基于深度学习的网络漏洞评估分析

韩 菊*
HAN Ju

摘 要 在计算机应用技术快速发展的过程中，数字经济也呈现出全球化、国际化的发展态势。然而国民在享受信息技术所带来的便利时，却面临着巨大的网络风险。主要包括非法破坏、篡改、截取、嗅探等内容。根据相关数据调查显示，截至2019年底，我国全年公布的网络漏洞达17209个，高危漏洞约5209个。除部分机构和组织外，我国大部分政府机构和企业单位都难以快速准确地查询并评估网络漏洞。因此需要结合深度学习系统，重新建构计算机网络漏洞的评估体系，确定传统漏洞评估方法所存在的问题，提出相应的应对策略。

关键词 深度学习；漏洞；评估分析

doi：10.3969/j.issn.1672-9528.2020.09.067

0 引言

入侵响应、入侵检测属于传统的被动防御策略，即当计算机系统遭受网络攻击后，才进行相应的响应，如切断连接、发出警报等。然而如果要想切实地保障计算机系统的稳定和安全，就必须采取积极的、主动的应对方案，并对计算机系统漏洞进行准确、科学、合理的分析和评价，从而发现和监测计算机系统中的漏洞，并进行防范，以此提升计算机系统的稳定性与安全性。然而传统的网络漏洞评估方案及策略拥有较大的局限性，结合深度学习理论，可以构建出全新的漏洞防范及评估机制。

1 深度学习系统的基本内涵

深度学习主要指机器学习的重要分支，是以神经网络为依托，对信息进行学习的特殊算法。现阶段已经有卷积神经、深度神经、递归神经及置信网络等神经网络系统，被广泛应用到自然语言、语音识别、计算机视觉、信息学及音频识别等领域中。在理论研究层面上，深度学习能够通过计算机多层处理的机制，将原始层的特征转变为特定的高层特征，并利用模型展示的方式，完成较为复杂的学习任务。因此，我们可以将深度学习理论理解为“表示学习”或“特征学习”。在传统的深度学习层面，需要相关专家来描述学习样本的基本特征，以此构建出相应的“特征工程”。但如果“特征”不够突出或优秀，将导致计算机神经网络深度学习的泛化性能受到制约。而特征学习（深度学习）的关键是通过计算机学习的方式来形成良好的特征，进而让计算机学习呈现出自动化、智能化的发展特征及特点。在技术应用等层面上，计算机深度学习主要应用到：“信息论”“概率”“线性代数”“随机梯度”“自适应算法”“循环网络”及“表征”学习等技术。在工作原理层面上，深度学习，能够从传输节点形成传输节点所需要数据信息，以此表示不同的计算函数值。而当计算结果被广泛融入子节点后，便会形成特殊的函数族，即当数据从输入节点，传向子节点后，便会完成“深度计算”的任务，使节点值更加精确，更加明了。而在实际应用的过程中，深度学习需要破解“深度不足”（层次不深）所形成的问题，保障神经网络与人脑拥有相同的深度结构。

2 网络漏洞评估的基本内容及方法

2.1 网络漏洞评估的基本内容

计算机网络漏洞的安全与稳定取决于计算机内外两个层面的影响。其中内部影响主要指计算机系统所存在的网络漏洞，而外部影响则指一般性的安全事件。如黑客攻击、网络病毒等。所以，根据评估内容和方向，可以将网络漏洞评估划分为威胁评估和漏洞评估两个内容。其中威胁评估主要指对组织、系统及资产结构造成影响的外部要素。该评估内容属于计算机网络评估的最后环节，是在系统得到安全、稳定运行后，对外部因素进行评估及分析的重要环节。在威胁分析层面上，需要分析并处理多种信息员，其中主要包括人工评估、安全审计、文档分析、入侵测试等内容。而网络漏洞评估，则指客户端、商业应用、网络设计、操作系统、浏览器、安全软件的漏洞。这些漏洞如果不能得到及时有效的处理，将导致计算机基本的应用功能难以得到发挥，从而影响到计算机系统的稳定性。在计算机网络漏洞分析层面上，主要包括网络漏洞分析和评估、数据库漏洞分析和评估、计算机逐级漏洞分析和评估三个层面。

2.2 网络漏洞评估的传统方法

传统的网络漏洞评估和分析的方法主要有资产探测和网

* 太原学院 山西太原 030012

络漏洞扫描两种。首先是资产探测，通常来讲漏洞评估的基础是资产探测，技术人员在对计算机系统进行漏洞评估的过程中，需要进行相应的资产探测，以此明确系统或网络中所存在的资产信息，譬如打印机、服务器等。然而资产探测主要通过 TCP 的方式对网络漏洞进行扫描，发包量大、持续时间较长，经常出现连接失败等问题，很容易造成计算机网络堵塞，实效性低下等问题。其次是漏洞扫描。漏洞扫描通常是根据特征匹配的方式，识别并评估相应的网络漏洞的。即通过发放含有漏洞特征的数据包，并以此判断计算机网络是否存在网络漏洞。然而该方法却存在严重的弊端。即验证漏洞所发放的数据包极易被杀毒软件阻断，且数据包的评估精度较低，很容易出现漏报或误报等问题。所以在新时代发展的背景下，传统的网络漏洞评估方法已经难以适应现代化发展的需求，需要结合神经网络的应用优势，评估并检测网络漏洞，从而营建出更健康、更安全、更稳定的网络信息环境。

