Explore-Exploit: 一种模拟真实网络渗透场景的安全竞赛

章 秀[1,2], 刘宝旭[1,2], 龚晓锐[1,2*], 于 磊[1,2], 宋振宇[1,2]

[1]中国科学院信息工程研究所 北京 中国 100093
[2]中国科学院大学网络空间安全学院 北京 中国 100049

摘要 安全竞赛对网络安全领域人才的培养和选拔至关重要, 然而在有限资源条件下如何设计与实现真实度高的竞赛场景是经典难题。本研究围绕着解决该难题的 3 个关键挑战展开。本研究首先将现实世界中的网络渗透场景建模为多步骤、多跳板、多漏洞组合渗透过程; 然后应用攻击图技术对复杂网络信息系统中脆弱点及其关联关系的描述能力进行设计; 最后借助于网络靶场平台的大规模复杂异构网络快速复现能力进行实现。本研究以内网攻防渗透赛的形式展开实验, 取名为 *Explore-Exploit*, 实验中最长的渗透路径包含 4 个跳板机, 组合利用了 3 个漏洞和 1 个服务, 达到了预期的演训效果。相比现有竞赛场景, *Explore-Exploit* 包含更丰富的场景元素, 比如网络拓扑探测、内网横向移动、数据资产发现等, 对真实网络渗透场景的还原度更高。

关键词 真实网络渗透场景; 攻击图技术; 网络靶场; 人才培养; 安全竞赛
中图法分类号 TP309.1 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2020.07.05

Explore-Exploit: A Security Competition Modeling the Real-world Network Penetration Scenario

ZHANG Xiu[1,2], LIU Baoxu[1,2], GONG Xiaorui[1,2*], YU Lei[1,2], SONG Zhenyu[1,2]

[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Security competitions have become increasingly popular events for cultivating and selecting elites in the field of information security. However, how to design a highly realistic scenario under the condition of limited resources is a classic problem. This research revolves around three key challenges in solving this difficult problem. In this paper, we first model the network penetration scenario in the real-world as a multi-step, multi-host infiltration process combined with multiple vulnerabilities. Then the design is performed by making use of attack graph techniques which are capable of describing the dependency between vulnerabilities in a complex network information system. Finally, with the support of a cybersecurity testbed which is born to an experimental platform with the ability to quickly reproduce and reconfigure a large-scale network, we implement the entire design. In this study, the experiment was conducted in the form of an intranet attack-defense network penetration competition, named as *Explore-Exploit*. The longest penetration path in the experiment included four hosts and combined with three vulnerabilities, along with a service, which achieved the motivated goal. Compared to the existing competitions, *Explore-Exploit* contains more elements, such as network topology exploring, intranet lateral movement, data asset discovery and more. It's proved that *Explore-Exploit* is more faithful to the authenticity of the real-world network penetration scenario.

Key words real-world network penetration scenario; attack-graph technique; cybersecurity testbed; talent training; security competition

1 引言

网络空间已成为公认的第五空间[1], 人才是网络安全第一资源[2]。随着我国“互联网+”新经济形态的推进, 社会基础产业全面互联网化, 网络安全成为关乎国计民生的大事。2017 年中国互联网安全

通讯作者: 龚晓锐, 硕士, 正高级工程师, Email: gongxiaorui@iie.ac.cn。
本论文获得中国科学院网络测评技术重点实验室和网络安全防护技术北京市重点实验室资助。获得了北京市科学技术委员会(No.D161100001216001, No.Z161100002616032)课题资助。
收稿日期: 2017-12-19; 修改日期: 2018-04-10; 定稿日期: 2020-06-19

大会提出“万物皆变 人是安全的尺度”[3]。在会上, 针对复杂的网络攻击问题展开讨论, 认为原来用硬件设备和软件构成的、以防护为主的安全体系已经不适用了, 取而代之的是防护系统与安全人员应急处置相结合, 并且人的作用会越来越大。

网络安全领域人才缺口已呈现出井喷趋势, 供求失衡情况下人才的选、育、留成为高校和企业普遍关注的焦点问题。注重动手实践成为网络安全人才培养的核心理念。在多个以“网络安全竞技实战和人才培养”为主题的论坛[4-5]中, 将安全领域的人才分为学院派和极客派, 提出了理论与实践并重, 产学研通力合作, 探索网络空间安全人才培养新模式; 并且通过将网络空间安全学院的教学与同样要求实践的临床医学院教学做对比研究, 提出了“分科理才”的培养理念。全国高校网安联赛(National University Cybersecurity Association, X-NUCA[6])也提出了“寓学于赛, 以赛促学”的理念, 推出“竞赛+”模式。

安全竞赛成为网络安全领域人才培养和选拔的有效手段。夺旗赛(Capture the Flag, CTF)起源于 1996 年的 DEF CON 全球黑帽大会[7], 已经成为全球范围内安全领域受众最广、影响最深远的竞赛范式。夺旗赛以“Flag”(显式的符合一定正则表达式约束的字符串)作为计分依据来设计交互模式, 从而代替之前黑帽们通过互相发起真实攻击进行技术比拼的方式。高质量的夺旗赛中, 题目设计小巧精致, 对技能点的考察十分聚焦, 并且以软件漏洞挖掘、利用、修补为核心考察技能, 却不涉及网络层业务场景相关的环境探测与多跳板组合渗透, 故而在真实性上存在欠缺, 也因此颇受微词。

学术上关于安全竞赛设计和实现的研究, 也主要是基于夺旗赛场景展开。从设计的角度, 以增加趣味性元素为导向, 比如僵尸网络[8]、网络寻宝[8]、黑市洗钱[9]、安卓应用商店[10]等。从实现的角度, 围绕着竞赛系统、靶机部署、题目生成发布了多个开源代码框架, 比如 iCTF[11]、CTF-as-a-Service[12]、NetKotH[13]、SecGen[14]、Labtainer[15]等。但是, 以夺旗赛为主流的竞赛场景在网络业务层的真实性上存在缺失, 针对这个问题, 目前并没有相关研究提出可行方案。

在有限资源条件下设计与实现真实度高的竞赛场景是经典难题, 这面临以下 3 个需要解决的关键问题: (1)从建模的角度, 真实世界中的网络渗透场景复杂多变、时间跨度长, 如何将其关键元素抽象出来, 建模为一个在有限资源条件下、有限时间尺度下可模拟的场景。针对这个问题, 本研究将将现实世界中的网络渗透场景的关键因素抽象为多步骤、多跳板、多漏洞组合渗透过程, 是一个逐步提升控制权限、扩大控制范围的过程。(2)从设计的角度, 要模拟多步骤、多跳板、多漏洞组合渗透, 其场景规模必须足够大, 主机之间、脆弱点之间必须是有关联的。相比现有竞赛场景, 这种新型竞赛场景的设计讲究整体的复杂度和可操作性, 如何将设计想法用一种规范的描述方式来表达, 以方便后续使其从设计模型落实到一个可部署的竞赛场景。针对这个问题, 本研究利用攻击图技术对复杂网络信息系统及其中脆弱点之间关联关系的描述能力进行设计。(3)从实现的角度, 构建一个复杂的竞赛场景, 首先需要大量的物理资源, 比如层级纵深结构的实验网络, 其次需要大量的人力投入, 比如业务漏洞选取和复现, 这本身就提高了此类研究的门槛。针对这个问题, 本研究依托于网络靶场平台, 并借助其大规模复杂异构网络快速复现功能来实现。

本研究以内网攻防渗透赛的形式展开实验, 实验中最长的渗透路径包含 4 个跳板机, 组合利用了 3 个漏洞和 1 个服务, 达到了多步骤、多跳板、多漏洞组合渗透的演训效果。本研究的核心价值在于这种新型竞赛场景的设计和实现是一个“从 0 到 1”的过程, 而不是“从 1 到 n”, 其设计的精细程度和演训达到的效果是前所未有的。

本文结构如下: 第二章是对本文研究要解决的 3 个挑战进行分析, 包括场景真实性、攻击图技术和网络靶场; 第三章介绍 *Explore-Exploit* 的整体设计思想; 第四章讲述应用攻击图技术的竞赛场景设计, 包括内网渗透模型和靶机权重模型; 第五章详细介绍将攻击图设计模型在有限资源条件下实现为基于网络靶场平台的一个竞赛场景, 包括物理拓扑、网络连通、业务漏洞和交互计分; 第六章介绍实验过程, 分析实验结果, 并评估此次实验的真实性; 第七章对本研究进行对比分析, 并讨论研究的可扩展性; 第八章介绍安全竞赛领域的相关研究; 第九章对全文进行总结。

2 背景

2.1 场景真实性

针对本研究要解决的第一个关键问题, 首先定义“真实性”。不论是仿真还是模拟, 在真实性上必定存在折中, 追求绝对的真实性并无意义。本研究将真实性定义为面向演训的真实性, 一个场景的真实

性是允许适度的抽象, 但是这种抽象应该是在抓住关键因素的基础上。而真实性的度量, 是根据演训效果来评估。基于这个定义, 本小节来分析体现一个网络渗透场景真实性的关键因素。

从黑帽视角, 相比传统网络安全事件, 比如病毒感染、蠕虫扩散, 以“震网”[16]事件的披露为代表, 现代网络空间中的攻击表现出一个鲜明的特征: 针对性。针对性攻击的实施需要针对目标网络及信息系统的类型、防御机制, 以及部署的安全设备进行攻击规划, 在攻击进行时通过采集到的信息、状态数据等动态调整攻击策略, 以实现最优的攻击效果。针对性攻击的典型代表是高级持续性威胁(Advanced Persistent Threat, APT), 趋势科技研究人员根据其在各个阶段所表现出来的行为特点, 将其分为6个阶段[17]: 情报收集、突破门户、建立命令和控制通道、横向移动、资产或数据传递、数据外泄, 并且认为横向移动阶段是进一步深入内网的关键。类似的描述模型还有网络杀伤链模型(Cyber Kill Chain, CKC[18]), 敌手战术、技术和通用知识库(Adversary Tactic、Technique and Common Knowledge, ATT&CK[19])。

从白帽视角, 渗透测试是一种模拟攻击者挫败目标系统的安全措施并取得访问控制权的安全测试方法。渗透测试的标准执行流程(Penetration Testing Execution Standard, PTES[20])包含 7 个核心步骤: 前期交互、情报搜集、威胁建模、漏洞分析、渗透攻击、后渗透阶段、报告。对于一次渗透测试, 威胁建模阶段是攻击路径的规划阶段, 探测和分析目标网络主机之间的关联和漏洞之间的关联构成了一个渗透测试的核心。

