文章编号:1671-4598(2022)06-0017-06 DOI:10.16526/j.cnki.11-4762/tp.2022.06.003 中图分类号:TP37 文献标识码:A

基于机器学习的自动化渗透测试系统技术的研究

牛月坤，曹 慧，田晨雨，李 涛，吴昊天
（国能信息技术有限公司，北京 100011）

摘要：为加强目标系统网络的安全等级，验证目标存在的威胁与漏洞，研究设计出基于机器学习的自动化渗透测试系统，利用多种入侵方法对目标进行自动化渗透测试；针对目标系统的各个网路节点的脆弱性和连接关系生成全局攻击图，计算对攻击目标的攻击路径的攻击价值，自动化生成最优攻击路径；采用多阶段渗透攻击的方法，建立渗透攻击的动态划分模型，利用网络中的漏洞不断接近并攻击目标；模拟企业网络架构进行渗透测试，实验结果显示该研究系统发起渗透攻击的成功率较高，最高达到95.4%，攻击目标主机能够生成最优的攻击路径，攻击价值最高达到27.3。

关键词：机器学习；自动化渗透；网路节点脆弱性；全局攻击图；最优攻击路径；多阶段渗透

Research on Automatic Penetration Testing System Technology Based on Machine Learning

NIU Yuekun, CAO Hui, TIAN Chenyu, LI Tao, WU Haotian
(CHN Energy Information Technology Co., LTD., Beijing 100011, China)

Abstract: In order to strengthen the security level of the target system network and verify the threats and vulnerabilities of the target, an automatic penetration testing system based on machine learning is designed, a variety of intrusion methods are used to to carry out automatic penetration testing on the target. The global attack map is generated based on the vulnerability and connection of each network node of the target system, the attack value of the attack path on the target is calculated, and the optimal attack path is automatically generated. By using the method of the multi-stage infiltration attack, the dynamic partition model of the infiltration attack is established, and the loopholes in the network are used to approach and attack the target. The penetration test was conducted by simulating the enterprise network architecture. The experimental results show that, the success rate of penetration attack launched by this research system is high, up to 95.4%. The target host can generate the optimal attack path, and the attack value is up to 27.3.

Keywords: machine learning; automatic penetration; network node vulnerability; global attack map; optimal attack path; multi-stage infiltration

0 引言

当前许多公司和企业将开发出的应用程序架设在Web平台上，但更多地关注网络和服务器硬件性能，对应用安全的方面关注较少，可能导致Web站点存在安全漏洞，容易受到恶意攻击[1]。自动化渗透测试平台（DAS-APEN-TEST）在很多厂家，通过用自己的规则方法和程序等方式去解释安全问题，通过构建渗透测试平台，实现自动化、立体化的渗透测试系统。现有技术研究背景还基于应用学角度，一切从实际应用出发，通过应用程序提高了渗透测试对系统的逻辑缺陷和技术漏洞分析能力。比如通过发明漏洞检测程序，或者人为在不用位置检测，提高应用能力。但这种技术现状通过非法入侵的调度攻击目标主机获取目标系统的权限，在测试过程中评估系统的网络安全性能，最大限度地探测出系统存在的安全漏洞。但当前的渗透测试的测量效率不高，现有的Fuzzing测试漏洞搜索范围不大，且人工分析成本过高[2]。

针对上述存在的问题，文献[3]系统开发出基于DJANGO的网络渗透测试实验平台，结合了网络爬虫计技术，对获取的资产数据进行扫描和渗透测试。文献[4]系统使用Java语言编写出多方协同的渗透攻击框架，集成了端口转发、socket代理和远程控制木马等功能，包含了攻击链中所需的各种功能模块。文献[5]系统提出基于PENET理论的渗透测试模型，将动态分析法应用到测试中，提高目标设备和系统的安全性。文献[6]系统利用综合分析法建立判断矩阵，对渗透测试的各工具和平台进行

收稿日期:2021-12-09； **修回日期**:2022-01-15。

作者简介:牛月坤(1990-),男,黑龙江哈尔滨人,大学本科,工程师,主要从事等级保护建设、网络安全攻防对抗、漏洞挖掘、全网资产测绘、代码安全及网络架构安全等方向的研究。

引用格式:牛月坤,曹 慧,田晨雨,等.基于机器学习的自动化渗透测试系统技术的研究[J].计算机测量与控制,2022,30(6):17-22,31.

