基于改进攻击树理论的网络信息安全渗透测试技术研究

Abstract:当前网络信息安全渗透测试技术存在多样化和复杂性的特点，网络安全管理人员面对不同的测试场景时难以抉择正确渗透测试方式、制定安全应对措施。因此本文提出了一种基于改进的攻击应对措施树（attack countermeasure tree）的网络信息安全渗透测试模型。该模型通过攻击应对措施树计算对应的攻击概率，同时构建对应的网络信息安全渗透测试模型。此外，该模型在工程师工作站网络中构建了真实的攻击机和目标机，以开展渗透测试实验。其中以 Windows 漏洞执行 SQL 注入攻击具有最大的攻击效果，其评估结果为 0.9834。同时网络交换机保留接口访问、获取系统驱动程序和 USB 接口访问的攻击发生概率分别为 0.548、0.492 和 0.475。结果表明本文提出的模型能有效抉择渗透测试方式，并对网络安全提供有针对性的保护建议。

Keywords: 网络信息安全; 攻击树理论; 攻击应对措施树; 渗透测试; 攻击效果

1. Introduction

随着时代的发展，信息网络在给人们带来许多便利的同时许多信息网络安全威胁也随之而来。在整个信息技术产业中专业技术的飞速发展趋势使得攻击者的攻击方式日益复杂[1-4]。在网络威胁日益严峻的情况下，越来越多的公司选择将信息网络安全放在首要位置上。信息网络专家主动安装各种补丁和管理配置项，不断的监视系统防御项

并且确保已经安全地配置各种系统和应用[5-8]。但是网络威胁始终存在，并且无处不在：

2023 年 6 月 23 日，俄罗斯勒索软件组织 Clop 利用 MOVEit 文件传输软件的 0dayLoudon，对美国能源部在内的多个联邦机构的系统发动攻击；

2023 年 6 月 9 日，位于日本的国际制药巨头公司 Eisai 称相关攻击者加密了公司的部分服务器，并遭到了勒索软件攻击；

2023 年 5 月 24 日，德国汽车公司 Rheinmetall 披露，近期遭到了勒索软件团伙的攻击，窃取了莱茵金属等交易记录数据。

从上述情况可知，网络攻击被视为信息网络安全中的棘手问题。美国信息保障论坛指出，随着不断发展的网络技术，网络攻击的方式会变得越来越复杂[9-10]。网络渗透测试是从攻击者的角度模拟网络攻击的整个过程，渗透测试的过程将揭示网络系统中的弱点以及各种类型的网络攻击所引发的影响[11-13]。为了制定和修复网络防御策略，渗透测试与网络攻击密不可分。渗透测试本质上是执行网络攻击的过程，需要发现和利用目标网络系统中的安全漏洞，只不过整个过程是安全和可控的 [14-16]。因此，为了解决不同场景下如何抉择渗透测试方式、做出何种应对措施的困难，本文提出了一种基于攻击应对措施树构建了一个网络信息安全渗透测试模型。该模型以网络信息安全渗透测试技术为切入点，分别讨论了渗透测试的策略和过程，并给出了攻击树模型的基本结构。在攻击树模型的基础上，扩展了攻击应对措施树模型，并提供了模型的概率计算方法和模型生成方法。以期利

用攻击树理论实现对网络信息安全进行有效的渗透测试、对网络信息安全保护提供决策支撑。

2. Related Work

渗透测试是指通过模拟真实恶意攻击，检查目标系统的容错性和安全指标，从而对网络信息安全进行测试和评估。作为评估方式的一种，根据对象的不同可分为主机操作系统渗透、数据库系统渗透、应用系统渗透和网络设备渗透四种类型。在操作系统渗透中，陆华军等人基于 Kali Linux 构建了一种针对无线网络信息安全漏洞的 WiFi 渗透测试方法。通过该方法对无线网络的监测、扫描、数据捕获和数据分析的模拟表明，它可以有效提高无线网络的信息安全评估 [18]；数据库渗透测试研究中，Nuno Antunes 等人通过实例分析了网络信息安全测试中的 SQL 注入漏洞，利用三种创新的网络渗透测试工具进行检测。结果显示，这三种工具可以适应不同场景下的网络信息安全渗透测试，并具有更广泛的覆盖范围和更高的识别率 [21]；应用系统测试研究中，陈志等人讨论了网络渗透攻击对网络安全问题的影响，并利用蚁群分类规则挖掘算法检测网络渗透攻击。结果表明，该方法可以有效针对电力物联网中的安全漏洞进行检测，并提高攻击检测方法的有效性 [19]；Rak 等人分析了安全评估专家系统在识别物联网生态系统中的威胁、漏洞和攻击方面的应用效果，并显示该系统可以有效地帮助测试人员进行网络信息安全渗透测试，并为物联网生态系统安全提供有效的处理解决方案 [20]。网络设备渗透研究中，李勇等人分析了网络结构中节点属性之间的关联性，并显示网络拓扑在节点属性

之间形成一定的网络依赖关系。分析是通过邻接矩阵进行的，显示了网络结构与节点属性之间的非线性和高维网络依赖关系 [22]。

渗透测试也因为测试对象所处目标不同，使用的技术方面具有一定的差异。例如当模仿管理人员的蓄意或无意攻击行为，进行内网渗透测试时，常用的方法有远程缓冲区溢出、口令猜测、B/S 或 C/S 应用程序测试；而当模仿黑客等外部人员的恶意攻击时，常用方法有口令管理安全性测试、防火墙规则试探或规避、Web 及其他开放应用服务的安全性测试。

