自动化渗透测试技术思考与展望

Thinking and Prospect of Automated Penetration Testing Technology

杨　飞[1]，周　晗[2]，曹京卫[3]，赵　通[1]，吴　涛[1]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 安徽理工大学，安徽 合肥 230041；3. 中国联合网络通信集团有限公司，北京 100033）

Yang Fei[1], Zhou Han[2], Cao Jingwei[3], Zhao Tong[1], Wu Tao[1]（1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 2. Anhui University of Science and Technology, Hefei 230041, China; 3. China United Network Communications Group Co., Ltd., Beijing 100033, China）

摘　要：

渗透测试能够对目标网络系统的安全进行评估，有效地预防网络攻击，保护目标系统。传统的渗透测试过程依赖专业人员的背景知识，人力和时间开销大。自动化测试通过对目标网络的自动分析，发现并验证其潜在的脆弱性，极大地降低了人工参与的程度。当前的自动化测试主要依赖自动化渗透工具和自动化渗透框架，主流的自动渗透测试工具和框架的实现逻辑各不相同。针对各种渗透工具，论述了多种框架的实现功能和实现逻辑，对比了传统渗透测试和自动化渗透测试的差别，并对渗透测试的发展和未来进行总结和展望。

关键词：渗透测试；自动化渗透测试；渗透测试工具

doi：10.12045/j.issn.1007-3043.2022.09.002

文章编号：1007-3043（2022）09-0005-04

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

Penetration testing can evaluate the security of the target network system, effectively prevent network attacks, and protect the target system. The traditional penetration testing process relies on the background knowledge of professionals, which is costly in manpower and time. Automated testing discovers and verifies the potential vulnerabilities through automatic analysis of the target network, greatly reducing the degree of manual involvement. The current automated testing mainly relies on automated penetration tools and automated penetration frameworks, and the implementation logic of mainstream automated penetration testing tools and frameworks varies. For various penetration tools, the implementation functions and implementation logic of various frameworks are discussed, the differences between traditional penetration testing and automated penetration testing are compared, and the development and future of penetration testing are summarized and prospected.

Keywords：

Penetration testing; Automatic penetration testing; Penetration testing tools

引用格式：杨飞，周晗，曹京卫，等. 自动化渗透测试技术思考与展望[J]. 邮电设计技术，2022(9)：5-8.

1　概述

互联网面临的安全威胁与日俱增，高级可持续攻击的出现使得网络空间的安全问题更加严峻，网络安全防护显得更加重要。传统的网络防护手段仅仅站在防御者的角度，检测网络攻击行为[1]。

渗透测试是一种安全测试和评估的方法，能够从攻击者角度，发现目标系统的安全漏洞以及钓鱼攻击等社会工程学操作的脆弱点[2]。渗透测试所产出的结果都将以报告的形式输出，根据渗透测试报告，有针对性地对网络系统进行完善，提高系统的安全性[3]。

收稿日期：2022-07-15

2　渗透测试

当前各种威胁网络安全事件频发，渗透测试越来越多地被组织和企业用于保障系统和服务的安全。根据渗透测试过程中人工参与程度的不同，可以将渗

透测试分为传统渗透测试和自动化渗透测试。

2.1 传统渗透测试

传统渗透测试技术,主要依赖测试人员借助渗透测试工具。测试人员需要根据自己的经验利用多种方法获取目标系统信息,探索并确定脆弱点,进行漏洞利用和后渗透测试。最后使用报告文档来描述渗透测试的整个流程、分析系统存在的风险点以及提供修复建议。整个过程中对测试人员的经验水平有很强的依赖,对相关知识的掌握有很高的要求,同时渗透操作复杂繁琐,存在大量重复的操作,需要投入较大的时间和人力成本。

2.2 自动化渗透测试

自动化渗透测试在一定程度上克服了传统渗透测试的弊端。自动化渗透测试在整体流程上和传统渗透测试相似,不同点在于自动化渗透测试能够自动分析目标系统所在网络环境,发现并验证目标系统潜在的漏洞点和脆弱性[4]。自动化渗透测试的出现,将安全专家从复杂重复的劳动中解放出来,降低了渗透测试的成本。

2.2.1 自动化渗透测试工具

当前的自动化渗透领域,主要依赖自动化渗透工具。渗透测试领域的专家针对相关技术做了充分的研究和总结,开发出多款自动化渗透测试工具和框架。

APT2是集成在Kali Linux中的一款自动渗透测试工具集。它可以利用NMAP进行扫描,也可以在获取Nexpose、Nessus和NMAP等工具扫描结果的基础上进行渗透测试。在渗透测试过程中,它会自动调用Metasploit、NMAP、SNMPwalk等工具并获取其执行结果,应用到系统运行过程中。还可以进行定向化的安全配置,保护被检测的节点主机安全。