通过以上分析, 本研究认为体现一个网络渗透场景真实性的关键因素是满足: 从攻击者的起始接入到达成最终目标是一个多步骤、多跳板、多漏洞组合的渗透过程, 是一个逐步提升控制权限、扩大控制范围的过程。设计和实现这样的一个竞赛场景, 网络拓扑必须是复杂的, 脆弱点之间必须是有业务关联的。作为一次安全竞赛来说, 参赛队伍不再是求解一个一个孤立的题目, 而是要想办法发现这些看似孤立的靶机之间的联系, 必须“连点成线”(Connect the dots[21])才能达成此次竞赛的终极目标。

2.2 攻击图技术

针对本研究要解决的第二个关键问题, 需要寻找一种描述复杂网络渗透场景的方法, 该方法能够对复杂网络信息系统进行建模, 并能描述其中存在的脆弱点以及脆弱点之间的关联关系。在网络安全风险评估[22]领域, 为了描述网络信息系统上的脆弱点之间的关联关系, 先后提出了多种描述模型, 比如故障树、攻击树、特权图以及攻击图, 而攻击图技术是该领域发展演化最成熟的产物。

攻击图技术是在对目标网络和攻击者建模的基础上, 根据二者之间的相互作用关系产生攻击图, 以展示攻击者利用目标网络脆弱点实施网络攻击的各种可能的攻击路径。在属性攻击图的研究中, 欧新民教授提出了一个多主机多阶段脆弱性分析引擎(Multi-host, Multi-stage Vulnerability Analysis Language, MulVAL[23-26]), 并开源了相应的攻击图生成工具。该引擎通过定义逻辑原语来描述系统的相关属性以及存在的脆弱点, 并使用逻辑推理分析网络的脆弱性, 具有良好的可扩展性, 适合应用于大规模网络的分析, 在很多科研机构获得了普遍应用。

以 MulVAL 为例, 攻击图作为一种网络安全评估技术, 它的研究流程如下: (1)对目标网络进行建模, 定义描述原语, 包括网络拓扑结构、网络节点之间的可达性、主机的操作系统、应用软件等信息; (2)基于这些原始信息查询漏洞数据库, 或者对目标网络进行漏洞扫描, 找出可能存在的脆弱点或者攻击面, 并结合通用漏洞评价体系(Common Vulnerability Scoring System, CVSS[27])对其进行量化; (3)使用逻辑编程(Programming in Logic, Prolog[28]), 通过原语之间的逻辑来推理, 绘制成攻击图, 通常还伴随着图优化算法, 比如同类节点合并、去掉不可达的分支等; (4)应用图论、概率论、信度理论等方法, 进行数据处理, 得出每个资产在各种假设下可能被攻击的概率。某个资产被攻击概率高就表明从安全防护的角度, 这个资产属于“木桶效应”中亟待补全的那个短板, 故而这个资产的安全防护优先级高。

攻击图技术作为一个网络安全风险评估技术逐渐失去研究热点, 但是 MulVAL 模型定义了一套非常好的原语, 这一系列原语非常适合描述一个多步骤、多跳板、多漏洞组合式网络渗透场景。本研究逆向应用了攻击图技术, 这体现在两个方面: (1)以攻击图为蓝本, 构建网络攻防竞赛场景的上层逻辑模型, 再反向推演出一个满足攻击图描述模型的物理可部署场景; (2)以靶机映射到攻击图中节点的位置, 来影响靶机在网络攻防竞赛场景中的权重。

具体来说, 本研究首先借助攻击图设计出网络攻防竞赛场景的上层故事情节——企业内网渗透模型(参见 4.1 节); 然后以这个模型为原型, 反向推演出来一个满足这个攻击图所描述的可部署场景的物理拓扑图(参见 5.2 节)、约定实验网络中节点的连通性(参见 5.3 节)、复现业务漏洞(参见 5.4 节)和制定交

互计分策略(参见 5.5 节); 最后借助网络靶场的大规模复杂异构网络快速复现能力构建出实验网络; 同时, 在攻击图设计的时候, 约定关键路径节点权重高, 非关键路径节点权重低, 映射到实验网络中的靶机权重模型(参见 4.2 节)。

2.3 网络靶场

针对本研究要解决的第三个关键问题, 需要寻求一个支撑平台, 该平台必须拥有足够的物理资源, 能够支撑一个大规模的复杂网络, 而且, 该平台本身必须拥有很好的隔离性, 可以在其中开展攻防实验而不用担心破坏真实运营系统。网络靶场是信息安全领域人才演训的完美平台。因此, 本研究选定网络靶场作为研究的支撑平台。

近年来, 以美国国家网络靶场(National Cyber Range, NCR[29])为代表, 世界各国纷纷启动国家网络靶场建设项目。国家网络靶场是面向各类用户、涵盖各领域各行业典型应用的、军民结合的科研与实验保障环境, 具有网络空间安全体系规划论证、网络安全攻击防御技术演示验证和体系化安全性评估等能力[30]。在学术界, 也称为空间安全测试床(Testbed[31]), 以防御技术实验研究项目(DEfense Technology Experimental Research, DETER[32])为代表。

国家网络靶场[33]作为支撑网络空间安全技术演示验证、网络工具研制试验、攻防对抗演训和网络风险评估分析的重要场所。在国家网络靶场的建设过程中, 将对靶场建设和运行过程中涉及的网络复现、多维度测试、靶场资源动态管理等一系列关键技术进行研究和突破, 具体包括: 复杂异构网络快速复现技术、网络空间安全自动化多维度测试技术、面向任务的靶场引擎构建技术、靶场资源自动配置和快速释放技术、非易失性存储数据安全擦除技术、靶场安全隔离和受控交换技术、木马及其攻击行为识别技术、网络追踪溯源技术等。

按照文献[30]中的定义, 本研究所依赖的网络靶场平台属于第三时期的虚实结合的综合型网络空间靶场。本次实验主要依托于该网络靶场平台的一项必备功能——大规模复杂异构网络快速复现。

3 *Explore-Exploit*

相比现有的安全竞赛场景, 本研究所提出的新型竞赛场景旨在模拟真实网络攻击中多步骤、多跳板、多漏洞组合渗透的过程。从参赛队伍的起始接入到达成最终目标, 需要利用多个脆弱点, 需要发现其间的关联关系, 需要想办法“连点成线”。这种新型竞赛场景的特点体现在四个方面: 靶机环境模拟、网络拓扑、计分依据和博弈策略。

在靶机环境模拟上, 这种新型竞赛场景旨在模拟真实的目标对象的网络环境, 所以靶机数量会大大增加, 靶机上植入的漏洞种类会更加丰富, 靶机上的脆弱性服务或者应用程序会更加接近真实的信息系统, 通常是针对特定真实业务系统中漏洞的复现, 而且靶机之间的关联会更加密切, 讲究的是业务逻辑的复杂度和交互的合理性, 而区别于夺旗赛中的小巧精致。在数量众多的靶机中, 只有一个靶机上面驻留着重要的数据资产, 作为竞赛的终极目标主机, 需要参赛队伍去寻找和识别。

在网络拓扑上, 这种新型竞赛场景会构建出层级纵深的网络结构, 每一个靶机会被赋予一个新的属性——网络位置。一个靶机的网络位置属性直接影响这个靶机在竞赛场景中的网络连通性。参赛队伍的初始接入网段和目标主机所在的网段之间, 需要跨越多个网段, 才能实现网络访问。对应于文献[17]的 6 个阶段描述模型, 层级纵深的网络结构可以培养和考察参赛队伍建立通道和横向移动的能力, 这是当前的安全竞赛场景所不能满足的。

在计分依据上, 对比传统“Flag”形式的计分依据, 本研究选取靶机控制权为计分依据。反思现代攻击, 不论攻击者的目标是信息窃取还是系统破坏, 只要攻击者能够获得目标系统足够高的控制权限就可以随心所欲地实施下一步攻击。所以在这种新型竞赛场景中, 以操作系统的最高控制权(System 权限或者 Root 权限)为计分依据。而且, 从安全竞赛计分的角度, 控制权本身是一个明确可度量的指标。

在博弈策略上面, 这种新型竞赛场景引入了一个新的概念——攻击收益, 即描述一个靶机被成功控制之后, 参赛队伍可以获得的除了得分之外的收益。在多跳攻击中, 攻击者发起每一次攻击需要具备一些前置条件, 而攻击成功之后可能会获得一些新的后置条件, 比如基于这个靶机带来的网络访问权限、靶机上存留的敏感信息等。攻击收益属性是参赛队伍“连点成线”的重要线索或辅助, 这也是当前的安全竞赛场景所不具备的设计元素。

在这种新型竞赛场景中, 演训任务之间不再是孤立的, 而是互相之间有着业务关联, 参赛队伍需要发现这些看似孤立的任务之间的关联, 通过网络上的多跳访问, 借助多个跳板靶机, 逐步提升控制权, 并扩大控制范围, 以最终实现对远程目标的控制。并且, 在多个参赛队伍参与的情况下, 参赛队伍之间不得不互相争夺关键攻击路径上的靶机控制

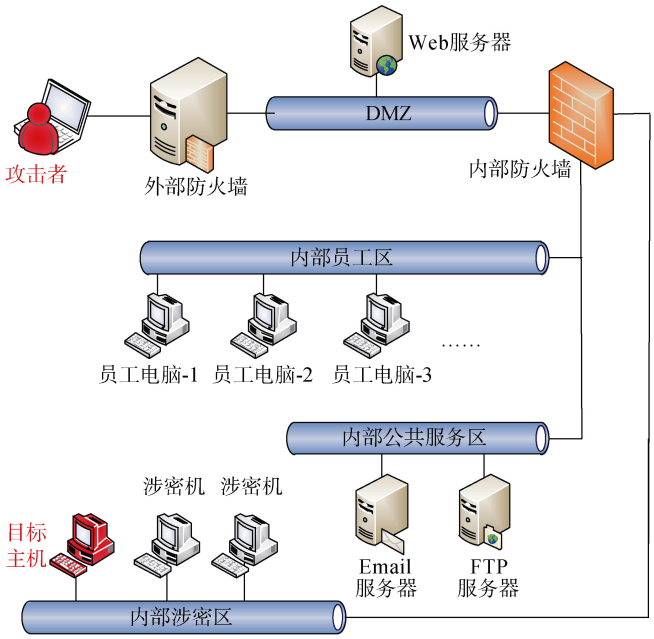
权。这种新型安全竞赛取名为 *Explore-Exploit*, 是网络探索和漏洞利用(*Network Exploring & Vulnerability Exploiting*)的缩写。该命名借鉴博弈论理论中的多臂老虎机问题, 对未知特征空间的采样称为探索, 利用探索的结果开展更为有效的行动称为利用。