由上述的研究情况表明当前渗透测试方法很多、测试效果参差不齐。因此在不同的场景下如何选择最佳的测试方法，辅助管理人员对网络安全测试进行决策指引也是当前的研究重点。其中以根节点、子节点和叶子节点分别表示的攻击目标、子目标和到达攻击目标的攻击手法的树结构，可以表示从攻击节点到目标节点的完整攻击过程。同时基于攻击树的拓展，通过对节点赋予不同数值能实现更加复杂网络的攻击手段分析。Ray 等人提出的增强攻击树、Yager 等人提出 OWA 攻击树、代等人提出结合故障树、威胁树、事件树等不同角度对网络安全进行分析。

3. 基于攻击树理论的渗透测试模型构建

渗透测试的目的是通过安全技术手段入侵目标系统，获取目标系统的有价值信息，并实施非破坏性攻击，最终将攻击实施后的入侵路径和对系统的影响编制成渗透测试报告，并针对渗透测试过程中发现的系统漏洞提出合理的防御建议，以增强系统的安全性。本章基于攻

击树理论构建了渗透测试模型，以展示攻击树理论在网络信息安全渗透测试中的应用效果。

3.1 网络信息安全渗透测试技术

3.1.1 渗透测试策略

完成渗透测试需要同时满足软件和硬件方面的要求。对于硬件方面，主要元素包括基本的网络设备、漏洞端口扫描工具、专用于渗透测试的关键服务器等。对于软件方面，运维工程师和网络安全工程师是核心，他们在工程师的指导下模拟黑客的非破坏性攻击行为。在将硬件和软件相结合的过程中，渗透测试人员记录具体的测试操作和生成的相关数据，最后形成一份记录结果的文档报告，呈现给客户。

根据要达到的具体目标和测试者可用的信息量，现有的渗透测试策略可按照图 1 所示进行分类。

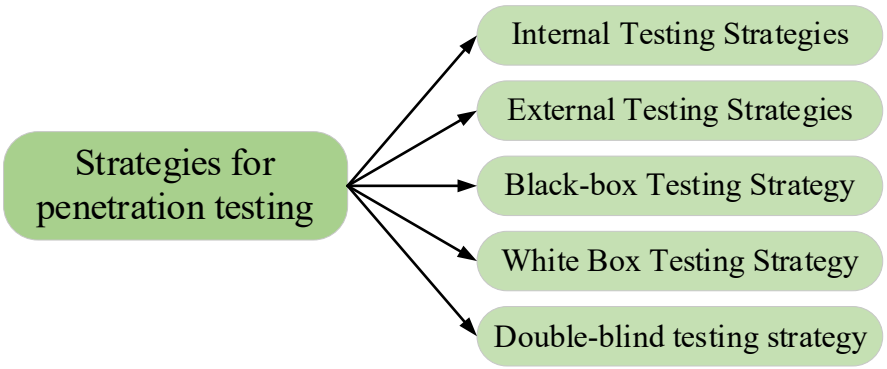

图 1 渗透测试策略分类

3.1.2 渗透测试过程

渗透测试由测试人员模拟黑客的行为，在网络上进行攻击以检测系统的漏洞。该过程可以分为三个阶段，即信息收集阶段、攻击阶段和安全分析阶段。

(1) 信息收集阶段

信息收集阶段主要是收集与目标系统相关的信息，为下一阶段的攻击做准备。图 2 展示了在这个阶段使用的技术，具体包括地址扫描、操作系统扫描、端口扫描和漏洞扫描。

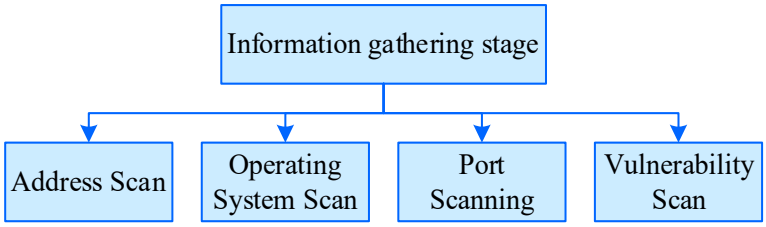

图 2 信息收集阶段的扫描技术

为了收集系统的信息，我们首先发现目标网络中的存活主机，然后对网络中的每个主机进行信息扫描，了解主机的操作系统、端口、协议和漏洞状态，最后抓取数据包以了解主机之间的端口通信情况。

(2) 攻击阶段

攻击阶段是渗透测试过程中最关键和具有挑战性的步骤。测试人员应充分利用前一阶段收集到的目标系统信息，规划对目标系统具有最大影响的渗透路径，以获取更高权限并模拟入侵者的思维攻击目标系统，然后根据攻击路径对目标系统进行实施攻击。

(3) 安全分析阶段

在信息收集阶段和攻击阶段，测试人员站在入侵者的角度进行攻击测试，但在系统的安全分析中，测试人员需要站在用户的角度，分析目标系统的漏洞以及应用漏洞后对系统运行的影响，并针对目标系统的漏洞提出相应的防御措施，提高系统的整体安全防御水平。