AutoSploit是一款基于Python开发的自动化大规模漏洞利用工具,它可以利用Shodan、Quake或Zoomeye等网络空间搜索引擎来筛选攻击目标,可以选择目标并进行利用[7]。选定攻击目标后,调用Metasploit中的相关模块实现漏洞利用。正常情况下,AutoSploit具备300多种Metasploit基础攻击模块,能够利用它们在各种系统服务、Web应用和IDS、IPS等应用设施上实现代码执行。还可以通过修改相关配置文件来为系统增加其他攻击模块。

渗透测试工具的出现,降低了渗透测试的门槛,同时提高了渗透测试的效率。但是,这些渗透工具存在如下弊端。

a)大多数自动化渗透测试工具的爬虫技术无法解决通用性问题。

b)无法持续进行攻击载荷的更新。

c)对于多种漏洞数据无法综合利用并进行深层次化的攻击。

d)无法整合各个渗透测试模块之间的数据,难以保证全流程渗透测试的精准性。

2.2.2 基于人工智能的自动化渗透测试

随着机器学习和深度学习技术的发展,人工智能技术已经应用于各个领域。智能化、自动化是渗透测试未来的方向。

2.2.2.1 基于网络信息增益的自动化渗透测试

NIG-AP提出了一种基于网络信息增益的自动攻击规划算法[5],实现了攻击路径的自主发现。在该算法中,将渗透测试转换为马尔可夫决策形式,利用网络信息增益引导Agent选择最合适的Actor。

NIG-AP提出了网络信息增益的概念,通过重构强化学习模型,根据网络信息增益来指导攻击路径的发现,不需要先验证网络结构、软件配置等相关信息就可以发现攻击路径,提取渗透测试中必不可少的渗透信息。

a)网络信息增益。渗透测试以攻击者的角度,所采取使目标网络的信息熵最大化的行动,该信息熵由目标主机系统信息熵和网络环境信息熵2个部分组成[6]。其计算公式如下:

$$H(P)=-\sum_{k=1}^{M}\sum_{j=1}^{|p_k|}\left\{p_{kj}\log p_{kj}+\left(1-p_{kj}\right)\log\left(1-p_{kj}\right)\right\}-\sum_{i=1}^{|P_{os}|}p_i\log\left(p_i\right)$$

在给定的网络信息熵的情况下,采用网络信息增益作为评价Agent行为的信号[7],其公式为:

$$\Delta H=H\left(P_{\text{before}}\right)-H\left(P_{\text{after}}\right)$$

$H\left(P_{\text{before}}\right)$为Action前的网络信息熵,$H(P_{\text{after}})$为Action后的网络信息熵。网络信息增益会有3种情况。

(a)在对目标主机进行操作系统识别,端口扫描等行为之后,不确定性并没有消除,此时信息增益是2个概率分布的差值。

(b)目标主机在Action后被控制,信息增益是行动前状态的信息熵。

（c）Action对目标主机的状态没有影响，且Action后概率分布相同，此时信息增益为0。

b）深度强化学习。强化学习是机器学习的一种形式，目标是Agent与Environment的交互中，根据积累的Reward，寻找最优的决策序列[8]，NIG-AP将深度神经网络纳入强化学习，使之变成深度强化学习（DRL）[9]，其网络结构如图1所示。Action的奖励由信息增益和行动成本2个部分组成。相对于原来的恒定奖励，信息增益更加灵活，用于引导Agent选择更好的Action，从而获得更多的累积奖励。设置行动成本是为了限制动作的数量，避免出现无限循环，同时为了引导Agent找到尽可能好的攻击路径。

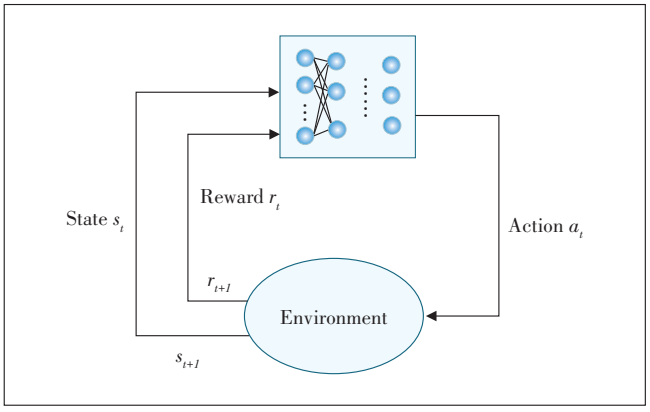

图1　深度强化学习网络结构图

c）基于网络信息增益的自动攻击规划算法。渗透测试过程可以看作马尔科夫决策（Markov Decision Process，MDP）的过程。不同的策略会得到不同的奖励，MDP的目标是找到使得累积奖励最大的最佳策略。

