[大语言模型知识引擎驱动的ACT树渗透测试框架研究 2](#_Toc161421816)

[1.引入 2](#_Toc161421817)

[2. Related Work 4](#_Toc161421818)

[3. 基于AT理论的渗透测试模型构建 6](#_Toc161421819)

[3.1 网络信息安全渗透测试技术 6](#_Toc161421820)

[3.1.1 渗透测试策略 6](#_Toc161421821)

[3.1.2 渗透测试过程 7](#_Toc161421822)

[3.2 AT理论和ACT 8](#_Toc161421823)

[3.2.1 AT模型的基本结构 8](#_Toc161421824)

[3.2.2 ACT的概率计算和生成 9](#_Toc161421825)

[3.3 大语言模型知识引擎与ACT泛攻击层 13](#_Toc161421826)

[3.3.1 大语言模型知识引擎 13](#_Toc161421827)

[3.3.2 ACT泛攻击层与DBSCAN展开算法 14](#_Toc161421828)

[3.4 基于ACT的渗透测试模型结构 16](#_Toc161421829)

[3.5 基于XXX（图算法名称）的网络节点威胁态势分析算法 17](#_Toc161421830)

[4. 基于ACT的渗透测试模型应用的分析 19](#_Toc161421831)

[4.1 构建工程师工作站攻击的对策树模型 20](#_Toc161421832)

[4.2 对ACT的每个叶节点进行攻击发生概率分析 21](#_Toc161421833)

[4.3 基于ACT中每个叶节点的影响系数分析 22](#_Toc161421834)

[4.4 对于每个攻击序列的攻击效果评估进行分析 23](#_Toc161421835)

[4.5 网络节点威胁态势分析算法效果实验 24](#_Toc161421836)

[5. 总结 25](#_Toc161421837)

[References 25](#_Toc161421838)

大语言模型知识引擎驱动的ACT树渗透测试框架研究

**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。因此本文使用大语言模型作为知识引擎，结合改进的攻击应对措施树（Attack Countermeasure Tree，ACT）构建了冷启动的网络信息安全渗透测试模型。该模型通过ACT计算对应的攻击概率，并且使用大语言模型知识引擎和DBSCAN聚类算法对ACT进行展开，从而构建了设备级别的网络信息安全渗透测试模型。同时本文还使用了图算法对多台设备组成的网络进行了整体分析。此外，本文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。该结果表明，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; 大语言模型；DBSCAN算法；图算法；冷启动

# 1.引入

随着时代的发展，信息网络在给人们带来了许多便利，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（Attack Countermeasure Tree）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（Attack Tree， AT）模型的基本结构。在AT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基于大语言模型知识引擎的模型生成方法，并且对多设备网络进行整体分析，以期利用AT理论为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。

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AT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。

（加一段大语言模型的论述，论述大语言模型作为知识引擎的用处：降低专家知识的重要性，提高系统的易用性，无需前置知识就可冷启动）

近年来，随着预训练大语言模型技术的快速发展，如GPT系列、BERT等模型在自然语言处理领域的广泛应用，它们已经展现出了强大的知识理解和生成能力。这些模型能够通过大规模数据训练，吸收和理解海量文本中的网络信息安全相关知识，并能够以人类可读的方式进行解释和推断。将大语言模型融入渗透测试这一研究方向，有望推动网络信息安全领域渗透测试技术朝着智能化、自动化方向发展，提高整体网络安全管理水平。

（加一段图算法的论述，论述图算法对多设备网络分析的例子）

# 3. 基于AT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AT理论构建了渗透测试模型。

## 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 AT理论和ACT

### 3.2.1 AT模型的基本结构

AT是一个多层次的树结构，包括根节点、非叶节点和叶节点。在AT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。AT的每个分支代表达到最终目标的可能路径。

AT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AT模型中的节点关系。



图3 AT模型中的节点关系

在图中，根节点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。

设为父节点实现的概率，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：

 (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：

 (2)

### 3.2.2 ACT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AT（Attack Tree， AT）和防御树的分析方法。ACT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：

 (3)

其中

 (4)

 (5)

 (6)

同时  为ACT的状态向量， 是对应事件的三个布尔型变量。

ACT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  门。请注意，最后一种门控关系在原始AT中不存在，这表示  事件是从  攻击事件中选择进行与操作，并且对于这些  事件的选择没有优先级要求。