3.2 攻击树理论和攻击对策树模型

3.2.1 攻击树模型的基本结构

攻击树是一个多层次的树结构，包括根节点、非叶节点和叶节点。在攻击树中，树的根节点表示攻击者要达到的最终攻击目标，非叶节点表示为实现最终目标需要完成的中间步骤，叶节点表示具体的攻击行为和方法。攻击树的每个分支代表达到最终目标的可能路径。

攻击树的节点之间存在以下三种关系，即“或（OR）”关系、“与（AND）”关系和“顺序与（SAND）”关系。“或（OR）”关系表示如果任何子节点的攻击目标实现，则其父节点的目标也将实现。“与（AND）”关系表示在实现父节点的目标之前，必须实现所有子节点的攻击目标。“顺序与（SAND）”关系表示为了实现父节点的目标，必须按顺序实现所有子节点的攻击目标。图 3 展示了攻击树模型中的节点关系。

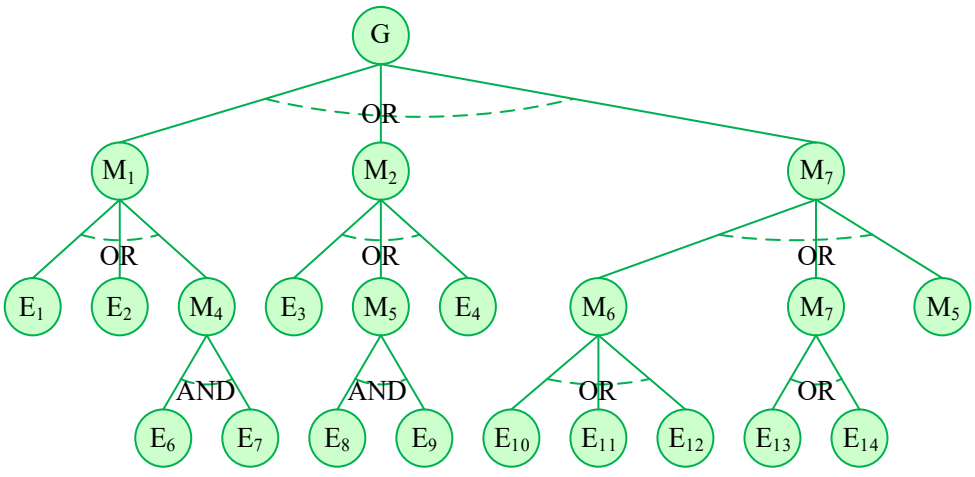

图 3 攻击树模型中的节点关系

在图中，根节点G代表攻击者的最终攻击目标，即服务器的固件，叶节点代表采取的各种攻击，即具体的攻击事件，而中间节点则代表

攻击的中间步骤。

设P_m为父节点实现的概率，$P_{m1},P_{m2},...,P_{mn}$为其下每个子节点实现的概率。对于具有 AND 关系的节点，父节点的实现概率是其下每个子节点实现概率的乘积，即：

$$P_m = P_{m1} \times P_{m2} \times ... \times P_{mn} \tag{1}$$

对于具有 OR 关系的节点，父节点的实现概率是其下每个子节点实现概率的最大值，即：

$$P_m = \max\{P_{m1},P_{m2},...,P_{mn}\} \tag{2}$$

3.2.2 攻击对策树模型的概率计算和生成

攻击对策树（Attack Countermeasure Tree，简称 ACT）是由罗伊（Roy）、金（Kim）和特里韦迪（Trivedi）于 2010 年在杜克大学提出的攻击和防御建模方法，该方法统一了攻击树和防御树的分析方法。攻击对策树允许在树的任何节点上添加防御，并通过引入概率分析扩展了定量分析的能力。ACT 的理论定义如下：

$$ACT = \{V, \psi, E\} \tag{3}$$

其中

$$V = \{\forall k, v_k : v_k \in \{A_j\} \| v_k \in \{D_j\} \| v_k \in \{M_j\}\} \tag{4}$$

$$\psi = \{\psi_k : \psi_k \in \{AND, OR, k-of-n\ gate\}\} \tag{5}$$

$$E = \{\forall k, e_k : e_k \in (v_i, \psi_j) \| e_k \in (\psi_i, \psi_j)\} \tag{6}$$

同时 $X = (x_{A_1}x_{A_2},...,x_{D_1}x_{D_2},...,x_{M_1}x_{M_2})$ 为攻击对策树的状态向量，x_{A_k},x_{D_k},x_{M_k} 是对应事件A_k,D_k,M_k的三个布尔型变量。

攻击对策树中有三种类型的事件，即攻击事件、检测事件和缓解

事件。属于同一父节点的事件之间有三种类型的门控关系，包括与门（AND）、或门（OR）和 $k-of-n$ 门。请注意，最后一种门控关系在原始攻击树中不存在，这表示 k 事件是从 n 攻击事件中选择进行与操作，并且对于这些 k 事件的选择没有优先级要求。