设定主机集合来保存检测到的主机，当集合为空或Agent选择的Action对信息获取没有影响时，会通过扫描来发现新的可用主机。当存在多个影响信息收益的Action时，会选择对累积收益贡献最大的行为，采用蒙特卡罗方法来估计训练阶段的状态转移概率。

2.2.2.2　Deep Exploit

Deep Exploit是一款基于强化学习的自动化渗透框架，其底层调用Metasploit执行渗透测试，采用强化学习（Reinforcement Learning，RL）技术来提升渗透成功率及效率，实现了高度自动化的渗透测试。Deep Exploit与Metasploit之间通过RPC协议通信，通过RPC接口发送指令，接收结果。

A3C（Asynchronous Advantage Actor-critic）是针对Actor-Critic算法的优化算法[10]，引入多线程的处理方式，在每个线程中和环境进行交互学习，把每个线程的学习结果汇总并保存，定期地利用学习结果指导后续和环境的交互学习。Deep Exploit的关键在于A3C算法，由训练和测试2个部分组成。

在训练阶段，Deep Exploit先进行状态空间的初始化，获取可利用模块列表，从中随机选择一个模块。确定状态后，A3C算法会计算每个payload的概率并选择概率最大的payload，调用Metasploit进行漏洞利用。若失败，会随机更换target并选择针对该target的概率最大的payload进行漏洞利用。若达到预先设定的次数仍未成功，Deep Exploit会重新初始化状态空间，选择其他的模块进行尝试。

在测试阶段，Deep Exploit会计算每个状态空间中payload的概率，按照payload概率的大小，依次调用Metasploit尝试漏洞利用，成功之后，则进行后渗透攻击。

2.2.2.3　AutoPentest-DRL

AutoPentest-DRL是一款自动化渗透测试框架，核心思想是利用深度强化学习模型（DRL）智能规划攻击路径，并调用其他渗透工具实现自动化渗透测试。通过构建DQN决策引擎来根据目标网络环境和漏洞信息选择正确的攻击路径。决策引擎接收攻击树的矩阵表示，输出可行性最高的攻击路径。通过拓扑生成器创建网络拓扑，用于提高模型的适应性，同时利用深度优先搜索（DFS）算法简化输入矩阵。

a）攻击树。AutoPentest-DRL利用开源工具MulVAL生成攻击树。根据利用互联网设备搜索引擎Shodan建立的网络拓扑结构，找到所有的攻击路径，并根据所发现的攻击路径构建攻击路径矩阵，然后利用深度优先搜索（DFS）算法优化攻击路径矩阵。

b）DQN。DQN（Deep Q-learning）是Q-learning的进阶版，是将强化学习和深度学习结合的产物，使用经历回放来实现损失函数$\mathcal{L}$的收敛：

$$\mathcal{L}=E\left[\left\|\overbrace{\left(r+\Upsilon\max_{a'}Q\left(s',a'\right)\right)}^{\text{target}}-\overbrace{Q(s,a)}^{\text{predicted}}\right\|^2\right]$$

DQN网络结构如图2所示。

AutoPentest-DRL中，通过DQN的训练得到决策模型，用来选择可行性最大的攻击路径。模型的输入为经过深度优先搜索（DFS）算法优化的攻击路径矩阵，输出为针对该目标的最佳攻击路径。在训练过程