(1) ACT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：

 (7)

a) 如果进行ACT实例分析，则对应目标节点的直接成功攻击的概率表示为：

 (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：

 (9)

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

 (10)

在ACT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 。然而，如果缓解事件不完美，即 ，这意味着ACT需要除了缓解技术之外还需要使用检测机制。

d) 当ACT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：

 (11)

e) 当ACT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：

 (12)

f) 当ACT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：

 (13)

g) 当ACT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：

 (14)

(2) ACT的生成

与AT类似，ACT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AT，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“”。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AT的叶节点。

在ACT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”。AT扩展为相应的ACT的过程如图4所示。



图4：AT扩展为ACT

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ACT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。ACT的构建过程如图5所示。



图5：ACT生成过程图

## 3.3 大语言模型知识引擎与ACT泛攻击层

### 3.3.1 大语言模型知识引擎

随着大语言模型技术的飞速发展，模型中的先验知识随着模型本身的参数量一起变得越来越丰富。因此在包括恶意代码检测、视觉问答系统等多个经典机器学习问题中，大语言模型因其海量的先验知识，被采用为高效的自然语言知识引擎。

采用大语言模型作为知识引擎的好处在于，大语言模型的预训练中就已经对所需专家知识进行了采样，因此在系统中大语言模型可以很大程度的替代专家知识，并且大语言模型的使用无需特定领域的先验知识，这就使得系统可以具有冷启动的特性，并且具有着向自动化方向发展的潜力。

为了在本项目中使用大语言模型作为渗透测试的知识引擎，我们基于Prompt工程设计了如下的提示词。

“你是一名渗透测试工程师，现在有一台设备，设备情况为：[设备情况细节]。现在请你作为渗透测试工程师列出多种这台设备可能受到的攻击的实现方式。”

接受到大语言模型对提示词的回应后，系统相当于获得了对于目标设备的多种建议攻击方式的具体实现，这些实现方式构成了ACT树在叶子节点。

### 3.3.2 ACT泛攻击层与DBSCAN展开算法

实践发现，无论攻击方式的细节如何变化，攻击方式所属类别是有限且很少变化的。在ACT中，这就意味着对于同一个设备，其ACT树上的非叶子节点的可扩展空间是恒定的。此时，定义所有的可受到攻击的电子设备为集合，则对于每一种电子设备，可以通过包括专家知识或大语言模型知识引擎等方法获取可能攻破它的攻击方式类别（即ACT树中的非叶子节点）集合为。此时，可以定义ACT泛攻击层为：

对泛攻击层中的网络攻击方法数据进行层次聚类算法（具体用哪个还没选），系统可以得到ACT泛攻击层的树形结构，其中是树的节点集合，是树的边集合。使用层次聚类算法得到的是有根树，其根为目标设备，其余节点为前文所述的攻击方式类别。其中，任意节点到达根节点的路径可以表示为：

，其中

此时考虑层次聚类算法的特性，定义节点所属类别在语义空间中占据空间为，则对于路径中父节点和子节点，有如下关系：

如果父节点在中有多个子节点，则其语义空间也存在关系：

对于大语言模型返回的建议攻击方式的具体实现集合，我们使用如下算法将集合中的元素插入ACT泛攻击层树中。

（算法伪代码）

function **insert\_attack\_to\_tree**(T, attack\_method, current\_node = root):

4 *// 如果当前节点为空，直接将攻击方法作为新节点插入，并返回该新节点*

5 if current\_node is None:

6 new\_node = create\_new\_node(attack\_method)

7 return new\_node

8

9 *// 检查当前节点的空间范围是否包含输入的攻击方法*

10 if **space\_range\_of**(current\_node) contains attack\_method:

11 *// 继续遍历子节点*

12 for child in **children\_of**(current\_node):

13 *// 递归调用函数，检查子节点*

14 result\_node = insert\_attack\_to\_tree(T, attack\_method, child)

15 *// 若子节点成功插入了攻击方法，则返回该子节点*

16 if result\_node is not None:

17 return result\_node

18

19 *// 当前层所有子节点都不包含攻击方法时，在当前节点下创建新节点*

20 new\_node = create\_new\_node(attack\_method)