(1) 攻击对策树模型的概率计算

值得注意的是，在本文中，我们在检测和防御事件的节点上使用“and not”连接符，并将“and not”定义为新的连接符，而在其下方的检测和缓解事件的计算是根据实际情况进行的，即“未检测到攻击”和“检测到攻击但未进行缓解”，因此应为：

$$P_G = \overline{P}_D + P_D \times \overline{P}_M \tag{7}$$

a) 如果进行攻击对策树实例分析，则对应目标节点的直接成功攻击的概率表示为：

$$P_{goal} = P_A \tag{8}$$

b) 如果使用攻击事件和检测事件，则对于未被检测到的攻击成功的概率的相应表达式为：

$$P_{goal} = P_A(1-p_D) \tag{9}$$

c) 如果将检测事件扩展到 n 个以检测一个攻击事件，则对应的攻击成功概率表示为：

$$P_{goal} = P_A(1-p_{D1})(1-p_{D2})...(1-p_{D3}) \tag{10}$$

在攻击对策树中，如果只有检测事件可用，那么认为缓解事件是完美的，即缓解事件的概率 $P_M=1$。然而，如果缓解事件不完美，即 $0<P_M<1$，这意味着攻击对策树需要除了缓解技术之外还需要使用检

测机制。

d) 当攻击对策树具有攻击事件，并对应于检测事件和缓解事件时，其对应攻击成功的概率表示为：

$$P_{goal} = P_A(1 - p_D + p_D(1 - p_M)) = P_A(1 - p_D \times p_M) \tag{11}$$

e) 当攻击对策树中存在与多个检测事件和一个缓解事件对应的攻击事件时，匹配攻击成功的概率表达式为：

$$P_{goal} = P_A(1 - (1 - \prod_{i=1}^{n}(1 - p_{D_i})) \times p_M) \tag{12}$$

f) 当攻击对策树中存在与一个检测事件和多个缓解事件对应的攻击事件时，攻击成功的概率为：

$$P_{goal} = P_A(1 - p_D \times (1 - \prod_{i=1}^{n}(1 - p_{M_i}))) \tag{13}$$

g) 当攻击对策树中包含多对检测事件和缓解事件对应的攻击事件时，触发的缓解事件的属性取决于入侵检测的属性。攻击成功的概率为：

$$P_{goal} = P_A \prod_{i=1}^{n}(1 - p_{D_i} \times p_{M_i}) \tag{14}$$

(2) 攻击对策树的生成

与攻击树类似，攻击对策树也可以抽象为具有根节点的有向无环图，其构建过程是一个向后推理的过程。

首先确定攻击目标作为树的根节点，先构建攻击树，通过向后分析获取根节点事件发生所需的前提条件或事件组合，并表示事件之间的关系，“with”、“or”和“$k-of-n$”。然后继续向下扩展和延伸子目标，直到树中的节点无法继续细化，或已成为原子攻击事件的具体实现，

即攻击树的叶节点。

在攻击对策树中，考虑到实现成功攻击的两种情况：“未检测到攻击”和“检测到攻击但未实现缓解”。按照上述描述进行概率计算，统一用“与非”连接器表示“检测事件”和“缓解事件”。攻击树扩展为相应的攻击对策树的过程如图 4 所示。

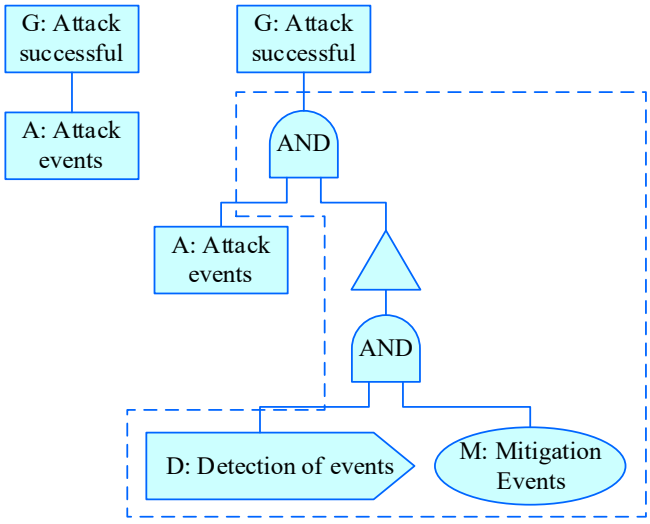

图 4：攻击树扩展为攻击对策树

在实际的网络信息安全渗透测试建模中，可以根据不同的分析需求选择性地对攻击对策树中最关键或最感兴趣的节点进行深入细化。通过从根节点到叶节点的逐步细化和完善，可以构建出针对系统目标的所有可能攻击防御场景和相关路径的模型。攻击对策树的构建过程如图 5 所示。

