可能性	发生概率
E1	1	2	1	0.836 1
E2	1	2	2	0.694 0
E3	1	1	2	0.861 2
E4	2	2	1	0.643 8
E5	1	2	3	0.646 6
E6	1	2	1	0.836 1
E7	1	2	1	0.836 1
E8	1	1	2	0.694 0
E9	2	2	1	0.811 0
E10	1	2	2	0.861 2
E11	2	2	2	0.694 0
E12	1	2	1	0.836 1
E13	1	2	1	0.836 1
E14	1	4	1	0.836 1
E15	3	2	3	0.646 6

$$\boldsymbol{\Omega}\_\text{Engineer\_station}=\begin{bmatrix}0.5 & 0.4 & 0.3\\ 0.6 & 0.5 & 0.4\\ 0.7 & 0.6 & 0.5\end{bmatrix} \tag{9}$$

$$\boldsymbol{\Omega}\_\text{Operator\_station}=\begin{bmatrix}0.5 & 0.4 & 0.3\\ 0.6 & 0.5 & 0.4\\ 0.7 & 0.6 & 0.5\end{bmatrix} \tag{10}$$

$$\boldsymbol{\Omega}\_\text{Wireless\_AP}=\begin{bmatrix}0.5 & 0.7 & 0.6\\ 0.3 & 0.5 & 0.4\\ 0.4 & 0.6 & 0.5\end{bmatrix} \tag{11}$$

(2)根据模糊层次分析属性权值求解方法，可以得到表 4 中各设备的保密性、完整性和可用性上的需求权值：

$$\overrightarrow{A}_{\text{\_Mail\_server}}=[0.383\ 3, 0.283\ 3, 0.333\ 3] \tag{12}$$

$$\overrightarrow{A}_{\text{\_Office\_host}}=[0.283\ 3, 0.333\ 3, 0.383\ 3] \tag{13}$$

$$\overrightarrow{A}_{\text{\_PCS7\_server}}=[0.283\ 3, 0.333\ 3, 0.383\ 3] \tag{14}$$

$$\overrightarrow{A}_{\text{\_Engineer\_station}}=[0.283\ 3, 0.333\ 3, 0.383\ 3] \tag{15}$$

$$\overrightarrow{A}_{\text{\_Operator\_station}}=[0.283\ 3, 0.333\ 3, 0.383\ 3] \tag{16}$$

$$\overrightarrow{A}_{\text{\_Wireless\_AP}}=[0.283\ 3, 0.333\ 3, 0.383\ 3] \tag{17}$$

(3)根据 CVSS 评价字符串可得各叶节点漏洞对设备节点保密性、完整性和可用性的影响系数，具体如表 5 所示。

根据式(3)、式(4)分别求出对应的叶节点安全损失和设备节点安全损失，最后根据式(5)求得各攻击序列对应的攻击效果量化评估结果，如表 6 所示。

对表 6 中各攻击序列的攻击效果评估结果分析可知，$S_3>S_4>S_2>S_1>S_5$，其中攻击效果较大的攻击方法是通过网络攻击目标系统中的控制器和上位机自动化集成系统，其中，S_3、S_4 为通过现场无线热点和 PLC 网络访问的方式开展攻击。为此，应针对上述攻击方式对系统进行有针对性的防护。此外，本文所得攻击效果评估结果与文献[21]对应的安全风险评估结果排序一致，进一步

表 5 各叶节点对应漏洞的保密性、完整性和可用性的影响系数

叶节点	保密性影响系数	完整性影响系数	可用性影响系数
E1	0.22	0.22	0.22
E2	0.56	0.56	0.56
E3	0.56	0.56	0.56
E4	0.22	0	0
E5	0.22	0	0
E6	0.22	0.22	0.22
E7	0.56	0.56	0.56
E8	0.22	0.22	0.22
E9	0.22	0.22	0.22
E10	0	0.22	0
E11	0	0	0.56
E12	0.56	0.56	0.56
E13	0.22	0	0
E14	0.56	0.56	0.56
E15	0.56	0.56	0.56

表 6 各攻击序列攻击效果评估结果

攻击序列 $S_j \in S$	步数	攻击效果
S_1={E1,E2,E3,E4,E5}	5	0.182 7
S_2={E6,E7,E8}	3	0.620 9
S_3={E9,E11}	2	0.961 5
S_4={E10,E11}	2	0.719 0
S_5={E12,E13,E14,E15}	4	0.178 7