4 场景设计

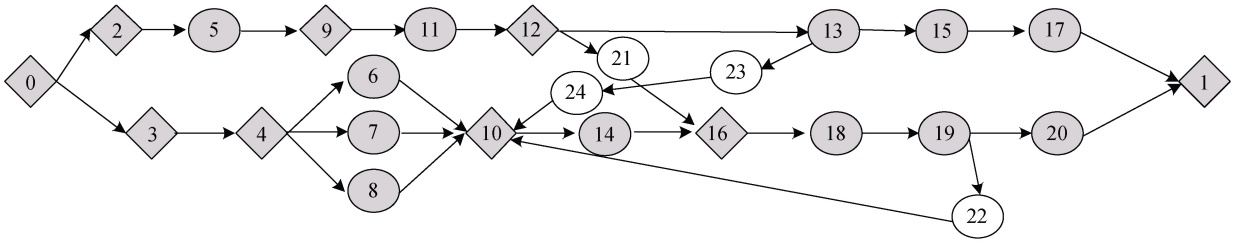
4.1 内网渗透模型

如图 1 所示, 参考文献[25]中的攻击图示例, 应用 MulVAL 定义的描述原语, 本研究建立了一个典型的企业内网渗透模型: 外部网络攻击者想办法突破企业边界防火墙, 通过内网游走和横向移动, 逐步提升控制权限, 并且扩大控制范围, 从而潜入内网深处, 最终达成在特定的目标机器上窃取重要数据资产的目的。在图 1 中, 对于每一种原语, 选取其第一次出现作为例子予以解释, 其余部分可以参照理解。

该内网渗透模型假设外部攻击者初始获得了两个企业内网的访问入口: (1)位于非军事化区域



0. 攻击者接入 (Intranet)
1. 代码执行 (目标主机, Administrator权限)
2. 直接网络访问 (Web服务器)
3. 直接网络访问 (内部员工区)
4. 网络连接 (员工电脑-1, 员工电脑-2, 员工电脑-3)
5. 远程漏洞利用 (Web服务器, 服务漏洞)
6. 远程漏洞利用 (员工电脑-1, 操作系统漏洞)
7. 远程漏洞利用 (员工电脑-2, 网络服务漏洞)
8. 弱口令破解 (员工电脑-3, 远程访问服务)
9. 代码执行 (Web服务器, 非Root/Administrator权限)
10. 代码执行 (员工电脑, Root/Administrator权限)
11. 本地提权漏洞利用 (Web服务器, 操作系统漏洞)
12. 代码执行 (Web服务器, Root/Administrator权限)
13. 攻击行为 (Web服务器, 构建恶意链接)
14. 攻击行为 (员工电脑, 部署网络跳板)
15. 受害者 (目标主机, 点击恶意链接)
16. 多跳网络访问 (FTP服务器)
17. 远程漏洞利用 (目标主机, 浏览器及其插件漏洞)
18. 配置缺陷利用 (FTP服务器, 访问控制策略)
19. 攻击行为 (FTP服务器, 上传木马)
20. 受害者 (目标主机, 下载并执行木马程序)
21. 攻击行为 (Web服务器, 部署网络跳板)
22. 受害者 (员工电脑, 下载并执行木马程序)
23. 受害者 (员工电脑, 点击恶意链接)
24. 远程漏洞利用 (员工电脑, 浏览器及其插件漏洞)



原语解释:
0. 攻击者接入–攻击者获得了一个初始立足点;
1. 代码执行 (目标主机, Administrator) -攻击者获得了在目标主机以管理员特权执行命令的权限;
2. 直接网络访问 (Web服务器) –攻击者可以直接访问Web服务器;
4. 网络连接 (员工电脑) -员工电脑组成一个局域网, 彼此之间可以直接访问;
5. 远程漏洞利用 (Web服务器, 服务漏洞) –Web服务器上存在服务漏洞, 攻击者可以利用这个漏洞发起远程利用;
8. 弱口令破解 (员工电脑-3, 远程访问服务) -员工电脑-3开启了远程访问服务并且使用弱口令, 攻击者可以爆破弱口令, 实现远程访问;
11. 本地提权漏洞利用 (Web服务器, 操作系统漏洞) -Web服务器操作系统存在本地提权漏洞, 攻击者可以利用这个漏洞, 实现权限提升;
13. 攻击行为 (Web服务器, 构建恶意链接) -攻击者在Web服务器上植入恶意链接;
15. 受害者 (目标主机, 点击恶意链接) -使用目标主机的受害者点击了攻击者植入的恶意链接;
16. 多跳网络访问 (FTP服务器) -攻击者本不具备访问FTP服务器的权限, 却通过部署网络跳板, 实现了对FTP服务器的访问;
18. 配置缺陷利用 (FTP服务器, 访问控制策略) -FTP服务器的访问控制策略配置存在缺陷, 可被攻击者利用;

菱形 - 在当前条件下获得的客观条件、情报、信息
椭圆形 - 攻击者发动的攻击或者受害者进行的恶意操作

图 1 利用攻击图技术建立的内网渗透模型

Figure 1 Intranet Penetration Model by Using Attack Graph Techniques

(Demilitarized Zone, DMZ)的 Web 服务器作为企业的门户网站, 外部攻击者可以通过网络直接访问; (2)私有公共服务区(FTP 服务器和 Email 服务器)部署着这个企业的私有公共服务, 这些私有公共服务对企业内部主机开放访问, 外部攻击者初始可以网络访问内部员工区。

该内网渗透模型假设外部攻击者有两条渗透目标主机的攻击路径。因为目标主机只访问该企业的门户网站和私有公共服务, 所以只能: (1)通过 Web 服务器, 采用网页挂马的方式, 利用目标主机上的浏览器漏洞植入远控后门; (2)借助于 FTP 服务器或 Email 服务器, 采用木马植入或邮件钓鱼的方式, 利用目标主机上的客户端应用程序植入远控后门。

为了使攻击图直观上更加清晰, 在图中区分标记了深色节点和浅色节点, 来显示攻击路径上可能存在的回溯, 在语义上二者没有差别。深色节点构成两条明晰的攻击路径, 表达了外部攻击者从获得初始接入权限开始, 以目标主机为导向, 沿着一条无回溯的路径, 逐步探索前进, 直至获得目标主机的最高控制权限, 这是最符合预期的理想情况。浅色节点表达外部攻击者在渗透过程中可能产生的回溯, 具体来说, 攻击者利用已经取得的成果, 反过去渗透之前尚不具备渗透条件的靶机, 这其实更加符合实际情况, 因为攻击者在寻找目标主机的过程中需要花费不少精力在网络探索和横向移动上。

4.2 靶机权重模型

基于指标体系的分析方法主要以专家评议法(The Delphi Method[34])和层次分析法(Analytic Hierarchy Process, AHP[35])为主。专家评议法旨在形成领域专家对具体问题的共识, 而层次分析法旨在构造权重判断矩阵以得到权重量化数值。

应用以上方法, 本研究构建的靶机权重模型如图 2 所示。准则层分为两个维度: 基本评价和攻击图评价。基本评价描述靶机作为一个独立个体其本身的属性, 包括三个子准则: 攻击收益、网络位置和漏洞利用难度。攻击图评价描述靶机之间的关联关系, 包括两个子准则: 不可缺失性和资源竞争性。靶机之间的关系, 来源于攻击图(图 1)中节点和实验网络物理拓扑图(图 3)中靶机之间的映射关系。攻击图评价是从靶机是否映射为攻击图中的关键路径节点的角度, 赋予靶机不同的权重。