分析，具有多个漏洞利用程序和辅助测试模块，实时更新最新漏洞的利用插件。

上述技术中仍旧存在一些不足，大部分渗透测试工具只能对外网系统的漏洞进行扫描，无法构成自动化的流量信道，因此就需要一种新型的自动化渗透测试系统实现内网及其他主机的安全测试，提高第三方插件测试的自动化程度。

1 系统架构及原理

为全方位检测出系统中存在的安全漏洞和网络脆弱性节点，保证目标系统的网络安全性能，本研究加入机器学习技术建立自动化渗透测试系统，从不同的角度出发，利用各类非法入侵方法对目标系统进行渗透测试，最终输出渗透测试报告。渗透测试原理为通过非法入侵和调度攻击目标主机，获取系统的权限和篡改数据库的数据，在测试过程中对目标系统的网络安全性进行评估，从非法入侵的角度对系统中存在的逻辑缺陷、网路漏洞和系统脆弱节点进行分析，利用各类攻击手段对系统内网和外网进行渗透测试，尽可能的发现系统汇总存在的全部漏洞，最终生成渗透测试报告。本研究基于机器学习的自动化渗透测试系统架构如图 1 所示。

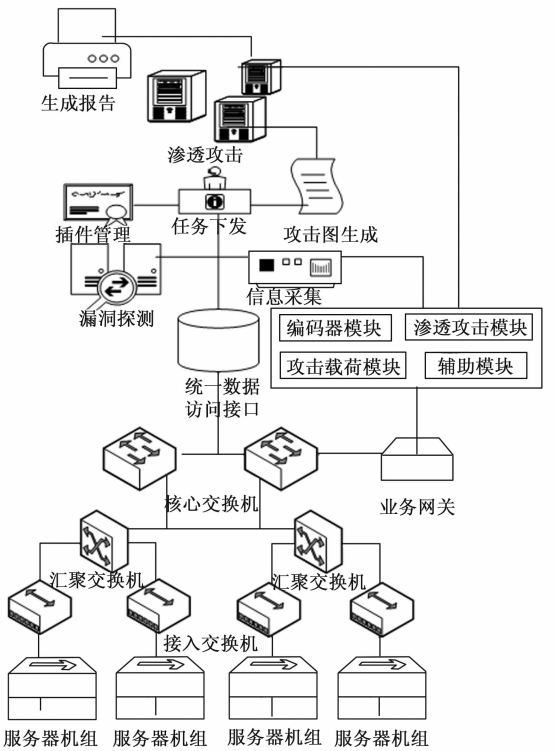

图 1 基于机器学习的自动化渗透测试系统架构

系统原理可以描述为：系统首先根据测试工具和用户需求制定合理的测试方案，确定测试周期、测试权限、测试的业务范围和执行流程，避免对目标系统网络的正常运营造成影响[7]。系统对目标系统进行渗透攻击，利用系统漏洞和部署在系统的攻击载荷获取目标系统的权限和服务器的 ROOT 权限，破坏系统内部逻辑结构，恶意修改系统数据库数据，并避免 IPS、IDS、WAF 等网络安全设备的检测[8]。系统中机器学习模块主要分为攻击负载标注部分和训练学习部分，将攻击测试语句分解为最小分片的测试语句，将绕过 WAF 的攻击测试的标签进行标记，生产具有标签的攻击测试训练集。

本研究系统使用 Metasploit 开源的渗透测试框架，包含了大量针对应用程序、协议、服务和操作系统的漏洞利用代码，当系统确认目标系统存在漏洞时，渗透测试人员可以利用与漏洞相匹配的模块进行攻击。系统包含有多个有效载荷，为测试人员提供一个反弹形 SHELL 接口，可以连接到目标计算机运行测试人员在目标系统上执行操作和指令[9]。系统在进行攻击前，漏洞利用模块对有效载荷进行配置，使用合适的脚本 Metasploit 可以自动化完成整个配置过程，基于 msfconsole、msfgui 和 msfapi 接口完成用户与框架之间的交互[10]。