验证本文所提方法的正确性和有效性。

5 结论

为了对网络攻击效果进行有效评估，明确系统存在的安全风险，本文提出了一种基于攻击树和 CVSS 的网络攻击效果评估方法。所提网络攻击效果评估方法有效解决了评估过程中对评估指标数据的依赖性；同时，本文给出了对网络攻击效果评估的方法步骤，对网络攻击的效果进行了准确有效评估，为制定相应的安全防护策略提供依据和指导，从而更好地应对不同的网络攻击威胁。

参考文献

[1] 汪生，孙乐昌.网络攻击效果评估系统的研究与实现—基于指标体系[J].计算机工程与应用，2005(34)：149-153.
[2] 刘进，王永杰，张义荣，等.层次分析法在网络攻击效果评估中的应用[J].计算机应用研究，2005(3)：113-115.
[3] 王永杰，鲜明，王国玉，等.计算机网络攻击效能评估研究[J].计算机工程与设计，2005，26(11)：2868-2901.
[4] 冯永新，赵运弢，苏广楠，等.一种 SOAP 泛洪攻击效能模糊评估方法[J].兵工学报，2015，36(11)：2203-2208.
[5] 陈娟，马涛.移动 Ad Hoc 网络 DoS 攻击效果评估方法[J].电光与控制，2012，19(3)：86-89.
[6] 王松.面向 WebService 的网络攻击效果评估技术的研究[D].沈阳：沈阳理工大学，2016.
[7] 李佳.一种基于模糊层次分析的智能手机攻击效果评估方法[C]//第十三届中国科协年会第 11 分会场-中国智慧城市论坛，天津，2011.
[8] 曾辰熙，吴泉源，李爱平，等.基于模糊层次分析的木马攻击效果评估技术研究[J].网络与信息安全学报，2016，2(7)：49-58.
[9] 王会梅，王永杰，张义荣，等.粗糙集理论在网络攻击效果评估中的应用研究[J].计算机应用研究，2007，24(6)：118-120.
[10] 彭子枚.网络攻击效能评估若干关键技术研究[D].长沙：国防科学技术大学，2011.
[11] 刘勇.针对 WLAN 攻击的效能评估技术研究[D].西安：西安电子科技大学，2017.
[12] 王会梅，江亮，鲜明，等.计算机网络攻击效果灰色评估模型和算法[J].通信学报，2009，30(11A)：17-22.
[13] 王燮，刘孙俊，唐毅谦，等.一种基于灰色层次分析法的网络攻击危害性评估指标量化方法[J].成都大学学报(自然科学版)，2012，31(1)：57-60.
[14] 贾薇.无线局域网攻击效果评估技术研究与实现[D].北京：北京邮电大学，2015.
[15] 何明亮，陈泽茂，龙小东.一种基于层次分析法的攻击树模型改进[J].计算机应用研究，2016，33(12)：3755-3758.
[16] 张恺伦，江全元.基于攻击树模型的 WAMS 通信系统脆弱性评估[J].电力系统保护与控制，2013，41(7)：116-122.
[17] 张春明，陈天平，张新源，等.基于攻击树的网络安全事件发生概率评估[J].火力与指挥控制，2010，35(11)：17-19.
[18] 黄慧萍，肖世德，孟祥印.基于攻击树的工业控制系统信息安全风险评估[J].计算机应用研究，2015，32(10)：3022-3025.
[19] 任秋洁，潘刚，白永强，等.基于 FAHP 和攻击树的信息系统安全风险评估[J].电子技术应用，2018，44(8)：113-117.
[20] CHANG Y D.Applications of the extent analysis method on fuzzy AHP[J].European Journal of Operational Research，1996，95(3)：649-655.
[21] 王作广，魏强，刘雯雯.基于攻击树与 CVSS 的工业控制系统风险量化评估[J].计算机应用研究，2016，33(12)：3785-3790.

(收稿日期：2020-03-16)

作者简介：
潘刚(1987-)，男，博士，工程师，主要研究方向：信息系统安全性测试及风险评估。

扫码下载电子文档

版权声明