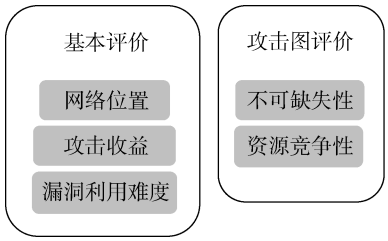


图 2 靶机权重模型

Figure 2 Gamebox Weight Model

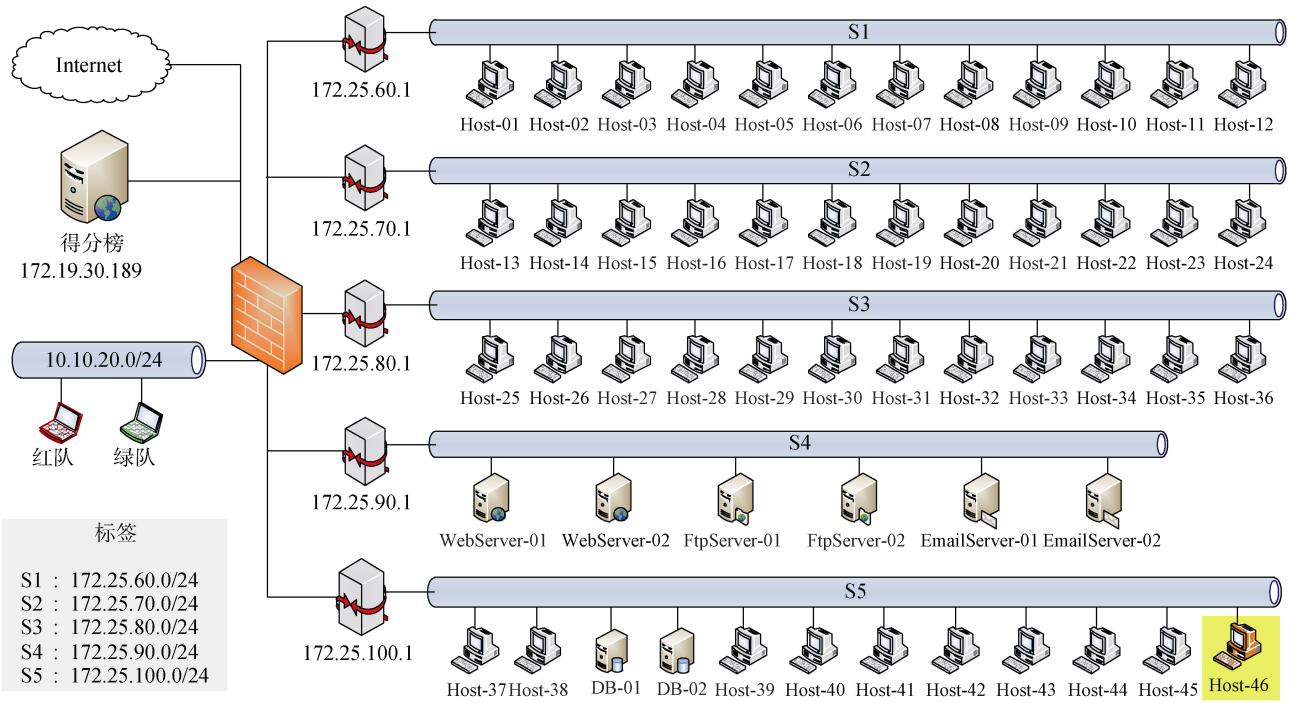


图 3 内网渗透模型对应的物理拓扑图

Figure 3 Physical Topology corresponding with Intranet Penetration Model

漏洞利用难度是靶机的固有属性, 攻击收益属性和网络位置属性可参考第三章理解。不可缺失性属性描述靶机映射到攻击图中的节点, 属于关键路径节点, 即攻击者从起始接入到控制目标主机需要借助多个跳板节点, 该节点属于其中一个不可缺失的跳板。比如, 参照图 1, 攻击者有多个途径渗透普通员工电脑(图中 6.7.8 节点), 却必须通过 Web 服务器或者 FTP 服务器才可能有机会访问到目标主机(图中 17.20 节点), 所以 Web 服务器和 FTP 服务器的不可缺失性指标权重就高于普通员工电脑。资源竞争性是描述实验网络中因为同一角色的资源数量不同, 带来的资源竞争属性, 这种竞争属性通常是设计者故意为之, 用来增加攻防演训的对抗强度。比如, 不管有多少参赛队伍, 目标主机却只有一个, 故而在整个实验网络中, 目标主机的资源竞争性指标权重最高。

5 竞赛实现

5.1 有限资源

此次实验有 5 个物理服务器, 以桥接模式模拟出 5 个网段, 共计 54 个虚拟机, 构成实验网络; 1 个防火墙, 设置基于 IP 的访问控制, 来实现靶机的网络位置属性和层级纵深的实验网络结构; 1 个 Web 服务器运行得分榜, 展示竞赛的实时进展; 2 支参赛队伍, 红队和绿队。此次实验的时间为 72 个小时。

5.2 物理拓扑

图 3 为在有限资源条件下映射攻击图设计模型到网络靶场可部署场景的物理拓扑图。防火墙左边为支撑网络, 提供参赛队伍的接入和展示得分进展。防火墙右边为实验网络, 实验网络是一个和因特网隔离的封闭网络, 这是网络靶场的固有特性。对比图 1 和图 3, 实验网络共有结构相似的 3 个内部员工区(*S1, S2, S3*); 合并了 DMZ 和私有公共服务区为 1 个公共服务区(*S4*), 部署有 Web 服务器、FTP 服务器、Email 服务器; 1 个隐藏的内部隔离区(*S5*), 驻留有目标主机, 目标主机在图 3 中用黄色背景标出, 位于图 3 的右下角。

5.3 网络连通

表 1 采用有向图可达矩阵的方式来表达参赛队伍和实验网络中各元素的连通性, 描述如下: (1)实验网络是一个和因特网物理隔离的封闭网络; (2)实验网络中位于同一个网段的靶机构成总线型局域网, 彼此可以直接访问; (3)实验网络共有 3 个互相连通的内部员工区(*S1, S2, S3*); (4)实验网络中的所有靶机都可以访问公共服务区(*S4*), 包括 Web 服务器、FTP 服务器、Email 服务器; (5)目标主机在内网最深处的内部隔离域(*S5*); (6)参赛队伍可访问因特网和得分榜; (7)红队和绿队分别接入实验网络的两个内部员工区(*S1, S2*), 作为初始访问入口; (8)*WebServer-01/ WebServer-02* 作为企业门户, 是参赛队伍的另一个初始访问入口。

表 1 网络连通性的可达矩阵表示

Table 1 Network Accessibility Represented in Reachable Matrix

	*S*1	*S*2	*S*3	*S*5	Web 服务器	FTP 服务器	Email 服务器	得分榜	互联网
红队	1				1			1	1
绿队		1			1			1	1
*S*1	1	1	1		1	1	1		
*S*2	1	1	1		1	1	1		
S3	1	1	1		1	1	1		
*S*5				1	1	1	1		

5.4 业务漏洞

表 2 为实验网络中复现的业务漏洞的类型及描述, 按照操作系统、Web 应用平台、网络服务和客户端应用程序分为四大类。涉及的漏洞类型包括远程代码执行、本地权限提升、Java 反序列化、PHP Web 组件漏洞、未授权访问、配置缺陷、弱口令等。

依据每一个靶机上的一个确认可以被利用的漏洞为一个计数基本单位, 统计了实验网络中实际复现的漏洞数量, 并计算了它们的百分比, 如表 3 所示。实验网络中复现漏洞共计 93 个, 平均每个靶机上包含的漏洞数量为 1.72, 因为单一漏洞往往不能达到获取系统最高权限的利用效果, 需要组合多个漏洞, 比如 PHP 组件漏洞结合操作系统提权漏洞。

5.5 交互计分

计分模式上, 以靶机控制权替代传统基于“Flag”的计分依据。基于靶机权重模型, 每一个靶机初始被赋予一定的权重, 随着竞赛的进行, 如果参赛队伍能够获得这个靶机的控制权, 就获得和这个靶机权重等值的分值。如果一方参赛队伍对已经控制的靶机没有做好防护, 致使靶机的控制权被另一方参赛队伍接管, 则这个靶机对应的分值也会发生转移。此次内网攻防渗透赛设有专业裁判组, 采用人工方式对得分进行审计。

表 2 复现的业务漏洞类型和详细描述信息

Table 2 Description of Operational Vulnerabilities Reproduced in Experimental Environment

漏洞类型(根据漏洞所影响的软件类型)			描述或者 CVE 编号
操作系统	Windows XP	SMB	远程代码执行漏洞, MS08-067
	Ubuntu	OverlayFS 组件	本地权限提升漏洞, CVE-2015-1328
Web 应用平台	Java	Jboss	Java 反序列化漏洞
	PHP	Joomla, phpStudy, Discuz!, phpFile-Manager, ComsenzEXP	PHP 系列组件漏洞, 可以用来上传 Webshell
网络服务	数据库	Redis, MySQL	未授权访问或者认证绕过
	远程访问	SSH, Telnet, RDP	弱口令暴力破解
	文件共享	FTP, Samba, SVN	配置缺陷(用户组和权限设置不当)
客户端应用程序	文档阅读器	Microsoft Office 2013	CVE-2014-4114(沙虫漏洞)
		Adobe Acrobat Reader	CVE-2011-2462
	浏览器及插件	Internet Explorer 8	CVE-2014-6332
		Adobe Flash Player	CVE-2015-5119
		Mozilla Firefox	CVE-2011-2110
	设备管理器	WebGate eDVR Manager	CVE-2015-2098

6 实验评估

6.1 关键过程

此次内网攻防渗透赛过程中, 得分榜截图如图 4 所示。得分榜基于 ECharts[36]的模拟迁徙图实现, 表达参赛队伍从起点开始, 在实验环境的每一次攻击所控制的靶机, 这些靶机连在一起呈现出一条明显的攻击路径。从图 4 中可以看到, 从某些靶机延展出来很多出边, 如 *Host-15*, 表示这些靶机发挥着非常重要的跳板作用。本小节选取四个体现了这种新型竞赛场景的核心设计理念的环节来详细介绍:

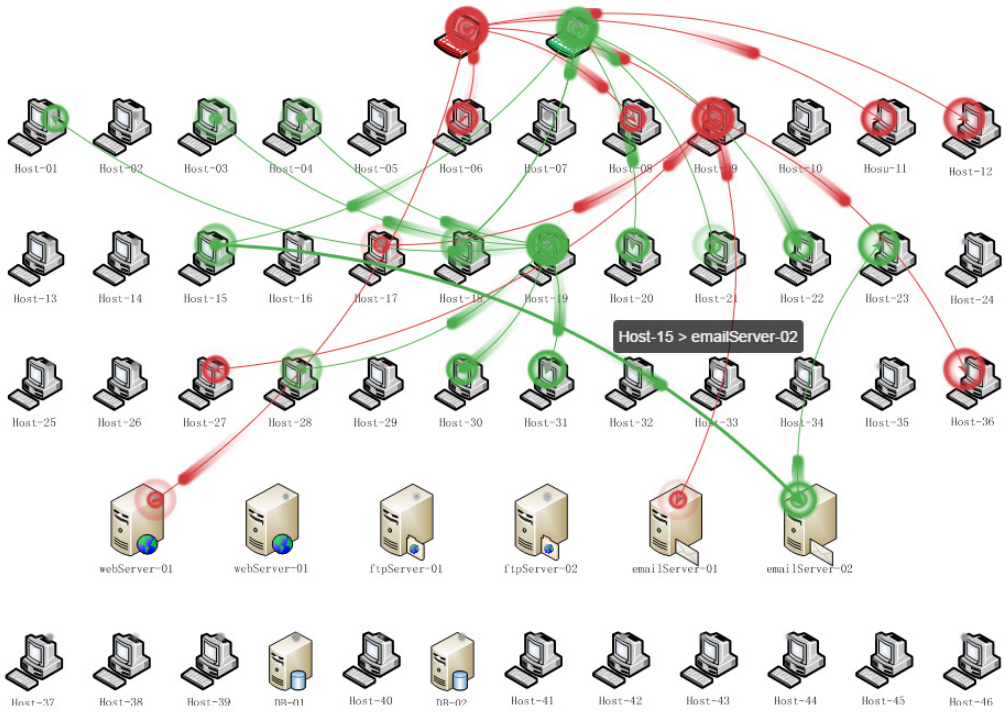


图 4 *Explore-Exploit* 得分榜截图

Figure 4 Screenshot of Scoreboard during *Explore-Exploit*

(1) 网络探索: 弱口令破解

红队成员发现了靶机 *Host-11* 上面开放着 22 号端口, 这是一个 OpenSSH 服务。通过常用密码字典暴力破解, 建立起来一个有效的 SSH 会话。红队成