系统由 OPENVAS 开放漏洞评估提供全面的漏洞扫描和漏洞管理方案，OpenVAS 扫描器定期更新一个网络漏洞测试 NVTs，通过 OpenVAS NVT feed 扫描引擎执行漏洞扫描，将漏洞扫描结果全部整合到漏洞管理器中[11]。系统使用 AUXiliary 辅助模块，包含了对目标系统的攻击场景中的各种脚本，assistantscanner 模块用来破解 SSH 证书，打开一个 msfcon，RHOSTS 选项可以设置扫描器的目标地址。经过机器学习对目标服务器进行分析后得到最佳攻击路径，使用自动化生成攻击脚本进行渗透攻击，将目标系统的反馈消息存储在数据库中。数据库使用 HBase 开源 data 管理模块，为列存储 Nosql 数据库，在 HDFS 上实时读写和快速随机访问数据层的结构化数据。系统客户端包含 Zookeeper 存储 HBase 的元数据，客户端进行读取和写入操作时在 Zookeeper 中访问 meta 元数据。对目标系统完成全面扫描和漏洞检测后，量化渗透攻击的成功率，对于相应的目标服务器和网络系统生成渗透测试报告。系统通过接入第三方用户图表绘制库 ANTV 为用户提供可视化的应用，在图表核心库使用 ANV 作为构建图表的核心部分，应用基于海量图形应用的底层数据引擎，以大量图形数据分析为驱动，提供多种图形应用语义和交互方案，将系统的网络漏洞数、漏洞位置和脆弱节点数量等数据以可视化图形的形式展示。

系统的前端利用 JAVAScript 框架 VUE 构件的 web 用户界面，系统界面具有相应的用户管理模块、情报收集模块、漏洞探测模块、攻击模块和生成报告模块等，用户根据需求进行相应的模块完整测试工作。metasploit 测试工具提供了渗透攻击所需的编码器模块、辅助模块、攻击模块和空指令模块。在获取到目标系统的权限后，对系统进行各种攻击行为，比如降低权限、修改日志文件、删除用户数据、植入后门和运行其他程序等，渗透模块通过 metasploit 接口对接到系统中，通过后渗透攻击脚本 Meterpreter

与目标系统进行会话，执行 Meterpreter 服务端提供的 API。

2　基于攻击图的最优攻击路径自动化生成

一般的攻击图生成过程由渗透测试人员分析得到的，没有实现完全的自动化生成，基于状态转移的攻击图生成方式可能会出现生成环，增加了对攻击路径分析的难度。本研究根据目标系统的各个网路节点的脆弱性和连接关系，利用攻击图生成最优攻击路径。基于攻击图的最优攻击路径自动化生成流程如图 2 所示。