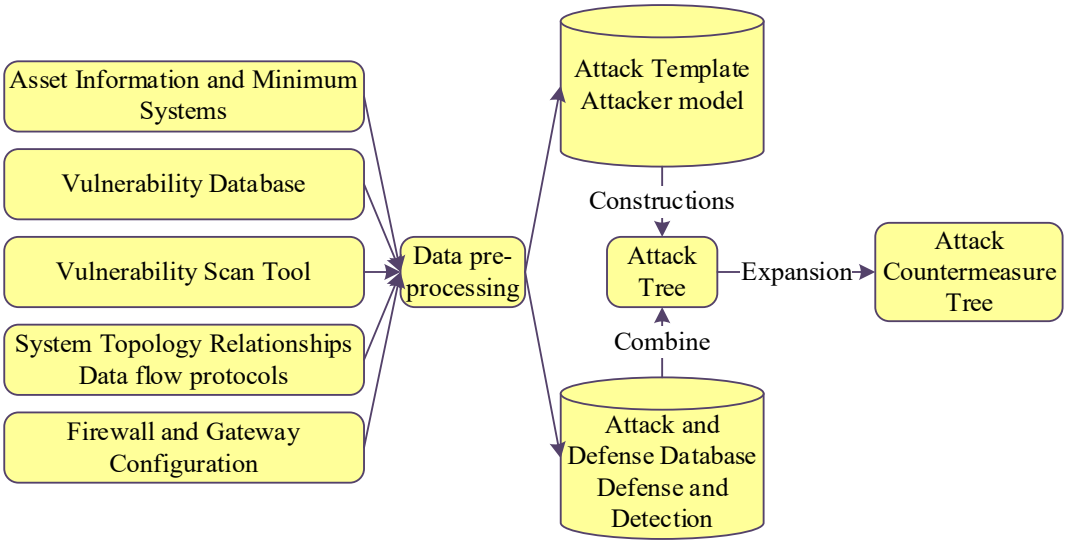

图 5：攻击对策树生成过程图

3.3 基于攻击对策树的渗透测试模型结构

基于攻击对策树模型和攻击对策树基本结构的前述论文，本文提出了基于攻击对策树的渗透测试模型结构，以实现网络信息安全渗透测试。该模型主要包括四个模块，即构建攻击对策树、生成攻击路径、信息收集与数据预处理、以及执行网络信息安全渗透测试。基于攻击对策树的渗透测试模型结构示意图如图 6 所示。

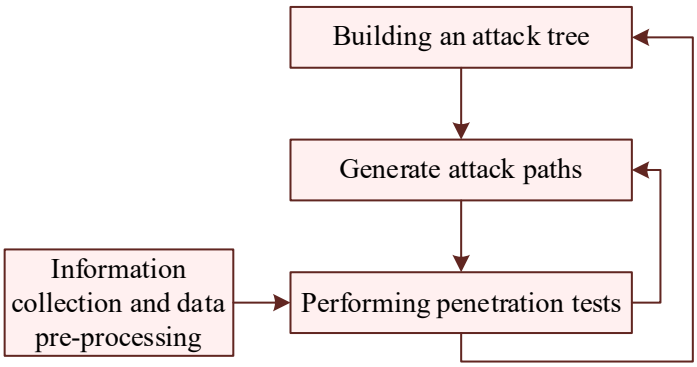

图 6：基于攻击对策树的渗透测试模型

网络信息安全渗透测试模型基于攻击对策树的过程如下：

(1) 将最终目标作为根节点构建攻击对策树。

(2) 基于“或”节点和“与”节点策略生成最佳攻击路径。

(3) 收集目标网络信息并进行数据预处理，然后根据生成的最佳路径执行渗透测试。如果执行成功，则报告攻击成功并退出。如果执行失败，则从攻击树中找到下一个最佳攻击路径并继续渗透测试。如果攻击树中的所有路径都遍历完毕而没有成功，基于渗透测试获取的信息重新构建攻击树，并重复上述过程。

4. 基于攻击对策树的渗透测试模型应用的分析

在本文中，我们设计了实验网络拓扑环境，在虚拟平台上建立了真实的攻击机器和目标机器，模拟了渗透测试过程，并使用前一章节构建的基于攻击对策树的渗透测试模型对实验环境的整体网络安全状态进行了分析。通过验证，我们得出结论：基于收益的概率攻击图模型在渗透测试过程的实施中具有更好的全局性和分析性指导。当然，这个实验确保了渗透测试过程的可控性，不涉及不规范操作。

4.1 构建工程师工作站攻击的对策树模型

工程师工作站用于配置和管理安全级别 DCS 系统的自身参数和工程应用数据，以满足工程设计、系统调试和运维等各个阶段的功能要求。其核心是工程师工作站软件，在 PC 上离线运行，能够生成逻辑配置和图形配置程序代码，生成工程配置信息，监控变量和状态等。通过研究工程师工作站的相关配置信息，分析其漏洞，并以“工程师工作站受到攻击”作为根节点，建立了一个工程师工作站的攻击树模