员猜测, 这可能是实验网络初始化部署时使用的一个默认口令, 所以就用这个口令去尝试所有能够探测到的远程访问服务, 包括 OpenSSH 服务、Telnet 服务和远程桌面服务。这一次大胆的猜测和尝试, 让红队一举控制了实验网络中的 8 个靶机。因为规则禁止修改靶机的用户名和密码, 所以红队在控制这些靶机之后, 通过设置 IPtables 来从网络上只允许红队成员的设备可以连接, 以达到了防御的目的。

(2) 漏洞利用: 上传 Webshell

红队成员过扫描发现 *Host-06* 靶机上开放着数据库服务端口 3306, 然后尝试渗透 phpMyAdmin(一个让管理者可以使用 Web 接口管理 MySQL 数据库的工具), 成功地获得了数据库部分权限。然后上传了一个木马 red.php 到 C:/WWW/目录, 并通过下面的 SQL 查询语句执行它:

select '<?php @ eval(\$_POST[pass]);?)'
INFO OUTFILE 'C:/WWW/red.php'

从而成功地建立起来 Webshell。PHP Webshell 将会拥有和运行 PHP 进程同样的用户特权, 在 *Host-06* 这个实例中, PHP 是由用户 nt authority system 启动运行的, 所以红队成员就获取了 *Host-06* 最高控制权。在另一个实例 *Host-08* 中, PHP 进程是由 www-data 用户启动运行的, 所以还必须利用 Ubuntu 系统漏洞(CVE-2015-1328)来提升权限。红队成员通过注释首页相关的 html 代码来达到防御的目的。

(3) 横向移动: 跳板技术

绿队另辟蹊径, 开始从系统漏洞角度寻找突破。绿队成员发现了部分靶机的操作系统版本信息显示是 Windows XP English, 还在这些靶机上发现了开放的 445 端口。对于接触过 Metasploit 框架的人来说, 一个臭名昭著的漏洞, 编号 MS08-067 几乎出现在了所有渗透测试入门教程上。所以, 绿队成员就尝试利用这个系统漏洞, 成功建立起来了 meterpreter 远程控制会话。之后, 绿队成员尝试在实验网络中寻找尽可能多的具有同种漏洞的靶机来放大这一次探索成功的收益。绿队成员使用同样的方法控制了在同一网段(*S2*)的另外 3 个靶机, 并且利用跳板技术(Pivoting), 以靶机 *Host-19* 为跳板, 通过 autoroute 命令添加数据包转发路由, 实现从网段 *S2* 访问到了另外两个网段 *S1* 和 *S3*, 并在使用同样的方法控制了另外 6 台靶机。表现在图 4 中, 就是上面 3 层靶机间密集的绿色曲线。

(4) 资产发现: 攻击收益

攻击收益是参赛队伍在成功控制靶机之后, 在这个靶机上发现的进一步可利用的数据资产, 即后渗透价值。在图 4 中, 一个典型示例是一条明显的绿色曲线, 它从 *emailServer-02* 反弹到上层的靶机 *Host-23*。绿队成员绕过了这个 *emailServer-02* 因为用户组和权限的缺陷配置所带来的认证问题, 然后又利用其系统组件漏洞提权, 完全控制了这台靶机。之后, 绿队成员发现了一个可用的 FTP 服务, 于是在本地生成了一个针对 Windows 的木马, 将其上传到该 FTP 的公共目录, 等待可能的 FTP 客户端在同步文件的时候下载木马, 进一步运行该程序而被植入木马。靶机 *Host-23*, 同步了目录并且执行了这个恶意程序。在木马运行起来的一瞬间, 一条反向的 TCP 控制会话就建立起来了。这里, *emailServer-02* 发挥了一个非常好的跳板作用, 这种污染软件供应链的跳板与转发网络数据包的跳板是不同类型的攻击收益。

6.2 结果分析

实验网络中共有 54 个靶机, 在结束时有 24 个靶机被控制, 比例为 46%, 进展十分可观。图 5 统计了不同类型的操作系统部署和被控制的情况。表 3 统计了各种类型的漏洞复现和被利用的数量与比例。根据统计数据, 对实验过程分析如下:

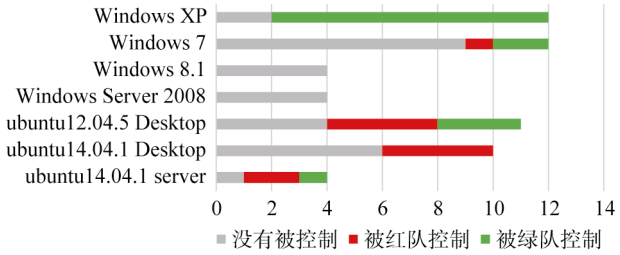


图 5 靶机部署数量和被控制情况

Figure 5 Statistics of Gamebox Deployed and Compromised

(1) 操作系统服务组件漏洞, 允许远程代码执行的靶机是最容易被控制的。在扫描了操作系统指纹信息和开放服务之后, 这种漏洞非常容易被识别出来, 而且通常可以在渗透测试框架中找到现成可用的利用模块。

(2) PHP 组件中的脆弱点, 尤其是那些可以用来上传 Webshell 的漏洞, 从而非常方便地建立起控制信道。因为 Webshell 能够获得的权限是和运行 PHP 进程的权限是一致的。所以如果用户限制了 PHP 的权限, 这类漏洞要达到完全控制的目的, 通常还需要进一步利用靶机上的操作系统本地权限提升漏洞。

(3) 两个复现有 Java 反序列化漏洞的 Jboss 服务器都没有被渗透成功。因为在竞赛进行时, 这个漏洞

是最近披露出来的漏洞, 尚没有发布可用的漏洞利用代码。红队队员已经识别了这个漏洞, 他们在这里尝试了许久没有获得成功。这也从间接佐证了漏洞概念验证(Proof of concept)和漏洞被实际利用之间存在着很大的距离。

(4) 网络服务漏洞利用同样是控制靶机的一个非常便捷的通道。对于缺陷配置漏洞的利用, 需要攻击者对这种服务器的配置有足够的了解, 这样可以不断地构建恶意请求, 通过服务器的返回信息来识别潜在的配置缺陷, 从而达到某种未授权访问或认证绕过的目的。登录口令作为一个特殊的类别, 仍然是一个容易被突破的薄弱环节。

表 3 复现漏洞的数量和比例、被利用漏洞的数量和比例

Table 3 Statistics of Operational Vulnerabilities Reproduced and Exploited

漏洞类型		复现数量	复现比例/%	利用数量	利用比例/%
操作系统	Windows XP, MS08-067, 远程代码执行	12	22	10	80
	Ubuntu, CVE-2015-1328, 本地提权漏洞	22	41	2	5
web 应用平台	Java 反序列化漏洞	2	4	0	0
	PHP Web 组件漏洞	6	11	4	67
网络服务	数据库服务未授权访问或认证绕过	2	4	1	50
	远程访问服务弱口令暴力破解	15	28	8	53
	文件共享服务配置缺陷	2	4	1	50
客户端应用程序		32	59	0	0
合计		93	172	26	48

表 4 *Explore-Exploit* 的属性分析

Table 4 Attribute Analysis of *Explore-Exploit*

	面向对象	接入方式	有无交互	博弈模式	场景类型	参赛者角色	面向领域
CGC	机器	线下赛	有交互模式	攻防模式	夺旗赛	攻防双方	传统网络安全
DEF CON CTF Qualifiers	人	线上赛	无交互模式	解题模式		对等关系	
iCTF 2017							
DEF CON CTF Final 2016			有交互模式	攻防模式		攻防双方	
Pwn2Own		线下赛	无交互模式	面向攻击的模式	破解赛	攻击者	
CDX				面向防御的模式	防御赛	防御者	工控系统
CPS_CDC							
GeekPwn				面向攻击的模式	破解赛	攻击者	智能生活设备
DEF CON Social Engineering CTF		N/A①	N/A	N/A	N/A	N/A	N/A
Explore-Exploit		线下赛	有交互模式	攻防模式	渗透赛	攻防双方	传统网络安全

① “INA”是“Not Applicable”的缩写, 表示此属性在此处不适用。

表 5 *Explore-Exploit* 的技能分析

Table 5 Skill Analysis of *Explore-Exploit*

	自动化攻防	程序分析和逆向	漏洞挖掘和利用	Web 渗透	密码学	数字取证和审计	系统管理和防护	社会工程学	环境探测	漏洞关联和适配
CGC	★★★	★	★							
iCTF2017 DEF CON CTF Final	★	★★	★★	★★	★★	★★	★			
DEF CON CTF Qualifiers		★★	★★	★★	★★	★				
Pwn2Own / GeekPwn		★★★	★★★							
CDX / CPS_CDC		★				★★★	★★★			
DEF CON Social Engineering CTF								★★★		
Explore-Exploit			★	★		★	★		★★★	★★★

(5) 客户端应用程序漏洞都没有被利用, 因为实验网络中缺乏漏洞触发操作, 比如浏览器漏洞需要点击恶意链接触发。这需要用到网络靶场的虚拟用户模拟服务, 是此次实验的局限。

分析实验过程可以发现红队更加擅长 Web 服务漏洞利用, 而绿队则更擅长系统组件服务漏洞利用。

6.3 真实性评估

本实验所构建的企业内网渗透模型, 具备层级纵深的网络结构和复杂的业务交互, 允许参赛队伍构建更长的攻击链: 网络探测、路径规划、横向移动、远程控制等, 这是当前的安全竞赛场景所不能满足的。

本实验过程中出现了两种类型的跳板, 一种是借助靶机的网络位置优势, 将其转化为一个网络数据包转发节点, 实现向深层次的网段进一步渗透。另一种是利用靶机上开放的服务, 污染软件供应链的上游以达到在客户端植入木马的目的。这两种类型的跳板, 体现了两种不同的攻击收益, 也是当前的竞赛场景中所没有的。

从演训效果看, 本实验中最长的攻击路径包含 4 个跳板机, 利用了 3 个漏洞(弱口令、配置缺陷、本地提权)和 1 个服务(FTP 服务), 达到了多步骤、多跳板、多漏洞组合渗透的演训效果, 示例如下:

GreenTeam → Host-15 → emailServer-02 → Host-23

因此, 相比现有竞赛场景, *Explore-Exploit* 对真实网络渗透场景的还原度更高。

7 分析讨论

7.1 对比分析

在文献[37]中, 选取了 9 个典型竞赛实例, 对其进行了全面的分析, 建立了一套描述安全竞赛的规范。本文在其基础上, 讨论以模拟攻防双方、多步骤、多跳板、多漏洞组合渗透为目标的内网攻防渗透赛的设计和实现方法。根据文献[37]中定义的安全竞赛的描述方法, *Explore-Exploit* 对应的分类属性如表 4 所示, 其所覆盖的技能维度标定如表 5 所示。

现有的竞赛场景考察的技能主要有: (1)自动化攻防[38], 用程序来驱动计算机, 从而代替人去完成相应的工作, 包括自动化分析、补丁、漏洞扫描、服务维护和适应性调整及网络防御; (2)程序分析和逆向, 针对各类操作系统上的可执行文件、各类硬件平台上的固件代码, 通过对抗加解密、反调试和代码混淆, 以理解其程序逻辑; (3)漏洞挖掘和利用, 针对软件或者信息系统中的“0-day”漏洞进行挖掘, 绕过系统安全机制, 实现控制流、数据流攻击, 或逻辑漏洞利用; (4)Web 渗透, 基于对 Web 通信机制、编程语言及框架的特性、服务器端漏洞模式等的深入理解, 针对 Web 服务进行漏洞探测和利用, 主要包括结构化查询语句注入(Structured Query Language injection, SQli)、跨站脚本攻击(Cross Site Scripting, XSS)、客户端跨站请求伪造(Cross-Site Request Forgery, CSRF)等; (5)密码学, 对加密算法的破解和对加密信息的还原, 包括古典密码和现代密码; (6)数字取证和审计, 广义的图片、音频或嵌套压缩包中的隐藏数据提取, 磁盘、内存或网络流量中的攻击发现等; (7)网络管理和策略, 对当前网络环境的运营状况和防御部署有敏锐的洞察力, 并能够对网络入侵做出快速地服务维护和应急处置; (8)社会工程学[39], 通过与他人合法地交流, 来使其心理受到影响, 以致做出某些动作或者透露某些机密信息。

相比现有竞赛场景, *Explore-Exploit* 的设计理念讲究的是真实大规模复杂业务系统的还原, 而不是“精心设计的脆弱性”(Vulnerable-by-design[40]), 故而引进了 2 个新的技能维度: (9)环境探测, 通过网络扫描, 去发现网络中的活跃主机, 对其进行信息枚举, 包括它的 IP、操作系统、开放端口、系统或服务或应用程序中的脆弱点、与网络中其他主机间可能存在的交互等, 从而完成网络拓扑还原和攻击面建模; (10)漏洞关联和适配, 基于自身对漏洞知识的储备, 通过环境探测得到的信息, 能够迅速检索出可能存在的“1-day”漏洞, 并且能够根据目标环境对公开的漏洞利用模块进行适配性修改, 以实现漏洞利用。

7.2 扩展性讨论

美国国家网络安全教育倡议组织(National Initiative for Cybersecurity Education, NICE)提出了网络安全劳动力框架(NICE Cybersecurity Workforce Framework, NCWF[41])。该框架用知识-技能-能力(Knowledge-Skill-Abilities, KSA)来描述人才角色。文献[42]进一步提出了 KSA 立方模型, 如图 6 所示, 该模型定义了认知的 3 个维度: (1)知识, 对一个概念、策略或者流程的理解, 用理解的深度来度量知识, 从浅到深; (2)技能, 运用知识来达到预期目的可靠性, 用发挥的可靠程度来度量技能, 从不一致到一致; (3)能力, 用技能从一个领域转移到另一个领域的程度来度量能力, 从窄到宽。

参照这个框架反观当前的安全教育, 本研究认为: (1)知识是对基本原理、方法、流程的理解和掌握, 比如密码学原理、IDA Pro 调试方法、渗透测试标准

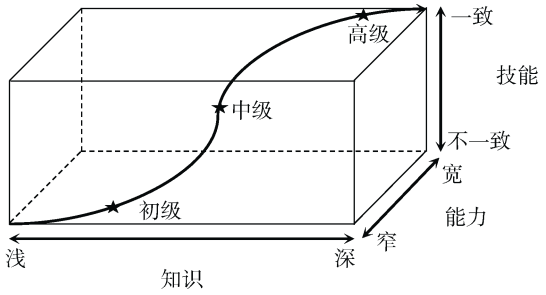


图 6　知识-技能-能力立方模型

Figure 6　Competency Box of Knowledge-Skill-Abilities

流程等, 传统的理论教学可以解决知识层面的传授; (2)技能是运用知识和经验执行一定活动来达成预期目标, 比如程序分析和逆向、漏洞挖掘和利用、Web 渗透等; 夺旗赛通过出题人的精心设计, 每一个题目考察明确的技能点, 故而频繁参加夺旗赛可以牢固地掌握特定技能; (3)能力是运用已有技能解决变化环境中的不确定问题, 比如通过利用社会工程学、网络钓鱼、水坑攻击等方法突破目标门户, 利用 Rootkit 技术长期驻留, 利用域名系统(Domain Name System, DNS)协议报文实现隐蔽的命令与控制(Command and Control, C&C)等。要提升人才的能力, 注重的是提升人才面对动态复杂情景时, 对特定技能的领域迁移能力, 考察的是一个全局的、动态的、“连点成线”的决策能力, 而这就是 *Explore-Exploit* 有望解决的问题。

8　相关工作

(1) 竞赛场景

主流竞赛场景包括三类: 夺旗赛, 破解赛和防御赛。夺旗赛作为经典的竞赛形式, 以网站 CTFtime[43]为依据, 2019 年记录在册的夺旗赛共有 197 场次, 共有 24563 支参赛队伍。夺旗赛分为解题模式和攻防模式。夺旗赛中每一个题目出题意图明确, 考察的技能点十分具体, 非常适合安全领域的新手入门, 并通过反复练习达到精通。

破解赛要求参赛队伍展示“0-day”漏洞利用, 更像是安全极客的炫技平台, 其典型代表是 Pwn2Own[44]。Pwn2Own 的破解对象是由全球著名的信息科技公司的安全团队倾力打造的安全体系, 比如系统提权、沙箱逃逸等。而这两年逐渐获得关注的 GeekPwn[45]则是面向智能家居设备, 比如摄像头、智能锁、保险柜等。

防御赛中, 参赛队伍扮演防御者角色, 起源于网络空间防御赛(Cyber Defense Exercise, CDX[46])。此类竞赛将参与者角色定义为白、灰、红、蓝四方。白方是竞赛组织方, 灰方是扮演正常网络用户的志愿者, 红方是扮演攻击者的志愿者, 蓝方是扮演网络管理员的参赛队伍。此类竞赛考察的是参赛队伍洞察网络安全形势和制定安全策略抵御攻击的能力。因为 CDX 仅面向美国军事学院, 所以发展出面向美国高中生的网络空间爱国者(CyberPatriot[47])和面向美国大学生的网络空间防御联赛 NCCDC (National Collegiate Cyber Defense Competitions[48])。在 2016 年, 作为 CDX 的姊妹篇, 出现了针对网络物联设备的防御赛(Cyber-Physical System based Cyber Defense Competition, CPS_CDC[49]), 其面向领域已经从传统网络安全扩展至电力、运输、交通、航空、水利等关乎国计民生的基础工控设施。

网络渗透赛, 作为一个新的模式在近几年开始出现。2017 年美国发起了全国大学生渗透测试比赛(Collegiate Penetration Testing Competition, CPTC), 并整理发布了一个公开数据集[50]。文献[51]考虑现有竞赛不涉及网络渗透中的安装植入和网络跳板环节, 以这两个点为核心设计了一例网络渗透赛。

(2) 竞赛设计

在竞赛设计上, 新的竞赛元素被不断引入, 以增加竞赛的趣味性。iCTF 自 2003 年到 2013 年, 设计了 11 个独立的竞赛主题[11], 比如 2008 年的网络寻宝场景[8], 2009 年的僵尸网络场景[8], 2011 年的黑市洗钱场景[9]。MIT/LL CTF[10]结合安卓应用商店来设计攻防模式的夺旗赛。文献[52]引入蜜罐来向计算机学院的学生传授网络欺骗相关知识 PicoCTF[53]用特定的故事线来串联起来一系列安全相关的题目。

人工智能(Artificial Intelligence, AI)的元素也逐渐被引入到竞赛的设计模式中。在 2016 年美国国防高级研究计划局(Defense Advanced Research Projects Agency, DARPA)组织网络安全挑战赛(Cyber Grand Challenge, CGC[54])首次引入网络安全领域的机器人大战。而紧随其后的 DEF CON CTF 2017 决赛则首次引入网络安全领域的人机大战。国内也在 2017 年尝试组织第一届机器人网络安全大赛(Robot Hacking Game, RHG[55])。

除了竞赛设计本身的创新之外, 围绕着对设计的评估也有相关研究。文献[56]提出了一种评估夺旗赛的方法, 以指导参赛选手更好的选择适合自己的竞赛。文献[57]从“游戏平衡(Game Balance)”的角度出发, 考虑通过匹配参赛选手水平和题目难度来提高新手的参与度, 降低新手一开始的沮丧感。

(3) 竞赛实现

在2014年, Giovanni Vigna教授总结自己组织十年 iCTF 的经验, 开源了攻防模式的夺旗赛竞赛系统[11]; 在2017年该团队又发布了另一个攻防模式的夺旗赛竞赛系统 CTF-as-a-Service[12], 这个新系统是基于亚马逊云平台的, 实现了攻防模式夺旗赛的在线接入形式, 并且该服务使得举办一个大规模的攻防模式夺旗赛变得更加简单和轻量。

区别于发布一个功能完整的夺旗赛竞赛系统, NetKotH[13](Network King of the Hill, 通俗解释为"网络空间的占山为王"), 是一个计分引擎(Scorebot), 该引擎需要安装在每一个靶机上, 参赛队伍在渗透靶机之后, 在特定位置写入自己的身份标识, 计分引擎监视该位置, 负责向中心服务器报靶。该计分引擎, 需要结合安全社区的开源靶机一起使用, 比如知名社区 Vulnhub[40], 其发布有400多个封装好的靶机镜像, 可供离线下载使用。