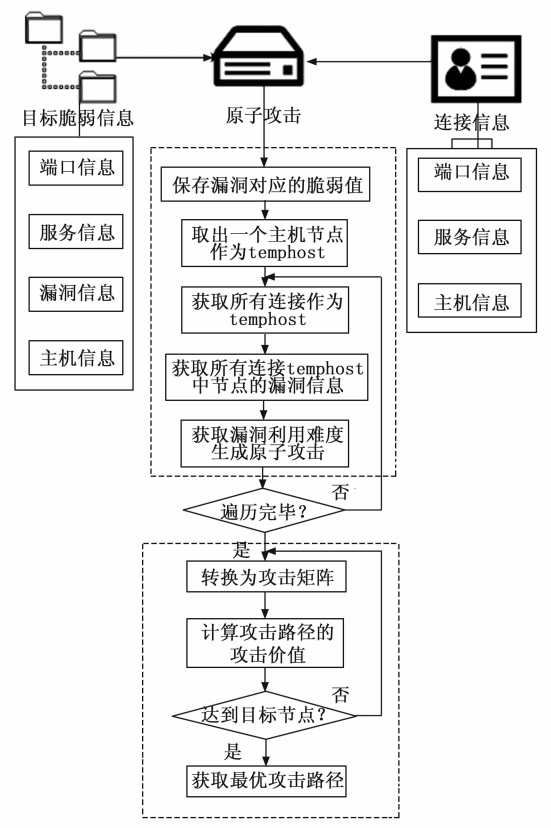

图 2　基于攻击图的最优攻击路径自动化生成流程

生成攻击路径前首先需要获取目标系统的信息，通过网路基扫描工具采集目标系统节点之间的连接关系，获取系统节点的 IP 信息、ARP 表。完成目标系统的信息采集后结合漏洞数据库，根据节点的连接关系分析目标系统的网络架构和拓扑结构，分析出目标系统中节点的脆弱信息。综合目标系统的脆弱节点和连接关系，生成漏洞利用关系，得到目标系统节点之间的原子攻击，原子攻击包括攻击的前提条件、攻击结果和漏洞信息。一次原子攻击作为攻击图的边生成全局攻击图。

对生成的全局攻击图进行分析，生成对目标系统中目标节点的对应攻击路径。为防止生成的全局攻击图存在节点过多、生成攻击环、攻击路径分析难度较大的问题，本研究设计的攻击图模块，网络设备为最小粒度，简化了攻击图，在生成的所有攻击路径中，以网络设备和主机构成攻击节点，使攻击图不会出现环形结构。目标系统中的脆弱节点可以根据攻击路径到下一个目标节点，在复杂的网络结构中不会因为节点数据的增加，导致攻击性能的下降。

在攻击图中，一次实际漏洞利用形成了攻击图中的一条边，表示发生了一次原子攻击：

$$atomicAttack = (vul, peoC, result) \tag{1}$$

其中：vul 表示原子攻击利用的漏洞，peoC 表示攻击的前提条件，result 表示原子攻击产生的后果[12]。

通过公式（1）可以通过数据量化方式表示实际漏洞所形成了攻击图，并将攻击内容通过数据量化的方式表示出来。

原子攻击的前提条件可表示为：

$$peoC = (applyWay, Authority_{src}, Authority_{dst}) \tag{2}$$

其中：applyWay 表示漏洞利用难度，$Authority_{src}$ 表示发起攻击的主机需要获取的最低权限，$Authority_{dst}$ 表示被攻击的主机的最低权限[13]。目标系统网络节点的脆弱性与漏洞利用难度 applyWay 有关，通过原子攻击量化计算，将漏洞和 applyWay 存储在 VulProbility 中。从 Host 中任意取出有关主机节点作为 TempHost，直到所有网络可访问节点遍历完毕[14]。从 HostLink 中获取所有与 TempHost 相关的连接作为 TempLink，从 Hostvul 中获取到所有连接中的节点的漏洞信息，并判断漏洞是否为可达性漏洞。获取漏洞利用难度 applyWay 并生成一个原子攻击，并表示为攻击图中的有向边，重复以上过程直到生成可视化的全局攻击图。

通过上述描述，能够将多种数据信息生成最优攻击路径，在具体应用中，还需考虑到攻击的有效性和可以得到的最大利益，将从漏洞中获取到目标系统的节点信息进行量化，表示为该节点的资产价值 assetValue。第 j 个原子攻击的价值可表示为：

$$attackV_j = (assetValue + Threatvalue)/D \tag{3}$$

其中：$attackV_j$ 为原子攻击的价值，assetValue 为节点的资产价值，Threatvalue 为节点的威胁价值，D 为原子攻击难度。通过式（3）能够实现威胁价值数据信息的计算。

在一次渗透攻击当中攻击路径的攻击价值可表示为：

$$attackWV_j = \Pi_{j=1}^{NB} attackV_j \tag{4}$$

式（4）中，$attackWV_j$ 表示攻击路径的攻击价值，N 表示攻击路径总数，j 表示原子攻击次数。根据全局攻击图转换为攻击矩阵，矩阵中的值表示节点的原子攻击价值，采用深度优先搜索算法，对走过的攻击路径进行编码。对于新的攻击路径判断是否已经到达目标节点，如果达到则更新攻击价值 $attackV_j$，对目标系统中的节点依次尝试，并标记已经走过的路径。路径探索完毕时，选取其中攻击价值 $attackWV_j$ 最大值作为最优路径。通过最优路径，能够实现威胁信息的获取与计量。从目标系统的初始节点到目标节点的攻击路径生成核心代码如下所示：

```
# 保存最大攻击价值
MaxAttackValue = 0
```

```
Book = [0]
def dfs(Cur, Dis, n, AttackMatrix):
"""
:param Cur:当前所在位置
:param Dis:走过的路径
:param n:总节点数
:param AttackMatrix:攻击矩阵
:return:攻击路径信息,包括最大攻击价值和攻击路径
"""
if Cur == n:
if Dis["Val"] >MaxAttackValue:
return Dis
for i in range(1, n + 1):
if AttackMatrix[Cur][i] ! = -1 and Book[i] == 0:
Book[i] = 1
# 继续搜索
Dis["Val"] += AttackMatrix[Cur][i]
Dis["Way"] += "->" + str(i)
dfs(i, Dis)
# 路径探索完毕,取消标记
Book[i] = 0
```