型，其具体结构如图 7 所示。

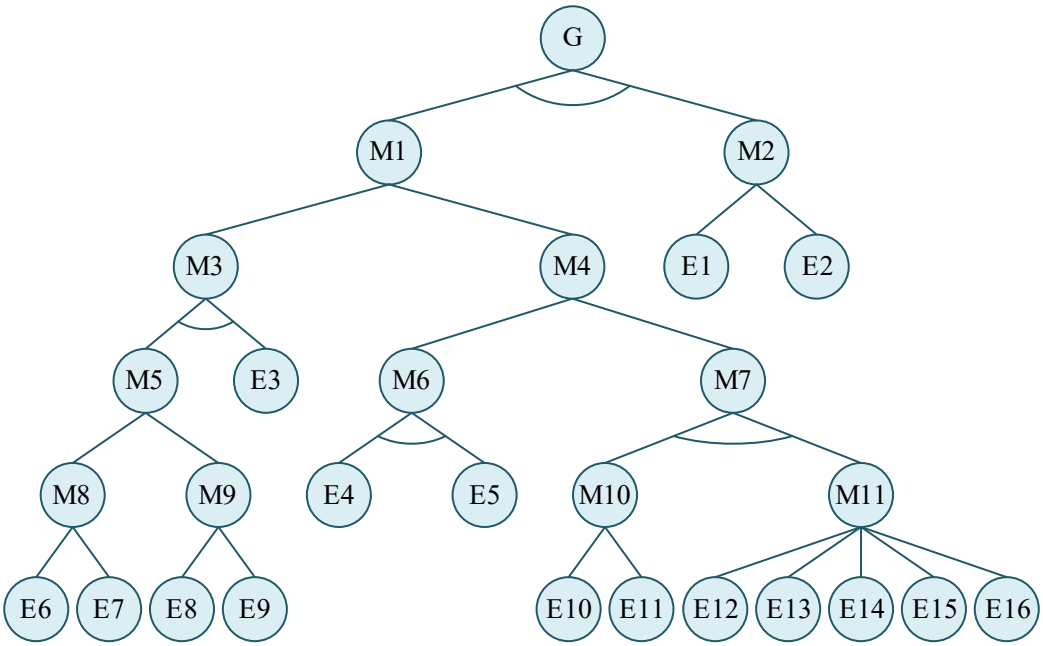

图 7 工程师工作站攻击对策树模型

表 1 显示了这个攻击对策树的根节点、中间节点和叶节点的含义。

表 1 攻击对策树中各节点的含义

Symbols	Meaning	Symbols	Meaning
G	Engineer station under attack	E3	Malicious download of applications
M1	Attack behavior	E4	Obtain system drivers
M2	Access to the site to start and connect to the MTS	E5	Connecting to black box attack tools
M3	Physical attack	E6	Decrypting user logs
M4	Logical attack	E7	Installing special cameras to monitor
M5	Obtain high privilege accounts	E8	Unintentional disclosure
M6	Using black box attacks	E9	Intentional leakage
M7	Malware attacks	E10	USB port access
M8	Use of special hardware	E11	Network switch reserved interface access
M9	Person of interest compromise	E12	windows vulnerability
M10	Reserved interfaces to load malware	E13	SQL injection attack

M11	Writing and running malware	E14	Configuration Software Vulnerability
E1	Person of interest on site	E15	Communication Protocol Vulnerability
E2	Other means of access	E16	Engineer Station Software Vulnerability

4.2 对攻击对策树的每个叶节点进行攻击发生概率分析

根据第 3.2 节攻击对策树中叶节点的成功攻击发生概率计算，本节首先使用专家评估方法对每个叶节点的属性值进行评分，并找出每个叶节点的攻击事件发生概率，结果如图 8 所示。

从每个叶节点的攻击概率来看，E11 节点的发生概率最高，为 0.548，其次是 E4 节点的发生概率为 0.492，E10 节点为 0.475，E13 节点为 0.467，这表明对于工程站网络安全系统而言，最高的攻击威胁是通过网络交换机保留接口访问本地接口，并利用恶意代码进入工程站的数据库漏洞，然后执行 SQL 注入攻击以窃取数据和破坏系统。这表明在网络信息安全中需要关注交换机接口的安全性，并且开发人员需要升级网络系统访问通道和数据库以确保其信息安全保护能力。