3 深度学习下的网络漏洞评估原则及方法

相较于传统的网络漏洞评估方法，深度学习能够以快速、高效、自动化的优势，帮助计算机网络信息安全人员实现对网络漏洞的评估和监测，极大地提升漏洞检测的准确性和时效性，使网络漏洞检测逐渐呈现自动化、智能化及信息化的发展特征及特点。而在实际的应用过程中，技术人员只需要对深度学习（即神经网络）的训练机制进行设计，便可实现自动检测网络漏洞的目标。不过，要想真正地利用深度学习系统开展计算机网络漏洞评估和检测工作，首先需要明确几点应用原则。

3.1 深度学习下的网络漏洞评估原则

首先，怎样表示程序。因为深度学习是以数据向量作为“标准输入”的，因此需要将程序转变为相应的计算机向量。然而这种转变不能太过随意，需要根据相应的原则进行转换。即先将程序或软件转化为能够保存“语义关系”的计算机“中间表达态”。随后将这个表达态转变为特定的向量表达态，使其成为深度学习的实际输入。其次，明确合适的粒度。如果要想检测程序或计算机系统是否存在相应的网络漏洞，技术人员需要明确网络漏洞的具体位置，因此需要用相应的粒度对其进行评估和监测。在这个过程中，需要以合适的计算机粒度作为单元，而非特定的函数或程序。最后，确定神经网络。通常来讲，神经网络在语言识别、音频识别及图像处理等层面上，拥有较为显著的优势。而在网络漏洞评估层面上，要想确定相应的代码或程序是否存在网络漏洞，则需要结合上下环境，选择合适的深度学习系统（神经网络系统）来评估网络漏洞。

3.2 深度学习下的网络漏洞评估的方法

首先界定 code gadget（代码工具）。通常来讲 code gadget 是由很多语句构成的，在控制依赖和数据依赖层面上存在着明显的正相关性。因此要想形成良好的 code gadget。需要深入分析 key point 的理论内涵。key point 主要指由于错误使用所形成的网络漏洞函数。然而需要明确的是，相同类型的网络漏洞在实际测试或评估中，很可能产生形式多样、内容不同的 key point。而相同的 key point 可能存在于多种不同类型的网络漏洞中。因此，技术人员在利用 code gadget 生成数据流时，需要特别注意这个问题。其次，神经网络的学习阶段。网络安全管理人员需要在神经网络学习阶段，提取相应的系统程序切片或 API 函数切片，以此生成相应的训练命令及事实标签（即用 label 方式，使 1 表示计算机系统存在漏洞，使 0 表示计算机应用系统不存在漏洞），随后将 code gadget 变为标准的“向量表达”，进而开始实现神经网络的自动化训练。最后，在训练阶段，即将目标系统、程序或网络转变为向量 W 与 code gadgets，利用已经训练完毕的模型对其进行测试。此外，为评估深度学习的有效性和实效性，则需要选取大量含有网络漏洞的计算机系统、程序、代码进行评估。而在评估软件程序时，技术人员需要根据学习阶段的基本原则，生成多个 Gadget，将其分别应用到计算机深度学习检测和训练的过程中。而针对资源管理和缓冲器漏洞，则需要应用 VulDeePecker（深度学习网络漏洞评估系统）工具，进行相应的代码审计工作，以此提升深度学习的实效性和有效性。

4 结语

深度学习主要指神经网络机制，能够广泛地应用在图片处理、语音识别、自然语言等层面，拥有智能化、自动化、现代化及信息化的应用优势，将其应用在网络漏洞评估的层面上，能够有效地弥补传统漏洞评估方法所存在的问题，提升网络漏洞评估的精准性、实效性及效率。然而要想真正地发挥深度学习在计算机网络漏洞检测层面的功能和作用，则需要明确深度学习在网络漏洞评估和漏洞检测层面的原则，随后从训练学习与评估测试的角度出发，完善已构建好的深度学习体系，使其实现既定的网络漏洞评估目标。

参考文献：

[1] 范立敏 . 客运专线 CTC 网络安全防御体系的系统组成及功能研究 [J]. 工程建设与设计 ,2017(10):198-199.
[2] 李鑫 , 李京春 , 郑雪峰 , 等 . 一种基于层次分析法的信息系统漏洞量化评估方法 [J]. 计算机科学 ,2012,39(7):58-63.
[3] 李涛 , 李太浩 . GFI LANguard N.S.S 在网络漏洞扫描中的应用 [J]. 农业网络信息 ,2011(1):100-101.
[4] 任晓贤 , 陈洁 , 李晨阳 , 等 . 基于风险矩阵的物联网系统漏洞关联性危害评估 [J]. 信息网络安全 ,2018(11):81-88.

【作者简介】

韩菊（1983—），女，汉族，山西娄烦人，硕士，太原学院讲师，研究方向：计算机网络。

（收稿日期：2020-06-24 修回日期：2020-07-19）