3 威胁驱动的多阶段渗透攻击

随着目标系统的网络节点数和网络结构的复杂程度的提高，进行渗透攻击很难直接与设定的攻击目标直接获取连接。本研究提出威胁驱动的多阶段渗透攻击方法，从外部网络发动紧密的单步攻击不断接近目标系统，最终攻破攻击目标，这种攻击方法持续时间较长且具有明显的阶段性。

渗透攻击者对目标网络进行扫描，对可利用的主机进行定位，使用攻击武器将该主机攻破后在目标网络中占据据点，利用据点对网络内部进行持续探测，进而利用目标网络中的漏洞不断接近并攻击目标。当攻击者具有主机 H1 的 User 权限时，目标网络中主机 H1 与 H2 通过 Http 连接，当主机 H2 上存在远程攻击漏洞 CVE，攻击者能够发动原子攻击 V，攻击后获取主机 H2 的 Root 权限[15]。多阶段渗透攻击如图 3 所示。

多阶段渗透攻击可分为 3 个阶段，准备阶段、利用阶段和攻击阶段。准备阶段作为攻击者的初始节点，攻击者在目标网络中建立节点，为后续的攻击提供基础，对目标网络进行扫描并将可利用的主机标记出来。在准备阶段中定制为该主机的攻击武器，准备完成后将攻击武器投到进行攻击的主机上，攻击目的为完成该主机的入侵控制，控制完成后在目标网络中建立据点。利用阶段利用攻击者在目标网络中占据的节点，接着在目标网络内部进行探测，利用目标网络中的漏洞，不断横向移动以逼近攻击目标。攻击阶段为渗透攻击的最后阶段，攻击者距离目标节点更近，对攻击目标发起攻击，当攻击成功后，目标系统表现