不同于此类封装好的黑盒子靶机, Metasploitable 3[58]实现了一种"零件集成式"靶机生成方案, 该方法基于多种跨平台虚拟化技术和软件包管理工具, 用户只需要定义操作系统、应用软件、配置文件等一系列零件信息并提供源文件, 由该框架完成零件的组装。Metasploit 漏洞服务模拟器(Metasploit Vulnerable Service Emulator[59])从漏洞服务模拟的角度来构建虚拟漏洞。该方法通过模拟漏洞服务, 在交互上满足一个真实漏洞存在的交互特征, 来使攻击者以为漏洞真实存在。其好处在于, 使得漏洞的复现可以脱离该漏洞依赖的外部物理环境, 比如操作系统、应用软件、配置文件等。

SecGen[14]实现了一种随机靶机环境生成方法, 该方法中"随机"体现在用户只需要按照需求定义配置意图, 比如漏洞种类, 然后框架会从漏洞库随机中选择满足需求的漏洞。Labtainers[15]提出了一种基于容器(Docker)的靶机部署方案, 相比以上几种方案, 使用容器最大好处就是提升了部署速度。同样是基于容器, 安全社区 Vulhub[60]复现了大量的网络服务漏洞环境。

文献[61]提出了自动问题生成技术(Automatic Problem Generation, APG), 同一个题目却有不同的变种, 因此有不完全相同的求解脚本。使用该方法可以针对同一个技能点进行反复练习, 而且在实际比赛环境中可以规避多个参赛队伍之间剽窃"Flag"的问题。

(4) 安全教育和人才培养

为了更好的普及基本的安全概念、知识、策略、威胁模型等, 产出了一波以安全教育元素为主题内容的游戏, 比如纸牌游戏 Control-Alt-Hack[62-63], Elevation of Privilege[64], 电子游戏[xd0x3d!][65]、CyberCIEGE[66]、SecurityEmpire[67]等。而文献[68]则是基于"狼人"游戏的在线场景展开, 学生使用命令行环境来发现泄露的信息流, 以侧信道的方式来识别"狼人"。

因为传统夺旗赛题目的技能点过度集中, 解题难度大, 而且注重解题技巧而脱离了真实业务实践, 故而不适合新手学习, 所以学术界提出了一个新的概念——"泛夺旗赛"(Class CTF, CCTF[69]), 其讲究更加轻量、更加常态化、更加接近于实际网络安全业务实践的题目设计, 对新手更加友好。

由雪城大学杜文亮教授发起的安全教育项目(Hands-on Labs for SEcurity EDucation, SEED[70-71]), 作为信息安全学科的课堂教学动手实验, 被世界范围内成千上百个高校采用。该项目构建了非常全面的知识体系, 提供6个类别超过30个威胁模型的动手实验室, 比如针对最近英特尔芯片漏洞发布的"融化"攻击实验室(Meltdown Attack Lab)和"幽灵"攻击实验室(Specter Attack Lab)。

国内i春秋[72]平台, 以"培育信息时代的安全感"为理念, 其闪电实验室模块紧跟最新安全动向, 针对最新披露的安全漏洞或安全事件, 提供在线验证环境以供学习实践。自2016年底至今, 该平台已发布的在线验证环境接近70个。

(5) 竞赛促进安全领域研究

除了以安全人才培养和选拔为初衷的安全竞赛之外, 也存在一类安全竞赛, 以"游戏化"(Gamification[73])的思想来解决特定领域的科学问题, 比如软件开发-破解-修复竞赛(Build it Break it Fix it Contest, BiBiFi[74-76])。BiBiFi竞赛分为三个阶段, 参赛队伍首先完成特定功能软件的开发构建, 然后互相挖掘其它参赛队伍所开发的软件中的漏洞, 即破解, 最后对漏洞进行修复。通过这样一个过程, 研究在软件开发过程中哪些因素有助于构建一个更加安全的软件。

安全竞赛也促进了特定领域的安全问题研究, 比如机器人自动化攻防赛 CGC, 极大地促进了自动化程序分析和漏洞利用领域的研究。其决赛第三名Shellphish团队及其核心成员根据参赛经验先后发表Angr[77](一个整合静态分析和动态符号执行技术的二进制分析工具)、Driller[78](一个结合模糊测试和选择性符号执行以挖掘更深层次的软件漏洞的工具)、HaCRS[79](一个以工具自动化为核心的、人辅助决策的二进制程序分析推理系统)、ShellSwap[80](一个基

于捕获的远程利用中的网络攻击流量来实现攻击载荷自动迁移的工具)等。

安全竞赛产生的数据集也可以用来做进一步的科学实验, 比如追踪溯源、攻击发现等。文献[81]使用 DEF CON 的网络流量数据来研究网络攻击的追踪溯源。另外, 在 DARPA 组织的一次针对 APT 攻击模拟的竞赛中, 参赛队伍扮演攻击方, 文献[82]的研究作为该竞赛的一个后端支撑模块, 该模块利用污点传播的方法实时重建攻击场景, 来对竞赛过程中参赛队伍的攻击效能进行评估。

9 总结

本文研究了在有限资源条件下设计与实现真实度高的网络攻防竞赛场景要解决的 3 个关键问题: 建模、设计与实现。实验中最长的渗透路径包含 4 个跳板机, 组合利用了 3 个漏洞和 1 个服务, 达到了多步骤、多跳板、多漏洞组合渗透的演训效果。相比现有竞赛场景, *Explore-Exploit* 包含更丰富的场景元素, 比如网络拓扑探测、内网横向移动、数据资产发现等, 对真实网络渗透场景的还原度更高。从网络安全领域人才培养和选拔角度, *Explore-Exploit* 能够考察其在动态复杂环境下的技能迁移能力和“连点成线”的全局决策能力, 因此对网络安全人才的综合能力培养和选拔是非常有意义的。

致　谢　本论文获得中国科学院网络测评技术重点实验室和网络安全防护技术北京市重点实验室资助。获得了北京市科学技术委员会 D161100001216001, Z161100002616032 课题资助。同时, 在此向作为主要参赛队员参与本研究实验的王奥辉、赵建军、王琰、吴炜等同学表示感谢, 向给文章提出宝贵修改建议的评审专家表示感谢。

参考文献

[1] Department of defense strategy for operating in cyberspace.www.defense.gov/news/d20110714cyber.pdf, 2011.

[2] Opinions on Strengthening Cyber Security Discipline Construction and Talent Training. http://www.moe.edu.cn/srcsite/A08/s7056/201607/t20160707_271098.html.

[3] China Internet security Conference. http://isc.360.cn/2017/index.html, 2017.

[4] Capital Cyber Security Day. http://special.btime.com/sdwlaq2016.shtml, 2016.

[5] China Cybersecurity Week. http://www.cac.gov.cn/2016wlaqz/, Sep, 2016.

[6] X-NUCA. http://xnuca.erangelab.com/.

[7] A history of Capture the Flag at DEFCON. https://www.defcon.org/html/links/dc-ctf-history.html.

[8] Childers N, Boe B, Cavallaro L, et al. Organizing Large Scale Hacking Competitions[M]. Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010: 132-152.

[9] Shoshitaishvili Y, Invernizzi L, Doupe A, et al. Do You Feel Lucky?: A Large-scale Analysis of Risk-rewards Trade-offs in Cyber Security[C]. *Proceedings of the 29th Annual ACM Symposium on Applied Computing - SAC '14*, 2014: 1649-1656.

[10] A. Davis, T. Leek, M. Zhivich, et al. The Fun and Future of CTF[C]. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, 2014:156-162.

[11] G. Vigna, K. Borgolte, J. Corbetta, et al. Ten Years of iCTF: The Good, The Bad, and The Ugly[C]. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, 2014:135-142.

[12] E. Trickel, F. Disperati, E. Gustafson, et al. Shell We Play A Game? CTF-as-a-service for Security Education[C]. *USENIX Workshop on Advances in Security Education (ASE)*, 2017:45-52.

[13] NetKotH. https://netkoth.github.io/.

[14] Z. Schreuders, T .Shaw, M.Shan-A-Khuda. Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting {CTF} Events[C]. *USENIX Workshop on Advances in Security Education (ASE)*, 2017:35-46.

[15] C.E. Irvine, M.F. Thompson, M. McCarrin et al. Live Lesson: Labtainers: A Docker-based Framework for Cybersecurity Labs[C]. *USENIX Workshop on Advances in Security Education (ASE)*, 2017:65-72.

[16] Langner R. Stuxnet: Dissecting a Cyberwarfare Weapon[J]. *IEEE Security & Privacy Magazine*, 2011, 9(3): 49-51.

[17] How Do Threat Actors Move Deeper Into your Network? Micro TREND, http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf.

[18] A LOCKHEED MARTIN OVERVIEW. https://www. lockheed-martin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[19] MITRE ATT&CK, https://attack.mitre.org/.

[20] Penetration Testing Execution Standard (PTES), http://www. pentest-standard.org/index.php/Main_Page.

[21] Connect the dots, https://en.wikipedia.org/wiki/Connect_the_dots.

[22] Wu J Y. Research on key Technologies of Network Security Risk Assessment[D]. Beijing: Beijing University of Posts and Telecom, 2013.(吴金宇. 网络安全风险评估关键技术研究[D]. 北京: 北京邮电大学, 2013.)

[23] X.M. Ou, S. Govindavajhala, A. W. Appel. MulVAL: A Logic-based Network Security Analyzer[C]. *USENIX Security Symposium*. 2005:26-35.

[24] Ou X M, Boyer W F, McQueen M A. A Scalable Approach to Attack Graph Generation[C]. *the 13th ACM conference on Computer and communications security - CCS '06*, 2006: 336-345.

[25] Ou X M, Singhal A. Attack Graph Techniques[M]. Quantitative Security Risk Assessment of Enterprise Networks. New York, NY: Springer New York, 2011: 5-8.

[26] Ou X M, Singhal A. Security Risk Analysis of Enterprise Networks Using Attack Graphs[M]. Quantitative Security Risk Assessment of Enterprise Networks. New York, NY: Springer New York, 2011: 13-23.

[27] CVSS-v30-specification-v1.7. Common Vulnerability Scoring System v3.0 specification Document, FIRST. Retrived from, 2015.

[28] Programming in Logic (Prolog), https://en.wikibooks.org/wiki/Prolog.

[29] B. Ferguson, A. Tall, D. Olsen. National cyber range overview[C]. *IEEE Trans. Military Communications Conference (MILCOM)*, 2014: 123-128.