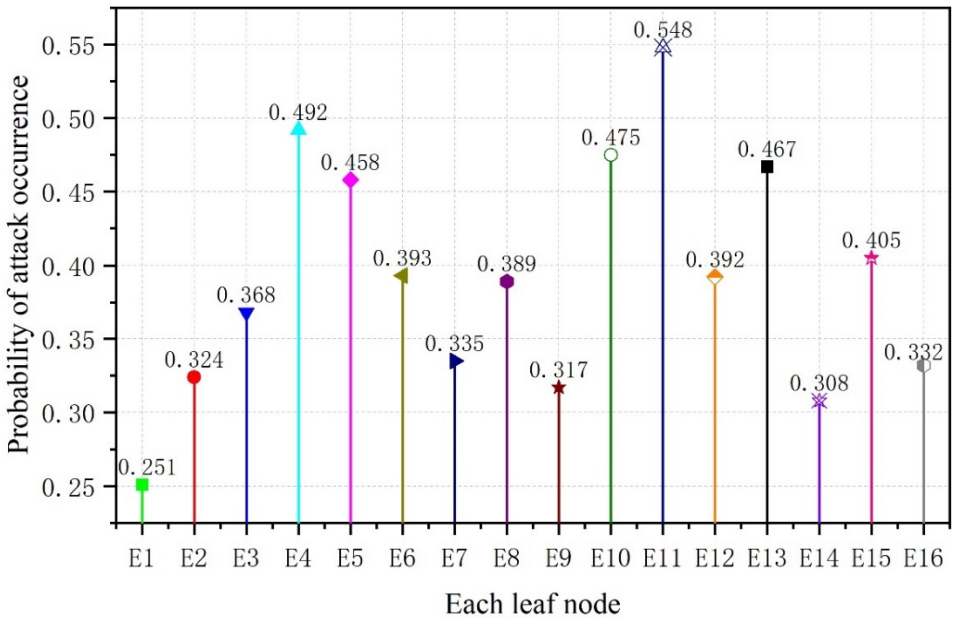

图 8：每个叶节点攻击发生概率

4.3 基于攻击对策树中每个叶节点的影响系数分析

为了进一步了解网络信息安全渗透测试的影响，本节分析了攻击对策树中每个叶节点对应漏洞的机密性、完整性和可用性的影响系数，并得出了分析结果，如图 9 所示。

从攻击对策树中每个叶节点对应漏洞的影响系数来看，其他途径影响系数较大的是 E2 节点，其机密性、完整性和可用性的影响系数分别为 0.58、0.45 和 0.54。这也表明，在进行工程师站的网络信息安全分析过程中，存在其他途径使漏洞攻击更有可能成功。在后续过程中，我们需要进一步提高工程师站的整体网络防护能力，使工程师站的防护网络覆盖范围更广，减少其他途径的影响。此外，E11 节点的可用性影响因素为 0.55，这表明利用网络交换机保留接口访问工程师站网络可以促进工程师站网络资源的共享。然而，如前一节所给出的攻击成功概率，该节点对网络信息安全也会产生一定影响，因此需要在确保网络信息安全的条件下谨慎使用，并进行启用，以防止信息泄

露。

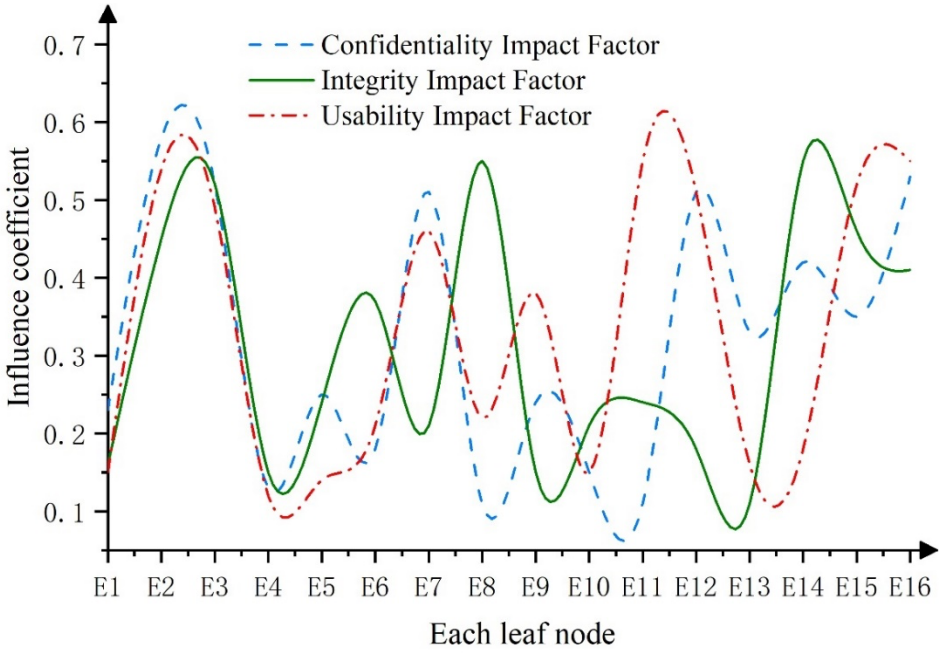

Figure 9 Analysis of the influence coefficient of each leaf node

4.4 对于每个攻击序列的攻击效果评估进行分析

为了进一步分析攻击对工程师站网络信息安全的影响，使用攻击效果的定量评估算法对数据进行定量分析，具体表达如下：

如果利用同一设备 $l = \in \{1,2,...,L\}$ 的多个漏洞进行攻击，设备节点所产生的损失表示为

$$Lost\_H_i = imp_i \cdot \prod_{l=1}^{L} P_{i,l} \cdot (\vec{A}_{i,l} \cdot \vec{w}_{i,l}) \tag{15}$$

其中，imp_i表示设备节点的重要性，$\vec{A}_{i,l}$表示对设备的机密性、完整性和可用性的需求权重，$\vec{w}_{i,l}$表示第l个设备的第i个弱点对设备节点的机密性、完整性和可用性的影响系数。

不失一般性，假设攻击序列为

$$S_j = \{E_{1,l},...,E_{i,l},...,E_{m,l}\} \tag{16}$$

$$\begin{cases} j = \{1,2,...,J\}; i \in \{1,2,...,m\} \\ m \in \{1,2,...,n\}; l = \in \{1,2,...,L\} \end{cases} \tag{17}$$

然后将攻击效果进行量化，并表示为

$$AssResult\_S_j = \prod_{i \in \{1,2,...,m\}} Lost\_H_i \tag{18}$$

根据第 4.3 节给出的每个叶节点的保密性、完整性和可用性的影响系数，使用公式（15）计算了设备节点的安全损失，并使用公式（18）得出了每个攻击序列对应的攻击效果的定量评估结果，具体结果如表 2 所示。

表 2 每个攻击序列攻击效果的评估结果

Attack Sequence $S_j \in S$	Number of steps	Attack effect
$S_1 = \{E4, E10, E11\}$	3	0.6342
$S_2 = \{E12, E13\}$	2	0.9834
$S_3 = \{E15, E16\}$	2	0.7396
$S_4 = \{E1, E2, E5, E13\}$	4	0.1457
$S_5 = \{E3, E6, E7, E8, E9\}$	5	0.1628