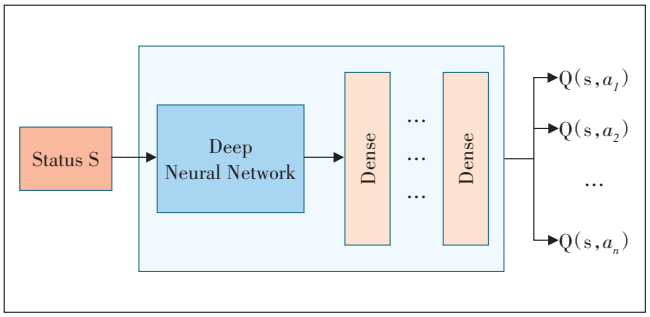

图2 DQN模型的网络结构

中,每个攻击者对应DQN中的一个Agent,攻击者在攻击矩阵中实现状态转移,最终达到攻击树的根节点。

3 传统渗透测试与自动化渗透测试对比

综合上述传统渗透测试和自动化渗透测试,二者对比如表1所示。

表1 传统渗透测试和自动化渗透测试对比

对比项	传统渗透测试	自动化渗透测试
实效性	周期性	持续性
渗透效率	依赖安全测试人员	较高
工作强度	较低	高,可配置
标准化程度	依赖安全测试人员	高
行为可控性	依赖安全测试人员	严格受控
数据可靠性	依赖安全测试人员	严格受控
整体成本	较高	适中

4 自动化渗透测试的总结和展望

传统渗透测试需要渗透测试人员具备各方面的专业知识、熟悉漏洞机理、熟练运用各种安全测试工具。因此,要摆脱渗透测试对人工的依赖,需要不断推进自动化渗透测试技术的发展。

随着人工智能技术的发展,会有更多更成熟的人工智能算法应用到渗透测试的各个阶段中。基于机器学习和深度学习的指纹识别,智能识别测试目标的端口服务、中间件、主机操作系统等指纹信息,能够有效地提高渗透的效率;在渗透攻击阶段,通过知识推理,根据目标的网络环境,智能化选择攻击目标,优先攻击具备高渗透价值的目标,智能化选择最合适的攻击载荷,减少渗透尝试的次数,提高渗透测试的效率。智能化关联漏洞挖掘过程中的漏洞,实现多个漏洞之间的联合利用。针对整个渗透测试过程,通过优先级调度算法对多线程渗透任务的各个线程进行智能网络资源分配,提高渗透效率。相信随着人工智能技术的发展,会使得渗透测试的成功率,自动化程度变得更高。

参考文献:

[1] KRUTZ R L, VINES R D. The CISSP and CAP prep guide: Platinum edition[M]. Hoboken: John Wiley & Sons, 2007.

[2] DIMKOV T, VAN CLEEFF A, PIETERS W, et al. Two methodologies for physical penetration testing using social engineering[C]//Proceedings of the 26th Annual Computer Security Applications Conference. Austin: Association for Computing Machinery, 2010: 399-408.

[3] XIAO Y, WANG Y J, HUANG Z G. Survivability analysis of SOA based on attack tree models[C]//2012 IEEE 14th International Conference on Communication Technology. Chengdu: IEEE, 2012: 819-823.

[4] STEFINKO Y, PISKOZUB A, BANAKH R. Manual and automated penetration testing. Benefits and drawbacks. Modern tendency[C]// 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), 2016: 488-491.

[5] ZHOU T Y, ZANG Y C, ZHU J H, et al. NIG-AP: a new method for automated penetration testing[J]. Frontiers of Information Technology & Electronic Engineering, 2019, 20(9): 1277-1288.

[6] LIANG J Y, SHI Z Z. The information entropy, rough entropy and knowledge granulation in rough set theory[J]. International Journal of Uncertainty Fuzziness and Knowledge-Based Systems, 2004, 12(1): 37-46.

[7] LEE C, LEE G G. Information gain and divergence-based feature selection for machine learning-based text categorization[J]. Information Processing & Management, 2006, 42(1): 155-165.

[8] SUTTON R S, BARTO A G. Reinforcement learning: an introduction [M]. Cambridge: MIT Press, 1998.

[9] MNIH V, KAVUKCUOGLU K, SILVER D, et al. Human-level control through deep reinforcement learning[J]. Nature, 2015, 518 (7540): 529-533.

[10] MNIH V, BADIA A P, MIRZA M, et al. Asynchronous methods for deep reinforcement learning[C]//Proceedings of the 33rd International Conference on International Conference on Machine Learning - Volume 48. New York: JMLR.org, 2016: 1928-1937.

作者简介:
杨飞,毕业于合肥学院,高级工程师,学士,主要从事网络安全技术的研究工作;周晗,毕业于中国科学技术大学,副教授,硕士,主要从事网络安全技术的研究和教学工作;曹京卫,毕业于北京科技大学,高级工程师,学士,主要从事运营商数据网规划运维、网络安全技术研究及安全产品研发运营工作;赵通,毕业于中国农业大学,工程师,主要从事安全产品研究,安全技术研究工作;吴涛,毕业于天津大学,工程师,学士,主要从事IT运维安全管理工作。