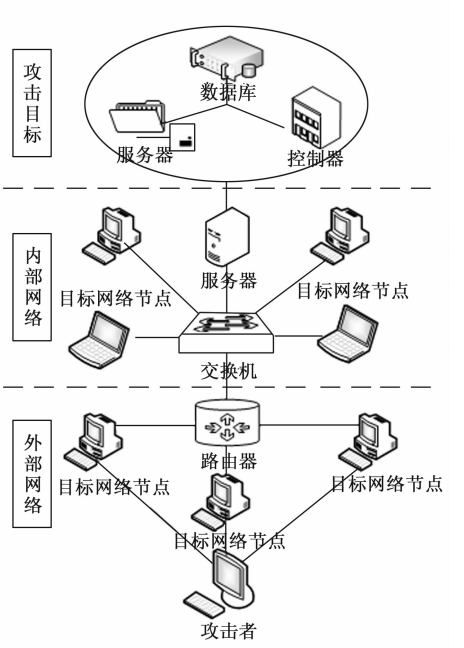

图 3 多阶段渗透攻击

为无法进行正常工作，业务数据被修改，系统无法正常访问，敏感数据被窃取。攻击图用来描述多阶段渗透攻击，多阶段渗透攻击图可表示为：

$$AG=(N,E,K)=(S\bigcup V,S\times V\bigcup V\times S,K) \quad (5)$$

式（5）中，N 表示为目标系统的节点集合，E 表示有向边集合，K 表示状态转移概率集合，S 表示状态节点集合，V 表示原子攻击集合[16]。

由图 3 中的攻击链模型可知，多段渗透攻击从目标系统的外部发起，攻击者逐渐向系统内部靠近攻击目标，攻击者与攻击目标的距离越小，则表示攻击者对目标网络的威胁越大。目标网络节点集合为 $NC=O\cap I\cap G$，由外部网络 O、内部网络 I 和攻击目标 G 组成。能够通过外网直接连接的外部节点构成外部网络，外部节点被攻击后成为据点，攻击目标 G 为攻击的最终目的，一般为系统的控制主机、服务器和数据库等。攻击者在 T_0 发动攻击，并在 T_1、T_2、T_3、T_4、T_5 时刻攻破外部节点和内部节点 $HostA$、$HostB$、$HostC$、$HostD$、$HostE$。已攻破的节点集合为 AS，攻击者不断利用节点漏洞对其他节点进行攻击，在 T_5 时刻，攻击者已攻破的节点集合为 $AS_{T_5}=\{HostA,HostB,HostC,HostD,HostE\}$。攻击者在不同时刻在目标网络中所在的位置也不同，对攻击目标的威胁大小也将动态改变，攻破目标节点的数量越多对目标网络的威胁也越大。威胁驱动的攻击阶段动态划分模型可表示为：

$$AP_T=f(TH_t,TH_{thsh})=\begin{cases}AP_I & \text{if} \quad AS=\Phi\\ AP_M & \text{if} \quad TH_t<TH_{thsh}\\ AP_E & \text{if} \quad TH_t\geqslant TH_{thsh}\end{cases} \quad (6)$$

其中：TH_t 表示攻击者对目标网络的威胁，TH_{thsh} 表示防御者设定的威胁阈值，AP_I 表示渗透攻击初期，AP_M 表示渗透攻击中期，AP_E 表示渗透攻击后期[18]。攻击图模型能够很好反映攻击进程的问题，当前目标网络中的攻击行为有相对宏观的了解，将攻击者对目标网络的威胁融入攻击阶段划分中，能够更好地表示攻击阶段的动态变化。

威胁驱动的攻击阶段动态划分模型能够更好地分析渗透攻击过程中目标系统的漏洞利用关系，和漏洞对目标节点的威胁，使用户可根据攻击特点和攻击进程防御自身网络，可根据实际攻击情况设定威胁阈值 TH_{thsh}，更有利于用户设定灵活的网络安全防御措施。如果防御者修复了受到攻击系统中的所有节点，攻击者将失去占有的据点，返回渗透攻击初期阶段 AP_I。防御者可通过威胁值 TH_t 的变化，直观显示防御手段的效果。

4　应用测试

本研究系统采用前端通用框架实现展示效果，系统界面主要有 IP、端口、扫描方式 3 种参数配置，为渗透攻击提供必要的配置信息。扫描任务指令通过 AJAX 传输方式，获取到界面命令后封装为固定接口格式，将命令传输到服务端的命令解析模块执行。对目标系统完成一次扫描后，在系统界面上显示出目标 IP 和 IP 端多个目标的端口开发情况、Mac 地质和操作系统等信息。系统界面如图 4 所示。

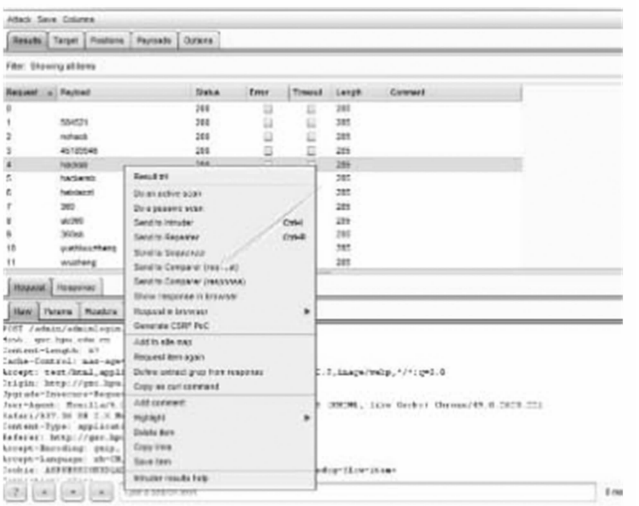

图 4　系统界面

为验证本研究自动化渗透测试系统的可用性，本研究搭建实验环境模拟企业网络架构，并部署存在漏洞的网络节点。实验渗透测试平台采用 Win10 操作系统，利用虚拟机装载 kali-linux-2020-4 系统，在系统上的 metasploit6.0.15 环境下运行。搭建的实验网络结构分为核心区、业务区和开发区，业务区可以通过外网直接进行访问，部分关键业务通过核心交换机进行 NAT 网络转换，开发区主要模拟网络的开发环境，并部署了 3 台虚拟服务器。实验目标系统网络结构如图 5 所示。