21 add\_child\_to(current\_node, new\_node)

22 return new\_node

23

24 *// 当前节点空间范围不包含攻击方法，向上回溯*

25 return None

## 3.4 基于ACT的渗透测试模型结构

基于ACT和ACT基本结构的前述论文，本文提出了基于ACT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ACT、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ACT的渗透测试模型结构示意图如图6所示。



图6：基于ACT的渗透测试模型

网络信息安全渗透测试模型基于ACT的过程如下：

(1) 将最终目标作为根节点，结合大语言模型知识引擎构建ACT。

(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AT中找到下一个最佳攻击路径并继续渗透测试。如果AT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AT，并重复上述过程。

## 3.5 基于XXX（图算法名称）的网络节点威胁态势分析算法

在使用ACT树对单个设备进行分析后，我们可以通过简化设备细节的方式构建多设备拓扑，结合ACT树分析结果对设备拓扑网络进行分析，从而感知设备拓扑网络中的威胁态势、关键区域与核心节点。在此基础上，我们可以进一步对整个设备网络安全态势有更全面的认知。

定义设备脆弱性为，则多设备网络被记为，其中，，。

在无向图中，使用拉普拉斯矩阵分析节点脆弱性可以通过计算其特征值和特征向量来实现。拉普拉斯矩阵是图论中的一个重要工具，它反映了图中节点间的连通性和结构特性。

对于一个无向图 \( G=(V,E) \)，其中 \( V \) 是节点集合，\( E \) 是边的集合，每个节点 \( i \in V \) 有一个脆弱值 \( r\_i \)。首先，定义以下两个矩阵：

1. 邻接矩阵 \( A \)：如果节点 \( i \) 和节点 \( j \) 之间有一条边，则 \( A\_{ij}=A\_{ji} \) 是该边的权重（若权值表示紧密程度，则紧密连接的节点间边权较小）；否则 \( A\_{ij}=0 \)。

2. 度矩阵 \( D \)：对角线元素为节点 \( i \) 的度（即与之相连的所有边的权重之和），非对角线元素为零，即 \( D\_{ii} = \sum\_j A\_{ij} \) 且 \( D\_{ij} = 0 \) 对于 \( i \neq j \)。

\*\*拉普拉斯矩阵\*\* 定义为：

\[ L = D - A \]

拉普拉斯矩阵具有许多有趣的性质，其中之一是它的特征分解可以用来识别图的重要节点或社区结构。令拉普拉斯矩阵 \( L \) 的特征值为 \( \lambda\_1, \lambda\_2, ..., \lambda\_n \)，对应的归一化特征向量为 \( u\_1, u\_2, ..., u\_n \)，其中 \( n = |V| \) 为节点数量。

- \*\*Fiedler Vector\*\*（第二小特征值对应的特征向量）：在无向图中，最小特征值始终为 0，并对应所有元素都相同的特征向量。而第二小的特征值 \( \lambda\_2 \) 及其对应的特征向量 \( u\_2 \) 被称为 Fiedler 向量，在某些情况下，它可以用于近似地分割图成两个“最弱”的部分，这里的“弱”可以根据具体应用来定义。例如，在本问题中，若节点的脆弱值乘以它们在 Fiedler 向量上的分量（正负号指示所属的组别），则正分量较大的节点可能构成了相对更脆弱的一个区域。

- \*\*PageRank-like 分析\*\*：通过对拉普拉斯矩阵进行随机游走的解释，可以将其与 PageRank 进行类比。通过预处理将节点脆弱值纳入考虑，如构造一个带脆弱性权重的随机跳转矩阵，然后求解类似 PageRank 的迭代过程，找出那些由于自身脆弱且在拓扑结构中位置重要而导致脆弱性传播快的节点。

- \*\*谱聚类\*\*：基于拉普拉斯矩阵的谱聚类方法也是常用的社区检测手段。通过对 \( L \) 或其归一化的版本 \( L\_{sym} = D^{-\frac{1}{2}}LD^{-\frac{1}{2}} \) 进行特征分解，然后选取前 k 个特征向量构成低维空间，接着在该空间内应用聚类算法（如 K-Means），可以发现网络中的社区结构。在这些社区中，综合考虑节点脆弱值可确定哪些区域最为脆弱。