根据每个攻击序列攻击效果的定量评估结果，我们可以得到每个攻击序列的大小关系为 $S_2 > S_3 > S_1 > S_5 > S_4$。攻击效果最大的攻击方法是通过 Windows 漏洞执行的 SQL 注入攻击，其评估结果为 0.9834。这表明为了确保网络信息安全，我们需要尽快升级 Windows 系统，更新系统病毒数据库，找到漏洞并及时修复，从而确保网络信息安全。

5. 总结

在本文中，我们从网络信息安全渗透测试技术出发，分析了攻击树理论并将其扩展到攻击对策树模型的构建。基于攻击对策树构建了一个网络信息安全渗透模型，并进行了实证分析，验证了模型应用的有效性。以下是得出的结论：

(1) 从攻击对策树每个叶节点的攻击概率来看，前三个节点是网络交换机保留接口访问、获取系统驱动程序和 USB 接口访问，它们的攻击概率分别为 0.548、0.492 和 0.475。这表明在构建网络信息安全系统时，需要对网络交换机接口进行安全检测，确保系统驱动程序的使用并减少使用 USB 存储设备，从而确保网络信息安全系统的安全性。

(2) 从攻击对策树每个叶节点的影响系数来看，E2 节点代表的其他途径方法的影响系数较大，其保密性、完整性和可用性的影响系数分别为 0.58、0.45 和 0.54。这表明其他途径方法会使网络信息安全系统具有一定的攻击概率，需要关注各种类型的系统访问方法以确保系统安全。

(3) 从每个攻击序列的攻击效果评估结果来看，攻击网络信息安全最有效的方法是通过 Windows 漏洞执行 SQL 注入攻击，其评估结果为 0.9834。这表明有必要定期修复系统漏洞，提升系统安全保护网络，以避免外部漏洞攻击。

References

[1] Sun, T. (2018). A risk assessment standard and application method of computer network information security. Basic & clinical pharmacology & toxicology.(S7), 123.
[2] Feng, L., Han, R., Wang, H., Zhao, Q., Fu, C., & Han, Q. (2021). A virus propagation model and optimal control strategy in the point-to-group network to information security investment. Complexity, 2021.
[3] Hongfeng, C. (2020). Information network security construction based on depth learning and modulus algorithm. Journal of Intelligent and Fuzzy Systems, 38(4), 1-12.
[4] He, D., Zhang, Y., Li, T., Chan, S., & Guizani, N. (2020). Vulnerability analysis and security compliance testing for networked surveillance cameras. IEEE Network, PP(99), 1-7.
[5] Sun, L., & Gao, D. (2022). Security attitude prediction model of secret-related computer information system based on distributed parallel computing programming. Mathematical Problems in Engineering, 2022.
[6] Liu, Lin, Xinbao, Pei, Jun, & Pardalos, et al. (2017). A game-theoretic analysis of information security investment for multiple firms in a network. Journal of the Operational Research Society.
[7] Wang, Y. Z., Gao, B., & Lu, W. C. (2018). Application of bp neural network based on pca in information security. Basic & clinical pharmacology & toxicology.(Suppl.3), 123.
[8] Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Investigation into the formation of information security influence: network analysis of an emerging organisation. Computers & Security, 70(sep.), 111–123.
[9] Zhang, R., & Hu, Z. (2021). Access control method of network security authentication information based on fuzzy reasoning algorithm. Measurement, 185, 110103-.
[10] Garg, ShreePeddoju, Sateesh K.Sarje, Anil K. (2017). Network-based detection of android malicious apps. International Journal of Information Security, 16(4).
[11] Ji, B. K. D. H. (2021). Evaluating visualization approaches to detect abnormal activities in network traffic data. International Journal of Information Security, 20(3).
[12] Ficco, M., Choras, M., & Kozik, R. (2017). Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. Journal of Computational Science, 22(sep.), 179-186.
[13] Shitharth, S., Shaik, M., Sirajudeen, A. J., & Sangeetha, K. (2019). Mining of intrusion attack in scada network using clustering and genetically seeded flora based optimal classification algorithm. IET Information Security, 14(6).
[14] Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace. Information & Management.
[15] Du, M. (2020). Application of information communication network security management and control based on big data technology. International Journal of Communication Systems.
[16] Erdodi, L., & Zennaro, F. M. (2022). The agent web model: modeling web hacking

for reinforcement learning. International Journal of Information Security(2), 21.
[17] Guangxu, Y. (2020). Research on computer network information security based on improved machine learning. Journal of Intelligent and Fuzzy Systems, 40(3), 1-12.
[18] Lu, H. J., & Yu, Y. (2021). Research on wifi penetration testing with kali linux. Complexity, 2021.
[19] Chen, Z., Zuo, X., Dong, N., & Hou, B. (2019). Application of network security penetration technology in power internet of things security vulnerability detection. Transactions on Emerging Telecommunications Technologies(2).
[20] Rak, M., Salzillo, G., & Granata, D. (2022). Esseca: an automated expert system for threat modelling and penetration testing for iot ecosystems. Computers & Electrical Engineering, 99, 107721-.
[21] Nuno Antunes, & Marco Vieira. (2017). Designing vulnerability testing tools for web services: approach, components, and tools. International Journal of Information Security.
[22] Lee, Y., Shen, C., & Vogelstein, J. T. (2017). Network dependence testing via diffusion maps and distance-based correlations. Biometrika.