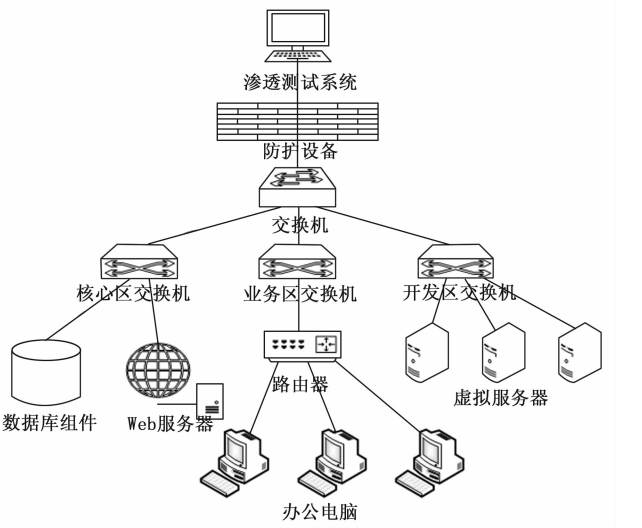

图 5　实验目标系统网络结构

实验环境中各测试机器软硬件配置参数如表 2 所示。

表 2　软硬件配置参数

名称		属性
测试系统	处理器	1.4 GHz Intel Core i5
	安装内存	16 GB 2133 MHz LPDDR3
	硬盘	APPLE SSD 512GB
防护设备	处理器	Intel CPUE5-2673 v3@2.40 GHz
	核心数	48C
	硬盘	250 GB Samsung SSD+2T WD2005FBYZ
	网卡	双千兆网卡
主机	IP	192.168.1.100 192.168.1.101 192.168.1.102
	操作系统	Windows7
	服务类型和版本	Tomcat7.0.0
服务器	IP	192.168.2.100
	操作系统	Ubuntu16.04
	服务类型和版本	Mysql5.7

进行实验前对目标系统网络的各个主机进行扫描，使用 metasploit 框架集成的 nmap 扫描工具，针对主机的 IP 地址常用的端口号执行信息收集任务，得到目标系统的主机信息如表 3 所示。

为验证本研究系统的渗透成功率，在实验环境下攻击者对目标系统进行攻击。目标系统中网络节点交换渗透信息的时间间隔设定为 1 分钟，主机更新渗透信息表。使用本研究系统对目标系统中的网络节点进行渗透攻击，文献[3]系统和文献[4]系统作为对比实验进行测试，渗透测试时间设定为 10 分钟，得到各系统的渗透成功率如图 6 所示，具体数据如表 4 所示。

表 3 主机信息表

主机编号	开发端口	状态	网络协议	服务名
OA1	55	开放	Tcp	Domain
	58	开放	Tcp	http
	91	开放	Tcp	https
OA2	02	开放	Tcp	Domain
	45	开放	Tcp	http
	71	开放	Tcp	https
OA3	11	开放	Tcp	Domain
	20	开放	Tcp	http
	86	开放	Tcp	https

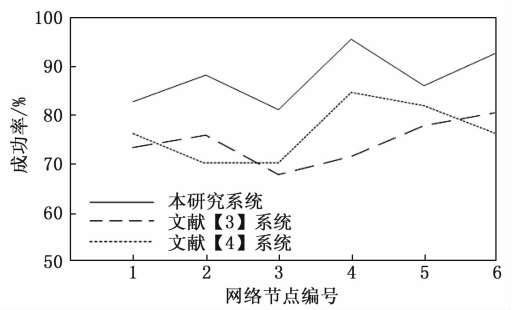

图 6 各系统的渗透成功率

表 4 渗透成功率

网络节点编号	1	2	3	4	5	6
本研究系统	83.5	88.9	82.0	95.4	86.2	93.9
文献[3]系统	74.2	76.4	68.7	72.1	78.5	81.1
文献[4]系统	77.2	70.8	70.6	85.1	82.8	76.2