总之，利用拉普拉斯矩阵的方法不是直接计算节点脆弱性，而是通过挖掘图的内在结构信息找到潜在的分区或者重要节点，再结合节点的脆弱值指标来评估整个图中各个区域的脆弱性水平。

# 4. 基于ACT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ACT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。本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AT模型，其具体结构如图7所示。



图7 工程师工作站ACT

表1 显示了这个ACT的根节点、中间节点和叶节点的含义。

表1 ACT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ACT的每个叶节点进行攻击发生概率分析

根据第3.2节ACT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。

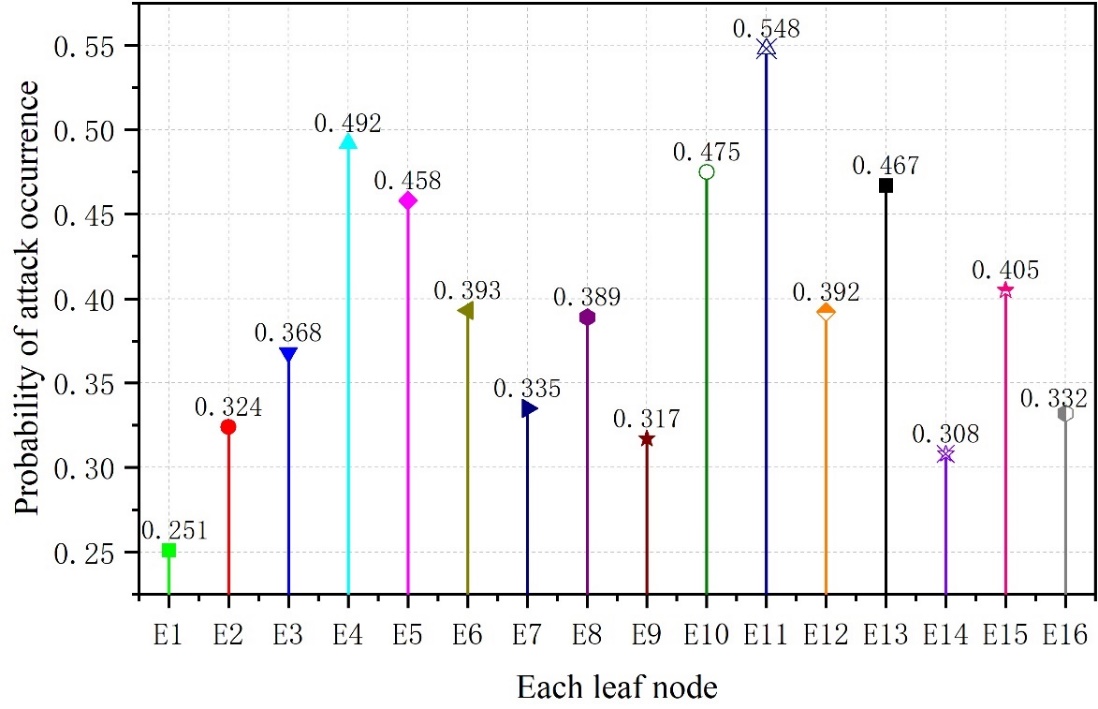


图8：每个叶节点攻击发生概率

## 4.3 基于ACT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ACT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ACT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。