[30] Fang B X, Jia Y, Li A P, et al. Cyber Ranges: State-of-the-art and Research Challenges[J]. *Journal of Cyber Security*, 2016, 1(3): 1-9. (方滨兴, 贾焰, 李爱平, 等. 网络空间靶场技术研究[J]. *信息安全学报*, 2016, 1(3): 1-9.)

[31] T. Benzel, B. Braden, T. Faber, et al. Current developments in DETER cybersecurity testbed technology[C]. *IEEE. Conference for Homeland security, Cybersecurity applications & technology (CATCH)*.2009: 57-70.

[32] J. Mirkovic, T.V. Benzel, T. Faber, et al. The DETER project: Advancing the science of cyber security experimentation and test[C]. *IEEE International Conference on Technologies for Homeland Security (HST)*, 2010: 1-7.

[33] Cheng J, Lei J, Yuan X F. Construction and Development of National Cyber Range[J]. *Journal of China Academy of Electronics and Information Technology*, 2014, 9(5): 446-452. (程静, 雷璟, 袁雪芬. 国家网络靶场的建设与发展[J]. *中国电子科学研究院学报*, 2014, 9(5): 446-452.)

[34] Linstone, H. A., Turoff, M. The delphi method[M]. Addison-Wesley, 1975: 3-12.

[35] Saaty T L. Decision Making with the Analytic Hierarchy Process[J]. *International Journal of Services Sciences*, 2008, 1(1): 83-93.

[36] ECharts, https://ecomfe.github.io/echarts-doc/public/en/index.html.

[37] Zhang X, Liu B X, Gong X R, et al. State-of-the-Art: Security Competition in Talent Education[M]. Information Security and Cryptology. Cham: Springer International Publishing, 2018: 461-481.

[38] Cyber Grand Challenge rules, https://dtsn.darpa.mil/cybergrand-challenge/CyberGrandChallenge_Rules_v1.pdf.

[39] Social engineering definition, https://en.oxforddictionaries.com/definition/social_engineering.

[40] VulnHub, Vulnerable By Design, https://www.vulnhub.com/.

[41] Newhouse W, Keith S, Scribner B, et al. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework[R]. National Institute of Standards and Technology, 2017.

[42] O'Neil L R, Assante M, Tobey D. Smart Grid Cybersecurity: Job Performance Model Report[R]. Office of Scientific and Technical Information (OSTI), 2012.

[43] CTFtime.org / All about CTF (Capture The Flag), https://ctftime.org/.

[44] Pwn2Own, http://zerodayinitiative.com/Pwn2Own2017Rules.html.

[45] GeekPwn, http://2017.geekpwn.org/en/index.html.

[46] W.M. Petullo, K. Moses, B. Klimkowski, et al. The Use of Cyber-Defense Exercises in Undergraduate Computing Education[C]. *USENIX Workshop on Advances in Security Education (ASE)*. 2016:125-134.

[47] White G B, Williams D, Harrison K. The CyberPatriot National High School Cyber Defense Competition[J]. *IEEE Security & Privacy Magazine*, 2010, 8(5): 59-61.

[48] Carlin A, Manson D, Zhu J. Developing the Cyber Defenders of tomorrow with Regional Collegiate Cyber Defense Competitions (CCDC)[C]. 2008, 25:23-31.

[49] You are invited to the National's first Cyber-Physical System(CPS) based Cyber Defense Competition(CDC), http://www.iserink.org/wp-content/uploads/2015/12/2016-CPS_CDC_invite.pdf.

[50] Munaiah N, Pelletier J, Su S H, et al. A Cybersecurity Dataset Derived from the National Collegiate Penetration Testing Competition[C]. *HICSS Symposium on Cybersecurity Big Data Analytics*. 2019:265-274.

[51] Bock K, Hughey G, Levin D. King of the hill: A novel cybersecurity competition for teaching penetration testing[C]. *USENIX Workshop on Advances in Security Education (ASE)*. 2018:267-271.

[52] F. Araujo, M. Shapouri, S. Pandey et al. Experiences with honey-patching in active cyber security education[C]. *USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, 2015:234-241.

[53] P. Chapman, J. Burket, D. Brumley. PicoCTF: A Game-Based Computer Security Competition for High School Students[C]. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, 2014:295-302.

[54] Cyber Grand Challenge, https://www.darpa.mil/news-events/2016-08-05a.

[55] Robot Human Game (RHG), https://baijia.baidu.com/s?id=1579206335113948331&wfr=pc&fr=_lst.

[56] R. Raman, S. Sunny, V. Pavithran et al. Framework for evaluating Capture the Flag (CTF) security competitions[C]. *IEEE International Conference for Convergence of Technology (I2CT)*, 2014: 1-5.

[57] P. Pusey, D.H. Tobey, R. Soule et al. An Argument for Game Balance: Improving Student Engagement by Matching Difficulty Level with Learner Readiness[C]. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*. 2014:264-274.

[58] Metasploitable3, https://blog.rapid7.com/2016/11/15/test-your-might-with-the-shiny-new-metasploitable3/.

[59] Metasploit Vulnerable Service Emulator, https://blog.rapid7.com/2017/03/02/vulnerable-service-emulator/.

[60] Vulhub, Make vulnerability environments easier, https://vulhub.org/.

[61] J. Burket, P. Chapman, T. Becker, et al. Automatic Problem Generation for Capture-the-Flag Competitions[C]. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE')*, 2015:368-374.

[62] Denning T, Lerner A, Shostack A, et al. Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education[C]. the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13, 2013: 915-928.

[63] T. Denning, A. Shostack, T. Kohno. Practical Lessons from Creating the Control-Alt-Hack Card Game and Research Challenges for Games In Education and Research[C]. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, 2014: 654-662.

[64] A. Shostack. Elevation of Privilege: Drawing Developers into Threat Modeling[C]. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, 2014:857-862.

[65] M. Gondree, Z.N.J. Peterson. Valuing Security by Getting [d0x3d!][C]. *USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, 2013:568-578.

[66] M.F. Thompson, C.E. Irvine. CyberCIEGE Scenario Design and Implementation[C]. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, 2014:654-662.

[67] M. Olano, A.T. Sherman, L. Oliva et al. SecurityEmpire: Development and Evaluation of a Digital Game to Promote Cybersecurity Education[C]. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, 2014:26-35.

[68] R. Ensafi, M. Jacobi, J.R. Crandall. A Case Study in Helping Students to Covertly Eat Their Classmates[C]. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, 2014:458-462.

[69] J.Mirkovic, P.Peterson. Class Capture-the-Flag Exercises[C]. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, 2014:65-72.

[70] W.L. Du, Z. Teng, R. Wang. SEED: a suite of instructional laboratories for computer SEcurity Education[J]. *ACM SIGCSE Bulletin. ACM*, 2007, 39(1): 486-490.

[71] SEED project, http://www.cis.syr.edu/~wedu/ seed/.

[72] iChunQiu, https://www.ichunqiu.com/.

[73] Deterding S, Dixon D, Khaled R, et al. From Game Design Elements to Gamefulness: Defining "Gamification"[C]. *Proceedings of the 15th International Academic MindTrek Conference on Envisioning Future Media Environments - MindTrek '11*, 2011: 9-15.

[74] A. Ruef, M. Hicks, J. Parker, et al. Build it break it: Measuring and comparing development security[C]. *USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, 2015:89-96.

[75] Ruef A, Hicks M, Parker J, et al. Build It, Break It, Fix It: Contesting Secure Development[C]. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016: 690-703.

[76] Votipka D, Fulton K R, Parker J, et al. Understanding security mistakes developers make: Qualitative analysis from build it, break it, fix it[C]. *USENIX Security Symposium* 2020:58-67.

[77] Y. Shoshitaishvili, R.Y. Wang, C. Salls, et al. Sok:(state of) the art of war: Offensive techniques in binary analysis[C]. *IEEE Symposium on Security and Privacy (S&P)*,2016: 138-157.

[78] Stephens N, Grosen J, Salls C, et al. Driller: Augmenting Fuzzing through Selective Symbolic Execution[C]. *Proceedings 2016 Network and Distributed System Security Symposium*, 2016: 1-16.

[79] Shoshitaishvili Y, Weissbacher M, Dresel L, et al. Rise of the HaCRS: Augmenting Autonomous Cyber Reasoning Systems with Human Assistance[C]. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017: 347-362.

[80] T. Bao, R.Y. Wang, Y. Shoshitaishvili, et al. Your Exploit is Mine: Automatic Shellcode Transplant for Remote Exploits[C]. *IEEE Symposium on Security and Privacy (S&P)*, 2017:56-68.

[81] E. Nunes, P. Shakarian, G.I. Simari, et al. Argumentation models for cyber attribution[C]. *IEEE/ACM International Conference on Social Networks Analysis and Mining (ASONAM)*, 2016: 837-844.

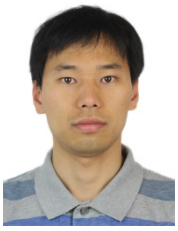
[82] M.N. Hossain, S.M. Milajerdi, J. Wang, et al. SLEUTH: Real-time Attack Scenario Reconstruction from COTS Audit Data[C]. *USENIX Security Symposium,* 2017:369-375

章秀 于 2013 年在华中科技大学获得学士学位。现在中国科学院信息工程研究所攻读博士学位。研究领域为网络安全领域人才培养和能力评估, 研究兴趣包括攻防场景、安全竞赛等。Email: zhangxiu@iie.ac.cn

刘宝旭 于 2002 年在中国科学院研究生院获得博士学位。现任中国科学院信息工程研究所研究员。第六研究室主任。研究领域为网络安全攻防对抗、网络安全评测技术等。Email: liubaoxu@iie.ac.cn

龚晓锐 于 2014 年在北京大学获得硕士学位。现任中国科学院信息工程研究所正高级工程师。研究领域为攻防对抗。研究兴趣包括移动互联网安全、网络安全攻防对抗。Email: gongxiaorui@iie.ac.cn

于磊 于 2013 年在山东科技大学获得电子与通信工程硕士学位, 现在中国科学院信息工程研究所攻读博士学位。研究领域为攻防对抗。研究兴趣包括: 漏洞挖掘、网络安全等。Email: yulei@iie.ac.cn



宋振宇 于 2013 年在意大利都灵理工大学获得博士学位。现任中国科学院信息工程研究所高级工程师。研究领域为网络安全。研究兴趣包括信息安全、网络安全靶场等。Email: songzhenyu@iie.ac.cn