在对目标系统网络进行渗透攻击过程中，网络节点之间的渗透路径具有多样性，两个网络节点的直接渗透并不一定为最优渗透路径，造成网络节点渗透成功率不一致。本研究渗透测试系统发起渗透攻击的成功率较高，能够将目标系统的网络节点攻破，并利用占据的节点继续对其他网络节点发动攻击，对目标系统各节点的渗透成功率都高于 80%，其中 4 号网络节点的渗透成功率最高达到 95.4%。

文献［3］系统对各网络节点发起渗透攻击，渗透成功率较低，其中 3 号网络节点的渗透成功率最低为 68.7%，对 6 号网络节点的渗透成功率最高达到 81.1%. 文献［4］系统的渗透成功率普遍高于 70%，其中 4 号网络节点的渗透成功率最高达到 85.1%，仍与本研究系统的成功率存在较大的差异。由于存在防火墙等防护设备的原因，识别到目标系统的端口数比实际数量要少，导致渗透攻击过程耗时较长，文献［3］系统和文献［4］系统的渗透成功率较低。

由于攻击节点的不同和与攻击目标的距离不同，导致进行渗透攻击的攻击价值存在一定的差异。使用本研究系统生成全局攻击图，对攻击目标进行渗透攻击，使用公司(4) 计算攻击价值，3 种系统对不同目标主机的攻击价值如图 7 所示，具体数据如表 5 所示。

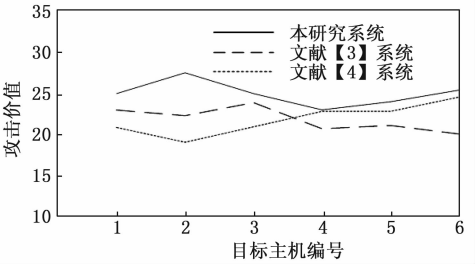

图 7 攻击价值

表 5 攻击价值

目标主机编号	1	2	3	4	5	6
本研究系统	25.0	27.3	25.2	23.4	24.1	25.8
文献[3]系统	23.2	22.6	24.0	20.8	21.5	20.3
文献[4]系统	21.3	19.4	21.6	23.3	23.4	24.9

由于生成的全局攻击图规模较小，对同一目标主机攻击路径可能出现相同的情况，得到的攻击价值相差不大。本研究系统根据目标系统网络结构生成的攻击路径，发起渗透攻击的攻击价值较高，最高达到 27.3，对 4 号目标主机的攻击价值较低为 23.4。文献［3］系统对 6 号目标主机发起渗透攻击的攻击价值最小为 20.3，相对于其他系统的攻击价值较低，文献［3］系统的攻击路径并非为最优攻击路径。文献［4］系统对 4 号、5 号、6 号目标主机的攻击价值与本研究接近，最高达到 24.9，但 1 号、2 号目标主机的攻击价值最低，攻击节点的前置属性节点存在冗余的信息。

5 结束语

本研究基于机器学习技术设计出自动化渗透测试系统，利用网络工具和端口扫描工具收集目标系统网络信息，对目标系统发起渗透攻击，输出渗透测试报告对测试全过程进行总结。本研究的创新点在于：

1）为提出有效的攻击策略，采集目标系统网路的节点脆弱性和连接关系，通过生成全局攻击图得到最优的攻击路径。将目标系统节点的资产和信息进行量化，计算节点的攻击难度和攻击价值，采用深度优先搜索获取最优攻击路径。

2）提出威胁驱动的多阶段渗透攻击方法，建立渗透攻击的动态划分模型，更好地反应攻击进程及攻击者对目标网络的威胁，攻击者反复利用目标网络中多个漏洞，攻破多个网络节点最终实现对网络目标的攻击。

当前网络环境下，系统的威胁和漏洞在不断的演变，在以后研究中还需完善和发展渗透测试方法和测试工具。

参考文献：

[1] 邱春旭，郑荣添，邹 丹，等. 渗透测试在医院信息系统网络安全管理方面的应用探讨［J］. 中国数字医学，2021，16(10)：112－116.

（下转第 31 页）