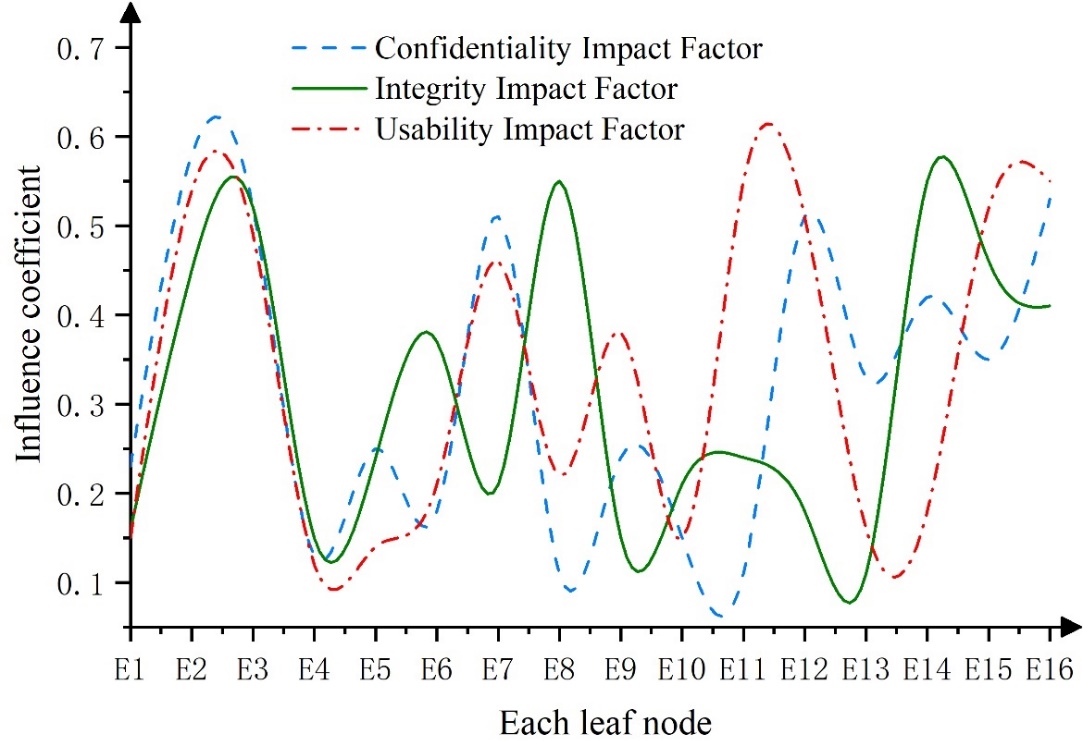


Figure 9 Analysis of the influence coefficient of each leaf node

## 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  的多个漏洞进行攻击，设备节点所产生的损失表示为

 (15)

其中，表示设备节点的重要性，表示对设备的机密性、完整性和可用性的需求权重，表示第个设备的第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

 (16)

 (17)

然后将攻击效果进行量化，并表示为

 (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 | Number of steps | Attack effect |
|  | 3 | 0.6342 |
|  | 2 | 0.9834 |
|  | 2 | 0.7396 |
|  | 4 | 0.1457 |
|  | 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 。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。

## 4.5 网络节点威胁态势分析算法效果实验

为了测试网络节点威胁态势算法对于节点拓扑关系的理解能力，我们以计算机网络为例，按照计算机网络的图论特性，设计了一个拥有XXX节点的网络拓扑结构。

对于计算机网络而言，其度分布具有非正态分布的性质。具体而言，网络中存在如下类型的几类节点。

（画一个图，展示核心节点、中继节点、服务节点和说明，最好是在度分布图上画出三类的示意图）

为了更好的模拟实际中的环境，我们从度分布的角度入手，设计了如下的网络拓扑结构，并按照实际情况设计了各边的边权和各点的点权。网络的可视化效果如下图所示。

（画出可视化的图）

（实验结果XXX）

# 5. 总结

在本文中，我们以网络信息安全渗透测试技术为核心，深入探讨了攻击树（Attack Tree, AT）理论及其在构建攻击应对措施树（Attack Countermeasure Tree, ACT）中的扩展应用。通过精心设计和实现的基于ACT的网络信息安全渗透测试模型，我们不仅详尽分析了系统内部的安全漏洞及潜在风险，而且借助实证研究验证了该模型在实际场景下的高效性和实用性。

为了更全面地理解和评估整个设备网络的安全态势，我们进一步创新性地提出了网络节点威胁态势分析算法，旨在从全局视角出发，实时、准确地捕捉并量化网络中各个节点面临的潜在安全威胁，为网络安全防护提供更加宏观而精细的决策依据。

随着人工智能技术日新月异的发展，在当前时代背景下，我们的系统成功地将渗透测试过程转向数字化和自动化，大大提升了检测效率与准确性，降低了对专业人员依赖程度的同时，有力推动了网络信息安全领域智能化管理进程。通过集成大语言模型知识引擎、DBSCAN聚类算法以及图算法等先进技术，本研究有效地解决了冷启动状态下的渗透测试策略选择难题，并为网络安全管理人员提供了针对性强且易于实施的安全建议和解决方案。

# 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.